MASARYKOVA UNIVERZITA

# Matematika drsně a svižně

Jan Slovák, Martin Panák, Michal Bulant
a kolektiv

Brno 2013

Projekt netradiční základní učebnice matematiky pro studenty přírodních věd, informatiky, technických věd, ekonomie, sociálních věd apod., přibližující podstatnou část matematiky v rozsahu čtyř semestrálních přednášek. Práce na učebnici byly podpořeny projektem Univerzitní výuka matematiky v měnícím se světě (CZ.1.07/2.2.00/15.0203).




**Autorský kolektiv:**
Mgr. Michal Bulant, Ph.D.
Mgr. Aleš Návrat, Dr. rer. nat.
Mgr. Martin Panák, Ph.D.
prof. RNDr. Jan Slovák, DrSc.
RNDr. Michal Veselý, Ph.D.

**Grafický návrh publikace a ilustrace:**
Mgr. Petra Rychlá

© 2013 Masarykova univerzita

ISBN 978-80-210-6307-5
ISBN 978-80-210-6308-2 (online : pdf)
DOI:10.5817/CZ.MUNI.O210-6308-2013

# Obsah


Kapitola 1. Rozcvička 6
1. Čísla a funkce 6
2. Kombinatorické veličiny 10
3. Diferenční rovnice 14
4. Pravděpodobnost 17
5. Geometrie v rovině 26
6. Relace a zobrazení 38

Kapitola 2. Počítání s vektory 65
1. Vektory a matice 65
2. Determinanty 76
3. Vektorové prostory a lineární zobrazení 84
4. Vlastnosti lineárních zobrazení 100

Kapitola 3. Lineární modely a maticový počet 123
1. Lineární procesy 123
2. Diferenční rovnice 129
3. Iterované lineární procesy 136
4. Více maticového počtu 144
5. Rozklady matic a pseudoinverze 163

Kapitola 4. Analytická geometrie 191
1. Afinní a euklidovská geometrie 191
2. Geometrie kvadratických forem 210
3. Projektivní geometrie 218

Kapitola 5. Zřízení ZOO funkcí 234
1. Interpolace polynomy 234
2. Reálná čísla a limitní procesy 243
3. Derivace 261
4. Mocninné řady 273

Kapitola 6. Diferenciální a integrální počet 325
1. Derivování 325
2. Integrování 341
3. Nekonečné řady 360

Kapitola 7. Spojité modely 396
1. Fourierovy řady 396
2. Metrické prostory 408
3. Integrální operátory 424

Kapitola 8. Spojité modely s více proměnnými 435
1. Funkce a zobrazení na $\mathbb{R}^n$ 435
2. Integrování podruhé 465
3. Diferenciální rovnice 487

Kapitola 9. Statistické a pravděpodobnostní metody 523
1. Popisná statistika 523
2. Pravděpodobnost 532
3. Matematická statistika 570

Kapitola 10. Teorie čísel 589
1. Základní pojmy 589
2. Prvočísla 593
3. Kongruence 599
4. Řešení kongruencí a jejich soustav 610
5. Aplikace – počítání s velkými čísly, kryptografie 623

Kapitola 11. Algebraické struktury 641
1. Grupy 641
2. Okruhy polynomů 656
3. Systémy polynomiálních rovnic 668
4. Uspořádané množiny a Booleovská algebra 685
5. Kódování 697

Kapitola 12. Kombinatorické metody, grafy a algoritmy 708
1. Grafy a algoritmy 708
2. Příklady využití grafových technik 734
3. Kombinatorické výpočty 747

# Předmluva

Příprava tohoto učebního textu byla motivována přednáškami pro informatické obory na Masarykově univerzitě. Studijní programy jsou tam založeny na precizním matematickém přístupu. Chtěli jsme proto rychle, ale zároveň pořádně, pokrýt zhruba tolik matematiky, jako je obvyklé u větších kurzů v klasických technických oborech opřených o matematické metody. Zároveň jsme ale nechtěli rezignovat na úplný a matematicky korektní výklad. Chtěli jsme vedle sebe vyložit i obtížnější partie matematiky a spoustu elementárních i náročnějších konkrétních příkladů, jak s uvedenými postupy ve skutečnosti pracovat. Nechtěli jsme přitom za čtenáře řešit, v jakém pořadí a kolik „teorie“ či „praxe“ pročítat.

Z těchto podnětů vznikl dvousloupcový formát s oddělenými teoretickými úvahami a praktickými postupy. Snažíme se tím vyjít vstříc jak čtenářům, kteří si napřed chtějí procvičit postupy při řešení úloh a teprve pak přemýšlet, proč a jak algoritmy fungují, tak těm druhým, kteří si napřed chtějí dělat jasno o tom proč a jak věci fungují a pak případně zkouší řešit konkrétní příklady. Zároveň tím čtenáře nutíme, aby se sami rozhodli o pořadí i rozsahu toho, co chtějí číst, a snad je zbavujeme i stresu, že by měli přečíst úplně vše. Naopak, měli by mít radost z brouzdání textem a prožitku objevování vlastní cestičky k matematickému příběhu.

Text se v obou svých částech snaží prezentovat standardní výklad matematiky s akcentem na smysl a obsah představovaných matematických metod. Řešené úlohy procvičují základní pojmy, ale zároveň obsahují i komplexnější příklady užití matematických modelů.

Teoretický text je prezentován dosti kompaktním způsobem, mnoho prostoru je ponecháno pro dotažení podrobností čtenáři. Uváděné příklady se snaží pokrýt celou škálu složitosti, od velmi jednoduchých až po perličky ke skutečnému přemýšlení.

Čtenářům bychom rádi pomohli:

- přesně formulovat definice základních pojmů a dokazovat jednoduchá matematická tvrzení,
- vnímat obsah i přibližně formulovaných závislostí, vlastností a výhledů použití matematických nástrojů,
- vstřebat návody na užívání matematických modelů a osvojit si jejich využití.

K těmto ambiciózním cílům nelze dojít lehce a pro většinu lidí to znamená hledat si vlastní cestu s tápáním různými směry (s potřebným překonáváním odporu či nechuti). I proto je celý výklad strukturován tak, aby se pojmy a postupy vždy několikrát vracely s postupně rostoucí složitostí a šíří diskuse. Jsme si vědomi, že se tento postup může jevit jako chaotický. Domníváme se ale, že dává mnohem lepší šanci na pochopení u těch, kteří vytrvají.

Vstup do matematiky je skoro pro každého obtížný — pokud už „rozumíme“, nechce se nám přemýšlet o podrobnostech, pokud „nerozumíme“, je to ještě horší. Jediný spolehlivý postup pro orientaci v matematice je hledat porozumění v mnoha pokusech, a to pokud možno při četbě v různých zdrojích a přemýšlení o souvislostech. Určitě nepovažujeme tento text za dostatečný jediný zdroj pro každého. Doufáme, že může být dobrým začátkem a případně i dlouhodobým pomocníkem zvláště pro ty, kdo se k jednotlivým částem budou znovu a znovu vracet.

Pro ulehčení vícekolového přístupu ke čtení je text doprovázen emotivně laděnými ikonkami, které snad nejen oživí obvyklou strohou strukturu matematického textu, ale naznačí čtenáři, kde by složitější text měl být čten pozorněji, ale určitě ne přeskakován, případně kde by bylo možná lépe náročné pasáže přinejmenším napoprvé vůbec nečíst.

Volba jednotlivých ikonek samozřejmě odráží hlavně pocity a představy autorů. Měly by být přesto dobrým vodítkem pro jednotlivé čtenáře, kteří si sami postupně vytvoří jejich význam. Sloupec zaměřený na výklad teorie (užší a hustší sloupec) a sloupec zaměřující se na příkladovou část jsou přitom opatřeny odlišnými sadami ikonek. Co se týče sloupce teorie, používáme ikonky varující před pracností/složitostí/náročností, např.



Další označují ne úplně pohodovou zdlouhavost práce a potřebu trpělivosti či nadhledu při pročítání následujících odstavců:



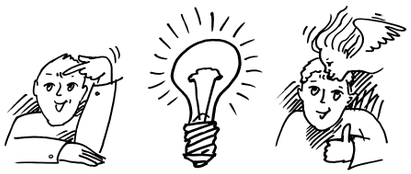
A konečně máme také ikonky vyjadřující pohodu nebo radost ze hry, třeba následující



Co se týče příkladového sloupce, tak používáme ikonky



pro základní příklady, které by čtenář rozhodně měl být schopen zvládnout a pokračovat ve čtení až po jejich vyřešení, ikonky



pro obtížnější příklady se zajímavým obratem, či praktickou aplikací, ikonka



značí velmi obtížný příklad a konečně ikonka



indikuje, že při řešení příkladu je vhodné použít výpočetní software.

Snažili jsme se sloupce s příklady sepsat tak, aby byly čitelné prakticky samostatně. Bez ambicí pochopit hlubší důvody, proč uváděné postupy fungují (nebo s prostým cílem „projít písemkou“), by mělo skoro stačit probírat se jen příklady. To ale neznamená, že by bylo možné je číst bezmyšlenkovitě a postupy jen mechanicky kopírovat. I v řešených příkladech počítáme s aktivní spoluprací čtenářů, kteří si většinou sami musí rozmyslet, jak uvedené řešení funguje a co se vlastně přesně dělá.

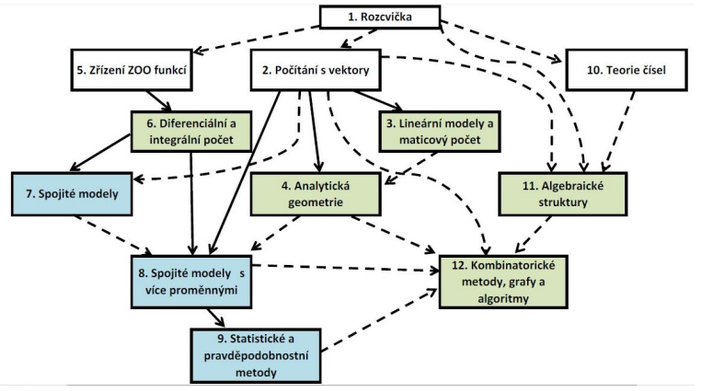
Definice pojmů či popisy jejich vlastností používaných při řešení příkladů jsou v teoretickém sloupci často vyznačeny zatržením, aby o ně bylo možno snadno pohledem zavadit. Souvislost řešených příkladů s paralelně studovanou teorií je přitom spíše volná, snažili jsme ale ulehčit přeskakování „z praxe do teorie a zpět“ co nejvíce.

Obsahově je celá učebnice ovlivněna představou, že pro praktické využití jsou velmi podstatné metody tzv. diskrétní matematiky, zatímco tzv. spojité modely jsou matematicky dobře uchopitelná přiblížení veskrze diskrétního světa kolem nás. Počítat koneckonců stejně umíme vždy jen s konečně mnoha racionálními čísly naráz. Bez spojité matematiky si ale lze jen těžko dobře představit koncepty jako konvergence procesu k limitnímu stavu nebo robustnost výpočtu. Bylo by bez ní také obtížné pracovat s odhady chyb při numerických procesech.

Všechna témata a velmi podstatnou část textu jsme v létech 2005–2013 postupně ověřovali při výuce studentů informatiky a později i matematiky na Masarykově univerzitě. Paralelně jsme přitom vytvořili také podklady pro praktické semináře matematického modelování a numerických metod. V nich se studenti věnují skutečnému využití výpočtových nástrojů a modelů.

Celá učebnice plně pokrývá témata odpřednášená ve čtyřech semestrálních kurzech matematiky, a to v plné verzi se čtyřmi hodinami přednášek doplněnými dvěma hodinami cvičení týdně. V prvním semestru jsme odpřednášeli kapitoly 1 a 2 a výběr z kapitol 3 a 4. V dalším semestru pak byly odpřednášeny kapitoly 5 a 6 a částečně i kapitola 7. Třetí semestr je věnován podstatné části kapitol 8 a 9 a na čtvrtý semestr pak zbýval výběr z kapitol 10–12, přičemž ale teorie grafů byla již dříve přednášena v jiných informatických předmětech.

Samozřejmě předpokládáme, že si čtenáři a přednášející vyberou témata a jejich pořadí sami. Následující obrázek naznačuje bloky, se kterými lze takto nezávisle zacházet.




Bez vážných problémů s návaznostmi považujeme za možné začít druhou, pátou nebo desátou kapitolou, přičemž úvodní rozcvička bude více či méně užitečná pro všechny případy. Tučné šipky v obrázku naznačují podstatné závislosti, čárkovanými označujeme přímou závislost nebo alespoň doporučený postup pro některé části kapitol.

Kapitoly 11 a 12 jsou tedy do značné míry nezávislé na zbytku, naopak části náročnějších kapitol 3, 4, 7, 8, 9 se patrně do základních kurzů matematiky vůbec nevejdou. Prakticky v libovolném pořadí, resp. paralelně lze přednášet bloky kapitol 1–4, 5–6, případně i 10–12 (nebo jejich části). Naopak hodně závislé na některých předchozích částech jsou kapitoly 7–9.

Úvodní motivační kapitola se snaží ilustrovat několik přístupů k matematickému popisu problémů. Považujeme ji skutečně za rozcvičku, kterou začínáme nejjednoduššími funkcemi (základní *kombinatorické vzorce*). Pak naznačujeme, jak pracovat se závislostmi zadanými pomocí okamžitých změn (jednoduché *diferenční rovnice*), užití kombinatoriky a množinové algebry diskutujeme prostřednictvím konečné klasické *pravděpodobnosti*. Předvádíme maticový počet pro jednoduché úlohy rovinné geometrie (práce s pojmem *pozice* a *transformace*) a závěrem vše trochu zformalizujeme (*relace, uspořádání, ekvivalence*). Nenechte se zde uvrhnout do chaotického zmatku rychlým střídáním témat — cílem je nashromáždit něco málo netriviálních námětů k přemýšlení a hledání jejich souvislostí i použití, ještě než zabředneme do úrovně problémů a teorií složitějších. Ke všem tématům této úvodní kapitoly se časem vrátíme.

Další dvě kapitoly jsou věnovány základům počtu, který umožňuje práci s vícerozměrnými daty i grafikou. Jde o postupy tzv. *lineární algebry*, které jsou základem a konečným výpočetním nástrojem pro většinu matematických modelů. Nejprve probíráme jednoduché postupy pro práci s *vektory a maticemi*, třetí kapitola je pak věnována aplikacím maticového počtu v různých lineárních modelech (*systémy lineárních rovnic, lineární procesy, lineární diferenční rovnice, Markovovy procesy, lineární regrese*). Čtvrtá kapitola pak ilustruje použití maticového počtu v geometrických úlohách. Dozvíme se něco málo o *afinní, euklidovské a projektivní geometrii*.

V tomto okamžiku přerušíme v textu diskusi diskrétních modelů a přejdeme ke spojitým. Ukazujeme, že pracovat i se složitými funkcemi bývá jednoduché. Stručně řečeno, velmi jednoduché úvahy spojené s popisem okamžitých změn sledovaných veličin umožňují dělat závěry pro jejich vlastnosti

lokálně i globálně. Složitosti se pojí skoro výhradně se zvládnutím rozumně velké třídy funkcí, pro které mají naše postupy být použitelné.

Začínáme proto kapitolou, kde diskutujeme jaké funkce potřebujeme pro nelineární modely. Po *polynomech a splajnech* postupně diskutujeme pojmy *kontinuum reálných čísel*, *spojitost*, *limity posloupností a funkcí* a *derivace funkcí*, připomeneme všechny základní *elementární funkce* a závěrem se seznámíme s *mocninnými řadami*. Tím je připravena půda pro klasický diferenciální a integrální počet. Ten prezentujeme v kapitole šesté s důrazem na co nejpřímočařejší pochopení souvislostí *limitních procesů*, *integrace* a *aproximací*.

Sedmá kapitola se věnuje náznakům aplikací a snaží se co nejvíce připomínat analogie k postupům jednoduché lineární algebry. Místo lineárních zobrazení mezi konečně rozměrnými vektorovými prostory tak pracujeme s lineárními operacemi mezi vektorovými prostory funkcí. Ty bývají definovány buď integrálními nebo diferenciálními operátory. Zatímco diskusi diferenciální rovnic necháváme na později, zde studujeme nejprve aproximace funkcí s pomocí vzdálenosti definované integrálem (tzv. *Fourierovy řady*). Pak se věnujeme základům tzv. *Fourierovy analýzy*, tj. souvislostem s některými integrálními operátory (např. *konvoluce*) a integrálními transformacemi (zejména *Fourierova transformace*). Po cestě nahlédneme na abstraktní pojem vzdálenosti v kontextu *metrických prostorů* a neodpustíme si ilustrace obecného principu, že spojité modely jsou zpravidla ideovým podkladem a zároveň dobrou aproximací pro modely diskrétní. Poslouží nám k tomu stručné nahlédnutí na problematiky tzv. *waveletů* a *diskrétní Fourierovy transformace*.

V osmé kapitole pokračujeme v našem stručném nastínění analytických spojitých metod, tentokrát pro modely s více proměnnými veličinami. Nejprve rozšíříme základní postupy a výsledky týkající se derivací na *funkce více proměnných*, včetně *funkcí zadaných implicitně* a tzv. *vázaných extrémů*. Hned poté rozšíříme teorii integrování o tzv. násobné integrály a obecné integrování po křivkách, plochách apod., včetně výkladu obecné Stokesovy věty. Tuto pasáž je možné vnímat jako stručné nastínění základů tzv. globální analýzy. Poté se věnujeme modelům opřeným o známou okamžitou změnu našich objektů, tj. *diferenciálním rovnicím*.

Devátá kapitola je věnována popisné statistice, pravděpodobnosti a matematické statistice. Po stručném přiblížení terminologie a metod popisné statistiky se seznámíme s pojmy *pravděpodobnostní prostor, náhodná veličina, hustota pravděpodobnosti, střední hodnota náhodné veličiny, medián, kvantil, rozptyl*. Potkáme přitom příklady prakticky důležitých diskrétních a spojitých rozdělení a budeme se náznakem věnovat *statistickému zpracování dat*, tj. výběrovým statistikám a jejich spolehlivosti, včetně stručných náznaků rozdílů mezi klasickým frekvenčním a bayesovským přístupem.

V další kapitole zamíříme zpět do světa diskrétních metod. Zabýváme se v ní elementární teorií čísel. Po zavedení základní terminologie a symboliky se spolu s řešením hravých teoretických úloh poměrně rychle snažíme dospět k tomu, jaké praktické úlohy teorie čísel pomáhá řešit a se kterými (vyřešenými i otevřenými) problémy se tyto úlohy pojí. V závěrečných pasážích kapitoly jsou stručně zmíněny výpočetní aspekty teorie čísel a základní postupy v kryptografii s veřejným klíčem.

Předposlední kapitola se věnuje nejprve obecným algebraickým strukturám s důrazem na elementární poznatky z teorie grup a okruhů polynomů. Jako příklady použití jsou zmíněny základní metody počítačové algebry, zejména použití *Gröbnerových bází* při eliminaci proměnných v polynomiálních systémech rovnic. Zmíníme i něco málo o *uspořádáních, svazech a boolovských algebrách* a závěrem uvádíme aplikace algebraických metod při *kódování dat*.

Úplně poslední kapitola se vrací k diskrétní matematice z jiného pohledu. Je věnována základním pojmům a poznatkům teorie grafů a jejich využitím v praktických problémech (např. prohledávání do šířky a hloubky, *minimální pokrývající kostry*, *toky v sítích*, *hry popisované stromy*). V závěru kapitoly jsou také studovány některé další problémy a postupy související s kombinatorickými výpočty (zejména se vracíme k řešení rekurentních rovnic ve chvíli, kdy díky spolupráci spojitých a diskrétních metod můžeme využít *vytvořující funkce*, které se ukazují být v této situaci docela silným nástrojem).

**Použitá literatura.** Jak je u učebnic obvyklé, původní je koncepce celkového uspořádání textu a výběr a kombinace obecných témat. Autoři přitom čerpali z mnoha zdrojů, často jistě i podvědomně, a nečiní si nároky na autorství žádných výsledků či použitých postupů při jejich důkazech.

Několik učebnic výrazně ovlivnilo již přípravu přednášek, ze kterých tento text vznikal. Byly to zejména následující zdroje:

K.F. Riley, M.P. Hobson, S.J. Bence, *Mathematical Methods for Physics and Engineering*, second edition, Cambridge University Press, Cambridge 2004, ISBN 0-521-89067-5, xxiii+1232 s.
William J. Gilbert, W. Keith Nicholson, *Modern algebra with applications*, 2nd ed. John Wiley and Sons (Pure and applied mathematics), 2004, ISBN 0-471-41451-4, xvii+330 s.
J. Herman, R. Kučera, J. Šimša, *Metody řešení matematických úloh I*, Brno: Masarykova univerzita, 2011. 278 s. ISBN 978-80-210-5636-7.
J. Herman, R. Kučera, J. Šimša, *Metody řešení matematických úloh II*, Brno: Masarykova univerzita, 1997. 355 s. ISBN 80-210-1630-2.
Paul. J. Nahin, *When Least is Best*, Princeton University Press, 2004, ISBN-13:978-0-691-13052-1, 370 s.
Jiří Matoušek, Jaroslav Nešetřil, *Kapitoly z diskrétní matematiky*, Univerzita Karlova v Praze, Karolinum, Praha, 2000, ISBN 80-246-0084-6, 377 s.
Karel Zvára, Josef Štěpán, Pravděpodobnost a matematická statistika, Matfyzpress, Universita Karlova, 2006, ISBN 80-85863-93-6, 230 s.

Občas jsou v textu přebírány teoretické pasáže nebo příklady z dalších zdrojů a v takových případech uvádíme odkazy formou poznámek pod čarou.

**Poděkování.** Na vzniku učebního textu se podílel velmi široký tým spolupracovníků, vyučujících i studentů. Za celkovou koncepci a rozpracování jsou ale zodpovědní tři hlavní autoři – Jan Slovák, Martin Panák a Michal Bulant. Zatímco prvně jmenovaný má na svědomí celkový koncept učebnice a je autorem převážné většiny teoretických částí textu, Martin Panák s podporou širšího autorského kolektivu sestavil drtivou většinu příkladů. Michal Bulant vytvořil zejména celou desátou kapitolu a podstatné části kapitoly poslední.

Na vyhledávání a rozpracování mnoha set praktických úloh v jednotlivých kapitolách (celkem přes 1600 úloh, z toho přes 1000 řešených) se významně podíleli také Aleš Návrat a Michal Veselý.

Celkové grafické řešení knihy, včetně všech ilustrací, je dílem Petry Rychlé.

Za to, že se knihu podařilo vysázet v netradičním dvousloupcovém formátu, který si autoři vymysleli, vděčíme Tomáši Janouškovi, který se také o sazbu učebnice skoro vzorně staral. Za úpravy textu vděčíme také Karolíně Malé a Monice Stančíkové, které nám hodně pomohly v závěrečné fázi tvorby textů.

Nezanedbatelně obsahově i koncepčně přispěli Zdeněk Pospíšil, Lenka Přibylová, Jiří Zelinka a poděkování patří i Gabrielu Harangimu a Ottovi Suchánkovi za poskytnutí zpracovaných příkladů.

Podrobnému čtení a komentování částí textu se věnovali Roman Šimon Hilscher, Lenka Přibylová, Zdeněk Pospíšil, Jiří Zelinka, Matej Hajnal, Lukáš Vokřínek, Ondřej Klíma, Petr Pupík, Milan Werl, Jana Soukopová. Mnoho chyb, nešikovností a nedostatků se podařilo odstranit jejich zásluhou a patří jim vřelý dík autorů.

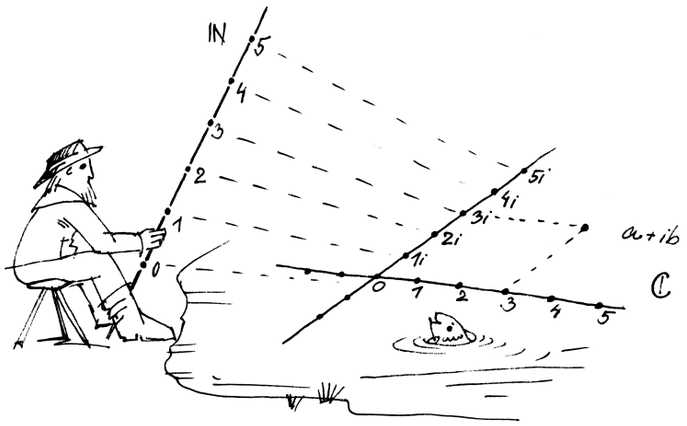
Za ty chyby a nedodělky, co zůstaly, si ale mohou autoři sami. Budeme čtenářům vděčni za všechna upozornění, na jejichž základě budeme občas vylepšovat elektronickou verzi učebního textu na stránkách projektu, s jehož podporou text vznikl, viz `www.math.muni.cz/Matematika_drsne_svizne`.

19. srpna 2013, Jan Slovák, Martin Panák, Michal Bulant

KAPITOLA 1

# Rozcvička

*„hodnota, změna, poloha“*
*– co to je a jak to uchopit?*




## A. Čísla a funkce

S přirozenými, celými, racionálními a reálnými čísly již počítat umíme. Zamyslíme se, proč racionální čísla nestačí (byť v počítači s jinými doopravdy počítat neumíme) a připomeneme si tzv. čísla komplexní (protože ani s reálnými čísly si při výpočtech nevystačíme).

**1.1.** Najděte nějaké reálné číslo, které není racionální.

**Řešení.** Jedna z mnoha možných odpovědí je $\sqrt{2}$. Již staří Řekové věděli, že předepíšeme-li plochu čtverce $a^2 = 2$, pak nelze najít racionální $a$, které by předpisu vyhovovalo. Proč?

Víme, že každé přirozené číslo $n$ lze jednoznačným způsobem vyjádřit jako součin $n = p_1^{r_1} \cdot p_2^{r_2} \dots p_k^{r_k}$, až na pořadí v součinu, kde $p_1, \dots, p_k$ jsou po dvou různá prvočísla.

Pokud by tedy platilo $(p/q)^2 = 2$ pro přirozená čísla $p$ a $q$, pak tedy $p^2 = 2q^2$. Na levé straně máme v rozkladu na prvočísla $2^r$ se sudým $r$ (případně $r = 0$), na pravé straně ale bude vždy mocnina dvojky lichá. To je spor s naším tvrzením a tedy předpoklad nemůže platit a žádné racionální číslo nemůže mít za svoji druhou mocninu dvojku. □

Cílem první kapitoly je uvést čtenáře do fascinujícího světa matematického myšlení. Vybíráme si k tomu co nejkonkrétnější příklady modelování reálných situací pomocí abstraktních objektů a souvislostí. Zároveň projdeme několik témat a postupů, ke kterým se postupně budeme vracet a v závěru kapitoly se budeme chvíli věnovat samotnému jazyku matematiky (se kterým budeme jinak zacházet spíše intuitivně).

O co jednodušší jsou východiska a objekty, se kterými zde budeme pracovat, o to složitější je pochopit do důsledku jemnosti použitých nástrojů a postupů. Většinou je možné proniknout k podstatě věcí teprve v jejich souvislostech. Proto je také představujeme hned z několika pohledů zároveň.

Přecházení od tématu k tématu se možná bude zdát jako zmatečné, ale to se jistě postupně spraví při našich návratech k jednotlivým úvahám a pojmům v pozdějších kapitolách.

Název kapitoly lze chápat i jako nabádání k trpělivosti. I nejjednodušší úlohy a úvahy budou snadné jen pro ty, kteří už podobné řešili. K postupnému poznání a ovládnutí matematického myšlení vede jen pozvolná a spletitá cesta.

Začneme s tím nejjednodušším: obyčejnými čísly.

### 1. Čísla a funkce



Lidé odjakživa chtějí mít jasno, „kolik“ něčeho je, případně „za kolik“ to je, „jak dlouho“ něco trvá apod. Výsledkem takových úvah je většinou nějaké „číslo“. Za číslo přitom považujeme něco, co umíme sčítat a násobit a splňuje to obvyklé zákonitosti, ať už všechny nebo jen některé. Například výsledek sčítání nezávisí na pořadí, v jakém čísla sčítáme. Máme k dispozici číslo nula, které přičtením výsledek nezmění, číslo jedna, kterým můžeme násobit, aniž bychom změnili výsledek, apod.

Nejjednodušším příkladem jsou tzv. čísla přirozená, budeme je značit $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. Všimněme si, že jsme mezi přirozená čísla vzali i nulu, jak je obvyklé zvláště v informatice.

Počítat „jedna, dvě, tři, …“ se učí děti už ve školce. O něco později se setkáváme s čísly celými $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ a nakonec si zvykneme na desetinná čísla a víme, co znamená 1,19-násobek ceny díky 19% dani z přidané hodnoty.

**1.1. Vlastnosti čísel.** Abychom mohli s čísly pracovat opravdu,



musíme se jejich definici a vlastnostem věnovat pořádněji. V matematice se těm základním tvrzením o vlastnostech objektů, jejichž platnost předpokládáme, aniž bychom se zabývali jejich dokazováním,

**1.2. Poznámka.** Lze dokonce dokázat, že odmocnina přirozeného stupně z přirozeného čísla je buď přirozená, nebo není racionální (viz ‖1.95‖).

**1.3.** Najděte řešení rovnice $x^2 = b$ pro libovolné reálné číslo $b$.

**Řešení.** Víme, že tato rovnice má vždy řešení $x$ v oboru reálných čísel, pokud je $b$ nezáporné. Jestliže je $b = -1$, pak ale zjevně takové reálné $x$ existovat nemůže. Musíme proto najít větší obor čísel, ve kterém už řešení existovat bude.

K reálným číslům nejprve přidáme nové číslo $i$, tzv. *imaginární jednotku* a zkusíme dodefinovat sčítání a násobení tak, abychom i nadále zajistili obvyklé chování čísel, jak je shrnuto v odstavci 1.1.

Jistě musíme umět nové číslo $i$ násobit reálnými čísly a výsledky sčítat s jakýmikoliv reálnými čísly. Nutně proto musíme v novém číselném oboru *komplexních čísel* $\mathbb{C}$ pracovat s formálními výrazy $z = a + i\,b$.

Aby byly splněny vlastnosti asociativity a distributivity, zavedeme sčítání tak, že se nezávisle sčítají reálné složky a imaginární složky. Stejně tak chceme násobení tak, jak by se násobily dvojčleny reálných čísel s jediným dodatečným pravidlem $i^2 = -1$, tj.

$$(a + i\,b) + (c + i\,d) = (a + c) + i\,(b + d),$$
$$(a + i\,b) \cdot (c + i\,d) = (ac - bd) + i\,(bc + ad).$$

□

Reálnému číslu $a$ říkáme *reálná složka* komplexního čísla $z$, reálnému číslu $b$ pak *imaginární složka* komplexního čísla $z$, píšeme $\mathrm{re}(z) = a$, $\mathrm{im}(z) = b$.

**1.4.** Ověřte, že skutečně platí všechny vlastnosti (KG1–KG4), (O1–O4) a (P) skalárů z 1.1.

**Řešení.** Nulou je číslo $0 + i\,0$, jedničkou číslo $1 + i\,0$, obě tato čísla pro jednoduchost opět píšeme jako 0 a 1. Všechny vlastnosti se ověří přímočarým výpočtem. □

Komplexní číslo je dáno dvojicí reálných čísel, jde tedy o bod v reálné rovině $\mathbb{R}^2$.

**1.5.** Ukažte, že vzdálenost komplexního čísla $z = a + i\,b$ od počátku (značíme ji $|z|$) je dána výrazem $z\bar{z}$, kde $\bar{z}$ je *komplexně sdružené číslo* $a - i\,b$.

**Řešení.** Součin

$$z\bar{z} = (a^2 + b^2) + i\,(-ab + ba) = a^2 + b^2$$

je vždy reálné číslo a dává nám skutečně kvadrát vzdálenosti čísla $z$ od počátku 0. Platí tedy $|z|^2 = z\bar{z}$. □

říká *axiomy*. Vhodná volba axiomů předurčuje jak dosah z nich vycházející teorie, tak její použitelnost v matematických modelech skutečnosti.

Uveďme si teď základní vlastnosti operací sčítání a násobení pro naše počty s čísly, která píšeme jako písmena $a, b, c, \ldots$. Obě tyto operace fungují tak, že vezmeme dvě čísla $a$, $b$ a aplikací sčítání nebo násobení dostaneme výsledné hodnoty $a + b$ a $a \cdot b$.

VLASTNOSTI SKALÁRŮ

**Vlastnosti sčítání:**

(KG1) $(a + b) + c = a + (b + c)$, pro všechna $a, b, c$

(KG2) $a + b = b + a$, pro všechna $a, b$

(KG3) existuje číslo 0 tak, že pro všechna $a$ platí $a + 0 = a$

(KG4) pro všechna $a$ existuje $b$ takové, že $a + b = 0$

Vlastnostem (KG1)–(KG4) říkáme vlastnosti *komutativní grupy*. Jsou to po řadě *asociativita*, *komutativita*, *existence neutrálního prvku* (říkáme u sčítání také nulového prvku), *existence inverzního prvku* (říkáme u sčítání také opačného prvku k $a$ a značíme ho $-a$).

**Vlastnosti násobení:**

(O1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, pro všechna $a, b, c$

(O2) $a \cdot b = b \cdot a$, pro všechna $a, b$

(O3) existuje číslo 1 tak, že pro všechna $a$ platí $1 \cdot a = a$

(O4) $a \cdot (b + c) = a \cdot b + a \cdot c$, pro všechna $a, b, c$

Vlastnosti (O1)–(O4) se postupně nazývají *asociativita*, *komutativita*, existence *jednotkového prvku* a *distributivita* sčítání vůči násobení.

Množiny s operacemi $+$, $\cdot$ a vlastnostmi (KG1)–(KG4), (O1)–(O4) se nazývají *komutativní okruhy*.

Další vlastnosti násobení:

(P) pro každé $a \neq 0$ existuje $b$ takové, že $a \cdot b = 1$.

(OI) je-li $a \cdot b = 0$, potom buď $a = 0$ nebo $b = 0$.

Vlastnost (P) se nazývá existence *inverzního prvku* vzhledem k násobení (tento prvek se pak značí $a^{-1}$) a vlastnost (OI) říká, že neexistují „dělitelé nuly“.



Vlastnosti těchto operací sčítání a násobení budeme soustavně využívat, aniž bychom museli přesně vědět, s jakými objekty skutečně pracujeme. Tak se dostaneme k obecným matematickým nástrojům, je však vždy dobré mít představu o typických příkladech.

Celá čísla $\mathbb{Z}$ jsou dobrým příkladem komutativní grupy, přirozená čísla nikoliv, protože nesplňují (KG4) (a případně neobsahují neutrální prvek, pokud někdo nulu do $\mathbb{N}$ nezahrnuje).

Když komutativní okruh navíc splňuje i vlastnost (P), hovoříme o *poli* (často také o *komutativním tělese*).

Poslední uvedená vlastnost (OI) je automaticky splněna, pokud platí (P). Opačně to ovšem neplatí a tak říkáme, že vlastnost (OI) je slabší než (P). Např. okruh celých čísel $\mathbb{Z}$ nesplňuje (P), ale splňuje (OI). Hovoříme v takovém případě o *oboru integrity*.

Všimněme si, že množina všech nenulových prvků v poli společně s operací násobení splňuje (O1), (O2), (O3), (P), a je proto také komutativní grupa. Jen se místo sčítání mluví o násobení. Jako příklad můžeme vzít všechna nenulová reálná čísla.

**1.6. Poznámka.** Vzdálenost $|z|$ nazýváme též absolutní hodnotou komplexního čísla $z$.

**1.7. Goniometrický tvar komplexního čísla.** Nejprve uvažme komplexní čísla tvaru $z = \cos\varphi + i\,\sin\varphi$, kde $\varphi$ je reálný parametr udávající úhel mezi reálnou přímkou a spojnicí $z$ s počátkem (měřený v kladném smyslu). Tato čísla popisují právě všechny body na jednotkové kružnici v komplexní rovině. Každé nenulové číslo $z$ pak lze právě jedním způsobem napsat jako

$$z = |z|(\cos\varphi + i\,\sin\varphi).$$

Číslu $\varphi$ říkáme argument komplexního čísla $z$.

**1.8. Násobení komplexních čísel v goniometrickém tvaru.** Mějme dána čísla $z_1 = |z_1|\,(\cos\varphi_1 + i\,\sin\varphi_1)$ a $z_2 = |z_2|\,(\cos\varphi_2 + i\,\sin\varphi_2)$, a upravujme jejich součin:

$$\begin{aligned} z_1 \cdot z_2 &= |z_1|\,(\cos\varphi_1 + i\,\sin\varphi_1)\cdot|z_2|\,(\cos\varphi_2 + i\,\sin\varphi_2) = \\ &= |z_1||z_2|\big[\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + \\ &\quad + i\,(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)\big] = \\ &= |z_1||z_2|\,[\cos(\varphi_1+\varphi_2) + i\,\sin(\varphi_1+\varphi_2)]\,, \end{aligned}$$

kde poslední rovnost je důsledkem součtových vzorců pro goniometrické funkce. Opakovanou aplikací předchozího vztahu na součin čísla $z$ sama se sebou dostáváme tzv. „Moivreovu větu“:

$$z^n = [|z|(\cos\varphi + i\,\sin\varphi)]^n = |z|^n(\cos(n\varphi) + i\,\sin(n\varphi)).$$

**1.9.** Vyjádřete číslo $z_1 = 2 + 3\,i$ v goniometrickém tvaru a naopak číslo $z_2 = 3(\cos(\pi/3) + i\,\sin(\pi/3))$ v algebraickém tvaru.

**Řešení.** Absolutní hodnota daného čísla (vzdálenost bodu s kartézskými souřadnicemi $[2,3]$ v rovině od počátku souřadnic) je $\sqrt{2^2+3^2} = \sqrt{13}$. Z pravoúhlého trojúhelníka v obrázku pak snadno spočteme $\sin(\varphi) = 3/\sqrt{13}$, $\cos(\varphi) = 2/\sqrt{13}$. Je tedy $\varphi = \arcsin(3/\sqrt{13}) = \arccos(2/\sqrt{13}) \doteq 53{,}3°$. Celkem

$$\begin{aligned} z_1 &= \sqrt{13}\left(\frac{2}{\sqrt{13}} + i\,\frac{3}{\sqrt{13}}\right) = \\ &= \sqrt{13}\left[\cos\left(\arccos\frac{2}{\sqrt{13}}\right) + i\,\sin\left(\arcsin\frac{3}{\sqrt{13}}\right)\right]. \end{aligned}$$

Převod komplexního čísla z goniometrického do algebraického tvaru je ještě jednodušší:

$$z_2 = 3\left(\cos\frac{\pi}{3} + i\,\sin\frac{\pi}{3}\right) = 3\left(\frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right) = \frac{3}{2} + i\,\frac{3\sqrt{3}}{2}\,. \quad \square$$

Prvky nějaké množiny s operacemi $+$ a $\cdot$ splňujícími (ne nutně všechny) výše uvedené vlastnosti (tj. komutativní okruh, obor integrity, pole) budeme nazývat *skaláry*. Budeme pro ně vesměs užívat malá latinská písmena ze začátku nebo konce abecedy.

Všechny vlastnosti (KG1)–(KG4), (O1)–(O4), (P), (OI) z našich úvah je třeba brát jako *axiomatickou definici* příslušných matematických pojmů. Pro naše potřeby bude stačit si průběžně uvědomovat, že při dalších diskusích budeme důsledně používat pouze tyto vlastnosti skalárů a že i naše výsledky proto budou platné pro všechny objekty s těmito vlastnostmi.

V tomto je pravá síla matematických teorií – nejsou platné jen pro konkrétní řešený příklad. Naopak, při rozumné výstavbě mají vždy univerzální použití. Budeme se snažit tento aspekt zdůrazňovat, přestože naše ambice mohou být v rámci daného rozsahu učebnice jen velice skromné.

**1.2. Existence skalárů.**  K tomu, aby ale skutečně bylo možné budovat matematickou teorii, je třeba ověřit, že takové objekty mohou existovat. Pro pořádek si proto budeme postupně ukazovat, jak je možné zkonstruovat základní číselné obory. Pro konstrukci přirozených čísel začneme s předpokladem, že víme, co jsou to množiny.

Prázdnou množinu si označíme $\emptyset$ a definujeme

$$0 := \emptyset, \quad n+1 := n \cup \{n\}, \tag{1.1}$$

neboli

$$0 := \emptyset,\ 1 := \{\emptyset\},\ 2 := \{0,1\},\ \ldots,\ n+1 := \{0,1,\ldots,n\}.$$

Tímto zápisem říkáme, že pokud už máme definovaná všechna čísla $0, 1, 2, \ldots n$, pak číslo $n+1$ definujeme jako množinu všech předchozích (tj. již definovaných) čísel.

Přirozená čísla takto ztotožňujeme s počty prvků konkrétních množin. Číslo $n$ je množina, která má $n$ prvků a dvě přirozená čísla $a$, $b$ jsou stejná, právě když příslušné množiny mají stejně mnoho prvků. V teorii množin se místo slovního spojení „počet prvků množiny“ používá pojem „mohutnost množiny“. Tento pojem má smysl (na rozdíl od toho předchozího) i pro nekonečné množiny.

Na první pohled je také vidět obvyklá definice uspořádání přirozených čísel podle velikosti (o číslu $a$ řekneme, že je ostře menší než $b$ tehdy a jen tehdy, když $a \neq b$ a $a \subseteq b$ jako množina). Dalším formálním krokem by měla být definice sčítání a násobení a důkaz všech základních vlastností přirozených čísel, včetně výše uvedených axiomů komutativního okruhu. Snadno lze např. ukázat, že každá podmnožina v $\mathbb{N}$ má nejmenší prvek a spoustu dalších vlastností, o kterých zpravidla už dávno nepřemýšlíme a máme je za samozřejmé.

Nebudeme se tu konstrukcí číselných oborů zabývat podrobně a předpokládáme, že čtenář čísla racionální ($\mathbb{Q}$), reálná ($\mathbb{R}$) a komplexní ($\mathbb{C}$) důvěrně zná. Při dalším výkladu budeme občas jen připomínat teoretické i praktické souvislosti. Podrobně bude konstrukce racionálních čísel z přirozených diskutována v 1.40. Konstrukci reálných čísel bude vhodné zmínit při studiu limitních procesů později a již dříve budeme z různých algebraických pohledů zkoumat čísla komplexní. Titulní obrázek kapitoly naznačuje, jak je možné vnímat číselné obory jako vnořené jeden do druhého (tj. komplexní rovina obsahuje mnohokrát vložená přirozená nebo celá čísla, reálnou přímku atd.).

**1.10.** Vyjádřete $z = \cos 0 + \cos\frac{\pi}{3} + i\ \sin\frac{\pi}{3}$ v goniometrickém tvaru.

**Řešení.** Pro vyjádření čísla $z$ v goniometrickém tvaru potřebujeme zjistit jeho absolutní hodnotu a argument. Nejprve určeme absolutní hodnotu:

$$|z| = \sqrt{\left(\cos 0 + \cos\tfrac{\pi}{3}\right)^2 + (\sin\tfrac{\pi}{3})^2} = \sqrt{\left(1+\tfrac{1}{2}\right)^2 + \left(\tfrac{\sqrt{3}}{2}\right)^2} = \sqrt{3}.$$

Nyní pro argument $\varphi$ platí:

$$\cos\varphi = \frac{\mathrm{re}(z)}{|z|} = \frac{1+\frac{1}{2}}{\sqrt{3}} = \frac{\sqrt{3}}{2}, \quad \sin\varphi = \frac{\mathrm{im}(z)}{|z|} = \frac{1}{2},$$

tedy $\varphi = \pi/6$. Celkem jsme tak získali

$$z = \sqrt{3}\left(\cos\frac{\pi}{6} + i\ \sin\frac{\pi}{6}\right). \qquad \square$$

**1.11.** Pomocí Moivreovy věty vypočítejte

$$\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)^{31}.$$

**Řešení.** Ihned dostáváme

$$\left(\cos\frac{\pi}{6} + i\ \sin\frac{\pi}{6}\right)^{31} = \cos\frac{31\pi}{6} + i\ \sin\frac{31\pi}{6} =$$
$$= \cos\frac{7\pi}{6} + i\ \sin\frac{7\pi}{6} = -\frac{\sqrt{3}}{2} - i\,\frac{1}{2}\,. \qquad \square$$

**1.12.** Zjednodušte $\dfrac{1+i}{2+i}$.

**Řešení.** Zjednodušením rozumíme zejména odstranění komplexních čísel ze jmenovatele zlomku. Zlomek proto rozšíříme komplexně sdruženým výrazem ke jmenovateli (tím dostaneme ve jmenovateli reálné číslo):

$$\frac{1+i}{2+i} = \frac{(1+i)(2-i)}{(2+i)(2-i)} = \frac{3+i}{5}. \qquad \square$$

Další příklady pro osvojení základních vlastností komplexních čísel viz ‖1.96‖ a následující příklady.

**1.13.** Komplexní čísla nejsou pouze nástrojem, abychom získali „divná“ řešení kvadratických rovnic, ale jsou potřeba i k tomu, abychom určili reálná řešení kubických rovnic. Jak vyjádřit řešení kubické rovnice

$$x^3 + ax^2 + bx + c = 0$$

pomocí reálných koeficientů $a$, $b$, $c$? Ukažme si metodu, na kterou přišli v šestnáctém století pánové Ferro, Cardano, Tartaglia a možná další. Zaveďme substituci $x := t - a/3$ (abychom odstranili kvadratický člen v rovnici), dostaneme rovnici:

$$t^3 + pt + q = 0,$$

kde $p = b - a^2/3$ a $q = c + (2a^3 - 9ab)/27$. Nyní zaveďme neznámé $u$, $v$ splňující podmínky $u + v = t$ a $3uv + p = 0$. Dosazením první

Navíc, jak je v matematice obvyklé, budeme místo s čísly manipulovat s písmeny abecedy, případně jinými znaky, ať už jejich hodnota je nebo není předem známá.

**1.3. Skalární funkce.** Často pracujeme s číselnou hodnotou, která není dána jako konkrétní číslo. Místo toho něco víme o závislosti naší hodnoty na hodnotách jiných. Formálně píšeme, že hodnota $y = f(x)$ naší „závislé“ proměnné veličiny $y$ je dána „nezávislou“ veličinou $x$. Přitom můžeme znalost $f$ brát formálně (prostě je to nějaká, blíže nespecifikovaná, závislost) nebo operačně, tj. $f(x)$ je dáno vzorcem poskládaným z (prozatím si představme konečně mnoha) známých operací. Pokud je hodnotou skalár, hovoříme o *skalární funkci*. Každá funkce je definována na nějaké množině, mluvíme o *definičním oboru funkce*, a množina všech hodnot je pak tzv. *obor hodnot funkce*.



Také mohou být ale hodnoty funkce $f$ dány pouze přibližně nebo s jistou pravděpodobností.

Smyslem matematických úvah pak bývá z neformálního popisu závislostí najít explicitní vzorce pro funkce, které je popisují, nebo aspoň explicitní vyjádření pro konkrétní hodnoty závislých proměnných, případně jejich přiblížení. Podle typu úlohy a cíle pracujeme:

- s přesným a konečným výrazem
- s nekonečným výrazem
- s přiblížením neznámé funkce známým odhadem (většinou s vyčíslenou možnou chybou)
- s odhadem hodnot s vyčíslením jejich pravděpodobnosti apod.

Skalární funkcí je např. roční mzda pracovníka nějaké firmy (hodnoty nezávislé veličiny, tj. definiční obor funkce, jsou jednotliví pracovníci $x$ z množiny všech sledovaných pracovníků, $f(x)$ je jejich roční mzda za dané období). Stejně tak můžeme sledovat měsíční mzdu konkrétního pracovníka v čase (nezávislou hodnotou je čas v měsících, závislou příjem v jednom každém měsíci). Jiným příkladem je třeba plocha obrazce v rovině, objem tělesa v prostoru, rychlost konkrétního auta v čase atd. Dovedeme si jistě představit, že ve všech uvedených případech může být hodnota dána nějakou volně popsanou souvislostí nebo naměřena přibližně nebo odhadnuta atd.

**1.4. Operačně definované funkce.** Funkce můžeme mít dány výčtem jejich hodnot – např. ve firmě je jen konečně mnoho zaměstnanců a umíme sestavit tabulku s jejich aktuálními měsíčními platy. Častěji ale máme místo hodnot pravidla, jak k hodnotám dojít.



FUNKCE FAKTORIÁL

Důležitou skalární funkcí na přirozených číslech je *faktoriál*, který definujeme vztahy

$$f(0) = 1,\ f(n) = n \cdot f(n-1)$$

pro $n = 1, 2, \ldots$. Píšeme $f(n) = n!$ a definice zjevně znamená

$$n! = n \cdot (n-1) \cdot \ldots \cdot 1.$$

podmínky do původní rovnice dostáváme

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0,$$

dosazením druhé pak

$$u^6 + qu^3 - \frac{p^3}{27} = 0,$$

což je kvadratická rovnice v neznámé $s = u^3$. Máme tedy

$$u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Celkem pak zpětným dosazením

$$x = -p/3u + u - a/3. \tag{1.1}$$

Ve výrazu pro $u$ se vyskytuje třetí odmocnina. Abychom dostali všechna tři řešení, je nutno pracovat i s komplexními odmocninami. Rovnice $x^3 = a, a \neq 0$, s neznámou $x$ má totiž právě tři řešení v oboru komplexních čísel (Základní věta algebry, viz (11.20)). Všechna tato řešení nazýváme třetí odmocninou z čísla $a$. Je tedy výraz $\sqrt[3]{a}$ v komplexním oboru trojznačný. Pokud se chce přisoudit výrazu $\sqrt[3]{a}$ jednoznačný význam, pak se za třetí odmocninu uvažuje řešení s nejmenším argumentem.

Navíc ještě dodejme, že při popsaném postupu se mohlo vyskytnout dělení nulou. V tom případě je nutno použít jiného (většinou snadnějšího) postupu.

**1.14.** Řešte rovnici

$$x^3 + x^2 - 2x - 1 = 0.$$

**Řešení.** Jak snadno zjistíme, tak rovnice nemá racionální kořeny Dosazením do získaných vztahů získáme $p = b - a^2/3 = -7/3$, $q = -7/27$, pro $u$ pak dostáváme

$$u = \frac{\sqrt[3]{28 \pm 12\sqrt{-147}}}{6},$$

kde můžeme teoreticky volit až šest možností pro $u$ (dvě volby znaménka plus či mínus a k tomu tři nezávislé volby třetí odmocniny). Jak však snadno nahlédneme, dostáváme pro $x$ pouze tři různé hodnoty. Dosazením do (‖1.1‖) pak jeden z kořenů má tvar

$$\frac{14}{\sqrt[3]{3(28 - 84i\sqrt{3})}} + \frac{\sqrt[3]{28 - 84i\sqrt{3}}}{6} - \frac{1}{3} \doteq 1{,}247.$$

Obdobně pro ostatní dva kořeny (přibližně $-0{,}445$ a $-1{,}802$). Jak jsme předeslali, vidíme, že i když se ve vzorcích pro kořeny vyskytují komplexní čísla, tak výsledek je reálný. □

Naše definice funkce faktoriál říká, jak se změní hodnota $f(n)$, když změníme hodnotu $n$ o jedničku. Vzorec pro $n!$ již explicitně říká, kolik to je doopravdy. V tomto případě to není příliš efektivní vzorec, protože se jeho složitost zvětšuje s rostoucím $n$, lepší ale těžko hledat.

Podívejme se ještě na obyčejné sčítání přirozených čísel jako na operačně definovanou skalární funkci. Definičním oborem je množina všech dvojic $(a, b)$ přirozených čísel. Definujeme $a + b$ jako výsledek procedury, ve které k $a$ několikrát po sobě přičítáme 1. Tak jsme vlastně obecně $a + 1$ definovali v rovnicích (1.1). Při každém přičtení odebereme z $b$ největší prvek a postupujeme tak, dokud není $b$ prázdná (tj. $b$ se postupně zmenšuje o jedničku a v každém kroku nám říká, kolik ještě zbývá přičíst).

Je evidentní, že takto definované sčítání sice je dáno (iterativním) vzorcem, postup ale není vhodný pro praktické počítání. Tak tomu bude v našem výkladu často – teoreticky korektní definice pojmu či operace neznamená, že úkony s nimi spojené jsou efektivně vykonavatelné. Právě k tomu budeme postupně rozvíjet celé teorie, abychom praktické nástroje získávali. Co se týče přirozených čísel, od školky je umíme sčítat zpaměti a rychle (pokud jsou malá), pro větší známe ze základní školy algoritmus písemného sčítání a s velkými si poradí počítače (pokud nejsou příliš velká).

### 2. Kombinatorické veličiny



Typickým „kombinatorickým“ problémem je napočítat, kolika různými způsoby se může něco stát. Např. kolika způsoby lze vybrat v samoobsluze dva různé sendviče z dané nabídky? Myslíme si přitom, že jsou všechny sendviče v regálu po dvou různé nebo rozlišujeme jen různé typy sendvičů? Připouštíme pak, že si také můžeme vzít dva stejné? Nepřeberně takových otázek máme u karetních a jiných her.

Pravidlo součtu a součinu

Při řešení konkrétních problémů většinou používáme buď tzv. „pravidlo součinu“, kdy v navzájem nezávislých úkonech kombinujeme každý výsledek s každým, nebo „pravidlo součtu“, kdy sčítáme počty pro různé neslučitelné možnosti.

Prakticky to uvidíme v mnoha příkladech.

**1.5. Permutace.** Jestliže z množiny $n$ předmětů vytváříme nějaké pořadí jejich prvků, máme pro volbu prvního prvku $n$ možností, další je volen z $n - 1$ možností atd., až nám nakonec zbude jediný poslední prvek. Zjevně tedy je na dané konečné množině $S$ s $n$ prvky právě $n!$ různých pořadí. Procesu uspořádávání prvků množiny $S$ říkáme *permutace* prvků množiny $S$. Výsledkem permutace je pak vždy nějaké pořadí prvků. Jestliže si předem prvky v $S$ očíslujeme, tj. ztotožníme si $S$ s množinou $S = \{1, \ldots, n\}$, která má $n$ přirozených čísel, pak permutace odpovídají možným pořadím čísel od jedné do $n$. Máme tedy příklad jednoduché matematické věty a naši předchozí diskusi je možné považovat za její důkaz:

Počet permutací

**Tvrzení.** *Počet $p(n)$ různých pořadí na konečné množině s $n$ prvky je dán známou funkcí faktoriál:*

$$p(n) = n! \tag{1.2}$$

## B. Kombinatorika

V této kapitole si budeme hrát s přirozenými čísly, která budou popisovat různé nedělitelné předměty nacházející se v našem životním prostoru a budeme se zabývat tím, jak spočítat počet jejich uspořádání, přeuspořádání, výběrů a tak podobně. Ve velké většině takovýchto problémů lze vystačit se „selským rozumem“. Stačí vhodně používat pravidel *součtu* a *součinu*, která si ukážeme na následujících příkladech:

**1.15.** Maminka chce Jeníkovi a Mařence rozdělit pět hrušek a šest jablek. Kolika způsoby to může udělat? (Hrušky mezi sebou považujeme za nerozlišitelné, stejně tak jablka. Připouštíme, že některé z dětí nic nedostane.)

**Řešení.** Pět hrušek samostatně může maminka rozdělit šesti způsoby. (Rozdělení je určeno tím, kolik hrušek dá Jeníkovi, zbytek připadne Mařence.) Šest jablek pak nezávisle sedmi způsoby. Podle pravidla součinu pak obě ovoce současně může rozdělit $6 \cdot 7 = 42$ způsoby. □

**1.16.** Určete počet čtyřciferných čísel, která začínají cifrou 1 a nekončí cifrou 2, nebo končí cifrou 2 a nezačínají cifrou 1.

**Řešení.** Množina uvažovaných čísel je složená ze dvou disjunktních množin, totiž čísel, která začínají cifrou 1 a nekončí cifrou 2 (první množina) a čísel, která nezačínají cifrou 1 a končí cifrou 2. Celkový počet popsaných čísel dostaneme podle pravidla součtu tak, že sečteme počty čísel v těchto dvou množinách. V první z těchto množin máme čísla tvaru „1XXY“, kde $X$ je libovolná cifra a $Y$ je libovolná cifra mimo dvojky. Můžeme tedy provést deset voleb druhé cifry, nezávisle na tom můžeme provést deset voleb třetí cifry a opět nezávisle devět voleb poslední cifry. Tyto tři nezávislé volby jednoznačně určují dané číslo a podle pravidla součinu máme tedy $10 \cdot 10 \cdot 9 = 900$ takových čísel. Obdobně ve druhé skupině máme $8 \cdot 10 \cdot 10 = 800$ čísel (na první cifru máme pouze osm možností, neboť číslo nemůže začínat nulou a jedničku máme zakázánu). Celkem podle pravidla součtu je $900 + 800 = 1700$ uvažovaných čísel. □

**1.17.** Určete počet způsobů, jak lze na šachovnici ($8 \times 8$ polí) postavit bílou a černou věž tak, aby se neohrožovaly (nebyly ve stejném řádku ani sloupci).

**Řešení.** Nejprve umístíme např. bílou věž. Pro ni máme na výběr z $8^2$ polí. Ve druhém kroku umístíme věž černou. Nyní máme „k dispozici“ $7^2$ polí. Podle pravidla součinu je výsledek $8^2 \cdot 7^2 = 3\,136$.

□

V následujících příkladech už budeme při řešení používat pojmů kombinace, permutace, variace (případně s opakováním), které jsme definovali v odstavcích 1.5 a 1.6 teoretického sloupce.

**1.6. Kombinace a variace.** Dalším jednoduchým příkladem



hodnoty určené vzorcem jsou tzv. *kombinační čísla*, která vyjadřují, kolika způsoby lze vybrat $k$ různých rozlišitelných předmětů z množiny $n$ předmětů. Zjevně máme

$$n(n-1)\cdots(n-k+1)$$

možných výsledků postupného výběru našich $k$ prvků, přitom ale stejnou výslednou $k$–tici dostaneme v $k!$ různých pořadích. Pokud nám záleží i na pořadí vybrané $k$-tice prvků, hovoříme o *$k$-prvkové variaci*.

Jak jsme si právě ověřili, počet kombinací a variací udávají následující vzorce, které také nejsou pro výpočet moc efektivní při velikých $k$ a $n$, protože obsahují výrazy pro faktoriály.

KOMBINACE A VARIACE

**Tvrzení.** *Pro počet $c(n,k)$ $k$-prvkových kombinací z $n$ prvků, kde $0 \le k \le n$, platí*

$$c(n,k) = \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1} = \frac{n!}{(n-k)!k!}. \tag{1.3}$$

*Pro počet $v(n,k)$ variací platí*

$$v(n,k) = n(n-1)\dots(n-k+1) \tag{1.4}$$

*pro všechna $0 \le k \le n$ (a nula jinak).*

Kombinační číslo $\binom{n}{k}$ čteme „$n$ nad $k$“ a nazýváme ho také někdy *binomickým číslem*. Tento název čísla dostala od tzv. *binomického rozvoje*, tj. roznásobení $n$-té mocniny dvojčlenu. Počítáme-li totiž $(a+b)^n$, bude koeficient u mocniny $a^k b^{n-k}$ pro každé $0 \le k \le n$ roven právě počtu možností, jak vybrat $k$–tici z $n$ závorek v součinu (ty, kde bereme do výsledku $a$). Platí proto

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}. \tag{1.5}$$

Všimněme si, že pro odvození jsme potřebovali pouze distributivitu, komutativitu a asociativitu násobení a sčítání. Formule (1.5) proto platí v každém komutativním okruhu.

Jako další jednoduchou ukázku, jak vypadá matematický důkaz, si odvoďme několik jednoduchých tvrzení o kombinačních číslech. Pro zjednodušení formulací definujme $\binom{n}{k} = 0$, kdykoliv je buď $k < 0$ nebo $k > n$.

**1.7. Tvrzení.** *Pro všechna přirozená čísla $k$ a $n$ platí*

*(1)* $\binom{n}{k} = \binom{n}{n-k}$,
*(2)* $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$,
*(3)* $\sum_{k=0}^{n} \binom{n}{k} = 2^n$,
*(4)* $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$.

DŮKAZ. První tvrzení je zjevné přímo z formule (1.3). Jestliže vyčíslíme pravou stranu z tvrzení (2), dostáváme

$$\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} = \frac{(k+1)n! + (n-k)n!}{(k+1)!(n-k)!} = \frac{(n+1)!}{(k+1)!(n-k)!},$$

**1.18.** Během schůze má vystoupit 8 řečníků. Stanovte počet všech pořadí, v nichž dva předem určení řečníci nevystupují ihned po sobě.

**Řešení.** Označme si zmíněné dva řečníky jako osoby $A$ a $B$. Pokud hned po vystoupení osoby $A$ následuje vystoupení osoby $B$, můžeme na to nahlížet jako na projev jediného řečníka. Počet všech pořadí, v nichž vystupuje $B$ ihned po $A$, je tedy roven počtu všech permutací ze sedmi prvků. Stejný je pochopitelně také počet všech pořadí, v nichž vystupuje $A$ ihned po $B$. Neboť počet všech možných pořadí 8 řečníků je 8!, číslo $8! - 2 \cdot 7!$ udává hledaný počet pořadí. □

**1.19.** Kolik existuje přesmyček slova PROBLÉM takových, že v nich

a) písmena B a R stojí vedle sebe,

b) písmena B a R nestojí vedle sebe.

**Řešení.** a) Dvojici písmen B a R můžeme považovat za jedno nedělitelné dvojpísmeno. Celkem tedy máme k dispozici šest různých písmen a šestipísmenných slov složených z různých písmen je 6!. V našem případě však tento počet musíme ještě vynásobit dvěma, neboť naše dvojpísmeno může být jak BR tak RB. Celkem dostáváme $2 \cdot 6!$ různých přesmyček.

b) $7! - 2 \cdot 6!$ (doplněk části a) do počtu všech sedmipísmenných slov složených z různých písmen). □

**1.20.** Kolika způsoby může sportovec umístit 10 různých pohárů do 5 polic, jestliže se na každou polici vejde všech 10 pohárů?

**Řešení.** K pohárům přidáme 4 navzájem nerozlišitelné předměty, kupř. tužky. Počet všech různých pořadí pohárů a tužek je zřejmě 14!/4! (tužky jsou nerozlišitelné). Každé umístění pohárů do polic ovšem odpovídá právě jednomu seřazení pohárů a tužek. Stačí třeba říci, že poháry před první tužkou v pořadí dáme do první police (při zachování pořadí), poháry před druhou tužkou do druhé police atd. To znamená, že číslo 14!/4! je výsledkem. □

**1.21.** Určete počet čtyřciferných čísel sestavených z právě dvou různých cifer.

**Řešení.** Dvě různé cifry použité na zápis můžeme vybrat $\binom{10}{2}$ způsoby, ze dvou vybraných cifer můžeme sestavit $2^4 - 2$ různých čtyřciferných čísel (dvojku odečítáme za dvě čísla složená pouze z jedné cifry). Celkem máme $\binom{10}{2}(2^4 - 2) = 630$ čísel. Nyní jsme ale započítali i čísla začínající nulou, těch je $\binom{9}{1}(2^3 - 1) = 63$. Celkově dostáváme $630 - 63 = 567$ čísel. □

**1.22.** Určete počet sudých čtyřciferných čísel sestavených z právě dvou různých cifer.

což je ale levá strana tohoto tvrzení.

Tvrzení (3) dokážeme tzv. *matematickou indukcí*. Tento typ



důkazu je vhodný právě pro tvrzení, která říkají, že něco má platit pro všechna přirozená čísla $n$. Matematická indukce se skládá ze dvou kroků. V prvním se tvrzení dokáže pro $n = 0$ (popřípadě $n = 1$ nebo další hodnoty $n$). V druhém, tzv. indukčním, kroku předpokládáme, že tvrzení platí pro nějaké $n$ (a všechny předešlé hodnoty), a za pomoci tohoto předpokladu dokážeme, že tvrzení platí i pro $n + 1$. Dohromady z toho pak vyvodíme, že tvrzení platí pro všechna přirozená $n$.

Tvrzení (3) zjevně platí pro $n = 0$, protože $\binom{0}{0} = 1 = 2^0$. (Stejně tak je přímo vidět i pro $n = 1$.) Předpokládejme, že platí pro nějaké $n$ a spočtěme příslušnou sumu pro $n + 1$ s využitím tvrzení (2) i (3). Dostaneme

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = \sum_{k=0}^{n+1} \left[ \binom{n}{k-1} + \binom{n}{k} \right] =$$

$$= \sum_{k=-1}^{n} \binom{n}{k} + \sum_{k=0}^{n+1} \binom{n}{k} = 2^n + 2^n = 2^{n+1}.$$

Všimněme si, že vzorec (3) udává počet všech podmnožin $n$–prvkové množiny, neboť $\binom{n}{k}$ je počet všech jejích $k$–prvkových podmnožin. Všimněme si také, že tvrzení (3) plyne přímo z (1.5) volbou $a = b = 1$.

Tvrzení (4) dokážeme opět matematickou indukcí, podobně jako (3). Zjevně platí pro $n = 0$, čímž je hotov první krok. Indukční předpoklad říká, že (4) platí pro nějaké $n$. Spočtěme nyní příslušnou sumu pro $n + 1$ s využitím tvrzení (2) a indukčního předpokladu. Dostaneme

$$\sum_{k=0}^{n+1} k\binom{n+1}{k} = \sum_{k=0}^{n+1} k \left[ \binom{n}{k-1} + \binom{n}{k} \right] =$$

$$= \sum_{k=-1}^{n} (k+1)\binom{n}{k} + \sum_{k=0}^{n+1} k\binom{n}{k} =$$

$$= \sum_{k=0}^{n} \binom{n}{k} + \sum_{k=0}^{n} k\binom{n}{k} + \sum_{k=0}^{n} k\binom{n}{k} =$$

$$= 2^n + n2^{n-1} + n2^{n-1} = (n+1)2^n.$$

Tím je proveden indukční krok a tvrzení je dokázáno pro všechna přirozená $n$. □

Druhá vlastnost z našeho tvrzení umožňuje sestavit všechna kombinační čísla do tzv. *Pascalova trojúhelníku*, kde každé číslo obdržíme jako součet dvou bezprostředně nad ním ležících sousedů:

$$\begin{array}{lccccccccccc}
n = 0: & & & & & & 1 & & & & & \\
n = 1: & & & & & 1 & & 1 & & & & \\
n = 2: & & & & 1 & & 2 & & 1 & & & \\
n = 3: & & & 1 & & 3 & & 3 & & 1 & & \\
n = 4: & & 1 & & 4 & & 6 & & 4 & & 1 & \\
n = 5: & 1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Všimněme si, že v jednotlivých řádcích máme právě koeficienty u jednotlivých mocnin z výrazu (1.5), např. poslední uvedený řádek říká

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

**Řešení.** Obdobně jako v předchozím příkladu se nejprve nebudeme ohlížet na cifru nula. Dostaneme tak $\binom{5}{2}(2^4-2)+5\cdot 5(2^3-1)$ čísel (nejprve počítáme čísla pouze ze sudých cifer, druhý sčítanec udává počet sudých čtyřciferných čísel složených ze sudé a liché cifry). Opět musíme odečíst čísla začínající nulou, těch je $(2^3-1)4+(2^2-1)5$. Hledaný počet cifer tak je

$$\binom{5}{2}(2^4-2)+5\cdot 5(2^3-1)-(2^3-1)4-(2^2-1)5=272\,. \qquad \square$$

**1.23.** Jak se může rozsadit pět osob v pětimístném autě, když jen dva z nich mají řidičský průkaz? Jak se může rozsadit 20 cestujících a dva řidiči v 25-místném minibuse?

**Řešení.** Na místě řidiče máme dvě možnosti a na zbylých místech už je pořadí libovolné, tzn. pro spolujezdce 4 možnosti, pro další místo 3, pak 2 a 1. Celkově $2\cdot 4!=48$ možností. Podobně v minibuse máme dvě možnosti na místě řidiče a druhý řidič plus cestující mohou na zbylých 24 místech sedět libovolně. Nejprve vybereme místa, která budou obsazená, tj. $\binom{24}{21}$ a na těchto místech může být 21! různých pořadí. Dohromady máme $2\cdot\binom{24}{21}21!=\frac{24!}{3}$ možností. $\square$

**1.24.** Určete počet různých vět, které vzniknou přesmyčkami v jednotlivých slovech věty SKOKAN NA KOKS (vzniklé věty ani slova nemusejí dávat smysl).

**Řešení.** Určíme nejprve počty přesmyček jednotlivých slov. Ze slova SKOKAN dostaneme 6!/2 různých přesmyček (permutace s opakováním $P(1,1,1,1,2)$), obdobně ze slova NA dvě a ze slova KOKS 4!/2. Celkem podle pravidla součinu $(6!/2)\cdot 2\cdot(4!/2)=8640$. $\square$

**1.25.** Kolika způsoby můžeme do pěti různých důlků vybrat po jedné kouli, vybíráme-li ze čtyř bílých, čtyř modrých a tří červených koulí?

**Řešení.** Nejprve řešme úlohu v případě, že bychom měli k dispozici alespoň pět koulí od každé barvy. V tomto případě se jedná o volný výběr pěti prvků ze tří možností, tedy o variace s opakováním (viz 1.8). Máme

$$V(3,5)=3^5.$$

Nyní odečteme ty výběry, ve kterých se vyskytují buď pouze koule stejné barvy (takové výběry jsou tři), nebo právě čtyři koule červené (takových výběrů je $2\cdot 5=10$; nejprve vybereme barvu koule, která nebude červená – dvě možnosti – a poté důlek, ve kterém bude – pět možností). Celkem tedy máme

$$3^5-3-10=230$$

možných výběrů. $\square$

**1.8. Výběr s opakováním.** Pořadí $n$ prvků, z nichž mezi některými nerozlišujeme, nazýváme *permutace s opakováním.*



Nechť je mezi $n$ danými prvky $p_1$ prvků prvního druhu, $p_2$ prvků druhého druhu, až $p_k$ prvků $k$-tého druhu a $p_1+p_2+\cdots+p_k=n$. Potom počet pořadí těchto prvků s opakováním budeme značit $P(p_1,\ldots,p_k)$.

Podobně jako u permutací a kombinací bez opakování, pro výběr prvního z nich máme $n$ možností, pro další $n-1$ a tak dále, až po poslední, který zbude. Přitom ale za stejná považujeme pořadí nerozlišitelných objektů. Těch je pro každou skupinku o $p_i$ objektech právě $p_i!$, takže zřejmě platí

PERMUTACE S OPAKOVÁNÍM

$$P(p_1,\ldots,p_k)=\frac{n!}{p_1!\cdots p_k!}.$$

Volný výběr $k$ prvků z $n$ možností, včetně pořadí, nazýváme *$k$-prvkové variace s opakováním*, jejich počet budeme značit $V(n,k)$. Volný výběr v tomto případě znamená, že předpokládáme, že stále máme pro výběr stejně možností, např. díky tomu, že vybrané prvky před dalším výběrem vracíme nebo třeba házíme pořád stejnou kostkou. Zřejmě platí

VARIACE S OPAKOVÁNÍM

$$V(n,k)=n^k.$$

Pokud nás výběr zajímá bez zohlednění pořadí, hovoříme o *kombinacích s opakováním* a pro jejich počet píšeme $C(n,k)$. Zde se na první pohled nezdá tak jednoduché, jak výsledný počet zjistit. Důkaz následující věty je pro matematiku typický – podaří se nám nový problém převést na problém jiný, který jsme už dříve zvládli. V našem případě je to převedení na problém standardních kombinací bez opakování.

KOMBINACE S OPAKOVÁNÍM

**Věta.** *Počet $k$-prvkových kombinací s opakováním z $n$ prvků je pro všechna $k\ge 0$ a $n\ge 1$*

$$C(n,k)=\binom{n+k-1}{k}.$$

DŮKAZ. Důkaz je opřen o trik (jednoduchý, jakmile ho pochopíme). Uvedeme dva různé postupy.



Představme si nejprve, že taháme postupně karty z balíku $n$ různých karet. Abychom mohli případně některou z nich vytáhnout vícekrát, přidáme si k balíku ještě $k-1$ různých žolíků (alespoň jednou určitě chceme jednu z původních karet). Řekněme, že postupně vytáhneme $r$ původních karet a $s$ žolíků, tj. $r+s=k$. Zdá se, že bychom měli vymyslet postup, jak z těch $s$ žolíků poznat, které karty nám zastupují. Ve skutečnosti nám ale stačí diskuse počtů možností takových voleb.

K tomu můžeme použít matematickou indukci a předpokládat, že dokazovaná věta platí pro menší argumenty než jsou $n$ a $k$. Skutečně potřebujeme obsáhnout $s$-prvkové kombinace s opakováním z pouze $r$ původních karet, což dává $\binom{r+k-r-1}{s}=\binom{k-1}{s}$, což

**1.26.** Pro libovolné pevné $n \in \mathbb{N}$ určete počet všech řešení rovnice

$$x_1 + x_2 + \cdots + x_k = n$$

v množině nezáporných celých čísel.

**Řešení.** Každé řešení $(r_1, \ldots, r_k)$, $\sum_{i=1}^{k} r_i = n$ můžeme jednoznačně zašifrovat jako posloupnost jedniček a nul, ve které napíšeme nejprve $r_1$ jedniček, pak nulu, pak $r_2$ jedniček, nulu a tak dále. Posloupnost bude celkem obsahovat $n$ jedniček a $k-1$ nul. Každá taková posloupnost navíc zřejmě určuje nějaké řešení dané rovnice. Je tedy řešení tolik, kolik je posloupností, tedy $\binom{n+k-1}{n}$. □

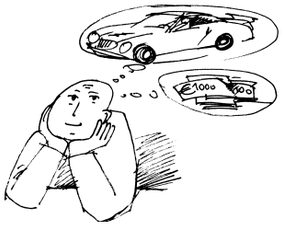
Další kombinatorické příklady naleznete v doplňujících úlohách ke kapitole od strany 44.

## C. Diferenční rovnice

Diferenční rovnice (jinak řečeno též rekurentní vztahy) jsou vztahy mezi členy nějaké posloupnosti, přičemž následující člen je dán pomocí členů předchozích. Vyřešit diferenční rovnici pak znamená najít explicitní vzorec pro $n$-tý (libovolný) člen dané posloupnosti. Rekurentní vztah nám totiž po zadání několika prvních členů posloupnosti zadává $n$-tý člen přímo pouze pomocí postupného vyčíslení všech předchozích členů.

Pokud je následující člen posloupnosti určen pouze předchozím členem, hovoříme o diferenčních rovnicích prvního řádu. S nimi se můžeme v životě opravdu setkat, například, pokud si chceme zjistit dobu splácení nějaké půjčky při pevné měsíční splátce, nebo naopak chceme zjistit výši měsíční splátky, zadáme-li si dobu, za kterou chceme půjčku splatit.

**1.27.** Mirek si chce koupit nové auto, které stojí 300 000 Kč. Mirek by chtěl auto koupit na měsíční splátky. Prodávající společnost mu nabízí půjčku na koupi auta s ročním úrokem 6%. Mirek by chtěl auto splatit za tři roky. Jak vysoká bude měsíční splátka?



**Řešení.** Označme $S$ Mirkovu měsíční splátku. Předpokládejme, že při „koupi“ auta Mirek zaplatí jednu měsíční splátku a pak po měsíci vždy další. Částku, kterou bude Mirek dlužit po uplynutí $k$ měsíců, označme $d_k$. Cenu auta označme $C$ a měsíční úrok $u$ (je tedy $u = \frac{0{,}06}{12}$). Po prvním měsíci bude Mirek dlužit

$$d_1 = C - S + u(C - S)$$

je právě počet $s$-prvkových kombinací (bez opakování) ze všech žolíků. Tím je věta dokázána.

Druhý přístup (bez matematické indukce): Na množině

$$S = \{a_1, \ldots, a_n\},$$

ze které vybíráme kombinace, si zafixujeme uvedené pořadí prvků a pro naše volby prvků z $S$ si připravíme $n$ přihrádek, do kterých si již předem dáme v námi zvoleném pořadí po právě jednom prvku z $S$.

Jednotlivé volby $x_i \in S$ přidáváme do přihrádky, která již tento prvek obsahuje. Nyní si uvědomme, že pro rozpoznání původní kombinace nám stačí vědět, kolik je prvků v jednotlivých přihrádkách. Například

$$a \mid bbb \mid cc \mid d \;\simeq\; * \mid *** \mid ** \mid *$$

vypovídá o volbě $b, b, c$ z množiny $S = \{a, b, c, d\}$.

V obecném případě výběru $k$ prvků z $n$ možných tedy máme řetězec $n + k$ znaků a počet $C(n, k)$ je roven počtu možných umístění přihrádek | mezi jednotlivé znaky. To odpovídá výběru $n - 1$ pozic z $n + k - 1$ možných. Protože je

$$\binom{n+k-1}{k} = \binom{n+k-1}{n+k-1-k} = \binom{n+k-1}{n-1},$$

je věta dokázána i podruhé. □

### 3. Diferenční rovnice

V předchozích odstavcích jsme viděli vzorce, které zadávaly hodnotu skalární funkce definované na přirozených číslech (faktoriál) nebo dvojicích čísel (binomická čísla) pomocí předcházejících hodnot. Zatímco v odstavci 1.5 jsou kombinační čísla definována přímo spočítatelným výrazem, lze rozumět vztahům v 1.8 také tak, že místo hodnoty naší funkce zadáváme její změnu při odpovídající změně nezávislé proměnné.



Takto se skutečně velice často postupuje při matematické formulaci modelů, které popisují reálné systémy v ekonomice, biologii apod. My si tu povšimneme jen několika jednoduchých případů a budeme se k této tématice postupně vracet.

**1.9. Lineární diferenční rovnice prvního řádu.** Obecnou *diferenční rovnicí prvního řádu* rozumíme výraz

$$f(n+1) = F(n, f(n)),$$

kde $F$ je známá skalární funkce závislá na dvojici přirozených čísel. Známe–li „počáteční“ hodnotu $f(0)$, můžeme spočítat $f(1) = F(0, f(0))$, poté $f(2) = F(1, f(1))$ atd. Tímto postupným způsobem můžeme tedy nakonec spočítat hodnotu $f(n)$ pro libovolné $n \in \mathbb{N}$. Všimněme si, že tato úvaha je podobná konstrukci přirozených čísel z prázdné množiny nebo principu matematické indukce.

Jako příklad může sloužit definiční formule pro faktoriál, tj.

$$(n+1)! = (n+1) \cdot n!$$

Vidíme, že skutečně vztah pro $f(n+1)$ závisí na $n$ i na hodnotě $f(n)$.

Dalším obzvlášť jednoduchým příkladem je $f(n) = C$ pro nějaký pevný skalár $C$ a všechna $n$ a tzv. *lineární diferenční rovnice*

$$f(n+1) = a \cdot f(n) + b, \tag{1.6}$$

kde $a \neq 0$, a $b$ jsou známé skaláry.

(na počátku Mirek splatí jednu splátku, zbytek dluhu se pak úročí). Obecně po uplynutí $k$-tého měsíce dluží Mirek

$$d_k = d_{k-1} - S + u d_{k-1}. \tag{1.2}$$

Podle vztahu (1.9) v teoretické části je $d_k$ dáno následovně (při označení $q = 1 + u$.

$$d_k = d_0 q^k - S\left(\frac{q^k - 1}{q - 1}\right) = \\ = (1+u)^k C - \left(\frac{(1+u)^{k+1} - 1}{u}\right) S.$$

Splacení po třech letech se rovná podmínce $d_{36} = 0$, odkud dostáváme

$$S = C\left(\frac{(1+u)^{36} u}{(1+u)^{37} - 1}\right) \doteq 8857. \tag{1.3}$$

□

Všimněme si, že rekurentní vztah (‖1.2‖) můžeme použít na náš příklad pouze tak dlouho, dokud budou všechna $d_n$ kladná, tj. dokud bude Mirek skutečně něco dlužit.

**1.28.** Uvažujme situaci z předchozího příkladu. Jak dlouho by Mirek auto splácel, kdyby chtěl měsíčně splácet 5000 Kč?

**Řešení.** Při označení $q = 1{,}005$, $C = 300000$ nám podmínka $d_k = 0$ dává vztah

$$q^k = -\frac{S}{Cu - S},$$

jehož logaritmováním obdržíme

$$k = \frac{\ln S - \ln(S - Cu)}{\ln q},$$

což pro $S = 5000$ dává přibližně $k = 71{,}5$, tedy splácení půjčky by trvalo 72 měsíců, tj. šest let (poslední splátka by nebyla plných 5 000 Kč).

□

*1.29.* Určete posloupnost $\{y_n\}_{n=1}^{\infty}$, která vyhovuje následujícímu rekurentnímu vztahu

$$y_{n+1} = \frac{3y_n}{2} + 1,\ n \geq 1,\ y_1 = 1.$$ ○

Lineární rekurentní vtahy se mohou vyskytnout například v geometrických problémech:

**1.30.** Na kolik nejvýše oblastí může dělit rovinu $n$ přímek?

**Řešení.** Označme hledaný počet oblastí $p_n$. Pokud v rovině nemáme dánu žádnou přímku, je celá rovina jedinou oblastí, je tedy $p_0 = 1$. Pokud je v rovině dáno $n$ přímek, tak přidáním $(n+1)$. přímky přibude nejvýše $(n+1)$ oblastí: oblastí přibude právě tolik, kolika (původními) oblastmi bude přímka procházet (každou takovou oblast rozdělí na dvě části, jedna oblast tedy přibude). Přidaná přímka může mít nejvýše $n$ různých průsečíků s $n$ přímkami, které už v rovině byly. Část přímky

Takovou diferenční rovnici umíme snadno řešit, je-li $b = 0$. Pak se totiž jedná o dobře známou rekurentní definici geometrické posloupnosti a platí

$$f(1) = af(0), \quad f(2) = af(1) = a^2 f(0) \quad \text{atd.}$$

Máme tedy pro všechna $n$

$$f(n) = a^n f(0).$$

To je např. vztah pro tzv. Malthusiánský model populačního růstu, který vychází z představy, že za zvolený časový interval vzroste populace s konstantní úměrou $a$ vůči předchozímu stavu.

Dokážeme si obecný výsledek pro rovnice prvního řádu, které se podobají lineárním, ale připouští proměnné koeficienty $a$ a $b$,

$$f(n+1) = a_n \cdot f(n) + b_n. \tag{1.7}$$

Nejdříve se ale zamysleme, co mohou takové rovnice popisovat.

Lineární diferenční rovnici (1.6) můžeme pěkně interpretovat jako matematický model pro spoření nebo splácení úvěru s pevnou úrokovou mírou $a$ a pevnou splátkou $b$ (tyto dva případy se liší pouze znaménkem u parametru $b$).

S proměnnými parametry dostáváme obdobný model, ovšem



s proměnlivými jak úroky, tak splátkami. Můžeme si představit třeba $n$ jako počet měsíců, $a_n$ bude vyjadřovat úrokovou míru v měsíci $n$, $b_n$ příslušnou splátku v měsíci $n$.

Neděste se zdánlivě složitého sčítání a násobení v následujícím výsledku. Jde o typický příklad technického matematického tvrzení, kdy těžké je „uhodnout“, jak zní. Naopak důkaz je už pak jen docela snadné cvičení na základní vlastnosti skalárů a matematickou indukci. Skutečně zajímavé jsou teprve důsledky, viz 1.11 níže.

Ve formulaci používáme vedle obvyklých znaků pro součet $\sum$ také obdobné znaky pro součin $\prod$. V dalším budeme vždy používat také konvenci, že pokud u součtu je množina uvedených indexů prázdná, pak je součet nula, zatímco u součinu je ve stejném případě výsledek jedna.

**1.10. Tvrzení.** *Obecné řešení diferenční rovnice (1.7) prvního řádu s počáteční podmínkou $f(0) = y_0$ je dáno vztahem*

$$f(n) = \left(\prod_{i=0}^{n-1} a_i\right) y_0 + \sum_{j=0}^{n-2} \left(\prod_{i=j+1}^{n-1} a_i\right) b_j + b_{n-1}. \tag{1.8}$$

Důkaz. Tvrzení dokážeme matematickou indukcí.

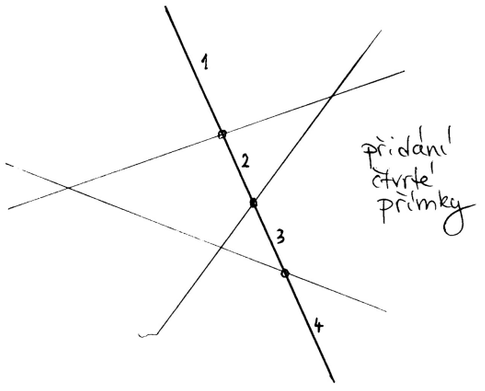


Zjevně tvrzení platí pro $n = 1$, kdy se jedná právě o definiční vztah $f(1) = a_0 y_0 + b_0$. Předpokládáme-li, že tvrzení platí pro nějaké pevně zvolené $n$, můžeme snadno spočíst

$$f(n+1) = a_n \left(\left(\prod_{i=0}^{n-1} a_i\right) y_0 + \sum_{j=0}^{n-2} \left(\prod_{i=j+1}^{n-1} a_i\right) b_j + b_{n-1}\right) + \\ + b_n = \\ = \left(\prod_{i=0}^{n} a_i\right) y_0 + \sum_{j=0}^{n-1} \left(\prod_{i=j+1}^{n} a_i\right) b_j + b_n,$$

jak se přímo vidí roznásobením výrazů. □

mezi libovolnými dvěma sousedními průsečíky prochází právě jednou oblastí, celkem může přidaná přímka procházet nejvýše $n+1$ oblastmi, tedy může přibýt maximálně $n+1$ oblastí, navíc v rovině bylo před přidáním $(n+1)$-ní přímky nejvýše $p_n$ oblastí (tak jsme číslo $p_n$ totiž definovali).




Celkem dostáváme rekurentní vztah

$$p_{n+1} = p_n + (n+1),$$

ze kterého získáme explicitní formuli pro $p_n$ buď pomocí vzorce 1.10 nebo přímo:

$$\begin{aligned} p_n &= p_{n-1} + n = p_{n-2} + (n-1) + n = \\ &= p_{n-3} + (n-2) + (n-1) + n = \cdots = p_0 + \sum_{i=1}^{n} i = \\ &= 1 + \frac{n(n+1)}{2} = \frac{n^2+n+2}{2}. \end{aligned}$$

□

Rekurentní vztahy mohou mít i složitější podobu než je rekurze prvního řádu. Uveďme si příklady kombinatorických úloh, při jejichž řešení můžeme rekurze s výhodou využít.

**1.31.** Kolik existuje slov délky 12 složených pouze z písmen $A$ a $B$, které neobsahují skupinu $BBB$?

**Řešení.** Nechť $a_n$ značí počet slov délky $n$ složených pouze z písmen $A$ a $B$ neobsahujících skupinu $BBB$. Pak pro $a_n$ $(n \geq 3)$ platí rekurentní vztah

$$a_n = a_{n-1} + a_{n-2} + a_{n-3},$$

neboť slova délky $n$ splňující danou podmínku musí končit buď na $A$, nebo na $AB$, nebo na $ABB$. Slov končících na $A$ je právě $a_{n-1}$ (před posledním $A$ může být libovolné slovo délky $n-1$ splňující danou

Opět si všimněme, že jsme pro důkaz nepotřebovali o použitých skalárech nic víc než vlastnosti komutativního okruhu.

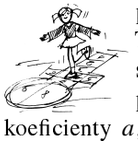
**1.11. Důsledek.** *Obecné řešení lineární diferenční rovnice (1.6) s $a \neq 1$ a počáteční podmínkou $f(0) = y_0$ je*

$$f(n) = a^n y_0 + \frac{1-a^n}{1-a} b. \tag{1.9}$$

Důkaz. Dosazením konstantních hodnot za $a_i$ a $b_i$ do obecného vzorce (1.8) dostáváme

$$f(n) = a^n y_0 + b\left(1 + \sum_{j=0}^{n-2} a^{n-j-1}\right).$$

Pro vyčíslení součtu součinů v druhém sčítanci si je třeba všimnout, že se jedná o výrazy $(1+a+\cdots+a^{n-1})b$. Součet této geometrické řady spočteme ze vztahu $1-a^n = (1-a)(1+a+\cdots+a^{n-1})$ a dostaneme právě požadovaný výsledek. □



Všimněme si, že pro výpočet součtu geometrické řady jsme potřebovali existenci inverze pro nenulové skaláry. To bychom nad celými čísly neuměli. Poslední výsledek tedy platí pro pole skalárů a můžeme jej bez problému použít pro lineární diferenční rovnice, kde koeficienty $a$, $b$ a počáteční podmínka $f(0) = y_0$ jsou racionální, reálné nebo komplexní, ale také nad okruhem zbytkových tříd $\mathbb{Z}_k$ s prvočíselným $k$ (zbytkové třídy budeme definovat v odstavci 1.41).

Pozoruhodné je, že ve skutečnosti vzorec (1.9) platí i s celočíselnými koeficienty a počáteční podmínkou. Pak totiž předem víme, že všechny $f(n)$ budou také celočíselné, a celá čísla jsou podmnožinou v číslech racionálních. Musí proto nutně náš vzorec dávat ta správná celočíselná řešení.

Při pozornějším pohledu na důkaz je zřejmé, že $1-a^n$ je vždy dělitelné $1-a$, takže nás poslední pozorování nemělo překvapit. Nicméně je vidět, že třeba nad skaláry ze $\mathbb{Z}_4$ a třeba $a = 3$ už neuspějeme, protože pak $1-a = 2$ je dělitelem nuly.

**1.12. Nelineární příklad.** Vraťme se na chvíli k rovnici prvního řádu (1.6), kterou jsme použili na velice primitivní model populačního růstu závisející přímo úměrně na okamžité velikosti populace $p$. Na první pohled je zřejmé, že takový model vede při úměře $a > 1$ k příliš rychlému a hlavně neomezenému růstu.



Realističtější model bude mít takto úměrnou změnu populace $\Delta p(n) = p(n+1) - p(n)$ jen při malých hodnotách $p$, tj. $\Delta p/p \sim r > 0$. Pokud tedy budeme chtít nechat růst populaci o 5% za období při malém $p$, budeme $r$ volit 0,05. Při určité limitní hodnotě $p = K > 0$ ale naopak už populace neroste a při ještě větších už klesá (třeba protože zdroje pro její obživu jsou omezené, jedinci ve veliké populaci si navzájem překáží apod.).

Předpokládejme, že právě hodnoty $y_n = \Delta p(n)/p(n)$ se v závislosti na $p(n)$ mění lineárně. Graficky si tedy tuto závislost můžeme představit jako přímku v rovině proměnných $p$ a $y$, která prochází body $[0, r]$ (tj. při $p = 0$ máme $y = r$) a $[K, 0]$ (což dává druhou podmínku, že při $p = K$ se populace nemění). Položíme proto

$$y = -\frac{r}{K} p + r.$$

podmínku). Obdobně pro zbylé dvě skupiny. Dále snadno vyčíslíme $a_1 = 2, a_2 = 4, a_3 = 7$. Postupným dopočítáním

$$a_{12} = 1705.$$

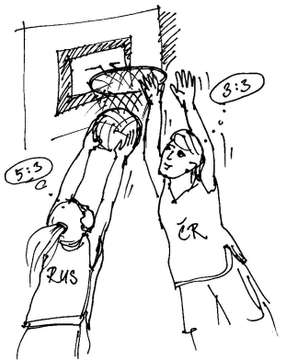
Též bychom dle uvedené teorie mohli odvodit explicitní vzorec pro $n$-tý člen takto zadané posloupnosti (viz 3.10). Charakteristický polynom dané rekurentní rovnice je $x^3 - x^2 - x - 1$ s jedním reálným a dalšími dvěma komplexními kořeny, které můžeme vyjádřit pomocí vztahů (‖1.1‖). □

**1.32.**  Skóre basketbalového utkání mezi týmy České republiky a Ruska vyznělo po první čtvrtině 12 : 9 pro ruský tým. Kolika způsoby se mohlo vyvíjet skóre?

**Řešení.** Označíme-li $P_{(k,l)}$ počet způsobů, kterými se mohlo vyvíjet skóre basketbalového utkání, které skončilo $k : l$, tak pro $k, l \geq 3$ platí rekurentní vztah:

$$P_{(k,l)} = P_{(k-3,l)} + P_{(k-2,l)} + P_{(k-1,l)} + P_{(k,l-1)} + P_{(k,l-2)} + P_{(k,l-3)}.$$

(Způsoby, kterými se mohlo vyvíjet utkání s výsledným skóre $k : l$, si rozdělíme na šest po dvou disjunktních podmnožin podle toho, které družstvo vstřelilo koš a za kolik bodů (1, 2, či 3).) Ze symetrie úlohy zřejmě platí $P_{(k,l)} = P_{(l,k)}$. Dále pro $k \geq 3$ platí:




$$P_{(k,2)} = P_{(k-3,2)} + P_{(k-2,2)} + P_{(k-1,2)} + P_{(k,1)} + P_{(k,0)},$$
$$P_{(k,1)} = P_{(k-3,1)} + P_{(k-2,1)} + P_{(k-1,1)} + P_{(k,0)},$$
$$P_{(k,0)} = P_{(k-3,0)} + P_{(k-2,0)} + P_{(k-1,0)},$$

což spolu s počátečními podmínkami $P_{(0,0)} = 1, P_{(1,0)} = 1, P_{(2,0)} = 2, P_{(3,0)} = 4, P_{(1,1)} = 2, P_{(2,1)} = P_{(1,1)} + P_{(0,1)} + P_{(2,0)} = 5, P_{(2,2)} = P_{(0,2)} + P_{(1,2)} + P_{(2,1)} + P_{(2,0)} = 14$ dává

$$P_{(12,9)} = 497178513.$$ □

**Poznámka.** Vidíme, že rekurentní vztah v tomto příkladu má složitější formu, než kterou jsme se zabývali v teorii a tudíž neumíme vyčíslit libovolné číslo $P_{(k,l)}$ explicitně, nýbrž pouze postupným výpočtem od počátečních členů. Takové rovnice nazýváme parciální diferenční rovnice, protože členy posloupnosti jsou značeny dvěma nezávislými proměnnými $(k, l)$.

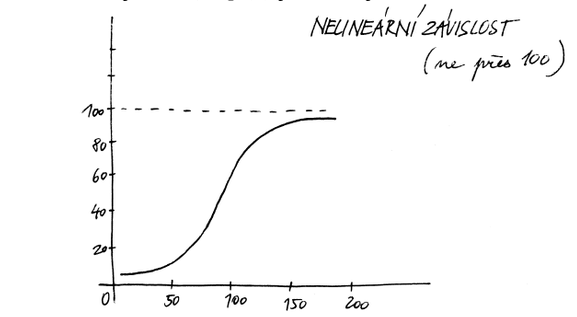
Dosazením $y_n$ za $y$ a $p(n)$ za $p$ dostáváme

$$\frac{p(n+1) - p(n)}{p(n)} = -\frac{r}{K}p(n) + r,$$

tj. roznásobením dostáváme diferenční rovnici prvního řádu (kde hodnota $p(n)$ vystupuje v první i v druhé mocnině)

$$p(n+1) = p(n)\Big(1 - \frac{r}{K}p(n) + r\Big). \tag{1.10}$$

Zkuste si promyslet nebo vyzkoušet chování tohoto modelu pro různé hodnoty $r$ a $K$. Na obrázku je průběh hodnot pro parametry $r = 0{,}05$ (tj. pětiprocentní nárůst v ideálním stavu), $K = 100$ (tj. zdroje limitují hodnotu na 100 jedinců) a $p(0)$ jsou dva jedinci.




Všimněme si, že počáteční přibližně exponenciální růst se skutečně později zlomí a hodnota se postupně blíží kýženému limitu 100 jedinců. Pro $p$ blízké jedné a $K$ daleko větší než $r$ bude pravá strana rovnice (1.10) přibližně $p(n)(1 + r)$, tzn. chování je obdobné Malthusiánskému modelu. Naopak při $p$ přibližně $K$ bude pravá strana přibližně $p(n)$. Pro větší počáteční hodnoty $p$ než $K$ budou hodnoty klesat, pro menší než $K$ růst, takže systém bude zpravidla postupně oscilovat kolem hodnoty $K$.

### 4. Pravděpodobnost



Teď se podíváme na jiný obvyklý případ skalárních hodnot funkcí – sledované hodnoty často nejsou známy ani explicitně vzorcem, ani implicitně nějakým popisem. Jsou výsledkem nějaké nahodilosti a my se snažíme popsat s jakou *pravděpodobností* nastane ta či ona možnost.

**1.13. Co je pravděpodobnost?** Jako jednoduchý příklad může sloužit obvyklé házení kostkou se šesti stěnami s označeními

$$1,\ 2,\ 3,\ 4,\ 5,\ 6.$$

Pokud popisujeme matematický model takového házení „poctivou“ kostkou, budeme očekávat a tudíž i předepisovat, že každá ze stran padá stejně často. Slovy to vyjadřujeme „každá předem vybraná stěna padne s pravděpodobností $\frac{1}{6}$“.

Pokud si ale třeba sami nožíkem vyrobíme takovou kostku z kusu dřeva, je jisté, že skutečné relativní četnosti výsledků nebudou stejné. Pak můžeme z velikého počtu pokusů usoudit na relativní četnosti jednotlivých výsledků hodů a tyto ustanovit jako pravděpodobnosti v našem matematickém popisu. Nicméně při sebevětším počtu pokusů nemůžeme vyloučit možnost, že se náhodou povedla velice nepravděpodobná kombinace výsledků a že jsme proto náš matematický model skutečnosti pro naši kostku nevybrali dobře.

O lineárních rekurentních formulích (diferenčních rovnicích) vyšších řádů s konstantími koeficienty si povíme více v kapitole 3.

### D. Pravděpodobnost

Uveďme si několik jednoduchých příkladů na klasickou pravděpodobnost, kdy zkoumáme nějaký pokus, který má konečně mnoho možných výsledků („všechny případy“) a nás zajímá, kdy výsledek pokusu bude náležet nějaké podmnožině možných výsledků („příznivé případy“). Hledaná pravděpodobnost je pak rovna poměru počtu příznivých případů ku počtu všech případů. Klasickou pravděpodobnost můžeme použít tam, kde předpokládáme (víme), že každý z možných výsledků má stejnou pravděpodobnost toho, že nastane (například při hodech kostkou).

**1.33.** Jaká je pravděpodobnost, že při hodu šestibokou kostkou padne číslo větší než 4?

**Řešení.** Všech možných výsledků je šest (tvoří množinu $\{1,2,3,4,5,6\}$), příznivé možnosti jsou dvě ($\{5,6\}$). Hledaná pravděpodobnost je tedy $2/6 = 1/3$. □

**1.34.** Ze skupiny osmi mužů a čtyř žen náhodně vybereme skupinu pěti lidí. Jaká je pravděpodobnost, že v ní budou alespoň tři ženy?

**Řešení.** Pravděpodobnost spočítáme jako podíl počtu příznivých případů ku počtu všech případů. Příznivé případy rozdělíme podle toho, kolik je v náhodně vybrané skupině mužů: mohou v ní být buď dva, nebo jeden muž. Skupinek o pěti lidech s jedním mužem je osm (záleží pouze na výběru muže, ženy v ní musí být všechny), skupinek se dvěma muži je potom $c(8,2)\cdot c(4,3) = \binom{8}{2}\cdot\binom{4}{3}$ (vybereme dva muže z osmi a nezávisle na tom tři ženy ze čtyř, tyto dva výběry můžeme nezávisle kombinovat a podle pravidla součinu dostáváme uvedený počet skupin). Všech možných skupin o pěti lidech pak můžeme sestavit $c(12,5) = \binom{12}{5}$. Hledaná pravděpodobnost je tedy

$$\frac{8+\binom{4}{3}\binom{8}{2}}{\binom{12}{5}}.$$

□

Uveďme si příklad, při jehož řešení není vhodné používat klasické pravděpodobnosti:

**1.35.** Jaká je pravděpodobnost toho, že čtenář této úlohy vyhraje příští týden alespoň milión dolarů v loterii?

**Řešení.** Takováto formulace úlohy je neúplná, neposkytuje dostatek údajů. Předvedeme **chybné** řešení. Základní prostor všech možný jevů je dvouprvkový: buď vyhraje nebo nevyhraje. Příznivý jev je jeden (vyhraje), hledaná pravděpodobnost je tedy $1/2$ (a to je zjevně špatná odpověď). □



V dalším budeme pracovat s abstraktním matematickým popisem pravděpodobnosti v nejjednodušším přiblížení. To, do jaké míry je takový popis adekvátní pro konkrétní pokusy či jiný problém, je záležitostí mimo samotnou matematiku. To ale neznamená, že by se takovým přemýšlením neměli zabývat matematici (nejspíše ve spolupráci s jinými experty). Později se vrátíme k pravděpodobnosti coby teorii popisující chování nahodilých procesů nebo i plně determinovaných dějů, kde ovšem neznáme přesně všechny určující parametry.

Matematická statistika pak umožňuje posuzovat, do jaké míry lze očekávat, že vybraný model je ve shodě s realitou, resp. umožňuje určit parametry modelu tak, aby docházelo k co nejlepší shodě s pozorováním a zároveň umí odhadnout míru spolehlivosti zvoleného modelu.

K matematické pravděpodobnosti i statistice ovšem budeme potřebovat dosti rozsáhlý matematický aparát, který budeme mezitím několik semestrů budovat.

Na příkladu naší neumělé kostky si to můžeme představit tak, že v teorii pravděpodobnosti budeme pracovat s parametry $p_i$ pro pravděpodobnost jednotlivých hodnot stran a budeme požadovat pouze, aby všechny tyto pravděpodobnosti byly nezáporné a jejich součet byl

$$p_1 + p_2 + p_3 + p_4 + p_5 + p_6 = 1.$$

Při volbě konkrétních hodnot $p_i$ pro konkrétní kostku pak v matematické statistice budeme schopni odhadnout s jakou spolehlivostí tento model naší kostce odpovídá.



Naším skromným cílem je teď pouze naznačit, jak abstraktně zachytit pravděpodobnostní úvahy ve formalizovaných matematických objektech. Následující odstavce tak budou ve své podstatě pouhými cvičeními v jednoduchých operacích nad množinami a jednoduché kombinatorice (tj. výpočtech počtu možností, jak mohou být splněny dané podmínky kladené na konečné množiny prvků).

**1.14. Náhodné jevy.** Budeme pracovat s neprázdnou pevně zvolenou množinou $\Omega$ všech možných výsledků, kterou nazýváme *základní prostor*. Pro jednoduchost bude pro nás $\Omega$ konečná množina s prvky $\omega_1, \ldots, \omega_n$ představujícími jednotlivé *možné výsledky*. Každá podmnožina $A \subseteq \Omega$ představuje možný *jev*. Systém podmnožin $\mathcal{A}$ základního prostoru se nazývá *jevové pole*, jestliže

- $\Omega \in \mathcal{A}$ (tj. základní prostor je jevem),
- jsou-li $A, B \in \mathcal{A}$, pak $A \setminus B \in \mathcal{A}$ (tj. pro každé dva jevy je jevem i jejich množinový rozdíl),
- jsou-li $A, B \in \mathcal{A}$, pak $A \cup B \in \mathcal{A}$ (tj. pro každé dva jevy je jevem i jejich sjednocení).

Zjevně je i komplement $A^c = \Omega \setminus A$ jevu $A$ jevem, který nazýváme *opačný jev* k jevu $A$. Průnik dvou jevů je opět jevem, protože pro každé dvě podmnožiny $A, B \subseteq \Omega$ platí

$$A \setminus (\Omega \setminus B) = A \cap B.$$

Slovy se tak dá jevové pole charakterizovat jako systém podmnožin (konečného) základního prostoru uzavřený na průniky, sjednocení a rozdíly. Jednotlivé množiny $A \in \mathcal{A}$ nazýváme *náhodné jevy* (vzhledem k $\mathcal{A}$).

**Poznámka.** V předchozím příkladě je porušena základní podmínka použití klasické pravděpodobnosti, totiž to, že každý z elementárních jevů má stejnou pravděpodobnost toho, že nastane.

**1.36.** Do řady v kině o $2n$ místech je náhodně rozmístěno $n$ mužů a $n$ žen. Jaká je pravděpodobnost, že žádné dvě osoby stejného pohlaví nebudou sedět vedle sebe?

**Řešení.** Všech možných rozmístění lidí v řadě je $(2n)!$, rozmístění splňujících podmínky je $2(n!)^2$: máme dvě možnosti výběru pozice mužů, tedy i žen – buď všichni muži budou sedět na lichých místech (a tedy ženy na sudých), nebo všichni muži na sudých (a tedy ženy na lichých místech); na nich jsou pak muži i ženy rozmístěny libovolně. Výsledná pravděpodobnost je tedy

$$p(n) = \frac{2(n!)^2}{(2n)!},$$

$$p(2) \doteq 0{,}33,\ \ p(5) \doteq 0{,}0079,\ \ p(8) \doteq 0{,}00016\,. \qquad \square$$

**1.37.** Do výtahu osmipatrové budovy nastoupilo 5 osob. Každá z nich vystoupí se stejnou pravděpodobností v libovolném poschodí. Jaká je pravděpodobnost, že vystoupí

i) všichni v šestém poschodí,
ii) všichni ve stejném poschodí,
iii) každý v jiném poschodí?

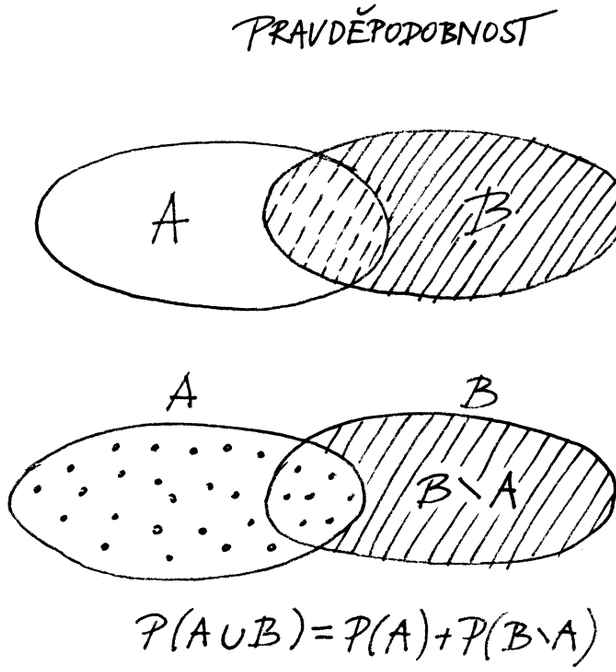
**Řešení.** Základní prostor všech možných jevů je prostor všech možných způsobů vystoupení 5 osob z výtahu. Těch je $8^5$.

V prvním případě je jediná příznivá možnost vystoupení, hledaná pravděpodobnost je tedy $\frac{1}{8^5}$, ve druhém případě máme osm možností, hledaná pravděpodobnost je tedy $\frac{1}{8^4}$ a konečně ve třetím je počet příznivých případů dán pětiprvkovou variací z osmi prvků (z osmi pater vybíráme pět, ve kterých se vystoupí a dále kteří lidé vystoupí ve vybraných poschodích), celkem je hledaná pravděpodobnost ve třetím případě rovna (viz 1.6 a 1.8)

$$\frac{v(5,8)}{V(5,8)} = \frac{8 \cdot 7 \cdots 4}{8^5} \doteq 0{,}2050781250. \qquad \square$$

**1.38.** Náhodně vybereme celé kladné číslo menší než $10^5$. Jaká je pravděpodobnost, že bude složeno pouze z cifer 0, 1, 5 a zároveň bude dělitelné číslem 5?

**Řešení.** Čísel splňující danou podmínku je $2 \cdot 3^4 - 1$ (kromě poslední cifry máme na každý řád na výběr ze tří cifer, případné číslice 0 na začátku slova nepíšeme. Všech celých kladných čísel menších než $10^5$ je $10^5 - 1$, podle klasické pravděpodobnosti dostáváme, že hledaná pravděpodobnost je $\frac{2 \cdot 3^4 - 1}{10^5 - 1}$. $\square$




Pro naše házení kostkou je $\Omega = \{1, 2, 3, 4, 5, 6\}$ a jevové pole je tvořeno všemi podmnožinami množiny $\Omega$. Např. náhodný jev $\{1, 3, 5\}$ pak interpretujeme jako „padne liché číslo“.

Něco málo terminologie, která by měla dále připomínat souvislosti s popisem skutečných modelů:

- celý základní prostor $\Omega$ se nazývá *jistý jev*, prázdná podmnožina $\emptyset \in \mathcal{A}$ se nazývá *nemožný jev*,
- jednoprvkové podmnožiny $\{\omega\} \subseteq \Omega$ se nazývají *elementární jevy*,
- *společné nastoupení jevů* $A_i$, $i \in I$, odpovídá jevu $\cap_{i\in I} A_i$, *nastoupení alespoň jednoho z jevů* $A_i$, $i \in I$, odpovídá jevu $\cup_{i\in I} A_i$,
- $A, B \in \mathcal{A}$ jsou *neslučitelné jevy*, je-li $A \cap B = \emptyset$,
- jev $A$ má za *důsledek* jev $B$, když $A \subseteq B$,

Přestavte si příklady všech uvedených pojmů pro jevový prostor popisující házení kostkou nebo obdobně pro házení mincí!

**1.15. Definice.** *Pravděpodobnostní prostor* je trojice $(\Omega, \mathcal{A}, P)$, kde $\mathcal{A}$ je jevové pole podmnožin (konečného) základního prostoru $\Omega$, na kterém je definována skalární funkce $P : \mathcal{A} \to \mathbb{R}$ s následujícími vlastnostmi:

- $P$ je nezáporná, tj. $P(A) \geq 0$ pro všechny jevy $A$,
- $P$ je aditivní, tj. $P(A \cup B) = P(A) + P(B)$, kdykoliv je $A, B \in \mathcal{A}$ a $A \cap B = \emptyset$,
- pravděpodobnost jistého jevu je 1, tj. $P(\Omega) = 1$.

Funkci $P$ nazýváme *pravděpodobností* na jevovém poli $\mathcal{A}$.

Zjevně je okamžitým důsledkem našich definic řada prostých, ale užitečných tvrzení. Např. pro všechny jevy platí

$$P(A^c) = 1 - P(A),$$

kde $A^c = \Omega \setminus A$ je *jev opačný* (používá se též pojmů doplňkový či komplementární) k jevu $A$. Dále můžeme matematickou indukcí

**1.39.** Ze sáčku s pěti bílými a pěti červenými koulemi náhodně vytáhneme tři (koule do sáčku nevracíme). Jaká je pravděpodobnost, že dvě budou bílé a jedna červená?

**Řešení.** Rozdělme uvažovaný jev na sjednocení tří disjunktních jevů: podle toho, kolikátou vytáhneme červenou kouli. Pravděpodobnosti, že vytáhneme koule přesně ve zvoleném pořadí jsou: $\frac{1}{2}\cdot\frac{4}{9}\cdot\frac{5}{8}$, $\frac{1}{2}\cdot\frac{5}{9}\cdot\frac{1}{2}$, $\frac{1}{2}\cdot\frac{5}{9}\cdot\frac{1}{2}$. Celkem $\frac{5}{12}$.

**Jiné řešení.** Uvažme počet všech možných trojic vytažených koulí (koule jsou mezi sebou rozlišitelné), tedy $\binom{10}{3}$. Trojic, které obsahují právě dvě bílé koule je potom $\binom{5}{2}\cdot\binom{5}{1}$ (dvě bílé koule můžeme vytáhnout $\binom{5}{2}$ způsoby, k nim pak červenou pěti způsoby). □

**1.40.** Z klobouku, ve kterém je pět bílých, pět červených a šest černých koulí, náhodně vytahujeme koule (bez vracení). Jaká je pravděpodobnost, že pátá vytažená koule bude černá?

**Řešení.** Spočítáme dokonce obecnější úlohu. Totiž pravděpodobnost toho, že $i$-tá vytažená koule bude černá, je stejná pro všechna $i$, $1 \le i \le 16$. Můžeme si totiž představit, že vytáhneme postupně všechny koule. Každá taková posloupnost vytažených koulí (od první vytažené koule po poslední), složená z pěti bílých, pěti červených a šesti černých koulí, má stejnou pravděpodobnost vytažení a pro výpočet hledané pravděpodobnosti můžeme opět použít model klasické pravděpodobnosti. Zmíněných posloupností je $P(5,5,6) = \frac{16!}{5!\cdot5!\cdot6!}$. Počet posloupností, kde na $i$-tém místě je černá koule, zbytek libovolný, je tolik, kolik je libovolných posloupností pěti bílých, pěti červených a pěti černých koulí, tedy $P(5,5,5) = \frac{15!}{5!5!5!}$ Celkem je tedy hledaná pravděpodobnost

$$\frac{P(5,5,5)}{P(5,5,6)} = \frac{\frac{15!}{5!5!5!}}{\frac{16!}{6!5!5!}} = \frac{3}{8}.$$ □

**Poznámka.** Vraťme se k házení kostkou a zkusme popsat jevy ze základního prostoru $\Omega$ vznikající při házení tak dlouho, dokud nepadne šestka, ne však více než stokrát.

Pro jeden hod samostatně je základním prostorem šest čísel od jedné do šesti a jde o klasickou pravděpodobnost. Pro celé série našich hodů bude základní prostor daleko větší – bude to množina konečných posloupností čísel od jedné do šestky, které buď končí šestkou, mají nejvýše 100 členů a všechna předchozí čísla jsou menší než šest, nebo jde o 100 čísel od jedné do pěti. Jevem $A$ může být např. podmnožina „házení končí druhým pokusem“. Všechny příznivé elementární jevy pak jsou

$$[1,6],\ [2,6],\ [3,6],\ [4,6],\ [5,6].$$

snadno rozšířit aditivitu na jakýkoliv konečný počet vzájemně neslučitelných jevů $A_i \subseteq \Omega$, $i \in I$, tj.

$$P(\cup_{i\in I} A_i) = \sum_{i\in I} P(A_i),$$

kdykoliv $A_i \cap A_j = \emptyset$, pro všechna $i, j \in I$, $i \neq j$.

**1.16. Definice.** Nechť $\Omega$ je konečný základní prostor a nechť jevové pole $\mathcal{A}$ je právě systém všech podmnožin v $\Omega$. *Klasická pravděpodobnost* je pravděpodobnostní prostor $(\Omega, \mathcal{A}, P)$ s pravděpodobnostní funkcí

$$P : \mathcal{A} \to \mathbb{R}, \quad P(A) = \frac{|A|}{|\Omega|},$$

kde $|A|$ značí počet prvků množiny $A \in \mathcal{A}$.

Zjevně takto zadaná funkce skutečně definuje pravděpodobnost, ověřte si samostatně všechny požadované axiomy.

**1.17. Sčítání pravděpodobností.** U neslučitelných jevů je sčítání pravděpodobností pro výskyt alespoň jednoho z nich přímo požadováno v základní definici pravděpodobnosti. Obecně je sčítání pravděpodobností pro výskyty jevů složité. Problém totiž je, že pokud jsou jevy slučitelné, částečně máme v součtu pravděpodobností započteny příznivé výskyty vícekrát.



Nejjednodušší je si nejprve představit situaci se dvěma slučitelnými jevy $A$, $B$. Uvažme nejprve klasickou pravděpodobnost, kde jde vlastně o počítání prvků v podmnožinách. Pravděpodobnost výskytu alespoň jednoho z nich, tj. pravděpodobnost jejich sjednocení, je dána vztahem

$$P(A \cup B) = P(A) + P(B) - P(A \cap B), \tag{1.11}$$

protože ty prvky, které patří do množiny $A$ i $B$, jsme nejprve započetli dvakrát, a tak je musíme jednou odečíst.

Tentýž výsledek dostaneme i pro obecnou pravděpodobnost $P$ na nějakém jevovém poli. Protože $A \cap B$ a $A \setminus B$ jsou nezávislé jevy, platí

$$P(A) = P(A \setminus B) + P(A \cap B).$$

Podobně pro $A \cup B$ máme

$$P(A \cup B) = P(A \setminus B) + P(B \setminus A) + P(A \cap B).$$

Dosazením za pravděpodobnosti množinových rozdílů dostáváme opět vztah (1.11).



Následující věta je přímým promítnutím tzv. kombinatorického *principu inkluze a exkluze* do naší konečné pravděpodobnosti a říká, jakým způsobem vícenásobné započítávání výsledků kompenzovat v obecném případě.

Jde patrně o dobrý příklad matematického tvrzení, kde nejtěžší je najít dobrou formulaci a pak se dá říci, že (intuitivně) je tvrzení zřejmé.

Na obrázku je situace znázorněna pro tři množiny $A$, $B$, $C$ a pro klasickou pravděpodobnost. Jednoduše šrafované oblasti v prostém součtu máme dvakrát, dvojitě šrafované třikrát. Pak ty jednoduše šrafované jednou odečteme, přitom ty dvojitě šrafované opět třikrát odečteme, proto je tam nakonec ještě jednou započteme.

Ze známé klasické pravděpodobnosti pro jednotlivé hody umíme odvodit pravděpodobnosti našich jevů v $\Omega$. Není to ale jistě klasická pravděpodobnost. Tak pro diskutovaný jev chceme popsat, s jakou pravděpodobností nepadne šestka při prvém hodu a zároveň padne při druhém. Vnucuje se řešení

$$P(A) = \frac{5}{6} \cdot \frac{1}{6} = \frac{5}{36},$$

protože v prvém hodu padne s pravděpodobností $1 - \frac{1}{6}$ jiné číslo než šest a druhý hod, ve kterém naopak požadujeme šestku, je zcela nezávislý na prvním. Samozřejmě toto není poměr počtu příznivých výsledků k velikosti celého stavového prostoru!

Obecněji můžeme říci, že po právě $1 < k < 100$ hodech pokus skončí s pravděpodobností $(\frac{5}{6})^{k-1} \cdot \frac{1}{6}$. Ze všech možností je tedy nejpravděpodobnější, že skončí již napoprvé.

Jiný příklad, jak z házení kostkou dostat různě pravděpodobné jevy, je pozorovat součty při hodu více kostkami. Uvažujme takto: při hodu jednou kostkou je každý výsledek stejně pravděpodobný s pravděpodobností $\frac{1}{6}$. Při hodu dvěma kostkami je každý předem zvolený výsledek $(a, b)$, tj. dvojice přirozených čísel od jedné do šesti (včetně pořadí), stejně pravděpodobný s pravděpodobností $\frac{1}{36}$. Pokud se budeme ptát po dvou pětkách, je tedy pravděpodobnost poloviční než u dvou různých hodnot bez uvedení pořadí. Pro jednotlivé možné součty uvedené v horním řádku nám vychází počet možností v řádku dolním:

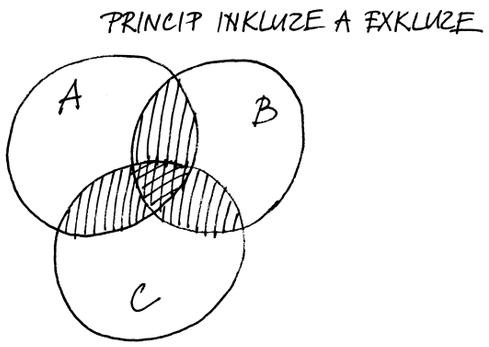
| Součet | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Počet | 1 | 2 | 3 | 4 | 5 | 6 | 5 | 4 | 3 | 2 | 1 |

.

Podobně vyjde pravděpodobnost $\frac{1}{216}$ jednotlivých výsledků hodu třemi kostkami, včetně určeného pořadí. Pokud se budeme ptát na pravděpodobnost výsledného součtu při hodu více kostkami, musíme pouze určit, kolik je možností, jak daného součtu dosáhnout a příslušné pravděpodobnosti sečíst.

**1.41. Princip inkluze a exkluze.** Sekretářka má rozeslat šest dopisů šesti různým lidem. Dopisy pro různé adresáty vkládá do obálek s adresami náhodně. Jaká je pravděpodobnost, že alespoň jeden člověk dostane dopis určený pro něj?






Obecně si díky aditivní vlastnosti pravděpodobnosti můžeme představit, že každý jev rozložíme na elementární (tj. jednobodové) jevy, jakkoliv ve skutečnosti nemusí jednoprvkové podmnožiny do uvažovaného jevového pole patřit. Pak je pravděpodobnost každého jevu dána součtem pravděpodobností jednotlivých elementárních jevů do něj patřících a můžeme při vyjádření pravděpodobnosti nastoupení alespoň jednoho z jevů postupovat takto: sečteme všechny pravděpodobnosti výsledků pro všechna $A_i$ zvlášť, pak ovšem musíme odečíst ty, které tam jsou započteny dvakrát (tj. prvky v průnicích dvou). Teď si ovšem dovolujeme odečíst příliš mnoho tam, kde ve skutečnosti byly prvky třikrát, tj. korigujeme přičtením pravděpodobností ze třetího členu, atd.

**Věta.** *Buďte $A_1, \ldots, A_k \in \mathcal{A}$ libovolné jevy na základním prostoru $\Omega$ s jevovým polem $\mathcal{A}$. Pak platí*

$$P\left(\cup_{i=1}^{k} A_i\right) = \sum_{i=1}^{k} P(A_i) - \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} P(A_i \cap A_j) + \\ + \sum_{i=1}^{k-2} \sum_{j=i+1}^{k-1} \sum_{\ell=j+1}^{k} P(A_i \cap A_j \cap A_\ell) - \ldots + \\ + (-1)^{k-1} P(A_1 \cap A_2 \cap \ldots \cap A_k).$$

Důkaz. Aby se výše naznačený postup stal důkazem, je zapotřebí si ujasnit, že skutečně všechny korekce, tak jak jsou popsány, jsou skutečně s koeficienty jedna. Místo toho můžeme snáze dát dohromady formálnější důkaz matematickou indukcí přes počet $k$ jevů, jejichž pravděpodobnosti sčítáme. Zkuste si průběžně porovnávat oba postupy, mělo by to vést k vyjasnění, co to znamená „dokázat“ a co „porozumět“.



Pro $k = 1$ tvrzení zjevně platí, vztah pro $k = 2$ je totožný s rovností (1.11) a tu jsme pro obecné pravděpodobnostní funkce již dokázali také.

Předpokládejme tedy, že věta platí pro všechny počty množin až do pevně zvoleného $k \geq 1$. Nyní můžeme pracovat v indukčním kroku se vztahem pro $k + 1$ jevů, když sjednocení prvních $k$ jevů bereme jako $A$ ve vzorci (1.11) výše, zatímco zbývající jev hraje roli $B$:

$$P\left(\cup_{i=1}^{k+1} A_i\right) = P\left(\left(\cup_{i=1}^{k} A_i\right) \cup A_{k+1}\right) = \\ = \sum_{j=1}^{k} \left( (-1)^{j+1} \sum_{1 \leq i_1 < \cdots < i_j \leq k} P(A_{i_1} \cap \cdots \cap A_{i_j}) \right) + \\ + P(A_{k+1}) - P((A_1 \cup \cdots \cup A_k) \cap A_{k+1}).$$

**Řešení.** Spočítejme pravděpodobnost jevu opačného, tedy toho, že ani jeden člověk neobdrží správný dopis. Stavový prostor všech možných jevů odpovídá všem možným pořadím pěti prvků (obálek). Označíme-li jak obálky tak dopisy čísly od jedné do šesti, tak všechny příznivé jevy (tedy žádný dopis nepřijde do obálky se stejným číslem) odpovídají takovým pořadím šesti prvků, kdy $i$-tý prvek není na $i$-tém místě ($i = 1, \dots, 6$), tzv. pořadím bez pevného bodu. Jejich počet spočítáme pomocí principu inkluze a exkluze. Označíme-li $M_i$ množinu permutací s pevným bodem $i$ (permutace v $M_i$ ale mohou mít i jiné pevné body), tak výsledný počet $d$ permutací bez pevného bodu je roven

$$d = 6! - |M_1 \cup \dots \cup M_6|.$$

Počet prvků průniku $|M_{i_1} \cap \dots \cap M_{i_k}|, k = 1, \dots, 6$, je $(6-k)!$ (pořadí prvků $i_1, \dots, i_k$ je pevně dáno, ostatních $6-k$ prvků řadíme libovolně). Podle principu inkluze a exkluze je

$$|M_1 \cup \dots \cup M_6| = \sum_{k=1}^{6} (-1)^{k+1} \binom{6}{k} (6-k)!$$

a tedy pro hledaný počet $d$ dostáváme vztah

$$d = 6! - \sum_{k=1}^{6} (-1)^{k+1} \binom{6}{k} (n-k)! =$$
$$= \sum_{k=0}^{6} (-1)^{k} \binom{6}{k} (6-k)! = 6! \sum_{k=0}^{6} \frac{(-1)^k}{k!}.$$

Pravděpodobnost toho, že žádný člověk neobdrží „svůj“ dopis je tedy

$$\sum_{k=0}^{6} \frac{(-1)^k}{k!} = \frac{53}{144}$$

a hledaná pravděpodobnost pak

$$1 - \textstyle\sum_{k=0}^{6} \frac{(-1)^k}{k!} = \frac{91}{144}. \qquad \square$$

**Poznámka.** Všimněme si, že odpověď na stejnou otázku se s rostoucím počtem dopisů příliš nemění. Pro $n$ dopisů je pravděpodobnost, že sekretářka dá alespoň jeden do správné obálky, rovna

$$1 - \sum_{k=0}^{n} \frac{(-1)^k}{k!} \doteq 1 - \frac{1}{e}.$$

Jak totiž uvidíme později, uvedená suma konverguje (blíží se) k hodnotě $1/e$.

Následující příklad je jednoduchým modelem, který odhaduje pravděpodobnost úmrtí osoby při dopravní nehodě.

To už připomíná formuli pro $k+1$ sčítaných jevů, nicméně nám ve velké sumě chybějí všechny výrazy obsahující $A_{k+1}$ a člen s pravděpodobností současného nastoupení všech jevů. Zato nám však přebývá poslední člen. Tento člen výrazu můžeme nahradit výrazem

$$-P((A_1 \cap A_{k+1}) \cup \dots \cup (A_k \cap A_{k+1}))$$

a pro tento výraz opět použít indukční předpoklad, tj. formuli ve větě. Při troše trpělivosti (a dostatečně velkém papíru na rozepsání všech členů) ověříme, že tím právě přidáme všechny dosud chybějící členy. $\square$

**1.18. Princip inkluze a exkluze.** Speciálním případem předchozí věty je případ klasické pravděpodobnosti, kdy všechny konečné podmnožiny základního prostoru jsou jevy a všechny elementární jevy mají stejnou pravděpodobnost. Ve vzorci z předchozí věty pak všechny pravděpodobnosti dávají právě počet prvků příslušných podmnožin až na společný faktor $\frac{1}{n}$, kde $n$ je počet prvků základního prostoru.



Takto můžeme z věty 1.17 vyčíst následující tvrzení pro mohutnosti obecné konečné množiny $M$ a jejích podmnožin $A_1, \dots, A_k$. Jako obvykle píšeme $|M|$ pro počet prvků množiny $M$.

Samozřejmě pro konečnou množinu $M$ a její podmnožiny platí

$$|M \setminus (\cup_{i=1}^{k} A_i)| = |M| - |\cup_{i=1}^{k} A_i|.$$

Nyní můžeme dosadit z předchozí věty za mohutnost sjednocení na pravé straně a dostáváme tvrzení, kterému se říká *princip inkluze a exkluze*.

$$|M \setminus (\cup_{i=1}^{k} A_i)| =$$
$$= |M| + \sum_{j=1}^{k} \Big( (-1)^j \sum_{1 \le i_1 < \dots < i_j \le k} |A_{i_1} \cap \dots \cap A_{i_j}| \Big).$$

Opět je snadné nakreslit si tvrzení pro dvě nebo tři množiny, viz obrázek před větou 1.17.

**1.19. Nezávislé jevy.** Vraťme se na chvíli k jednoduchému modelu dokonalé hrací kostky. Bude nás zajímat, jak mohou být jevy závislé.

Např. pravděpodobnost, že nastanou zároveň jevy „padne liché číslo“ a „padne alespoň trojka“, je $\frac{1}{3}$. To je totéž jako $\frac{1}{2} \cdot \frac{2}{3}$, tedy součin pravděpodobností jednotlivých jevů. To odpovídá představě, že můžeme nezávisle testovat obě podmínky a výsledná pravděpodobnost současného splnění bude dána součinem pravděpodobnostní dílčích. Jestliže budeme naopak uvažovat neslučitelné jevy, jako jsou např. „padne sudé číslo“ a „padne liché číslo“, bude pravděpodobnost současného výskytu obou nulová, zatímco součin dílčích pravděpodobností nulový není.

To odpovídá přestavě, že tyto dva jevy musí být závislé, protože výskyt jednoho z nich ten druhý už vylučuje. Samozřejmě může nastávat slabší závislost, např. jev „padne liché číslo“ je důsledkem jevu „padne trojka“ a proto také není dána pravděpodobnost společného výskytu těchto dvou jevů pomocí součinu.

Pro pravděpodobnosti $P$ na libovolných jevových polích řekneme, že jevy $A$ a $B$ jsou *stochasticky nezávislé*, jestliže platí

$$P(A \cap B) = P(A) \cdot P(B).$$

**1.42.** Ročně zahyne na silnicích v ČR přibližně 1200 českých občanů. Určete pravděpodobnost, že někdo z vybrané skupiny pěti set Čechů zemře v následujících deseti letech při dopravní nehodě. Předpokládejte pro zjednodušení, že každý občan má v jednom roce stejnou „šanci" zemřít při dopravní nehodě a to $1200/10^7$.

**Řešení.** Spočítejme nejprve pravděpodobnost, že jeden vybraný člověk v následujících deseti letech **nezahyne** při dopravní nehodě. Pravděpodobnost, že nezahyne v jednom roce, je $\left(1-\frac{12}{10^5}\right)$. Pravděpodobnost, že nezahyne v následujících deseti letech, je pak $\left(1-\frac{12}{10^5}\right)^{10}$. Pravděpodobnost, že v následujících deseti letech nezahyne nikdo z daných pěti set lidí, je opět podle pravidla součinu (jedná se o nezávislé jevy) $\left(1-\frac{12}{10^5}\right)^{5000}$. Pravděpodobnost jevu opačného, tedy toho, že někdo z vybraných pěti set lidí zahyne, je

$$1-\left(1-\tfrac{12}{10^5}\right)^{5000} \doteq 0{,}4512. \qquad \square$$

**Poznámka.** Model, který jsme použili v předchozím příkladu k popisu zadané situace, je pouze přibližný. Problém spočívá v podmínce, že každý občan z vyšetřovaného vzorku má stejnou pravděpodobnost toho, že v průběhu roku zahyne, kterou jsme odhadli z počtu usmrcených osob za rok. Počet tragických nehod se totiž rok od roku mění a i kdyby se neměnil, tak se mění populace. Ukažme si jednu z nepřesností příkladu na jiném způsobu řešení: zahyne-li 1200 osob za rok, tak za deset let zahyne 12000. Pravděpodobnost toho, že konkrétní člověk zahyne v průběhu deseti let tedy můžeme odhadnout i zlomkem $12000/10^7$. Pravděpodobnost, že konkrétní osoba nezahyne v průběhu 10 let je tedy $\left(1-\frac{12}{10^4}\right)$ (to jsou první dva členy binomického rozvoje $\left(1-\frac{12}{10^5}\right)^{10}$). Celkem dostáváme analogicky jako v předchozím řešení odhad pravděpodobnosti

$$1-\left(1-\frac{12}{10^4}\right)^{500} \doteq 0{,}4514.$$

Vidíme, že oba odhady jsou velmi blízké.

Snaha použít matematických znalostí k výhře v nejrůznějších hazardních hrách je velmi stará. Podívejme se na jednoduchý příklad.

Nyní si procvičme tzv. „podmíněnou" pravděpodobnost, viz (1.20).

**1.43.** Jaká je pravděpodobnost toho, že při hodu dvěma kostkami padne součet 7, víme-li, že ani na jedné z kostek nepadlo číslo 2?

**Řešení.** Označme jako $B$ jev, že ani na jedné kostce nepadne dvojka, jev „padne součet 7" označme jako $A$. Množinu všech možných výsledků budeme značit opět jako $\Omega$. Pak

$$P(A|B)=\frac{P(A\cap B)}{P(B)}=\frac{\frac{|A\cap B|}{|\Omega|}}{\frac{|B|}{|\Omega|}}=\frac{|A\cap B|}{|B|}.$$

Zkusme ale tutéž hru s kostkou s více jevy, třebas jev $A$ „padne liché číslo", jev $B$ „padne alespoň 3" a jev $C$ „padne nejvýše 3". Pravděpodobnosti jsou

$$P(A)=\frac{1}{2},\ P(B)=\frac{2}{3},\ P(C)=\frac{1}{2},$$
$$P(A\cap B\cap C)=\frac{1}{6}=\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{1}{2},$$

ale po dvojicích dostáváme např. $P(A\cap C)=\frac{2}{3}\neq\frac{1}{2}\cdot\frac{1}{2}$.

Naopak ani tři jevy $A$, $B$, $C$ které jsou po dvou nezávislé, nemusí splňovat vlastnost $P(A\cap B\cap C)=P(A)\cdot P(B)\cdot P(C)$: nechť $\Omega$ je devítiprvkový základní prostor složený ze slov $aaa$, $bbb$, $ccc$, $abc$, $acb$, $bac$, $bca$, $cab$, $cba$. Označme jako $A$ jev „na prvním místě slova je písmeno $a$". Dále nechť $B$ je jev „na druhém místě slova je písmeno $a$" a $C$ je jev „na třetím místě slova je písmeno $a$". Pak $P(A)=P(\{aaa,abc,acb\})=\frac{1}{3}$ a obdobně $P(B)=P(C)=\frac{1}{3}$. Potom $P(A\cap B)=P(A\cap C)=P(B\cap C)=P(\{aaa\}=\frac{1}{9}$. Tedy jevy jsou po dvou nezávislé, ale $P(A\cap B\cap C)=P(\{aaa\}=\frac{1}{9}\neq P(A)\cdot P(B)\cdot P(C)$.

Obecně tedy definujeme nezávislé jevy takto:



**Definice.** Uvažme libovolný pravděpodobnostní prostor $(\Omega,\mathcal{A},P)$ a v něm $k$ jevů $A_1,\dots,A_k$. Řekneme, že tyto jevy jsou *stochasticky nezávislé* (vzhledem k pravděpodobnosti $P$), jestliže pro libovolné z nich vybrané jevy $A_{i_1},\dots,A_{i_\ell}$, $1\le\ell\le k$ platí

$$P(A_{i_1}\cap\cdots\cap A_{i_\ell})=P(A_{i_1})\cdot\ldots\cdot P(A_{i_\ell}).$$

Zjevně je každý podsystém stochasticky nezávislých jevů opět stochasticky nezávislý. Dále si pro dva stochasticky nezávislé jevy $A$, $B$ spočtěme

$$P\left(A\cap B^c\right)=P(A\setminus B)=P(A)-P(A\cap B)=$$
$$=P(A)(1-P(B))=P(A)P\left(B^c\right).$$

Odtud už snadno dovodíme, že záměnou jednoho nebo více stochasticky nezávislých jevů za jejich opačné jevy obdržíme opět stochasticky nezávislé jevy.

Často je potřebná pravděpodobnost, že nastane alespoň jeden ze stochasticky nezávislých jevů, tzn. hledáme $P(A_1\cup\cdots\cup A_k)$. Můžeme pak použít elementární vlastnosti množinových operací, tzv. de Morganova pravidla

$$(\cup_{i\in I}A_i)^c=\cap_{i\in I}A_i^c,$$
$$(\cap_{i\in I}A_i)^c=\cup_{i\in I}A_i^c,$$

a dostáváme

$$P(A_1\cup\cdots\cup A_k)=1-P\left(A_1^c\cap\cdots\cap A_k^c\right)=$$
$$=1-(1-P(A_1))\dots(1-P(A_k)). \tag{1.12}$$

**1.20. Podmíněná pravděpodobnost.** Míru závislosti dvou jevů



můžeme přeformulovat s představou, že zkoumáme jeden z nich za podmínky, že druhý nastal. U nezávislých by podmínka neměla mít žádný vliv. Např. „jaká je pravděpodobnost, že při hodu dvěma kostkami padly dvě pětky, je-li součet hodnot deset?". Formalizovat takový postup umíme následovně.

Číslo 7 může padnout čtyřmi různými způsoby, pokud nepadne dvojka, tedy $|A \cap B| = 4$, $|B| = 5 \cdot 5 = 25$, tedy

$$P(A|B) = \frac{4}{25}.$$

Všimněme si, že $P(A) = \frac{1}{6}$, tedy jevy $A$ a $B$ jsou závislé. □

**1.44.** Michal má dvě poštovní schránky, jednu na gmail.com a jednu na seznam.cz. Uživatelské jméno má stejné na obou serverech, hesla různá (ale nepamatuje si, které heslo má na kterém serveru). Při zadávání hesla při přístupu do schránky se splete s pravděpodobností 5% (tj. jestliže chce zadat jemu známé slovo jako heslo, tak jej s pravděpodobností 95% skutečně správně na klávesnici zadá). Michal zadal na serveru seznam.cz jméno a heslo a server mu oznámil, že něco není v pořádku. Jaká je pravděpodobnost, že chtěl zadat správné heslo, ale pouze se „překlepnul" při zadávání? (Předpokládáme, že uživatelské jméno zadá vždy bez chyby.)

**Řešení.** Označme $A$ jev, že Michal fyzicky zadal na serveru seznam.cz špatné heslo. Tento jev je sjednocením dvou disjunktních jevů:

$A_1$ : chtěl zadat správné heslo a přepsal se,

$A_2$ : chtěl zadat špatné heslo (to z gmail.com) a buď se přepsal nebo ne.

Hledáme tedy podmíněnou pravděpodobnost $P(A_1|A)$, ta je podle vztahu pro podmíněnou pravděpodobnost rovna

$$P(A_1|A) = \frac{P(A_1 \cap A)}{P(A)} = \frac{P(A_1)}{P(A_1 \cup A_2)} = \\ = \frac{P(A_1)}{P(A_1) + P(A_2)}.$$

Potřebujeme tedy určit pravděpodobnosti $P(A_1)$ a $P(A_2)$. Jev $A_1$ je konjunkcí (průnikem) dvou nezávislých jevů: Michal chtěl zadat správné heslo a Michal se při zadávání přepsal. Dle zadání je pravděpodobnost prvního z nich 1/2, druhého 1/20, celkem $P(A_1) = \frac{1}{2} \cdot \frac{1}{20} = \frac{1}{40}$ (pravděpodobnosti násobíme, protože se jedná o nezávislé jevy). Dále je ze zadání $P(A_2) = \frac{1}{2}$. Celkem $P(A) = P(A_1) + P(A_2) = \frac{1}{40} + \frac{1}{2} = \frac{21}{40}$, a můžeme vyčíslit:

$$P(A_1|A) = \frac{P(A_1)}{P(A)} = \frac{\frac{1}{40}}{\frac{21}{40}} = \frac{1}{21}.$$ □

Metodu *geometrické pravděpodobnosti*, (viz 1.21 můžeme použít v případě, že daný základní prostor sestává z nekonečně mnoha elementárních jevů, které dohromady vyplňují nějakou oblast na přímce, rovině, prostoru (u které umíme určit její délku, obsah, objem, ...). Předpokládáme, že pravděpodobnost toho, že nastane elementární jev

### Podmíněná pravděpodobnost

**Definice.** Nechť $H$ je jev s nenulovou pravděpodobností v jevovém poli $\mathcal{A}$ v pravděpodobnostním prostoru $(\Omega, \mathcal{A}, P)$. *Podmíněná pravděpodobnost* $P(A|H)$ jevu $A \in \mathcal{A}$ vzhledem k hypotéze $H$ je definována vztahem

$$P(A|H) = \frac{P(A \cap H)}{P(H)}.$$

Jak je vidět přímo z definice, hypotéza $H$ a jev $A$ jsou skutečně nezávislé tehdy a jen tehdy, je-li $P(A) = P(A|H)$. Přímo z definice také vyplývá tzv. „věta o násobení pravděpodobností". Mámeli dva jevy $A_1$, $A_2$ splňující $P(A_1 \cap A_2) > 0$, potom

$$P(A_1 \cap A_2) = P(A_2)P(A_1|A_2) = P(A_1)P(A_2|A_1).$$

Všechna tato čísla vyjadřují pravděpodobnost toho, že nastanou oba jevy $A_1$ i $A_2$, jenom jinými způsoby. Například v posledním případě nejprve sledujeme, zda nastane první jev. Potom za předpokladu, že ten první nastal, sledujeme zda nastane i ten druhý. Podobně pro tři jevy $A_1$, $A_2$, $A_3$ splňující $P(A_1 \cap A_2 \cap A_3) > 0$ dostaneme

$$P(A_1 \cap A_2 \cap A_3) = P(A_1)P(A_2|A_1)P(A_3|A_1 \cap A_2).$$

Slovy to lze opět popsat tak, že pravděpodobnost výskytu všech tří jevů zároveň můžeme spočítat tak, že se nejprve zabýváme výskytem pouze prvního z nich, potom druhého za předpokladu, že první už nastal, a naposledy třetího za předpokladu, že oba předešlé jevy již nastaly.

Máme-li obecný počet $k$ jevů $A_1, \ldots, A_k$ splňujících $P(A_1 \cap \cdots \cap A_k) > 0$, pak věta říká následující:

$$P(A_1 \cap \cdots \cap A_k) = P(A_1)P(A_2|A_1)\cdots P(A_k|A_1 \cap \cdots \cap A_{k-1}).$$

Skutečně, dle předpokladu jsou i pravděpodobnosti všech průniků, které jsou brány ve výrazu za hypotézy, nenulové. Pokrácením čitatelů a jmenovatelů získáme i napravo právě pravděpodobnost jevu odpovídajícího průniku všech uvažovaných jevů.

**1.21. Geometrická pravděpodobnost.** V praktických problémech se často setkáváme s daleko složitějšími modely, kde základní prostor není konečnou množinou. Nemáme momentálně k dispozici ani základní nástroje pro dostatečné zobecnění pojmu pravděpodobnosti, nicméně můžeme uvést alespoň jednoduchou ilustraci.



Uvažme rovinu $\mathbb{R}^2$ dvojic reálných čísel a v ní podmnožinu $\Omega$ se známým obsahem $\mathrm{vol}\,\Omega$ (symbol „vol" je od anglického „volume", tj. obsah/objem). Příkladem může sloužit třeba jednotkový čtverec. Náhodné jevy budou reprezentovány podmnožinami $A \subseteq \Omega$ a za jevové pole $\mathcal{A}$ bereme nějaký vhodný systém podmnožin, u kterých umíme určit jejich obsah. Nastoupení nebo nenastoupení jevu je dáno výběrem bodu v $\Omega$, kterým se trefíme nebo netrefíme do množiny reprezentující jev $A$.

Uvažme jako příklad problém, kdy náhodně vybereme dvě hodnoty $a < b$ v intervalu $[0, 1] \subseteq \mathbb{R}$. Všechny hodnoty $a$ i $b$ jsou stejně pravděpodobné a otázka zní „jaká je pravděpodobnost, že interval $(a, b)$ bude mít velikost alespoň jedna polovina?". Volba čísel $a, b$ je volbou libovolného bodu $[a, b]$ ve vnitřku trojúhelníku $\Omega$ s hraničními vrcholy $[0, 0]$, $[0, 1]$, $[1, 1]$ (viz obrázek).

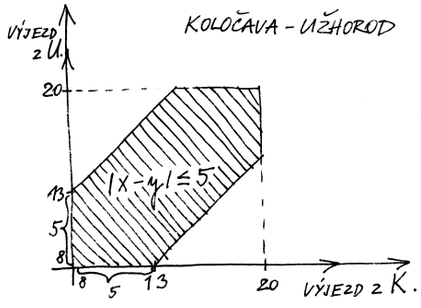
z určité podoblasti je rovna poměru její velikosti (délce, obsahu, ...) k velikosti celého základního prostoru.

**1.45.** Z Těšína vyjíždí vlaky co půl hodinu (směrem na Bohumín) a z tohoto směru přijíždějí také každé půl hodiny. Předpokládejme, že vlaky se mezi těmito dvěma stanicemi pohybují rovnoměrnou rychlostí 72 km/h a jsou dlouhé 100 metrů, cesta trvá 30 minut, vlaky se míjejí někde na trase. Nevyspalý hazardér Jarek si vybere jeden z těchto vlaků a během cesty z Těšína do Bohumína náhodně vystrčí hlavu z okna na pět vteřin nad kolejiště pro protější směr. Jaká je pravděpodobnost, že mu bude uražena? (Předpokládáme, že jiné než zmíněné vlaky na trati nejezdí.)

**Řešení.** Vzájemná rychlost protijedoucích vlaků je $40\,m/s$, protijedoucí vlak mine Jardovo okno za dvě a půl sekundy. Prostor všech možností je tedy interval $[0, 1800\,s]$, prostor „příznivých" možností je potom interval délky $7{,}5\,s$ ležící někde uvnitř předchozí úsečky. Pravděpodobnost uražení hlavy je tedy $7, 5/1800 \doteq 0{,}004$. □

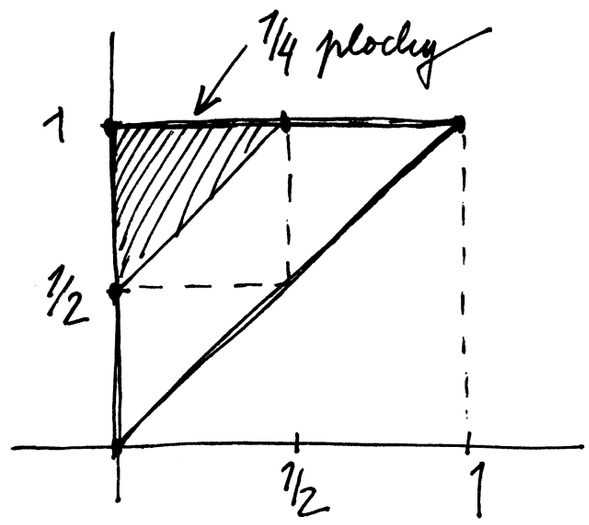
**1.46.** Jednou denně někdy mezi osmou hodinou ranní a osmou hodinou večerní vyjíždí náhodně autobus z Koločavy do Užhorodu. Jednou denně ve stejném časovém rozmezí jezdí jiný autobus náhodně opačným směrem. Cesta tam trvá pět hodin, zpět též pět hodin. Jaká je pravděpodobnost, že se autobusy potkají, jezdí-li po stejné trase?

**Řešení.** Prostor všech možných jevů je čtverec $12 \times 12$, Označíme-li doby odjezdu obou autobusů $x$, resp. $y$, pak se tyto na trase potkají právě když $|x - y| \leq 5$. Tato nerovnost vymezuje v daném čtverci oblast „příznivých jevů". Obsah zbylé části spočítáme přímo jednodušeji, neboť je sjednocením dvou pravoúhlých rovnoramenných trojúhelníků o odvěsnách délky 7, tedy je roven 49, obsah části odpovídající „příznivým jevům" je tedy $144 - 49 = 95$, celkem je hledaná pravděpodobnost $p = \frac{95}{144} \doteq 0{,}66$.




□

**1.47.** Dvoumetrová tyč je náhodně rozdělena na tři díly. Určete pravděpodobnost, že alespoň jeden díl bude nejvýše 20 cm dlouhý.




Úlohu si můžeme představit jako popis problému, kdy se hodně unavený účastník večírku nad ránem pokouší dvěma řezy rozdělit párek na tři díly pro sebe a své dva kamarády. Jaká je pravděpodobnost, že se na někoho dostane aspoň půlka?

Odpověď je docela jednoduchá: Podobně jako u klasické pravděpodobnosti definujeme pravděpodobnostní funkci $P : \mathcal{A} \to \mathbb{R}$ vztahem

$$P(A) = \frac{\operatorname{vol} A}{\operatorname{vol} \Omega},$$

kde $A$ jsou podmnožiny v rovině, které odpovídají námi vybraným jevům.

Potřebujeme tedy znát plochu podmnožiny, která odpovídá bodům s $b \geq a + \frac{1}{2}$, tj. vnitřku trojúhelníku $A$ ohraničeného vrcholy $[0, \frac{1}{2}]$, $[0, 1]$, $[\frac{1}{2}, 1]$. Evidentně dostáváme $P(A) = \frac{1}{4}$.

Zkuste si samostatně odpovědět na otázku „pro jakou požadovanou minimální délku intervalu $(a, b)$ dostaneme pravděpodobnost jedna polovina?".

**1.22. Metody Monte Carlo.** Jednou z účinných výpočetních metod přibližných hodnot je naopak simulace známé takovéto pravděpodobnosti pomocí relativní četnosti nastoupení vhodně zvoleného jevu. Např. známá formule pro obsah kruhu o daném poloměru říká, že obsah jednotkového kruhu je roven právě konstantě

$$\pi = 3, 1415\ldots,$$

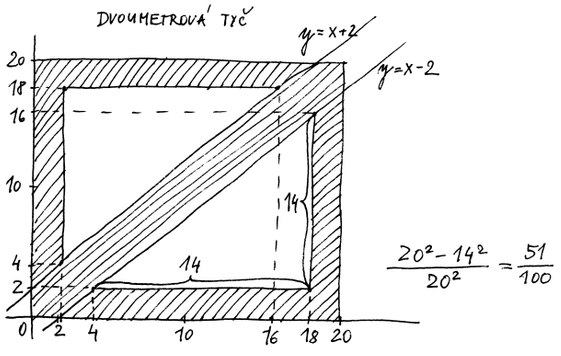
která vyjadřuje poměr obsahu kruhu a druhé mocniny jeho poloměru. (Tady si také povšimněme východiska, které jsme nedokázali – proč by měl být obsah kruhu roven konstantnímu násobku druhé mocniny poloměru? Matematicky to budeme umět ukázat, až zvládneme tzv. integrování. Experimentálně si to ale můžeme ověřit níže uvedeným postupem s různými velikostmi strany čtverce.)

Pokud zvolíme za $\Omega$ jednotkový čtverec a za $A$ průnik $\Omega$ a jednotkového kruhu se středem v počátku, pak $\operatorname{vol} A = \frac{1}{4}\pi$. Máme-li tedy spolehlivý generátor náhodných čísel mezi nulou a jedničkou a počítáme relativní četnosti, jak často bude vzdálenost bodu $[a, b]$ (určeného vygenerovanou dvojicí $a, b$) od počátku menší než jedna, tj. $a^2 + b^2 < 1$, pak výsledek bude při velkém počtu pokusů s velikou jistotou dobře aproximovat číslo $\frac{1}{4}\pi$.

**Řešení.** Náhodné rozdělení tyče na tři díly je dáno dvěma body řezu, čísly $x$ a $y$ (nejprve tyč rozřízneme ve vzdálenosti $x$ od počátku, nehýbeme s ní a dále ji rozřízneme ve vzdálenosti $y$ od počátku). Pravděpodobnostní prostor je tedy čtverec $C$ o straně 2 m. Umístíme-li čtverec $C$ tak, aby dvě jeho strany ležely na kartézských osách v rovině, tak podmínka, že alespoň jeden díl má být nejvýše 20 cm dlouhý, nám vymezuje ve čtverci následující oblast $O$:

$$O = \{(x, y) \in C \mid (x \leq 20) \vee (x \geq 180) \vee (y \leq 20) \vee \\ \vee (y \geq 180) \vee (|x - y|) \leq 20\}.$$

Jak snadno nahlédneme, zaujímá takto vymezená oblast $\frac{51}{100}$ obsahu čtverce.




□

## E. Geometrie v rovině

Vraťme se na chvíli ke komplexním číslům. Komplexní rovina je totiž „normální“ rovina, kde ovšem máme dáno něco navíc:

**1.48.** Interpretujte násobení imaginární jednotkou a vzetí komplexně sdruženého čísla jako geometrickou transformaci v rovině.

**Řešení.** Imaginární jednotka $i$ odpovídá bodu $(0, 1)$ a všimněme si, že vynásobení jakéhokoliv čísla $z = a + i\,b$ imaginární jednotkou dává výsledek

$$i \cdot (a + i\,b) = -b + i\,a$$

což v interpretaci v rovině znamená otočení bodu $z$ o pravý úhel v kladném smyslu, tj. proti směru hodinových ručiček.

Přiřazení komplexně sdruženého čísla je symetrie podle osy reálných čísel:

$$z = (a + i\,b) \mapsto (a - i\,b) = \bar{z}\,.$$ □

Nyní jeden známý, ale velmi pěkný příklad.

**1.49.** Určete součet úhlů, které v rovině $\mathbb{R}^2$ svírají s osou $x$ postupně vektory $(1, 1)$, $(2, 1)$ a $(3, 1)$

**Řešení.** Uvážíme-li rovinu $\mathbb{R}^2$ jakožto Gaussovu rovinu komplexních čísel, tak uvedené vektory odpovídají komplexním číslům $1 + i$, $2 + i$

Numerickým postupům založeným na tomto principu se říká *metody Monte Carlo*.

## 5. Geometrie v rovině



V posledních odstavcích jsme intuitivně používali elementární pojmy z geometrie reálné roviny. Teď budeme podrobněji zkoumat, jak se vypořádávat s potřebou popisovat „polohu v rovině“, resp. dávat do souvislostí polohy různých bodů roviny.

Nástrojem k tomu budou opět zobrazení, tentokrát to ale budou velice speciální pravidla přiřazující dvojicím hodnot $(x, y)$ dvojice $(w, z) = F(x, y)$. Zároveň půjde o předzvěst úvah z oblasti matematiky, které se říká *lineární algebra* a kterou se budeme podrobně zabývat v dalších třech kapitolách.

**1.23. Vektorový prostor $\mathbb{R}^2$.** Podívejme se na „rovinu“ jakožto na množinu dvojic reálných čísel $(x, y) \in \mathbb{R}^2$. Budeme jim říkat *vektory* v $\mathbb{R}^2$. Pro takové vektory umíme definovat sčítání „po složkách“, tj. pro vektory $u = (x, y)$ a $v = (x', y')$ klademe

$$u + v = (x + x', y + y').$$

Protože pro jednotlivé složky platí všechny vlastnosti komutativní grupy, evidentně budou tyto vlastnosti platit i pro naše nové sčítání vektorů. Zejména tedy máme tzv. *nulový vektor* $0 = (0, 0)$, jehož přičtením k jakémukoliv vektoru $v$ dostaneme opět vektor $v$. Záměrně teď používáme tentýž symbol 0 pro vektor i jeho skalární složky – z kontextu je vždy jasné, jakou „nulu“ máme kdy na mysli.

Dále definujeme násobení vektorů a skalárů tak, že pro $a \in \mathbb{R}$ a $v = (x, y) \in \mathbb{R}^2$ klademe

$$a \cdot v = (ax, ay).$$

Zpravidla budeme znak $\cdot$ vynechávat a pouhé zřetězení znaků $a\,v$ bude označovat skalární násobek vektoru. Přímo se ověří další vlastnosti pro násobení skaláry $a$, $b$ a sčítání vektorů $u$, $v$, např.

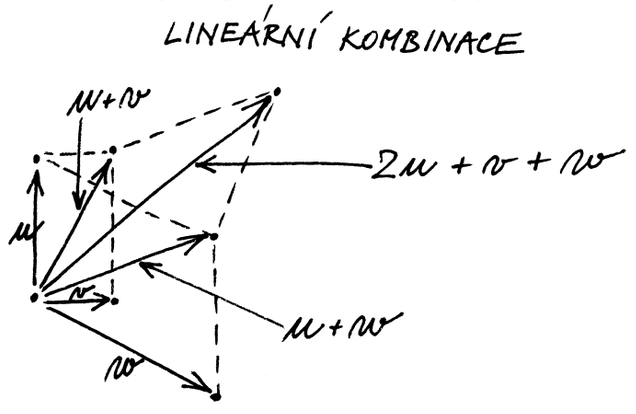
$$a\,(u + v) = a\,u + a\,v,\ \ (a + b)u = a\,u + b\,u,\ \ a(b\,u) = (ab)u,$$

kde opět používáme stejný znak plus pro sčítání vektorů i skalárů.



Tyto operace si můžeme dobře představit, jestliže uvažujeme vektory $v$ jako šipky začínající v počátku $0 = [0, 0]$ a končící v bodě $[x, y]$ v rovině.

Takové šipky pak můžeme přikládat jednu za druhou a to přesně odpovídá sčítání vektorů. Násobení skalárem $a$ pak odpovídá natažení dané šipky na $a$-násobek.



a $3+i$ a máme najít součet jejich argumentů, tedy podle Moivreovy věty argument jejich součinu. Jejich součin je $(1+i)\,(2+i)\,(3+i) = (1+3i)\,(3+i) = 10i$, tedy ryze imaginární číslo s argumentem $\pi/2$ a tedy hledaný součet je roven právě $\pi/2$. □

**1.50.** Napište obecnou rovnici přímky $p : x = 2-t,\ y = 1+3t,\ t \in \mathbb{R}$.

**Řešení.** Vektor $(-1, 3)$ je směrovým vektorem přímky $p$. Proto vektor $(3, 1)$ je jejím normálovým vektorem a obecná rovnice přímky $p$ má tvar

$$3x + y + c = 0$$

pro jisté $c \in \mathbb{R}$. Tuto konstantu $c$ určíme dosazením $x = 2$, $y = 1$ (přímka $p$ prochází bodem $[2, 1]$ daným volbou $t = 0$). Získáváme tak $c = -7$ a následně výsledek $3x + y - 7 = 0$. □

**1.51.** Je dána přímka

$$p :\ [2, 0] + t(3, 2),\ t \in \mathbb{R}.$$

Určete její obecnou rovnici a nalezněte průnik s přímkou

$$q :\ [-1, 2] + s(1, 3),\ s \in \mathbb{R}.$$

**Řešení.** Souřadnice bodů na přímce jsou dány dle daného parametrického zadání jako $x = 2+3t$ a $y = 0+2t$. Vyloučením parametru $t$ ze soustavy těchto dvou rovnic dostáváme obecnou rovnici přímky $p$:

$$2x - 3y - 4 = 0.$$

Průnik s přímkou $q$ získáme dosazením parametrického vyjádření bodů přímky $q$, tedy $x = -1 + s$ a $y = 2 + 3s$, do obecné rovnice přímky $p$:

$$2(-1 + s) - 3(2 + 3s) - 4 = 0,$$

odkud $s = -12/7$ a dosazením do parametrického vyjádření přímky $q$ dostáváme souřadnice průsečíku $P$:

$$P = \left[-\tfrac{19}{7}, -\tfrac{22}{7}\right].$$ □

**1.52.** Stanovte průsečík přímek

$$p : x + y - 4 = 0, \quad q : x = -1 + 2t,\ y = 2 + t,\ t \in \mathbb{R}.$$

**Řešení.** Nejdříve poznamenejme, že směrovým vektorem přímky $p$ je $u_p = (1, -1)$ (libovolný nenulový vektor kolmý k vektoru $(1, 1)$ z obecné rovnice přímky) a směrovým vektorem přímky $q$ je $u_q = (2, 1)$. To, že vektor $u_p$ není násobkem vektoru $u_q$, pak zaručuje, že se přímky protínají (přímky nejsou rovnoběžné).



Nyní můžeme udělat podstatný krok: jestliže si zapamatujeme dva významné vektory $e_1 = (1, 0)$ a $e_2 = (0, 1)$, pak každý jiný vektor dostaneme jako

$$u = (x, y) = x\,e_1 + y\,e_2.$$

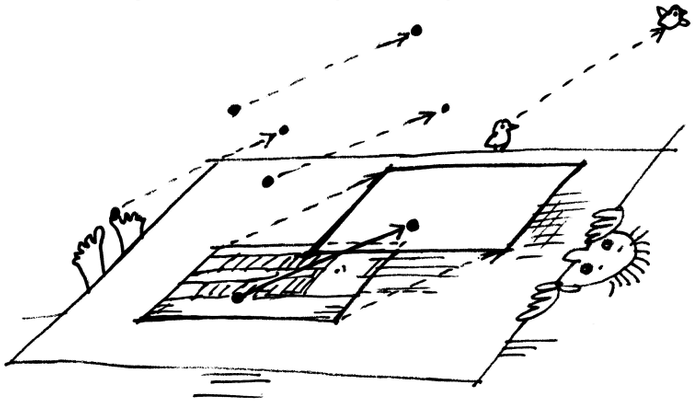
Výrazu napravo říkáme *lineární kombinace vektorů* $e_1$ a $e_2$. Dvojici vektorů $\underline{e} = (e_1, e_2)$ říkáme *báze* vektorového prostoru $\mathbb{R}^2$.

Jestliže si ale vybereme jiné dva vektory $u$, $v$, které nejsou jeden násobek druhého, tj. jinou bázi v $\mathbb{R}^2$, budeme moci udělat totéž. Lineární kombinace $w = x\,u + y\,v$ nám pro všechny různé dvojice $(x, y)$ dá právě všechny vektory $w$ v rovině.



Nakonec můžeme nahlížet vektory jako naše šipky v abstraktní poloze, tj. zapomeneme na ztotožnění bodů v rovině s dvojicemi čísel. Jenom budou naše šipky všechny „upoutány“ v bodě 0, který je zároveň nulovým vektorem. Zůstanou nám operace sčítání a násobení skaláry a teprve volbou báze $e_1$, $e_2$ ztotožníme naši rovinu šipek s $\mathbb{R}^2$.

**1.24. Afinní rovina.** Když si pevně vyvolíme nějaký vektor $u \in \mathbb{R}^2$, můžeme jej přičítat (tj. coby šipku přikládat) k libovolnému bodu $P = [x, y]$. Máme tak tedy s pevným vektorem definované *posunutí*, které každý bod roviny $P$ zobrazí na $P + u$.



Zkusme teď úplně zapomenout na souřadnice a vnímat celou rovinu jako množinu, na které fungují naše posunutí. Takovou množinu $A = \mathbb{R}^2$ si můžeme představit z pohledu pozorovatele, který sedí v některém pevně zvoleném místě (můžeme mu říkat třeba bod $O = [x_0, y_0] \in \mathbb{R}^2$). Předpokládejme, že ji vnímá jako nekonečnou desku bez jakýchkoliv zvolených měřítek a popisů a jenom ví, co to znamená posunout se o libovolný násobek nějakého vektoru $u \in \mathbb{R}^2$. Takové rovině budeme říkat „afinní rovina“.



Aby mohl vidět kolem sebe „dvojice reálných čísel“, musí si vybrat nějaký bod $E_1$, kterému řekne „bod $[1, 0]$“ a jiný bod $E_2$, kterému začne říkat „bod $[0, 1]$“. Jinými slovy, zvolí si bázi $e_1 = (1, 0), e_2 = (0, 1)$ mezi vektory posunutí. Do všech ostatních se pak dostane tak, že poskočí „$a$–krát ve směru $e_1$“ a pak „$b$–krát ve směru $e_2$“ a takovému bodu bude říkat „bod $[a, b]$“. Pokud to bude dělat obvyklým způsobem, nebude výsledek záviset na pořadí, tzn. může také napřed jít $b$–krát ve směru $e_2$ a pak teprve ve směru $e_1$.

To, co jsme popsali, se nazývá volba *(afinního) souřadného systému v rovině*, bod $O$ je jeho *počátkem*, a obecně každý bod $P$ roviny je ztotožněn s dvojicí čísel $[a, b]$, kterou také budeme psát jako *posunutí* $P - O$.

Bod $[x, y]$ je hledaným průsečíkem, právě když jeho souřadnice vyhovují rovnici přímky $p$ a současně existuje reálné číslo $t$, pro které

$$x = -1 + 2t, \quad y = 2 + t.$$

Dosadíme-li odsud do obecné rovnice $p$, obdržíme

$$(-1 + 2t) + (2 + t) - 4 = 0.$$

Této rovnici vyhovuje právě $t = 1$, což dává průsečík se souřadnicemi $x = 1, y = 3$. □

**1.53.** Najděte obecnou rovnici přímky $p$, jež prochází bodem $[2, 3]$ a je rovnoběžná s přímkou $x - 3y + 2 = 0$, a parametrickou rovnici přímky $q$ procházející body $[1, 3]$ a $[-2, 1]$.

**Řešení.** Každá přímka rovnoběžná s přímkou $x-3y+2 = 0$ je zadána rovnicí

$$x - 3y + c = 0$$

pro nějaké $c \in \mathbb{R}$. Přímka $p$ prochází bodem $[2, 3]$. Musí tedy platit

$$2 - 3 \cdot 3 + c = 0, \quad \text{tj.} \quad c = 7.$$

Pro přímku $q$ lze ihned uvést její parametrické vyjádření

$$q : [1, 3] + t\,(1 - (-2), 3 - 1) = [1, 3] + t\,(3, 2)\,, \ t \in \mathbb{R}. \quad \square$$

**1.54.** Zjistěte, zda některé z přímek

$$p_1 : 2x + 3y - 4 = 0, \qquad p_2 : x - y + 3 = 0,$$
$$p_3 : -2x + 2y = -6, \qquad p_4 : -x - \frac{3}{2}y + 2 = 0,$$
$$p_5 : x = 2 + t,\ y = -2 - t,\ t \in \mathbb{R}$$

(ne)jsou totožné.

**Řešení.** Je vidět, že

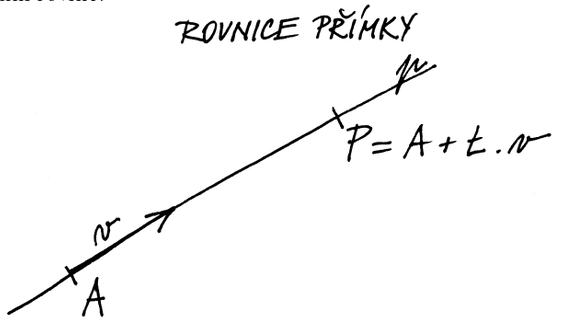
$$-2 \cdot \left(-x - \frac{3}{2}y + 2\right) = 2x + 3y - 4.$$

Obecné rovnice $p_1$ a $p_4$ tudíž zadávají stejnou přímku. Normálový vektor přímky $p_1$ je $(2, 3)$, pro přímku $p_2$ je $(1, -1)$, pro $p_3$ je $(-2, 2)$ a pro $p_5$ je $(1, 1)$ (kolmý vektor k vektoru $(1, -1)$). Přímky $p_2$ a $p_3$ jsou rovnoběžné (normálový vektor jedné je násobkem normálového vektoru druhé). Další dvojice rovnoběžných přímek neexistují. Neboť soustava

$$x - y + 3 = 0, \quad -2x + 2y + 6 = 0$$

zjevně nemá řešení, přímky $p_1$ a $p_4$ tvoří jedinou dvojici totožných přímek. □

Budeme dále pracovat v pevně zvolených souřadnicích, tj. s dvojicemi reálných čísel, ale pro lepší orientaci budeme vektory zapisovat s kulatými závorkami místo hranatých u souřadnic bodů v afinní rovině.




**1.25. Přímky v rovině.** Když se náš pozorovatel umí posouvat o libovolný násobek pevného vektoru, pak také ví, co je to *přímka*.



Je to podmnožina $p \subseteq A$ v rovině taková, že existují bod $O$ a nenulový vektor $v$ takové, že

$$p = \{P \in A;\ P - O\ = t \cdot v,\ t \in \mathbb{R}\}.$$

Popišme si $P = P(t) \in p$ ve zvolených souřadnicích s volbou $v = (\alpha, \beta)$:

$$x(t) = x_0 + \alpha \cdot t, \quad y(t) = y_0 + \beta \cdot t.$$

Protože vektor $v = (\alpha, \beta)$ je nenulový, musí být aspoň jedno z čísel $\alpha$, $\beta$ různé od nuly. Když pro určitost předpokládáme, že třeba $\alpha \neq 0$, pak vyloučíme $t$ z parametrického vyjádření pro $x$ a $y$ a jednoduchým výpočtem dostaneme

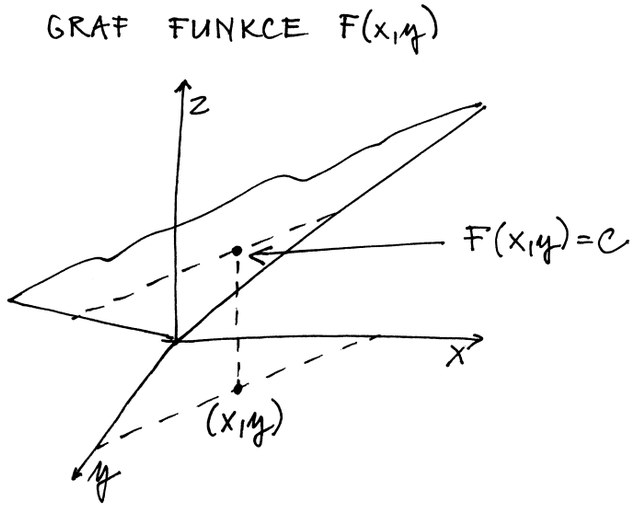
$$-\beta x + \alpha y = -\beta x_0 + \alpha y_0.$$

To je obecná rovnice přímky

$$ax + by = c \tag{1.13}$$

se známým vztahem dvojice čísel $(a, b) = (-\beta, \alpha)$ a směrového vektoru přímky $v = (\alpha, \beta)$

$$a\alpha + b\beta = 0. \tag{1.14}$$



**1.55.** Určete přímku $p$, která je kolmá k přímce $q : 6x - 7y + 13 = 0$ a prochází bodem $[-6, 7]$.

**Řešení.** Protože normálový vektor přímky $q$ je směrový vektor přímky $p$, můžeme bezprostředně napsat výsledek

$$p : x = -6 + 6t,\ y = 7 - 7t,\ t \in \mathbb{R}. \qquad \square$$

**1.56.** Udejte příklad čísel $a, b \in \mathbb{R}$, pro něž je vektor $u$ normálovým vektorem přímky $AB$, je-li $A = [1, 2]$, $B = [2b, b]$, $u = (a - b, 3)$.

**Řešení.** Směrovým vektorem přímky $AB$ je $(2b - 1,\ b - 2)$ (tento vektor je vždy nenulový), a proto jejím normálovým vektorem je $(2 - b,\ 2b - 1)$. Položíme-li

$$2 - b = a - b, \quad 2b - 1 = 3,$$

dostáváme $a = b = 2$. $\square$

**1.57.** Určete vzájemnou polohu přímek $p$ a $q$ v rovině, jestliže je $p : 2x - y - 5 = 0$ a $q : x + 2y - 5 = 0$. Pokud se jedná o různoběžky, nalezněte souřadnice jejich průsečíku.

**Řešení.** Z obecných rovnic přímek $p, q$ známe jejich normálové vektory $(2, -1)$, $(1, 2)$. Přímky jsou rovnoběžné právě tehdy, je-li normálový vektor jedné násobkem normálového vektoru druhé, což zřejmě pro přímky $p, q$ splněno není. Jde tedy o různoběžky. Průsečík nalezneme vyřešením soustavy

$$2x - y - 5 = 0, \quad x + 2y - 5 = 0.$$

Když z první rovnice vyjádříme $y = 2x - 5$ a dosadíme za $y$ do druhé, získáme

$$x + 2(2x - 5) - 5 = 0, \quad \text{tj. } x = 3.$$

Poté snadno určíme $y = 2 \cdot 3 - 5 = 1$. Přímky se tak protínají v bodě $[3, 1]$. $\square$

**1.58.** Uvažujme rovinu $\mathbb{R}^2$ se standardní soustavou souřadnic. Z počátku $[0, 0]$ je vyslán laserový paprsek ve směru $(3, 1)$. Dopadne na zrcadlovou přímku $p$ danou parametricky jako

$$p : [4, 3] + t(-2, 1)$$

a poté se odrazí (úhel dopadu je shodný s úhlem odrazu). V jakém bodě dopadne odražený paprsek na přímku $q$ danou parametricky jako

$$q : [7, -10] + t(-1, 6)?$$

**Řešení.** Směr paprsku svírá s přímkou $p$ úhel 45°, odražený paprsek tedy bude kolmý na dopadající, jeho směrový vektor bude $(1, -3)$ (Pozor na orientaci! Daný směrový vektor můžeme též získat například



Výraz nalevo v rovnici přímky (1.13) můžeme vidět jako skalární funkci $F$ závislou na bodech v rovině a s hodnotami v $\mathbb{R}$, samu rovnici pak jako požadavek na její hodnotu. Časem uvidíme, že vektor $(a, b)$ je v tomto případě právě směrem, ve kterém $F$ nejrychleji roste. Proto bude směr kolmý na $(a, b)$ právě tím směrem, ve kterém zůstává naše funkce $F$ konstantní. Konstanta $c$ pak určuje, kterou ze všech rovnoběžných přímek rovnice určuje.

Mějme nyní dvě přímky $p$ a $q$ a ptejme se po jejich průniku $p \cap q$. Ten bude popsán jako bod, splňující obě rovnice přímek současně. Pišme je takto

$$\begin{aligned} ax + by &= r, \\ cx + dy &= s. \end{aligned} \tag{1.15}$$

Opět můžeme levou stranu vnímat jako přiřazení, které každé dvojici souřadnic $[x, y]$ bodů $P$ v rovině přiřadí vektor hodnot dvou skalárních funkcí $F_1$ a $F_2$ daných levými stranami jednotlivých rovnic (1.15). Můžeme tedy naše rovnice napsat jako jediný vztah $F(v) = w$, kde $F$ je přiřazení, které vektor $v$ popisující polohu obecného bodu v rovině (v našich souřadnicích) zobrazí na vektor zadaný levou stranou rovnic, a požadujeme, aby se toto zobrazení strefilo do předem zadané hodnoty $w = (r, s)$.

**1.26. Lineární zobrazení a matice.** Přiřazení $F$, se kterými jsme



pracovali při popisu průniku přímek, mají jednu velice podstatnou společnou vlastnost: respektují operace sčítání a násobení s vektory a skaláry, tj. respektují lineární kombinace:

$$F(a \cdot v + b \cdot w) = a \cdot F(v) + b \cdot F(w)$$

pro všechna $a, b \in \mathbb{R}$, $v, w \in \mathbb{R}^2$. Říkáme, že $F$ je *lineární zobrazení* z $\mathbb{R}^2$ do $\mathbb{R}^2$, a píšeme $F : \mathbb{R}^2 \to \mathbb{R}^2$. Slovy lze podmínku také vyjádřit tak, že lineární kombinace vektorů se zobrazuje na tutéž lineární kombinaci jejich obrazů, tj. lineární zobrazení jsou ta zobrazení, která zachovávají lineární kombinace.

Se stejným chováním jsme se setkali i v rovnici (1.13) pro přímku, kde šlo o lineární zobrazení $F : \mathbb{R}^2 \to \mathbb{R}$ a jeho předepsanou hodnotu $c$. To je také důvodem, proč jsou hodnoty zobrazení $z = F(x, y)$ na obrázku vyobrazeny jako rovina v $\mathbb{R}^3$.

Stručně budeme zapisovat taková zobrazení pomocí tzv. *matic* a jejich násobení. Maticí rozumíme obdélníkové schéma skalárů, např.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{nebo} \quad v = \begin{pmatrix} x \\ y \end{pmatrix},$$

hovoříme o (čtvercové) matici $A$ a (sloupcovém) vektoru $v$. Jejich násobení definujeme takto:

$$A \cdot v = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Podobně, můžeme místo vektoru $v$ zprava násobit jinou maticí $B$ stejného rozměru jako je $A$. Prostě aplikujeme předchozí formule po jednotlivých sloupcích matice $B$ a obdržíme jako výsledek opět čtvercovou matici.

Neumíme násobit vektor $v$ zprava maticí $A$ protože nám ne-



vychází počty skalárů na řádcích $v$ s počty skalárů ve sloupcích $A$. Umíme však napsat vektor $w$ do řádku skalárů (tzv. transponovaný vektor) $w^T = (a, b)$ a ten zprava našimi maticemi $A$ nebo vektory $v$ již násobit umíme.

zrcadlením (osovou symetrií) podle kolmého vektoru k přímce $p$.). Paprsek dopadne v bodě $[6, 2]$, odražený paprsek tedy bude mít rovnici

$$[6, 2] + t(1, -3),\ t \geq 0.$$

Průnik přímky dané odraženým paprskem s přímkou $q$ je bod $[4, 8]$, což je mimo polopřímku, která je daná odraženým paprskem ($t = -2$). Odražený paprsek tedy přímku $q$ neprotne. □

**Poznámka.** Odraz paprsku v třírozměrném prostoru je studován v příkladu ‖3.42‖.

**1.59.** Z bodu $[-2, 0]$ vyrazila v pravé poledne konstantní rychlostí 1 $\mathrm{ms}^{-1}$ ve směru $(3, 2)$ úsečka délky 1. Rovněž v poledne vyrazila z bodu $[5, -2]$ druhá úsečka délky 1 ve směru $(-1, 1)$, ovšem dvojnásobnou rychlostí. Srazí se?

**Řešení.** Přímky, po kterých se pohybují dané úsečky, můžeme popsat parametrickým vyjádřením:

$$p : [-2, 0] + r(3, 2),$$
$$q : [5, -2] + s(-1, 1).$$

Obecná rovnice přímky $p$ je

$$2x - 3y + 4 = 0.$$

Dosazením parametrického vyjádření přímky $q$ získáme průsečík $P = [1, 2]$.

Nyní se snažme zvolit jediný parametr $t$ pro obě úsečky tak, aby nám odpovídající bod na přímkách $p$, resp. $q$, popisoval polohu počátku první, resp. druhé, úsečky v čase $t$. V čase 0 je první úsečka v bodě $[-2, 0]$, druhá v bodě $[5, -2]$. Za čas $t$ sekund urazí první úsečka $t$ jednotek délky ve směru $(3, 2)$ druhá pak $2t$ jednotek délky ve směru $(-1, 1)$. Odpovídající parametrizace jsou tedy

$$p : [-2, 0] + \frac{t}{\sqrt{13}}(3, 2),$$
$$q : [5, -2] + t\sqrt{2}(-1, 1).$$

Počátek první úsečky dorazí do bodu $[1, 2]$ v čase $t_1 = \sqrt{13}$ s, počátek druhé úsečky v čase $t = 2\sqrt{2}$ s, tedy více než o půl vteřiny dříve. Tedy v době, kdy dorazí do průsečíku $P$ počátek první úsečky, bude již konec druhé úsečky pryč a úsečky se tak nesrazí. □

**1.60.** Rovinný fotbalista vystřelí míč z bodu $F = [1, 0]$ ve směru $(3, 4)$ na bránu (úsečku) ohraničenou body $A = [23, 36]$ a $B = [26, 30]$. Směřuje míč do brány?

**Řešení.** Vzhledem k tomu, že se situace odehrává v prvním kvadrantu, stačí uvažovat směrnice vektorů $\vec{FA}$, $(3, 4)$, $\vec{FB}$. Tvoří-li (v tomto pořadí) buď rostoucí nebo klesající posloupnost, míč směřuje na bránu.

Snadno ověříme tzv. asociativitu násobení (propočítejte pro obecné matice $A$, $B$ a vektor $v$ detailně):

$$(A \cdot B) \cdot v = A \cdot (B \cdot v).$$

Místo vektoru $v$ můžeme samozřejmě psát i libovolnou matici $C$ správného rozměru. Stejně snadno je vidět i distributivita

$$A \cdot (B + C) = A \cdot B + A \cdot C.$$

Neplatí však komutativita a existují „dělitelé nuly“. Např.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Zejména vidíme, že násobení vektorů pevnou maticí zadává lineární zobrazení, a naopak, pomocí hodnot lineárního zobrazení $F$ na dvou pevných vektorech báze už dostaneme celé příslušné zobrazení. Body v rovině jsou tedy obecně vzory hodnot lineárních zobrazení $F$ roviny do roviny, přímky jsou obecně vzory hodnot lineárních zobrazení z roviny do reálné přímky $\mathbb{R}$. S maticemi a vektory umíme rovnice pro přímky a body psát

$$w^T \cdot v = \begin{pmatrix} a & b \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = c,$$
$$A \cdot v = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r \\ s \end{pmatrix} = u.$$

Ve zvláštních situacích tomu tak být nemusí. Tak třeba průnikem dvou stejných přímek je opět sama přímka (a vzorem vhodné hodnoty pro takové lineární zobrazení bude celá přímka), nulové zobrazení má za vzor nuly celou rovinu. V prvém případě to poznáme tak, že jsou nalevo v rovnicích (1.15) stejné výrazy až na skalární násobek (nebo jinak řečeno, řádky matice $A$ jsou stejné až na skalární násobek). V takovém případě buď nebude v průniku příslušných přímek žádný bod (rovnoběžné různé přímky) nebo tam budou všechny body přímky (stejné přímky). Tuto podmínku může vyjádřit tak, že poměry $a/c$ a $b/d$ musí být stejné, neboli

$$ad - bc = 0. \tag{1.16}$$

Všimněme si, že toto vyjádření už zahrnuje i případy, kdy $c$ nebo $d$ je nulové.

**1.27. Determinant matice.** Výrazu nalevo v (1.16) říkáme *determinant* matice $A$ a píšeme pro něj

$$\det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Naši diskusi teď můžeme vyjádřit takto:

**Tvrzení.** *Determinant je skalární funkce* $\det A$ *definovaná na všech čtvercových maticích* $A$ *a rovnice* $A \cdot v = u$ *je jednoznačně řešitelná, právě když je* $\det A \neq 0$.



Zkuste promyslet, že pro tuto úvahu bylo podstatné, že pracujeme s polem skalárů. Například nad celými čísly obecně neplatí. Když prostě spočteme řešení rovnic s celočíselnými koeficienty (tj. matice $A$ má pouze celočíselné vstupy), tak toto řešení celočíselné být nemusí.

Tato posloupnost je 36/22, 4/3, 30/25, což je klesající posloupnost, míč tedy směřuje do brány. □

**1.61.** Upravte $(A-B)^T \cdot 2C \cdot u$, přičemž

$$A = \begin{pmatrix} 0 & 5 \\ -2 & 2 \end{pmatrix},\ B = \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix},$$

$$C = \begin{pmatrix} 2 & -2 \\ 4 & 5 \end{pmatrix},\ u = \begin{pmatrix} 3 \\ 2 \end{pmatrix}.$$

**Řešení.** Dosazením

$$A - B = \begin{pmatrix} -2 & 5 \\ -1 & 1 \end{pmatrix},\ (A-B)^T = \begin{pmatrix} -2 & -1 \\ 5 & 1 \end{pmatrix},$$

$$2C = \begin{pmatrix} 4 & -4 \\ 8 & 10 \end{pmatrix}$$

a násobením matic dostáváme

$$(A-B)^T \cdot 2C \cdot u = \begin{pmatrix} -2 & -1 \\ 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 & -4 \\ 8 & 10 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} -52 \\ 64 \end{pmatrix}.$$

□

**1.62.** Uveďte příklad matic $A$ a $B$, pro něž

(a) $(A+B)\cdot(A-B) \neq A\cdot A - B\cdot B$,

(b) $(A+B)\cdot(A+B) \neq A\cdot A + 2A\cdot B + B\cdot B$.

**Řešení.** Připomeňme, že uvažujeme dvojrozměrné (čtvercové) matice $A$ a $B$. Pro libovolné matice $A$ a $B$ ovšem platí

$$(A+B)\cdot(A-B) = A\cdot A - A\cdot B + B\cdot A - B\cdot B.$$

Identitu

$$(A+B)\cdot(A-B) = A\cdot A - B\cdot B$$

tak dostaneme, právě když je $-A\cdot B + B\cdot A$ nulovou maticí, tj. právě když matice $A$ a $B$ komutují. Příkladem hledaných matic jsou tedy právě ty dvojice matic, které nekomutují (matice součinu se při záměně pořadí násobených matic změní). Můžeme např. zvolit

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix},\ B = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix},$$

neboť při této volbě je

$$A\cdot B = \begin{pmatrix} 8 & 5 \\ 20 & 13 \end{pmatrix},\ B\cdot A = \begin{pmatrix} 13 & 20 \\ 5 & 8 \end{pmatrix}.$$

Analogicky pro každou dvojici matic $A$, $B$ platí

$$(A+B)\cdot(A+B) = A\cdot A + A\cdot B + B\cdot A + B\cdot B.$$

To znamená, že

$$(A+B)\cdot(A+B) = A\cdot A + A\cdot B + A\cdot B + B\cdot B$$

**1.28. Afinní zobrazení.** Podíváme se, jak maticová symbolika



umožňuje pracovat s jednoduchými zobrazeními v afinní rovině. Viděli jsme, že násobením maticí je dáno lineární zobrazení. Posunutí v afinní rovině $\mathbb{R}^2$ o pevný vektor $t = (r,s) \in \mathbb{R}^2$ umíme v maticové formě také snadno zapsat:

$$P = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto P + t = \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} x+r \\ y+s \end{pmatrix}.$$

Jestliže k výsledku lineárního zobrazení ještě dovolíme přičíst pevný vektor $t = (r,s)$, pak naše zobrazení bude mít tvar

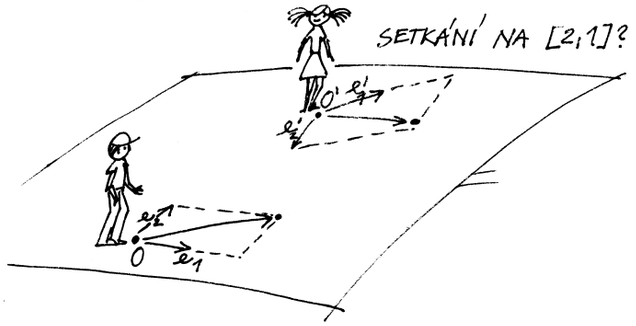
$$v = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A\cdot v + t = \begin{pmatrix} ax+by+r \\ cx+dy+s \end{pmatrix}.$$

Takto jsou popsána právě všechna tzv. *afinní zobrazení roviny* do sebe.

Taková zobrazení nám umožní přepočítávání souřadnic vznik-



lých různými volbami počátků a bází směrů pro posunutí. Co se stane, když náš pozorovatel z odstavce 1.23 bude tutéž rovinu shlížet z jiného bodu nebo si aspoň vybere jiné body $E_1$, $E_2$? Zkuste si promyslet, že na úrovni souřadnic to skutečně bude právě změna realizovaná pomocí afinního zobrazení. Časem budeme vidět obecné důvody, proč tomu tak je ve všech dimenzích.




**1.29. Euklidovská rovina.** Přidejme nyní schopnost našeho pozorovatele vidět vzdálenosti. Např. může věřit obvyklému vzorci pro velikost vektoru $v = (a,b)$

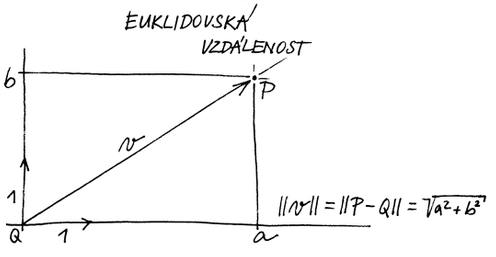
$$\|v\| = \sqrt{a^2+b^2}$$

v jím zvolených afinních souřadnicích. Okamžitě pak můžeme definovat pojmy jako jsou úhel a otočení v rovině.

Jednoduše si to můžeme představit takto: náš člověk se roz-



hodne o nějakých bodech $E_1$ a $E_2$, že jsou od něj ve vzdálenosti jedna, a zároveň si řekne, že jsou na sebe kolmé. Vzdálenosti ve směrech souřadných os pak jsou dány příslušným poměrem, obecně používá Euklidovu (nebo Pythagorovu) větu. Odtud vyjde právě výše uvedený vzorec.



je splněno tehdy a jenom tehdy, když $A \cdot B = B \cdot A$. Ve druhém případě jsou tak hledané dvojice matic $A$, $B$ zcela totožné s případem prvním. □

**1.63.** Rozhodněte, zda jsou zobrazení $F, G : \mathbb{R}^2 \to \mathbb{R}^2$ zadaná přiřazeními

$$F : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 7x - 3y \\ -2x + 5y \end{pmatrix}, \ x, y \in \mathbb{R},$$
$$G : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 2x + 2y - 4 \\ 4x - 9y + 3 \end{pmatrix}, \ x, y \in \mathbb{R}$$

lineární.

**Řešení.** Pro libovolný vektor $(x, y)^T \in \mathbb{R}^2$ můžeme vyjádřit

$$F\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 7 & -3 \\ -2 & 5 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix},$$
$$G\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 2 & 2 \\ 4 & -9 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} -4 \\ 3 \end{pmatrix}.$$

Odtud vyplývá, že obě zobrazení jsou afinní. Připomeňme, že afinní zobrazení je lineární, právě když se nulový vektor zobrazí sám na sebe. Víme, že platí

$$F\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \ G\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} -4 \\ 3 \end{pmatrix},$$

a proto je zobrazení $F$ je lineární, zobrazení $G$ nikoli. □

**1.64.** Spočtěte délky stran trojúhelníka s vrcholy

$$A = [2, 2] \ B = [3, 0] \ C = [4, 3].$$

**Řešení.** Užitím známého vzorce pro velikost vektoru

$$||u|| = \sqrt{u_1^2 + u_2^2}, \ u = (u_1, u_2) \in \mathbb{R}^2$$

obdržíme výsledky

$$|AB| = ||A - B|| = \sqrt{(2-3)^2 + (2-0)^2} = \sqrt{5},$$
$$|BC| = ||B - C|| = \sqrt{(3-4)^2 + (0-3)^2} = \sqrt{10},$$
$$|AC| = ||A - C|| = \sqrt{(2-4)^2 + (2-3)^2} = \sqrt{5}\,. \quad \square$$

**1.65. Rovnoběžníková rovnost.** Dokažme jako ilustraci našich nástrojů tzv. „rovnoběžníkovou rovnost“: Jsou-li $u, v \in \mathbb{R}^2$, pak:

$$2(\|u\|^2 + \|v\|^2) = \|u + v\|^2 + \|u - v\|^2.$$

Neboli součet druhých mocnin délek úhlopříček rovnoběžníka je roven dvojnásobku součtu druhých mocnin délek jeho stran.

Náš pozorovatel roviny může samozřejmě postupovat i jinak. Může použít nějaký standard pro skutečné měření vzdálenosti bodů $P$ a $Q$ v rovině a říci, že to je právě velikost vektoru $Q - P$, který potřebujeme na posunutí z $P$ do $Q$. Pak si vybere nějaký z vektorů, které skutečně mají velikost 1 a třeba pomocí trojúhelníku o stranách s velikostmi 3, 4 a 5 zkonstruuje kolmý vektor o velikosti jedna a dále pokračuje jako výše.

*Euklidovská rovina* je afinní rovina s výše zavedeným pojmem vzdálenosti.

**1.30. Úhel vektorů.** Jak jsme již používali při diskusi komplexních čísel coby bodů v rovině, tzv. goniometrická funkce $\cos\varphi$ je dána hodnotou reálné první souřadnice jednotkového vektoru, jehož úhel s vektorem $(1, 0)$ je $\varphi$.

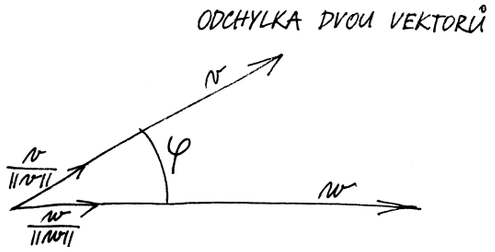


Zjevně je pak druhá souřadnice takového vektoru dána reálnou hodnotou $0 \leq \sin\varphi \leq 1$ splňující

$$(\cos\varphi)^2 + (\sin\varphi)^2 = 1.$$

Obecně pak pro dva vektory $v$ a $w$ můžeme jejich úhel popsat pomocí souřadnic $v = (v_x, v_y)$, $w = (w_x, w_y)$ takto:

$$\cos\varphi = \frac{v_x w_x + v_y w_y}{\|v\| \cdot \|w\|}.$$




Tento vztah si snadno ověříme, pokud věříme, že otočení roviny kolem počátku nemění úhly. Pak totiž můžeme napřed libovolně zvolené vektory vynásobit vhodnými skaláry tak, abychom dostali vektory velikosti jedna (náš vzorec totiž po násobení vektorů libovolnými skaláry dává pochopitelně neměnné výsledky). Poté můžeme vhodným otočením naší roviny dosáhnout toho, že první z vektorů bude právě prvním bázovým vektorem $(1, 0)$. Potom dává náš vzorec



$$\cos\varphi = \frac{w_x}{\|w\|},$$

což je pouze opakováním definice funkce $\cos\varphi$.

**1.31. Rotace kolem bodu v rovině.** Matici libovolného známého zobrazení $F : \mathbb{R}^2 \to \mathbb{R}^2$ lze vcelku snadno uhádnout: Je-li totiž výsledkem matice se sloupci $(a, c)$ a $(b, d)$, pak první sloupec dostaneme násobením této matice s prvním vektorem báze $(1, 0)$ a druhý je vyčíslením na druhém vektoru báze $(0, 1)$.

**Řešení.** Rozepsáním obou stran rovnice do souřadnic $u = (u_1, u_2)$, $v = (v_1, v_2)$ obdržíme:

$$\begin{aligned} 2(\|u\|^2 + \|v\|^2) &= 2(u_1^2 + u_2^2 + v_1^2 + v_2^2) = \\ &= u_1^2 + 2u_1v_1 + v_1^2 + u_2^2 + 2u_2v_2 + v_2^2 + \\ &\quad + u_1^2 - 2u_1v_1 + v_1^2 + u_2^2 - 2u_2v_2 + v_2^2 = \\ &= (u_1 + v_1)^2 + (u_2 + v_2)^2 + \\ &\quad + (u_1 - v_1)^2 + (u_2 - v_2)^2 = \\ &= \|u + v\|^2 + \|u - v\|^2. \end{aligned}$$

□

**1.66.** Určete úhel, který svírají vektory

(a) $u = (-3, -2)$, $v = (-2, 3)$;

(b) $u = (2, 6)$, $v = (-3, -9)$.

**Řešení.** Hledaný úhel $\varphi$ vypočítáme ze vzorce (1.36). Všimněme si, že vektor $(-3, -2)$ můžeme získat tak, že zaměníme pořadí souřadnic ve vektoru $(-2, 3)$ a jednu z nich vynásobíme číslem $-1$. To je ovšem úprava, která se provádí, když chceme ze směrového vektoru přímky získat normálový (nebo naopak). Vektory ve variantě (a) jsou tedy kolmé, tj. $\varphi = \pi/2$. Neboť $-3 \cdot (2, 6) = 2 \cdot (-3, -9)$, je ve variantě (b) vektor $u$ násobkem vektoru $v$. Pokud jeden vektor přejde na druhý tak, že ho vynásobíme kladným číslem, svírají tyto vektory evidentně nulový úhel. V našem příkladu je třeba násobit záporným číslem, což bezprostředně dává $\varphi = \pi$. □

**1.67.** Určete úhel (odchylku) $\varphi$, který svírají úhlopříčky $A_3A_7$ a $A_5A_{10}$ pravidelného dvanáctiúhelníku $A_0A_1A_2 \ldots A_{11}$.

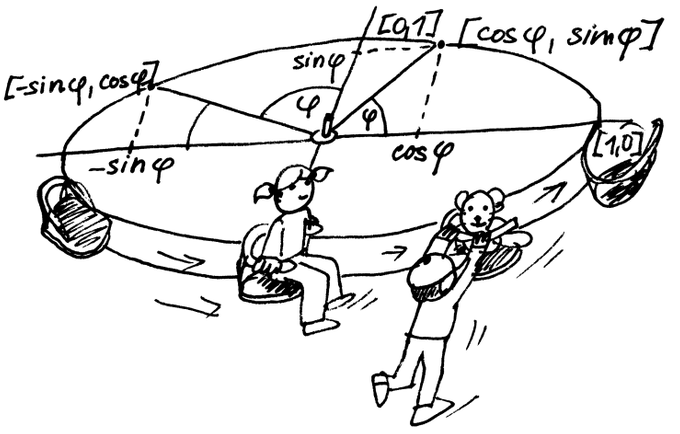
**Řešení.** Odchylka nezávisí na velikosti daného dvanáctiúhelníku. Volme dvanáctiúhelník vepsaný do kružnice o poloměru 1. Jako v předchozím příkladě určíme souřadnice jeho vrcholů a podle vzorce snadno dopočítáme, že $\cos\varphi = \frac{1}{2\sqrt{2+\sqrt{3}}}$, tedy $\varphi = 75°$.

**Jiné řešení.** Úlohu lze řešit čistě metodami syntetické geometrie: označíme $S$ střed dvanáctiúhelníku a $T$ průsečík úhlopříček $A_3A_7$ a $A_5A_{10}$. Nyní $|\angle A_7A_5A_{10}| = 45°$ (obvodový úhel příslušný středovému úhlu $A_7SA_{10}$, který je pravý), dále $|\angle A_5A_7A_3| = 30°$ (obvodový úhel příslušný středovému úhlu $A_5SA_3$, jehož velikost je 60°). Velikost úhlu $A_5TA_7$ je pak doplňkem výše zmíněných úhlů do 180°, tedy je rovna 105°. Hledaná odchylka je pak $180° - 105° = 75°$. □

**1.68.** Zjistěte, jaká lineární zobrazení $\mathbb{R}^2$ do $\mathbb{R}^2$ jsou zadána maticemi (tj. popište jejich geometrický význam)

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix}.$$

ROTACE KOLEM BODU V ROVINĚ




Z obrázku je proto vidět, že pro rotaci o úhel $\psi$ proti směru hodinových ručeček jsou v matici sloupce

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\psi \\ \sin\psi \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\psi \\ \cos\psi \end{pmatrix}$$

Směr proti směru hodinových ručeček označujeme jako *kladný směr rotace*, opačný je pak záporný. Proto dostáváme tvrzení:

MATICE ROTACE

Rotace o předem daný úhel $\psi$ v kladném směru kolem počátku souřadnic je dána maticí $R_\psi$:

$$v = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto R_\psi \cdot v = \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$



Nyní, když už víme, jak vypadá matice otočení v rovině, můžeme ověřit, že otočení zachovává vzdálenosti a úhly (definované předešlým vzorcem). Označíme-li obraz vektoru $v$ jako

$$v' = \begin{pmatrix} v'_x \\ v'_y \end{pmatrix} = R_\psi \cdot v = \begin{pmatrix} v_x\cos\psi - v_y\sin\psi \\ v_x\sin\psi + v_y\cos\psi \end{pmatrix}$$

a podobně $w' = R_\psi \cdot w$, pak lze snadno přepočítat, že opravdu platí

$$\|v'\| = \|v\|,$$
$$v'_xw'_x + v'_yw'_y = v_xw_x + v_yw_y.$$

Předchozí výraz lze pomocí vektorů a matic napsat následovně

$$(R_\psi \cdot w)^T(R_\psi \cdot v) = w^Tv.$$

Transponovaný vektor $(R_\psi \cdot w)^T$ je roven $w^T \cdot R_\psi^T$, kde $R_\psi^T$ je tzv. transponovaná matice k matici $R_\psi$. To je matice, jejíž řádky tvoří sloupce původní matice a sloupce naopak tvoří řádky původní matice. Vidíme tedy, že matice otočení splňují vztah $R_\psi^T \cdot R_\psi = I$, matice $I$ (někdy píšeme prostě 1 a máme tím na mysli jednotku v okruhu matic) je tzv. *jednotková matice*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

**Řešení.** Nechť $(x, y)^T$ je nadále libovolný reálný vektor. Pro matici $A_1$ dostáváme

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix},$$

což znamená, že lineární zobrazení, které tato matice zadává, je (kolmá) projekce na osu $x$. Podobně vidíme, že matice $A_2$ určuje zrcadlení vzhledem k ose $y$, protože

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ y \end{pmatrix}.$$

Matici $A_3$ lze vyjádřit ve tvaru

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

pro $\varphi = \pi/4$, a tudíž zadává otočení roviny kolem počátku o úhel $\pi/4$ (v kladném smyslu, tj. proti pohybu hodinových ručiček). □

**1.69.** Buď dán pravidelný šestiúhelník $ABCDEF$ (vrcholy jsou označeny po řadě v kladném smyslu) se středem v bodě $S = [1, 0]$ a vrcholem $A = [0, 2]$. Určete souřadnice vrcholu $C$.

**Řešení.** Souřadnice vrcholu $C$ získáme otočením bodu $A$ okolo středu $S$ šestiúhelníka o 120° v kladném smyslu:

$$\begin{aligned} C &= \begin{pmatrix} \cos 120° & -\sin 120° \\ \sin 120° & \cos 120° \end{pmatrix} (A - S) + S = \\ &= \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix} + [1, 0] = \\ &= \left[\tfrac{3}{2} - \sqrt{3}, -1 - \tfrac{\sqrt{3}}{2}\right]. \end{aligned}$$

□

**1.70.** Buď dán rovnostranný trojúhelník s vrcholy $[1, 0]$ a $[0, 1]$ ležící celý v prvním kvadrantu. Určete souřadnice jeho třetího vrcholu.

**Řešení.** Třetí souřadnice je $\left[\frac{1}{2} + \frac{\sqrt{3}}{2}, \frac{1}{2} + \frac{\sqrt{3}}{2}\right]$ (otáčíme bod $[1, 0]$ o 60° kolem bodu $[0, 1]$ v kladném smyslu). □

**1.71.** Jsou dány body $A = [1, 1]$, $B = [2, 3]$ a $S = [0, 0]$. Určete souřadnice vrcholů trojúhelníka, který vznikne otočením rovnostranného trojúhelníka $ABC$ o 60° v kladném smyslu kolem bodu $S$ (bod $C$ leží v polorovině dané přímkou $AB$ a bodem $S$).

**Řešení.** Třetí vrchol trojúhelníka dostaneme např. otočením o 60° jednoho z vrcholů kolem druhého (ve správném smyslu). Hledané body mají pak souřadnice $\left[-\frac{3}{2}\sqrt{3}, \sqrt{3} - \frac{1}{2}\right]$, $\left[\frac{1}{2} - \frac{1}{2}\sqrt{3}, \frac{1}{2}\sqrt{3} + \frac{1}{2}\right]$, $\left[1 - \frac{3}{2}\sqrt{3}, \sqrt{3} + \frac{3}{2}\right]$. □

**1.72.** Najděte matice $A$ takové, že

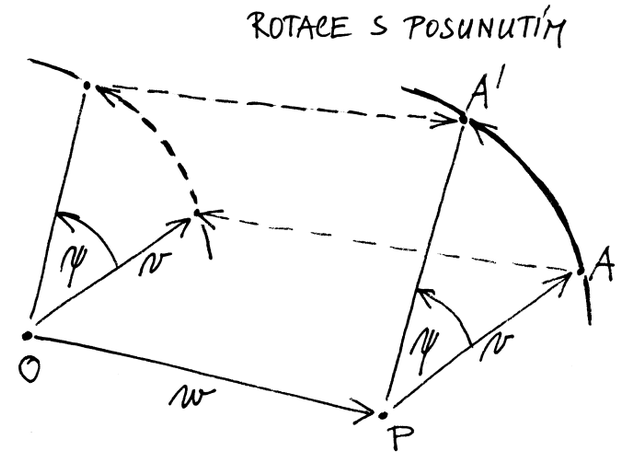
$$A^2 = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}.$$

Nápověda: jaké geometrické zobrazení v rovině zadává matice $A^2$?

Tím jsme odvodili pozoruhodné tvrzení — matice $F$ s vlastností, že $F \cdot R_\psi = I$ (budeme takové říkat inverzní matice k matici rotace $R_\psi$) je maticí transponovanou k původní. To je logické, neboť inverzní zobrazení k rotaci o úhel $\psi$ je opět rotace, ale o úhel $-\psi$, tj. inverzní matice $R_\psi^T$ je rovna matici

$$R_{-\psi} = \begin{pmatrix} \cos(-\psi) & -\sin(-\psi) \\ \sin(-\psi) & \cos(-\psi) \end{pmatrix} = \begin{pmatrix} \cos\psi & \sin\psi \\ -\sin\psi & \cos\psi \end{pmatrix}.$$

Pokud bychom chtěli zapsat rotaci kolem jiného bodu $P = O + w$, $P = [w_x, w_y]$ opět pomocí matice, snadno napíšeme potřebný vzorec pomocí posunutí:




Stačí si k tomu uvědomit, že můžeme místo rotace kolem daného bodu $P$ napřed posunout $P$ do našeho počátku, pak provést rotaci a pak udělat opačné posunutí, kterým celou rovinu vrátíme tam, kde měla celou dobu být, viz obrázek. Počítejme tedy

$$\begin{aligned} v = \begin{pmatrix} x \\ y \end{pmatrix} &\mapsto v - w \mapsto R_\psi \cdot (v - w) \\ &\mapsto R_\psi \cdot (v - w) + w = \\ &= \begin{pmatrix} \cos\psi(x - w_x) - \sin\psi(y - w_y) + w_x \\ \sin\psi(x - w_x) + \cos\psi(y - w_y)) + w_y \end{pmatrix}. \end{aligned}$$

**1.32. Zrcadlení.** Dalším dobře známým příkladem zobrazení, která zachovávají velikosti, je tzv. *zrcadlení vzhledem k přímce*. Opět nám bude stačit popsat zrcadlení vzhledem k přímkám procházejícím počátkem $O$ a ostatní se z nich odvodí pomocí posunutí, resp. rotací.



Hledejme tedy matici $Z_\psi$ zrcadlení vzhledem k přímce s jednotkovým směrovým vektorem $v$ svírajícím úhel $\psi$ s vektorem $(1, 0)$. Nejprve si uvědomme, že

$$Z_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

**Řešení.** $A^2$ je matice rotace o 60° v kladném smyslu, takže hledané matice jsou

$$A = \pm \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix},$$

tj. jsou to matice rotace o 30°, resp. o 210°. □

**1.73.** Stanovte $A \cdot A$ pro

$$A = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \text{ kde } \varphi \in \mathbb{R}.$$

**Řešení.** Víme, že zobrazení

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}, \ x, y \in \mathbb{R}$$

je rotací roviny $\mathbb{R}^2$ kolem počátku soustavy souřadnic o úhel $\varphi$ v kladném smyslu. Vzhledem k asociativitě násobení matic dostáváme, že zobrazení

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix},$$

$x, y \in \mathbb{R}$, je rotací o úhel $2\varphi$. To znamená, že platí

$$A \cdot A = \begin{pmatrix} \cos 2\varphi & -\sin 2\varphi \\ \sin 2\varphi & \cos 2\varphi \end{pmatrix}.$$

Poznamenejme, že jsme samozřejmě mohli přímo vynásobit $A \cdot A$ (a aplikovat vzorce pro sinus a kosinus dvojnásobného úhlu). Opakováním výše uvedeného (příp. použitím matematické indukce) lze ovšem snadněji obdržet

$$A^n = \begin{pmatrix} \cos n\varphi & -\sin n\varphi \\ \sin n\varphi & \cos n\varphi \end{pmatrix}, \ n = 2, 3, \ldots,$$

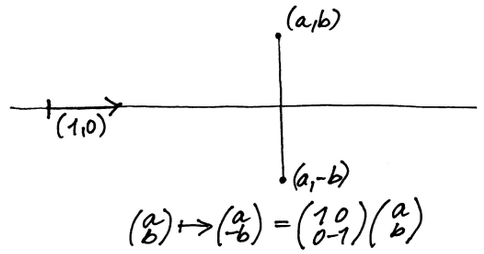
jestliže klademe $A^2 = A \cdot A$, $A^3 = A \cdot A \cdot A$ atd. □

**1.74. Osová symetrie.** Najděte matici osové symetrie (též zrcadlení) podle přímky $y = x$.

**Řešení.** V této symetrii přechází osa $x$ na osu $y$ a naopak. V působení uvažované osové symetrie na obecný bod to znamená, že se pouze vymění $x$-ová a $y$-ová souřadnice zobrazovaného bodu. Tato výměna je výsledkem násobení maticí $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, což je tedy matice dané symetrie. □

**1.75.** Ukažte, že složením lichého počtu středových souměrností v rovině dostaneme opět středovou symetrii.

**Řešení.** Středovou souměrnost v rovině se středem $S$ reprezentujme předpisem $X \mapsto S - (X - S)$, neboli $X \mapsto 2S - X$. (Obraz bodu $X$ ve středové symetrii podle středu $S$ dostaneme tak, že k souřadnicím bodu $S$ přičteme souřadnice vektoru opačného k vektoru $X - S$.) Postupnou aplikací tří středových souměrností se středy $S$, $T$ a $U$ tak dostáváme $X \mapsto 2S - X \mapsto 2T - (2S - X) \mapsto 2U - (2T - (2S - X)) =$




Obecně můžeme každou přímku otočit do směru vektoru $(1, 0)$ a tedy zapsat obecnou matici zrcadlení jako

$$Z_\psi = R_\psi \cdot Z_0 \cdot R_{-\psi},$$

kdy nejprve otočíme maticí $R_{-\psi}$ přímku do „nulové“ polohy, odzrcadlíme maticí $Z_0$ a vrátíme zpět otočením $R_\psi$.

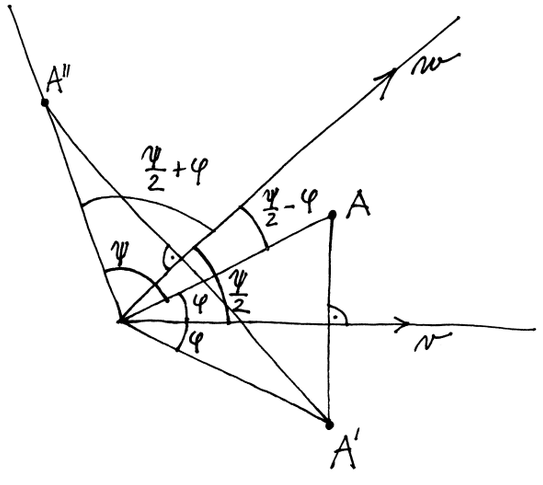
Můžeme proto (díky asociativitě násobení matic) spočíst:

$$\begin{aligned} Z_\psi &= \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos\psi & \sin\psi \\ -\sin\psi & \cos\psi \end{pmatrix} = \\ &= \begin{pmatrix} \cos\psi & \sin\psi \\ \sin\psi & -\cos\psi \end{pmatrix} \cdot \begin{pmatrix} \cos\psi & \sin\psi \\ -\sin\psi & \cos\psi \end{pmatrix} = \\ &= \begin{pmatrix} \cos^2\psi - \sin^2\psi & 2\sin\psi\cos\psi \\ 2\sin\psi\cos\psi & -(\cos^2\psi - \sin^2\psi) \end{pmatrix} = \\ &= \begin{pmatrix} \cos 2\psi & \sin 2\psi \\ \sin 2\psi & -\cos 2\psi \end{pmatrix}. \end{aligned}$$

Použili jsme přitom obvyklé součtové vzorce pro goniometrické funkce. Povšimněme si také, že $Z_\psi \cdot Z_0$ je dáno:

$$\begin{pmatrix} \cos 2\psi & \sin 2\psi \\ \sin 2\psi & -\cos 2\psi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos 2\psi & -\sin 2\psi \\ \sin 2\psi & \cos 2\psi \end{pmatrix}.$$

Toto pozorování lze zakreslit a zformulovat následovně.




**Tvrzení.** *Otočení o úhel $\psi$ obdržíme následným provedením dvou zrcadlení vzhledem ke směrům, které spolu svírají úhel $\frac{1}{2}\psi$.*



Pokud umíme odůvodnit předchozí tvrzení ryze geometrickou úvahou (zkuste si zahrát na „syntetického geometra“), dokázali jsme právě standardní vzorce pro goniometrické funkce dvojnásobného úhlu.

$= 2(U - T + S) - X$, celkem $X \mapsto 2(U - T + S) - X$, což je středová souměrnost se středem $S-T+U$. Složení libovolného lichého počtu středových souměrností tak postupně redukujeme až na složení tří středových souměrností, jde tedy o středovou symetrii (v principu se jedná o důkaz matematickou indukcí, zkuste si jej sami zformulovat). □

**1.76.** Sestrojte $(2n + 1)$-úhelník, jsou-li dány všechny středy jeho stran.

**Řešení.** K řešení využijeme toho, že složením lichého počtu středových souměrností je opět středová souměrnost (viz příklad ‖1.75‖). Označme vrcholy hledaného $(2n + 1)$-úhelníku po řadě $A_1$, $A_2, \ldots, A_{2n+1}$ a středy stran (počínaje středem strany $A_1A_2$) postupně $S_1, S_2, \ldots, S_{2n+1}$. Provedeme-li středové souměrnosti po řadě podle těchto středů, tak bod $A_1$ je zjevně pevným bodem výsledné středové souměrnosti, tedy jejím středem. K jeho nalezení tedy stačí provést uvedenou středovou souměrnost s libovolným bodem $X$ roviny. Bod $A_1$ leží pak ve středu úsečky $XX'$, kde $X'$ je obrazem bodu $X$ ve zmíněné středové symetrii. Další vrcholy $A_2, \ldots, A_{2n+1}$ získáme zobrazováním bodu $A_1$ ve středových souměrnostech podle $S_1, \ldots, S_{2n+1}$. □

**1.77.** Určete obsah trojúhelníka $ABC$, je-li

$$A = [-8, 1],\ B = [-2, 0],\ C = [5, 9].$$

**Řešení.** Víme, že obsah je roven polovině determinantu matice, jejíž první sloupec je dán vektorem $B-A$ a druhý sloupec vektorem $C-A$, tj. determinantu matice

$$\begin{pmatrix} -2-(-8) & 5-(-8) \\ 0-1 & 9-1 \end{pmatrix}.$$

Jednoduchý výpočet tak dává výsledek

$$\frac{1}{2}\left((-2-(-8))\cdot(9-1) - (5-(-8))\cdot(0-1)\right) = \frac{61}{2}.$$

Dodejme, že při záměně pořadí vektorů by hodnota determinantu měla opačné znaménko (její absolutní hodnota by tedy zůstala stejná) a že by se vůbec nezměnila, kdybychom vektory (při zachování pořadí) napsali do řádků. □

**1.78.** Spočtěte obsah $S$ čtyřúhelníka vymezeného jeho vrcholy [1, 1], [6, 1], [11, 4], [2, 4].

**Řešení.** Nejprve si označme vrcholy (proti směru pohybu hodinových ručiček)

$$A = [1, 1],\ B = [6, 1],\ C = [11, 4],\ D = [2, 4].$$

Hlubší je následující rekapitulace předchozích úvah (skoro si můžeme říci, že už umíme dokázat skutečně zajímavý matematický výsledek):

ZOBRAZENÍ ZACHOVÁVAJÍCÍ VELIKOSTI

**1.33. Věta.** *Lineární zobrazení euklidovské roviny je složeno z jednoho nebo více zrcadlení, právě když je dáno maticí $R$ splňující*

$$R = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad ab + cd = 0, \quad a^2 + c^2 = b^2 + d^2 = 1.$$

*To nastane, právě když toto zobrazení zachovává velikosti.*

*Otočením je takové zobrazení přitom právě tehdy, když je determinant matice $R$ roven jedné, což odpovídá sudému počtu zrcadlení. Při lichém počtu zrcadlení je determinant roven $-1$.*

DŮKAZ. Zkusme napřed spočíst, jak může vypadat obecně matice $A$, když příslušné zobrazení zachovává velikosti. Tj. máme zobrazení



$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Zachování velikosti tedy znamená, že pro všechna $x$ a $y$ je

$$\begin{aligned} x^2 + y^2 &= (ax + by)^2 + (cx + dy)^2 = \\ &= (a^2 + c^2)x^2 + (b^2 + d^2)y^2 + 2(ab + cd)xy. \end{aligned}$$

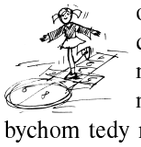
Protože má tato rovnost platit pro všechna $x$ a $y$, musí si být rovny koeficienty u jednotlivých mocnin $x^2$, $y^2$ a $xy$ na pravé i levé straně. Tím jsme spočetli, že rovnosti kladené na matici $R$ v prvním tvrzení dokazované věty jsou ekvivalentní vlastnosti, že příslušné zobrazení zachovává velikosti.

Díky vztahu $a^2+c^2 = 1$ můžeme předpokládat, že $a = \cos\varphi$ a $c = \sin\varphi$ pro vhodný úhel $\varphi$. Jakmile takto zvolíme první sloupec matice $R$, až na násobek nám vztah $ab+cd = 0$ určuje i druhý sloupec. Zároveň ale víme, že i velikost vektoru ve druhém sloupci je jedna a dostáváme tedy právě dvě možnosti pro matici $R$:

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \qquad \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}.$$

V prvém případě jde o rotaci o úhel $\varphi$, ve druhém pak o rotaci složenou se zrcadlením podle první souřadné osy. Jak jsme viděli v předchozím tvrzení 1.31, každá rotace odpovídá dvěma zrcadlením a determinant matice $R$ je v těchto dvou případech skutečně jedna nebo mínus jedna a rozlišuje je. □

**1.34. Obsah trojúhelníka.** Závěrem našeho malého výletu do geometrie se zaměřme na *obsah* rovinných objektů. Budou nám stačit trojúhelníky. Každý trojúhelník je vymezen dvojicí vektorů $v$ a $w$, které, přiloženy do jednoho z vrcholů $P$, zadají zbylé dva vrcholy. Chtěli bychom tedy najít vzorec (skalární funkci vol), která dvěma vektorům přiřadí číslo rovné obsahu vol $\Delta(v, w)$ takto definovaného trojúhelníka $\Delta(v, w)$, kde si pro určitost za $P$ volíme počátek a posunutím se obsah stejně nemění.



Ze zadání je vidět, že hledaná hodnota je polovinou plochy rovnoběžníku nataženého na vektory $v$ a $w$ a snadno se spočte (pomocí

Pokud rozdělíme čtyřúhelník $ABCD$ na trojúhelníky $ABC$ a $ACD$, můžeme získat jeho obsah jako součet obsahů těchto trojúhelníků, a to vyčíslením determinantů

$$d_1 = \begin{vmatrix} 6-1 & 11-1 \\ 1-1 & 4-1 \end{vmatrix} = \begin{vmatrix} 5 & 10 \\ 0 & 3 \end{vmatrix},$$
$$d_2 = \begin{vmatrix} 11-1 & 2-1 \\ 4-1 & 4-1 \end{vmatrix} = \begin{vmatrix} 10 & 1 \\ 3 & 3 \end{vmatrix},$$

kde ve sloupcích jsou postupně vektory $B-A$, $C-A$ (pro $d_1$) a $C-A$, $D-A$ (pro $d_2$). Potom

$$S = \frac{d_1}{2} + \frac{d_2}{2} = \frac{5\cdot 3 - 10\cdot 0}{2} + \frac{10\cdot 3 - 1\cdot 3}{2} = \\ = \frac{15+27}{2} = 21.$$

(díky uspořádání vrcholů v kladném smyslu vyšly všechny determinanty kladné). Správnost výsledku můžeme snadno potvrdit, neboť čtyřúhelník $ABCD$ je lichoběžníkem se základnami délek 5, 9 a jejich vzdáleností $v = 3$. □

**1.79.** Které strany čtyřúhelníka zadaného vrcholy $[-2,-2]$, $[1,4]$, $[3,3]$ a $[2,1]$ jsou viditelné z pozice bodu $[3,\pi-2]$?

**Řešení.** Jedná se o modelovou úlohu na viditelnost stran konvexního mnohoúhelníka v rovině. V prvním kroku uspořádáme vrcholy tak, aby jejich pořadí odpovídalo směru proti pohybu hodinových ručiček. Když jako první vrchol zvolíme např. $A = [-2,-2]$, je další pořadí $B = [2,1]$, $C = [3,3]$, $D = [1,4]$.

Uvažujme nejprve stranu $AB$. Ta společně s bodem $X = [3, \pi - 2]$ zadává matici

$$\begin{pmatrix} -2-3 & 2-3 \\ -2-(\pi-2) & 1-(\pi-2) \end{pmatrix}$$

tak, že její první sloupec je rozdílem $A - X$ a druhý sloupec je $B - X$. To, zda je vidět z bodu $[3,\pi-2]$, pak určuje znaménko determinantu

$$\begin{vmatrix} -2-3 & 2-3 \\ -2-(\pi-2) & 1-(\pi-2) \end{vmatrix} = \begin{vmatrix} -5 & -1 \\ -\pi & 3-\pi \end{vmatrix} = \\ = -5\cdot(3-\pi) - (-1)(-\pi) < 0.$$

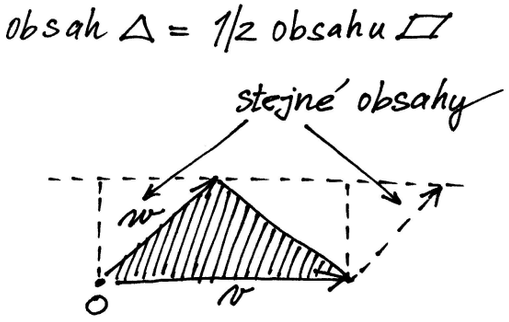
Záporná hodnota znamená, že strana je vidět. Doplňme, že nezáleží na tom, zda uvažujeme rozdíly $A - X$ a $B - X$, nebo $X - A$ a $X - B$. Kdybychom však zaměnili pořadí sloupců, příslušná strana by byla vidět právě tehdy, když by byl determinant kladný.

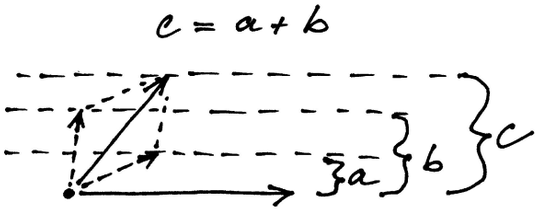
Pro stranu $BC$ analogicky obdržíme

$$\begin{vmatrix} 2-3 & 3-3 \\ 1-(\pi-2) & 3-(\pi-2) \end{vmatrix} = \begin{vmatrix} -1 & 0 \\ 3-\pi & 5-\pi \end{vmatrix} = \\ = -1\cdot(5-\pi) - 0 < 0.$$

známého vzorečku: základna krát příslušná výška) nebo prostě vidíme z obrázku, že nutně platí

$$\operatorname{vol}\Delta(v+v', w) = \operatorname{vol}\Delta(v,w) + \operatorname{vol}\Delta(v',w),$$
$$\operatorname{vol}\Delta(av, w) = a\operatorname{vol}\Delta(v,w).$$




Nakonec ještě přidáme k našemu zadání požadavek

$$\operatorname{vol}\Delta(v,w) = -\operatorname{vol}\Delta(w,v),$$

který odpovídá představě, že opatříme plochu znaménkem podle toho, v jakém pořadí bereme vektory (tj. jestli se na ni díváme shora nebo zespodu).

Pokud vektory $v$ a $w$ napíšeme do sloupců matice $A$, pak

$$A = (v,w) \mapsto \det A$$

splňuje všechny tři naše požadavky. Kolik takových zobrazení ale může být? Každý vektor umíme vyjádřit pomocí dvou bázových vektorů $e_1 = (1,0)$ a $e_2 = (0,1)$ a díky linearitě je tedy každá možnost pro $\operatorname{vol}\Delta$ jednoznačně určena už vyčíslením na těchto vektorech. Protože ale pro obsah, stejně jako pro determinant, je zjevně $\operatorname{vol}\Delta(e_1,e_1) = \operatorname{vol}\Delta(e_2,e_2) = 0$ (kvůli požadované antisymetrii), je nutně každá taková skalární funkce jednoznačně zadána hodnotou na jediné dvojici argumentů $(e_1,e_2)$. Jsou si tedy všechny možnosti rovny až na skalární násobek. Ten umíme určit požadavkem

$$\operatorname{vol}\Delta(e_1,e_2) = \frac{1}{2},$$

tj. volíme *orientaci* a *měřítko* pomocí volby bázových vektorů, a chceme, aby jednotkový čtverec měl plochu jedna.

Vidíme tedy, že determinant zadává plochu rovnoběžníku určeného sloupci matice $A$ a plocha trojúhelníku je tedy poloviční.

Tato strana je tudíž vidět. Zbývají strany $CD$ a $DA$. Pro ně dostáváme po řadě

$$\begin{vmatrix} 3-3 & 1-3 \\ 3-(\pi-2) & 4-(\pi-2) \end{vmatrix} = \begin{vmatrix} 0 & -2 \\ 5-\pi & 6-\pi \end{vmatrix} =$$
$$= 0-(-2)\cdot(5-\pi) > 0,$$
$$\begin{vmatrix} 1-3 & -2-3 \\ 4-(\pi-2) & -2-(\pi-2) \end{vmatrix} = \begin{vmatrix} -2 & -5 \\ 6-\pi & -\pi \end{vmatrix} =$$
$$= -2\cdot(-\pi)-(-5)\cdot(6-\pi) > 0.$$

Z bodu $X$ jsou tedy vidět právě strany určené dvojicemi vrcholů $[-2,-2]$, $[2,1]$ a $[2,1]$, $[3,3]$. □

**1.80.** Uveďte strany pětiúhelníku s vrcholy v bodech $[-2,-2]$, $[-2,2]$, $[1,4]$, $[3,1]$ a $[2,-11/6]$, které je možné vidět z bodu $[300,1]$.

**Řešení.** Pro zjednodušení zápisů „tradičně“ položme

$$A=[-2,-2],\ B=[2,-11/6],\ C=[3,1],$$
$$D=[1,4],\ E=[-2,2].$$

Strany $BC$ a $CD$ jsou zjevně z pozice bodu $[300,1]$ viditelné; naopak strany $DE$ a $EA$ být vidět nemohou. Pro stranu $AB$ raději určeme

$$\begin{vmatrix} -2-300 & 2-300 \\ -2-1 & -\frac{11}{6}-1 \end{vmatrix} =$$
$$= -302\cdot\left(-\frac{17}{6}\right)-(-298)\cdot(-3) < 0.$$

Odsud plyne, že tato strana je z bodu $[300,1]$ vidět. □

### F. Zobrazení a relace

**1.81.** Rozhodněte, zda následující relace na množině $M$ jsou relace ekvivalence:

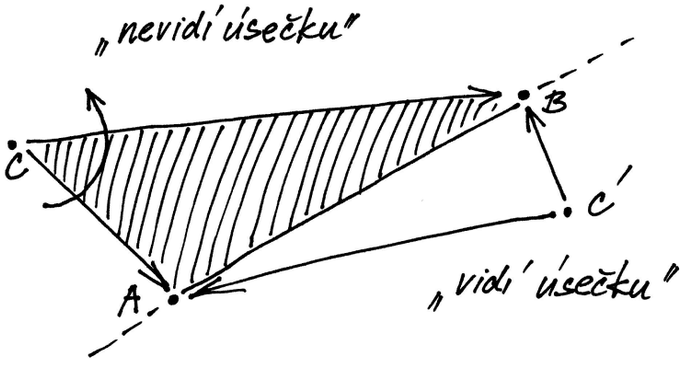
i) $M=\{f:\mathbb{R}\to\mathbb{R}\}$, kde $(f\sim g)$, pokud $f(0)=g(0)$.
ii) $M=\{f:\mathbb{R}\to\mathbb{R}\}$, kde $(f\sim g)$, pokud $f(0)=g(1)$.
iii) $M$ je množina přímek v rovině, přičemž dvě přímky jsou v relaci, jestliže se neprotínají.
iv) $M$ je množina přímek v rovině, přičemž dvě přímky jsou v relaci, jestliže jsou rovnoběžné.
v) $M=\mathbb{N}$, kde $(m\sim n)$, pokud $S(m)+S(n)=20$, přičemž $S(n)$ značí ciferný součet čísla $n$.
vi) $M=\mathbb{N}$, kde $(m\sim n)$, pokud $C(m)=C(n)$, kde $C(n)=S(n)$, pokud je ciferný součet $S(n)$ menší než 10, jinak definujeme $C(n)=C(S(n))$ (je tedy vždy $C(n)<10$).

**Řešení.**

i) Ano. Ověříme tři vlastnosti ekvivalence:

**1.35. Viditelnost v rovině.** Předchozí popis hodnot pro orientovaný obsah nám dává do rukou elegantní nástroj pro určování pozice bodu vůči orientovaným úsečkám. Orientovanou úsečkou rozumíme dva body v rovině $\mathbb{R}^2$ s určeným pořadím. Můžeme si ji představit jako šipku od prvého k druhému bodu. Taková orientovaná úsečka nám rozděluje rovinu na dvě poloroviny, říkejme jim „levou“ a „pravou“. Pro daný bod chceme poznat, jestli je v té levé nebo pravé.

Takové úlohy často potkáváme v počítačové grafice při řešení viditelnosti objektů. Pro zjednodušení si zde jen představme, že úsečku „je vidět“ z bodů napravo a není vidět z těch nalevo (což odpovídá představě, že objekt ohraničený orientovanými hranami proti směru hodinových ručiček má nalevo od nich svůj vnitřek, přes který tedy není hranu vidět).




Máme-li dán nějaký bod $C$, spočtěme orientovanou plochu příslušného trojúhelníku zadaného vektory $A-C$ a $B-C$. Pokud jsme s bodem $C$ nalevo od úsečky, pak při obvyklé kladné orientaci proti směru hodinových ruček bude vektor $A-C$ dříve než ten druhý a proto výsledná plocha (tj. hodnota determinantu matice jejímiž sloupci jsou tyto dva vektory) bude kladná. Naopak, při opačné poloze bude výsledkem záporná hodnota determinantu a podle záporné hodnoty determinantu zjistíme, že je náš bod od úsečky napravo.

Uvedený jednoduchý postup je skutečně často využíván pro testování polohy při standardních úlohách v 2D grafice.

### 6. Relace a zobrazení

V této závěrečné části úvodní motivační kapitoly se vrátíme k formálnímu popisu matematických struktur. Budeme se je ale průběžně snažit ilustrovat na již známých příkladech. Zároveň můžeme tuto část brát jako cvičení ve formálním přístupu k objektům a konceptům matematiky.

**1.36. Relace mezi množinami.** Nejprve potřebujeme definovat *kartézský součin* $A\times B$ dvou množin $A$ a $B$. Je to množina všech uspořádaných dvojic $(a,b)$ takových, že $a\in A$ a $b\in B$. *Binární relací* mezi množinami $A$ a $B$ pak rozumíme libovolnou podmnožinu $R$ kartézského součinu $A\times B$.

Často píšeme $a\simeq_R b$ pro vyjádření skutečnosti, že $(a,b)\in R$, tj. že body $a\in A$ a $b\in B$ jsou v relaci $R$. *Definičním oborem relace* je podmnožina

$$D\subseteq A,\quad D=\{a\in A;\exists b\in B,(a,b)\in R\}.$$

i) Reflexivita: pro libovolnou reálnou funkci $f$ je $f(0) = f(0)$.
ii) Symetrie: jestliže platí $f(0) = g(0)$, pak i $g(0) = f(0)$.
iii) Tranzitivita: jestliže platí $f(0) = g(0)$ a $g(0) = h(0)$, pak platí i $f(0) = h(0)$.

ii) Ne. Definovaná relace není reflexivní, např pro funkci sin máme $\sin 0 \neq \sin 1$ a není ani tranzitivní.
iii) Ne. Relace opět není reflexivní (každá přímka protíná sama sebe) ani tranzitivní.
iv) Ano. Třídy ekvivalence pak tvoří množinu neorientovaných směrů v rovině.
v) Ne. Relace není reflexivní. $S(1) + S(1) = 2$.
vi) Ano. □

*1.82.* Máme množinu $\{3, 4, 5, 6, 7\}$. Napište explicitně relaci

i) $a$ dělí $b$,
ii) $a$ dělí $b$ nebo $b$ dělí $a$,
iii) $a$ a $b$ jsou soudělná.

○

**1.83.** Nechť je na $\mathbb{R}^2$ definována relace $R$ tak, že $((a, b), (c, d)) \in R$ pro libovolná $a, b, c, d \in \mathbb{R}$, právě když $b = d$. Zjistěte, zda se jedná o relaci ekvivalence. Pokud jde o relaci ekvivalence, popište geometricky rozklad, který určuje.

**Řešení.** Z $((a, b), (a, b)) \in R$ pro všechna $a, b \in \mathbb{R}$ plyne, že relace je reflexivní. Stejně snadno vidíme, že relace je symetrická, neboť v rovnosti (druhých složek) můžeme zaměnit levou a pravou stranu. Je-li $((a, b), (c, d)) \in R$ a $((c, d), (e, f)) \in R$, tj. platí-li $b = d$ a $d = f$, lehce dostáváme splnění tranzitivní podmínky $((a, b), (e, f)) \in R$, tj. $b = f$. Relace $R$ je relací ekvivalence, kdy body roviny jsou spolu v relaci, právě když mají stejnou druhou souřadnici (přímka jimi zadaná je kolmá na osu $y$). Příslušný rozklad proto rozdělí rovinu na přímky rovnoběžné s osou $x$ . □

**1.84.** Určete, kolik různých binárních relací lze zavést mezi množinou $X$ a množinou všech jejích podmnožin, má-li množina $X$ právě 3 prvky.

**Řešení.** Nejprve si uvědomme, že množina všech podmnožin $X$ má $2^3 = 8$ prvků, a tudíž její kartézský součin s množinou $X$ má $8 \cdot 3 = 24$ prvků. Uvažovanými binárními relacemi jsou právě podmnožiny tohoto kartézského součinu, kterých je celkem $2^{24}$. □

Slovy vyjádřené, je to množina prvků $a$ z množiny $A$ takových, že existuje prvek $b$ z množiny $B$ tak, že $(a, b)$ patří do relace $R$. Stručněji, jsou to takové prvky z $A$, které mají alespoň jeden obraz v $B$. Podobně *oborem hodnot relace* je podmnožina

$$I \subseteq B, \quad I = \{b \in B; \exists a \in A, (a, b) \in R\},$$

to znamená takové prvky v $B$, které mají vzor v $A$.



Speciálním případem relace mezi množinami je *zobrazení z množiny $A$ do množiny $B$*. Je to případ, kdy pro každý prvek definičního oboru relace existuje právě jeden prvek z oboru hodnot, který je s ním v relaci. Nám známým případem zobrazení jsou všechny skalární funkce, kde oborem hodnot zobrazení je množina skalárů, třeba celých nebo reálných čísel. Pro zobrazení zpravidla používáme značení, které jsme také u skalárních funkcí zavedli. Píšeme

$$f : D \subseteq A \to I \subseteq B, f(a) = b$$

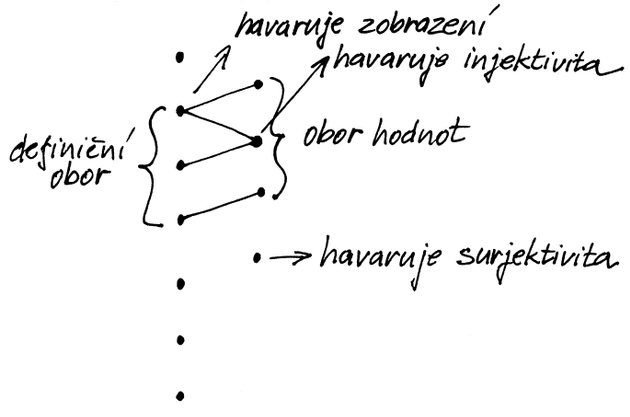
pro vyjádření skutečnosti, že $(a, b)$ patří do relace, a říkáme, že $b$ je hodnotou zobrazení $f$ v bodě $a$. Dále říkáme, že $f$ je

- zobrazení množiny $A$ *do* množiny $B$, jestliže je $D = A$,
- zobrazení množiny $A$ *na* množinu $B$, jestliže je $D = A$ a $I = B$, často také *surjektivní zobrazení*,
- prosté (často také *injektivní zobrazení*), jestliže je $D = A$ a pro každé $b \in I$ existuje právě jeden *vzor* $a \in A$ tak, že $f(a) = b$.

Vyjádření zobrazení $f : A \to B$ jakožto relace

$$f \subseteq A \times B, \quad f = \{(a, f(a)); a \in A\}$$

známe také pod názvem *graf zobrazení* $f$.




**1.37. Skládání relací a funkcí.** U zobrazení je jasná koncepce, jak se skládají. Máme-li dvě zobrazení $f : A \to B$ a $g : B \to C$, pak jejich *složení* $g \circ f : A \to C$ je definováno

$$(g \circ f)(a) = g(f(a)).$$

Ve značení používaném pro relace totéž můžeme zapsat jako

$$f \subseteq A \times B, \quad f = \{(a, f(a)); a \in A\},$$
$$g \subseteq B \times C, \quad g = \{(b, g(b)); b \in B\},$$
$$g \circ f \subseteq A \times C, \quad g \circ f = \{(a, g(f(a))); a \in A\}.$$



Zcela obdobně definujeme *skládání relací*, v předchozích vztazích jen doplníme existenční kvantifikátory, tj. musíme uvažovat všechny „vzory“ a všechny „obrazy“. Uvažme relace $R \subseteq A \times B$, $S \subseteq B \times C$. Potom $S \circ R \subseteq A \times C$,

$$S \circ R = \{(a, c); \exists b \in B, (a, b) \in R, (b, c) \in S\}.$$

**1.85.** Uveďte definiční obor $D$ a obor hodnot $I$ relace

$$R = \{(a, v), (b, x), (c, x), (c, u), (d, v), (f, y)\}$$

mezi množinami

$A = \{a, b, c, d, e, f\}$ a $B = \{x, y, u, v, w\}$.

Je relace $R$ zobrazení?

**Řešení.** Přímo z definice definičního oboru a oboru hodnot relace dostáváme

$$D = \{a, b, c, d, f\} \subseteq A, \quad I = \{x, y, u, v\} \subseteq B.$$

Nejedná se o zobrazení, protože $(c, x), (c, u) \in R$, tj. $c \in D$ má dva obrazy. □

**1.86.** O každé z následujících relací na množině $\{a, b, c, d\}$ rozhodněte, zda se jedná o relaci uspořádání (příp. zda se jedná o úplné uspořádání):

$$R_a = \{(a, a), (b, b), (c, c), (d, d), (b, a), (b, c), (b, d)\},$$
$$R_b = \{(a, a), (b, b), (c, c), (d, d), (d, a), (a, d)\},$$
$$R_c = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (b, d)\},$$
$$R_d = \{(a, a), (b, b), (c, c), (a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\},$$
$$R_e = \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}.$$

**Řešení.** $R_a$ je uspořádání, které není úplné (např. $(a, c) \notin R_a$ ani $(c, a) \notin R_a$). Relace $R_b$ není antisymetrická (je totiž $(a, d) \in R_b$ i $(d, a) \in R_b$), a tudíž se nejedná o uspořádání (jde o ekvivalenci). Relace $R_c$ a $R_d$ rovněž nejsou uspořádáními, protože $R_c$ není tranzitivní ($(a, b), (b, c) \in R_c, (a, c) \notin R_c$) a $R_d$ není reflexivní ($(d, d) \notin R_d$). Relace $R_e$ je úplné uspořádání (pokud budeme $(a, b) \in R$ interpretovat jako $a \leq b$, pak $a \leq b \leq c \leq d$). □

**1.87.** Rozhodněte, zda je zobrazení $f$ injektivní, resp. surjektivní, jestliže

(a) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad f((x, y)) = x + y - 10x^2$,

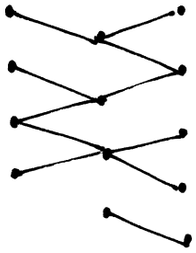
(b) $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}, \quad f(x) = \left(2x, x^2 + 10\right)$.

**Řešení.** Ve variantě (a) je uvedeno surjektivní zobrazení (postačuje položit $x = 0$), které není injektivní (stačí zvolit $(x, y) = (0, -9)$ a $(x, y) = (1, 0)$). Ve variantě (b) se naopak jedná o injektivní zobrazení (obě jeho složky, tj. funkce $y = 2x$ a $y = x^2 + 10$, jsou evidentně rostoucí na $\mathbb{N}$), které není surjektivní (např. dvojice $(1, 1)$ nemá vzor). □

Zvláštním případem relace je *identické zobrazení*

$$\mathrm{id}_A = \{(a, a) \in A \times A; a \in A\}$$

na množině $A$. Je neutrální vzhledem ke skládání s každou relací s definičním oborem nebo oborem hodnot $A$.



složení relací = v relaci jsou body, které lze spojit nějakou cestou zleva doprava

Pro každou relaci $R \subseteq A \times B$ definujeme *inverzní relaci*

$$R^{-1} = \{(b, a); (a, b) \in R\} \subset B \times A\,.$$

Pozor, u zobrazení je stejný pojem užíván ve specifičtější situaci. Samozřejmě že existuje pro každé zobrazení jeho inverzní relace, ta však nemusí být zobrazením. Zcela logicky proto hovoříme o existenci inverzního zobrazení, pokud každý prvek $b \in B$ je obrazem pro právě jeden vzor v $A$. V takovém případě je samozřejmě inverzní zobrazení právě inverzní relací.

Všimněme si, že složením zobrazení a jeho inverzního zobrazení (pokud obě existují) vždy vznikne identické zobrazení, u obecných relací tomu tak být nemusí.

**1.38. Relace na množině.** V případě $A = B$ hovoříme o relaci na množině $A$. Říkáme, že relace $R$ je:

- *reflexivní*, pokud $\mathrm{id}_A \subseteq R$, tj. $(a, a) \in R$ pro všechny $a \in A$,
- *symetrická*, pokud $R^{-1} = R$, tj. pokud $(a, b) \in R$, pak i $(b, a) \in R$,
- *antisymetrická*, pokud $R^{-1} \cap R \subseteq \mathrm{id}_A$, tj. pokud $(a, b) \in R$ a zároveň $(b, a) \in R$, pak $a = b$,
- *tranzitivní*, pokud $R \circ R \subseteq R$, tj. pokud z $(a, b) \in R$ a $(b, c) \in R$ vyplývá i $(a, c) \in R$.

Relace se nazývá *ekvivalence*, pokud je současně reflexivní, symetrická i tranzitivní.



Relace se nazývá *uspořádání* jestliže je reflexivní, tranzitivní a antisymetrická. Relaci uspořádání obvykle značíme symbolem $\leq$, tj. skutečnost, že prvek $a$ je v relaci s prvkem $b$, značíme $a \leq b$.

Zde je dobré si uvědomit, že relace $<$, tj. „býti ostře menší než“, mezi reálnými (racionálními, celými, přirozenými) čísly není relace uspořádání, protože není reflexivní.

Dobrým příkladem uspořádání je inkluze. Uvažme množinu $2^A$ všech podmnožin konečné množiny $A$ (značení je speciálním případem obvyklé notace $B^A$ pro množinu všech zobrazení množiny $A$ do množiny $B$; prvky množiny $2^A$ jsou tedy zobrazení $A \to \{0, 1\}$, které "říkají", zda určitý prvek je či není v dané podmnožině). Na množině $2^A$ máme relaci $\subseteq$ danou vlastností

**1.88.** Stanovte počet zobrazení množiny $\{1, 2\}$ do množiny $\{a, b, c\}$. Kolik z nich je surjektivních a kolik injektivních?

**Řešení.** Prvku 1 můžeme v rámci zobrazení přiřadit libovolně jeden ze tří prvků $a, b, c$. Podobně také pro prvek 2 máme tři možnosti. Podle (kombinatorického) pravidla součinu tak existuje celkem $3^2$ zobrazení množiny $\{1, 2\}$ do množiny $\{a, b, c\}$. Surjektivní žádné z nich být nemůže, neboť konečná množina $\{a, b, c\}$ má více prvků než množina $\{1, 2\}$. Při libovolném zobrazení prvku 1 (tři možnosti) obdržíme injektivní zobrazení, právě když prvek 2 zobrazíme na jiný prvek (dvě možnosti). Vidíme tedy, že injektivních zobrazení množiny $\{1, 2\}$ do množiny $\{a, b, c\}$ je 6. □

**1.89.** Určete počet injektivních zobrazení množiny $\{1, 2, 3\}$ do množiny $\{1, 2, 3, 4\}$.

**Řešení.** Libovolné injektivní zobrazení mezi uvažovanými množinami je dáno výběrem (uspořádané) trojice z množiny $\{1, 2, 3, 4\}$ (prvky ve vybrané trojici budou po řadě obrazy čísel $1, 2, 3$) a obráceně každé injektivní zobrazení nám zadává takovou trojici. Je tedy hledaných injektivních zobrazení stejně jako možností výběru uspořádaných trojic ze čtyř prvků, tedy $v(3, 4) = 4 \cdot 3 \cdot 2 = 24$. □

**1.90.** Určete počet surjektivních zobrazení množiny $\{1, 2, 3, 4\}$ na množinu $\{1, 2, 3\}$.

**Řešení.** Hledaný počet určíme tak, že od počtu všech zobrazení odečteme ta, která nejsou surjektivní, to jest ta, jejichž oborem hodnot je buď jednoprvková nebo dvouprvková množina. Všech zobrazení je $V(3, 4) = 3^4$, zobrazení, jejichž oborem hodnot je jednoprvková množina, jsou tři. Počet zobrazení, jejichž oborem hodnot je dvouprvková množina, je $\binom{3}{2}(2^4 - 2)$ (Faktor $\binom{3}{2}$ udává počet způsobů, kterými můžeme vybrat obor hodnot, a máme-li již dva prvky fixovány, máme $2^4 - 2$ možností, jak na ně zobrazit čtyři prvky). Celkem je tedy počet hledaných surjektivních zobrazení

$$3^4 - \binom{3}{2}(2^4 - 2) - 3 = 36. \tag{1.4}$$

□

**1.91.** Vypište všechny relace na dvouprvkové množině $\{1, 2\}$, jež současně nejsou reflexivní, jsou symetrické a nejsou tranzitivní.

**Řešení.** Reflexní relace jsou právě ty, které obsahují obě dvojice $(1, 1)$, $(2, 2)$. Tím jsme vyloučili relace

$\{(1, 1), (2, 2)\}$, $\{(1, 1), (2, 2), (1, 2)\}$,

$\{(1, 1), (2, 2), (2, 1)\}$, $\{(1, 1), (2, 2), (1, 2), (2, 1)\}$.

„být podmnožinou“. Je tedy $X \subseteq Z$ právě, když je $X$ podmnožinou v $Z$. Evidentně jsou přitom splněny všechny tři vlastnosti pro uspořádání: skutečně, je-li $X \subseteq Y$ a zároveň $Y \subseteq X$, musí být nutně množiny $X$ a $Y$ stejné. Je-li $X \subseteq Y \subseteq Z$, je také $X \subseteq Z$. Reflexivita je také zřejmá.

Říkáme, že uspořádání $\leq$ na množině $A$ je *úplné*, když pro každé dva prvky $a, b \in A$ platí, že jsou *srovnatelné*, tj. buď $a \leq b$ nebo $b \leq a$. Všimněme si, že ne všechny dvojice $(X, Y)$ podmnožin v $A$ jsou srovnatelné v tomto smyslu. Přesněji, pokud je v $A$ více než jeden prvek, existují podmnožiny $X$ a $Y$, kdy není ani $X \subseteq Y$ ani $Y \subseteq X$.

Připomeňme rekurentní definici přirozených čísel $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, kde

$$0 = \emptyset, \quad n + 1 = \{0, 1, 2, \dots, n\}.$$

Na této množině $\mathbb{N}$ definujeme relaci $\leq$ následovně: $m \leq n$, právě když $m \in n$ nebo $m = n$. Evidentně jde o úplné uspořádaní. Např. $2 \leq 4$, protože

$$2 = \{\emptyset, \{\emptyset\}\} \in \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} = 4.$$

Jinak řečeno, samotná rekurentní definice zadává vztah $n \leq n + 1$ a tranzitivně pak $n \leq k$ pro všechna $k$, která jsou tímto postupem definována později.

**1.39. Rozklad podle ekvivalence.** Každá ekvivalence $R$ na množině $A$ zadává zároveň *rozklad* množiny $A$ na podmnožiny vzájemně ekvivalentních prvků, tzv. *třídy ekvivalence*. Pro libovolné $a \in A$ uvažujeme třídu (množinu) prvků, které jsou ekvivalentní s prvkem $a$, tj.



$$R_a = \{b \in A;\, (a, b) \in R\}.$$

Často budeme psát pro $R_a$ prostě $[a]$, je-li z kontextu zřejmé, o kterou ekvivalenci jde.

Zjevně $R_a = R_b$, právě když $(a, b) \in R$ a každá taková třída ekvivalence je tedy reprezentována kterýmkoliv svým prvkem, tzv. *reprezentantem*. Zároveň $R_a \cap R_b \neq \emptyset$, právě když $R_a = R_b$, tj. třídy ekvivalence jsou po dvou disjunktní. Konečně, $A = \cup_{a \in A} R_a$, tj. celá množina $A$ se skutečně rozloží na jednotlivé třídy.

Můžeme také třídám rozkladu rozumět tak, že třídu $[a]$ vnímáme jako prvek $a$ „až na ekvivalenci“.

**1.40. Konstrukce celých a racionálních čísel.** Na přirozených



číslech umíme sice sčítat a víme, že přičtením nuly se číslo nezmění. Umíme i definovat odečítání, při něm ale jen někdy existuje výsledek v množině $\mathbb{N}$.

Základní ideou konstrukce celých čísel z přirozených je tedy přidat k nim chybějící rozdíly. To můžeme udělat tak, že místo výsledku odečítání budeme pracovat s uspořádanými dvojicemi čísel, které nám samozřejmě vždy výsledek dobře reprezentují. Zbývá jen dobře definovat, kdy jsou (z hlediska výsledku odečítání) takové dvojice ekvivalentní. Potřebný vztah tedy je:

$$(a, b) \sim (a', b') \iff a - b = a' - b' \iff a + b' = a' + b.$$

Všimněme si, že zatímco výrazy v prostřední rovnosti v přirozených číslech neumíme, výrazy vpravo už ano. Snadno ověříme, že skutečně jde o ekvivalenci a její třídy označíme jako celá čísla $\mathbb{Z}$. Na nich definujeme operaci sčítání (a s ní i odečítání) pomocí reprezentantů, např.

$$[(a, b)] + [(c, d)] = [(a + c, b + d)],$$

Zbývající relace, které jsou symetrické a nejsou tranzitivní, musejí obsahovat $(1,2)$, $(2,1)$. Pokud taková relace obsahuje jednu z těchto dvou uspořádaných dvojic, musí obsahovat rovněž druhou (podmínka symetrie). Kdyby neobsahovala ani jednu z těchto dvou uspořádaných dvojic, pak by očividně byla tranzitivní. Z celkového počtu 16 relací na dvouprvkové množině jsme tak vybrali

$$\{(1,2),(2,1)\},\quad \{(1,2),(2,1),(1,1)\},$$

$$\{(1,2),(2,1),(2,2)\}.$$

Je vidět, že každá z těchto 3 relací není reflexivní, je symetrická a není tranzitivní. □

**1.92.** Určete počet relací ekvivalence na množině $\{1,2,3,4\}$.

**Řešení.** Ekvivalence můžeme počítat podle toho, kolik prvků mají jejich třídy rozkladu. Pro počty prvků tříd rozkladu ekvivalencí na čtyřprvkové množině jsou tyto možnosti:

| Počty prvků ve třídách rozkladu | Počet ekvivalencí daného typu |
|---|---|
| 1, 1, 1, 1 | 1 |
| 2, 1, 1 | $\binom{4}{2}$ |
| 2, 2 | $\frac{1}{2}\binom{4}{2}$ |
| 3, 1 | $\binom{4}{1}$ |
| 4 | 1 |

Celkem tedy máme 15 různých ekvivalencí. □

**Poznámka.** Obecně počet tříd rozkladu $n$-prvkové množiny udává *Bellovo číslo* $B_n$, pro které lze odvodit rekurentní formuli $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.

**1.93.** Kolik existuje relací na $n$-prvkové množině?

**Řešení.** Relace je libovolná podmnožina kartézského součinu množiny se sebou samou. Tento kartézský součin má $n^2$ prvků, a je tedy počet všech relací na $n$-prvkové množině $2^{n^2}$. □

V 1.41 jsme si zavedli zbytkové třídy a ukázali, že $\mathbb{Z}_p$ je těleso pro libovolné prvočíslo $p$. Přesto se v tomto tělese vyskytují jevy, na které nejsme u reálných či komplexních čísel zvyklí:

**1.94. Nenulový mnohočlen s nulovými hodnotami.** Najděte nenulový mnohočlen jedné neznámé s koeficienty v $\mathbb{Z}_7$, tj. výraz typu $a_n x^n + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}_7$, $a_n \neq 0$, takový, že na množině $\mathbb{Z}_7$ nabývá pouze nulových hodnot (tj. dosadíme-li za $x$ libovolný z prvků $\mathbb{Z}_7$ a výraz v $\mathbb{Z}_7$ vyčíslíme, dostaneme vždy nulu).

**Řešení.** Při konstrukci tohoto mnohočlenu se opřeme o Malou Fermatovu větu, která říká, že pro libovolné prvočíslo $p$ a číslo $a$ s ním což zjevně nezávisí na výběru reprezentantů.

Lze si přitom vždy volit reprezentanty $(a,0)$ pro kladná čísla a reprezentanty $(0,a)$ pro čísla záporná, se kterými se nám bude patrně počítat nejlépe.

Tento jednoduchý příklad ukazuje, jak důležité je umět nahlížet na třídy ekvivalence jako na celistvý objekt a soustředit se na vlastnosti těchto objektů, nikoliv formální popisy jejich konstrukcí. Ty jsou však důležité k ověření, že takové objekty vůbec existují.

U celých čísel nám už platí všechny vlastnosti skalárů (KG1)–(KG4) a (O1)–(O4), viz odstavec 1.1. Pro násobení je neutrálním prvkem jednička, ale pro žádné číslo $a$ různé od nuly a jedničky neumíme najít číslo $a^{-1}$ s vlastností $a \cdot a^{-1} = 1$, tzn. chybí nám inverzní prvky pro násobení.
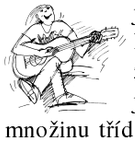
Zároveň si povšimněme, že platí vlastnost oboru integrity (OI), viz 1.1, tzn. je-li součin dvou čísel nulový, musí být alespoň jedno z nich nula.

Díky poslední jmenované vlastnosti můžeme zkonstruovat racionální čísla $\mathbb{Q}$ přidáním všech chybějících inverzí zcela obdobným způsobem, jak jsme konstruovali $\mathbb{Z}$ z množiny $\mathbb{N}$. Na množině uspořádaných dvojic $(p,q)$, $q \neq 0$, celých čísel definujeme relaci $\sim$ tak, jak očekáváme, že se mají chovat podíly $p/q$:

$$(p,q) \sim (p',q') \iff p/q = p'/q' \iff p \cdot q' = p' \cdot q.$$

Opět neumíme očekávané chování v prostřední rovnosti v množině $\mathbb{Z}$ formulovat, nicméně rovnost na pravé straně ano. Zjevně jde o dobře definovanou relaci ekvivalence (ověřte podrobnosti!) a racionální čísla jsou pak její třídy ekvivalence. Když budeme formálně psát $p/q$ místo dvojic $(p,q)$, budeme definovat operace násobení a sčítání právě pomocí formulí, které nám jsou jistě dobře známy.

**1.41. Zbytkové třídy.** Jiným dobrým a jednoduchým příkladem



jsou tzv. zbytkové třídy celých čísel. Pro pevně zvolené přirozené číslo $k$ definujeme ekvivalenci $\sim_k$ tak, že dvě čísla $a, b \in \mathbb{Z}$ jsou ekvivalentní, jestliže jejich zbytek po dělení číslem $k$ je stejný. Výslednou množinu tříd ekvivalence označujeme $\mathbb{Z}_k$. Nejjednodušší je tato procedura pro $k = 2$. To dostáváme $\mathbb{Z}_2 = \{0,1\}$, kde nula reprezentuje sudá čísla, zatímco jednička čísla lichá. Opět lze snadno zjistit, že pomocí reprezentantů můžeme korektně definovat násobení a sčítání na každém $\mathbb{Z}_k$.

**Věta.** *Zbytkové třídy $\mathbb{Z}_k$ jsou komutativním tělesem skalárů (tj. splňují i vlastnost (P) z odstavce 1.1), právě když je $k$ prvočíslo.*

*Pokud $k$ prvočíslem není, obsahuje $\mathbb{Z}$ vždy dělitele nuly. Není proto ani oborem integrity.*

Důkaz. Okamžitě je vidět druhé tvrzení. Jestliže $x \cdot y = k$ pro přirozená čísla $x$, $y$, pak samozřejmě je výsledek násobení příslušných tříd $[x] \cdot [y]$ nulový.

Naopak, jsou-li $x$ a $k$ nesoudělná, existují podle tzv. Bezoutovy rovnosti, kterou dovodíme později (viz 10.2), přirozená čísla $a$ a $b$ splňující

$$a\,x + b\,k = 1,$$

což pro odpovídající třídy ekvivalence dává

$$[a] \cdot [x] + [0] = [a] \cdot [x] = [1],$$

a proto je $[a]$ inverzním prvkem k $[x]$. □

nesoudělné platí

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p).$$

Hledaný polynom je tedy například polynom $x^7 - x$ (polynom $x^6 - 1$ by neměl nulovou hodnotu v čísle 0). □

Tělesa $\mathbb{Z}_p$ mají některé vlastnosti, na které nejsme v tělesech $\mathbb{R}$ či $\mathbb{Q}$ zvyklí. Zkoumejme například mnohočlen

$$x^2 + x$$

v tělese $\mathbb{Z}_2$. Dosadíme-li za $x$ libovolný prvek tělesa $\mathbb{Z}_2$ (tj. nulu nebo jedničku), hodnota daného mnohočlenu bude vždy nulová. Přesto tento mnohočlen není nulovým mnohočlenem. Jak uvidíme v odstavci 5.2, tak to je možné pouze v tělesech s konečným počtem prvků.

## G. Doplňující příklady k celé kapitole

**1.95.** Nechť $t$ a $m$ jsou kladná celá čísla. Ukažte, že číslo $\sqrt[m]{t}$ je buď přirozené, nebo není racionální.



**Řešení.** Ukažte, že pokud uvažovaná odmocnina není přirozená, pak není ani racionální. Pokud $\sqrt[m]{t}$ není přirozená, tak existuje prvočíslo $r$ a přirozené $s$ taková, že $r^s$ dělí $t$, $r^{s+1}$ nedělí $t$ a $m$ nedělí $s$ (zápis $\operatorname{ord}_r t = s$). Předpokládejte, že $\sqrt[m]{t} = \frac{p}{q}$, $p, q \in \mathbb{Z}$, neboli $t \cdot p^m = q^m$. Uvažte $\operatorname{ord}_r L$ a $\operatorname{ord}_r R$ a jejich dělitelnost číslem $m$ ($L$ značí levou stranu rovnice, ...). □

**1.96.** Stanovte

$$\left| \frac{(2+3i)\left(1+i\sqrt{3}\right)}{1-i\sqrt{3}} \right|.$$

**Řešení.** Neboť absolutní hodnota součinu (podílu) dvou libovolných komplexních čísel je součin (podíl) jejich absolutních hodnot a každé komplexní číslo má stejnou absolutní hodnotu jako číslo s ním komplexně sdružené, platí

$$\left| \tfrac{(2+3i)(1+i\sqrt{3})}{1-i\sqrt{3}} \right| = |2+3i| \cdot \tfrac{|1+i\sqrt{3}|}{|1-i\sqrt{3}|} = |2+3i| = \sqrt{2^2+3^2} = \sqrt{13}.$$ □

**1.97.** Číslo $\left(5\sqrt{3}+5i\right)^{12}$ zapište v co nejjednodušším tvaru.

**Řešení.** Úpravy jako postupné umocňování nebo rozvoj podle binomické věty jsou v tomto případě časově náročné. Při vyjádření

$$5\sqrt{3}+5i = 10\left(\tfrac{\sqrt{3}}{2}+\tfrac{i}{2}\right) = 10\left(\cos\tfrac{\pi}{6}+i\sin\tfrac{\pi}{6}\right)$$

užitím Moivreovy věty však snadno obdržíme

$$\left(5\sqrt{3}+5i\right)^{12} = 10^{12}\left(\cos\tfrac{12\pi}{6}+i\sin\tfrac{12\pi}{6}\right) = 10^{12}.$$ □

*1.98.* Vyjádřete $z_1+z_2$, $z_1 \cdot z_2$, $\bar{z}_1$, $|z_2|$, $\frac{z_1}{z_2}$, pro

a) $z_1 = 1-2i$, $z_2 = 4i-3$

b) $z_1 = 2$, $z_2 = i$

○

**1.99.** Uveďte vzdálenost $d$ čísel $z$, $\bar{z}$ v komplexní rovině, je-li

$$\bar{z} = \tfrac{\sqrt{3}\sqrt{3}}{2} - i\,\tfrac{3}{2}.$$

**Řešení.** Není obtížné si uvědomit, že komplexně sdružená čísla jsou v komplexní rovině souměrně sdružená podle osy $x$ a že vzdálenost komplexního čísla od osy $x$ je rovna absolutní hodnotě jeho imaginární části. To již dává $d = 3$. □

**1.100.** Setkání se zúčastnilo šest mužů. Pokud si všichni navzájem potřásli rukama, vyčíslete počet potřesení.

**Řešení.** Počet potřesení rukou zřejmě odpovídá počtu způsobů, jak lze vybrat neuspořádanou dvojici ze 6 prvků, tj. výsledek je $c\,(6,2) = \binom{6}{2} = 15$. □

**1.101.** Určete, kolika způsoby lze z 15 poslanců vybrat čtyřčlennou komisi, není-li možné, aby jistí 2 poslanci pracovali spolu.

**Řešení.** Výsledek je

$$\binom{15}{4} - \binom{13}{2} = 1\,287.$$

Obdržíme ho tak, že nejprve určíme počet všech možných výběrů čtyřčlenné komise, potom od něj odečteme počet těch výběrů, kdy oba zmínění poslanci budou vybráni (v takovém případě vybíráme pouze 2 další členy komise ze 13 poslanců). □

**1.102.** Kolika způsoby můžeme rozdělit 8 žen a 4 muže do 2 šestičlenných skupin (v nichž nerozlišujeme pořadí – jsou neuspořádané) tak, aby v obou skupinách byl alespoň 1 muž?

**Řešení.** Rozdělení 12 osob do 2 šestičlenných skupin bez jakýchkoli podmínek je dáno libovolným výběrem 6 z nich do první ze skupin, což lze provést $\binom{12}{6}$ způsoby. Skupiny ale nejsou rozlišitelné (nevíme, která z nich je první), a proto je počet všech možných rozdělení $\frac{1}{2} \cdot \binom{12}{6}$. V $\binom{8}{2}$ případech pak budou všichni muži v jedné skupině (volíme 2 ženy z 8, které skupinu doplní). Správná odpověď je tudíž

$$\tfrac{1}{2} \cdot \binom{12}{6} - \binom{8}{2} = 434.$$ □

**1.103.** Kolika způsoby lze do tří různých obálek rozmístit pět shodných stokorun a pět shodných tisícikorun tak, aby žádná nezůstala prázdná?

**Řešení.** Nejdříve zjistíme všechna rozmístění bez podmínky neprázdnosti. Těch je podle pravidla součinu (rozmísťujeme nezávisle stokoruny a tisícikoruny) $C(3,5)^2 = \binom{7}{2}^2$. Odečteme postupně rozmístění, kdy je právě jedna obálka prázdná, a poté kdy jsou dvě obálky prázdné. Celkem $C(3,5)^2 - 3(C(2,5)^2 - 2) - 3 = \binom{7}{2}^2 - 3(6^2 - 2) - 3 = 336$. □

**1.104.** Jaký je počet čtyřciferných čísel složených z číslic 1, 3, 5, 6, 7 a 9, ve kterých se žádná z cifer neopakuje?

**Řešení.** K dispozici máme šest různých číslic. Ptáme se: Kolik různých uspořádaných čtveřic z nich můžeme vybrat? Výsledek je proto $v(6,4) = 6 \cdot 5 \cdot 4 \cdot 3 = 360$. □

**1.105.** Řecká abeceda se skládá z 24 písmen. Kolik různých slov majících právě pět písmen z ní lze utvořit? (Bez ohledu na to, zda tato slova mají nějaký jazykový význam.)

**Řešení.** Pro každou z pěti pozic ve slově máme 24 možností, neboť písmena se mohou opakovat. Výsledek je tedy $V(24,5) = 24^5$. □

**1.106.** Noví hráči se sejdou v jednom volejbalovém týmu (6 lidí). Kolikrát si při seznamování (každý s každým) podají ruce? Kolikrát si hráči podají ruce se soupeřem po odehrání zápasu?

**Řešení.** Seznamuje se každá dvojice z šesti hráčů. Počet podání rukou je teda roven kombinaci $C(2,6) = \binom{6}{2} = 15$. Po zápase si každý z šesti hráčů podá ruku šestkrát (s každým z šesti soupeřů). Počet je tedy dohromady $6^2 = 36$. □

*1.107.* Na koncertě je 730 lidí. Mají někteří z nich stejné iniciály? (Neuvažujeme háčky ani čárky) ○

**1.108.** K vytrvalostnímu závodu, v němž běžci vybíhají jeden po druhém s danými časovými odstupy, se přihlásilo $k$ závodníků, mezi nimi také tři kamarádi. Stanovte počet startovních listin, v rámci kterých žádní dva z trojice kamarádů nestartují těsně po sobě. Pro jednoduchost uvažujte $k \geq 5$.

**Řešení.** Ostatních $k-3$ závodníků můžeme seřadit $(k-3)!$ způsoby. Pro uvažované tři kamarády pak máme $k-2$ míst (začátek, konec a $k-4$ mezer), na které je můžeme rozmístit $v\,(k-2, 3)$ způsoby. Podle (kombinatorického) pravidla součinu je tak výsledek

$$(k-3)! \cdot (k-2) \cdot (k-3) \cdot (k-4) = (k-2)! \cdot (k-3) \cdot (k-4). \qquad \square$$

**1.109.** Kolik existuje různých přesmyček slova KRAKATIT takových, že mezi písmeny K je právě jedno jiné písmeno?

**Řešení.** V uvažovaných přesmyčkách je šest možností, jak umístit skupinu dvou K. Fixujeme-li pevně místa pro dvě písmena K, pak ostatní písmena můžeme rozmístit na zbylých šest míst libovolně, tedy $P(1, 1, 2, 2)$ způsoby. Celkem podle pravidla součinu je hledaný počet

$$6 \cdot P(1, 1, 2, 2) = \tfrac{6 \cdot 6!}{2 \cdot 2} = 1080. \qquad \square$$

**1.110.** Turnaje se zúčastní 32 lidí. Podle požadavků organizátorů se musí libovolným způsobem rozdělit do čtyř skupin tak, aby první skupina měla 10 účastníků, druhá 8, třetí také 8 a poslední čtvrtá potom 6. Kolika způsoby se mohou takto rozdělit?

**Řešení.** Můžeme si představit, že z 32 účastníků vytvoříme řadu, kdy prvních 10 utvoří první skupinu, dalších 8 druhou atd. Celkem můžeme účastníky seřadit 32! způsoby. Uvědomme si ovšem, že na rozdělení do skupin nemá vliv, když zaměníme pořadí osob, které patří do stejné skupiny. Proto je počet navzájem různých rozdělení roven

$$P\,(10, 8, 8, 6) = \tfrac{32!}{10! \cdot 8! \cdot 8! \cdot 6!}. \qquad \square$$

**1.111.** Je potřeba ubytovat 9 osob v jednom čtyřlůžkovém, jednom třílůžkovém a jednom dvoulůžkovém pokoji. Zjistěte, kolika způsoby to lze provést.

**Řešení.** Jestliže např. hostům ve čtyřlůžkovém pokoji, přiřadíme číslici 1, v třílůžkovém pokoji číslici 2 a v dvoulůžkovém číslici 3, pak vytváříme permutace s opakováním ze tří prvků 1, 2, 3, v nichž jednička se vyskytuje čtyřikrát, dvojka třikrát a trojka dvakrát. Příslušný počet permutací je

$$P\,(4, 3, 2) = \tfrac{9!}{4! \cdot 3! \cdot 2!} = 1\,260. \qquad \square$$

*1.112.* Kolika způsoby můžeme do řady posadit 50 lidí tak, aby Pavel s Petrem ob jedno místo a Martin sousedil alespoň s jedním z nich? (Ve skupině je právě jeden Pavel, Petr i Martin) ◯

**1.113.** Určete počet způsobů, jak lze rozdělit mezi tři osoby $A$, $B$ a $C$ 33 různých mincí tak, aby osoby $A$ a $B$ měly dohromady právě dvakrát více mincí, než má osoba $C$.

**Řešení.** Ze zadání vyplývá, že osoba $C$ má obdržet 11 mincí. To lze provést $\binom{33}{11}$ způsoby. Každou ze zbývajících 22 mincí může získat osoba $A$ nebo $B$, což dává $2^{22}$ možností. Z (kombinatorického) pravidla součinu plyne výsledek $\binom{33}{11} \cdot 2^{22}$. $\square$

**1.114.** Kolika způsoby můžete mezi 4 chlapce rozdělit 40 stejných kuliček?

**Řešení.** Přidejme ke 40 kuličkám troje zápalky. Poskládáme-li kuličky a zápalky do řady, rozdělí zápalky kuličky na 4 úseky. Náhodně seřaďme chlapce. Dáme-li prvnímu chlapci všechny kuličky z prvního úseku, druhému chlapci všechny kuličky z druhého úseku atd., je již vidět, že všech rozdělení je právě $\binom{43}{3} = 12\,341$. $\square$

**1.115.** Podle kvality dělíme výrobky do skupin $I$, $II$, $III$, $IV$. Zjistěte počet všech možných rozdělení 9 výrobků do těchto skupin. Při rozdělení hledíme pouze na počet výrobků v jednotlivých skupinách.

**Řešení.** Zapisujeme-li přímo uvažované devítičlenné skupiny z prvků $I$, $II$, $III$, $IV$, vytváříme kombinace s opakováním deváté třídy ze čtyř prvků. Počet takových kombinací je $\binom{12}{9} = 220$. □

**1.116.** Kolika způsoby mohla skončit tabulka první fotbalové ligy, víme-li o ní, že žádné dva z trojice týmů Zbrojovka Brno, Baník Ostrava a Sigma Olomouc spolu v tabulce „nesousedí"? (Ligu hraje 16 mužstev.)

**Řešení.** *První způsob.* Hledaný počet spočítáme podle principu inkluze a exkluze tak, že od počtu všech možných tabulek odečteme počet tabulek, ve kterých sousedí některá dvojice z uvedených tří týmů a přičteme počet těch tabulek, ve kterých sousedí všechny tři týmy. Hledaný počet tedy je

$$16! - \binom{3}{2} \cdot 2! \cdot 15! + 3! \cdot 14! = 13599813427200.$$

*Jiné řešení.* Zmíněné tři týmy budeme považovat za „oddělovače". Zbylých třináct týmů musíme rozdělit tak, aby mezi libovolnými dvěma oddělovači byl alespoň jeden tým. Navíc zbylé týmy můžeme mezi sebou nezávisle permutovat a rovněž tak oddělovače. Celkem tedy dostáváme

$$\binom{14}{3} \cdot 13! \cdot 3! = 13599813427200$$

možností. □

**1.117.** Kolika způsoby mohla skončit tabulka první fotbalové ligy, víme-li o ní pouze, že alespoň jeden z týmů z dvojice Ostrava, Olomouc je v tabulce za týmem Brna (ligu hraje 16 mužstev).

**Řešení.** Nejprve určíme tři místa, na kterých se umístily celky Brna, Olomouce a Ostravy. Ty lze vybrat $c(3, 16) = \binom{16}{3}$ způsoby. Z šesti možných pořadí zmíněných tří týmů na vybraných třech místech vyhovují podmínce ze zadání čtyři. Pro libovolné pořadí těchto týmů na libovolně vybraných třech místech pak můžeme nezávisle volit pořadí zbylých 13 týmů na ostatních místech tabulky. Podle pravidla součinu je tedy hledaný počet tabulek roven

$$\binom{16}{3} \cdot 4 \cdot 13! = 13948526592000.$$ □

**1.118.** Kolik je možných uspořádání (v řadě) na fotce volejbalového týmu (6 hráčů), když

i) Gould a Bamba chtějí stát vedle sebe,

ii) Gould a Bamba chtějí stát vedle sebe a uprostřed,

iii) Gould a Kamil nechtějí stát vedle sebe.

**Řešení.**

i) Goulda a Bambu můžeme v tomto případě počítat za jednoho, rozlišíme jen jak stojí vzájemně. Máme $2 \cdot 5! = 240$ pořadí.

ii) Tady je to podobné,jen pozice Goulda a Bamby je pevně daná. Dostáváme $2 \cdot 4! = 48$ možností.

iii) Nejjednodušší je asi odečíst případy, kdy stojí vedle sebe (viz (i)) od všech pořadí. Dostaneme $6! - 2 \cdot 5! = 720 - 240 = 480$.

□

*1.119.* Házení mincí. Šestkrát hodíme mincí.

i) Kolik je všech různých posloupností panna, orel?
ii) Kolik je takových, že padnou právě čtyři panny?
iii) Kolik je takových, že padnou aspoň dvě panny?

○

**1.120.** Kolik existuje přesmyček slova BAZILIKA takových, že se v nich střídají souhlásky a samohlásky?

**Řešení.** Protože souhlásky i samohlásky jsou v daném slově čtyři, tak se v každé takové přesmyčce střídají pravidelně souhlásky a samohlásky. Slovo tedy může být typu $BABABABA$ nebo $ABABABAB$. Na daných čtyřech místech můžeme pak samohlásky permutovat mezi sebou ($P_o(2,2) = \frac{4!}{2!2!}$ způsoby) a nezávisle na tom i souhlásky (4! způsoby). Hledaný počet je pak dle pravidla součinu $2 \cdot 4! \cdot \frac{4!}{2!2!} = 288$. □

**1.121.** Kolika způsoby lze rozdělit 9 děvčat a 6 chlapců do dvou skupin tak, aby každá skupina obsahovala alespoň dva chlapce?

**Řešení.** Rozdělíme zvlášť děvčata a chlapce: $2^9(2^5 - 7) = 12800$. □

**1.122.** Materiál je tvořen pěti vrstvami, každá z nich má vlákna v jednom z daných šesti směrů. Kolik takových materiálů existuje? Kolik je jich takových, že dvě sousední vrstvy nemají vlákna ve stejném směru?

**Řešení.** $6^5$ a $6 \cdot 5^5$. □

**1.123.** Pro libovolné pevné $n \in \mathbb{N}$ určete počet všech řešení rovnice

$$x_1 + x_2 + \cdots + x_k = n$$

v množině kladných celých čísel.

**Řešení.** Hledáme-li řešení v oboru kladných celých čísel, tak si všimněme, že přirozená čísla $x_1, \ldots x_k$ jsou řešením dané rovnice, právě když jsou celá nezáporná čísla $y_i = x_i - 1, i = 1, \ldots, k$, řešením rovnice

$$y_1 + y_2 + \cdots + y_k = n - k.$$

Podle ‖1.26‖ je jich $\binom{n-1}{k-1}$. □

**1.124.** Kolik peněz naspořím na stavebním spoření za pět let, vkládám-li 3000 Kč měsíčně (vždy k 1. v měsíci), vklad je úročen roční úrokovou mírou 3% (úročení probíhá jednou za měsíc) a od státu obdržím ročně příspěvek 1500 Kč (státní příspěvek se připisuje vždy až 1. května následujícího roku)?

**Řešení.** Označme množství naspořených peněz po $n$-tém roce jako $x_n$. Potom dostáváme (pro $n > 2$) následující rekurentní formuli (navíc předpokládáme, že každý měsíc je přesně dvanáctina roku)

$$\begin{aligned} x_{n+1} &= 1,03(x_n) + 36000 + 1500 + \\ &+ \underbrace{0{,}03 \cdot 3000 \left(1 + \frac{11}{12} + \cdots + \frac{1}{12}\right)}_{\text{úroky z vkladů za aktuální rok}} + \\ &+ \underbrace{0{,}03 \cdot \frac{2}{3} \cdot 1500}_{\text{úrok ze státního příspěvku připsaného v aktuálním roce}} = \\ &= 1{,}03(x_n) + 38115. \end{aligned}$$

Tedy

$$x_n = 38115 \sum_{i=0}^{n-2} (1{,}03)^i + (1{,}03)^{n-1} x_1 + 1500,$$

přičemž $x_1 = 36000 + 0{,}03 \cdot 3000 \left(1 + \frac{11}{12} + \cdots + \frac{1}{12}\right) = 36585$. Celkem

$$x_5 = 38115 \left(\frac{(1{,}03)^4 - 1}{0{,}03}\right) + (1{,}03)^4 \cdot 36585 + 1500 \doteq 202136.$$

□

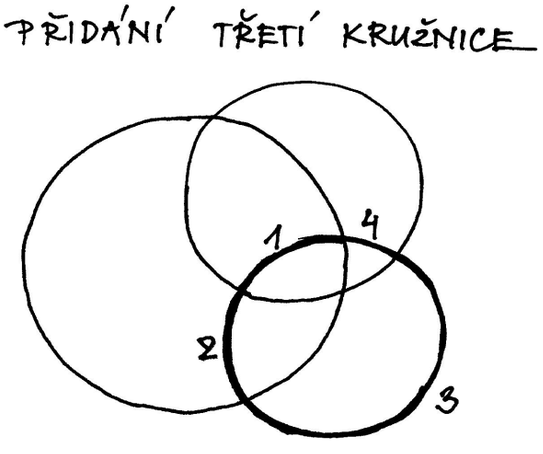
**1.125. Poznámka.** Ve skutečnosti úročení probíhá podle počtu dní, které jsou peníze na účtu. Obstarejte si skutečný výpis ze stavebního spoření, zjistěte si jeho úročení a zkuste si spočítat připsané úroky za rok. Porovnejte je se skutečně připsanou sumou. Počítejte tak dlouho, dokud sumy nebudou souhlasit.

**1.126.** Na kolik maximálně částí dělí rovinu $n$ kružnic?

**Řešení.** Pro maximální počet $p_n$ oblastí, na které dělí rovinu kružnice odvodíme rekurentní vzorec

$$p_{n+1} = p_n + 2n.$$

Všimněme si totiž, že $(n+1)$-ní kružnice protíná $n$ předchozích maximálně v $2n$ průsečících (a tato situace skutečně může nastat).



Navíc zřejmě $p_1 = 2$. Pro počet $p_n$ tedy dostáváme

$$p_n = p_{n-1} + 2(n-1) = p_{n-2} + 2(n-2) + 2(n-1) = \dots$$
$$= p_1 + \sum_{i=1}^{n-1} 2i = n^2 - n + 2.$$

□

**1.127.** Na kolik nejvýše částí dělí třírozměrný prostor $n$ rovin?

**Řešení.** Označme hledaný počet $r_n$. Vidíme, že $r_0 = 1$. Podobně jako v příkladu ‖1.30‖ uvažujme, že máme v prostoru $n$ rovin, přidejme jednu další a ptejme se, kolik nejvýše částí prostoru přibude. Opět to bude přesně tolik, kolika původními částmi prostoru přidaná rovina prochází. Kolik to může být? Počet částí prostoru, kterými $(n+1)$-ní rovina prochází je roven počtu částí, na které je přidaná $(n+1)$-ní rovina rozdělena průsečnicemi s $n$ rovinami, které v prostoru již byly rozmístěny. Těchto částí však může být podle příkladu ‖1.30‖ nejvýše $1/2 \cdot (n^2+n+2)$, dostáváme tak rekurentní formuli

$$r_{n+1} = r_n + \frac{n^2+n+2}{2}.$$

Danou rovnici opět můžeme vyřešit přímo:

$$r_n = r_{n-1} + \frac{(n-1)^2 + (n-1) + 2}{2} = r_{n-1} + \frac{n^2 - n + 2}{2} =$$
$$= r_{n-2} + \frac{(n-1)^2 - (n-1) + 2}{2} + \frac{n^2 - n + 2}{2} =$$
$$= r_{n-2} + \frac{n^2}{2} + \frac{(n-1)^2}{2} - \frac{n}{2} - \frac{(n-1)}{2} + 1 + 1 =$$
$$= r_{n-3} + \frac{n^2}{2} + \frac{(n-1)^2}{2} + \frac{(n-3)^2}{2} - \frac{n}{2} - \frac{(n-1)}{2} - \frac{(n-2)}{2} +$$
$$+ 1 + 1 + 1 =$$
$$= \dots = r_0 + \frac{1}{2}\sum_{i=1}^{n} i^2 - \frac{1}{2}\sum_{i=1}^{n} i + \sum_{i=1}^{n} 1 =$$
$$= 1 + \frac{n(n+1)(2n+1)}{12} - \frac{n(n+1)}{4} + n =$$
$$= \frac{n^3 + 5n + 6}{6},$$

kde jsme použili známého vztahu

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6},$$

který lze snadno dokázat matematickou indukcí. □

*1.128.* Na kolik maximálně částí dělí trojrozměrný prostor $n$ koulí? ○

**1.129.** Na kolik částí dělí prostor $n$ navzájem různých rovin, které všechny prochází jedním daným bodem?

**Řešení.** Pro hledaný počet $x_n$ odvodíme rekurentní formuli

$$x_n = x_{n-1} + 2(n-1),$$

dále $x_1 = 2$, tedy

$$x_n = n(n-1) + 2.$$

□

**1.130.** Z balíčku 52 karet náhodně vybereme 16 karet. Vyjádřete pravděpodobnost, že vybereme právě 10 červených a 6 černých karet.

**Řešení.** Nejdříve si uvědomme, že nemusíme zohledňovat pořadí výběru karet. (Ve výsledném zlomku bychom uspořádané výběry získali tak, že bychom číslem 16! vynásobili čitatele i jmenovatele.) Počet všech možných (neuspořádaných) výběrů 16 karet z 52 je $\binom{52}{16}$. Podobně je počet všech možných výběrů 10 karet z 26 roven $\binom{26}{10}$ a 6 karet z 26 pak $\binom{26}{6}$. Neboť vybíráme nezávisle na sobě 10 karet z 26 červených a 6 karet z 26 černých, užití (kombinatorického) pravidla součinu dává výsledek

$$\frac{\binom{26}{10}\cdot\binom{26}{6}}{\binom{52}{16}} \doteq 0{,}118. \qquad \square$$

**1.131.** V urně je 7 bílých, 6 žlutých a 5 modrých koulí. Vylosujeme (bez vracení) 3 koule. Určete pravděpodobnost, že právě 2 jsou bílé.

**Řešení.** Celkem máme $\binom{7+6+5}{3}$ způsobů, jak lze vybrat 3 koule. Vylosovat právě 2 bílé umožňuje $\binom{7}{2}$ výběrů bílých a současně $\binom{11}{1}$ výběrů zbylé (třetí) koule. Podle pravidla součinu je tak počet způsobů, jak lze vylosovat právě 2 bílé, roven $\binom{7}{2}\cdot\binom{11}{1}$. Odsud již plyne výsledek

$$\frac{\binom{7}{2}\cdot 11}{\binom{18}{3}} \doteq 0{,}283. \qquad \square$$

**1.132.** Z karetní hry o 108 kartách ($2\times 52+4$ žolíci) bez vracení vybereme 4 karty. Jaká je pravděpodobnost, že aspoň jedna z nich je eso nebo žolík?

**Řešení.** Lehce můžeme určit pravděpodobnost opačného (komplementárního) jevu znamenajícího, že ve vybrané čtveřici není žádná z 12 uvažovaných karet (8 es a 4 žolíků). Tato pravděpodobnost je dána poměrem počtu výběrů 4 karet z 96 a počtu výběrů 4 karet ze 108, tj. je rovna $\binom{96}{4}/\binom{108}{4}$. Opačný jev má tudíž pravděpodobnost

$$1 - \frac{\binom{96}{4}}{\binom{108}{4}} \doteq 0{,}380. \qquad \square$$

**1.133.** Při házení kostkou padla jedenáctkrát po sobě čtyřka. Uveďte pravděpodobnost, že padne podvanácté.

**Řešení.** Předchozí výsledky (podle našich předpokladů) nijak neovlivňují, co padne na kostce při dalších hodech. Proto je hledaná pravděpodobnost $1/6$. $\square$

**1.134.** Z balíčku 32 karet náhodně vypadne 6 karet. Jaká je pravděpodobnost, že jsou všechny téže barvy?

**Řešení.** K tomu, abychom získali výsledek

$$\frac{4\cdot\binom{8}{6}}{\binom{32}{6}} \doteq 1{,}234\cdot 10^{-4},$$

stačí nejprve zvolit jednu ze 4 barev a uvědomit si, že existuje $\binom{8}{6}$ způsobů, jak vybrat 6 karet z 8 této barvy. $\square$

**1.135.** Tři hráči dostanou po 10 kartách a 2 zbudou (z balíčku připraveného na mariáš nebo prší – 32 karet, z toho 4 esa). Je pravděpodobnější, že někdo dostane listovou sedmu, osmu a devítku, nebo to, že zbyla dvě esa?

**Řešení.** Protože pravděpodobnost, že nějaký z hráčů dostane uvedené tři karty, je rovna hodnotě

$$3\,\frac{\binom{29}{7}}{\binom{32}{10}},$$

zatímco pravděpodobnost, že zbudou dvě esa, je rovna číslu

$$\frac{\binom{4}{2}}{\binom{32}{2}},$$

je pravděpodobnější, že nějaký z hráčů dostal zmíněné tři karty. Poznamenejme, že nerovnost

$$\frac{3\cdot\binom{29}{7}}{\binom{32}{10}} > \frac{\binom{4}{2}}{\binom{32}{2}}$$

lze dokázat úpravou obou jejích stran, kdy opakovaným krácením (po vyjádření kombinačních čísel dle definice) lehce dostaneme $6 > 1$. □

**1.136.** Dva přátelé střílejí nezávisle na sobě do jednoho terče, každý po jednom výstřelu. Pravděpodobnost zásahu terče pro prvního je 0, 4, pro druhého je 0, 3. Nalezněte pravděpodobnost $P$ jevu, že po střelbě bude v terči právě jeden zásah.

**Řešení.** Výsledek stanovíme tak, že sečteme pravděpodobnosti těchto dvou neslučitelných jevů: trefil se první střelec a druhý nikoli; první střelec minul, zatímco druhý terč zasáhl. Při nezávislosti jevů (která se zachovává také tehdy, když uvažujeme komplementy některých z jevů) je pravděpodobnost společného nastoupení dána součinem pravděpodobností jednotlivých jevů. Užitím toho dostáváme

$$P = 0{,}4 \cdot (1 - 0{,}3) + (1 - 0{,}4) \cdot 0{,}3 = 0{,}46.$$ □

**1.137.** Dvanáctkrát po sobě házíme třemi mincemi. Jaká je pravděpodobnost, že alespoň v jednom hodu padnou tři líce?

**Řešení.** Uvážíme-li, že při opakovaní téhož pokusu jsou jednotlivé výsledky nezávislé, a označíme-li pro $i \in \{1, \ldots, 12\}$ jako $A_i$ jev „při $i$-tém hodu padly tři líce“, určujeme

$$P\left(\bigcup_{i=1}^{12} A_i\right) = 1 - (1 - P(A_1)) \cdot (1 - P(A_2)) \cdots (1 - P(A_{12})).$$

Pro každé $i \in \{1, \ldots, 12\}$ je však $P(A_i) = 1/8$, neboť na každé ze tří mincí padne líc s pravděpodobností $1/2$ nezávisle na tom, zda na ostatním mincích padl líc, příp. rub. Nyní již můžeme napsat výsledek

$$1 - \left(\tfrac{7}{8}\right)^{12}.$$ □

**1.138.** V jisté zemi mají parlament, ve kterém zasedá 200 poslanců. Dvě hlavní politické strany, které v zemi existují, si při „volbách“ házejí o každý poslanecký mandát zvlášť mincí. Každá z těchto stran má přidělenu jednu stranu mince. Té straně, jejíž strana mince padne, náleží mandát, o který se právě losovalo. Jaká je pravděpodobnost, že každá ze stran získá 100 mandátů? (mince je „poctivá“)

**Řešení.** Všech možných výsledků losování (uvažovaných jako dvousetčlenné posloupnosti rubů a líců) je $2^{200}$. Pokud každá strana získá právě sto mandátů, je ve vylosované posloupnosti právě sto líců a sto rubů. Takových posloupností je $\binom{200}{100}$ (taková posloupnost je jednoznačně určená výběrem sto členů z dvou set možných, na kterých budou např. líce). Celkem je hledaná pravděpodobnost

$$\frac{\binom{200}{100}}{2^{200}} = \frac{\frac{200!}{100!\cdot 100!}}{2^{200}} \doteq 0{,}056.$$ □

**1.139.** Sedm Čechů a pět Angličanů náhodně rozdělíme na dvě (neprázdné) skupiny. Jaká je pravděpodobnost, že v jedna ze skupin bude tvořena pouze Čechy?

**Řešení.** Všech možností je $2^{12} - 1$. Jestliže jsou v jedné skupině pouze Češi, znamená to, že všichni Angličané jsou v jedné skupině (buď v první nebo druhé). Zbývá rozdělit Čechy na dvě neprázdné skupiny, to můžeme $2^7 - 1$ způsoby. Na závěr ještě přičíst rozdělení, kdy jsou skupiny podle národností:

$$\frac{2\cdot(2^7-1)+1}{2^{12}-1}.$$ □

**1.140.** Zjistěte pravděpodobnost, že při hodu dvěma kostkami padla alespoň na jedné kostce čtyřka, jestliže padl součet 7.

**Řešení.** Příklad řešíme pomocí klasické pravděpodobnosti, kdy podmínku interpretujeme jako zúžení pravděpodobnostního prostoru. Ten má vzhledem k podmínce tedy 6 prvků, z čehož právě 2 jsou příznivé vyšetřovanému jevu. Správná odpověď je $2/6 = 1/3$. □

**1.141.** Hodíme dvěma kostkami. Určete podmíněnou pravděpodobnost, že na první kostce padla pětka za podmínky, že padl součet 9. Na základě tohoto výsledku rozhodněte o nezávislosti jevů „na první kostce padla pětka“ a „padl součet 9“.

**Řešení.** Označíme-li jev „na první kostce padla pětka“ jako $A$ a jev „padl součet 9“ jako $H$, pak platí

$$P(A|H) = \frac{P(A\cap H)}{P(H)} = \frac{\frac{1}{36}}{\frac{4}{36}} = \frac{1}{4}.$$

Uvědomme si, že součet 9 můžeme získat tak, že na první kostce padne 3 a na druhé 6, na první 4 a na druhé 5, na první 5 a na druhé 4 nebo na první 6 a na druhé 3. Z těchto čtyř (stejně pravděpodobných) výsledků jevu A vyhovuje právě jeden. Protože pravděpodobnost jevu A je očividně $1/6 \neq 1/4$, nejsou uvedené jevy nezávislé. □

**1.142.** Uvažujme rodiny se dvěma dětmi a pro jednoduchost předpokládejme, že všechny možnosti v množině $\Omega = \{kk, kh, hk, hh\}$, kde $k$ značí „kluk“ a $h$ znamená „holka“ při zohlednění stáří dětí, jsou stejně pravděpodobné. Zaveďme náhodné jevy

$$H_1 \text{ – rodina má kluka}, \qquad A_1 \text{ – rodina má 2 kluky}.$$

Vypočtěte $P(A_1|H_1)$.

Podobně uvažujme rodiny se třemi dětmi, kdy je

$$\Omega = \{kkk, kkh, khk, hkk, khh, hkh, hhk, hhh\}.$$

Jestliže

$$H_2 \text{ – rodina má kluka i holku}, \qquad A_2 \text{ – rodina má nejvýše jednu holku},$$

rozhodněte o nezávislosti náhodných jevů $A_2$ a $H_2$.

**Řešení.** Uvážením, které ze čtyř prvků množiny $\Omega$ (ne)vyhovují jevu $A_1$, resp. $H_1$, lehce získáváme

$$P(A_1|H_1) = \frac{P(A_1\cap H_1)}{P(H_1)} = \frac{P(A_1)}{P(H_1)} = \frac{\frac{1}{4}}{\frac{3}{4}} = \frac{1}{3}.$$

Dále máme zjistit, zda platí

$$P(A_2 \cap H_2) = P(A_2) \cdot P(H_2).$$

Opět si stačí pouze uvědomit, že jevu $A_2$ vyhovují právě prvky $kkk, kkh, khk, hkk$ množiny $\Omega$, jevu $H_2$ prvky $kkh, khk, hkk, khh, hkh, hhk$ a jevu $A_2 \cap H_2$ prvky $kkh, khk, hkk$. Odtud plyne

$$P(A_2 \cap H_2) = \frac{3}{8} = \frac{4}{8} \cdot \frac{6}{8} = P(A_2) \cdot P(H_2),$$

což znamená, že jevy $A_2$ a $H_2$ jsou nezávislé. □

**1.143.** V osudí je 9 červených a 7 bílých koulí. Postupně vytáhneme 3 koule (bez vracení). Určete pravděpodobnost, že první dvě budou červené a třetí bílá.

**Řešení.** Příklad budeme řešit pomocí věty o násobení pravděpodobností. Nejprve požadujeme vytažení červené koule, což se podaří s pravděpodobností 9/16. Pokud byla poprvé vytažena červená koule, při druhém tahu vytáhneme znovu červenou kouli s pravděpodobností 8/15 (v osudí je 15 koulí, z toho 8 červených). Konečně, pokud byla dvakrát vytažena červená koule, pravděpodobnost, že

potom bude vytažena bílá, je 7/14 (v osudí je 7 bílých koulí a 7 červených koulí). Celkem dostáváme

$$\frac{9}{16} \cdot \frac{8}{15} \cdot \frac{7}{14} = 0{,}15. \qquad \square$$

**1.144.** V osudí je 10 koulí, a to 5 černých a 5 bílých. Postupně budeme losovat po jedné kouli, přičemž vytaženou kouli nevrátíme zpět. Stanovte pravděpodobnost, že nejprve vytáhneme bílou, poté černou, pak bílou a v posledním čtvrtém tahu opět bílou kouli.

**Řešení.** Použijeme větu o násobení pravděpodobností. V prvním tahu vytáhneme bílou kouli s pravděpodobností 5/10, poté černou s pravděpodobností 5/9, následně bílou s pravděpodobností 4/8 a na závěr bílou s pravděpodobností 3/7. Dohromady to dává

$$\frac{5}{10} \cdot \frac{5}{9} \cdot \frac{4}{8} \cdot \frac{3}{7} = \frac{5}{84}. \qquad \square$$

**1.145.** Jaká je pravděpodobnost, že součet dvou náhodně zvolených kladných čísel menších než 1 bude menší než 3/7?

**Řešení.** Je vidět, že jde o jednoduchý příklad na geometrickou pravděpodobnost, kdy jako základní prostor $\Omega$ se nabízí čtverec s vrcholy [0, 0], [1, 0], [1, 1], [0, 1] (volíme dvě čísla mezi 0 a 1). Zajímá nás pravděpodobnost jevu udávajícího, že pro náhodně zvolený bod $[x, y]$ v tomto čtverci bude platit $x + y < 3/7$; tj. pravděpodobnost toho, že zvolený bod se bude nacházet uvnitř trojúhelníku $A$ s vrcholy [0, 0], [3/7, 0], [0, 3/7]. Nyní již snadno vyčíslíme

$$P(A) = \frac{\operatorname{vol} A}{\operatorname{vol} \Omega} = \frac{\left(\frac{3}{7}\right)^2/2}{1} = \frac{9}{98}. \qquad \square$$

**1.146.** Nechť je náhodně rozlomena tyč na tři části. Stanovte pravděpodobnost, že délka druhé (prostřední) části bude větší než dvě třetiny délky tyče před jejím rozlomením.

**Řešení.** Nejprve si označme délku uvažované tyče jako $d$. Rozlomení tyče ve dvou místech je dáno volbou bodů, kde ji zlomíme. Označme jako $x$ bod, ve kterém je první (např. blíže nějakému předmětu) zlom, a jako $x + y$ bod, ve kterém je druhý zlom. To nám říká, že za základní prostor lze považovat množinu $\{[x, y];\ x \in (0, d), y \in (0, d - x)\}$, tj. trojúhelník s vrcholy v bodech [0, 0], $[d, 0]$, $[0, d]$. Délka prostřední části je dána hodnotou $y$. Požadavek ze zadaní lze nyní zapsat v jednoduchém tvaru $y > 2d/3$, což odpovídá trojúhelníku s vrcholy $[0, 2d/3]$, $[d/3, 2d/3]$, $[0, d]$. Obsahy uvažovaných pravoúhlých rovnoramenných trojúhelníků jsou $d^2/2$ a $(d/3)^2/2$, a proto je hledaná pravděpodobnost

$$\frac{\frac{d^2}{3^2 \cdot 2}}{\frac{d^2}{2}} = \frac{1}{9}. \qquad \square$$

**1.147.** Tyč o délce 2 m je náhodně rozřezána na tři části. Nalezněte pravděpodobnost jevu, že třetí část měří méně než 1, 5 m.

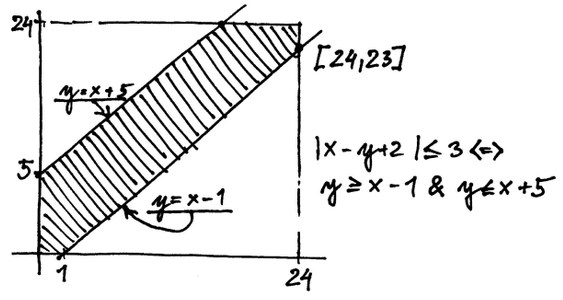
**Řešení.** Tento příklad je na užití geometrické pravděpodobnosti, kdy hledáme pravděpodobnost toho, že součet délek prvních dvou částí je větší než čtvrtina délky tyče. Určeme pravděpodobnost opačného jevu, tj. pravděpodobnost, když budou náhodně (a nezávisle na sobě) zvolena dvě místa, ve kterých bude tyč rozřezána, že budou obě v první čtvrtině tyče. Pravděpodobnost tohoto jevu je $1/4^2$, neboť pravděpodobnost výběru místa v první čtvrtině tyče je zřejmě 1/4 a tento výběr se (nezávisle) jednou opakuje. Pravděpodobnost hledaného (opačného) jevu je tak 15/16. $\square$

**1.148.** Mirek a Marek chodí na obědy do univerzitní menzy. Menza má otevřeno od 11h do 14h. Každý z nich stráví na obědě půl hodiny a dobu příchodu (mezi 11h a 14h) si vybírá náhodně. Jaká je pravděpodobnost, že se na obědě v daný den potkají, sedávají-li oba u stejného stolu?

**Řešení.** Prostor všech možných jevů je čtverec $3 \times 3$. Označíme-li $x$ dobu příchodu Mirka a $y$ dobu příchodu Marka, tak tito se potkají, právě když $|x - y| \leq 1/2$. Tato nerovnost vymezuje ve čtverci možných událostí oblast, jejíž obsah je roven $11/36$ obsahu čtverce. Tomuto zlomku je tedy rovna i hledaná pravděpodobnost. □

**1.149.** Z Brna vyrazí náhodně někdy mezi polednem a čtvrtou hodinou odpolední Honza autem do Prahy a opačným směrem někdy ve stejném intervalu autem Martin. Oba si dávají půl hodiny pauzu v motorestu v polovině cesty (přístupném pro oba směry). Jaká je pravděpodobnost, že se tam potkají, jezdí-li Honza rychlostí 150 km/h a Martin 100 km/h? (Vzdálenost Brno-Praha je 200 km)

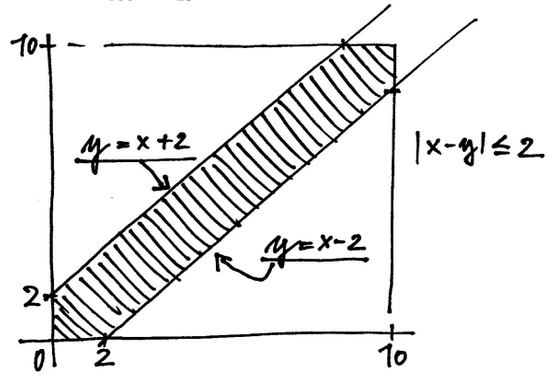
**Řešení.** Označíme-li dobu odjezdu Martina $x$ a dobu odjezdu Honzy $y$ a pro menší výskyt zlomků v následujících výpočtech zvolíme za jednotku deset minut, tak stavovým prostorem bude čtverec $24 \times 24$. Doba příjezdu Martina do motorestu je $x+6$, do příjezdu Honzy $x+4$. Stejně jako v předchozím příkladu to, že se v motorestu potkají, je ekvivalentní tomu, že doby jejich příjezdu se neliší o více než o půl hodiny, tedy $|(x+6)-(y+4)| \leq 3$. Tato podmínka nám pak ve stavovém čtverci vymezuje oblast o obsahu $24^2 - \frac{1}{2}(23^2 + 19^2)$ (viz obr.) a hledaná pravděpodobnost je




$$p = \frac{24^2 - \frac{1}{2}(23^2+19^2)}{24^2} = \frac{131}{576} \doteq 0{,}227.$$ □

**1.150.** Mirek vyjede náhodně mezi desátou hodinou dopolední a osmou hodinou večerní z Brna do Prahy. Marek vyjede náhodně ve stejném intervalu z Prahy do Brna. Oběma trvá cesta 2 hodiny. Jaká je pravděpodobnost, že se po cestě potkají (jezdí po stejné trase)?

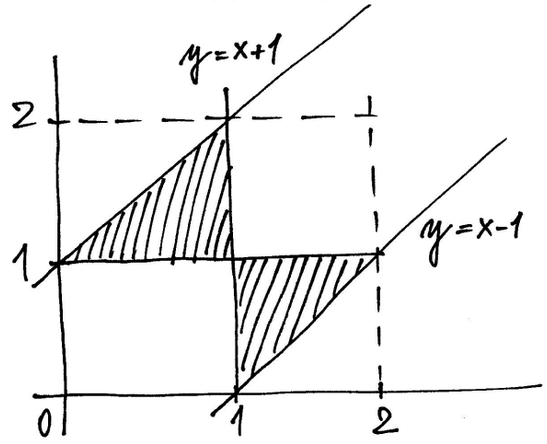
**Řešení.** Řešíme naprosto analogicky jako v předchozím příkladě. Prostor všech možných jevů je čtverec $10 \times 10$, Mirek, vyjíždějící v čase $x$, potká Marka, vyjíždějícího v čase $y$ právě když $|x-y| \leq 2$. Hledaná pravděpodobnost je $p = \frac{36}{100} = \frac{9}{25} = 0{,}36$.




□

**1.151.** Dvoumetrová tyč je náhodně rozdělena na tři díly. Určete pravděpodobnost, že ze vzniklých dílů půjde sestavit trojúhelník.

**Řešení.** Rozdělení tyče je dáno stejně jako v předchozím příkladě body řezu $x$ a $y$ a jevovým prostorem je opět čtverec $2 \times 2$. Aby z částí bylo možno sestavit trojúhelník, musejí jejich délky splňovat tzv. trojúhelníkové nerovnosti, tedy součet délek libovolných dvou částí musí být větší než délka třetí části. Vzhledem k tomu, že součet délek je roven 2 m, je tato podmínka ekvivalentní podmínce, že každá s částí musí být menší než 1 m. To pomocí řezů $x$ a $y$ vyjádříme tak, že nesmí platit současně $x \leq 1$ a $y \leq 1$ nebo současně $x \geq 1$ a $y \geq 1$ (odpovídá podmínkám, že krajní díly tyče jsou menší než 1), navíc $|x - y| \leq 1$ (prostřední díl musí být menší než jedna). Tyto podmínky splňuje vyšrafovaná oblast na obrázku a jak snadno nahlédneme, její obsah je 1/4.




□

**1.152.** Jsou rovnice

$$\text{(a)} \quad \begin{aligned} 4x_1 &- \sqrt{3}x_2 &&= 3, \\ x_1 &- 2\sqrt{7}x_2 &&= -2; \end{aligned}$$

$$\text{(b)} \quad \begin{aligned} 4x_1 &- \sqrt{3}x_2 &&= 16, \\ x_1 &- 2\sqrt{7}x_2 &&= -7; \end{aligned}$$

$$\text{(c)} \quad \begin{aligned} 4x_1 &+ 2x_2 &&= 7, \\ -2x_1 &- x_2 &&= -3 \end{aligned}$$

jednoznačně řešitelné (mají právě 1 řešení)?

**Řešení.** Soustava lineárních rovnic je jednoznačně řešitelná právě tehdy, když je nenulový determinant matice určené koeficienty na levé straně soustavy. Zejména tedy absolutní členy rovnic (čísla na pravé straně) neovlivňují jednoznačnost řešení soustavy. Musíme tedy ve variantách (a) a (b) dostat stejnou odpověď. Protože

$$\begin{vmatrix} 4 & -\sqrt{3} \\ 1 & -2\sqrt{7} \end{vmatrix} = 4 \cdot \left(-2\sqrt{7}\right) - \left(-\sqrt{3} \cdot 1\right) \neq 0,$$

$$\begin{vmatrix} 4 & 2 \\ -2 & -1 \end{vmatrix} = 4 \cdot (-1) - (2 \cdot (-2)) = 0,$$

mají soustavy ve variantách (a) a (b) právě 1 řešení a poslední soustava nikoliv. Vynásobíme-li druhou rovnici v (c) číslem $-2$, vidíme, že tato soustava nemá řešení. □

*1.153.* V $\mathbb{R}^2$ určete vrcholy nějakého rovnostranného trojúhelníka $ABC$ o straně délky 1, s bodem $C = [1, 1]$ a základnou $AB$ rovnoběžnou s přímkou $3x + 4y = 10^5$. ○

**1.154.** Vypočítejte obsah $S$ čtyřúhelníku zadaného vrcholy

$$[0, -2], \quad [-1, 1], \quad [1, 5], \quad [1, -1].$$

**Řešení.** Při obvyklém označení vrcholů

$$A = [0, -2], \quad B = [1, -1], \quad C = [1, 5], \quad D = [-1, 1]$$

a neméně obvyklém rozdělení čtyřúhelníku na trojúhelníky $ABC$ a $ACD$ s obsahy $S_1$ a $S_2$, dostáváme

$$S = S_1 + S_2 = \tfrac{1}{2}\begin{vmatrix} 1-0 & 1-0 \\ -1+2 & 5+2 \end{vmatrix} + \tfrac{1}{2}\begin{vmatrix} 1-0 & -1-0 \\ 5+2 & 1+2 \end{vmatrix} = \tfrac{1}{2}(7-1) + \tfrac{1}{2}(3+7) = 8. \qquad \square$$

**1.155.** Určete obsah čtyřúhelníka $ABCD$ s vrcholy $A = [1, 0]$, $B = [11, 13]$, $C = [2, 5]$ a $D = [-2, -5]$.

**Řešení.** Čtyřúhelník rozdělíme na dva trojúhelníky $ABC$ a $ACD$. Jejich obsahy pak spočítáme pomocí patřičných determinantů, viz 1.34,

$$S = \left|\tfrac{1}{2}\begin{vmatrix} 1 & 5 \\ 10 & 13 \end{vmatrix}\right| + \left|\tfrac{1}{2}\begin{vmatrix} 1 & 5 \\ -3 & -5 \end{vmatrix}\right| = \tfrac{47}{2}. \qquad \square$$

**1.156.** Spočítejte obsah rovnoběžníku s vrcholy v bodech [5, 5], [6, 8] a [6, 9].

**Řešení.** Přestože takový rovnoběžník není zadán jednoznačně (není uveden čtvrtý vrchol), trojúhelník s vrcholy [5, 5], [6, 8] a [6, 9] musí být nutně polovinou každého rovnoběžníku s těmito třemi vrcholy (jedna ze stran trojúhelníku se stane úhlopříčkou rovnoběžníku). Proto je hledaný obsah vždy roven determinantu

$$\begin{vmatrix} 6-5 & 6-5 \\ 8-5 & 9-5 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 3 & 4 \end{vmatrix} = 1 \cdot 4 - 1 \cdot 3 = 1. \qquad \square$$

**1.157.** Stanovte rozlohu louky, která je na pozemkové mapě ohraničena body o kótách $[-7, 1]$, $[-1, 0]$, $[29, 0]$, $[25, 1]$, $[24, 2]$ a $[17, 5]$. (Jednotky neuvažujte. Jsou určeny poměrem pozemkové mapy vůči skutečnosti.)

**Řešení.** Uvažovaný šestiúhelník můžeme rozdělit např. na čtyři trojúhelníky s vrcholy

$$[-7, 1], [-1, 0], [17, 5]; \qquad [-1, 0], [24, 2], [17, 5];$$
$$[-1, 0], [25, 1], [24, 2]; \qquad [-1, 0], [29, 0], [25, 1].$$

Jejich obsahy jsou po řadě 24, 89/2, 27/2 a 15, což dává výsledek

$$24 + 44\tfrac{1}{2} + 13\tfrac{1}{2} + 15 = 97. \qquad \square$$

**1.158.** Určete obsah trojúhelníka $A_2A_3A_{11}$, kde $A_0A_1 \ldots A_{11}$ jsou vrcholy pravidelného dvanáctiúhelníka vepsaného do kružnice o poloměru 1.

**Řešení.** Vrcholy dvanáctiúhelníka můžeme ztotožnit s dvanáctými odmocninami z čísla 1 v komplexní rovině. Zvolíme-li navíc $A_0 = 1$, pak můžeme psát $A_k = \cos(2k\pi/12) + i\sin(2k\pi/12)$. Pro vrcholy zkoumaného trojúhelníka máme:

$$A_2 = \cos(\pi/3) + i\sin(\pi/3) = 1/2 + i\sqrt{3}/2,$$
$$A_3 = \cos(\pi/2) + i\sin(\pi/2) = i,$$
$$A_{11} = \cos(-\pi/6) + i\sin(-\pi/6) = \sqrt{3}/2 - i/2,$$

neboli souřadnice těchto bodů v komplexní rovnině jsou $A_2 = [1/2, \sqrt{3}/2]$, $A_3 = [0, 1]$, $A_{11} = [\sqrt{3}/2, -\frac{1}{2}]$. Podle vzorce pro obsah trojúhelníka je potom hledaný obsah $S$ roven

$$S = \frac{1}{2}\begin{vmatrix} A_2 - A_{11} \\ A_3 - A_{11} \end{vmatrix} = \frac{1}{2}\begin{vmatrix} \frac{1}{2} - \frac{\sqrt{3}}{2} & \frac{1}{2} + \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{3}{2} \end{vmatrix} = \frac{3 - \sqrt{3}}{4}.$$

Vzhledem ke kladnosti předchozího determinantu jsme mohli z estetických důvodů vynechat jeho absolutní hodnotu. □

**1.159.** Je dán trojúhelník s vrcholy $A = [5, 6]$, $B = [7, 8]$, $C = [5, 8]$. Určete, které jeho strany je vidět z bodu $P = [0, 1]$.

**Řešení.** Uspořádáme vrcholy v kladném smyslu, tedy proti směru hodinových ručiček: [5, 6], [7, 8], [5, 8]. Pomocí příslušných determinantů určíme, zda-li je bod [0, 1] „nalevo“ či „napravo“ od jednotlivých stran trojúhelníka uvažovaných jako orientované úsečky

$$\begin{vmatrix} B - P \\ C - P \end{vmatrix} = \begin{vmatrix} 7 & 7 \\ 5 & 7 \end{vmatrix} > 0, \quad \begin{vmatrix} C - P \\ A - P \end{vmatrix} = \begin{vmatrix} 5 & 7 \\ 5 & 5 \end{vmatrix} < 0,$$
$$\begin{vmatrix} A - P \\ B - P \end{vmatrix} = \begin{vmatrix} 5 & 5 \\ 7 & 7 \end{vmatrix} = 0.$$

Z nulovosti posledního determinantu vidíme, že body [0, 1], [5, 6] a [7, 8] leží na přímce, stranu $AB$ tedy nevidíme. Stranu $BC$ rovněž tak nevidíme, na rozdíl od strany $AC$, pro kterou je příslušný determinant záporný. □

**1.160.** Určete, které strany čtyřúhelníka s vrcholy

$$A = [95, 99], \qquad B = [130, 106],$$
$$C = [40, 60], \qquad D = [130, 120].$$

jsou viditelné z bodu [2, 0].

**Řešení.** Nejprve je třeba určit strany čtyřúhelníka („správné“ pořadí vrcholů): $ACBD$. Po spočítání příslušných determinantů jako v předchozích příkladech zjistíme, že je vidět pouze strana $CB$. □

**1.161.** Určete počet relací na množině {1, 2, 3, 4}, které jsou současně symetrické i tranzitivní.

**Řešení.** Relace uvedených vlastností je relací ekvivalence na nějaké podmnožině množiny {1, 2, 3, 4}. Celkem $1 + 4 \cdot 1 + \binom{4}{2} \cdot 2 + \binom{4}{3} \cdot 5 + 15 = 52$. □

*1.162.* Určete počet relací uspořádání na tříprvkové množině. ○

*1.163.* Určete počet relací uspořádání na množině {1, 2, 3, 4} takových, že prvky 1 a 2 jsou nesrovnatelné (tedy neplatí $1 \prec 2$ ani $2 \prec 1$, kde $\prec$ je označení uvažované relace uspořádání). ○

**1.164.** Určete počet surjektivních zobrazení $f$ množiny {1, 2, 3, 4, 5} na množinu {1, 2, 3} takových, že $f(1) = f(2)$.

**Řešení.** Každé takové zobrazení je jednoznačně dáno obrazem prvků {1, 3, 4, 5}, těchto zobrazení je tedy přesně tolik, kolik je zobrazení surjektivních zobrazení množiny {1, 3, 4, 5} na množinu {1, 2, 3}, tedy 36, jak víme z předchozího příkladu. □

**1.165.** Výčtem prvků zadejte $S \circ R$, je-li

$$R = \{(2,4), (4,4), (4,5)\} \subseteq \mathbb{N} \times \mathbb{N},$$
$$S = \{(3,1), (3,2), (3,5), (4,1), (4,4)\} \subseteq \mathbb{N} \times \mathbb{N}.$$

**Řešení.** Uvážením všech výběrů dvou uspořádaných dvojic

$$(2,4), (4,1); \quad (2,4), (4,4); \quad (4,4), (4,1); \quad (4,4), (4,4)$$

splňujících, že druhá složka první uspořádané dvojice, která je prvkem $R$, je rovna první složce druhé uspořádané dvojice, která je prvkem $S$, dostáváme

$$S \circ R = \{(2,1), (2,4), (4,1), (4,4)\}. \qquad \square$$

**1.166.** Nechť je dána binární relace

$$R = \{(0,4), (-3,0), (5,\pi), (5,2), (0,2)\}$$

mezi množinami $A = \mathbb{Z}$ a $B = \mathbb{R}$. Vyjádřete $R^{-1}$ a $R \circ R^{-1}$.

**Řešení.** Ihned vidíme, že

$$R^{-1} = \{(4,0), (0,-3), (\pi,5), (2,5), (2,0)\}.$$

Odtud pak dále

$$R \circ R^{-1} = \{(4,4), (0,0), (\pi,\pi), (2,2), (4,2), (\pi,2), (2,\pi), (2,4)\}. \qquad \square$$

**1.167.** Rozhodněte, zda je relace $R$ určená podmínkou

(a) $(a,b) \in R \iff |a| < |b|$;
(b) $(a,b) \in R \iff |a| = |2b|$

na množině celých čísel $\mathbb{Z}$ tranzitivní.

**Řešení.** V prvním případě relace $R$ tranzitivní je, protože platí

$$|a| < |b|, \ |b| < |c| \implies |a| < |c|.$$

Ve druhém případě relace $R$ tranzitivní není. Stačí např. uvážit, že

$$(4,2), (2,1) \in R, \quad (4,1) \notin R. \qquad \square$$

**1.168.** Najděte všechny relace na $M = \{1,2\}$, které nejsou antisymetrické. Které z nich jsou tranzitivní?

**Řešení.** Hledané relace, jež nejsou antisymetrické, jsou čtyři. Jsou to právě ty podmnožiny $\{1,2\} \times \{1,2\}$, které obsahují prvky $(1,2)$, $(2,1)$ (jinak nemůže být podmínka antisymetrie porušena). Z těchto čtyř je tranzitivní pouze jediná relace

$$\{(1,1), (1,2), (2,1), (2,2)\} = M \times M,$$

protože nezahrnutí dvojic $(1,1)$ a $(2,2)$ do tranzitivní relace by znamenalo, že nemůže obsahovat zároveň $(1,2)$ a $(2,1)$. $\square$

**1.169.** Existuje relace ekvivalence, která je současně relací uspořádání, na množině všech přímek v rovině?

**Řešení.** Relace ekvivalence (příp. relace uspořádání) musí být reflexivní, a proto každá přímka musí být v relaci sama se sebou. Dále požadujeme, aby hledaná relace byla symetrická (ekvivalence) a zároveň antisymetrická (uspořádání). To dává, že přímka může být v relaci pouze sama se sebou. Zavedeme-li ovšem relaci tak, že dvě přímky jsou v relaci právě tehdy, když jsou totožné, dostaneme

„velmi přirozenou“ relaci ekvivalence i relaci uspořádání. Stačí si uvědomit, že je triviálně tranzitivní. Hledanou relací je právě identické zobrazení množiny všech přímek v rovině. □

**1.170.** Určete, zda je relace

$$R = \{(k, l) \in \mathbb{Z} \times \mathbb{Z};\ |k| \geq |l|\}$$

na množině $\mathbb{Z}$ ekvivalence, uspořádání.

**Řešení.** Relace $R$ není ekvivalencí: není symetrická (kupř. $(6, 2) \in R, (2, 6) \notin R$); není uspořádáním: není antisymetrická (mj. $(2, -2) \in R, (-2, 2) \in R$). □

**1.171.** Ukažte, že průnik libovolných relací ekvivalence na libovolně dané množině $X$ je rovněž relace ekvivalence a že sjednocení dvou relací uspořádání na $X$ nemusí být relace uspořádání.

**Řešení.** Postupně uvidíme, že průnik relací ekvivalence je reflexivní, symetrický a tranzitivní. Všechny relace ekvivalence na $X$ musí obsahovat dvojici $(x, x)$ pro každé $x \in X$, a proto ji musí obsahovat také daný průnik. Pokud v průniku ekvivalencí je prvek $(x, y)$, musí v něm být rovněž prvek $(y, x)$ (stačí využít toho, že každá ekvivalence je symetrická). To, že do průniku ekvivalencí náleží prvky $(x, y)$ a $(y, z)$, znamená, že se jedná o prvky každé z ekvivalencí. Z tranzitivnosti všech jednotlivých ekvivalencí již vyplývá, že do průniku náleží také prvek $(x, z)$.

Zvolíme-li $X = \{1, 2\}$ a relace uspořádání

$$R_1 = \{(1, 1), (2, 2), (1, 2)\}, \quad R_2 = \{(1, 1), (2, 2), (2, 1)\}$$

na $X$, dostáváme relaci

$$R_1 \cup R_2 = \{(1, 1), (2, 2), (1, 2), (2, 1)\},$$

která zřejmě není antisymetrická, a tedy ani uspořádáním. □

**1.172.** Na množině $M = \{1, 2, \ldots, 19, 20\}$ je zavedena relace ekvivalence $\sim$ tak, že $a \sim b$ pro libovolná $a, b \in M$ právě tehdy, když první cifry čísel $a, b$ jsou stejné. Sestrojte rozklad daný touto ekvivalencí.

**Řešení.** Dvě čísla z množiny $M$ jsou ve stejné třídě ekvivalence, právě když jsou spolu v relaci (první cifra je stejná). Rozklad jí určený se tedy skládá z množin

$$\{1, 10, 11, \ldots, 18, 19\}, \{2, 20\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}, \{8\}, \{9\}.$$ □

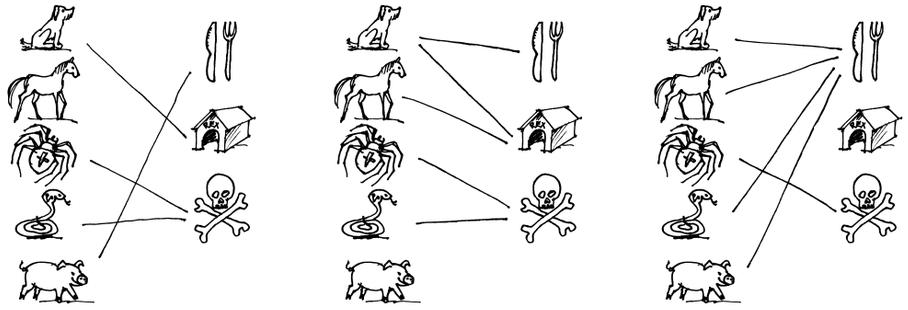
**1.173.** Je dán rozklad se dvěma třídami $\{b, c\}, \{a, d, e\}$ množiny $X = \{a, b, c, d, e\}$. Napište relaci ekvivalence $R$ na množině $X$ příslušnou tomuto rozkladu.

**Řešení.** Ekvivalence $R$ je určena tím, že v relaci jsou spolu ty prvky, které jsou ve stejné třídě rozkladu, a to v obou pořadích ($R$ musí být symetrická) a každý sám se sebou ($R$ musí být reflexivní). Proto $R$ obsahuje právě

$$(a, a), (b, b), (c, c), (d, d), (e, e),$$

$$(b, c), (c, b), (a, d), (a, e), (d, a), (d, e), (e, a), (e, d).$$

□



**1.174.** Na předchozích třech obrázcích jsou ikony spojeny čarami tak, jak by je možná přiřadili lidé v různých částech světa. Určete, zda jde o zobrazení, zda je injektivní, surjektivní nebo bijektivní.

**Řešení.** V prvním případě jde o zobrazení, které je surjektivní, ale není injektivní, protože had i pavouk jsou označeni jako jedovatí. Druhý případ není zobrazení ale jen relace, protože pes je určen jako domácí zvíře i na jídlo. V třetím případě máme opět zobrazení. Tentokrát není ani injektivní, ani surjektivní. □

**1.175.** Mějme množinu $\{a, b, c, d\}$ a na ní relaci

$$\{(a, a), (b, b), (a, b), (b, c), (c, b)\}.$$

Jaké členy je potřeba minimálně doplnit do této relace, aby to byla ekvivalence?

**Řešení.** Postupně projdeme všechny tři vlastnosti, které definují ekvivalenci. Za prvé je to reflexivita. Musíme tedy doplnit dvojice $\{(c, c), (d, d)\}$. Za druhé symetrie –musíme doplnit $(b, a)$ a za třetí musíme udělat tzv. tranzitivní obal. Protože je $a$ v relaci s $b$ a $b$ v relaci s $c$, musí být i $a$ v relaci s $c$. Nakonec tedy potřebujeme přidat $(a, c)$ a $(c, a)$. □

**1.176.** Uvažme množinu čísel, které mají pět cifer ve dvojkovém zápisu a relaci takovou, že dvě čísla jsou v relaci, právě když jejich ciferný součet má stejnou paritu. Napište příslušné třídy ekvivalence.

**Řešení.** Dostáváme dvě třídy ekvivalence (o osmi členech):

$[10000] = \{10000, 10011, 10101, 10110, 11001, 11010, 11100, 11111\}$

odpovídá množině $\{16, 19, 21, 22, 25, 26, 28, 31\}$ a

$[10001] = \{10001, 10010, 10100, 11000, 10111, 11011, 11101, 11110\}$

odpovídá množině $\{17, 18, 20, 24, 23, 27, 29, 30\}$. □

**1.177.** Uvažme množinu čísel, které mají tři cifry ve trojkové soustavě a relaci takovou, že dvě čísla jsou v relaci, právě když v této soustavě

i) začínají stejným dvojčíslím.
ii) končí stejným dvojčíslím.

Napište příslušné třídy ekvivalence.

**Řešení.**

i) Dostáváme šest tříprvkových tříd

$[100] = \{100, 101, 102\}$ odpovídá $\{9, 10, 11\}$,

$[110] = \{110, 111, 112\}$ odpovídá $\{12, 13, 14\}$,

$[120] = \{120, 121, 122\}$ odpovídá $\{15, 16, 17\}$,

$[200] = \{200, 201, 202\}$ odpovídá $\{18, 19, 20\}$,

$[210] = \{210, 211, 212\}$ odpovídá $\{21, 22, 23\}$,

$[220] = \{220, 221, 222\}$ odpovídá $\{24, 25, 26\}$.

ii) V tomto případě máme devět dvouprvkových tříd

$[100] = \{100, 200\}$ odpovídá $\{9, 18\}$,

$[101] = \{101, 201\}$ odpovídá $\{10, 19\}$,

$[102] = \{102, 202\}$ odpovídá $\{11, 20\}$,

$[110] = \{110, 210\}$ odpovídá $\{12, 21\}$,

$[111] = \{111, 211\}$ odpovídá $\{13, 22\}$,

$[112] = \{112, 212\}$ odpovídá $\{14, 23\}$,

$[120] = \{120, 220\}$ odpovídá $\{15, 24\}$,

$[121] = \{121, 221\}$ odpovídá $\{16, 25\}$,

$[122] = \{122, 222\}$ odpovídá $\{17, 26\}$.

□

**1.178.** Pro jaký maximální definiční obor $D$ a obor hodnot $H$ je zobrazení bijektivní a jaká je v tom případě inverzní funkce?

i) $x \mapsto x^4$,

ii) $x \mapsto x^3$,

iii) $x \mapsto \frac{1}{x+1}$.

**Řešení.**

i) $D = [0, \infty)$ a $H = [0, \infty)$ nebo také $D = (-\infty, 0]$ a $H = [0, \infty)$. Inverzní funkce je $x \mapsto \sqrt[4]{x}$.

ii) $D = H = \mathbb{R}$ a inverze je $x \mapsto \sqrt[3]{x}$.

iii) $D = \mathbb{R} \setminus \{-1\}$ a $H = \mathbb{R} \setminus \{0\}$. Inverzní funkce je $x \mapsto \frac{1}{x} - 1$.

□

**1.179.** Uvažme relaci na $\mathbb{R} \times \mathbb{R}$. Bod je v relaci, pokud pro něj platí

$$(x - 1)^2 + (y + 1)^2 = 1.$$

Můžeme body popsat pomocí funkce $y = f(x)$? Nakreslete obrázek bodů v relaci.

**Řešení.** Nemůžeme, protože např. $y = -1$ má dva vzory: $x = 0$ a $x = 2$. Body leží na kružnici se středem v bodě $(1, -1)$ s poloměrem 1. □

**1.180.** Nechť pro libovolná celá čísla $k, l$ platí $(k, l) \in R$ právě tehdy, když je číslo $4k - 4l$ celočíselným násobkem 7. Je takto zavedená relace $R$ ekvivalence, uspořádání?

**Řešení.** Uvědomme si, že dvě celá čísla jsou spolu v relaci $R$, právě když dávají stejný zbytek po dělení 7. Jde tedy o příklad tzv. zbytkové třídy celých čísel. Proto víme, že relace $R$ je relací ekvivalence. Její symetrie (např. $(3, 10), (10, 3) \in R, 3 \neq 10$) pak implikuje, že se nejedná o uspořádání. □

**1.181.** Nechť je na množině $N = \{3, 4, 5, \ldots, n, n + 1, \ldots\}$ definována relace $R$ tak, že dvě čísla jsou v relaci, právě když jsou nesoudělná (tedy neobsahuje-li prvočíselný rozklad uvažovaných dvou čísel ani jedno stejné prvočíslo). Zjistěte, zda je tato relace reflexivní, symetrická, antisymetrická, tranzitivní.

**Řešení.** Pro dvojici stejných čísel platí, že $(n, n) \notin R$. Nejedná se tedy o reflexivní relaci. Být „soudělný“ nebo „nesoudělný“ pro dvojici čísel z $N$ je zřejmě vlastnost neuspořádané dvojice – nezávisí na uvedeném pořadí uvažovaných čísel, a proto je relace $R$ symetrická. Ze symetrie relace $R$ plyne, že není antisymetrická (např. $(3, 5) \in R, 3 \neq 5$). Neboť je $R$ symetrická a $(n, n) \notin R$ pro libovolné číslo $n \in N$, volba dvou různých čísel, která jsou spolu v této relaci, dává, že $R$ není tranzitivní. □

**1.182.** Kolik existuje reflexivních relací na $n$-prvkové množině?

**Řešení.** Relace na množině $M$ je reflexivní, právě když je diagonální relace $\Delta_M = \{(a, a), \text{ kde } a \in M\}$ její podmnožinou. U zbylých $n^2 - n$ uspořádaných dvojic v kartézském součinu $M \times M$ máme nezávislou volbu, jestli daná dvojice v dané relaci bude či ne. Celkem tedy máme $2^{n^2-n}$ různých reflexivních relací na $n$-prvkové množině. □

**1.183.** Kolik existuje symetrických relací na $n$-prvkové množině?

**Řešení.** Relace na množině $M$ je symetrická, právě když je její průnik s každou množinou $\{(a, b), (b, a), \text{ kde } a \neq b, a, b \in M\}$ buď celá daná dvouprvková množina, nebo je tento průnik prázdný. Dvouprvkových podmnožin množiny $M$ je $\binom{n}{2}$, a pokud kromě průniků s těmito množinami ještě určíme průnik dané relace s diagonální relací $\Delta_M = \{(a, a), \text{ kde } a \in M\}$, je tímto daná relace jednoznačně určena. Celkem můžeme provést $\binom{n}{2} + n$ nezávislých voleb mezi dvěma alternativami: každá množina typu $\{(a, b), (b, a), \text{ kde } a \neq b, a, b \in M\}$ je buď podmnožinou dané relace, nebo ani jeden z jejích prvků v dané relaci neleží a každá dvojice $(a, a), a \in M$, potom také buď v relaci leží nebo ne. Celkem tedy máme $2^{\binom{n}{2}+n}$ symetrických relací na $n$-prvkové množině. □

**1.184.** Kolik existuje antisymetrických relací na $n$-prvkové množině?

**Řešení.** Relace na množině $M$ je antisymetrická, právě když její průnik s každou množinou $\{(a, b), (b, a), \text{ kde } a \neq b, a, b \in M\}$ není dvojprvkový (jsou tedy tři možnosti, jak průnik vypadá, buď je to množina $\{(a, b)\}$, nebo $\{(b, a)\}$, nebo je průnik prázdný). Průnik s diagonální relací pak může být libovolný. Určením těchto všech průniků je relace jednoznačně určena. Celkem máme $3^{\binom{n}{2}}2^n$ antisymetrických relací na $n$-prvkové množině. □

## Řešení cvičení

*1.29.* $y_n = 2(\frac{3}{2})^n - 2$.

*1.82.*

i) $(3,3), (4,4), (5,5), (6,6), (7,7), (3,6)$ ověřte, že jde o relaci uspořádání.

ii) opět $(i,i)$ pro $i = 1, \ldots, 7$ a k tomu $(3,6), (6,3)$ ověřte, že jde o relaci ekvivalence.

iii) $(i,i)$ pro $i = 1, \ldots, 7$ a k tomu $(3,6), (6,3), (4,6), (6,4)$ ověřte, že nejde o relaci ekvivalence, protože není splněna tranzitivita.

*1.98.*

a) $1 - 3 - 2i + 4i = -2 + 2i$, $1 \cdot (-3) - 8i^2 + 6i + 4i = 5 + 10i$, $1 + 2i$, $\sqrt{4^2 + (-3)^2} = 5$, $\frac{z_1}{z_2} = \frac{z_1 \bar{z}_2}{|z_2|^2} = 1 \cdot (-3) + 8i^2 + 6i - 4i25 = -\frac{11}{25} + \frac{2}{25}i$.

b) $2 + i$, $2i$ 2, 1, $\frac{2}{i} = -2i$.

*1.107.* Písmen v abecedě (včetně CH) je 27. Počet všech možných iniciálů je tedy $27^2 = 729$. Proto aspoň 2 lidé budou mít stejné iniciály.

*1.112.* $(3 \cdot 46 + 2 \cdot 2) \cdot 2 \cdot 47!$

*1.119.*

i) $2^6 = 64$.

ii) $\binom{6}{4} = 15$.

iii) Žádná panna je jedna možnost $\binom{6}{0} = 1$, jedna panna $\binom{6}{1} = 6$ možností. Posloupností s nejvýše jednou pannou je teda jen 7 a proto posloupností, kde jsou aspoň dvě panny je $64 - 7 = 57$.

*1.128.* Maximální počet $y_n$ částí, na které rozdělí $n$ kružnic rovinu, je $y_n = y_{n-1} + 2(n-1)$, $y_1 = 2$, tedy $y_n = n^2 - n + 2$.

Pro maximální počet $p_n$ částí, na které potom rozdělí $n$ koulí prostor, pak dostáváme rekurentní vztah $p_{n+1} = p_n + y_n$, $p_1 = 2$, tedy celkem $p_n = \frac{n}{3}(n^2 - 3n + 8)$.

*1.153.* Směry stran jsou $(3\sqrt{3}/2 - 2, 3/2 + 2\sqrt{3})$ a $(3\sqrt{3}/2 + 2, 2\sqrt{3} - \frac{3}{2})$. Jedna ze dvou možných dvojic potom je $A = [\frac{3\sqrt{3}}{10} + \frac{7}{5}, \frac{2\sqrt{3}}{5} + \frac{7}{10}]$. $B = [\frac{3\sqrt{3}}{10} + \frac{3}{5}, \frac{13}{10} + \frac{2\sqrt{3}}{5}]$,

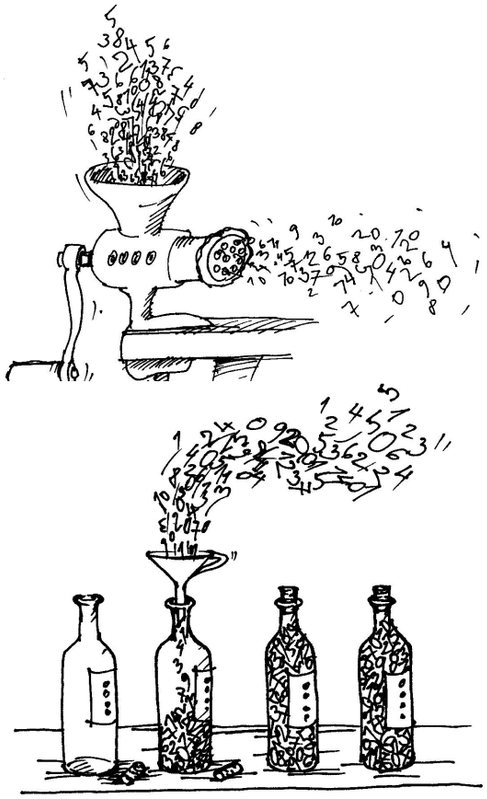
*1.162.* 19.

*1.163.* 87.

KAPITOLA 2

# Počítání s vektory

*neumíte ještě počítat se skaláry?*
*– zkusme to rovnou s maticemi...*



## A. Soustavy lineárních rovnic

Na vektorové prostory půjdeme od lesa. Začneme s něčím známým, totiž soustavami lineárních rovnic. I za nimi jsou totiž skryty vektorové prostory.

**2.1. A teď vám to pěkně natřeme.** Firma zabývající se velkoplošnými nátěry si objednala 810 litrů barvy, která má obsahovat stejné množství červené, zelené a modré barvy (tj. 810 litrů černé

V minulé kapitole jsme se snad rozehřáli s relativně jednoduchými úlohami, k jejichž řešení nebylo potřeba složitých nástrojů. Vystačili jsme si přitom se sčítáním a násobením skalárů. V této a dalších kapitolách se postupně budeme věnovat jednotlivým tématům souvisleji.

Hned tři kapitoly budou věnovány nástrojům pro práci s daty, kdy operace spočívají v obzvlášť jednoduchých úkonech se skaláry, jen je těch skalárů povíce naráz. Hovoříme o „lineárních objektech“ a „lineární algebře“. Jakkoliv to teď může vypadat jako hodně speciální nástroj, uvidíme později, že složitější objekty a závislosti stejně studujeme hlavně pomocí jejich „lineárních přiblížení“.

V této kapitole budeme pracovat přímo s konečnými posloupnostmi skalárů. Takové se objevují v praktických úlohách všude, kde máme objekty popisovány pomocí několika parametrů. Nedělejme si přitom problémy s představou, jak vypadá prostor s více než třemi „souřadnicemi“. Smiřme se se skutečností, že malovat si budeme umět jednu, dvě nebo tři dimenze, ale představovat ty obrázky mohou jakýkoliv jiný počet. A když budeme sledovat jakýkoliv parametr u třeba 500 studentů (např. jejich studijní výsledky), budou naše data mít hned zrovna několikrát 500 položek a budeme s nimi chtít pracovat. Naším cílem bude vytvořit nástroje, které budou dobře fungovat nezávisle na skutečném počtu těchto položek.



Také se neděsme slovních spojení jako pole či okruh skalárů $\mathbb{K}$. Prostě si můžeme představit jakýkoliv konkrétní číselný obor. Okruhy skalárů pak zahrnují i celá čísla $\mathbb{Z}$ a všechny zbytkové třídy, zatímco mezi poli jsou pouze $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ a zbytkové třídy $\mathbb{Z}_k$ s prvočíselným $k$. Zvláštní je mezi nimi $\mathbb{Z}_2$, kde ze vztahu $x = -x$ nemůžeme usoudit, že $x = 0$, zatímco u všech ostatních číselných oborů tomu tak je.



### 1. Vektory a matice

Většinou se o vektorech hovoří pouze ve spojení s poli skalárů, protože obecná teorie je při existenci neinvertibilních nenulových skalárů nesrovnatelně složitější. Jen v prvních dvou částech této kapitoly budeme pracovat s vektory a maticemi v kontextu konečných posloupností skalárů a tam bude zajímavé si i třeba případu celých čísel povšimnout. Bude přitom snad pěkně vidět, jak silné výsledky lze důsledným formálním uvažováním odvodit.

**2.1. Vektory nad skaláry.** Prozatím budeme *vektorem* rozumět uspořádanou $n$-tici skalárů z $\mathbb{K}$, kde pevně zvolené $n \in \mathbb{N}$ budeme nazývat *dimenzí*.

barvy). Obchod může splnit tuto zakázku smícháním běžně prodávaných barev (má skladem jejich dostatečné zásoby), a to

- načervenalé barvy – obsahuje 50 % červené, 25 % zelené a 25 % modré barvy;
- nazelenalé barvy – obsahuje 12,5 % červené, 75 % zelené a 12,5 % modré barvy;
- namodralé barvy – obsahuje 20 % červené, 20 % zelené a 60 % modré barvy.

Kolik litrů od každé z uskladněných barev se musí smíchat, aby byly splněny požadavky zákazníka?

**Řešení.** Označme jako

- $x$ – množství (v litrech) načervenalé barvy, které se použije;
- $y$ – množství (v litrech) nazelenalé barvy, které se použije;
- $z$ – množství (v litrech) namodralé barvy, které se použije.

Smícháním barev chceme získat barvu, která bude obsahovat 270 litrů červené barvy. Uvědomme si, že načervenalá barva obsahuje 50 % červené, nazelenalá obsahuje 12,5 % červené a namodralá 20 % červené barvy. Musí tudíž platit

$$0{,}5x + 0{,}125y + 0{,}2z = 270.$$

Analogicky požadujeme (pro zelenou a modrou barvu)

$$0{,}25x + 0{,}75y + 0{,}2z = 270,$$
$$0{,}25x + 0{,}125y + 0{,}6z = 270.$$

Nyní můžeme postupovat dvěma způsoby. Buď budeme postupně vyjadřovat proměnné pomocí ostatních (z první rovnice je $x = 540 - 0{,}25y - 0{,}4z$, dosadíme za $x$ do druhé a třetí rovnice a dostaneme dvě lineární rovnice o dvou neznámých $2{,}75y + 0{,}4z = 540$ a $0{,}25y + 2z = 540$. Ze druhé rovnice vyjádříme $z = 270 - 0{,}125y$ a dosazením do první dostáváme $2{,}7y = 432$, neboli $y = 160$, odkud $z = 270 - 0{,}125 \cdot 160 = 250$ a $x = 540 - 0{,}25 \cdot 160 + 0{,}4 \cdot 250 = 400$.

Druhým způsobem je zapsat si soustavu do matice, jejíž první řádek bude tvořen koeficienty u neznámých v první rovnici, druhý koeficienty ve druhé rovnici a třetí ve třetí. Je tedy *matice soustavy*

$$\begin{pmatrix} 0{,}5 & 0{,}125 & 0{,}2 \\ 0{,}25 & 0{,}75 & 0{,}2 \\ 0{,}25 & 0{,}125 & 0{,}6 \end{pmatrix},$$

*rozšířenou matici soustavy* potom získáme z matice soustavy připsáním sloupce pravých stran jednotlivých rovnic v systému:

$$\left(\begin{array}{ccc|c} 0{,}5 & 0{,}125 & 0{,}2 & 270 \\ 0{,}25 & 0{,}75 & 0{,}2 & 270 \\ 0{,}25 & 0{,}125 & 0{,}6 & 270 \end{array}\right).$$

Skaláry umíme sčítat a násobit. Vektory budeme také sčítat, násobit však vektor budeme umět jen skalárem. To odpovídá představě, kterou jsme již viděli v rovině $\mathbb{R}^2$, kde sčítání odpovídalo skládání vektorů coby šipek vycházejících z počátku a násobení skalárem pak jejich patřičnému natahování.



Násobení vektoru $u = (a_1, \dots, a_n)$ skalárem $c$ tedy definujeme tak, že každý prvek $n$-tice $u$ vynásobíme stejným skalárem $c$ a také sčítání vektorů definujeme po složkách. To znamená

ZÁKLADNÍ OPERACE S VEKTORY

$$\begin{aligned} u + v &= (a_1, \dots, a_n) + (b_1, \dots, b_n) = \\ &= (a_1 + b_1, \dots, a_n + b_n), \\ c \cdot u &= c \cdot (a_1, \dots, a_n) = (c \cdot a_1, \dots, c \cdot a_n). \end{aligned}$$

Pro sčítání vektorů a násobení vektorů skaláry budeme používat stále stejné symboly jako u skalárů samotných, tj. symboly plus a buď tečku nebo prosté zřetězení znaků.

**Konvence zápisu vektorů.** Nebudeme, na rozdíl od mnoha jiných učebnic, v textu používat pro vektory žádné speciální značení a ponecháváme na čtenáři, aby udržoval svoji pozornost přemýšlením o kontextu. Pro skaláry ale spíše budeme používat písmena ze začátku abecedy a pro vektory od konce (prostředek nám zůstane na indexy proměnných či komponent a také pro sčítací indexy v součtech).



Často budeme požadovat, aby skaláry byly z nějakého pole, viz 1.1, ale zatím budeme vesměs pracovat s operacemi, které tento předpoklad nepotřebují. V literatuře se pak většinou místo o vektorových prostorech hovoří o *modulech nad okruhy*. U obecné teorie se ale v příští kapitole již zcela omezíme na pole skalárů.

Pro sčítání vektorů v $\mathbb{K}^n$ zjevně platí (KG1)–(KG4) s nulovým prvkem

$$0 = (0, \dots, 0) \in \mathbb{K}^n.$$

Schválně zde používáme i pro nulový prvek stejný symbol jako pro nulový prvek skalárů.

VLASTNOSTI VEKTORŮ

Pro všechny vektory $v, w \in \mathbb{K}^n$ a skaláry $a, b \in \mathbb{K}$ platí

$$\text{(V1)} \qquad a \cdot (v + w) = a \cdot v + a \cdot w,$$
$$\text{(V2)} \qquad (a + b) \cdot v = a \cdot v + b \cdot v,$$
$$\text{(V3)} \qquad a \cdot (b \cdot v) = (a \cdot b) \cdot v,$$
$$\text{(V4)} \qquad 1 \cdot v = v.$$

Vlastnosti (V1)–(V4) našich vektorů, coby $n$–tic skalárů v $\mathbb{K}^n$, se snadno ověří pro kterýkoliv okruh skalárů $\mathbb{K}$, protože při ověřování vždy používáme pro jednotlivé souřadnice vektorů pouze vlastnosti skalárů uvedené v 1.1 a 1.3.

Budeme takto pracovat např. s $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$, ale také s $\mathbb{Z}^n$, $(\mathbb{Z}_k)^n$, $n = 1, 2, 3, \dots$.

**2.2. Matice nad skaláry.** O něco složitějším objektem, který budeme při práci s vektory používat, jsou matice.

Jejím postupným upravováním pomocí tzv. elementárních řádkových úprav (odpovídají ekvivalentním úpravám rovnic, více viz 2.7) pak dostáváme:

$$\left(\begin{array}{ccc|c} 0{,}5 & 0{,}125 & 0{,}2 & 270 \\ 0{,}25 & 0{,}75 & 0{,}2 & 270 \\ 0{,}25 & 0{,}125 & 0{,}6 & 270 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0{,}25 & 0{,}4 & 540 \\ 1 & 3 & 0{,}8 & 1\,080 \\ 1 & 0{,}5 & 2{,}4 & 1\,080 \end{array}\right) \sim$$
$$\sim \left(\begin{array}{ccc|c} 1 & 0{,}25 & 0{,}4 & 540 \\ 0 & 2{,}75 & 0{,}4 & 540 \\ 0 & 0{,}25 & 2 & 540 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0{,}25 & 0{,}4 & 540 \\ 0 & 11 & 1{,}6 & 2\,160 \\ 0 & 1 & 8 & 2\,160 \end{array}\right) \sim$$
$$\sim \left(\begin{array}{ccc|c} 1 & 0{,}25 & 0{,}4 & 540 \\ 0 & 1 & 8 & 2\,160 \\ 0 & 11 & 1{,}6 & 2\,160 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0{,}25 & 0{,}4 & 540 \\ 0 & 1 & 8 & 2\,160 \\ 0 & 0 & -86{,}4 & -21\,600 \end{array}\right).$$

A opět zpětně vypočítáme

$$z = \frac{-21\,600}{-86{,}4} = 250,$$
$$y = 2\,160 - 8 \cdot 250 = 160,$$
$$x = 540 - 0{,}4 \cdot 250 - 0{,}25 \cdot 160 = 400.$$

Je tedy potřeba smísit po řadě 400 l, 160 l, 250 l uvedených barev. □

**2.2.** Vypočtěte

$$\begin{array}{rcrcrcr} x_1 & + & 2x_2 & + & 3x_3 & = & 2, \\ 2x_1 & - & 3x_2 & - & x_3 & = & -3, \\ -3x_1 & + & x_2 & + & 2x_3 & = & -3. \end{array}$$

**Řešení.** Zadanou soustavu lineárních rovnic zapíšeme ve tvaru rozšířené matice

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 2 \\ 2 & -3 & -1 & -3 \\ -3 & 1 & 2 & -3 \end{array}\right),$$

kterou pomocí elementárních řádkových transformací postupně převedeme na schodovitý tvar

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 2 \\ 2 & -3 & -1 & -3 \\ -3 & 1 & 2 & -3 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 2 \\ 0 & -7 & -7 & -7 \\ 0 & 7 & 11 & 3 \end{array}\right) \sim$$
$$\sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 4 & -4 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{array}\right).$$

Nejdříve jsme přitom dvojnásobek prvního řádku odečetli od druhého a jeho trojnásobek přičetli ke třetímu. Poté jsme sečetli druhý a třetí řádek (součet napsali do třetího řádku) a druhý řádek vynásobili číslem $1/7$. Přejdeme nyní zpět k soustavě rovnic

$$\begin{array}{rcrcrcr} x_1 & + & 2x_2 & + & 3x_3 & = & 2, \\ & & x_2 & + & x_3 & = & 1, \\ & & & & x_3 & = & -1. \end{array}$$

### Matice typu $m/n$

Maticí typu $m/n$ nad skaláry $\mathbb{K}$ rozumíme obdélníkové schéma $A$ s $m$ řádky a $n$ sloupci

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

kde $a_{ij} \in \mathbb{K}$ pro všechna $1 \le i \le m$, $1 \le j \le n$. Pro matici $A$ s prvky $a_{ij}$ používáme také zápis $A = (a_{ij})$.

Vektory $(a_{i1}, a_{i2}, \dots, a_{in}) \in \mathbb{K}^n$ nazýváme ($i$–té) *řádky matice* $A$, $i = 1, \dots, m$, vektory $(a_{1j}, a_{2j}, \dots, a_{mj}) \in \mathbb{K}^m$ nazýváme ($j$–té) *sloupce matice* $A$, $j = 1, \dots, n$.

Matici můžeme také chápat jako zobrazení

$$A : \{1, \dots, m\} \times \{1, \dots, n\} \to \mathbb{K},$$

kde $A(i, j) = a_{ij}$. Matice typu $1/n$ nebo $n/1$ jsou vlastně právě vektory v $\mathbb{K}^n$.

I obecné matice lze chápat jako vektory v $\mathbb{K}^{m \cdot n}$, prostě zapomeneme na řádkování. Zejména tedy je definováno sčítání matic a násobení matic skaláry:



$$A + B = (a_{ij} + b_{ij}), \quad a \cdot A = (a \cdot a_{ij}),$$

kde $A = (a_{ij})$, $B = (b_{ij})$, $a \in \mathbb{K}$.

Matice $-A = (-a_{ij})$ se nazývá *matice opačná* k matici $A$ a matice

$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

se nazývá *nulová matice*. Zapomenutím řádkování tak získáme následující tvrzení, že matice jsou jen specificky zapsané vektory:

**Tvrzení.** *Předpisy pro $A + B$, $a \cdot A$, $-A$, $0$ zadávají na množině všech matic typu $m/n$ operace sčítání a násobení skaláry splňující axiomy (V1)–(V4).*

**2.3. Matice a rovnice.** Velmi častý nástroj pro popis nějakých matematických modelů jsou systémy lineárních rovnic. Právě matice lze vhodně využít pro jejich zápis. Zavedeme si k tomu účelu pojem *skalární součin* dvou vektorů, který vektorům $(a_1, \dots, a_n)$ a $(x_1, \dots, x_n)$ přiřadí jejich součin

$$(a_1, \dots, a_n) \cdot (x_1, \dots, x_n) = a_1x_1 + \dots + a_nx_n,$$

tj. postupně násobíme po dvou souřadnice vektorů a výsledky sčítáme.

Každý systém $m$ lineárních rovnic v $n$ proměnných

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

lze tedy vidět jako požadavek na hodnoty $m$ skalárních součinů neznámého vektoru $(x_1, \dots, x_n)$ s vektory souřadnic $(a_{i1}, \dots, a_{in})$.

Ihned vidíme, že $x_3 = -1$. Dosadíme-li $x_3 = -1$ do rovnice $x_2 + x_3 = 1$, dostaneme $x_2 = 2$. Podobně dosazení získaných hodnot $x_3 = -1, x_2 = 2$ do první rovnice dává $x_1 = 1$. □

Systémy lineárních rovnic tedy lze zapisovat v maticovém tvaru. Ale je to nějaká výhoda, když je stejně umíme řešit, aniž bychom hovořili o maticích? Ano je, o řešení můžeme hovořit koncepčněji, snadno v řeči matic určíme, kolik má soustava řešení a jazyk matic pak daleko lépe navádí k počítačovému zpracování problému. Zkusme si tedy osvojit lépe různé operace, které můžeme s maticemi provádět. Jak jsme viděli v předchozích příkladech, tak ekvivalentní úpravy lineárních rovnic odpovídají v řeči matic elementárním řádkovým (sloupcovým) úpravám. Dále jsme viděli, že převedeme-li těmito úpravami matici soustavy do schodovitého tvaru (tomuto procesu říkáme Gaussova eliminace, viz 2.7), tak je již vyřešení soustavy velmi jednoduché. Ukažme si to ještě na dalších příkladech, na kterých uvidíme, že soustava lineárních rovnic může mít nekonečně mnoho řešení.

**2.3.** Vyřešte soustavu lineárních rovnic

$$\begin{aligned} 2x_1 &- x_2 + 3x_3 = 0,\\ 3x_1 &+ 16x_2 + 7x_3 = 0,\\ 3x_1 &- 5x_2 + 4x_3 = 0,\\ -7x_1 &+ 7x_2 - 10x_3 = 0. \end{aligned}$$

**Řešení.** Vzhledem k nulovosti pravých stran všech rovnic (jedná se tedy o homogenní systém) budeme upravovat pouze matici systému. Řešení nalezneme převodem na schodovitý tvar pomocí elementárních řádkových transformací, které odpovídají záměně pořadí rovnic, vynásobení rovnice nenulovým číslem a přičítání násobků rovnic. Navíc můžeme kdykoli od maticového zápisu přejít zpět k zápisu rovnic s neznámými $x_i$. Postupně dostáváme:

$$\begin{pmatrix} 2 & -1 & 3 \\ 3 & 16 & 7 \\ 3 & -5 & 4 \\ -7 & 7 & -10 \end{pmatrix} \sim \begin{pmatrix} 2 & -1 & 3 \\ 0 & 35/2 & 5/2 \\ 0 & -7/2 & -1/2 \\ 0 & 7/2 & 1/2 \end{pmatrix}.$$

Odtud je vidět, že druhá, třetí a čtvrtá rovnice jsou násobky rovnice $7x_2 + x_3 = 0$. Pokračujme však v úpravách matice:

$$\begin{pmatrix} 2 & -1 & 3 \\ 0 & 35/2 & 5/2 \\ 0 & -7/2 & -1/2 \\ 0 & 7/2 & 1/2 \end{pmatrix} \sim \begin{pmatrix} 2 & -1 & 3 \\ 0 & 35/2 & 5/2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & -1 & 3 \\ 0 & 7 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Přestože byly zadány čtyři rovnice pro tři neznámé, má celá soustava nekonečně mnoho řešení, neboť pro libovolné $x_3 \in \mathbb{R}$ mají zbylé rovnice

$$\begin{aligned} 2x_1 &- x_2 + 3x_3 = 0,\\ &7x_2 + x_3 = 0 \end{aligned}$$



Vektor proměnných můžeme také vidět jako sloupec v matici typu $n/1$, a podobně hodnoty $b_1, \dots, b_n$ můžeme vnímat jako vektor $u$ a to opět jako jediný sloupec v matici typu $n/1$. Náš systém rovnic lze pak formálně psát ve tvaru $A \cdot x = u$ takto:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

kde levou stranu interpretujeme jako $m$ skalárních součinů jednotlivých řádků matice vytvářejících sloupcový vektor, jehož hodnotu rovnice určují. To znamená, že skutečně rovnost $i$-tých souřadnic zadává podmínku původní rovnice

$$a_{i1}x_1 + \dots + a_{in}x_n = b_i$$

a zápis $A \cdot x = u$ tak dává skutečně původní systém lineárních rovnic.

**2.4. Součin matic.** V rovině, tj. pro vektory dimenze 2, jsme už zavedli počet s maticemi a viděli jsme, že s ním lze pracovat velice efektivně (viz 1.26). Nyní budeme postupovat obecněji a zavedeme všechny nástroje již známé z roviny pro všechny dimenze $n$.



Násobení matic je možné definovat pouze, když to rozměry sloupců a řádků v maticích dovolí, tj. když je pro ně definován skalární součin jako výše:

SOUČIN MATIC

Pro libovolnou matici $A = (a_{ij})$ typu $m/n$ a libovolnou matici $B = (b_{jk})$ typu $n/q$ nad okruhem skalárů $\mathbb{K}$ definujeme jejich součin $C = A \cdot B = (c_{ik})$ jako matici typu $m/q$ s prvky

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}, \text{ pro libovolná } 1 \le i \le m,\ 1 \le k \le q.$$

Prvek $c_{ik}$ součinu je tedy právě skalárním součinem $i$-tého řádku matice nalevo a $k$-tého sloupce matice napravo. Například máme

$$\begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 3 \\ 3 & 1 & 0 \end{pmatrix}.$$

**2.5. Čtvercové matice.** Je-li v matici stejný počet řádků a sloupců, hovoříme o *čtvercové matici*. Počet řádků a sloupců pak nazýváme také *dimenzí matice*. Matici

$$E = (\delta_{ij}) = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}$$

se říká *jednotková matice*. Takto definovaným číslům $\delta_{ij}$ se říkává *Kroneckerovo delta*. Na množině čtvercových matic nad $\mathbb{K}$ dimenze $n$ je součin matic definován pro každé dvě matice, je tam tedy definována operace násobení, jejíž vlastnosti jsou velice podobné jako u skalárů:

**Tvrzení.** *Na množině všech čtvercových matic dimenze n nad libovolným okruhem skalárů $\mathbb{K}$ je definována operace násobení s následujícími vlastnostmi okruhů (viz 1.3):*

*(1) Platí asociativita násobení (O1).*

*(2) Jednotková matice $E = (\delta_{ij})$ je jednotkovým prvkem pro násobení dle (O3).*

řešení. Nahradíme tak proměnnou $x_3$ parametrem $t \in \mathbb{R}$ a vyjádříme

$$x_2 = -\frac{1}{7}x_3 = -\frac{1}{7}t \quad \text{a} \quad x_1 = \frac{1}{2}(x_2 - 3x_3) = -\frac{11}{7}t.$$

Pokud ještě nahradíme $t = -7s$, obdržíme výsledek v jednoduchém tvaru

$$(x_1,\, x_2,\, x_3) = (11s,\, s,\, -7s)\,,\ s \in \mathbb{R}. \qquad \square$$

**2.4.** Nalezněte všechna řešení soustavy lineárních rovnic

$$\begin{array}{rcrcrcrcr} 3x_1 & & & + & 3x_3 & - & 5x_4 & = & -8, \\ x_1 & - & x_2 & + & x_3 & - & x_4 & = & -2, \\ -2x_1 & - & x_2 & + & 4x_3 & - & 2x_4 & = & 0, \\ 2x_1 & + & x_2 & - & x_3 & - & x_4 & = & -3. \end{array}$$

**Řešení.** Soustavě rovnic odpovídá rozšířená matice

$$\left(\begin{array}{cccc|c} 3 & 0 & 3 & -5 & -8 \\ 1 & -1 & 1 & -1 & -2 \\ -2 & -1 & 4 & -2 & 0 \\ 2 & 1 & -1 & -1 & -3 \end{array}\right).$$

Záměnou pořadí řádků (rovnic) potom obdržíme matici

$$\left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 2 & 1 & -1 & -1 & -3 \\ -2 & -1 & 4 & -2 & 0 \\ 3 & 0 & 3 & -5 & -8 \end{array}\right),$$

kterou převedeme na schodovitý tvar:

$$\left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 2 & 1 & -1 & -1 & -3 \\ -2 & -1 & 4 & -2 & 0 \\ 3 & 0 & 3 & -5 & -8 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 0 & 3 & -3 & 1 & 1 \\ 0 & -3 & 6 & -4 & -4 \\ 0 & 3 & 0 & -2 & -2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 0 & 3 & -3 & 1 & 1 \\ 0 & 0 & 3 & -3 & -3 \\ 0 & 0 & 3 & -3 & -3 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 0 & 3 & -3 & 1 & 1 \\ 0 & 0 & 3 & -3 & -3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Soustava bude mít nekonečně mnoho řešení, neboť dostáváme tři rovnice pro čtyři neznámé, které mají právě jedno řešení pro každou volbu proměnné $x_4 \in \mathbb{R}$. Neznámou $x_4$ proto nahradíme parametrem $t \in \mathbb{R}$ a od maticového zápisu přejdeme zpět k rovnicím

$$\begin{array}{rcrcrcrcr} x_1 & - & x_2 & + & x_3 & - & t & = & -2, \\ & & 3x_2 & - & 3x_3 & + & t & = & 1, \\ & & & & 3x_3 & - & 3t & = & -3. \end{array}$$

Z poslední rovnice máme $x_3 = t - 1$. Dosazení za $x_3$ do druhé rovnice potom dává

$$3x_2 - 3t + 3 + t = 1,\ \text{tj.}\ x_2 = \frac{1}{3}(2t - 2)\,.$$

Konečně podle první rovnice je

$$x_1 - \frac{1}{3}(2t - 2) + t - 1 - t = -2,\ \text{tj.}\ x_1 = \frac{1}{3}(2t - 5)\,.$$

*(3) Platí distributivita sčítání a násobení (O4).*

*Obecně však neplatí axiomy (O2) ani (OI). Čtvercové matice pro $n > 1$ proto netvoří obor integrity, zejména tedy nejsou ani (nekomutativním) tělesem.*

Důkaz. Asociativita násobení – (O1): Protože skaláry jsou asociativní, distributivní i komutativní, můžeme pro tři matice $A = (a_{ij})$ typu $m/n$, $B = (b_{jk})$ typu $n/p$ a $C = (c_{kl})$ typu $p/q$ spočíst

$$A \cdot B = \left(\sum_j a_{ij} \cdot b_{jk}\right), \qquad B \cdot C = \left(\sum_k b_{jk} \cdot c_{kl}\right),$$

$$(A \cdot B) \cdot C = \left(\sum_k \left(\sum_j a_{ij} \cdot b_{jk}\right) \cdot c_{kl}\right) = \left(\sum_{j,k} a_{ij} \cdot b_{jk} \cdot c_{kl}\right),$$

$$A \cdot (B \cdot C) = \left(\sum_j a_{ij} \cdot \left(\sum_k b_{jk} \cdot c_{kl}\right)\right) = \left(\sum_{j,k} a_{ij} \cdot b_{jk} \cdot c_{kl}\right).$$

Všimněme si, že jsme při výpočtu vycházeli z toho, že je jedno v jakém pořadí uvedené součty a součiny provádíme, tj. využívali jsme podstatně našich vlastností skalárů.

Velmi snadno vidíme, že násobení jednotkovou maticí má skutečně vlastnost jednotkového prvku:

$$A \cdot E = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = A$$

a stejně pro násobení $E$ zleva.

Zbývá ukázat distributivitu násobení a sčítání. Opět díky distributivitě skalárů snadno spočteme pro matice $A = (a_{ij})$ typu $m/n$, $B = (b_{jk})$ typu $n/p$, $C = (c_{jk})$ typu $n/p$, $D = (d_{kl})$ typu $p/q$

$$\begin{aligned} A \cdot (B + C) &= \left(\sum_j a_{ij}(b_{jk} + c_{jk})\right) = \\ &= \left(\left(\sum_j a_{ij} b_{jk}\right) + \left(\sum_j a_{ij} c_{jk}\right)\right) = \\ &= A \cdot B + A \cdot C, \\ (B + C) \cdot D &= \left(\sum_k (b_{jk} + c_{jk}) d_{kl}\right) = \\ &= \left(\left(\sum_k b_{jk} d_{kl}\right) + \left(\sum_k c_{jk} d_{kl}\right)\right) = \\ &= B \cdot D + C \cdot D. \end{aligned}$$

Jak jsme již viděli v 1.26, dvě matice dimenze 2 nemusí komutovat:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Tím jsme získali zároveň protipříklad na platnost (O2) i (OI). Pro matice typu 1/1 ovšem oba axiomy samozřejmě platí, protože je mají samy skaláry. Pro větší matice získáme protipříklady snadno tak, že právě uvedené matice umístíme do levého horního rohu příslušných čtvercových schémat a doplníme nulami. (Ověřte si sami!) $\square$

Množinu řešení můžeme tudíž zapsat (pro $t = 3s$) ve tvaru

$$\left\{(x_1,\, x_2,\, x_3,\, x_4) = \left(2s - \frac{5}{3},\, 2s - \frac{2}{3},\, 3s - 1,\, 3s\right),\ s \in \mathbb{R}\right\}.$$

Nyní se vraťme k rozšířené matici naší soustavy a upravujme ji dále užitím řádkových transformací tak, aby (při schodovitém tvaru) první nenulové číslo každého řádku (tzv. *pivot*) bylo právě číslo 1 a aby všechna ostatní čísla v jeho sloupci byla 0. Platí

$$\left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 0 & 3 & -3 & 1 & 1 \\ 0 & 0 & 3 & -3 & -3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 0 & 1 & -1 & 1/3 & 1/3 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 1 & -1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -2/3 & -2/3 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & -2/3 & -5/3 \\ 0 & 1 & 0 & -2/3 & -2/3 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right),$$

přičemž nejdříve jsme vynásobili druhý a třetí řádek číslem $1/3$, pak přičetli třetí řádek ke druhému a jeho $(-1)$násobek k prvnímu a na závěr přičetli druhý řádek k prvnímu. Z poslední matice snadno dostáváme výsledek

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} -5/3 \\ -2/3 \\ -1 \\ 0 \end{pmatrix} + t \begin{pmatrix} 2/3 \\ 2/3 \\ 1 \\ 1 \end{pmatrix},\ t \in \mathbb{R}.$$

Volné proměnné jsou totiž ty, jejichž sloupce neobsahují žádného pivota (v našem případě neobsahuje pivota čtvrtý sloupec, je tedy volná čtvrtá proměnná, tj. používáme ji jako parametr). □

**2.5.** Určete řešení systému rovnic

$$\begin{array}{rcrcrcrcr} 3x_1 & & & + & 3x_3 & - & 5x_4 & = & 8, \\ x_1 & - & x_2 & + & x_3 & - & x_4 & = & -2, \\ -2x_1 & - & x_2 & + & 4x_3 & - & 2x_4 & = & 0, \\ 2x_1 & + & x_2 & - & x_3 & - & x_4 & = & -3. \end{array}$$

**Řešení.** Uvědomme si, že soustava rovnic v tomto příkladu se od soustavy z předešlého příkladu liší pouze v hodnotě 8 (místo $-8$) na pravé straně první rovnice. Provedeme-li totožné řádkové úpravy jako v minulém příkladu, obdržíme

$$\left(\begin{array}{cccc|c} 3 & 0 & 3 & -5 & 8 \\ 1 & -1 & 1 & -1 & -2 \\ -2 & -1 & 4 & -2 & 0 \\ 2 & 1 & -1 & -1 & -3 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 2 & 1 & -1 & -1 & -3 \\ -2 & -1 & 4 & -2 & 0 \\ 3 & 0 & 3 & -5 & 8 \end{array}\right) \cdots$$

$$\cdots \left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 0 & 3 & -3 & 1 & 1 \\ 0 & 0 & 3 & -3 & -3 \\ 0 & 0 & 3 & -3 & 13 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & -2 \\ 0 & 3 & -3 & 1 & 1 \\ 0 & 0 & 3 & -3 & -3 \\ 0 & 0 & 0 & 0 & 16 \end{array}\right),$$

V důkazu jsme vlastně pracovali s maticemi obecnějšího typu, dokázali jsme tedy příslušné vlastnosti obecněji:

ASOCIATIVITA A DISTRIBUTIVITA NÁSOBENÍ MATIC

**Důsledek.** *Násobení matic je asociativní a distributivní, tj.*

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C,$$
$$A \cdot (B + C) = A \cdot B + A \cdot C,$$

*kdykoliv jsou všechny uvedené operace definovány. Jednotková matice je neutrálním prvkem pro násobení zleva i zprava.*

**2.6. Inverzní matice.** Se skaláry umíme počítat tak, že z rovnosti $a \cdot x = b$ umíme vyjádřit $x = a^{-1} \cdot b$, kdykoliv inverze k $a$ existuje. Podobně bychom to chtěli umět i s maticemi, máme ale problém, jak poznat, zda taková matice existuje, a jak ji spočítat.



Říkáme, že $B$ je *matice inverzní* k matici $A$, když

$$A \cdot B = B \cdot A = E.$$

Píšeme pak $B = A^{-1}$ a z definice je zřejmé, že obě matice musí mít být čtvercové se stejnou dimenzí $n$. Matici, k níž existuje matice inverzní, říkáme *invertibilní matice* nebo také *regulární čtvercová matice*.

V následujících odstavcích mimo jiné odvodíme, že $B$ je inverzní k $A$, jakmile platí jedna z požadovaných identit (tj. druhá je pak důsledkem).

Pokud $A^{-1}$ a $B^{-1}$ existují, pak existuje i inverze k součinu $A \cdot B$

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}. \tag{2.1}$$

Je totiž, díky právě dokázané asociativitě násobení,

$$(B^{-1} \cdot A^{-1}) \cdot (A \cdot B) = B^{-1} \cdot (A^{-1} \cdot A) \cdot B = E$$
$$(A \cdot B) \cdot (B^{-1} \cdot A^{-1}) = A \cdot (B \cdot B^{-1}) \cdot A^{-1} = E.$$



Protože s maticemi umíme počítat podobně jako se skaláry, jen mají složitější chování, může nám existence inverzní matice skutečně hodně pomoci s řešením systémů lineárních rovnic: Jestliže vyjádříme soustavu $n$ rovnic pro $n$ neznámých součinem matic

$$A \cdot x = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = u$$

a jestliže existuje matice inverzní k matici $A$, pak lze násobit zleva $A^{-1}$ a dostaneme

$$A^{-1} \cdot u = A^{-1} \cdot A \cdot x = E \cdot x = x,$$

tj. $A^{-1} \cdot u$ je hledané řešení.

Naopak rozepsáním podmínky $A \cdot A^{-1} = E$ pro neznámé skaláry v hledané matici $A^{-1}$ dostaneme $n$ systémů lineárních rovnic se stejnou maticí na levé straně a různými vektory napravo.

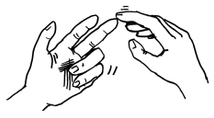
kde poslední úpravou bylo odečtení třetího řádku od čtvrtého. Ze čtvrté rovnice $0 = 16$ vyplývá, že soustava nemá řešení. Vyzdvihněme, že při úpravě na schodovitý tvar obdržíme rovnici $0 = a$ pro nějaké $a \neq 0$ (tj. nulový řádek na levé straně a nenulové číslo za svislou čarou) právě tehdy, když soustava nemá řešení. □

Další příklady na systémy lineárních rovnic naleznete na straně 109

### B. Manipulace s maticemi

V této podkapitole budeme pracovat pouze s maticemi, abychom si osvojili jejich vlastnosti.

**2.6. Násobení matic.** Proveďte násobení matic a zkontrolujte si výsledek. Všimněte si, že proto, abychom mohli dvě matice násobit, je nutná a postačující podmínka, aby měla první matice stejně sloupců jako druhá řádků. Počet řádků výsledné matice je pak dán počtem řádků první matice, počet sloupců je roven počtu sloupců druhé matice.



i) $\begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix}$,

ii) $\begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 1 & 7 \end{pmatrix}$,

iii) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 2 & 1 \\ 1 & 1 & -2 & -3 \\ 3 & 2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 12 & 7 & 1 & -5 \\ 3 & 0 & 5 & 4 \end{pmatrix}$,

iv) $\begin{pmatrix} 1 & 3 & 1 \\ -2 & 2 & -1 \\ 3 & 1 & -4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \\ -3 \end{pmatrix} = \begin{pmatrix} 7 \\ 7 \\ 18 \end{pmatrix}$,

v) $\begin{pmatrix} 1 & 3 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 & 3 \\ 3 & 2 & 1 \\ 1 & -1 & -4 \end{pmatrix} = \begin{pmatrix} 7 & 7 & 18 \end{pmatrix}$,

vi) $\begin{pmatrix} 1 & 2 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} -2 \end{pmatrix}$.

**Poznámka.** Body i) a ii) v předchozím příkladu ukazují, že násobení čtvercových matic není komutativní, v bodě iii) vidíme, že dané obdélníkové matice můžeme mezi sebou násobit pouze v jednom ze dvou možných pořadí. V bodech iv) a v) si pak všimněme, že $(A \cdot B)^T = B^T \cdot A^T$.

*2.7.* Vypočítejte $A^5$ a $A^{-3}$, je-li

$$A = \begin{pmatrix} 2 & -1 & 1 \\ -1 & 2 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

○

**2.7. Ekvivalentní úpravy matic.** Zkusme se praktičtěji zorientovat v předchozí úvaze o systémech rovnic a jejich maticích. Samozřejmě nás nalezení inverzní matice stojí jisté úsilí – větší než přímé vyřešení rovnice. Podstatné však je, že pokud máme mnohokrát za sebou řešit systémy se stejnou maticí $A$ ale různými pravými stranami $u$, pak se nám nalezení $A^{-1}$ opravdu hodně vyplatí.

Z hlediska řešení systémů rovnic $A \cdot x = u$ je jistě přirozené považovat za ekvivalentní matice $A$ a vektory $u$, které zadávají systémy rovnic se stejným řešením. Zkusme se teď zamyslet nad možnostmi, jak zjednodušovat matici $A$ tak, abychom se k řešení blížili.



Začneme jednoduchými manipulacemi s řádky rovnic, které řešení ovlivňovat nebudou, a stejným způsobem pak můžeme upravovat i vektor napravo. Když se nám u čtvercové matice podaří vlevo dostat systém s jednotkovou maticí, bude napravo řešení původního systému. Pokud při našem postupu nějaké řádky úplně vypadnou (při úpravách se vynulují), bude to také dávat další přímé informace o řešení. Naše jednoduché úpravy jsou:

ELEMENTÁRNÍ ŘÁDKOVÉ TRANSFORMACE

- záměna dvou řádků,
- vynásobení vybraného řádku nenulovým skalárem,
- přičtení řádku k jinému řádku.

Těmto operacím říkáme *elementární řádkové transformace*. Je zjevné, že odpovídající operace na úrovni rovnic v systému skutečně nemohou změnit množinu všech jeho řešení, pokud je náš okruh oborem integrity.

Analogicky, *elementární sloupcové transformace* matic jsou

- záměna dvou sloupců,
- vynásobení vybraného sloupce nenulovým skalárem,
- přičtení sloupce k jinému sloupci,

ty však nezachovávají řešení příslušných rovnic, protože mezi sebou míchají samotné proměnné.

Systematicky můžeme použít elementární řádkové úpravy k postupné eliminaci proměnných. Postup je algoritmický a většinou se mu říká *Gaussova eliminace* proměnných.



GAUSSOVA ELIMINACE PROMĚNNÝCH

**Tvrzení.** *Nenulovou matici nad libovolným okruhem skalárů $\mathbb{K}$ lze konečně mnoha elementárními řádkovými transformacemi převést na tzv. (řádkově) schodovitý tvar:*

- *Je-li $a_{ik} = 0$ pro všechna $k = 1, \ldots, j$, potom $a_{kj} = 0$ pro všechna $k \geq i$.*
- *Je-li $a_{(i-1)j}$ první nenulový prvek na $(i-1)$-ním řádku, pak $a_{ij} = 0$.*

DŮKAZ. Matice v řádkově schodovitém tvaru vypadá takto

$$\begin{pmatrix} 0 & \ldots & 0 & a_{1j} & \ldots & \ldots & \ldots & a_{1m} \\ 0 & \ldots & 0 & 0 & \ldots & a_{2k} & \ldots & a_{2m} \\ \vdots & & & & & & & \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 & a_{lp} & \ldots \\ \vdots & & & & & & & \end{pmatrix}$$

**2.8.** Nechť je

$$A = \begin{pmatrix} 4 & 0 & -5 \\ 2 & 7 & 15 \\ 2 & 7 & 13 \end{pmatrix}, \quad B = \begin{pmatrix} 7 & 2 & 0 \\ 0 & 0 & 3 \\ 0 & -19 & \sqrt{13} \end{pmatrix}.$$

Lze matici $A$ převést na matici $B$ pomocí elementárních řádkových transformací (pak říkáme, že jsou řádkově ekvivalentní)?

**Řešení.** Obě matice jsou zřejmě řádkově ekvivalentní s trojrozměrnou jednotkovou maticí. Snadno se vidí, že řádková ekvivalence na množině všech matic daných rozměrů je relací ekvivalence. Matice $A$ a $B$ jsou tudíž řádkově ekvivalentní. □

**2.9.** Nalezněte nějakou matici $B$, pro kterou je matice $C = B \cdot A$ ve schodovitém tvaru, kde

$$A = \begin{pmatrix} 3 & -1 & 3 & 2 \\ 5 & -3 & 2 & 3 \\ 1 & -3 & -5 & 0 \\ 7 & -5 & 1 & 4 \end{pmatrix}.$$

**Řešení.** Budeme-li matici $A$ postupně násobit zleva elementárními maticemi (uvažte, jakým řádkovým úpravám toto násobení matic odpovídá)

$$E_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -5 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$E_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -3 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad E_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -7 & 0 & 0 & 1 \end{pmatrix},$$

$$E_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad E_6 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$E_7 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -4 & 0 & 1 \end{pmatrix}, \quad E_8 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

obdržíme

$$B = E_8E_7E_6E_5E_4E_3E_2E_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1/12 & -5/12 & 0 \\ 1 & -2/3 & 1/3 & 0 \\ 0 & -4/3 & -1/3 & 1 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & -3 & -5 & 0 \\ 0 & 1 & 9/4 & 1/4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

□

a může, ale nemusí, končit několika nulovými řádky. K převodu libovolné matice můžeme použít jednoduchý algoritmus, kterým se postupně, řádek za řádkem, blížíme k výslednému schodovitému tvaru:

ALGORITMUS GAUSSOVY ELIMINACE

(1) Případnou záměnou řádků docílíme, že v prvním řádku bude v prvním nenulovém sloupci nenulový prvek, nechť je to $j$-tý sloupec.
(2) Pro $i = 2, \ldots$ vynásobením prvního řádku prvkem $a_{ij}$, $i$-tého řádku prvkem $a_{1j}$ a odečtením vynulujeme prvek $a_{ij}$ na $i$-tém řádku.
(3) Opakovanou aplikací bodů (1) a (2), vždy pro dosud neupravený zbytek řádků a sloupců v získané matici, dospějeme po konečném počtu kroků k požadovanému tvaru.

Tím je tvrzení dokázáno. □

Uvedený postup je skutečně právě obvyklá eliminace proměnných v systémech lineárních rovnic.

Zcela analogickým postupem definujeme sloupcově schodovitý tvar matic a záměnou řádkových na sloupcové transformace obdržíme algoritmus převádějící matici na takový tvar.

**Poznámka.** Gaussovu eliminaci jsme zformulovali pro obecné skaláry z nějakého okruhu. Zdá se být přirozené, že ve schodovitém tvaru ještě vynásobením vhodnými skaláry dosáhneme jednotkových koeficientů na výsledné nenulové „diagonále“ nad nulami v matici a dopočítáme řešení. To ale pro obecné skaláry nepůjde, představte si třeba celá čísla $\mathbb{Z}$.

Pro řešení systémů rovnic nemá ale vůbec uvedený postup rozumný smysl, když jsou mezi skaláry dělitelé nuly. Promyslete si pečlivě rozdíl mezi $\mathbb{K} = \mathbb{Z}$, $\mathbb{K} = \mathbb{R}$ a případně $\mathbb{Z}_2$ nebo $\mathbb{Z}_4$.

**2.8. Matice elementárních transformací.** Nyní už budeme pracovat s polem skalárů $\mathbb{K}$, každý nenulový skalár tedy má inverzní prvek.

Všimněme si, že elementární řádkové (resp. sloupcové) transformace odpovídají vynásobením zleva (resp. zprava) následujícími maticemi:

(1) Přehození $i$-tého a $j$-tého řádku (resp. sloupce)

$$\begin{pmatrix} 1 & 0 & \ldots & & & & \\ 0 & \ddots & & & & & \\ \vdots & & 0 & \ldots & 1 & & \\ & & \vdots & \ddots & \vdots & & \\ & & 1 & \ldots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow i \\ \\ \leftarrow j \\ \\ \\ \end{matrix}$$

(2) Vynásobení $i$-tého řádku (resp. sloupce) skalárem $a$:

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \end{matrix}$$

**2.10. Komplexní čísla jako matice.** Uvažme množinu matic $C = \left\{ \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right); a, b \in \mathbb{R} \right\}$. Všimněte si, že $C$ je uzavřená na sčítání a násobení matic a dále ukažte, že přiřazení $f : C \to \mathbb{C}$, $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi$ splňuje $f(M + N) = f(M) + f(N)$ i $f(M \cdot N) = f(M) \cdot f(N)$ (na levých stranách rovností se jedná o sčítání a násobení matic, na pravých o sčítání a násobení komplexních čísel). Na množinu $C$ spolu s násobením a sčítáním matic lze tedy nahlížet jako na těleso $\mathbb{C}$ komplexních čísel. Zobrazení $f$ se pak nazývá izomorfismem (těles). Je tedy například

$$\begin{pmatrix} 3 & 5 \\ -5 & 3 \end{pmatrix} \cdot \begin{pmatrix} 8 & -9 \\ 9 & 8 \end{pmatrix} = \begin{pmatrix} 69 & 13 \\ -13 & 69 \end{pmatrix},$$

což odpovídá tomu, že $(3 + 5i) \cdot (8 - 9i) = 69 - 13i$.

**2.11.** Vyřešte maticové rovnice

$$\begin{pmatrix} 1 & 3 \\ 3 & 8 \end{pmatrix} \cdot X_1 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad X_2 \cdot \begin{pmatrix} 1 & 3 \\ 3 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

**Řešení.** Zjevně neznámé $X_1$ a $X_2$ musejí být matice $2 \times 2$ (aby uvažované součiny matic existovaly a výsledkem byla matice $2 \times 2$). Položme

$$X_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \quad X_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

a roznásobme matice v první zadané rovnici. Má platit

$$\begin{pmatrix} a_1 + 3c_1 & b_1 + 3d_1 \\ 3a_1 + 8c_1 & 3b_1 + 8d_1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix},$$

tj. má být

$$\begin{aligned} a_1 \quad &+ \quad 3c_1 \quad &&= \quad 1, \\ b_1 \quad &+ \quad 3d_1 \quad &&= \quad 2, \\ 3a_1 \quad &+ \quad 8c_1 \quad &&= \quad 3, \\ 3b_1 \quad &+ \quad 8d_1 \quad &&= \quad 4. \end{aligned}$$

Sečtením $(-3)$násobku první rovnice se třetí dostáváme $c_1 = 0$ a následně $a_1 = 1$. Podobně sečtením $(-3)$násobku druhé rovnice se čtvrtou dostáváme $d_1 = 2$ a poté $b_1 = -4$. Je tedy

$$X_1 = \begin{pmatrix} 1 & -4 \\ 0 & 2 \end{pmatrix}.$$

Hodnoty $a_2, b_2, c_2, d_2$ najdeme odlišným způsobem. Využijeme vztah

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

který platí pro libovolná čísla $a, b, c, d \in \mathbb{R}$ (lze snadno odvodit; plyne také přímo z 2.2), spočtěme

$$\begin{pmatrix} 1 & 3 \\ 3 & 8 \end{pmatrix}^{-1} = \begin{pmatrix} -8 & 3 \\ 3 & -1 \end{pmatrix}.$$

(3) Sečtení $i$-tého řádku (resp. sloupce) s $j$-tým:

$$\begin{array}{c} \\ i \to \\ \\ \\

Vynásobení zadané rovnice touto maticí zprava dává

$$X_2 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} -8 & 3 \\ 3 & -1 \end{pmatrix},$$

a tudíž

$$X_2 = \begin{pmatrix} -2 & 1 \\ -12 & 5 \end{pmatrix}. \qquad \square$$

*2.12.* Řešte maticovou rovnici

$$X \cdot \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & -6 \\ 2 & 1 \end{pmatrix}. \qquad \bigcirc$$

**2.13. Výpočet inverzní matice.** Spočtěte inverzní matice k maticím

$$A = \begin{pmatrix} 4 & 3 & 2 \\ 5 & 6 & 3 \\ 3 & 5 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 1 \\ 3 & 3 & 4 \\ 2 & 2 & 3 \end{pmatrix}.$$

Poté určete matici $\left(A^T \cdot B\right)^{-1}$.

**Řešení.** Inverzní matici nalezneme tak, že vedle sebe napíšeme matici $A$ a matici jednotkovou. Pomocí řádkových transformací pak převedeme matici $A$ na jednotkovou. Tímto matice jednotková přejde na matici $A^{-1}$. Postupnými úpravami dostáváme

$$\left(\begin{array}{ccc|ccc} 4 & 3 & 2 & 1 & 0 & 0 \\ 5 & 6 & 3 & 0 & 1 & 0 \\ 3 & 5 & 2 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & -2 & 0 & 1 & 0 & -1 \\ 5 & 6 & 3 & 0 & 1 & 0 \\ 3 & 5 & 2 & 0 & 0 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & -2 & 0 & 1 & 0 & -1 \\ 0 & 16 & 3 & -5 & 1 & 5 \\ 0 & 11 & 2 & -3 & 0 & 4 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & -2 & 0 & 1 & 0 & -1 \\ 0 & 5 & 1 & -2 & 1 & 1 \\ 0 & 11 & 2 & -3 & 0 & 4 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & -2 & 0 & 1 & 0 & -1 \\ 0 & 5 & 1 & -2 & 1 & 1 \\ 0 & 1 & 0 & 1 & -2 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & -4 & 3 \\ 0 & 0 & 1 & -7 & 11 & -9 \\ 0 & 1 & 0 & 1 & -2 & 2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & -4 & 3 \\ 0 & 1 & 0 & 1 & -2 & 2 \\ 0 & 0 & 1 & -7 & 11 & -9 \end{array}\right),$$

přičemž v prvním kroku jsme odečetli od prvního řádku třetí, ve druhém jsme $(-5)$násobek prvního přičetli ke druhému a současně jeho $(-3)$násobek ke třetímu, ve třetím kroku jsme odečetli od druhého řádku třetí, ve čtvrtém jsme $(-2)$násobek druhého přičetli ke třetímu, v pátém kroku jsme $(-5)$násobek třetího řádku přičetli ke druhému a jeho 2násobek k prvnímu, v posledním kroku jsme pak zaměnili druhý a třetí řádek. Zdůrazněme výsledek

$$A^{-1} = \begin{pmatrix} 3 & -4 & 3 \\ 1 & -2 & 2 \\ -7 & 11 & -9 \end{pmatrix}.$$

Upozorněme, že při určování matice $A^{-1}$ jsme díky vhodným řádkovým úpravám nemuseli počítat se zlomky. Přestože bychom si mohli obdobně počínat při určování matice $B^{-1}$, budeme raději provádět více názorné (nabízející se) řádkové úpravy. Platí ve výsledku (řádkové) Gaussovy eliminace tedy vylučuje existenci $A^{-1}$.

Předpokládejme nyní, že $A^{-1}$ existuje. Podle předchozího nalezneme řádkově schodovitý tvar bez nulového řádku, tzn. že všechny diagonální prvky v $P' \cdot A$ jsou nenulové. Pak ovšem pokračováním eliminace pomocí řádkových elementárních transformací od pravého dolního rohu zpět a vynormováním diagonálních prvků na jedničky získáme jednotkovou matici $E$. Jinými slovy, najdeme další invertibilní matici $P''$ takovou, že pro $P = P'' \cdot P'$ platí $P \cdot A = E$. Výměnou řádkových a sloupcových transformací lze za předpokladu existence $A^{-1}$ stejným postupem najít $Q$ takovou, že $A \cdot Q = E$. Odtud

$$P = P \cdot E = P \cdot (A \cdot Q) = (P \cdot A) \cdot Q = Q.$$

To ale znamená, že jsme nalezli hledanou inverzní matici

$$A^{-1} = P = Q$$

k matici $A$. Zejména se tedy v okamžiku nalezení matice $P$ s vlastností $P \cdot A = E$ už nemusíme s žádnými dalšími výpočty namáhat, protože víme, že již jistě jde o inverzní matici.

Prakticky tedy můžeme postupovat takto:

VÝPOČET INVERZNÍ MATICE

Vedle sebe napíšeme původní matici $A$ a jednotkovou matici $E$, matici $A$ upravujeme řádkovými elementárními úpravami nejprve na schodovitý tvar, potom tzv. zpětnou eliminací na diagonální matici a v té násobíme řádky inverzními prvky z $\mathbb{K}$. Týmiž úpravy postupně prováděné s $E$ vedou právě k hledané matici $A^{-1}$. Pokud tento algoritmus narazí na vynulování celého řádku v původní matici, znamená to, že matice inverzní neexistuje.

**2.11. Lineární závislost a hodnost.** V předchozích úvahách a počtech s maticemi jsme stále pracovali se sčítáním řádků nebo sloupců coby vektorů, spolu s jejich násobením skaláry. Takové operaci říkáme *lineární kombinace*. V abstraktním pojetí se k operacím s vektory vrátíme za chvíli v 2.24, bude ale užitečné pochopit podstatu už nyní. Lineární kombinací řádků (nebo sloupců) matice $A = (a_{ij})$ typu $m/n$ rozumíme výraz



$$c_1 u_{i_1} + \cdots + c_k u_{i_k},$$

kde $c_i$ jsou skaláry, $u_j = (a_{j1}, \ldots, a_{jn})$ jsou řádky (nebo $u_j = (a_{1j}, \ldots, a_{mj})$ jsou sloupce) matice $A$.

Jestliže existuje lineární kombinace daných řádků s alespoň jedním nenulovým skalárním koeficientem, jejímž výsledkem je nulový řádek, říkáme, že jsou tyto řádky *lineárně závislé*. V opačném případě, tj. když jedinou možností jak získat nulový řádek je vynásobení výhradně nulovými skaláry, jsou tyto řádky *lineárně nezávislé*.

Obdobně definujeme lineárně závislé a nezávislé sloupce matice.



Předchozí výsledky o Gaussově eliminaci můžeme teď interpretovat tak, že počet výsledných nenulových „schodů“ v řádkově nebo sloupcově schodovitém tvaru je vždy roven počtu lineárně nezávislých řádků matice, resp. počtu lineárně nezávislých sloupců matice. Označme $E_h$ matici z věty 2.9 s $h$ jedničkami na diagonále a předpokládejme, že dvěma různými postupy dostaneme různá $h' < h$. Pak ovšem podle

$$\left(\begin{array}{ccc|ccc} 1&0&1&1&0&0\\ 3&3&4&0&1&0\\ 2&2&3&0&0&1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1&0&1&1&0&0\\ 0&3&1&-3&1&0\\ 0&2&1&-2&0&1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1&0&1&1&0&0\\ 0&3&1&-3&1&0\\ 0&0&1/3&0&-2/3&1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1&0&1&1&0&0\\ 0&1&\frac{1}{3}&-1&\frac{1}{3}&0\\ 0&0&\frac{1}{3}&0&-\frac{2}{3}&1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1&0&0&1&2&-3\\ 0&1&0&-1&1&-1\\ 0&0&\frac{1}{3}&0&-\frac{2}{3}&1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1&0&0&1&2&-3\\ 0&1&0&-1&1&-1\\ 0&0&1&0&-2&3 \end{array}\right),$$

tj.

$$B^{-1} = \begin{pmatrix} 1&2&-3\\ -1&1&-1\\ 0&-2&3 \end{pmatrix}.$$

Využitím identity

$$\left(A^T \cdot B\right)^{-1} = B^{-1} \cdot \left(A^T\right)^{-1} = B^{-1} \cdot \left(A^{-1}\right)^T$$

a znalosti výše vypočítaných inverzních matic lze obdržet

$$\left(A^T \cdot B\right)^{-1} = \begin{pmatrix} 1&2&-3\\ -1&1&-1\\ 0&-2&3 \end{pmatrix} \cdot \begin{pmatrix} 3&1&-7\\ -4&-2&11\\ 3&2&-9 \end{pmatrix} =$$

$$= \begin{pmatrix} -14&-9&42\\ -10&-5&27\\ 17&10&-49 \end{pmatrix}.$$

□

*2.14.* Vypočítejte inverzní matici k matici

$$A = \begin{pmatrix} 1&0&-2\\ 2&-2&1\\ 5&-5&2 \end{pmatrix}.$$

○

*2.15.* Nalezněte inverzní matici k matici

$$\begin{pmatrix} 8&3&0&0&0\\ 5&2&0&0&0\\ 0&0&-1&0&0\\ 0&0&0&1&2\\ 0&0&0&3&5 \end{pmatrix}.$$

○

*2.16.* Zjistěte, zda existuje inverzní matice k matici

$$C = \begin{pmatrix} 1&1&1&1\\ 1&1&-1&1\\ 1&-1&1&-1\\ 1&-1&-1&1 \end{pmatrix}.$$

Pokud ano, určete tuto matici $C^{-1}$ . ○

*2.17.* Stanovte $A^{-1}$, je-li

(a) $A = \begin{pmatrix} 1&i\\ -i&3 \end{pmatrix}$, přičemž $i$ je imaginární jednotka;

našeho postupu budou existovat také invertibilní matice $P$ a $Q$ takové, že

$$P \cdot E_{h'} \cdot Q = E_h.$$

V součinu $E_{h'} \cdot Q$ bude více nulových řádků ve spodní části matice, než kolik má být jedniček v $E_h$ a přitom se k nim máme dostat už jen řádkovými transformacemi. Zvýšit počet lineárně nezávislých řádků ale pomocí elementárních řádkových transformací nelze. Proto je počet jedniček v matici $P \cdot A \cdot Q$ ve větě 2.9 nezávislý na volbě našeho postupu eliminace a je roven jak počtu lineárně nezávislých řádků v $A$, tak počtu lineárně nezávislých sloupců v $A$. Tomuto číslu říkáme *hodnost matice* a značíme je $h(A)$. Zapamatujme si výsledné tvrzení:

**Věta.** *Nechť $A$ je matice typu $m/n$ nad polem skalárů $\mathbb{K}$. Matice $A$ má stejný počet $h(A)$ lineárně nezávislých řádků a lineárně nezávislých sloupců. Zejména je hodnost vždy nejvýše rovna menšímu z rozměrů matice $A$.*

Algoritmus pro výpočet inverzních matic také říká, že čtvercová matice $A$ dimenze $m$ má inverzi, právě když je její hodnost rovna počtu řádků $m$.

**2.12. Matice jako zobrazení.** Zcela stejně, jak jsme s maticemi pracovali v geometrii roviny, viz 1.29, můžeme každou čtvercovou matici $A$ interpretovat jako zobrazení

$$A : \mathbb{K}^n \to \mathbb{K}^n, \quad x \mapsto A \cdot x.$$

Díky distributivitě násobení matic je zřejmé, jak jsou zobrazovány lineární kombinace vektorů takovými zobrazeními:

$$A \cdot (a\,x + b\,y) = a\,(A \cdot x) + b\,(A \cdot y).$$

Přímo z definice je také vidět (díky asociativitě násobení matic), že skládání zobrazení odpovídá násobení matic v daném pořadí. Invertibilní matice tedy odpovídají bijektivním zobrazením.



Z tohoto pohledu je velice zajímavá věta 2.9. Můžeme ji číst tak, že hodnost matice určuje, jak velký je obraz celého $\mathbb{K}^n$ v tomto zobrazení. Skutečně, je-li $A = P \cdot E_k \cdot Q$ s maticí $E_k$ s $k$ jedničkami jako v 2.9, pak invertibilní $Q$ napřed jen bijektivně „zamíchá“ $n$–rozměrné vektory v $\mathbb{K}^n$, matice $E_k$ pak „zkopíruje“ prvních $k$ souřadnic a vynuluje $n-k$ zbývajících. Tento „$k$–rozměrný“ obraz už pak následně násobení invertibilní $P$ nemůže zvětšit.

**2.13. Řešení systémů lineárních rovnic.** K pojmům dimenze, lineární nezávislost apod. se vrátíme ve třetí části této kapitoly. Již teď si ale můžeme povšimnout, co právě odvozené výsledky říkají o řešení systému lineárních rovnic. Jestliže budeme uvažovat matici systému rovnic a přidáme k ní ještě sloupec požadovaných hodnot, hovoříme o rozšířené matici systému. Postup, který jsme předvedli, odpovídá postupné eliminaci proměnných v rovnicích a vyškrtání lineárně závislých rovnic (ty jsou prostě důsledkem ostatních).



Dovodili jsme tedy kompletní informaci o velikosti množiny řešení systému lineárních rovnic v závislosti na hodnosti matice systému. Pokud nám při přechodu na řádkově schodovitý tvar zůstane v rozšířené matici více nenulových řádků než v matici systému, pak žádné řešení nemůže existovat (prostě se daným lineárním zobrazením do požadované hodnoty vůbec netrefíme). Pokud je hodnost obou matic stejná, pak nám při zpětném dopočtu řešení zůstane právě tolik volných parametrů, kolik je rozdíl mezi počtem proměnných $n$ a hodností $h(A)$.

(b) $A = \begin{pmatrix} 1 & -5 & -3 \\ -1 & 5 & 4 \\ -1 & 6 & 2 \end{pmatrix}$.

○

*2.18.* Napište inverzní matici k $n \times n$ matici ($n > 1$)

$$A = \begin{pmatrix} 2-n & 1 & \cdots & 1 & 1 \\ 1 & 2-n & \ddots & \ddots & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & \ddots & \ddots & 2-n & 1 \\ 1 & 1 & \cdots & 1 & 2-n \end{pmatrix}.$$

○

## C. Permutace

Abychom mohli definovat stěžejní pojem kalkulu matic, totiž determinant, je nutné se věnovat permutacím (bijekcím na konečné množině), zejména pak jejich paritě.

Pro zápis permutací (tj. bijektivních zobrazení na dané konečné množině) budeme používat tzv. dvouřádkový zápis (viz 2.14). V prvním řádku uvedeme všechny prvky uvažované množiny, libovolný sloupeček je pak tvořen dvojicí vzor, obraz (v dané permutaci). Protože permutace je bijekce, je druhý řádek vskutku permutací (pořadím) řádku prvního, v souladu s názvoslovím používaným v kombinatorice.

**2.19.** Rozložte permutaci

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 6 & 7 & 8 & 9 & 5 & 4 & 2 \end{pmatrix}$$

na součin transpozic.

**Řešení.** Nejprve rozložíme permutaci na součin nezávislých cyklů: začneme s prvním prvkem (jedničkou) a ve druhém řádku odečteme, na jaký prvek se v dané permutaci zobrazuje. Je to trojka. Nyní se podíváme na sloupeček začínající trojkou a odečteme z něj, že se zobrazuje na šestku, atd. Pokračujeme tak dlouho, dokud se nám nějaký prvek nezobrazí na počáteční prvek (v tomto případě jednička). Dostáváme následující posloupnost prvků, které se na sebe v dané permutaci zobrazují:

$$1 \mapsto 3 \mapsto 6 \mapsto 9 \mapsto 2 \mapsto 1.$$

Zobrazení, které zobrazuje prvky výše uvedeným způsobem, je tzv. cyklus (viz 2.16), který zapisujeme $(1, 3, 6, 9, 2)$.

Nyní vezmeme prvek, který není obsažený v získaném cyklu, a opakujeme s ním postup jako s jedničkou. Dostáváme cyklus

### 2. Determinanty



V páté části první kapitoly jsme viděli (viz 1.27), že pro čtvercové matice dimenze 2 nad reálnými čísly existuje skalární funkce det, která matici přiřadí nenulové číslo, právě když existuje její inverze. Neříkali jsme to sice stejnými slovy, ale snadno si to ověříte (viz odstavce počínaje 1.26 a vzorec (1.16)). Determinant byl užitečný i jinak, viz odstavce 1.33 a 1.34, kde jsme si volnou úvahou odvodili, že obsah rovnoběžníku by měl být lineárně závislý na každém ze dvou vektorů definujících rovnoběžník a že je užitečné zároveň požadovat změnu znaménka při změně pořadí těchto vektorů. Protože tyto vlastnosti měl, až na pevný skalární násobek, jedině determinant, odvodili jsme, že je obsah dán právě takto. Nyní uvidíme, že podobně lze postupovat v každé konečné dimenzi.

V této části budeme pracovat s libovolnými skaláry $\mathbb{K}$ a maticemi nad těmito skaláry. Naše výsledky o determinantech tedy budou vesměs platit pro všechny komutativní okruhy, zejména tedy třeba pro celočíselné matice.

**2.14. Definice determinantu.** Připomeňme, že bijektivní zobrazení množiny $X$ na sebe se nazývá *permutace množiny* $X$, viz 1.7. Je-li $X = \{1, 2, \ldots, n\}$, lze permutace zapsat pomocí výsledného pořadí ve formě tabulky:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Prvek $x \in X$ se nazývá samodružným bodem permutace $\sigma$, je-li $\sigma(x) = x$. Permutace $\sigma$ taková, že existují právě dva různé prvky $x, y \in X$ s $\sigma(x) = y$, zatímco všechna ostatní $z \in X$ jsou samodružná, se nazývá *transpozice*, značíme ji $(x, y)$. Samozřejmě pro takovou transpozici platí také $\sigma(y) = x$, odtud název.



V dimenzi 2 byl vzorec pro determinant jednoduchý – vezmeme všechny možné součiny dvou prvků, po jednom z každého sloupce a řádku matice, opatříme je znaménkem tak, aby při přehození dvou sloupců došlo ke změně celkového znaménka, a výrazy všechny (tj. oba) sečteme:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ \det A = ad - bc.$$

Obecně, uvažujme čtvercové matice $A = (a_{ij})$ dimenze $n$ nad $\mathbb{K}$. Vzorec pro determinant matice $A$ bude také poskládaný ze všech možných součinů prvků z jednotlivých řádků a sloupců:

DEFINICE DETERMINANTU

*Determinant matice* $A$ je skalár $\det A = |A|$ definovaný vztahem

$$|A| = \sum_{\sigma \in \Sigma_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdots a_{n\sigma(n)},$$

kde $\Sigma_n$ je množina všech možných permutací na $\{1, \ldots, n\}$ a znaménko sgn pro každou permutaci $\sigma$ ještě musíme popsat. Každý z výrazů

$$\operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

nazýváme *člen determinantu* $|A|$.

V dimenzích 2 a 3 snadno uhádneme i správná znaménka. Součin prvků z diagonály má být s kladným znaménkem a chceme antisymetrii při přehození dvou sloupců nebo řádků.

(4, 7, 5, 8). Z postupu vyplývá, že musí být nezávislý na prvním. Každý prvek z dané množiny ($\{1, 2, \ldots, 9\}$) se již vyskytuje v některém z cyklů, můžeme tedy psát:

$$\sigma = (1, 3, 6, 9, 2) \circ (4, 7, 5, 8).$$

Pro cykly je rozklad na permutace jednoduchý. Je totiž

$$(1, 3, 6, 9, 2) = (1, 3)\circ(3, 6)\circ(6, 9)\circ(9, 2) = (1, 3)(3, 6)(6, 9)(9, 2).$$

Celkem dostáváme:

$$\sigma = (1, 3)(3, 6)(6, 9)(9, 2)(4, 7)(7, 5)(5, 8)\ . \qquad \square$$

**Poznámka.** Upozorněme, že operace $\circ$ je skládání zobrazení, je nutné tedy zobrazení ve složení provádět „odzadu“ tak, jak jsme u skládání zobrazení zvyklí. Aplikaci daného složení transpozic kupříkladu na prvek 2 můžeme postupně zapsat:

$$\begin{aligned}[(1, 3)(3, 6)(6, 9)(9, 2)](2) &= [(1, 3)(3, 6)(6, 9)]((9, 2)(2)) = \\ &= [(1, 3)(3, 6)(6, 9)](9) = \\ &= [(1, 3)(3, 6)](6) = (1, 3)(3) = 1,\end{aligned}$$

tedy vskutku dané zobrazení zobrazuje prvek 2 na prvek 1 (je to totiž pouze jinak zapsaný cyklus (1, 3, 6, 9, 2)). V zápisu skládání permutací však znak „$\circ$“ často vypouštíme a hovoříme o součinu permutací.

Při zápisu cyklu zapisujeme pouze prvky, na kterých cyklus (tj. zobrazení) netriviálně působí (tj. zobrazuje je jinam, než na sebe sama). Pevné body cyklu naopak v jeho notaci neuvádíme. Je tudíž nutné vědět, na které množině daný cyklus uvažujeme (většinou zřejmé z kontextu). Označme cyklus (4, 7, 5, 8) z předchozího příkladu jako $c$, je to tedy zobrazení (permutace), které by ve dvouřádkovém zápisu mělo tvar

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 7 & 8 & 6 & 5 & 4 & 9 \end{pmatrix}.$$

Pokud tedy má již původní permutace nějaké pevné body, tak se v rozkladu na cykly neobjevují.

Dále si všimněme, že zápis (1, 2, 3) zadává stejný cyklus jako (2, 3, 1) či (3, 1, 2). Cyklus (1, 3, 2) je však již jiné zobrazení.

**2.20.** Určete paritu následujících permutací:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 6 & 7 & 8 & 9 & 5 & 4 & 2 \end{pmatrix},\ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix}.$$

**Řešení.** Z předcházejícího příkladu víme, že platí:

$$\sigma = (1, 3)(3, 6)(6, 9)(9, 2)(4, 7)(7, 5)(5, 8).$$

Její parita je dána paritou počtu transpozic v jejím rozkladu (ta je na rozdíl od počtu transpozic v libovolném rozkladu dané permutace stejná). Transpozic je v rozkladu sedm, permutace je tudíž lichá. Bez

### Determinanty v dimenzi 2 a 3

Pro $n = 2$ je, jak jsme čekali,

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Podobně pro $n = 3$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{aligned} &a_{11}a_{22}a_{33} - a_{13}a_{22}a_{31} + a_{13}a_{21}a_{32} - \\ &-a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} - a_{12}a_{21}a_{33}. \end{aligned}$$

Tomuto vzorci se říká *Sarrusovo pravidlo.*

**2.15. Parita permutace.** Jak tedy najít správná znaménka permutací? Říkáme, že dvojice prvků $a, b \in X = \{1, \ldots, n\}$ tvoří *inverzi v permutaci* $\sigma$, je-li $a < b$ a $\sigma(a) > \sigma(b)$. Permutace $\sigma$ se nazývá *sudá* (resp. *lichá*), obsahuje-li sudý (resp. lichý) počet inverzí.



*Parita permutace* $\sigma$ je $(-1)^{\text{počet inverzí}}$ a značíme ji $\operatorname{sgn}(\sigma)$. Tolik tedy definice znamének našich členů determinantu. Chceme ale vědět, jak s paritou počítat. Z následujícího tvrzení o permutacích už je jasně vidět, že Sarrusovo pravidlo skutečně počítá determinant v dimenzi 3.

**Věta.** *Na množině $X = \{1, 2, \ldots, n\}$ je právě $n!$ různých permutací. Ty lze seřadit do posloupnosti tak, že každé dvě po sobě jdoucí se liší právě jednou transpozicí. Lze při tom začít libovolnou permutací. Každá transpozice mění paritu.*

Důkaz. Pro jednoprvkové a dvouprvkové $X$ tvrzení samozřejmě platí. Budeme postupovat indukcí přes dimenzi.

Předpokládejme, že tvrzení platí pro všechny množiny s $n - 1$ prvky a uvažme permutaci $\sigma(1) = a_1, \ldots, \sigma(n) = a_n$. Podle indukčního předpokladu všechny permutace, které mají na posledním místě $a_n$, dostaneme z tohoto pořadí postupným prováděním transpozic. Přitom jich bude $(n - 1)!$. V posledním z nich prohodíme $\sigma(n) = a_n$ za některý z prvků, který dosud nebyl na posledním místě, a znovu uspořádáme všechny permutace s tímto vybraným prvkem na posledním místě do posloupnosti s požadovanými vlastnostmi. Po $n$–násobné aplikaci tohoto postupu získáme $n(n - 1) = n!$ zaručeně různých permutací, tzn. všechny, právě předepsaným způsobem.

Všimněme si, že poslední věta dokazovaného tvrzení se nezdá příliš důležitá pro jeho využití. Je však velice důležitou částí postupu v našem důkazu indukcí přes počet prvků v $X$.

Zbývá tvrzení věty o paritách. Uvažme pořadí

$$(a_1, \ldots, a_i, a_{i+1}, \ldots, a_n),$$

ve kterém je $r$ inverzí. Pak zjevně je v pořadí

$$(a_1, \ldots, a_{i+1}, a_i, \ldots, a_n)$$

buď $r - 1$ nebo $r + 1$ inverzí. Každou transpozici $(a_i, a_j)$ lze přitom získat postupným provedením $(j - i) + (j - i - 1) = 2(j - i) - 1$ transpozic sousedních prvků. Proto se provedením libovolné transpozice parita permutace změní. Navíc již víme, že všechny permutace lze získat prováděním transpozic. $\square$

znalosti rozkladu $\sigma$ na transpozice, bychom mohli spočítat počet dvojic $(a,b) \subseteq \{1,2,\dots,9\} \times \{1,2,\dots,9\}$, které jsou v inverzi vůči $\sigma$ (viz 2.15): procházíme postupně druhý řádek zápisu permutace a pro každé číslo přičteme počet čísel, která jsou menší než ono číslo a která stojí v řádku za ním. Není těžké si rozmyslet, že počet inverzí v dané permutaci je právě počet dvojic čísel „větší před menším“ v druhém řádku. Pro $\sigma$ počítáme (procházíme druhý řádek): za trojkou je jednička i dvojka, tedy přičítáme 2, za jedničkou není pochopitelně žádné menší číslo, přičítáme 0, za šestkou je pětka, čtyřka a dvojka, tedy přičítáme 3, stejně tak za sedmičku, osmičku i devítku, za pětku přičítáme 2, za čtyřku 1 a dvojku nic. Celkem máme 17 inverzí, permutace je tedy vskutku lichá.

Obdobně můžeme rozložit $\tau$ buď na součin transpozic (pomocí rozkladu na nezávislé cykly):

$$\tau = (1,2,4)(3,6) = (1,2)(2,4)(3,6),$$

nebo zjistíme počet inverzí v $\tau$: $1+2+3+0+1=7$. Tak jako tak zjišťujeme, že $\tau$ je rovněž lichá permutace. □

### D. Determinanty

Ověřte si nejprve na následujícím příkladu, že umíte počítat determinanty matic $2\times 2$ a $3\times 3$ (pomocí Sarrusova pravidla):

*2.21.* Určete determinanty matic:

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & -1 & 2 \\ 3 & 2 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ -2 & 0 & 1 \end{pmatrix}.$$

○

**2.22.** Spočítejte determinant matice

$$\begin{pmatrix} 1 & 3 & 5 & 6 \\ 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

Spočítáme determinant dvěma způsoby. Nejprve použijeme postup, při kterém upravíme matici do schodovitého tvaru (viz 2.18). Při používání elementárních úprav, které jsme používali doposud, však musíme dbát zvýšené opatrnosti. Násobení řádku konstantou totiž mění o tento násobek i determinant, prohození řádků v matici mění

Zjistili jsme, že provedení libovolné transpozice změní paritu permutace a že každé pořadí čísel $\{1,2,\dots,n\}$ lze získat postupnými transpozicemi sousedních prvků. Dokázali jsme proto:

**Důsledek.** *Na každé konečné množině $X=\{1,\dots,n\}$ s $n$ prvky, $n>1$, je právě $\frac{1}{2}n!$ sudých a $\frac{1}{2}n!$ lichých permutací.*

Jestliže složíme dvě permutace za sebou, znamená to provést napřed všechny transpozice tvořící první a pak druhou. Proto pro libovolné permutace $\sigma, \eta : X \to X$ platí

$$\operatorname{sgn}(\sigma\circ\eta) = \operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\eta),$$

a proto také

$$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma).$$

**2.16. Rozklad permutace na cykly.** Dobrým nástrojem pro praktickou práci s permutacemi je jejich rozklad na tzv. cykly.

CYKLY

Permutace $\sigma$ na množině $X=\{1,\dots,n\}$ se nazývá *cyklus* délky $k$, jestliže je možné najít prvky $a_1,\dots,a_k \in X$, $2\le k\le n$, takové, že $\sigma(a_i)=a_{i+1}$, $i=1,\dots,k-1$, zatímco $\sigma(a_k)=a_1$ a ostatní prvky v $X$ jsou pro $\sigma$ samodružné. Cykly délky dva jsou právě transpozice.
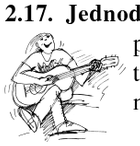
Každá permutace je složením cyklů. Cykly sudé délky mají paritu $-1$, cykly liché délky mají paritu 1.



Poslední tvrzení musíme ještě dokázat. Jestliže definujeme pro danou permutaci $\sigma$ relaci $R$ tak, že dva prvky $x$, $y\in X$ jsou v relaci, právě když $\sigma^r(x)=y$ pro nějakou iteraci permutace $\sigma$, pak zjevně jde o relaci ekvivalence (ověřte si podrobně!). Protože je $X$ konečná množina, musí pro nějaké $\ell$ být $\sigma^\ell(x)=x$. Jestliže zvolíme jednu třídu ekvivalence $\{x,\sigma(x),\dots,\sigma^{\ell-1}(x)\}\subseteq X$ a ostatní prvky definujeme jako samodružné, dostáváme cyklus. Evidentně je pak celá původní permutace $X$ složením všech těchto cyklů pro jednotlivé třídy naší ekvivalence a je jedno, v jakém pořadí cykly skládáme.

Pro určení parity si nyní stačí povšimnout, že cykly sudé délky lze napsat jako lichý počet transpozic, proto mají paritu $-1$. Obdobně cyklus liché délky dostaneme ze sudého počtu transpozic, a proto mají paritu 1.

**2.17. Jednoduché vlastnosti determinantu.** Poznání vlastností permutací a jejich parit z předchozích odstavců nám teď umožní rychle odvodit základní vlastnosti determinantů.



Pro každou matici $A=(a_{ij})$ typu $m/n$ nad skaláry z $\mathbb{K}$ definujeme *matici transponovanou* k $A$. Jde o matici $A^T=(a'_{ij})$ s prvky $a'_{ij}=a_{ji}$, která je typu $n/m$.

Čtvercová matice $A$ s vlastností $A=A^T$ se nazývá *symetrická*. Jestliže platí $A=-A^T$, pak se $A$ nazývá *antisymetrická*.

JEDNODUCHÉ VLASTNOSTI DETERMINANTŮ

**Věta.** *Pro každou čtvercovou matici $A=(a_{ij})$ platí následující tvrzení:*

*(1)* $|A^T|=|A|$.
*(2) Je-li jeden řádek v $A$ tvořen nulovými prvky z $\mathbb{K}$, pak $|A|=0$.*
*(3) Jestliže matice $B$ vznikla z $A$ výměnou dvou řádků, pak $|A|=-|B|$.*

znaménko determinantu. Použitím elementárních úprav postupně dostáváme:

$$\begin{pmatrix}1&3&5&6\\1&2&2&2\\1&1&1&2\\0&1&2&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&2\\1&2&2&2\\1&3&5&6\\0&1&2&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&2\\0&1&1&0\\0&2&4&4\\0&1&2&1\end{pmatrix}$$
$$\begin{pmatrix}1&1&1&2\\0&1&1&0\\0&0&2&4\\0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&2\\0&1&1&0\\0&0&1&1\\0&0&2&4\end{pmatrix}\sim\begin{pmatrix}1&1&1&2\\0&1&1&0\\0&0&1&1\\0&0&0&2\end{pmatrix}.$$

Determinantem horní (i dolní) trojúhelníkové matice je ovšem pouze součin čísel na hlavní diagonále. V průběhu úprav jsme dvakrát prohodili dva řádky, výsledek tedy dvakrát změní znaménko, tedy vlastně nezmění. Determinant je tedy roven číslu 2.

Jiný způsob výpočtu je založen na rozvíjení podle řádků (sloupců) matice, viz 2.21

**Řešení.** Začneme rozvíjet podle prvního sloupce, kde máme nejvíce (jednu) nul. Postupně dostáváme

$$\begin{vmatrix}1&3&5&6\\1&2&2&2\\1&1&1&2\\0&1&2&1\end{vmatrix}=1\cdot\begin{vmatrix}2&2&2\\1&1&2\\1&2&1\end{vmatrix}-1\cdot\begin{vmatrix}3&5&6\\1&1&2\\1&2&1\end{vmatrix}+1\cdot\begin{vmatrix}3&5&6\\2&2&2\\1&2&1\end{vmatrix}=$$
$$\overset{\text{Podle Sarrusova pravidla}}{=}-2-2+6=2.$$

□

**2.23.** Nalezněte všechny hodnoty argumentu $a$ takové, že

$$\begin{vmatrix}a&1&1&1\\0&a&1&1\\0&1&a&1\\0&0&0&-a\end{vmatrix}=1.$$

Pro komplexní $a$ uveďte buď jeho algebraický nebo goniometrický tvar.

**Řešení.** Spočítáme determinant rozvinutím podle prvního sloupce matice:

$$D=\begin{vmatrix}a&1&1&1\\0&a&1&1\\0&1&a&1\\0&0&0&-a\end{vmatrix}=a\cdot\begin{vmatrix}a&1&1\\1&a&1\\0&0&-a\end{vmatrix},$$

dále rozvíjíme podle posledního řádku:

$$D=a\cdot(-a)\begin{vmatrix}a&1\\1&a\end{vmatrix}=-a^2(a^2-1).$$

*(4) Jestliže matice $B$ vznikla z $A$ vynásobením řádku skalárem $a\in\mathbb{K}$, pak $|B|=a\,|A|$.*

*(5) Jsou-li prvky $k$-tého řádku v $A$ tvaru $a_{kj}=c_{kj}+b_{kj}$ a všechny ostatní řádky v maticích $A$, $B=(b_{ij})$, $C=(c_{ij})$ jsou stejné, pak $|A|=|B|+|C|$.*

*(6) Determinant $|A|$ se nezmění, přičteme-li k libovolnému řádku $A$ lineární kombinaci ostatních řádků.*

Důkaz. (1) Členy determinantů $|A|$ a $|A^T|$ jsou v bijektivní korespondenci. Členu $\operatorname{sgn}(\sigma)a_{1\sigma(1)}\cdot a_{2\sigma(2)}\cdots a_{n\sigma(n)}$ přitom v $A^T$ odpovídá člen (na pořadí skalárů v součinu totiž nezáleží)

$$\operatorname{sgn}(\sigma)a_{\sigma(1)1}\cdot a_{\sigma(2)2}\cdots a_{\sigma(n)n}=$$
$$=\operatorname{sgn}(\sigma)a_{1\sigma^{-1}(1)}\cdot a_{2\sigma^{-1}(2)}\cdots a_{n\sigma^{-1}(n)},$$

přičemž musíme ověřit, že je tento člen opatřen správným znaménkem. Parita $\sigma$ a $\sigma^{-1}$ je ale stejná, jde tedy opravdu o člen v determinantu $|A^T|$ a první tvrzení je dokázáno.

(2) Plyne přímo z definice determinantu, protože všechny jeho členy obsahují z každého řádku právě jeden člen. Je-li jeden z řádků nulový, budou tedy všechny členy determinantu nulové.

(3) Ve všech členech $|B|$ dojde ve srovnání s determinantem $|A|$ u permutací k přidání jedné transpozice, znaménko všech členů determinantu tedy bude opačné.

(4) Vyplývá přímo z definice, protože členy determinantu $|B|$ jsou členy $|A|$ vynásobené skalárem $a$.

(5) V každém členu $|A|$ je právě jeden součinitel z $k$-tého řádku matice $A$. Protože platí distributivní zákon pro násobení a sčítání v $\mathbb{K}$, vyplývá tvrzení přímo z definičního vztahu pro determinanty.

(6) Jsou-li v $A$ dva stejné řádky, jsou mezi členy determinantu vždy dva sčítance stejné až na znaménko. Proto je v takovém případě $|A|=0$. Je tedy podle tvrzení (5) možné přičíst k vybranému řádku libovolný jiný řádek, aniž by se změnila hodnota determinantu. Vzhledem k tvrzení (4) lze ale přičíst i skalární násobek libovolného jiného řádku. □

**2.18. Výpočetní důsledky.** Podle předchozí věty umíme převést elementárními řádkovými transformacemi každou čtvercovou matici $A$ na řádkově schodovitý tvar, aniž bychom změnili hodnotu jejího determinantu. Jen musíme dávat pozor, abychom vždy k upravovanému řádku pouze přičítali lineární kombinace řádků ostatních.

Výpočet determinantů eliminací

Je-li matice $A$ v řádkovém schodovitém tvaru, pak v každém členu $|A|$ je alespoň jeden součinitel prvkem pod diagonálou s výjimkou případu, kdy jsou všechny jen na diagonále. Pak je ale jediným nenulovým členem determinantu ten, který odpovídá identické permutaci. Vidíme tedy, že determinant takové matice ve schodovitém tvaru je

$$|A|=a_{11}\cdot a_{22}\cdot\cdots\cdot a_{nn}.$$

Předchozí věta tedy poskytuje velice efektivní metodu výpočtu determinantů pomocí Gaussovy eliminační metody, viz odstavec 2.7.

Celkem dostáváme následující podmínku pro $a$: $a^4 - a^2 + 1 = 0$. Substitucí $t = a^2$ pak máme $t^2 - t + 1$ s kořeny

$$t_1 = \frac{1 + i\sqrt{3}}{2} = \cos(\pi/3) + i\sin(\pi/3),$$
$$t_2 = \frac{1 - i\sqrt{3}}{2} = \cos(\pi/3) - i\sin(\pi/3) = \\ = \cos(-\pi/3) + i\sin(-\pi/3),$$

odkud snadno určíme čtyři možné hodnoty parametru $a$:

$$a_1 = \cos(\pi/6) + i\sin(\pi/6) = \sqrt{3}/2 + i/2,$$
$$a_2 = \cos(7\pi/6) + i\sin(7\pi/6) = -\sqrt{3}/2 - i/2,$$
$$a_3 = \cos(-\pi/6) + i\sin(-\pi/6) = \sqrt{3}/2 - i/2,$$
$$a_4 = \cos(5\pi/6) + i\sin(5\pi/6) = -\sqrt{3}/2 + i/2\,. \qquad \square$$

**2.24. Vandermondův determinant.** Dokažte vzorec pro tzv. Vandermondův determinant, tj. determinant Vandermondovy matice:

$$V_n = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i),$$

kde $x_1, \dots, x_n \in \mathbb{R}$ a na pravé straně rovnosti je součin všech rozdílů $x_j - x_i$, kde $j > i$.

**Řešení.** Odečtením prvního řádku od všech ostatních řádků a následným rozvojem podle prvního sloupce obdržíme

$$V_n(x_1, x_2, \dots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 0 & x_2 - x_1 & x_2^2 - x_1^2 & \dots & x_2^{n-1} - x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & x_n - x_1 & x_n^2 - x_1^2 & \dots & x_n^{n-1} - x_1^{n-1} \end{vmatrix} = \\ = \begin{vmatrix} x_2 - x_1 & x_2^2 - x_1^2 & \dots & x_2^{n-1} - x_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_n - x_1 & x_n^2 - x_1^2 & \dots & x_n^{n-1} - x_1^{n-1} \end{vmatrix}.$$

Vytkneme-li z $i$-tého řádku $x_{i+1} - x_1$ pro $i \in \{1, 2, \dots, n-1\}$, dostaneme

$$V_n(x_1, x_2, \dots, x_n) = \\ = (x_2 - x_1) \cdots (x_n - x_1) \begin{vmatrix} 1 & x_2 + x_1 & \dots & \sum_{j=0}^{n-2} x_2^{n-j-2} x_1^j \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n + x_1 & \dots & \sum_{j=0}^{n-2} x_n^{n-j-2} x_1^j \end{vmatrix}.$$

Odečtením od každého sloupce (počínaje posledním a konče druhým) $x_1$-násobku předcházejícího lze docílit úpravy

$$\begin{vmatrix} 1 & x_2 + x_1 & \dots & \sum_{j=0}^{n-2} x_2^{n-j-2} x_1^j \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n + x_1 & \dots & \sum_{j=0}^{n-2} x_n^{n-j-2} x_1^j \end{vmatrix} = \begin{vmatrix} 1 & x_2 & \dots & x_2^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^{n-2} \end{vmatrix}.$$



Všimněme si také hezkého důsledku prvního tvrzení předchozí věty o rovnosti determinantů matice a matice transponované. Zaručuje totiž, že kdykoliv se nám podaří dokázat nějaké tvrzení o determinantech formulované s využitím řádků příslušné matice, pak analogické tvrzení platí i pro sloupce. Např. tedy můžeme okamžitě všechna tvrzení (2)–(6) této věty přeformulovat i pro přičítání lineárních kombinací ostatních sloupců k vybranému. To můžeme hned použít pro odvození následujícího vzorce pro přímý výpočet řešení systémů lineárních rovnic:

CRAMEROVO PRAVIDLO

Uvažme systém $n$ lineárních rovnic pro $n$ proměnných s maticí sytému $A = (a_{ij})$ a sloupcem hodnot $b = (b_1, \dots, b_n)$, tj. v maticovém zápisu řešíme rovnici $A \cdot x = b$. Jestliže existuje inverze $A^{-1}$, pak jsou jednotlivé komponenty jediného řešení $x = (x_1, \dots, x_n)$ dány vztahem

$$x_i = \frac{|A_i|}{|A|},$$

kde matice $A_i$ vznikne z matice systému $A$ výměnou $i$-tého sloupce za sloupec hodnot $b$.

Skutečně, jak jsme viděli, inverze k matici systému existuje právě tehdy, když má systém jediné řešení. Jestliže tedy takové řešení $x$ máme, můžeme za sloupec $b$ dosadit do matice $A_i$ příslušnou kombinaci sloupců matice $A$, tj. hodnoty $b_i = a_{i1}x_1 + \dots + a_{in}x_n$. Pak ale odečtením $x_k$-násobků všech ostatních sloupců zůstane v $i$-tém sloupci pouze $x_i$-násobek původního sloupce z $A$. Číslo $x_i$ tedy můžeme vytknout před determinant a získáme rovnost $|A_i||A|^{-1} = x_i|A||A|^{-1} = x_i$, což je požadované tvrzení.

Dále si všimněme, že vlastnosti (3)–(5) z předchozí věty říkají, že determinant, jakožto zobrazení, které $n$ vektorům dimenze $n$ (řádkům nebo sloupcům matice) přiřadí skalár, je antisymetrické zobrazení lineární v každém svém argumentu, přesně jako jsme podle analogie z dimenze 2 požadovali.

**2.19. Další vlastnosti determinantu.** Časem uvidíme, že



skutečně stejně jako v dimenzi dva je determinant matice roven orientovanému objemu rovnoběžnostěnu určeného jejími sloupci. Uvidíme také, že když uvážíme zobrazení $x \mapsto A \cdot x$ zadané čtvercovou maticí $A$ na $\mathbb{R}^n$, pak můžeme determinant této matice vidět jako vyjádření poměru mezi objemem rovnoběžnostěnů daných vektory $x_1, \dots, x_n$ a jejich obrazy $A \cdot x_1, \dots, A \cdot x_n$. Protože skládání zobrazení $x \mapsto A \cdot x \mapsto B \cdot (A \cdot x)$ odpovídá násobení matic, je snad docela pochopitelná tzv. *Cauchyova věta*:

CAUCHYOVA VĚTA

**Věta.** *Nechť $A = (a_{ij})$, $B = (b_{ij})$ jsou čtvercové matice dimenze $n$ nad okruhem skalárů $\mathbb{K}$. Pak $|A \cdot B| = |A| \cdot |B|$.*

Všimněme si, že z Cauchyovy věty a z reprezentace elementárních řádkových transformací pomocí násobení vhodnými maticemi (viz 2.8) okamžitě vyplývají tvrzení (2), (3) a (6) z Věty 2.17.

Proto

$$V_n(x_1, x_2, \ldots, x_n) = (x_2 - x_1) \cdots (x_n - x_1)\ V_{n-1}(x_2, \ldots, x_n).$$

Neboť je zřejmě

$$V_2(x_{n-1}, x_n) = x_n - x_{n-1},$$

platí (uvažme matematickou indukci)

$$V_n(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Všimněme si, že tento determinant je nenulový, právě když jsou čísla $x_1, \ldots, x_n$ navzájem různá. □

**Poznámka.** Jiný důkaz vzorce pro Vandermondův determinant může čtenář najít v 5.5.

**2.25.** Zjistěte, zda je matice

$$\begin{pmatrix} 3 & 2 & -1 & 2 \\ 4 & 1 & 2 & -4 \\ -2 & 2 & 4 & 1 \\ 2 & 3 & -4 & 8 \end{pmatrix}$$

invertibilní.

**Řešení.** Matice je invertibilní (existuje k ní inverzní matice) právě tehdy, když ji lze pomocí řádkových transformací převést na jednotkovou matici. To je ekvivalentní např. s tím, že má nenulový determinant. Ten spočítáme pomocí Laplaceovy věty (2.32) například rozvojem podle prvního řádku:

$$\begin{vmatrix} 3 & 2 & -1 & 2 \\ 4 & 1 & 2 & -4 \\ -2 & 2 & 4 & 1 \\ 2 & 3 & -4 & 8 \end{vmatrix} = 3 \cdot \begin{vmatrix} 1 & 2 & -4 \\ 2 & 4 & 1 \\ 3 & -4 & 8 \end{vmatrix} - 2 \cdot \begin{vmatrix} 4 & 2 & -4 \\ -2 & 4 & 1 \\ 2 & -4 & 8 \end{vmatrix} +$$

$$+ (-1) \cdot \begin{vmatrix} 4 & 1 & -4 \\ -2 & 2 & 1 \\ 2 & 3 & 8 \end{vmatrix} - 2 \cdot \begin{vmatrix} 4 & 1 & 2 \\ -2 & 2 & 4 \\ 2 & 3 & -4 \end{vmatrix} =$$

$$= 3 \cdot 90 - 2 \cdot 180 + (-1) \cdot 110 - 2 \cdot (-100) =$$

$$= 0.$$

Tedy daná matice není invertibilní. □

## E. Soustavy lineárních rovnic podruhé

Se soustavami lineárních rovnic jsme se již setkali na začátku kapitoly. Nyní se budeme věnovat této problematice podrobněji. Zkusme nejprve využít výpočtu inverzní matice k řešení systému lineárních soustav rovnic.



My teď tuto větu odvodíme ryze algebraicky už proto, že předchozí odvolávka na geometrický argument těžko může fungovat pro libovolné skaláry. Základním nástrojem je tzv. *rozvoj determinantu* podle jednoho nebo více řádků či sloupců. Budeme proto potřebovat něco málo technické přípravy. Čtenář, který by snad tolik abstrakce nestrávil, může tyto pasáže přeskočit a vstřebat pouze znění Laplaceovy věty a jejích důsledků.

**2.20. Minory matice.** Při úvahách o maticích a jejich vlastnostech budeme často pracovat jen s jejich částmi. Budeme si proto muset zavést několik pojmů.



SUBMATICE A MINORY

Nechť $A = (a_{ij})$ je matice typu $m/n$ a $1 \le i_1 < \ldots < i_k \le m$, $1 \le j_1 < \ldots < j_l \le n$ jsou pevně zvolená přirozená čísla. Pak matici

$$M = \begin{pmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \ldots & a_{i_1 j_\ell} \\ \vdots & \vdots & & \vdots \\ a_{i_k j_1} & a_{i_k j_2} & \ldots & a_{i_k j_\ell} \end{pmatrix}$$

typu $k/\ell$ nazýváme *submaticí matice* $A$ určenou řádky $i_1, \ldots, i_k$ a sloupci $j_1, \ldots, j_\ell$. Zbývajícími $(m-k)$ řádky a $(n-l)$ sloupci je určena matice $M^*$ typu $(m-k)/(n-\ell)$, která se nazývá *doplňková submatice* k $M$ v $A$. Při $k = \ell$ je definován $|M|$, který nazýváme *subdeterminant* nebo *minor* řádu $k$ matice $A$. Je-li $m = n$, pak při $k = \ell$ je i $M^*$ čtvercová a $|M^*|$ se nazývá *doplněk minoru* $|M|$, nebo *doplňkový minor* k submatici $M$ v matici $A$. Skalár

$$(-1)^{i_1 + \cdots + i_k + j_1 + \cdots + j_l} \cdot |M^*|$$

se nazývá *algebraický doplněk* k minoru $|M|$.

Submatice tvořené prvními $k$ řádky a sloupci se nazývají *vedoucí hlavní submatice*, jejich determinanty *vedoucí hlavní minory* matice $A$. Zvolíme-li $k$ po sobě jdoucích řádků a sloupců, počínaje $i$–tým řádkem, hovoříme o *hlavních submaticích*, resp. *hlavních minorech*.

Při speciální volbě $k = \ell = 1$, $m = n$ říkáme příslušnému doplňkovému minoru *algebraický doplněk* $A_{ij}$ prvku $a_{ij}$ matice $A$.

**2.21. Laplaceův rozvoj determinantu.** Pokud je $|M|$ hlavní minor matice $A$ řádu $k$, pak přímo z definice determinantu je vidět, že každý z jednotlivých $k!(n-k)!$ sčítanců v součinu $|M|$ s jeho algebraickým doplňkem je členem determinantu $|A|$.



Obecně, uvažme submatici $M$, tj. čtvercovou matici, určenou řádky $i_1 < i_2 < \cdots < i_k$ a sloupci $j_1 < \cdots < j_k$. Pak pomocí $(i_1 - 1) + \cdots + (i_k - k)$ výměn sousedních řádků a $(j_1 - 1) + \ldots + (j_k - k)$ výměn sousedních sloupců v $A$ převedeme tuto submatici $M$ na hlavní submatici a doplňková matice přitom přejde právě na doplňkovou matici. Celá matice $A$ přejde přitom v matici $B$, pro kterou platí podle 2.17 a definice determinantu $|B| = (-1)^\alpha |A|$, kde $\alpha = \sum_{h=1}^{k} (i_h - j_h) - 2(1 + \cdots + k)$. Tím jsme ověřili:

**Tvrzení.** *Jestliže je $A$ čtvercová matice dimenze $n$ a $|M|$ je její minor řádu $k < n$, pak součin libovolného členu $|M|$ s libovolným členem jeho algebraického doplňku je členem $|A|$.*

**2.26. Účastníci zájezdu.** Dvoudenního autobusového zájezdu se zúčastnilo 45 osob. První den se platilo vstupné na rozhlednu 30 Kč za dospělého, 16 Kč za dítě a 24 Kč za seniora, celkem 1 116 Kč. Druhý den se platilo vstupné do botanické zahrady 40 Kč za dospělého, 24 Kč za dítě a 34 Kč za seniora, celkem 1 542 Kč. Kolik bylo mezi výletníky dospělých, dětí a seniorů?

**Řešení.** Zaveďme proměnné

$x$ udávající „počet dospělých“;

$y$ udávající „počet dětí“;

$z$ udávající „počet seniorů“.

Zájezdu se zúčastnilo 45 osob, a proto

$$x + y + z = 45.$$

Celkové vstupné na rozhlednu a do botanické zahrady při zavedení našich proměnných a při zachování pořadí činí $30x + 16y + 24z$ a $40x + 24y + 34z$. My je ovšem známe (1 116 Kč a 1 542 Kč). Máme tak

$$\begin{aligned} 30x + 16y + 24z &= 1\,116,\\ 40x + 24y + 34z &= 1\,542. \end{aligned}$$

Soustavu tří lineárních rovnic zapíšeme maticově jako

$$\begin{pmatrix} 1 & 1 & 1 \\ 30 & 16 & 24 \\ 40 & 24 & 34 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 45 \\ 1\,116 \\ 1\,542 \end{pmatrix}.$$

Řešením je

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \frac{1}{6} \begin{pmatrix} 16 & 5 & -4 \\ 30 & 3 & -3 \\ -40 & -8 & 7 \end{pmatrix} \cdot \begin{pmatrix} 45 \\ 1\,116 \\ 1\,542 \end{pmatrix} = \frac{1}{6} \begin{pmatrix} 132 \\ 72 \\ 66 \end{pmatrix} = \begin{pmatrix} 22 \\ 12 \\ 11 \end{pmatrix},$$

neboť

$$\begin{pmatrix} 1 & 1 & 1 \\ 30 & 16 & 24 \\ 40 & 24 & 34 \end{pmatrix}^{-1} = \frac{1}{6} \begin{pmatrix} 16 & 5 & -4 \\ 30 & 3 & -3 \\ -40 & -8 & 7 \end{pmatrix}.$$

Slovně vyjádřeno, zájezdu se zúčastnilo 22 dospělých, 12 dětí, 11 seniorů. □

*2.27.* Za pomoci výpočtu inverzní matice určete řešení soustavy

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 2,\\ x_1 + x_2 - x_3 - x_4 &= 3,\\ x_1 - x_2 + x_3 - x_4 &= 3,\\ x_1 - x_2 - x_3 + x_4 &= 5. \end{aligned}$$

○

Co když však matice soustavy není invertibilní? Potom nemůžeme k jejímu řešení inverzní matice využít. Taková soustava pak má jiný

Toto tvrzení už podbízí představu, že by se pomocí takových součinů menších determinantů skutečně mohl determinant matic vyjadřovat. Víme, že $|A|$ obsahuje právě $n!$ různých členů, právě jeden pro každou permutaci. Tyto členy jsou navzájem různé jakožto polynomy v prvcích (neznámé obecné) matice $A$. Jestliže tedy ukážeme, že navzájem různých výrazů z předchozího tvrzení je právě tolik, jako je tomu u determinantu $|A|$, pak dostaneme jejich součtem právě determinant $|A|$.

Zbývá proto ukázat, že uvažované součiny $|M|\cdot|M^*|$ obsahují právě $n!$ různých členů z $|A|$.

Ze zvolených $k$ řádků lze vybrat $\binom{n}{k}$ minorů $M$ a podle předchozího lemmatu je každý z $k!(n-k)!$ členů v součinech $|M|$ s jejich algebraickými doplňky členem $|A|$. Přitom pro různé výběry $M$ nemůžeme nikdy obdržet stejné členy a jednotlivé členy v $(-1)^{i_1+\cdots+i_k+j_1+\cdots+j_l} \cdot |M| \cdot |M^*|$ jsou také po dvou různé. Celkem tedy máme právě požadovaný počet $k!(n-k)!\binom{n}{k} = n!$ členů.

Tím jsme bezezbytku dokázali:

LAPLACEOVA VĚTA

**Věta.** *Nechť $A = (a_{ij})$ je čtvercová matice dimenze $n$ nad libovolným okruhem skalárů a nechť je pevně zvoleno $k$ jejích řádků. Pak $|A|$ je součet všech $\binom{n}{k}$ součinů $(-1)^{i_1+\cdots+i_k+j_1+\cdots+j_l} \cdot |M| \cdot |M^*|$ minorů řádu $k$ vybraných ze zvolených řádků, s jejich algebraickými doplňky.*

Laplaceova věta převádí výpočet $|A|$ na výpočet determinantů nižšího stupně. Této metodě výpočtu se říká *Laplaceův rozvoj* podle zvolených řádků či sloupců. Např. rozvoj podle $i$-tého řádku nebo podle $j$-tého sloupce:

$$|A| = \sum_{j=1}^{n} a_{ij} A_{ij},$$

kde $A_{ij}$ označuje algebraický doplněk k prvku $a_{ij}$ (tj. k minoru stupně 1).

Při praktickém počítání determinantů bývá výhodné kombinovat Laplaceův rozvoj s přímou metodou přičítání lineárních kombinací řádků či sloupců.

**2.22. Důkaz Cauchyovy věty.** Důkaz se opírá o trikovou ale elementární aplikaci Laplaceovy věty. Použijeme prostě dvakrát Laplaceův rozvoj na vhodné matice.



Uvažme nejprve následující matici $H$ dimenze $2n$ (používáme tzv. blokovou symboliku, tj. píšeme matici jakoby složenou ze (sub)matic $A$, $B$ atd.)

$$H = \begin{pmatrix} A & 0 \\ -E & B \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} & 0 & \dots & 0 \\ -1 & & 0 & b_{11} & \dots & b_{1n} \\ & \ddots & & \vdots & & \vdots \\ 0 & & -1 & b_{n1} & \dots & b_{nn} \end{pmatrix}.$$

Laplaceovým rozvojem podle prvních $n$ řádků obdržíme právě $|H| = |A| \cdot |B|$.

Nyní budeme k posledním $n$ sloupcům postupně přičítat lineární kombinace prvních $n$ sloupců tak, abychom obdrželi matici

počet než jedno řešení. Jak možná čtenář již ví, tak systém lineárních rovnic nad nekonečným tělesem buď nemá řešení, nebo má jedno řešení, nebo jich má nekonečně mnoho (například nemůže mít právě dvě řešení). Prostor řešení je buď vektorový prostor (v případě, že pravá strana všech rovnic v systému je nulová, hovoříme o *homogenním systému* lineárních rovnic) nebo afinní prostor, viz 4.1, (v případě, že pravá strana alespoň jedné z rovnic je nenulová, hovoříme o *nehomogenním systému* lineárních rovnic). Ukažme si tedy různé možné typy řešení soustavy lineárních rovnic na příkladech.

**2.28.** Pro jaké hodnoty parametrů $a, b \in \mathbb{R}$ má lineární systém

$$\begin{array}{rcrcrcl} x_1 & - & & ax_2 & - & 2x_3 & = & b, \\ x_1 & + & (1-a)x_2 & & & & = & b-3, \\ x_1 & + & (1-a)x_2 & + & ax_3 & = & & 2b-1 \end{array}$$

(a) právě 1 řešení;

(b) žádné řešení;

(c) alespoň 2 řešení?

**Řešení.** Soustavu „tradičně“ přepíšeme do rozšířené matice a upravíme

$$\left(\begin{array}{ccc|c} 1 & -a & -2 & b \\ 1 & 1-a & 0 & b-3 \\ 1 & 1-a & a & 2b-1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & -a & -2 & b \\ 0 & 1 & 2 & -3 \\ 0 & 1 & a+2 & b-1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|c} 1 & -a & -2 & b \\ 0 & 1 & 2 & -3 \\ 0 & 0 & a & b+2 \end{array}\right).$$

Dodejme, že v prvním kroku jsme první řádek odečetli od druhého a od třetího a ve druhém kroku pak druhý od třetího. Vidíme, že soustava bude mít právě jedno řešení (které lze určit zpětnou eliminací) tehdy a jenom tehdy, když $a \neq 0$. Pro $a = 0$ totiž ve třetím sloupci není první nenulové číslo nějakého řádku. Je-li $a = 0$ a $b = -2$, dostáváme nulový řádek, kdy volba $x_3 \in \mathbb{R}$ jako parametru dává nekonečně mnoho různých řešení. Pro $a = 0$ a $b \neq -2$ poslední rovnice $a = b+2$ nemůže být splněna – soustava nemá řešení.

Poznamenejme, že pro $a = 0, b = -2$ jsou řešeními

$$(x_1,\ x_2,\ x_3) = (-2+2t,\ -3-2t,\ t)\ ,\ t \in \mathbb{R},$$

a pro $a \neq 0$ je jediným řešením trojice

$$\left(\frac{-3a^2-ab-4a+2b+4}{a}, -\frac{2b+3a+4}{a}, \frac{b+2}{a}\right). \qquad \square$$

**2.29.** Nechť je dáno

$$A = \begin{pmatrix} 4 & 5 & 1 \\ 3 & 4 & 0 \\ 1 & 1 & 1 \end{pmatrix},\ x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},\ b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}.$$

Najděte taková reálná čísla $b_1, b_2, b_3$, aby systém lineárních rovnic $A \cdot x = b$ měl:

s nulami v pravém dolním rohu. Dostaneme

$$K = \begin{pmatrix} a_{11} & \dots & a_{1n} & c_{11} & \dots & c_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} & c_{n1} & \dots & c_{nn} \\ -1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & -1 & 0 & \dots & 0 \end{pmatrix}.$$

Prvky submatice nahoře vpravo přitom musí splňovat

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj},$$

neboli jde právě o prvky součinu $A \cdot B$ a $|K| = |H|$. Přitom rozvojem podle posledních $n$ sloupců dostáváme

$$|K| = (-1)^{n+1+\cdots+2n}|A \cdot B| = (-1)^{2n\cdot(n+1)} \cdot |A \cdot B| = |A \cdot B|.$$

Tím je Cauchyova věta bezezbytku dokázána.

**2.23. Determinant a inverzní matice.** Předpokládejme nejprve, že existuje matice inverzní k matici $A$, tj. $A \cdot A^{-1} = E$. Protože pro jednotkovou matici platí vždy $|E| = 1$, je pro každou invertibilní matici vždy $|A|$ invertibilní skalár a díky Cauchyově větě platí $|A^{-1}| = |A|^{-1}$.



My však nyní kombinací Laplaceovy věty a Cauchyho věty umíme říci víc.

VZOREC PRO INVERZNÍ MATICI

Pro libovolnou čtvercovou matici $A = (a_{ij})$ dimenze $n$ definujeme matici $A^* = (a^*_{ij})$, kde $a^*_{ij} = A_{ji}$ jsou algebraické doplňky k prvkům $a_{ji}$ v $A$. Matici $A^*$ nazýváme *algebraicky adjungovaná matice* k matici $A$.

**Věta.** *Pro každou čtvercovou matici $A$ nad okruhem skalárů $\mathbb{K}$ platí*

$$AA^* = A^*A = |A| \cdot E. \tag{2.2}$$

*Zejména tedy*

*(1) $A^{-1}$ existuje jako matice nad okruhem skalárů $\mathbb{K}$, právě když $|A|^{-1}$ existuje v $\mathbb{K}$.*

*(2) Pokud existuje $A^{-1}$, pak platí $A^{-1} = |A|^{-1} \cdot A^*$.*

DŮKAZ. Jak jsme již zmínili, Cauchyova věta ukazuje, že z existence $A^{-1}$ vyplývá invertibilita $|A| \in \mathbb{K}$.

Pro libovolnou čtvercovou matici $A$ spočteme přímým výpočtem $A \cdot A^* = (c_{ij})$, kde

$$c_{ij} = \sum_{k=1}^{n} a_{ik}a^*_{kj} = \sum_{k=1}^{n} a_{ik}A_{jk}\,.$$

Pokud $i = j$, je to právě Laplaceův rozvoj $|A|$ podle $i$-tého řádku. Pokud $i \neq j$, jde o rozvoj determinantu matice, v níž je $i$-tý a $j$-tý řádek stejný, a proto je $c_{ij} = 0$. Odtud plyne $A \cdot A^* = |A| \cdot E$ a dokázali jsme rovnost (2.2).

Předpokládejme navíc, že $|A|$ je invertibilní skalár. Jestliže zopakujeme předešlý výpočet pro $A^* \cdot A$, obdržíme $|A|^{-1}A^* \cdot A = E$. Proto náš výpočet skutečně dává inverzní matici $A$, jak je tvrzeno ve větě. $\square$

(a) nekonečně mnoho řešení;

(b) právě jedno řešení;

(c) žádné řešení;

(d) právě 4 řešení.

**Řešení.** Pro čtenáře jistě nebude problém najít odpovídající hodnoty v případech a) a c) (stačí volit $b_1 = b_2 + b_3$ v případě a) a naopak $b_1 \neq b_2 + b_3$ v případě c)). Povšimněme si dále, že $|A| = 0$, soustava tak má buď nekonečně mnoho, nebo žádné řešení. Obecně tvoří množina řešení homogenní soustavy lineárních rovnic vektorový prostor, varianta d) je proto apriori vyloučena. Varianta b) je možná pouze pro regulární matici soustavy (jediným řešením je pak nulový vektor). □

**2.30.** Nalezněte matici algebraicky adjungovanou a matici inverzní k matici

$$A = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 3 & 0 & 4 \\ 5 & 0 & 6 & 0 \\ 0 & 7 & 0 & 8 \end{pmatrix}.$$

**Řešení.** Adjungovaná matice je

$$A^* = \begin{pmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ A_{21} & A_{22} & A_{23} & A_{24} \\ A_{31} & A_{32} & A_{33} & A_{34} \\ A_{41} & A_{42} & A_{43} & A_{44} \end{pmatrix}^T,$$

kde $A_{ij}$ je algebraický doplněk prvku $a_{ij}$ matice $A$, tedy součin čísla $(-1)^{i+j}$ a determinantu trojrozměrné matice vzniklé z $A$ vynecháním $i$-tého řádku a $j$-tého sloupce. Platí

$$A_{11} = \begin{vmatrix} 3 & 0 & 4 \\ 0 & 6 & 0 \\ 7 & 0 & 8 \end{vmatrix} = -24, \qquad A_{12} = -\begin{vmatrix} 0 & 0 & 4 \\ 5 & 6 & 0 \\ 0 & 0 & 8 \end{vmatrix} = 0, \dots$$

$$A_{43} = -\begin{vmatrix} 1 & 0 & 0 \\ 0 & 3 & 4 \\ 5 & 0 & 0 \end{vmatrix} = 0, \qquad A_{44} = \begin{vmatrix} 1 & 0 & 2 \\ 0 & 3 & 0 \\ 5 & 0 & 6 \end{vmatrix} = -12.$$

Dosazením získáme

$$A^* = \begin{pmatrix} -24 & 0 & 20 & 0 \\ 0 & -32 & 0 & 28 \\ 8 & 0 & -4 & 0 \\ 0 & 16 & 0 & -12 \end{pmatrix}^T = \begin{pmatrix} -24 & 0 & 8 & 0 \\ 0 & -32 & 0 & 16 \\ 20 & 0 & -4 & 0 \\ 0 & 28 & 0 & -12 \end{pmatrix}.$$

Inverzní matici $A^{-1}$ určíme ze vztahu $A^{-1} = |A|^{-1} \cdot A^*$. Determinant matice $A$ je (rozvojem podle prvního řádku) roven

$$|A| = \begin{vmatrix} 1 & 0 & 2 & 0 \\ 0 & 3 & 0 & 4 \\ 5 & 0 & 6 & 0 \\ 0 & 7 & 0 & 8 \end{vmatrix} = \begin{vmatrix} 3 & 0 & 4 \\ 0 & 6 & 0 \\ 7 & 0 & 8 \end{vmatrix} + 2 \begin{vmatrix} 0 & 3 & 4 \\ 5 & 0 & 0 \\ 0 & 7 & 8 \end{vmatrix} = 16.$$

Jako přímý důsledek této věty můžeme znovu ověřit Cramerovo pravidlo pro řešení systémů lineárních rovnic, viz 2.18. Skutečně, pro řešení systému $A \cdot x = b$ stačí důsledně přečíst v rovnosti

$$x = A^{-1} \cdot b = |A|^{-1} A^* \cdot b$$

poslední výraz jako Laplaceův rozvoj determinantu matice $A_i$ vzniklé výměnou $i$–tého sloupce v $A$ za sloupec hodnot $b$.

### 3. Vektorové prostory a lineární zobrazení

**2.24. Abstraktní vektorové prostory.** Vraťme se teď na chvilku



k systémům $m$ lineárních rovnic pro $n$ proměnných z 2.3 a předpokládejme navíc, že jde o homogenní systém rovnic $A \cdot x = 0$, tj.

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Díky vlastnosti distributivity pro násobení matic je zřejmé, že součet dvou řešení $x = (x_1, \dots, x_n)$ a $y = (y_1, \dots, y_n)$ splňuje

$$A \cdot (x + y) = A \cdot x + A \cdot y = 0,$$

a je tedy také řešením. Stejně tak zůstává řešením i skalární násobek $a \cdot x$. Množina všech řešení pevně zvoleného systému rovnic je proto uzavřená na sčítání vektorů a násobení vektorů skaláry. To byly základní vlastnosti vektorů dimenze $n$ v $\mathbb{K}^n$, viz 2.1. Teď ale máme vektory v prostoru řešení s $n$ souřadnicemi a „rozměr" tohoto prostoru je dán rozdílem počtu proměnných a hodností matice $A$. Můžeme tedy snadno mít při řešení 1000 souřadnic jen jeden nebo dva volné parametry. Celý prostor řešení se pak bude chovat jako rovina nebo přímka, jak jsme je poznali již v odstavci 1.25 na straně 28.

Už v odstavci 1.9 jsme ale potkali ještě zajímavější příklad prostoru všech řešení homogenní lineární diferenční rovnice (prvního řádu). Všechna řešení jsme dostali z jednoho pomocí násobení skaláry a jsou tedy také uzavřená na součty a skalární násobky. Tyto „vektory" řešení jsou ovšem nekonečné posloupnosti čísel, přestože intuitivně očekáváme, že „rozměr" celého prostoru řešení by měl být jedna. Potřebujeme proto obecnější definici vektorového prostoru a jeho dimenze:

DEFINICE VEKTOROVÉHO PROSTORU

*Vektorovým prostorem* $V$ nad polem skalárů $\mathbb{K}$ rozumíme množinu, na které jsou definovány

- operace sčítání splňující axiomy (KG1)–(KG4) z odstavce 1.1 na straně 6,
- násobení skaláry, pro které platí axiomy (V1)–(V4) z odstavce 2.1 na straně 65.

Připomeňme také naši jednoduchou konvenci ohledně značení: skaláry budou zpravidla označovány znaky z počátku abecedy, tj. $a, b, c, \dots$, zatímco pro vektory budeme užívat znaky z konce abecedy, tj. $u, v, w, x, y, z$. Přitom ještě navíc většinou $x, y, z$ budou opravdu $n$-tice skalárů. Pro úplnost výčtu, písmena z prostředka, např. $i, j, k, \ell$, budou nejčastěji označovat indexy výrazů.

Dostáváme tedy

$$A^{-1} = \begin{pmatrix} -3/2 & 0 & 1/2 & 0 \\ 0 & -2 & 0 & 1 \\ 5/4 & 0 & -1/4 & 0 \\ 0 & 7/4 & 0 & -3/4 \end{pmatrix}.$$

□

### F. Vektorové prostory

Vlastnosti vektorového prostoru, kterých jsme si všimli u roviny či třírozměrného prostoru, ve kterém žijeme, má celá řada jiných množin. Ukažme si to na příkladech.

**2.31. Vektorový prostor ano či ne?** Rozhodněte o následujících množinách, jestli jsou vektorovými prostory nad tělesem reálných čísel:

i) Množina řešení soustavy

$$\begin{array}{rcrcccrcrcrcl} x_1 & + & x_2 & + & \cdots & + & x_{98} & + & x_{99} & + & x_{100} & = & 100x_1, \\ x_1 & + & x_2 & + & \cdots & + & x_{98} & + & x_{99} & & & = & 99x_1, \\ x_1 & + & x_2 & + & \cdots & + & x_{98} & & & & & = & 98x_1, \\ & & & & \vdots & & & & & & & & \\ x_1 & + & x_2 & & & & & & & & & = & 2x_1. \end{array}$$

ii) Množina řešení rovnice

$$x_1 + x_2 + \cdots + x_{100} = 0.$$

iii) Množina řešení rovnice

$$x_1 + 2x_2 + 3x_3 + \cdots + 100x_{100} = 1.$$

iv) Množina všech reálných, resp. komplexních, posloupností. (Reálnou, resp. komplexní posloupností rozumíme zobrazení $f : \mathbb{N} \to \mathbb{R}$, resp. $f : \mathbb{N} \to \mathbb{C}$. O obrazu čísla $n$ pak hovoříme jako o $n$-tém členu posloupnosti, většinou jej označujeme dolním indexem, např. $a_n$.)

v) Množina řešení homogenní diferenční rovnice.

vi) Množina řešení nehomogenní diferenční rovnice.

vii) $\{f : \mathbb{R} \to \mathbb{R} \mid f(1) = f(2) = c, c \in \mathbb{R}\}$.

**Řešení.**

i) Ano. Jsou to všechny reálné násobky vektoru $\underbrace{(1, 1, 1, \ldots, 1)}_{100 \text{ jedniček}}$, tedy vektorový prostor dimenze 1 (viz dále (2.29)).

ii) Ano. Jedná se o prostor dimenze 99 (odpovídá počtu volných parametrů řešení). Obecně tvoří množina řešení libovolné homogenní soustavy lineárních rovnic vektorový prostor.

iii) Ne. Např. dvojnásobek řešení $x_1 = 1, x_i = 0, i = 2, \ldots, 100$ není řešením dané rovnice. Množina řešení však tvoří tzv. afinní prostor (viz 4.1).



Abychom se trochu pocvičili ve formálním postupu, ověříme jednoduché vlastnosti vektorů, které pro $n$-tice skalárů byly samozřejmé, nicméně teď je musíme odvodit z axiomů.

**2.25. Tvrzení.** *Nechť $V$ je vektorový prostor nad polem skalárů $\mathbb{K}$, dále uvažme $a, b, a_i \in \mathbb{K}$ a vektory $u, v, u_j \in V$. Potom*

*(1)* $a \cdot u = 0$, *právě když* $a = 0$ *nebo* $u = 0$,
*(2)* $(-1) \cdot u = -u$,
*(3)* $a \cdot (u - v) = a \cdot u - a \cdot v$,
*(4)* $(a - b) \cdot u = a \cdot u - b \cdot u$,
*(5)* $\left(\sum_{i=1}^{n} a_i\right) \cdot \left(\sum_{j=1}^{m} u_j\right) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot u_j$.

Důkaz. Můžeme rozepsat

$$(a + 0) \cdot u \overset{(V2)}{=} a \cdot u + 0 \cdot u = a \cdot u,$$

což podle axiomu (KG4) zaručuje $0 \cdot u = 0$. Nyní

$$u + (-1) \cdot u \overset{(V2)}{=} (1 + (-1)) \cdot u = 0 \cdot u = 0$$

a odtud $-u = (-1) \cdot u$. Dále

$$a \cdot (u + (-1) \cdot v) \overset{(V2,V3)}{=} a \cdot u + (-a) \cdot v = a \cdot u - a \cdot v,$$

což dokazuje (3). Platí

$$(a - b) \cdot u \overset{(V2,V3)}{=} a \cdot u + (-b) \cdot u = a \cdot u - b \cdot u$$

a tím je ověřeno (4). Vztah (5) plyne indukcí z (V2) a (V1).

Zbývá (1): $a \cdot 0 = a \cdot (u - u) = a \cdot u - a \cdot u = 0$, což spolu s prvním tvrzením tohoto důkazu ukazuje jednu implikaci. K opačné implikaci poprvé potřebujeme axiom pole pro skaláry a axiom (V4) pro vektorové prostory: je-li $p \cdot u = 0$ a $p \neq 0$, pak $u = 1 \cdot u = (p^{-1} \cdot p) \cdot u = p^{-1} \cdot 0 = 0$. □

**2.26. Lineární (ne)závislost.** V odstavci 2.11 jsme pracovali s tzv. lineárními kombinacemi řádků matice. S obecnými vektory budeme zacházet zcela analogicky:

Lineární kombinace a nezávislost

Výrazy tvaru $a_1 \cdot v_1 + \cdots + a_k \cdot v_k$ nazýváme *lineární kombinace* vektorů $v_1, \ldots, v_k \in V$.

Konečnou posloupnost vektorů $v_1, \ldots, v_k$ nazveme *lineárně nezávislou*, jestliže jediná jejich nulová lineární kombinace je ta s nulovými koeficienty, tj. jestliže pro skaláry $a_1, \ldots, a_k \in \mathbb{K}$ platí

$$a_1 \cdot v_1 + \cdots + a_k \cdot v_k = 0 \implies a_1 = a_2 = \cdots = a_k = 0.$$

Je zjevné, že v nezávislé posloupnosti vektorů jsou všechny po dvou různé a nenulové.

Množina vektorů $M \subseteq V$ ve vektorovém prostoru $V$ nad $\mathbb{K}$ se nazývá *lineárně nezávislá*, jestliže každá konečná $k$-tice vektorů $v_1, \ldots, v_k \in M$ je lineárně nezávislá.

Množina $M$ vektorů je *lineárně závislá*, jestliže není lineárně nezávislá.



Přímo z definice vyplývá, že neprázdná podmnožina $M$ vektorů ve vektorovém prostoru nad polem skalárů $\mathbb{K}$ je závislá, právě když je jeden z jejích vektorů vyjádřitelný jako konečná lineární kombinace ostatních vektorů v $M$. Skutečně, alespoň jeden koeficient v příslušné nulové lineární kombinaci musí být nenulový, a protože jsme nad polem skalárů, můžeme jím podělit a vyjádřit tak u něj stojící vektor pomocí ostatních.

iv) Ano. Množina všech reálných, resp. komplexních, posloupností tvoří zřejmě reálný, resp. komplexní, vektorový prostor. Sčítání posloupností a násobení posloupnosti skalárem je totiž definováno člen po členu, kde se jedná o vektorový prostor reálných, resp. komplexních, čísel.

v) Ano. Abychom ukázali, že množina posloupností vyhovujících dané diferenční homogenní rovnici (více si o nich povíme v 3.9) tvoří vektorový prostor, stačí ukázat, že je uzavřená vzhledem ke sčítání i násobení reálným číslem (neboť se jedná o podmnožinu vektorového prostoru). Mějme posloupnosti $(x_j)_{j=0}^{\infty}$ a $(y_j)_{j=0}^{\infty}$ vyhovující stejné homogenní diferenční rovnici, tedy

$$a_n x_{n+k} + a_{n-1} x_{n+k-1} + \cdots + a_0 x_k = 0,$$
$$a_n y_{n+k} + a_{n-1} y_{n+k-1} + \cdots + a_0 y_k = 0.$$

Sečtením těchto rovnic dostaneme

$$a_n(x_{n+k} + y_{n+k}) + a_{n-1}(x_{n+k-1} + y_{n+k-1}) + \cdots \\ \cdots + a_0(x_k + y_k) = 0,$$

tedy i posloupnost $(x_j + y_j)_{j=0}^{\infty}$ vyhovuje stejné diferenční rovnici. Rovněž pokud posloupnost $(x_j)_{j=0}^{\infty}$ vyhovuje dané rovnici, tak i posloupnost $(ux_j)_{j=0}^{\infty}$, kde $u \in \mathbb{R}$.

vi) Ne. Součet dvou řešení nehomogenní rovnice

$$a_n x_{n+k} + a_{n-1} x_{n+k-1} + \cdots + a_0 x_k = c,$$
$$a_n y_{n+k} + a_{n-1} y_{n+k-1} + \cdots + a_0 y_k = c,\ c \in \mathbb{R} - \{0\}$$

vyhovuje rovnici

$$a_n(x_{n+k} + y_{n+k}) + a_{n-1}(x_{n+k-1} + y_{n+k-1}) + \cdots \\ \cdots + a_0(x_k + y_k) = 2c,$$

zejména pak nevyhovuje původní nehomogenní rovnici. Množina řešení však tvoří afinní prostor, viz 4.1.

vii) Je to vektorový prostor, právě když $c = 0$. Vezmeme-li dvě funkce $f$ a $g$ z dané množiny, pak $(f+g)(1) = (f+g)(2) = f(1) + g(1) = 2c$. Má-li funkce $f + g$ být prvkem dané množiny, musí být $(f + g)(1) = c$, tedy $2c = c$, tedy $c = 0$. □

**2.32.** Zjistěte, zda je množina

$$U_1 = \{(x_1, x_2, x_3) \in \mathbb{R}^3;\ |x_1| = |x_2| = |x_3|\}$$

podprostorem vektorového prostoru $\mathbb{R}^3$ a množina

$$U_2 = \{ax^2 + c;\ a, c \in \mathbb{R}\}$$

podprostorem prostoru polynomů stupně nejvýše 2.

Každá podmnožina lineárně nezávislé množiny $M$ je samozřejmě také lineárně nezávislá (požadujeme stejné podmínky na méně vektorů). Stejně snadno vidíme, že $M \subseteq V$ je lineárně nezávislá právě tehdy, když každá konečná podmnožina v $M$ je lineárně nezávislá.

**2.27. Generátory a podprostory.** Podmnožina $M \subseteq V$ se nazývá *vektorovým podprostorem*, jestliže spolu se zúženými operacemi sčítání a násobení skaláry je sama vektorovým prostorem, tzn. požadujeme



$$\forall a, b \in \mathbb{K},\ \forall v, w \in M,\ a \cdot v + b \cdot w \in M.$$

Rozeberme si hned několik příkladů: Prostor $m$-tic skalárů $\mathbb{R}^m$ se sčítáním a násobením po složkách je vektorový prostor nad $\mathbb{R}$, ale také vektorový prostor nad $\mathbb{Q}$. Např. pro $m = 2$ jsou vektory $(1, 0), (0, 1) \in \mathbb{R}^2$ lineárně nezávislé, protože z

$$a \cdot (1, 0) + b \cdot (0, 1) = (0, 0)$$

plyne $a = b = 0$. Dále vektory $(1, 0), (\sqrt{2}, 0) \in \mathbb{R}^2$ jsou lineárně závislé nad $\mathbb{R}$, protože $\sqrt{2} \cdot (1, 0) = (\sqrt{2}, 0)$, ovšem nad $\mathbb{Q}$ jsou lineárně nezávislé! Nad $\mathbb{R}$ tedy tyto dva vektory „generují“ jednorozměrný podprostor, zatímco nad $\mathbb{Q}$ je „větší“.

Polynomy stupně nejvýše $m$ tvoří vektorový prostor $\mathbb{R}_m[x]$. Polynomy můžeme chápat jako zobrazení $f : \mathbb{R} \to \mathbb{R}$ a sčítání a násobení skaláry definujeme takto: $(f + g)(x) = f(x) + g(x)$, $(a \cdot f)(x) = a \cdot f(x)$. Polynomy všech stupňů také tvoří vektorový prostor $\mathbb{R}_\infty[x]$ a $\mathbb{R}_m[x] \subseteq \mathbb{R}_n[x]$ je vektorový podprostor pro všechna $m \leq n \leq \infty$. Podprostory jsou také např. všechny sudé polynomy nebo liché polynomy, tj. polynomy splňující $f(-x) = \pm f(x)$.

Úplně analogicky jako u polynomů můžeme definovat strukturu vektorového prostoru na množině všech zobrazení $\mathbb{R} \to \mathbb{R}$ nebo všech zobrazení $M \to V$ libovolné pevně zvolené množiny $M$ do vektorového prostoru $V$.

Protože podmínka v definici podprostoru obsahuje pouze



univerzální kvantifikátory, je jistě průnik podprostorů opět podprostor. Snadno to ověříme i přímo: Nechť $W_i$, $i \in I$, jsou vektorové podprostory ve $V$, $a, b \in \mathbb{K}$, $u, v \in \cap_{i \in I} W_i$. Pak pro všechna $i \in I$, $a \cdot u + b \cdot v \in W_i$, to ale znamená, že $a \cdot u + b \cdot v \in \cap_{i \in I} W_i$.

Zejména je tedy podprostorem průnik $\langle M \rangle$ všech podprostorů $W \subseteq V$, které obsahují předem danou množinu vektorů $M \subseteq V$.

Říkáme, že množina $M$ *generuje* podprostor $\langle M \rangle$, nebo že prvky $M$ jsou *generátory* podprostoru $\langle M \rangle$.

Zformulujme opět několik jednoduchých tvrzení o generování podprostorů:

**Tvrzení.** *Pro každou neprázdnou podmnožinu $M \subseteq V$ platí*

*(1) $\langle M \rangle = \{a_1 \cdot u_1 + \ldots + a_k \cdot u_k;\ k \in \mathbb{N}, a_i \in \mathbb{K}, u_j \in M, j = 1, \ldots, k\}$;*

*(2) $M = \langle M \rangle$, právě když $M$ je vektorový podprostor;*

*(3) jestliže $N \subseteq M$, pak $\langle N \rangle \subseteq \langle M \rangle$ je vektorový podprostor.*

*Podprostor $\langle \emptyset \rangle$ generovaný prázdnou podmnožinou je triviální podprostor $\{0\} \subseteq V$.*

Důkaz. (1) Množina všech lineárních kombinací

$$a_1 u_1 + \cdots + a_k u_k$$

na pravé straně (1) je jistě vektorový podprostor a samozřejmě obsahuje $M$. Naopak, každá z jednotlivých lineárních kombinací nutně musí být v $\langle M \rangle$ a první tvrzení je dokázáno.

**Řešení.** Množina $U_1$ není vektorovým (pod)prostorem. Vidíme např., že je

$$(1,1,1)+(-1,1,1)=(0,2,2)\notin U_1.$$

Množina $U_2$ ovšem podprostor tvoří (nabízí se přirozené ztotožnění s $\mathbb{R}^2$), protože

$$(a_1x^2+c_1)+(a_2x^2+c_2)=(a_1+a_2)x^2+(c_1+c_2),$$
$$k\cdot(ax^2+c)=(ka)x^2+kc$$

pro všechna čísla $a_1, c_1, a_2, c_2, a, c, k \in \mathbb{R}$. □

### G. Lineární závislost a nezávislost, báze

**2.33.** Výpočtem determinantu vhodné matice rozhodněte o lineární nezávislosti vektorů $(1,2,3,1)$, $(1,0,-1,1)$, $(2,1,-1,3)$ a $(0,0,3,2)$.

**Řešení.** Protože je determinant

$$\begin{vmatrix}1&2&3&1\\1&0&-1&1\\2&1&-1&3\\0&0&3&2\end{vmatrix}=10\neq 0$$

nenulový, jsou uvedené vektory lineárně nezávislé. □

**2.34.** Nechť jsou dány libovolné lineárně nezávislé vektory $u, v, w, z$ ve vektorovém prostoru $V$. Rozhodněte, zda jsou ve $V$ lineárně závislé či nezávislé vektory

$$u-2v,\ 3u+w-z,\ u-4v+w+2z,\ 4v+8w+4z.$$

**Řešení.** Uvažované vektory jsou lineárně nezávislé právě tehdy, když jsou lineárně nezávislé vektory $(1,-2,0,0)$, $(3,0,1,-1)$, $(1,-4,1,2)$, $(0,4,8,4)$ v $\mathbb{R}^4$. Je však

$$\begin{vmatrix}1&-2&0&0\\3&0&1&-1\\1&-4&1&2\\0&4&8&4\end{vmatrix}=-36\neq 0,$$

tudíž jsou uvažované vektory lineárně nezávislé. □

**2.35.** Určete všechny konstanty $a \in \mathbb{R}$ takové, aby polynomy $ax^2+x+2$, $-2x^2+ax+3$ a $x^2+2x+a$ byly lineárně závislé (ve vektorovém prostoru $P_3[x]$ polynomů jedné proměnné stupně nejvýše 3 nad reálnými čísly).

**Řešení.** V bázi $1, x, x^2$ jsou souřadnice zadaných vektorů (polynomů) následující: $(a,1,2)$, $(-2,a,3)$, $(1,2,a)$. Polynomy budou lineárně závislé, právě když bude mít matice, jejíž řádky jsou tvořeny souřadnicemi zadaných vektorů, menší hodnost, než je počet vektorů. V tomto případě tedy hodnost dvě a menší. V případě čtvercové matice nižší

Tvrzení (2) vyplývá okamžitě z (1) a z definice vektorového podprostoru a obdobně je z prvního tvrzení zřejmé i tvrzení třetí.

Konečně, nejmenší vektorový podprostor je $\{0\}$, protože prázdnou množinu obsahují všechny podprostory a každý z nich obsahuje vektor 0. □

**2.28. Součty podprostorů.** Když už máme představu o generátorech a jimi vytvářených podprostorech, měli bychom rozumět i možnostem, jak několik podprostorů může vytvářet celý vektorový prostor $V$.



SOUČTY PODPROSTORŮ

Nechť $V_i$, $i \in I$, jsou podprostory ve $V$. Pak podprostor generovaný jejich sjednocením, tj. $\langle \cup_{i\in I} V_i \rangle$, nazýváme *součtem podprostorů* $V_i$. Značíme $\sum_{i\in I} V_i$. Zejména pro konečný počet podprostorů $V_1, \ldots, V_k \subseteq V$ píšeme

$$V_1+\cdots+V_k=\langle V_1\cup V_2\cup\cdots\cup V_k\rangle.$$

Vidíme, že každý prvek v uvažovaném součtu podprostorů můžeme vyjádřit jako lineární kombinaci vektorů z podprostorů $V_i$. Protože však je sčítání vektorů komutativní, lze k sobě poskládat členy patřící do stejného podprostoru a pro konečný součet $k$ podprostorů tak dostáváme

$$V_1+V_2+\cdots+V_k=\{v_1+\cdots+v_k;\ v_i\in V_i, i=1,\ldots,k\}.$$

Součet $W=V_1+\cdots+V_k\subseteq V$ se nazývá *přímý součet* podprostorů, jsou-li průniky všech dvojic triviální, tj. $V_i\cap V_j=\{0\}$ pro všechna $i\neq j$. Ukážeme, že v takovém případě lze každý vektor $w\in W$ napsat právě jedním způsobem jako součet

$$w=v_1+\cdots+v_k,$$

kde $v_i\in V_i$. Skutečně, pokud by tento vektor šlo zároveň vyjádřit jako $w=v_1'+\cdots+v_k'$, potom

$$0=w-w=(v_1-v_1')+\cdots+(v_k-v_k').$$

Pokud bude $v_i-v_i'$ první nenulový člen na pravé straně, pak tento vektor z $V_i$ umíme vyjádřit pomocí vektorů z ostatních podprostorů. To je ale ve sporu s předpokladem, že $V_i$ má se všemi ostatními nulový průnik. Jedinou možností tedy je, že všechny vektory na pravé straně jsou nulové a tedy je rozklad $w$ jednoznačný.

Pro přímé součty podprostorů píšeme

$$W=V_1\oplus\cdots\oplus V_k=\oplus_{i=1}^k V_i.$$

**2.29. Báze.** Nyní máme vše připravené pro pochopení minimálních množin generátorů tak, jak jsme se s nimi vypořádali v rovině $\mathbb{R}^2$.

BÁZE VEKTOROVÝCH PROSTORŮ

Podmnožina $M\subseteq V$ se nazývá *báze vektorového prostoru* $V$, jestliže $\langle M\rangle = V$ a $M$ je lineárně nezávislá.

Vektorový prostor, který má konečnou bázi, nazýváme *konečně rozměrný*, počet prvků báze nazýváme *dimenzí* $V$. Nemá-li $V$ konečnou bázi, říkáme, že $V$ je *nekonečně rozměrný*. Píšeme $\dim V=k$, $k\in\mathbb{N}$, případně $k=\infty$.

hodnost než je počet řádků je ekvivalentní nulovosti determinantu dané matice. Podmínka na $a$ tedy zní

$$\begin{vmatrix} a & 1 & 2 \\ -2 & a & 3 \\ 1 & 2 & a \end{vmatrix} = 0,$$

tj. $a$ bude kořenem polynomu $a^3 - 6a - 5 = (a+1)(a^2 - a - 5)$, tj. úloha má tři řešení $a_1 = -1$, $a_{2,3} = \frac{1 \pm \sqrt{21}}{2}$. □

**2.36.** Vektory $(1, 2, 1)$, $(-1, 1, 0)$, $(0, 1, 1)$ jsou lineárně nezávislé, a proto společně tvoří bázi $\mathbb{R}^3$. (v bázi je nutné zadat i jejich pořadí). Každý trojrozměrný vektor je tak nějakou jejich lineární kombinací. Jakou jejich lineární kombinací je vektor $(1, 1, 1)$, nebo-li jaké jsou souřadnice vektoru $(1, 1, 1)$ v bázi dané zmíněnými vektory?

**Řešení.** Hledáme $a, b, c \in \mathbb{R}$ taková, aby

$$a(1, 2, 1) + b(-1, 1, 0) + c(0, 1, 1) = (1, 1, 1).$$

Rovnost musí platit v každé souřadnici, dostáváme tak soustavu tří lineárních rovnic o třech neznámých:

$$\begin{array}{rcrcrcl} a & - & b & & & = & 1, \\ 2a & + & b & + & c & = & 1, \\ a & & & + & c & = & 1, \end{array}$$

jejímž vyřešením získáme $a = \frac{1}{2}$, $b = -\frac{1}{2}$, $c = \frac{1}{2}$. Je tedy

$$(1, 1, 1) = \frac{1}{2} \cdot (1, 2, 1) - \frac{1}{2} \cdot (-1, 1, 0) + \frac{1}{2} \cdot (0, 1, 1),$$

neboli souřadnice vektoru $(1, 1, 1)$ v bázi $((1, 2, 1), (-1, 1, 0), (0, 1, 1))$ jsou $\left(\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}\right)$. □

**2.37.** Uvažme komplexní čísla $\mathbb{C}$ jako reálný vektorový prostor. Určete souřadnice čísla $2+i$ v bázi dané kořeny polynomu $x^2 + x + 1$.

**Řešení.** Protože kořeny polynomu jsou $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ a $-\frac{1}{2} - i\frac{\sqrt{3}}{2}$, máme určit souřadnice $(a, b)$ vektoru $2+i$ v bázi $(-\frac{1}{2} + i\frac{\sqrt{3}}{2},\ -\frac{1}{2} - i\frac{\sqrt{3}}{2})$. Tato reálná čísla $a, b$ jsou jednoznačně určena požadavkem

$$a \cdot (-\frac{1}{2} + i\frac{\sqrt{3}}{2}) + b \cdot (-\frac{1}{2} - i\frac{\sqrt{3}}{2}) = 2 + i.$$

Rozepsáním rovnosti zvlášť pro reálnou a imaginární složku dostáváme soustavu dvou lineárních rovnic o dvou neznámých:

$$\begin{array}{rcrcl} -\frac{1}{2}a & - & \frac{1}{2}b & = & 2 \\ \frac{\sqrt{3}}{2}a & - & \frac{\sqrt{3}}{2}b & = & 1. \end{array}$$

Jejím vyřešením získáme $a = -2 + \frac{\sqrt{3}}{3}$, $b = -2 - \frac{\sqrt{3}}{3}$, hledané souřadnice tedy jsou $(-2 + \frac{1}{\sqrt{3}}, -2 - \frac{1}{\sqrt{3}})$. □

**2.38. Poznámka.** Jak pozorný čtenář jistě postřehl, úloha není zadána jednoznačně, nemáme totiž zadáno pořadí kořenů polynomu, tudíž ani pořadí bázových vektorů. Výsledek je tedy dán až na změnu pořadí souřadnic.



Abychom s takovou definicí dimenze mohli být spokojeni, potřebujeme vědět, že různé báze téhož prostoru budou mít vždy stejný počet prvků. To skutečně brzy dokážeme. Všimněme si hned, že triviální podprostor je generován prázdnou množinou, která je „prázdnou" bází. Má tedy triviální podprostor dimenzi nulovou.

Bázi $k$-rozměrného prostoru budeme obvykle zapisovat jako uspořádanou $k$-tici $\underline{v} = (v_1 \dots, v_k)$ bázových vektorů. Jde tu především o zavedení konvence: U konečně rozměrných podprostorů budeme totiž vždy uvažovat bázi včetně zadaného pořadí prvků, i když jsme to takto, striktně vzato, nedefinovali.

Zjevně, je-li $(v_1, \dots, v_n)$ bází $V$, je celý prostor $V$ přímým součtem jednorozměrných podprostorů

$$V = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle.$$

Okamžitým důsledkem výše odvozené jednoznačnosti rozkladu jakéhokoliv vektoru ve $V$ do komponent v přímém součtu dává jednoznačné vyjádření

$$w = x_1 v_1 + \cdots + x_n v_n$$

a dovoluje nám tedy po volbě báze opět vidět vektory jako $n$–tice skalárů. K tomuto pohledu se vrátíme vzápětí v odstavci 2.33, jak jen dokončíme diskusi existence bází a součtů podprostorů v obecné poloze.

**2.30. Věta.** *Z libovolné konečné množiny generátorů vektorového prostoru $V$ lze vybrat bázi. Každá báze konečněrozměrného prostoru $V$ má přitom stejný počet prvků.*

Důkaz. První tvrzení ukážeme snadno indukcí přes počet generátorů $k$.



Jedině nulový podprostor nepotřebuje žádný generátor a tedy umíme vybrat prázdnou bázi. Naopak, nulový vektor vybrat nesmíme (generátory by byly lineárně závislé) a nic jiného už v podprostoru není.

Abychom měli indukční krok přirozenější, probereme ještě přímo případ $k = 1$. Máme $V = \langle \{v\} \rangle$ a $v \neq 0$, protože $\{v\}$ je lineárně nezávislá množina vektorů. Pak je ovšem $\{v\}$ zároveň báze vektorového prostoru $V$.

Předpokládejme, že tvrzení platí pro $k = n$, a uvažme $V = \langle v_1, \dots, v_{n+1} \rangle$. Jsou-li $v_1, \dots, v_{n+1}$ lineárně nezávislé, pak tvoří bázi. V opačném případě existuje index $i$ takový, že

$$v_i = a_1 v_1 + \cdots + a_{i-1} v_{i-1} + a_{i+1} v_{i+1} + \cdots + a_{n+1} v_{n+1}.$$

Pak ovšem $V = \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_{n+1} \rangle$ a již umíme vybrat bázi (podle indukčního předpokladu).

Zbývá ověřit, že báze mají vždy stejný počet prvků. Uvažujme bázi $(v_1, \dots, v_n)$ prostoru $V$ a libovolný nenulový vektor

$$u = a_1 v_1 + \cdots + a_n v_n \in V$$

s $a_i \neq 0$ pro jisté $i$. Pak

$$v_i = \frac{1}{a_i}\big(u - (a_1 v_1 + \cdots + a_{i-1} v_{i-1} + a_{i+1} v_{i+1} + \cdots + a_n v_n)\big),$$

a proto také $\langle u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n \rangle = V$.

Ověříme, že je to opět báze: Kdyby přidáním $u$ k lineárně nezávislým vektorům $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$ vznikly lineárně závislé vektory, pak by $u$ bylo jejich lineární kombinací. To by znamenalo

$$V = \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n \rangle,$$

což není možné.

Dále se na tomto místě vyjádřeme k tzv. *„usměrňování“* zlomků, tedy odstraňování odmocnin z jejich jmenovatele. Autoři nemají vyhraněný názor, zda by se usměrňovat mělo, či ne (Je hezčí $\frac{\sqrt{3}}{3}$ nebo $\frac{1}{\sqrt{3}}$?). V některých případech však je usměrňování nežádoucí: ze zlomku $\frac{6}{\sqrt{35}}$ okamžitě odečteme, že jeho hodnota je o něco málo větší než 1 (neboť $\sqrt{35}$ je jen o málo menší než 6), kdežto z usměrněného zlomku $\frac{6\sqrt{35}}{35}$ nevidíme na první pohled nic.

*2.39.* Uvažme komplexní čísla $\mathbb{C}$ jako reálný vektorový prostor. Určete souřadnice čísla $2+i$ v bázi dané kořeny polynomu $x^2 - x + 1$.

*2.40.* Pro jaké hodnoty parametrů $a, b, c \in \mathbb{R}$ jsou vektory $(1, 1, a, 1)$, $(1, b, 1, 1)$, $(c, 1, 1, 1)$ lineárně závislé?

*2.41.* Nechť je dán vektorový prostor $V$ a nějaká jeho báze složená z vektorů $u, v, w, z$. Zjistěte, zda jsou vektory

$$u - 3v + z, \quad v - 5w - z, \quad 3w - 7z, \quad u - w + z$$

lineárně (ne)závislé.

*2.42.* Doplňte vektory $1 - x^2 + x^3$, $1 + x^2 + x^3$, $1 - x - x^3$ na bázi prostoru polynomů stupně nejvýše 3.

**2.43.** Tvoří matice

$$\begin{pmatrix} 1 & 0 \\ 1 & -2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 4 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -5 & 0 \\ 3 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & -2 \\ 0 & 3 \end{pmatrix}$$

bázi vektorového prostoru čtvercových dvourozměrných matic?

**Řešení.** Uvedené čtyři matice jsou jako vektory v prostoru $2\times2$ matic lineárně nezávislé. Vyplývá to z toho, že matice

$$\begin{pmatrix} 1 & 1 & -5 & 1 \\ 0 & 4 & 0 & -2 \\ 1 & 0 & 3 & 0 \\ -2 & -1 & 0 & 3 \end{pmatrix}$$

je tzv. regulární, což je mimochodem ekvivalentní libovolnému z následujících tvrzení: její hodnost je rovna rozměru; lze z ní pomocí řádkových elementárních transformací obdržet jednotkovou matici; existuje k ní matice inverzní; má nenulový determinant, roven 116; jí zadaná homogenní soustava lineárních rovnic má pouze nulové řešení; každý nehomogenní lineární systém s levou stranou určenou touto maticí má právě jedno řešení; obor hodnot lineárního zobrazení, jež zadává, je vektorový prostor dimenze 4; toto zobrazení je injektivní. □

**2.44.** V $\mathbb{R}^3$ jsou dány podprostory $U$ a $V$ generované po řadě vektory

$$(1, 1, -3)\,,\ (1, 2, 2) \quad \text{a} \quad (1, 1, -1)\,,\ (1, 2, 1)\,,\ (1, 3, 3)\,.$$

Nalezněte průnik těchto podprostorů.

Takže jsme dokázali, že pro libovolný nenulový vektor $u \in V$ existuje $i$, $1 \le i \le n$, takové, že $(u, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ je opět báze $V$.

Dále budeme místo jednoho vektoru $u$ uvažovat lineárně nezávislou množinu $u_1, \ldots, u_k$ a budeme postupně přidávat $u_1, u_2, \ldots$ vždy výměnou za vhodné $v_i$ podle předchozího postupu. Musíme přitom ověřit, že takové $v_i$ vždy bude existovat (tj. že se nebudou vektory $u$ vyměňovat vzájemně). Předpokládejme tedy, že již máme umístěné $u_1, \ldots, u_\ell$. Pak se $u_{\ell+1}$ jistě vyjádří jako lineární kombinace těchto vektorů a zbylých $v_j$. Pokud by pouze koeficienty u $u_1, \ldots, u_\ell$ byly nenulové, znamenalo by to, že již samy vektory $u_1, \ldots, u_{\ell+1}$ byly lineárně závislé, což je ve sporu s našimi předpoklady.

Pro každé $k \le n$ tak po $k$ krocích získáme bázi, ve které z původní báze došlo k výměně $k$ vektorů za nové. Pokud by $k > n$, pak již v $n$-tém kroku obdržíme bázi vybranou z nových vektorů $u_i$, což znamená, že tyto nemohou být lineárně nezávislé. Zejména tedy není možné, aby dvě báze měly různý počet prvků. □

Ve skutečnosti jsme dokázali silnější tvrzení, tzv. *Steinitzovu větu o výměně*, která říká, že pro každou konečnou bázi $\underline{v}$ a každý systém lineárně nezávislých vektorů ve $V$ umíme najít podmnožinu bázových vektorů $v_i$, po jejichž záměně za zadané nové vektory opět dostaneme bázi.

**2.31. Důsledky Steinitzovy věty o výměně.** Díky možnosti volně volit a vyměňovat bázové vektory můžeme okamžitě dovodit pěkné (a intuitivně snad také očekávané) vlastnosti bází vektorových prostorů:



**Tvrzení.** *(1) Každé dvě báze konečně rozměrného vektorového prostoru mají stejný počet vektorů, tzn. že naše definice dimenze nezávisí na volbě báze.*
*(2) Má-li $V$ konečnou bázi, lze každou lineárně nezávislou množinu doplnit do báze.*
*(3) Báze konečně rozměrných vektorových prostorů jsou právě maximální lineárně nezávislé množiny.*
*(4) Báze prostoru s konečnou dimenzí jsou právě minimální množiny generátorů.*

Malinko složitější, ale nyní snadno zvládnutelná, je situace kolem dimenzí podprostorů a jejich součtů:

**Důsledek.** *Nechť $W, W_1, W_2 \subseteq V$ jsou podprostory v prostoru $V$ konečné dimenze. Pak platí*

*(1)* $\dim W \le \dim V$,
*(2)* $V = W$, *právě když* $\dim V = \dim W$,
*(3)* $\dim W_1 + \dim W_2 = \dim(W_1 + W_2) + \dim(W_1 \cap W_2)$.



Důkaz. Zbývá dokázat pouze poslední tvrzení. To je zřejmé, pokud je dimenze jednoho z prostorů nulová. Předpokládejme tedy $\dim W_1 = r \ge 1$, $\dim W_2 = s \ge 1$ a nechť $(w_1 \ldots, w_t)$ je báze $W_1 \cap W_2$ (nebo prázdná množina, pokud je průnik triviální).

Podle Steinitzovy věty o výměně lze tuto bázi průniku doplnit na bázi $(w_1, \ldots, w_t, u_{t+1}, \ldots, u_r)$ pro $W_1$ a na bázi $(w_1 \ldots, w_t, v_{t+1}, \ldots, v_s)$ pro $W_2$. Vektory

$$w_1, \ldots, w_t, u_{t+1}, \ldots, u_r, v_{t+1} \ldots, v_s$$

**Řešení.** Podprostor $V$ má dimenzi pouze 2 (nejedná se tedy o celý prostor $\mathbb{R}^3$), neboť

$$\begin{vmatrix} 1 & 1 & -1 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ -1 & 1 & 3 \end{vmatrix} = 0$$

a neboť libovolná dvojice z uvažovaných třech vektorů je očividně lineárně nezávislá. Stejně snadno vidíme, že také podprostor $U$ má dimenzi 2. Současně je

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ -3 & 2 & -1 \end{vmatrix} = 2 \neq 0,$$

a proto vektor $(1, 1, -1)$ nemůže náležet do podprostoru $U$. Průnikem rovin procházejících počátkem (dvojrozměrných podprostorů) v trojrozměrném prostoru musí být alespoň přímka. V našem případu je jím právě přímka (podprostory nejsou totožné). Určili jsme dimenzi průniku – je jednodimenzionální. Všimneme-li si, že

$$1 \cdot (1, 1, -3) + 2 \cdot (1, 2, 2) = (3, 5, 1) = 1 \cdot (1, 1, -1) + 2 \cdot (1, 2, 1)\,,$$

dostáváme vyjádření hledaného průniku ve tvaru množiny všech skalárních násobků vektoru $(3, 5, 1)$ (jedná se o přímku procházející počátkem s tímto směrovým vektorem). □

**2.45.** Stanovte vektorový podprostor (prostoru $\mathbb{R}^4$) generovaný vektory $u_1 = (-1, 3, -2, 1)$, $u_2 = (2, -1, -1, 2)$, $u_3 = (-4, 7, -3, 0)$, $u_4 = (1, 5, -5, 4)$ vybráním nějaké maximální množiny lineárně nezávislých vektorů $u_i$ (tj. vybráním báze).

**Řešení.** Sepíšeme vektory $u_i$ do sloupců matice a obdrženou matici upravíme pomocí řádkových elementárních transformací. Takto získáme

$$\begin{pmatrix} -1 & 2 & -4 & 1 \\ 3 & -1 & 7 & 5 \\ -2 & -1 & -3 & -5 \\ 1 & 2 & 0 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 4 \\ -1 & 2 & -4 & 1 \\ 3 & -1 & 7 & 5 \\ -2 & -1 & -3 & -5 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 4 \\ 0 & 4 & -4 & 5 \\ 0 & -7 & 7 & -7 \\ 0 & 3 & -3 & 3 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 1 & 2 & 0 & 4 \\ 0 & 1 & -1 & 5/4 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 4 \\ 0 & 1 & -1 & 5/4 \\ 0 & 0 & 0 & -1/4 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Odtud vyplývá, že lineárně nezávislé jsou právě vektory $u_1, u_2, u_4$, tj. právě ty vektory odpovídající sloupcům, které obsahují první nenulové číslo nějakého řádku. Navíc odsud plyne (viz třetí sloupec)

$$2 \cdot (-1, 3, -2, 1) - (2, -1, -1, 2) = (-4, 7, -3, 0). \qquad \square$$

**2.46.** Ve vektorovém prostoru $\mathbb{R}^4$ jsou dány trojrozměrné podprostory

$$U = \langle u_1, u_2, u_3 \rangle, \qquad V = \langle v_1, v_2, v_3 \rangle,$$

jistě generují $W_1 + W_2$. Ukážeme, že jsou přitom lineárně nezávislé. Nechť tedy

$$a_1 w_1 + \cdots + a_t w_t + b_{t+1} u_{t+1} + \ldots$$
$$\cdots + b_r u_r + c_{t+1} v_{t+1} + \cdots + c_s v_s = 0.$$

Pak nutně

$$-(c_{t+1} \cdot v_{t+1} + \cdots + c_s \cdot v_s) =$$
$$= a_1 \cdot w_1 + \cdots + a_t \cdot w_t + b_{t+1} \cdot u_{t+1} + \cdots + b_r \cdot u_r$$

musí patřit do $W_1 \cap W_2$. To ale má za následek, že

$$b_{t+1} = \cdots = b_r = 0,$$

protože tak jsem doplňovali naše báze. Pak ovšem i

$$a_1 \cdot w_1 + \cdots + a_t \cdot w_t + c_{t+1} \cdot v_{t+1} + \cdots + c_s \cdot v_s = 0,$$

a protože příslušné vektory tvoří bázi $W_2$, jsou všechny koeficienty nulové.

Tvrzení (3) nyní vyplývá z přímého přepočítání generátorů. □

**2.32. Příklady.** (1) $\mathbb{K}^n$ má (jako vektorový prostor nad $\mathbb{K}$) dimenzi $n$. Bází je např. $n$-tice vektorů

$$((1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1)).$$

Tuto bázi nazýváme *standardní báze v* $\mathbb{K}^n$. Všimněme si, že v případě konečného pole skalárů, např. $\mathbb{Z}_k$, má celý vektorový prostor $\mathbb{K}^n$ jen konečný počet $k^n$ prvků.

(2) $\mathbb{C}$ jako vektorový prostor nad $\mathbb{R}$ má dimenzi 2, bázi tvoří např. čísla 1 a $i$.

(3) $\mathbb{K}_m[x]$, tj. prostor polynomů stupně nejvýše $m$, má dimenzi $m + 1$, bází je např. posloupnost $1, x, x^2, \ldots, x^m$.

Vektorový prostor $\mathbb{K}[x]$ všech polynomů má dimenzi $\infty$, umíme však ještě stále najít bázi (i když s nekonečně mnoha prvky): $1, x, x^2, \ldots$.

(4) Vektorový prostor $\mathbb{R}$ nad $\mathbb{Q}$ má dimenzi $\infty$ a nemá spočetnou bázi.

(5) Vektorový prostor všech zobrazení $f : \mathbb{R} \to \mathbb{R}$ má také dimenzi $\infty$ a nemá spočetnou bázi.

**2.33. Souřadnice vektorů.** Jestliže pevně zvolíme bázi $(v_1, \ldots, v_n)$ konečně rozměrného prostoru $V$, pak můžeme každý vektor $w \in V$ vyjádřit jako lineární kombinaci $v = a_1 v_1 + \cdots + a_n v_n$. Předpokládejme, že to uděláme dvěma způsoby:



$$w = a_1 v_1 + \cdots + a_n v_n = b_1 v_1 + \cdots + b_n v_n.$$

Potom ale

$$0 = (a_1 - b_1) \cdot v_1 + \cdots + (a_n - b_n) \cdot v_n,$$

a proto $a_i = b_i$ pro všechna $i = 1, \ldots, n$. Dospěli jsme proto k závěru:

V konečně rozměrném vektorovém prostoru lze každý vektor zadat právě jediným způsobem jako lineární kombinaci bázových vektorů. Koeficienty této jediné lineární kombinace vyjadřující daný vektor $w \in V$ ve zvolené bázi $\underline{v} = (v_1, \ldots, v_n)$ se nazývají *souřadnice vektoru* $w$ v této bázi.

Kdykoliv budeme mluvit o souřadnicích $(a_1, \ldots, a_n)$ vektoru $w$, které vyjadřujeme jako posloupnost, musíme mít pevně zvolenu i posloupnost bázových vektorů $\underline{v} = (v_1, \ldots, v_n)$. Jakkoliv jsme tedy báze zavedli jako minimální množiny generátorů, ve

přičemž

$$u_1 = \begin{pmatrix}1\\1\\1\\0\end{pmatrix}, \qquad u_2 = \begin{pmatrix}1\\1\\0\\1\end{pmatrix}, \qquad u_3 = \begin{pmatrix}1\\0\\1\\1\end{pmatrix},$$

$$v_1 = \begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}, \qquad v_2 = \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \qquad v_3 = \begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}.$$

Určete dimenzi a libovolnou bázi podprostoru $U \cap V$.

**Řešení.** Do podprostoru $U \cap V$ náleží právě ty vektory, které je možné obdržet jako lineární kombinaci vektorů $u_i$ a také jako lineární kombinaci vektorů $v_i$. Hledáme tedy čísla $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{R}$ taková, aby platilo

$$x_1\begin{pmatrix}1\\1\\1\\0\end{pmatrix} + x_2\begin{pmatrix}1\\1\\0\\1\end{pmatrix} + x_3\begin{pmatrix}1\\0\\1\\1\end{pmatrix} = y_1\begin{pmatrix}1\\1\\-1\\-1\end{pmatrix} + y_2\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix} + y_3\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix},$$

tj. hledáme řešení soustavy

$$\begin{array}{rcrcrcrcrcr} x_1 & + & x_2 & + & x_3 & = & y_1 & + & y_2 & + & y_3, \\ x_1 & + & x_2 & & & = & y_1 & - & y_2 & - & y_3, \\ x_1 & & & + & x_3 & = & -y_1 & + & y_2 & - & y_3, \\ & & x_2 & + & x_3 & = & -y_1 & - & y_2 & + & y_3. \end{array}$$

Při maticovém zápisu této homogenní soustavy (a při zachování pořadí proměnných) je

$$\begin{pmatrix}1&1&1&-1&-1&-1\\1&1&0&-1&1&1\\1&0&1&1&-1&1\\0&1&1&1&1&-1\end{pmatrix} \sim \begin{pmatrix}1&1&1&-1&-1&-1\\0&0&-1&0&2&2\\0&-1&0&2&0&2\\0&1&1&1&1&-1\end{pmatrix} \sim$$

$$\sim \begin{pmatrix}1&1&1&-1&-1&-1\\0&1&1&1&1&-1\\0&0&-1&0&2&2\\0&0&1&3&1&1\end{pmatrix} \sim \begin{pmatrix}1&1&1&-1&-1&-1\\0&1&1&1&1&-1\\0&0&1&0&-2&-2\\0&0&0&1&1&1\end{pmatrix} \sim$$

$$\sim \begin{pmatrix}1&1&1&0&0&0\\0&1&1&0&0&-2\\0&0&1&0&-2&-2\\0&0&0&1&1&1\end{pmatrix} \sim \begin{pmatrix}1&0&0&0&0&2\\0&1&0&0&2&0\\0&0&1&0&-2&-2\\0&0&0&1&1&1\end{pmatrix}.$$

Dostáváme tak řešení

$$x_1 = -2t,\ x_2 = -2s,\ x_3 = 2s + 2t,\ y_1 = -s - t,\ y_2 = s,\ y_3 = t,$$

$t, s \in \mathbb{R}$. Odtud dosazením získáváme obecný vektor průniku

$$\begin{pmatrix}x_1 + x_2 + x_3\\x_1 + x_2\\x_1 + x_3\\x_2 + x_3\end{pmatrix} = \begin{pmatrix}0\\-2t - 2s\\2s\\2t\end{pmatrix}.$$

skutečnosti s nimi budeme pracovat jako s posloupnostmi (tedy s uspořádanými množinami, kde je pevně zadáno pořadí bázových prvků).

PŘIŘAZENÍ SOUŘADNIC VEKTORŮM

Přiřazení, které vektoru $u = a_1v_1 + \cdots + a_nv_n$ přiřadí jeho souřadnice v bázi $\underline{v}$, budeme značit stejným symbolem $\underline{v} : V \to \mathbb{K}^n$. Má tyto vlastnosti:

(1) $\underline{v}(u + w) = \underline{v}(u) + \underline{v}(w);\ \forall u, w \in V,$
(2) $\underline{v}(a \cdot u) = a \cdot \underline{v}(u);\ \forall a \in \mathbb{K}, \forall u \in V.$

Všimněme si, že operace na levých a pravých stranách těchto rovnic nejsou totožné, naopak, jde o operace na různých vektorových prostorech! Při této příležitosti se také můžeme zamyslet nad obecným případem báze $M$ (možná nekonečně rozměrného) prostoru $V$. Báze pak nemusí být spočetná, pořád ale ještě můžeme definovat zobrazení $\underline{M} : V \to \mathbb{K}^M$ (tj. souřadnice vektoru jsou zobrazení z $M$ do $\mathbb{K}$).

Uvedené vlastnosti přiřazení souřadnic jsme viděli už dříve u zobrazení, kterým jsme v geometrii roviny říkali lineární (zachovávaly naši lineární strukturu v rovině). Než se budeme věnovat podrobněji závislosti souřadnic na volbě báze, podíváme se obecněji na pojem linearity zobrazení.

**2.34. Lineární zobrazení.** Pro jakékoliv vektorové prostory (konečné i nekonečné dimenze) definujeme „linearitu“ zobrazení mezi prostory obdobně, jako jsme to viděli již v rovině $\mathbb{R}^2$:

DEFINICE LINEÁRNÍCH ZOBRAZENÍ

Nechť $V$ a $W$ jsou vektorové prostory nad týmž polem skalárů $\mathbb{K}$. Zobrazení $f : V \to W$ se nazývá *lineární zobrazení (homomorfismus)*, jestliže platí:

(1) $f(u + v) = f(u) + f(v),\ \forall u, v \in V,$
(2) $f(a \cdot u) = a \cdot f(u),\ \forall a \in \mathbb{K},\ \forall u \in V.$

Samozřejmě, že jsme taková zobrazení již viděli ve formě násobení matic:

$$f : \mathbb{K}^n \to \mathbb{K}^m, x \mapsto A \cdot x$$

s maticí typu $m/n$ nad $\mathbb{K}$.

*Obraz* $\operatorname{Im} f := f(V) \subseteq W$ je vždy vektorový podprostor, protože lineární kombinace obrazů $f(u_i)$ je obrazem lineární kombinace vektorů $u_i$ se stejnými koeficienty.

Stejně tak je vektorovým podprostorem množina všech vektorů $\operatorname{Ker} f := f^{-1}(\{0\}) \subseteq V$, protože lineární kombinace nulových obrazů bude vždy zase nulovým vektorem. Podprostor $\operatorname{Ker} f$ se nazývá *jádro lineárního zobrazení* $f$.

Lineární zobrazení, které je bijekcí, nazýváme *izomorfismus*.

Podobně jako u abstraktní definice vektorových prostorů, opět je třeba ověřit zdánlivě samozřejmá tvrzení vyplývající z axiomů:

**Tvrzení.** *Nechť $f : V \to W$ je lineární zobrazení mezi libovolnými vektorovými prostory nad týmž polem skalárů $\mathbb{K}$. Pro všechny vektory $u, u_1, \ldots, u_k \in V$ a skaláry $a_1, \ldots, a_k \in \mathbb{K}$ platí:*

*(1)* $f(0) = 0,$
*(2)* $f(-u) = -f(u),$
*(3)* $f(a_1 \cdot u_1 + \cdots + a_k \cdot u_k) = a_1 \cdot f(u_1) + \cdots + a_k \cdot f(u_k),$

Vidíme, že

$$\dim U \cap V = 2, \quad U \cap V = \left\langle \begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \end{pmatrix} \right\rangle.$$

□

**2.47.** Uveďte nějakou bázi podprostoru

$$U = \left\langle \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 3 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} -2 & -1 \\ 0 & 1 \\ 2 & 3 \end{pmatrix} \right\rangle$$

vektorového prostoru reálných matic $3 \times 2$. Tuto bázi doplňte na bázi celého prostoru.

**Řešení.** Připomeňme, že bázi podprostoru tvoří množina lineárně nezávislých vektorů, které generují uvažovaný podprostor. Protože

$$\begin{aligned} -1 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 & 1 \\ 2 & 3 \\ 4 & 5 \end{pmatrix} &= \begin{pmatrix} -1 & 0 \\ 1 & 2 \\ 3 & 4 \end{pmatrix}, \\ -2 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 & 1 \\ 2 & 3 \\ 4 & 5 \end{pmatrix} &= \begin{pmatrix} -2 & -1 \\ 0 & 1 \\ 2 & 3 \end{pmatrix}, \end{aligned}$$

celý podprostor $U$ je generován pouze prvními dvěma maticemi. Ty jsou potom lineárně nezávislé (jedna není násobkem druhé), a tak zadávají bázi. Chceme-li ji doplnit na bázi celého prostoru reálných matic $3 \times 2$, musíme najít další čtyři matice (dimenze celého prostoru je zjevně 6) takové, aby výsledná šestice byla lineárně nezávislá. Můžeme využít toho, že známe např. standardní bázi

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

prostoru reálných matic $3 \times 2$, který lze přímo ztotožnit s $\mathbb{R}^6$. Sepíšeme-li dva vektory báze $U$ a vektory standardní báze celého prostoru v tomto pořadí, výběrem prvních 6 lineárně nezávislých vektorů dostaneme hledanou bázi. Pokud však uvážíme, že kupř.

$$\begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 \\ 3 & 2 & 1 & 0 & 0 & 0 \\ 4 & 3 & 0 & 1 & 0 & 0 \\ 5 & 4 & 0 & 0 & 1 & 0 \\ 6 & 5 & 0 & 0 & 0 & 1 \end{vmatrix} = 1,$$

můžeme ihned bázového vektory

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 2 & 3 \\ 4 & 5 \end{pmatrix}$$

*(4) pro každý vektorový podprostor $V_1 \subseteq V$ je jeho obraz $f(V_1)$ vektorový podprostor ve $W$,*
*(5) pro každý podprostor $W_1 \subseteq W$ je množina*

$$f^{-1}(W_1) = \{v \in V;\ f(v) \in W_1\}$$

*vektorový podprostor ve $V$.*

Důkaz. Počítáme s využitím axiomů, definic a již dokázaných výsledků (dohledejte si případně samostatně!):

$$\begin{aligned} f(0) &= f(u-u) = f((1-1)\cdot u) = 0 \cdot f(u) = 0, \\ f(-u) &= f((-1)\cdot u) = (-1)\cdot f(u) = -f(u). \end{aligned}$$

Vlastnost (3) se ověří snadno z definičního vztahu pro dva sčítance indukcí přes počet sčítanců. Z platnosti (3) nyní plyne, že $\langle f(V_1) \rangle = f(V_1)$, je to tedy vektorový podprostor.

Je-li naopak $f(u) \in W_1$ a $f(v) \in W_1$, pak pro libovolné skaláry bude i $f(a \cdot u + b \cdot v) = a \cdot f(u) + b \cdot f(v) \in W_1$. □

**2.35. Jednoduché důsledky.**

(1) Složení $g \circ f : V \to Z$ dvou lineárních zobrazení $f : V \to W$ a $g : W \to Z$ je opět lineární zobrazení.
(2) Lineární zobrazení $f : V \to W$ je izomorfismus, právě když $\operatorname{Im} f = W$ a $\operatorname{Ker} f = \{0\} \subseteq V$. Inverzní zobrazení k izomorfismu je opět izomorfismus.
(3) Pro libovolné podprostory $V_1, V_2 \subseteq V$ a lineární zobrazení $f : V \to W$ platí

$$\begin{aligned} f(V_1 + V_2) &= f(V_1) + f(V_2), \\ f(V_1 \cap V_2) &\subseteq f(V_1) \cap f(V_2). \end{aligned}$$

(4) Zobrazení „přiřazení souřadnic“ $\underline{u} : V \to \mathbb{K}^n$ dané libovolně zvolenou bází $\underline{u} = (u_1, \ldots, u_n)$ vektorového prostoru $V$ je izomorfismus.
(5) Dva konečně rozměrné vektorové prostory jsou izomorfní, právě když mají stejnou dimenzi.
(6) Složení dvou izomorfismů je izomorfismus.

Důkaz. Ověření prvního tvrzení je velmi snadné cvičení.



Pro důkaz druhého si uvědomme, že je-li $f$ lineární bijekce, pak je vektor $w$ vzorem lineární kombinace $au + bv$, tj. $w = f^{-1}(au + bv)$, právě když

$$f(w) = au + bv = f(a \cdot f^{-1}(u) + b \cdot f^{-1}(v)).$$

Je tedy také $w = af^{-1}(u) + bf^{-1}(v)$ a tedy je inverze k lineární bijekci opět lineární zobrazení.

Dále, $f$ je surjektivní, právě když $\operatorname{Im} f = W$, a pokud $\operatorname{Ker} f = \{0\}$, pak $f(u) = f(v)$ zaručuje $f(u - v) = 0$, tj. $u = v$. Je tedy v tom případě $f$ injektivní.

Další tvrzení se dokáže snadno přímo z definic. Najděte si protipříklad, že v dokazované inkluzi opravdu nemusí nastat rovnost! Zbývající body jsou již zřejmé. □

**2.36. Opět souřadnice.** Uvažujme libovolné vektorové prostory $V$ a $W$ nad $\mathbb{K}$ s $\dim V = n$, $\dim W = m$ a mějme lineární zobrazení $f : V \to W$. Pro každou volbu bází $\underline{u} = (u_1, \ldots, u_n)$ na $V$, $\underline{v} = (v_1, \ldots, v_n)$ na $W$ máme k dispozici příslušná přiřazení souřadnic a celou situaci několika právě zmíněných zobrazení zachycuje následující diagram:



podprostoru $U$ doplnit maticemi (vektory prostoru matic)

$$\begin{pmatrix}0&0\\1&0\\0&0\end{pmatrix},\quad \begin{pmatrix}0&0\\0&1\\0&0\end{pmatrix},\quad \begin{pmatrix}0&0\\0&0\\1&0\end{pmatrix},\quad \begin{pmatrix}0&0\\0&0\\0&1\end{pmatrix}$$

na bázi. Upozorněme, že výše uvedený determinant lze vyčíslit velmi snadno – je roven součinu prvků na diagonále, neboť matice je v dolním trojúhelníkovém tvaru (nad diagonálou jsou všechny prvky nulové). □

### H. Lineární zobrazení

Jak popsat analyticky shodná zobrazení v rovině či prostoru jako je rotace, osová symetrie či zrcadlení, nebo projekci třírozměrného prostoru na dvojrozměrné plátno? Jak popsat zvětšení obrázku? Co mají společného? Jsou to všechno lineární zobrazení. Znamená to, že zachovávají jistou strukturu roviny či prostoru. Jakou strukturu? Strukturu vektorového prostoru. Každý bod v rovině je popsán dvěma v prostoru pak třemi souřadnicemi. Pokud zvolíme počátek souřadnic, tak má smysl mluvit o tom, že nějaký bod je dvakrát dál od počátku stejným směrem než jiný bod. Také víme, kam se dostaneme, posuneme-li se o nějaký úsek v jistém směru a pak o jiný úsek v jiném směru. Tyto vlastnosti můžeme zformalizovat, hovoříme-li o vektorech v rovině, či prostoru a o jejich násobcích, či součtech. Lineární zobrazení má pak tu vlastnost, že obraz součtu vektorů je součet obrazů sčítaných vektorů a obraz násobku vektoru je ten stejný násobek obrazu násobeného vektoru. Tyto vlastnosti právě mají zobrazení zmíněná v úvodu tohoto odstavce. Takové zobrazení je pak jednoznačně určeno tím, jak se chová na vektorech nějaké báze (to je v rovině obrazem dvou vektorů neležících na přímce, v prostoru obrazem tří vektorů neležích v rovině).

A jak tedy zapsat nějaké lineární zobrazení $f$ na vektorovém prostoru $V$? Začněme pro jednoduchost s rovinou $\mathbb{R}^2$: předpokládejme, že obraz bodu (vektoru) $(1,0)$ je $(a,b)$ a obraz bodu $(0,1)$ je $(c,d)$. Tím už je jednoznačně určený obraz libovolného bodu o souřadnicích $(u,v)$: $f((u,v)) = f(u(1,0)+v(0,1)) = uf(1,0)+vf(1,0) = (ua,ub)+(vc,vd) = (au+cv, bu+dv)$, což můžeme výhodně zapsat následujícím způsobem:

$$\begin{pmatrix}a&c\\b&d\end{pmatrix}\begin{pmatrix}u\\v\end{pmatrix} = \begin{pmatrix}au+cv\\bu+dv\end{pmatrix}.$$

Lineární je tedy zobrazení jednoznačně dané maticí. Navíc pokud máme další lineární zobrazení $g$, dané maticí $\left(\begin{smallmatrix}e&f\\g&h\end{smallmatrix}\right)$, tak snadno spočítáme (čtenář si jistě ze zájmu sám ověří), že jejich složení $g\circ f$ je dáno maticí $\left(\begin{smallmatrix}ae+fc&be+df\\ag+ch&bg+dh\end{smallmatrix}\right)$.

$$\begin{array}{ccc} V & \xrightarrow{\quad f \quad} & W \\ {\scriptstyle \underline{u}}\downarrow\simeq & & \simeq\downarrow{\scriptstyle \underline{v}} \\ \mathbb{K}^n & \xrightarrow{\quad f_{\underline{u},\underline{v}} \quad} & \mathbb{K}^m \end{array}$$

Spodní šipka $f_{\underline{u},\underline{v}}$ je definována zbylými třemi, tj. jako zobrazení jde o složení

$$f_{\underline{u},\underline{v}} = \underline{v}\circ f\circ \underline{u}^{-1}.$$

#### Matice lineárního zobrazení

Každé lineární zobrazení je jednoznačně určeno svými hodnotami na libovolné množině generátorů, zejména tedy na vektorech báze $\underline{u}$. Označme

$$\begin{aligned} f(u_1) &= a_{11}\cdot v_1 + a_{21}\cdot v_2 + \cdots + a_{m1}v_m,\\ f(u_2) &= a_{12}\cdot v_1 + a_{22}\cdot v_2 + \cdots + a_{m2}v_m,\\ &\vdots\\ f(u_n) &= a_{1n}\cdot v_1 + a_{2n}\cdot v_2 + \cdots + a_{mn}v_m, \end{aligned}$$

tj. skaláry $a_{ij}$ tvoří matici $A$, kde sloupce jsou souřadnice hodnot $f(u_j)$ zobrazení $f$ na bázových vektorech vyjádřené v bázi $\underline{v}$ na cílovém prostoru $W$.

Matici $A = (a_{ij})$ nazýváme *maticí zobrazení* $f$ v bázích $\underline{u}$, $\underline{v}$.

Pro obecný vektor $u = x_1u_1 + \cdots + x_nu_n \in V$ spočteme (vzpomeňme, že sčítání vektorů je komutativní a distributivní vůči násobení skaláry)

$$\begin{aligned} f(u) &= x_1f(u_1) + \cdots + x_nf(u_n) = \\ &= x_1(a_{11}v_1 + \cdots + a_{m1}v_m) + \cdots + \\ &\quad + x_n(a_{1n}v_1 + \cdots + a_{mn}v_m) = \\ &= (x_1a_{11} + \cdots + x_na_{1n})v_1 + \cdots + (x_1a_{m1} + \cdots + x_na_{mn})v_m. \end{aligned}$$

Pomocí násobení matic lze nyní velice snadno a přehledně zapsat hodnoty zobrazení $f_{\underline{u},\underline{v}}(w)$ definovaného jednoznačně předchozím diagramem. Připomeňme si, že vektory v $\mathbb{K}^r$ chápeme jako sloupce, tj. matice typu $r/1$

$$f_{\underline{u},\underline{v}}(\underline{u}(w)) = \underline{v}\,(f(w)) = A\cdot\underline{u}(w).$$

Naopak, máme-li pevně zvoleny báze na $V$ i $W$, pak každá volba matice $A$ typu $m/n$ zadává jednoznačně lineární zobrazení $\mathbb{K}^n \to \mathbb{K}^m$ a tedy i zobrazení $f : V \to W$. Máme-li tedy zvoleny báze prostorů $V$ a $W$, odpovídá každé volbě matice typu $m/n$ právě jedno lineární zobrazení $V \to W$. Ukázali jsme bijekci mezi maticemi příslušného rozměru a lineárními zobrazeními $V \to W$.

**2.37. Matice přechodu mezi souřadnicemi.** Jestliže za $V$ i $W$ zvolíme tentýž prostor ale s různými bázemi, a za $f$ identické zobrazení, vyjadřuje postup z předchozího odstavce vektory báze $\underline{u}$ v souřadnicích vzhledem k $\underline{v}$. Označme výslednou matici $T$. Když pak zadáme vektor $u$



$$u = x_1u_1 + \cdots + x_nu_n$$

v souřadnicích vzhledem k $\underline{u}$ a dosadíme za $u_i$ jejich vyjádření pomocí vektorů z $\underline{v}$, obdržíme souřadné vyjádření $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_n)$ téhož vektoru v bázi $\underline{v}$. Stačí k tomu přeskládat pořadí sčítanců a vyjádřit skaláry u jednotlivých vektorů báze.

Ve skutečnosti teď děláme totéž, co v předchozím odstavci pro speciální případ identického zobrazení $\mathrm{id}_V$ na vektorovém prostoru

To nás vede k tomu, abychom násobení matic definovali tímto způsobem, tedy aby aplikace zobrazení na vektor byla dána maticovým násobením matice zobrazení se zobrazovaným vektorem a aby složení zobrazení bylo dáno součinem matic jednotlivých zobrazení. Obdobně to funguje v prostorech vyšší dimenze. Zároveň tato úvaha znovu ukazuje to, co již bylo dokázáno v (2.5), totiž že násobení matic je asociativní, ale není komutativní, neboť tomu tak je u skládání zobrazení. To je tedy další z motivací, proč se zabývat vektorovými prostory.

Připomeňme si nyní, že v první kapitole jsme již pracovali s maticemi některých lineárních zobrazení v rovině $\mathbb{R}^2$, zejména rotace kolem bodu a osové symetrie (viz 1.31 a 1.32).

Nyní zkusme zapsat matice lineárních zobrazení z $\mathbb{R}^3$ do $\mathbb{R}^3$. Jak vypadá matice rotace ve třech rozměrech? Začněme speciálními (pro popis jednoduššími) rotacemi kolem souřadnicových os.

**2.48. Matice rotací kolem os v $\mathbb{R}^3$.** Napište matice zobrazení rotací o úhel $\varphi$ postupně kolem (orientovaných) os $x$, $y$, $z$ v $\mathbb{R}^3$ .

**Řešení.** Při rotaci libovolného bodu kolem dané osy (řekněme $x$) se příslušná souřadnice daného bodu nemění, v rovině dané dvěma zbylými osami pak již je rotace dána známou maticí typu 2/2.

Postupně tedy dostáváme následující matice – rotace kolem osy $z$:

$$\begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

rotace kolem osy $y$:

$$\begin{pmatrix} \cos\varphi & 0 & \sin\varphi \\ 0 & 1 & 0 \\ -\sin\varphi & 0 & \cos\varphi \end{pmatrix},$$

rotace kolem osy $x$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix}.$$

U matice rotace kolem osy $y$ máme jinak znaménko u $\varphi$. Chceme totiž, stejně jako u ostatních os rotaci kolem osy $y$ v kladném smyslu, tedy takovou, že pokud se díváme proti směru osy $y$, tak se svět točí proti směru hodinových ručiček. Znaménka v maticích jsou závislá na orientaci naší souřadné soustavy. Obvykle se v třírozměrném prostoru volí tzv. „pravotočivá soustava souřadnic“: položíme-li ruku na osu $x$ tak, aby prsty byly po směru osy a abychom mohli osu $x$ otočit v rovině $xy$ do osy $y$ tak, aby souhlasily jejich směry, pak palec by měl ukazovat ve směru osy $z$. V takové soustavě jde o rotaci v záporném smyslu v rovině $xz$ (tedy osa $z$ se otáčí směrem k $x$). Rozmyslete si kladný a záporný smysl rotace podél všech tří os. □

$V$. Matice tohoto identického zobrazení je $T$ a tedy nutně musí naznačený přímý výpočet dát $\bar{x} = T \cdot x$. Situace je zobrazena na diagramu:

$$\begin{array}{ccc} V & \xrightarrow{\mathrm{id}_V} & V \\ \underline{u}\downarrow\simeq & & \simeq\downarrow\underline{v} \\ \mathbb{K}^n & \xrightarrow{T=(\mathrm{id}_V)_{\underline{u},\underline{v}}} & \mathbb{K}^n \end{array}$$

Výslednou matici $T$ nazýváme *matice přechodu* od báze $\underline{u}$ vektorového prostoru $V$ k bázi $\underline{v}$ téhož prostoru.

Přímo z definice vyplývá:

VÝPOČET MATICE PŘECHODU

**Tvrzení.** *Matici $T$ přechodu od báze $\underline{u}$ k bázi $\underline{v}$ získáme tak, že souřadnice vektorů báze $\underline{u}$ v bázi $\underline{v}$ napíšeme do sloupců matice $T$.*

Funkce matice přechodu je taková, že známe-li souřadnice $x$ vektoru v bázi $\underline{u}$, pak jeho souřadnice v bázi $\underline{v}$ se obdrží vynásobením sloupce $x$ maticí přechodu (zleva). Protože inverzní zobrazení k identickému je opět totéž identické zobrazení, je matice přechodu vždy invertibilní a její inverze je právě matice přechodu opačným směrem, tj. od báze $\underline{v}$ k bázi $\underline{u}$.

**2.38. Více souřadnic.** Nyní si ukážeme, jak se skládají souřadná vyjádření lineárních zobrazení. Uvažme ještě další vektorový prostor $Z$ nad $\mathbb{K}$ dimenze $k$ s bází $\underline{w}$, lineární zobrazení $g : W \to Z$ a označme příslušnou matici $g_{\underline{v},\underline{w}}$.



$$\begin{array}{ccccc} V & \xrightarrow{f} & W & \xrightarrow{g} & Z \\ \underline{u}\downarrow\simeq & & \simeq\downarrow\underline{v} & & \simeq\downarrow\underline{w} \\ \mathbb{K}^n & \xrightarrow{f_{\underline{u},\underline{v}}} & \mathbb{K}^m & \xrightarrow{g_{\underline{v},\underline{w}}} & \mathbb{K}^k \end{array}$$

Složení $g \circ f$ na horním řádku odpovídá matici zobrazení $\mathbb{K}^n \to \mathbb{K}^k$ dole a přímo spočteme (píšeme $A$ pro matici $f$ a $B$ pro matici $g$ ve zvolených bázích):

$$\begin{aligned} g_{\underline{v},\underline{w}} \circ f_{\underline{u},\underline{v}}(x) &= \underline{w} \circ g \circ \underline{v}^{-1} \circ \underline{v} \circ f \circ \underline{u}^{-1} = \\ &= B \cdot (A \cdot x) = (B \cdot A) \cdot x = (g \circ f)_{\underline{u},\underline{w}}(x) \end{aligned}$$

pro všechna $x \in \mathbb{K}^n$. Skládání zobrazení tedy odpovídá násobení příslušných matic. Všimněte si také, že isomorfismy odpovídají právě invertibilním maticím.

Stejný postup nám dává odpověď na otázku, jak se změní matice zobrazení, změníme-li báze na definičním oboru i oboru hodnot:

$$\begin{array}{ccccccc} V & \xrightarrow{\mathrm{id}_V} & V & \xrightarrow{f} & W & \xrightarrow{\mathrm{id}_W} & W \\ \underline{u}'\downarrow\simeq & & \underline{u}\downarrow\simeq & & \simeq\downarrow\underline{v} & & \simeq\downarrow\underline{v}' \\ \mathbb{K}^n & \xrightarrow{T} & \mathbb{K}^n & \xrightarrow{f_{\underline{u},\underline{v}}} & \mathbb{K}^m & \xrightarrow{S^{-1}} & \mathbb{K}^m \end{array}$$

kde $T$ je matice přechodu od $\underline{u}'$ k $\underline{u}$ a $S$ je matice přechodu od $\underline{v}'$ k $\underline{v}$. Je-li tedy $A$ původní matice zobrazení, bude nová dána jako $A' = S^{-1}AT$.

Ve speciálním případě lineárního zobrazení $f : V \to V$, tj. zobrazení má stejný prostor $V$ jako definiční obor i obor hodnot, vyjadřujeme zpravidla $f$ pomocí jediné báze $\underline{u}$ prostoru $V$. Pak tedy přechod k nové bázi $\underline{u}'$ s maticí přechodu $T$ od $\underline{u}'$ k $\underline{u}$ bude znamenat změnu matice zobrazení na $A' = T^{-1}AT$.

Znalost matic rotací kolem souřadnicových os nám již umožňuje napsat matici rotace kolem libovolné (orientované) osy. Začněme s konkrétním příkladem:

**2.49.** Nalezněte matici rotace v kladném smyslu o úhel $\pi/3$ kolem přímky procházející počátkem s orientovaným směrovým vektorem $(1, 1, 0)$ ve standardní bázi $\mathbb{R}^3$.

**Řešení.** Uvedené otočení lze získat složením po řadě těchto tří zobrazení:

- rotace o $\pi/4$ v záporném smyslu podle osy $z$ (osa rotace přejde na osu $x$),
- rotace o $\pi/3$ v kladném smyslu podle osy $x$,
- rotace o $\pi/4$ v kladném smyslu podle osy $z$ (osa $x$ přejde na osu rotace).

Matice výsledné rotace bude součinem matic odpovídajících uvedeným třem zobrazením, přičemž pořadí matic je dáno pořadím provádění jednotlivých zobrazení – prvnímu zobrazení odpovídá v součinu matice nejvíce napravo. Takto dostaneme hledanou matici

$$\begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} \frac{3}{4} & \frac{1}{4} & \frac{\sqrt{6}}{4} \\ \frac{1}{4} & \frac{3}{4} & -\frac{\sqrt{6}}{4} \\ -\frac{\sqrt{6}}{4} & \frac{\sqrt{6}}{4} & \frac{1}{2} \end{pmatrix}.$$

Uvědomme si, že výslednou rotaci bylo možné získat např. také složením následujících tří zobrazení:

- rotace o $\pi/4$ v kladném smyslu podle osy $z$ (osa rotace přejde na osu $y$),
- rotace o $\pi/3$ v kladném smyslu podle osy $y$,
- rotace o $\pi/4$ v záporném smyslu podle osy $z$ (osa $y$ přejde na osu rotace).

Analogicky tak dostáváme

$$\begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & 0 & \frac{\sqrt{3}}{2} \\ 0 & 1 & 0 \\ -\frac{\sqrt{3}}{2} & 0 & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} \frac{3}{4} & \frac{1}{4} & \frac{\sqrt{6}}{4} \\ \frac{1}{4} & \frac{3}{4} & -\frac{\sqrt{6}}{4} \\ -\frac{\sqrt{6}}{4} & \frac{\sqrt{6}}{4} & \frac{1}{2} \end{pmatrix}.$$

□

**2.50. Matice obecné rotace v $\mathbb{R}^3$.** Odvoďte matici obecné rotace v $\mathbb{R}^3$.

**2.39. Lineární formy.** Obzvlášť jednoduchým a zároveň důležitým případem lineárních zobrazení jsou tzv. *lineární formy*. Jde o lineární zobrazení z vektorového prostoru $V$ nad polem skalárů $\mathbb{K}$ do skalárů $\mathbb{K}$. Jsou-li dány souřadnice na $V$, je přiřazení jednotlivé $i$-té souřadnice vektorům právě takovou lineární formou. Přesněji řečeno, pro každou volbu báze $\underline{v} = (v_1, \ldots, v_n)$ máme k dispozici lineární formy $v_i^* : V \to \mathbb{K}$ takové, že $v_i^*(v_j) = \delta_{ij}$, tj. nula pro různé indexy $i$ a $j$ a jednička pro stejné.

Vektorový prostor všech lineárních forem na $V$ značíme $V^*$ a říkáme mu *duální prostor* k vektorovému prostoru $V$. Předpokládejme nyní, že prostor $V$ má konečnou dimenzi $n$. Bázi $V^*$ sestavenou z přiřazování jednotlivých souřadnic jako výše nazýváme *duální báze*. Skutečně se jedná o bázi prostoru $V^*$, protože jsou tyto formy zjevně lineárně nezávislé (prověřte si!). Je-li $\alpha$ libovolná forma, pak pro každý vektor $u = x_1 v_1 + \cdots + x_n v_n$ platí

$$\alpha(u) = x_1\alpha(v_1) + \cdots + x_n\alpha(v_n) = \\ = \alpha(v_1)v_1^*(u) + \cdots + \alpha(v_n)v_n^*(u),$$

a je tedy $\alpha$ lineární kombinací forem $v_i^*$.

Při pevně zvolené bázi $\{1\}$ na jednorozměrném prostoru skalárů $\mathbb{K}$ jsou s každou volbou báze $\underline{v}$ na $V$ lineární formy $\alpha$ ztotožněny s maticemi typu $1/n$, tj. s řádky $y$. Právě komponenty těchto řádků jsou souřadnicemi obecných lineárních forem v duální bázi $\underline{v}^*$. Vyčíslení takové formy na vektoru je pak dáno vynásobením příslušného řádkového vektoru $y$ se sloupcem souřadnic $x$ vektoru $u \in V$ v bázi $\underline{v}$:

$$\alpha(u) = y \cdot x = y_1x_1 + \cdots + y_nx_n.$$

Zejména tedy vidíme, že pro každý konečně rozměrný prostor $V$ je $V^*$ izomorfní prostoru $V$. Realizace takového izomorfismu je dána např. naší volbou duální báze ke zvolené bázi na prostoru $V$.

V tomto kontextu tedy znovu potkáváme skalární součin řádku $n$ skalárů se sloupcem $n$ skalárů, jak jsme s ním pracovali již v odstavci 2.3 na straně 67.

U nekonečně rozměrného prostoru se věci mají jinak. Např. už nejjednodušší příklad prostoru všech polynomů $\mathbb{K}[x]$ v jedné proměnné je vektorovým prostorem se spočetnou bází s prvky $v_i = x^i$ a stejně jako výše můžeme definovat lineárně nezávislé formy $v_i^*$. Jakýkoliv formální nekonečný součet $\sum_{i=0}^{\infty} a_i v_i^*$ je nyní dobře definovanou lineární formou na $\mathbb{K}[x]$, protože bude vyčíslován vždy pouze na konečné lineární kombinaci bázových polynomů $x^i$, $i = 0, 1, 2, \ldots$.

Spočetná množina všech $v_i^*$ tedy není bází. Ve skutečnosti lze ukázat, že tento duální prostor ani spočetnou bázi mít nemůže.

**2.40. Velikost vektorů a skalární součin.** V úvahách o geometrii roviny $\mathbb{R}^2$ jsme již v první kapitole v odstavci 1.29 pracovali nejen s bázemi a lineárními zobrazeními, ale také s velikostí vektorů a jejich úhly. Pro zavedení těchto pojmů jsme také použili skalárního součinu dvou vektorů $v = (x, y)$ a $v' = (x', y')$ ve tvaru $v \cdot v' = xx' + yy'$. Skutečně, souřadné vyjádření pro velikost $v = (x, y)$ je dáno

$$\|v\| = \sqrt{x^2 + y^2} = \sqrt{v \cdot v},$$

**Řešení.** Úvahu z předchozího příkladu můžeme provést i s obecnými hodnotami. Uvažme libovolný jednotkový vektor $(x, y, z)$. Rotace v kladném smyslu o úhel $\varphi$ kolem tohoto vektoru pak můžeme zapsat jako složení následujících rotací, jejichž matice již známe:

i) rotace $\mathcal{R}_1$ v záporném smyslu kolem osy $z$ o úhel s kosinem $x/\sqrt{x^2+y^2} = x/\sqrt{1-z^2}$, tedy sinem $y/\sqrt{1-z^2}$, ve které přejde přímka se směrovým vektorem $(x, y, z)$ na přímku se směrovým vektorem $(0, y, z)$, matice této rotace je

$$R_1 = \begin{pmatrix} x/\sqrt{1-z^2} & y/\sqrt{1-z^2} & 0 \\ -y/\sqrt{1-z^2} & x/\sqrt{1-z^2} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

ii) rotace $\mathcal{R}_2$ v kladném smyslu podle osy $y$ o úhel s kosinem $\sqrt{1-z^2}$, tedy sinem $z$, ve které přejde přímka se směrovým vektorem $(0, y, z)$ na přímku se směrovým vektorem $(1, 0, 0)$, matice této rotace je

$$R_2 = \begin{pmatrix} \sqrt{1-z^2} & 0 & z \\ 0 & 1 & 0 \\ -z & 0 & \sqrt{1-z^2} \end{pmatrix},$$

iii) rotace $\mathcal{R}_3$ v kladném smyslu kolem osy $x$ o úhel $\varphi$ s maticí

$$R_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix},$$

iv) rotace $\mathcal{R}_2^{-1}$ s maticí $R_2^{-1}$,

v) rotace $\mathcal{R}_1^{-1}$ s maticí $R_1^{-1}$.

Matice složení těchto zobrazení, tedy hledaná matice, je dána součinem matic jednotlivých rotací v opačném pořadí:

$$R_1^{-1} \cdot R_2^{-1} \cdot R_3 \cdot R_2 \cdot = \begin{pmatrix} \cos\varphi + tx^2 & txy - zs & txz + ys \\ yxt + zs & \cos\varphi + ty^2 & tyz - xs \\ zxt - ys & tzy + xs & \cos\varphi + tz^2 \end{pmatrix},$$

kde jsme označili $t = 1 - \cos\varphi$ a $s = \sin\varphi$. □

**2.51.** Je dáno lineární zobrazení $\mathbb{R}^3 \to \mathbb{R}^3$ ve standardní bázi následující maticí:

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 1 \\ 2 & 0 & 0 \end{pmatrix}.$$

Napište matici tohoto zobrazení v bázi

$$(f_1, f_2, f_3) = ((1, 1, 0), (-1, 1, 1), (2, 0, 1)).$$

**Řešení.** Matici přechodu $T$ od báze $\underline{f} = (f_1, f_2, f_3)$ k standardní bázi, tj. bázi danou vektory $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, získáme podle Tvrzení 2.25 zapsáním souřadnic vektorů $f_1, f_2, f_3$ ve standardní bázi zatímco (orientovaný) úhel $\varphi$ dvou vektorů $v = (x, y)$ a $v' = (x', y')$ je v rovinné geometrii dán vztahem

$$\cos\varphi = \frac{xx' + yy'}{\|v\|\|v'\|}.$$

Povšimněme si, že tento skalární součin je lineární v každém ze svých argumentů. Takto definovaný skalární součin je také symetrický ve svých argumentech a samozřejmě platí, že $\|v\| = 0$, právě když $v = 0$. Z našich úvah je také vidět, že v Euklidovské rovině jsou dva vektory kolmé, právě když je jejich skalární součin nulový.

V případě reálného vektorového prostoru jakékoliv dimenze budeme hledat obdobný postup, protože koncept úhlu dvou vektorů je samozřejmě vždy dvourozměrný (jistě chceme, aby úhel byl stejný v dvourozměrném podprostoru obsahujícím $u$ a $v$ jako úhel v celém prostoru). Budeme v několika dalších odstavcích uvažovat pouze konečně rozměrné vektorové prostory nad reálnými skaláry $\mathbb{R}$.

### Skalární součin a kolmost

*Skalární součin* na vektorovém prostoru $V$ nad reálnými čísly je zobrazení $\langle\ ,\ \rangle : V \times V \to \mathbb{R}$, které je symetrické ve svých argumentech, lineární v každém z nich a takové, že $\langle v, v\rangle \geq 0$ a $\|v\|^2 = \langle v, v\rangle = 0$ pouze při $v = 0$.

Číslu $\|v\| = \sqrt{\langle v, v\rangle}$ říkáme velikost vektoru $v$.

Vektory $v, w \in V$ se nazývají *ortogonální* nebo *kolmé*, jestliže $\langle v, w\rangle = 0$. Píšeme také $v \perp w$. Vektor $v$ se nazývá *normovaný*, jestliže $\|v\| = 1$.

Báze prostoru $V$ složená z ortogonálních vektorů se nazývá *ortogonální báze*. Jsou-li bázové vektory navíc i normované, je to *ortonormální báze*.

Skalární součin se také často zapisuje pomocí obvyklé tečky, tj. $\langle u, v\rangle = u \cdot v$. Z kontextu je pak třeba poznat, zda jde o součin dvou vektorů (tedy výsledkem je skalár) nebo něco jiného (stejně jsme značili součin matic a také někdy součin skalárů).



Protože je skalární součin lineární v každém ze svých argumentů, bude jistě úplně určen již svými hodnotami na dvojicích bázových vektorů. Skutečně, zvolme si bázi $\underline{u} = (u_1, \ldots, u_n)$ prostoru $V$ a označme

$$s_{ij} = \langle u_i, u_j\rangle.$$

Pak ze symetričnosti skalárního součinu plyne $s_{ij} = s_{ji}$ a z linearity součinu v každém z argumentů dostáváme:

$$\left\langle \sum_i x_i u_i, \sum_j y_j u_j \right\rangle = \sum_{i,j} x_i y_j \langle u_i, u_j\rangle = \sum_{i,j} s_{ij} x_i y_j.$$

Pokud je báze ortonormální, je matice $S$ jednotkovou maticí. Tím jsme dokázali následující užitečné tvrzení:

### Skalární součin a ortonormální báze

**Tvrzení.** *Skalární součin je v každé ortonormální bázi dán v souřadnicích výrazem*

$$\langle x, y\rangle = x^T \cdot y.$$

*Pro každou obecnou bázi prostoru $V$ existuje symetrická matice $S$ taková, že souřadné vyjádření skalárního součinu je*

$$\langle x, y\rangle = x^T \cdot S \cdot y.$$

do sloupců matice přechodu $T$. Máme tedy

$$T = \begin{pmatrix} 1 & -1 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Matice přechodu od standardní báze k bázi $\underline{f}$ je potom

$$T^{-1} = \begin{pmatrix} \frac{1}{4} & \frac{3}{4} & -\frac{1}{2} \\ -\frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{4} & -\frac{1}{4} & \frac{1}{2} \end{pmatrix}.$$

Matice zobrazení v bázi $\underline{f}$ je potom

$$T^{-1}AT = \begin{pmatrix} \frac{1}{4} & 2 & -\frac{3}{4} \\ \frac{5}{4} & 0 & \frac{7}{4} \\ \frac{3}{4} & -2 & \frac{9}{4} \end{pmatrix}.$$

□

**2.52.** Uvažme vektorový prostor mnohočlenů jedné neznámé stupně nejvýše 2 s reálnými koeficienty. V tomto prostoru uvažme bázi $1, x, x^2$. Napište matici zobrazení derivace v této bázi a také v bázi $1 + x^2, x, x + x^2$.

**Řešení.** $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 2 & 1 & 3 \\ 0 & -1 & -1 \end{pmatrix}$. □

**2.53.** Ve standardní bázi v $\mathbb{R}^3$ určete matici rotace o 90° v kladném smyslu kolem přímky $(t, t, t), t \in \mathbb{R}$, orientované ve směru vektoru $(1, 1, 1)$. Dále určete matici této rotace v bázi

$$\underline{g} = ((1, 1, 0), (1, 0, -1), (0, 1, 1)).$$

**Řešení.** Snadno určíme matici uvažované rotace, a to ve vhodné bázi, totiž v bázi dané směrovým vektorem přímky a dále dvěma navzájem kolmými vektory v rovině $x + y + z = 0$, tedy v rovině vektorů kolmých k vektoru $(1, 1, 1)$. Uvědomme si, že matice rotace v kladném smyslu o 90° v nějaké ortonormální bázi v $\mathbb{R}^2$ je $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, v ortogonální s velikostmi vektorů $k, l$ potom $\left(\begin{smallmatrix} 0 & -k/l \\ l/k & 0 \end{smallmatrix}\right)$. Zvolíme-li v rovině $x + y + z = 0$ kolmé vektory $(1, -1, 0)$ a $(1, 1, -2)$ o velikostech $\sqrt{2}$ a $\sqrt{6}$, tak v bázi $\underline{f} = ((1, 1, 1), (1, -1, 0), (1, 1, -2))$ má uvažovaná rotace matici $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & -\sqrt{3} \\ 0 & 1/\sqrt{3} & 0 \end{smallmatrix}\right)$. Abychom získali matici uvažované rotace ve standardní bázi, stačí nám transformovat matici již známým způsobem (viz 2.38). Matici přechodu $T$ od báze $\underline{f}$ ke standardní dostaneme zapsáním souřadnic (ve standardní bázi) vektorů báze $\underline{f}$ do sloupců matice $T$: $T = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 0 & -2 \end{smallmatrix}\right)$. Celkem tedy pro hledanou matici $R$ máme

**Poznámka.** Matice $S$ z předchozí věty je dokonce pozitivně definitní (pro definici pojmu pozitivní definitnosti viz 3.31)

**2.41. Ortogonální doplňky a projekce.** Pro každý pevně zvolený podprostor $W \subseteq V$ v prostoru se skalárním součinem definujeme jeho *ortogonální doplněk* takto



$$W^\perp = \{u \in V;\ u \perp v \text{ pro všechny } v \in W\}.$$

Přímo z definice je zjevné, že $W^\perp$ je vektorový podprostor. Jestliže $W \subseteq V$ má bázi $(u_1, \ldots, u_k)$, je podmínka pro $W^\perp$ dána jako $k$ homogenních rovnic pro $n$ proměnných. Bude tedy mít $W^\perp$ dimenzi alespoň $n - k$. Zároveň ale $u \in W \cap W^\perp$ znamená $\langle u, u\rangle = 0$ a tedy i $u = 0$ podle definice skalárního součinu. Zřejmě je tedy vždy celý prostor $V$ přímým součtem

$$V = W \oplus W^\perp.$$

Lineární zobrazení $f : V \to V$ na libovolném vektorovém prostoru se nazývá *projekce*, jestliže platí

$$f \circ f = f.$$

V takovém případě je pro každý vektor $v \in V$:

$$v = f(v) + (v - f(v)) \in \mathrm{Im}(f) + \mathrm{Ker}(f) = V,$$

a je-li $v \in \mathrm{Im}(f)$ a $f(v) = 0$, pak je i $v = 0$. Je tedy předchozí součet podprostorů přímý. Říkáme, že $f$ je projekce na podprostor $W = \mathrm{Im}(f)$ podél podprostoru $U = \mathrm{Ker}(f)$. Slovy se dá projekce popsat přirozeně takto: rozložíme daný vektor na komponentu ve $W$ a v $U$ a tu druhou zapomeneme.

Je-li na $V$ navíc skalární součin, říkáme že jde o kolmou projekci, když je jádro kolmé na obraz. Každý podprostor $W \neq V$ tedy definuje *kolmou projekci* na $W$. Je to projekce na $W$ podél $W^\perp$, která je dána pomocí jednoznačného rozkladu každého vektoru $u$ na komponenty $u_W \in W$ a $u_{W^\perp} \in W^\perp$, tj. lineární zobrazení, které $u_W + u_{W^\perp}$ zobrazí na $u_W$.

**2.42. Existence ortonormální báze.** Povšimněme si, že na každém konečně rozměrném reálném vektorovém prostoru jistě existují skalární součiny. Prostě si stačí vybrat libovolnou bázi, prohlásit ji za ortonormální a hned jeden dobře definovaný skalární součin máme. V této bázi pak skalární součiny počítáme podle vzorce v Tvrzení 2.40.



Umíme to ale i naopak. Máme-li zadán skalární součin na vektorovém prostoru $V$, můžeme vcelku jednoduše početně využít vhodných kolmých projekcí a jakoukoliv zvolenou bázi upravit na ortonormální.

Jde o tzv. *Gramův–Schmidtův ortogonalizační proces*. Cílem této procedury bude z dané posloupnosti nenulových generátorů $v_1, \ldots, v_k$ konečně rozměrného prostoru $V$ vytvořit ortogonální množinu nenulových generátorů pro $V$.

GRAMOVA–SCHMIDTOVA ORTOGONALIZACE

**Tvrzení.** *Nechť $(u_1, \ldots, u_k)$ je lineárně nezávislá $k$-tice vektorů prostoru $V$ se skalárním součinem. Pak existuje ortogonální systém vektorů $(v_1, \ldots, v_k)$ takový, že $v_i \in \langle u_1, \ldots, u_i\rangle$, $i = 1, \ldots, k$. Získáme jej následující procedurou:*

- *Nezávislost vektorů $u_i$ zaručuje, že $u_1 \neq 0$; zvolíme $v_1 = u_1$.*

$$R = T \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -\sqrt{3} \\ 0 & 1/\sqrt{3} & 0 \end{pmatrix} \cdot T^{-1} =$$
$$= \begin{pmatrix} 1/3 & 1/3-\sqrt{3}/3 & 1/3+\sqrt{3}/3 \\ 1/3+\sqrt{3}/3 & 1/3 & 1/3-\sqrt{3}/3 \\ 1/3-\sqrt{3}/3 & 1/3+\sqrt{3}/3 & 1/3 \end{pmatrix}.$$

Tento výsledek můžeme ověřit dosazením do matice obecné rotace (‖2.50‖), místo vektoru $(1, 1, 1)$ však musíme použít jednotkový vektor stejného směru, tedy vektor dostáváme vektor $(x, y, z) = (1/\sqrt{3}, 1/\sqrt{3}, 1/\sqrt{3})$, $\cos\varphi = 0$, $\sin\varphi = 1$. □

**2.54. Matice obecné rotace podruhé.** Zkusme odvodit matici (obecné) rotace z (‖2.50‖) o úhel $\varphi$ v kladném smyslu kolem jednotkového vektoru $(x, y, z)$ jiným způsobem, analogicky jako v předchozím příkladě. V bázi $\underline{f} = ((x, y, z), (-y, x, 0), (zx, zy, z^2-1))$, tedy v ortogonální bázi tvořené směrovým vektorem osy rotace a dvěma navzájem kolmými vektory o shodných velikostech $\sqrt{1-z^2}$ ležícími v rovině kolmé na osu, má uvažovaná rotace matici $A = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{smallmatrix}\right)$. Matice přechodu od báze $\underline{f}$ ke standardní bázi je potom $T = \left(\begin{smallmatrix} x & -y & zx \\ y & x & zy \\ z & 0 & z^2-1 \end{smallmatrix}\right)$ s inverzní maticí

$$T^{-1} = \begin{pmatrix} x & y & z \\ -\frac{y}{1-z^2} & \frac{x}{1-z^2} & 0 \\ \frac{zx}{1-z^2} & \frac{zy}{1-z^2} & -1 \end{pmatrix}.$$

Celkem pak pro matici $R$ hledané rotace dostáváme

$$R = T \cdot R \cdot T^{-1} =$$
$$\begin{pmatrix} \cos\varphi+(1-\cos\varphi)x^2 & (1-\cos\varphi)xy - z\sin\varphi & (1-\cos\varphi)xz + y\sin\varphi \\ yx(1-\cos\varphi)+z\sin\varphi & \cos\varphi+(1-\cos\varphi)y^2 & (1-\cos\varphi)yz - x\sin\varphi \\ zx(1-\cos\varphi)-y\sin\varphi & (1-\cos\varphi)zy + x\sin\varphi & \cos\varphi+(1-\cos\varphi)z^2 \end{pmatrix}.$$

Při násobení a následném zjednodušování je nutno opakovaně použít předpokladu $x^2+y^2+z^2 = 1$.

Podrobnějším rozborem vlastností různých typů lineárních zobrazení se nyní dostaneme k pořádnějšímu pochopení nástrojů, které nám vektorové prostory pro lineární modelování procesů a systémů nabízejí.

**2.55.** Uvažme komplexní čísla jako reálný vektorový prostor a za jeho bázi zvolme 1 a $i$. V této bázi určete matice následujících lineárních zobrazení:

a) konjugace,

b) násobení číslem $(2+i)$.

Určete matice těchto zobrazení v bázi $\underline{f} = ((1-i), (1+i))$.

- *Máme-li již vektory $v_1, \ldots, v_\ell$ potřebných vlastností, zvolíme $v_{\ell+1} = u_{\ell+1} + a_1 v_1 + \cdots + a_\ell v_\ell$, kde $a_i = -\frac{\langle u_{\ell+1}, v_i\rangle}{\|v_i\|^2}$, $i = 1, \ldots, \ell$.*

Důkaz. Začneme prvním (nenulovým) vektorem $v_1$ a spočteme kolmou projekci $v_2$ do

$$\langle v_1\rangle^\perp \subseteq \langle\{v_1, v_2\}\rangle.$$

Výsledek bude nenulový, právě když je $v_2$ nezávislé na $v_1$. Ve všech dalších krocích budeme postupovat obdobně.

V $\ell$-tém kroku tedy chceme, aby pro $v_{\ell+1} = u_{\ell+1} + a_1 v_1 + \ldots + a_\ell v_\ell$ platilo $\langle v_{\ell+1}, v_i\rangle = 0$ pro všechna $i = 1, \ldots, \ell$. Odtud plyne

$$0 = \langle u_{\ell+1} + a_1 v_1 + \cdots + a_\ell v_\ell, v_i\rangle = \langle u_{\ell+1}, v_i\rangle + a_i\langle v_i, v_i\rangle$$

a je vidět, že vektory s požadovanými vlastnostmi jsou určeny jednoznačně až na násobek. □

Kdykoliv máme ortogonální bázi vektorového prostoru $V$, stačí vektory vynormovat a získáme bázi ortonormální. Dokázali jsme proto:

**Důsledek.** *Na každém konečně rozměrném reálném vektorovém prostoru se skalárním součinem existuje ortonormální báze.*

V ortonormální bázi se obzvlášť snadno spočtou souřadnice a kolmé projekce. Skutečně, mějme ortonormální bázi $(e_1, \ldots, e_n)$ prostoru $V$. Pak každý vektor $v = x_1 e_1 + \cdots + x_n e_n$ splňuje

$$\langle e_i, v\rangle = \langle e_i, x_1 e_1 + \cdots + x_n e_n\rangle = x_i,$$

a platí tedy vždy

$$v = \langle e_1, v\rangle e_1 + \cdots + \langle e_n, v\rangle e_n. \tag{2.3}$$

Pokud máme zadán podprostor $W \subseteq V$ a jeho ortonormální bázi $(e_1, \ldots, e_k)$, jde ji jistě doplnit na ortonormální bázi $(e_1, \ldots, e_n)$ celého $V$. Kolmá projekce obecného vektoru $v \in V$ do $W$ pak bude dána vztahem

$$v \mapsto \langle e_1, v\rangle e_1 + \cdots + \langle e_n, v\rangle e_k.$$

Pro kolmou projekci nám tedy stačí znát jen ortonormální bázi podprostoru $W$, na nějž promítáme.

Povšimněme si také, že obecně jsou projekce $f$ na podprostor $W$ podél $U$ a projekce $g$ na $U$ podél $W$ svázány vztahem $g = \mathrm{id}_V - f$. Je tedy u kolmých projekcí na daný podprostor $W$ vždy výhodnější počítat ortonormální bázi toho podprostoru z dvojice $W$, $W^\perp$, který má menší dimenzi.

Uvědomme si také, že existence ortonormální báze nám zaručuje, že pro každý reálný prostor $V$ dimenze $n$ se skalárním součinem existuje lineární zobrazení, které je izomorfismem mezi $V$ a prostorem $\mathbb{R}^n$ se standardním skalárním součinem. Podrobně to bylo ukázáno již v Tvrzení 2.40, kde jsme ukázali, že hledaným izomorfismem je právě přiřazení souřadnic. Řečeno volnými slovy – v ortonormální bázi se skalární součin pomocí souřadnic počítá stejnou formulí jako standardní skalární součin v $\mathbb{R}^n$.

K otázkám velikosti vektorů a projekcím se vrátíme ještě v příští kapitole v obecnějších souvislostech.

**Řešení.** Abychom určili matici lineárního zobrazení v nějaké bázi, stačí určit obrazy bázových vektorů.

a) Pro konjugaci je $1 \mapsto 1$, $i \mapsto -i$, zapsáno v souřadnicích $(1,0) \mapsto (1,0)$ a $(0,1) \mapsto (0,-1)$. Zapsáním obrazů do sloupců dostáváme matici $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, V bázi $\underline{f}$ pak konjugace prohazuje bázové vektory, čili $(1,0) \mapsto (0,1)$ a $(0,1) \mapsto (1,0)$ a matice konjugace v této bázi je $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

b) Pro bázi $(1,i)$ dostáváme $1 \mapsto 2+i$, $i \mapsto 2i-1$, tedy $(1,0) \mapsto (2,1)$, $(0,1) \mapsto (2,-1)$. Celkem je matice násobení číslem $2+i$ v bázi $(1,i)$ tato: $\left(\begin{smallmatrix} 2 & -1 \\ 1 & 2 \end{smallmatrix}\right)$.

Nyní určeme matici v bázi $\underline{f}$. Násobením číslem $2+i$ dostáváme: $1-i \mapsto (1-i)(2+i) = 3-i$, $1+i \mapsto 1+3i$. Souřadnice $(a,b)_{\underline{f}}$ vektoru $3-i$ v bázi $\underline{f}$ jsou dány, jak již dobře víme, rovnicí $a \cdot (1-i) + b \cdot (1+i) = 3+i$, tedy $(3+i)_{\underline{f}} = (2,1)$. Obdobně $(1+3i)_{\underline{f}} = (-1,2)$. Dohromady jsme získali matici $\left(\begin{smallmatrix} 2 & -1 \\ 1 & 2 \end{smallmatrix}\right)$.

Zamyslete se, proč nám matice násobení číslem $2+i$ vyšla stejná v obou bázích. Byla by stejná matice násobení libovolným jiným komplexním číslem v těchto bázích? □

**2.56.** Určete matici $A$, která ve standardní bázi prostoru $\mathbb{R}^3$ zadává kolmou projekci do vektorového podprostoru generovaného vektory $u_1 = (-1,1,0)$ a $u_2 = (-1,0,1)$.

**Řešení.** Nejprve poznamenejme, že uvedený podprostor je rovinou procházející počátkem s normálovým vektorem $u_3 = (1,1,1)$. Uspořádaná trojice $(1,1,1)$ je totiž očividným řešením soustavy

$$\begin{aligned} -x_1 + x_2 &= 0, \\ -x_1 + x_3 &= 0, \end{aligned}$$

tj. vektor $u_3$ je kolmý na vektory $u_1, u_2$.

Při dané projekci se vektory $u_1$ a $u_2$ musejí zobrazit na sebe a vektor $u_3$ potom na nulový vektor. V bázi složené po řadě z vektorů $u_1$, $u_2, u_3$ je proto matice této projekce

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Pomocí matic přechodu

$$T = \begin{pmatrix} -1 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad T^{-1} = \begin{pmatrix} -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

**2.43. Úhel dvou vektorů.** Jak jsme již zmínili, úhel dvou lineárně nezávislých vektorů musí být stejný, když je budeme uvažovat v dvourozměrném podprostoru, který generují, nebo v okolním prostoru větším. Ve své podstatě je proto pojem úhlu dvou vektorů nezávislý na dimenzi okolního prostoru a pokud si zvolíme ortonormální bázi, jejíž první dva vektory budou generovat tentýž podprostor jako dané vektory $u$ a $v$, můžeme doslova převzít definici z rovinné geometrie. I bez volby báze tedy musí platit:

ÚHEL DVOU VEKTORŮ

Úhel $\varphi$ dvou vektorů $v$ a $w$ ve vektorovém prostoru se skalárním součinem je dán vztahem

$$\cos\varphi = \frac{\langle v, w\rangle}{\|v\|\|w\|}.$$

Takto definovaný úhel nezávisí na uvažovaném pořadí vektorů $v$, $w$ splňuje $0 \le \varphi \le \pi$.

K problematice skalárních součinů a úhlů vektorů se vrátíme v dalších kapitolách.

**2.44. Multilineární formy.** Skalární součin byl dán jako zobrazení ze součinu dvou kopií vektorového prostoru $V$ do prostoru skalárů, které bylo lineární v každém ze svých argumentů. Podobně budeme pracovat i se zobrazeními ze součinu $k$ kopií vektorového prostoru $V$ do skalárů, která jsou lineární v každém ze svých $k$ argumentů. Hovoříme o *$k$-lineárních* formách.



Nejčastěji se budeme setkávat s *bilineárními formami*, tj. případem $\alpha : V \times V \to \mathbb{K}$, kde pro jakékoliv vektory $u$, $v$, $w$, $z$ a skaláry $a$, $b$, $c$ a $d$ platí, stejně jako u skalárního součinu, že

$$\begin{aligned} \alpha(au + bv, cw + dz) = ac\,\alpha(u,w) + ad\,\alpha(u,z) + \\ + bc\,\alpha(v,w) + bd\,\alpha(v,z). \end{aligned}$$

Pokud navíc platí

$$\alpha(u,w) = \alpha(w,u),$$

hovoříme o *symetrické bilineární formě*. Jestliže záměna argumentů vede k obrácení znaménka výsledku, hovoříme o *antisymetrické bilineární formě*.

Již v rovinné geometrii jsme zavedli determinant jako bilineární antisymetrickou formu $\alpha$, tj. $\alpha(u,w) = -\alpha(w,u)$. Obecně víme z věty 2.17, že je na determinant v dimenzi $n$ možno nahlížet jako na $n$-lineární antisymetrickou formu.

Jako u lineárních zobrazení je zřejmé, že každá $k$-lineární forma je úplně určena svými hodnotami na všech $k$-ticích bázových prvků v pevné bázi. V analogii k lineárním zobrazením tyto hodnoty můžeme vnímat jako $k$–rozměrné analogie matic. Ukážeme si to v případě $k = 2$, kde půjde doopravdy o matice, jak jsme je zavedli.

MATICE BILINEÁRNÍ FORMY

Jestliže zvolíme bázi $\underline{u}$ na $V$ a definujeme pro danou bilineární formu $\alpha$ skaláry $a_{ij} = \alpha(u_i, u_j)$, pak zjevně dostaneme pro vektory $v$, $w$ se souřadnicemi $x$ a $y$ (jakožto sloupce souřadnic)

$$\alpha(v,w) = \sum_{i,j=1}^{n} a_{ij} x_i y_j = y^T \cdot A \cdot x,$$

kde $A$ je matice $A = (a_{ij})$.

od báze $(u_1, u_2, u_3)$ ke standardní bázi a od standardní báze k bázi $(u_1, u_2, u_3)$ získáme

$$A = \begin{pmatrix} -1 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix} = \\ = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \end{pmatrix}.$$

□

### I. Báze a skalární součiny

Pomocí skalárního součinu umíme řešit jiným způsobem (lépe?) problémy, které jsme již dříve zvládli pomocí transformace souřadnic.

**2.57.** V prostoru $\mathbb{R}^3$ napište matici zobrazení kolmé projekce do roviny procházející počátkem a kolmé na vektor $(1, 1, 1)$.

**Řešení.** Obraz libovolného bodu (vektoru) $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ v uvažovaném zobrazení získáme tak, že od daného bodu odečteme jeho kolmou projekci do normálového směru dané roviny, tedy do směru $(1, 1, 1)$. Tato projekce $p$ je dána (viz 2.3) jako

$$\frac{\langle x, (1,1,1)\rangle}{|(1,1,1)|^2} \cdot (1,1,1) = \\ = \left(\frac{x_1+x_2+x_3}{3}, \frac{x_1+x_2+x_3}{3}, \frac{x_1+x_2+x_3}{3}\right).$$

Výsledné zobrazení je tedy

$$x - p = \left(\frac{2x_1}{3} - \frac{x_2+x_3}{3}, \frac{2x_2}{3} - \frac{x_1+x_3}{3}, \frac{2x_3}{3} - \frac{x_1+x_2}{3}\right) = \\ = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

Vyšla nám tedy (správně) stejná matice jako v příkladu ‖2.56‖. □

**2.58.** V prostoru $\mathbb{R}^3$ určete matici zrcadlení podle roviny procházející počátkem a s normálovým vektorem $(1, 1, 1)$.

**Řešení.** Obdobně jako v předchozím příkladu (‖2.57‖) získáme obraz libovolného bodu (vektoru) $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ pomocí jeho kolmé projekce $p$ do normálového směru $(1, 1, 1)$. Na rozdíl od předchozího příkladu je však tuto projekci třeba odečíst dvakrát (viz obrázek). Je tedy

$$x - 2p = \left(\frac{x_1}{3} - \frac{2(x_2+x_3)}{3}, \frac{x_2}{3} - \frac{2(x_1+x_3)}{3}, \frac{x_3}{3} - \frac{2(x_1+x_2)}{3}\right) = \\ = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & -\frac{2}{3} \\ -\frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \\ -\frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

Přímo z definice matice bilineární formy je vidět, že forma je symetrická nebo antisymetrická, právě když má tutéž vlastnost její matice.

Každá bilineární forma $\alpha$ na vektorovém prostoru $V$ definuje zobrazení $V \to V^*$, $v \mapsto \alpha(\ , v)$, tj. dosazením pevného vektoru $v$ za druhý argument dostáváme lineární formu, která je obrazem tohoto vektoru. Zvolíme-li pevně bázi na konečně rozměrném prostoru $V$ a duální bázi na $V^*$, pak jde o zobrazení

$$y \mapsto (x \mapsto y^T \cdot A \cdot x).$$

### 4. Vlastnosti lineárních zobrazení

Podrobnějším rozborem vlastností různých typů lineárních zobrazení se nyní dostaneme k lepšímu pochopení nástrojů, které nám vektorové prostory pro lineární modelování procesů a systémů nabízejí.

**2.45.** Začneme čtyřmi příklady v nejnižší zajímavé dimenzi. Ve standardní bázi roviny $\mathbb{R}^2$ se standardním skalárním součinem uvažujme následující matice zobrazení $f : \mathbb{R}^2 \to \mathbb{R}^2$:



$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, C = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, D = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Matice $A$ zadává kolmou projekci podél podprostoru

$$W \subseteq \{(0, a);\ a \in \mathbb{R}\} \subseteq \mathbb{R}^2$$

na podprostor

$$V \subseteq \{(a, 0);\ a \in \mathbb{R}\} \subseteq \mathbb{R}^2,$$

tj. projekce na osu $x$ podél osy $y$. Evidentně pro toto zobrazení $f : \mathbb{R}^2 \to \mathbb{R}^2$ platí $f \circ f = f$ a tedy zúžení $f|_V$ daného zobrazení na obor hodnot je identické zobrazení. Jádrem $f$ je právě podprostor $W$.

Matice $B$ má vlastnost $B^2 = 0$, platí tedy totéž o příslušném zobrazení $f$. Můžeme si jej představit jako matici derivování polynomů $\mathbb{R}_1[x]$ stupně nejvýše jedna v bázi $(1, x)$ (derivacemi se budeme podrobně zabývat v kapitole páté, viz 5.6).

Matice $C$ zadává zobrazení $f$, které první vektor báze zvětší $a$-krát, druhý $b$-krát. Tady se nám tedy celá rovina rozpadá na dva podprostory, které jsou zobrazením $f$ zachovány a ve kterých jde o pouhou *homotetii*, tj. roztažení skalárním násobkem (první příklad byl speciální případem s $a = 1, b = 0$). Např. volba $a = 1$, $b = -1$ odpovídá osové symetrii (zrcadlení) podle osy $x$, což je totéž jako komplexní konjugace $x+iy \mapsto x-iy$ na dvourozměrném reálném prostoru $\mathbb{R}^2 \simeq \mathbb{C}$ v bázi $(1, i)$. Toto je lineární zobrazení dvourozměrného reálného vektorového prostoru $\mathbb{C}$, nikoliv však jednorozměrného komplexního prostoru $\mathbb{C}$.

Matice $D$ je maticí rotace o pravý úhel ve standardní bázi a na první pohled je vidět, že žádný jednorozměrný podprostor není zobrazením zachováván.

Taková rotace je bijekcí roviny na sebe, proto jistě umíme najít (různé) báze na definičním oboru a oboru hodnot, ve kterých bude jeho maticí jednotková matice $E$ (prostě vezmeme jakoukoliv bázi na definičním oboru a její obraz na oboru hodnot). Neumíme ale v tomto případě totéž s jednou bází na definičním oboru i oboru hodnot.

Uvedená matice je tedy hledanou maticí uvažovaného zrcadlení. Uvedený postup můžeme technicky také provést následujícím (myšlenkově shodným) způsobem. Normovaný normálový vektor je $n = \frac{1}{\sqrt{3}}(1,1,1)$. Zrcadlení $Z$ na vektoru $v$ lze pak vyjádřit $Zv = v - 2\langle v,n\rangle n = v - 2n\cdot(n^T\cdot v) = v - 2(n\cdot n^T)\cdot v = ((E - 2n\cdot n^T)v$ (pro standardní skalární součin je $\langle v,n\rangle = v\cdot n^T$; dále jsme využili asociativity násobení „·“ matic). Matice zrcadlení je tedy

$$E - 2n\cdot n^T = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} - \frac{2}{3}\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix} = \frac{1}{3}\begin{pmatrix}1&-2&-2\\-2&1&-2\\-2&-2&1\end{pmatrix}.$$

□

**2.59.** V $\mathbb{R}^3$ je dána standardní souřadnicová soustava. V rovině $z = 0$ je umístěno zrcadlo a v bodě $[4,3,5]$ svíčka. Pozorovatel v bodě $[1,2,3]$ o zrcadle neví, ale pozoruje odrazem v něm svíčku. V jakém bodě se mu jeví, že je svíčka umístěna?

**Řešení.** V zrcadle vidíme vždy (nezávisle na naší poloze) zrcadlový obraz pozorovaných objektů. Svíčka se tedy jeví v bodě, který je zrcadlovým obrazem skutečné polohy podle roviny zrcadla, tedy podle roviny $z = 0$. Zrcadlení podle této roviny má jednoduchý předpis, stačí změnit znaménko u souřadnice $z$ zobrazovaného bodu (rozmysli). Svíčku tudíž vidí pozorovatel v bodě $[4,3,-5]$. □

Pomocí skalárního součinu můžeme určovat odchylky vektorů:

**2.60.** Určete odchylku kořenů polynomu $x^2 - i$ uvažovaných jako vektory v komplexní rovině.

**Řešení.** Kořeny daného polynomu jsou druhé odmocniny z $i$. Argumenty druhých odmocnin z libovolného nenulového komplexního čísla se podle Moivreovy věty liší o $\pi$. Jejich odchylka tedy bude vždy $\pi$. □

*2.61.* Určete cosinus odchylky přímek $p, q$ v $\mathbb{R}^3$ daných obecnými rovnicemi jako

$$\begin{aligned} p:\ -2x + y + z &= 1,\\ x + 3y - 4z &= 5,\\ q:\ x - y &= -2,\\ z &= 6. \end{aligned}$$

**2.62.** Pomocí Gramova-Schmidtova ortogonalizačního procesu získejte ortogonální bázi podprostoru

$$U = \{(x_1,x_2,x_3,x_4)^T \in \mathbb{R}^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}$$

prostoru $\mathbb{R}^4$.



Zkusme však uvažovat matici $D$ jako matici zobrazení $g : \mathbb{C}^2 \to \mathbb{C}^2$ ve standardní bázi komplexního vektorového prostoru $\mathbb{C}^2$. Pak umíme najít vektory $u = (i,\ 1), v = (-i,\ 1)$, pro které bude platit

$$g(u) = \begin{pmatrix}0&-1\\1&0\end{pmatrix}\cdot\begin{pmatrix}i\\1\end{pmatrix} = \begin{pmatrix}-1\\i\end{pmatrix} = i\cdot u,$$

$$g(v) = \begin{pmatrix}0&-1\\1&0\end{pmatrix}\cdot\begin{pmatrix}-i\\1\end{pmatrix} = \begin{pmatrix}-1\\-i\end{pmatrix} = -i\cdot v.$$

To ale znamená, že v bázi $(u,v)$ na $\mathbb{C}^2$ má zobrazení $g$ matici

$$K = \begin{pmatrix}i&0\\0&-i\end{pmatrix}.$$

Povšimněme si, že tato komplexní analogie k případu matice $C$ má na diagonále prvky $a = \cos(\frac{1}{2}\pi) + i\sin(\frac{1}{2}\pi)$ a komplexně sdružené $\bar{a}$. Jinými slovy, argument v goniometrickém tvaru tohoto komplexního čísla udává úhel otočení.

Tomu lze snadno porozumět, když si označíme reálnou a imaginární část vektoru $u$ takto

$$u = x_u + iy_u = \operatorname{Re} u + i\operatorname{Im} u = \begin{pmatrix}0\\1\end{pmatrix} + i\cdot\begin{pmatrix}1\\0\end{pmatrix}.$$

Vektor $v$ je komplexně sdružený k $u$. Zajímá nás zúžení zobrazení $g$ na reálný vektorový podprostor $V = \mathbb{R}^2 \cap \langle u,v\rangle \subseteq \mathbb{C}^2$. Evidentně je

$$V = \langle u + \bar{u}, i(u - \bar{u})\rangle = \langle x_u, -y_u\rangle$$

celá reálná rovina $\mathbb{R}^2$. Zúžení zobrazení $g$ na tuto rovinu je právě původní zobrazení dané maticí $A$ a z definice násobení komplexní jednotkou jde o otočení o úhel $\frac{1}{2}\pi$ v kladném smyslu ve vztahu ke zvolené bázi $x_u, -y_u$ (ověřte si přímým výpočtem a uvědomte si také, proč případné prohození pořadí vektorů $u$ a $v$ povede k témuž výsledku, byť v jiné reálné bázi!).

**2.46. Vlastní čísla a vlastní vektory zobrazení.** Klíčem k popisu zobrazení v předchozích příkladech byly odpovědi na otázku „jaké jsou vektory splňující rovnici $f(u) = a\cdot u$ pro nějaké vhodné skaláry $a$?“.



Zvolme tedy pevně lineární zobrazeni $f : V \to V$ na vektorovém prostoru dimenze $n$ nad skaláry $\mathbb{K}$. Jestliže si představíme takovou rovnost zapsanou v souřadnicích, tj. s využitím matice zobrazení $A$ v nějakých bázích, jde o výraz

$$A\cdot x - a\cdot x = (A - a\cdot E)\cdot x = 0.$$

Z dřívějška víme, že taková soustava rovnic má jediné řešení $x = 0$, právě když je matice $A - aE$ invertibilní, viz odstavec 2.13. My tedy chceme najít takové hodnoty $a \in \mathbb{K}$, pro které naopak $A - aE$ invertibilní není, a nutnou a dostatečnou podmínkou je (viz Věta 2.23)

$$\det(A - a\cdot E) = 0. \tag{2.4}$$

Jestliže považujeme $\lambda = a$ za proměnnou v předchozí skalární rovnici, hledáme ve skutečnosti kořeny polynomu stupně $n$. Jak jsme viděli v případě matice $D$ výše, kořeny mohou, ale nemusí existovat podle volby pole skalárů $\mathbb{K}$.

VLASTNÍ ČÍSLA A VLASTNÍ VEKTORY

Skaláry $\lambda$ vyhovující rovnici $f(u) = \lambda\cdot u$ pro nenulový vektor $u \in V$ nazýváme *vlastní čísla zobrazení* $f$, příslušné nenulové vektory $u$ pak *vlastní vektory zobrazení* $f$.

**Řešení.** Množina řešení uvedené homogenní lineární rovnice je zřejmě vektorovým prostorem s bází

$$u_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad u_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad u_3 = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Vektory ortogonální báze získané užitím Gramová-Schmidtova ortogonalizačního procesu. Budeme značit $v_1$, $v_2$, $v_3$. Nejprve položme $v_1 = u_1$. Dále

$$v_2 = u_2 - \frac{u_2^T \cdot v_1}{||v_1||^2} v_1 = u_2 - \frac{1}{2} v_1 = \left(-\frac{1}{2}, -\frac{1}{2}, 1, 0\right)^T,$$

resp. zvolme násobek $v_2 = (-1, -1, 2, 0)^T$. Následně je

$$v_3 = u_3 - \frac{u_3^T \cdot v_1}{||v_1||^2} v_1 - \frac{u_3^T \cdot v_2}{||v_2||^2} v_2 = u_3 - \frac{1}{2} v_1 - \frac{1}{6} v_2 =$$
$$= \left(-\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}, 1\right)^T.$$

Máme tedy celkem

$$v_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} -1 \\ -1 \\ 2 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} -1 \\ -1 \\ -1 \\ 3 \end{pmatrix}.$$

Dodejme, že pro jednoduchost příkladu lze bezprostředně uvést ortogonální bázi z vektorů

$$(1, -1, 0, 0)^T, \quad (0, 0, 1, -1)^T, \quad (1, 1, -1, -1)^T$$

nebo

$$(-1, 1, 1, -1)^T, \quad (1, -1, 1, -1)^T, \quad (-1, -1, 1, 1)^T. \quad \square$$

*2.63.* Určete nějakou bázi vektorového prostoru antisymetrických reálných čtvercových matic typu $4 \times 4$. Uvažte standardní skalární součin v této bázi a pomocí tohoto součinu vyjádřete velikost matice

$$\begin{pmatrix} 0 & 3 & 1 & 0 \\ -3 & 0 & 1 & 2 \\ -1 & -1 & 0 & 2 \\ 0 & -2 & -2 & 0 \end{pmatrix}.$$

**2.64.** Najděte ortogonální doplněk $U^\perp$ podprostoru

$$U = \{(x_1, x_2, x_3, x_4) \mid x_1 = x_3, x_2 = x_3 + 6x_4\} \subseteq \mathbb{R}^4.$$

**Řešení.** Ortogonální doplněk $U^\perp$ tvoří právě ty vektory, které jsou kolmé na každé řešení soustavy

$$\begin{aligned} x_1 \quad - \quad x_3 \quad = \quad 0, \\ x_2 \quad - \quad x_3 \quad - \quad 6x_4 \quad = \quad 0. \end{aligned}$$

Vektor je ovšem řešením této soustavy tehdy a jenom tehdy, když je kolmý na oba vektory $(1, 0, -1, 0)$, $(0, 1, -1, -6)$. Je tedy

$$U^\perp = \{a \cdot (1, 0, -1, 0) + b \cdot (0, 1, -1, -6) \mid a, b \in \mathbb{R}\}. \quad \square$$

Jsou-li $u$, $v$ vlastní vektory příslušné k témuž vlastnímu číslu $\lambda$, pak i pro jejich jakoukoliv lineární kombinaci platí

$$f(au + bv) = af(u) + bf(v) = \lambda(au + bv).$$

Proto tvoří vlastní vektory příslušné k vlastnímu číslu $\lambda$, společně s nulovým vektorem, netriviální vektorový podprostor $V_\lambda$, tzv. vlastní podprostor příslušný $\lambda$. Např., je-li $\lambda = 0$ vlastním číslem, je jádro $\operatorname{Ker} f$ vlastním podprostorem $V_0$.

Z definice vlastních čísel je zřejmé, že jejich výpočet nemůže záviset na volbě báze a tedy matice zobrazení $f$. Skutečně, jako přímý důsledek transformačních vlastností z odstavce 2.38 a Cauchyovy věty 2.19 pro výpočet determinantu součinu dostáváme jinou volbou souřadnic matici $A' = P^{-1}AP$ s invertibilní maticí $P$ a

$$|P^{-1}AP - \lambda E| = |P^{-1}AP - P^{-1}\lambda EP| =$$
$$= |P^{-1}(A - \lambda E)P| = |P^{-1}||(A - \lambda E||P| =$$
$$= |A - \lambda E|,$$

protože násobení skalárů je komutativní a $|P^{-1}| = |P|^{-1}$.

Z těchto důvodů používáme pro matice a zobrazení společnou terminologii:

CHARAKTERISTICKÝ POLYNOM MATICE A ZOBRAZENÍ

Pro matici $A$ dimenze $n$ nad $\mathbb{K}$ nazýváme polynom $|A - \lambda E| \in \mathbb{K}_n[\lambda]$ *charakteristický polynom matice* $A$.

Kořeny tohoto polynomu jsou *vlastní čísla matice* $A$. Je-li $A$ matice zobrazení $f : V \to V$ v jisté bázi, pak $|A - \lambda E|$ nazýváme také *charakteristický polynom zobrazení* $f$.

Protože je charakteristický polynom lineárního zobrazení $f : V \to V$ nezávislý na volbě báze $V$, jsou i jeho koeficienty u jednotlivých mocnin proměnné $\lambda$ skaláry vyjadřující vlastnosti zobrazení $f$, tj. nemohou záviset na naší volbě báze. Zejména jako jednoduché cvičení na počítání determinantů vyjádříme koeficienty u nejvyšších a nejnižších mocnin (předpokládáme $\dim V = n$ a matici zobrazení $A = (a_{ij})$ v nějaké bázi):

$$|A - \lambda \cdot E| = (-1)^n \lambda^n + (-1)^{n-1}(a_{11} + \cdots + a_{nn}) \cdot \lambda^{n-1} +$$
$$+ \cdots + |A| \cdot \lambda^0.$$

Koeficient u nejvyšší mocniny jen říká, zda je dimenze prostoru $V$ sudá nebo lichá. O determinantu matice zobrazení jsme už zmiňovali, že vyjadřuje, kolikrát dané lineární zobrazení zvětšuje objemy.

Zajímavé je, že i součet diagonálních členů matice zobrazení nezávisí na volbě báze. Nazýváme jej *stopa matice* a značíme TrA. *Stopa zobrazení* je definována jako stopa jeho matice v libovolné bázi. Ve skutečnosti to natolik překvapivé není, protože metodami z kapitoly osmé je snadné ověřit, že stopa je ve skutečnosti lineárním přiblížením determinantu v okolí jednotkové matice $E$ (uvažujeme determinant vyčíslený na maticích v křivce $t \mapsto E + tA$, tj. tzv. derivaci determinantu ve směru $A$).

V dalším si uvedeme několik podstatných vlastností vlastních podprostorů.

**2.47. Věta.** *Vlastní vektory lineárního zobrazení $f : V \to V$ příslušné různým vlastním hodnotám jsou lineárně nezávislé.*

**2.65.** Nalezněte nějakou ortonormální bázi podprostoru $V \subseteq \mathbb{R}$, kde $V = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid x_1 + 2x_2 + x_3 = 0\}$.

**Řešení.** Vidíme, že čtvrtá souřadnice se v omezení na podprostor nevyskytuje, bude tedy vhodné volit za jeden z vektorů hledané ortonormální báze vektor $(0, 0, 0, 1)$ a redukovat problém do prostoru $\mathbb{R}^3$. I dále se zkusíme vyhnout počítání: vidíme, že položíme-li druhou souřadnici rovnu nule, tak ve vyšetřovaném prostoru leží vektory s opačnou první a třetí souřadnicí, zejména jednotkový vektor $(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}, 0)$. Na tento vektor je kolmý libovolný vektor, který má stejnou první a třetí souřadnici. Abychom se dostali do uvažovaného podprostoru, volíme druhou souřadnici rovnu záporné hodnotě součtu první a třetí souřadnice a normujeme, tedy volíme vektor $(\frac{1}{\sqrt{6}}, -\frac{2}{\sqrt{6}}, \frac{1}{\sqrt{6}}, 0)$ a jsme hotovi. □

### J. Vlastní čísla a vlastní vektory

**2.66.** Nalezněte vlastní čísla a jim příslušné vektorové prostory vlastních vektorů matice

$$A = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 3 & 0 \\ 2 & -2 & 2 \end{pmatrix}.$$

**Řešení.** Nejprve sestavíme charakteristický polynom dané matice:

$$\begin{vmatrix} -1-\lambda & 1 & 0 \\ -1 & 3-\lambda & 0 \\ 2 & -2 & 2-\lambda \end{vmatrix} = \lambda^3 - 4\lambda^3 + 2\lambda + 4.$$

Tento polynom má kořeny $2, 1+\sqrt{3}, 1-\sqrt{3}$, což jsou tak vlastní čísla zadané matice. Jejich algebraická násobnost je jedna (jsou to jednoduché kořeny charakteristického polynomu), každému tedy bude odpovídat právě jeden (až na nenulový násobek) vlastní vektor (tj. jejich tzv. geometrická násobnost bude také jedna, viz 2.52).

Určeme vlastní vektor příslušný vlastnímu číslu 2 (je řešením homogenní lineární soustavy s maticí $A - 2E$):

$$\begin{aligned} -3x_1 + x_2 &= 0, \\ -x_1 + x_2 &= 0, \\ 2x_1 - 2x_2 &= 0. \end{aligned}$$

Soustava má řešení $x_1 = x_2 = 0$, $x_3 \in \mathbb{R}$ libovolné, vlastním vektorem příslušným vlastní hodnotě 2 je tedy například vektor $(0, 0, 1)$ (a libovolný jeho nenulový násobek).

Analogickým způsobem určíme i zbývající dva vlastní vektory jakožto řešení soustavy $[A - (1+\sqrt{3})E]x = 0$, respektive $[A - (1+\sqrt{3})E]x = 0$. Řešením soustavy

$$\begin{aligned} (-2-\sqrt{3})x_1 + x_2 &= 0, \\ -x_1 + (2-\sqrt{3})x_2 &= 0, \\ 2x_1 - 2x_2 + (1-\sqrt{3})x_3 &= 0 \end{aligned}$$



Důkaz. Nechť $a_1, \dots, a_k$ jsou různé vlastní hodnoty zobrazení $f$ a $u_1, \dots, u_k$ vlastní vektory s těmito vlastními hodnotami. Důkaz provedeme indukcí přes počet lineárně nezávislých vektorů mezi zvolenými. Předpokládejme, že $u_1, \dots, u_\ell$ jsou lineárně nezávislé a $u_{l+1} = \sum_i c_i u_i$ je jejich lineární kombinací. Alespoň $\ell = 1$ lze zvolit, protože vlastní vektory jsou nenulové. Pak ovšem $f(u_{\ell+1}) = a_{l+1} \cdot u_{l+1} = \sum_{i=1}^{l} a_{l+1} \cdot c_i \cdot u_i$, tj.

$$f(u_{l+1}) = \sum_{i=1}^{l} a_{l+1} \cdot c_i \cdot u_i = \sum_{i=1}^{l} c_i \cdot f(u_i) = \sum_{i=1}^{l} c_i \cdot a_i \cdot u_i.$$

Odečtením druhého a čtvrtého výrazu v rovnostech dostáváme $0 = \sum_{i=1}^{l} (a_{l+1} - a_i) \cdot c_i \cdot u_i$. Všechny rozdíly vlastních hodnot jsou však nenulové a alespoň jeden koeficient $c_i$ je nenulový. To je spor s předpokládanou nezávislostí $u_1, \dots, u_\ell$, takže i vektor $u_{l+1}$ musí být lineárně nezávislý na předchozích. □

Na právě dokázané tvrzení se můžeme podívat jako na rozklad lineárního zobrazení $f$ na součet jednoduchých zobrazení. Pro vesměs různé vlastní hodnoty $\lambda_i$ charakteristického polynomu budeme dostávat jednorozměrné vlastní podprostory $V_{\lambda_i}$. Každý z nich pak zadává projekci na tento invariantní jednorozměrný podprostor, na němž je zobrazení dáno jako násobení vlastním číslem $\lambda_i$. Celý prostor $V$ je tak rozložen na přímý součet jednotlivých vlastních podprostorů. Navíc lze tento rozklad na vlastní podprostory snadno spočíst:

Báze z vlastních vektorů

**Důsledek.** *Jestliže existuje $n$ navzájem různých kořenů $\lambda_i$ charakteristického polynomu zobrazení $f : V \to V$ na $n$-rozměrném prostoru $V$, pak existuje rozklad $V$ na přímý součet vlastních podprostorů dimenze 1. To znamená, že existuje báze $V$ složená výhradně z vlastních vektorů a v této bázi má $f$ diagonální matici. Tato báze je určena jednoznačně až na pořadí prvků.*

*Příslušnou bázi (vyjádřenou v souřadnicích vzhledem k libovolně zvolené bázi $V$) obdržíme řešením $n$ systémů homogenních lineárních rovnic o $n$ neznámých s maticemi $(A - \lambda_i \cdot E)$, kde $A$ je matice $f$ ve zvolené bázi.*

**2.48. Invariantní podprostory.** Viděli jsme, že každý vlastní vektor $v$ zobrazení $f : V \to V$ generuje podprostor $\langle v \rangle \subseteq V$, který je zobrazením $f$ zachováván.



Obecněji říkáme, že vektorový podprostor $W \subseteq V$ je *invariantní podprostor* pro lineární zobrazení $f$, jestliže platí $f(W) \subseteq W$.

Jestliže je $V$ konečně rozměrný vektorový prostor a vybereme nějakou bázi $(u_1, \dots, u_k)$ podprostoru $W$, můžeme ji vždy doplnit na bázi $(u_1, \dots, u_k, u_{k+1}, \dots, u_n)$ celého $V$ a v každé takové bázi má naše zobrazení matici $A$ tvaru

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}, \tag{2.5}$$

kde $B$ je čtvercová matice dimenze $k$, $D$ je čtvercová matice dimenze $n - k$ a $C$ je matice typu $n/(n-k)$. Naopak, jestliže je v nějaké bázi $(u_1, \dots, u_n)$ matice zobrazení $f$ tvaru (2.5), je $W = \langle u_1, \dots, u_k \rangle$ invariantní podprostor zobrazení $f$.

je prostor $\left\{\left(\left(\frac{\sqrt{3}}{2}-1\right)t, -\frac{t}{2}\right);\ t\in\mathbb{R}\right\}$. To je tedy prostor vlastních vektorů příslušných vlastní hodnotě $1+\sqrt{3}$ (mimo nulového vektoru, který sice je řešením dané soustavy, ale za vlastní vektor jej nepovažujeme; tuto záležitost již nebudeme více zmiňovat a nebudeme nulový vektor explicitně vylučovat z množiny řešení).

Obdobně pak dostaneme, že prostor vlastních vektorů příslušných vlastní hodnotě $1-\sqrt{3}$ je $\langle(-1-\frac{\sqrt{3}}{2}, -\frac{1}{2}, 1)\rangle$. □

**2.67. Příklad i se změnou báze.** Určete vlastní čísla a vlastní vektory matice

$$A=\begin{pmatrix}1&1&0\\1&2&1\\1&2&1\end{pmatrix}.$$

Popište geometrickou interpretaci tohoto zobrazení a napište jeho matici v bázi:

$$\begin{aligned}e_1 &= (1,-1,1),\\ e_2 &= (1,2,0),\\ e_3 &= (0,1,1).\end{aligned}$$

**Řešení.** Charakteristický polynom dané matice je

$$\begin{vmatrix}1-\lambda&1&0\\1&2-\lambda&1\\1&2&1-\lambda\end{vmatrix}=-\lambda^3+4\lambda^2-2\lambda=-\lambda(\lambda^2-4\lambda+2).$$

Kořeny tohoto polynomu, vlastní čísla, udávají, kdy nebude mít matice

$$\begin{pmatrix}1-\lambda&1&0\\1&2-\lambda&1\\1&2&1-\lambda\end{pmatrix}$$

plnou hodnost, tedy soustava rovnic

$$\begin{pmatrix}1-\lambda&1&0\\1&2-\lambda&1\\1&2&1-\lambda\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}$$

bude mít i jiné řešení než řešení $x=(0,0,0)$. Vlastní čísla tedy jsou $0, 2+\sqrt{2}, 2-\sqrt{2}$. Spočítejme vlastní vektory příslušné jednotlivým vlastním hodnotám:

- 0: Řešíme tedy soustavu

$$\begin{pmatrix}1&1&0\\1&2&1\\1&2&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=0.$$

  Jejím řešením je jednodimenzionální vektorový prostor vlastních vektorů $\langle(1,-1,1)\rangle$.

- $2+\sqrt{2}$: Řešíme soustavu

$$\begin{pmatrix}-(1+\sqrt{2})&1&0\\1&-\sqrt{2}&1\\1&2&-(1+\sqrt{2})\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=0.$$

Pochopitelně bude v naší matici zobrazení (2.5) submatice $C$ nulová právě tehdy, když bude i podprostor $\langle u_{k+1},\dots,u_n\rangle$ generovaný doplněnými vektory báze invariantní.

Z tohoto pohledu jsou vlastní podprostory lineárního zobrazení extrémní případy invariantních podprostorů a zejména v případě existence $n=\dim V$ různých vlastních čísel zobrazení $f$ dostáváme rozklad $V$ na přímý součet $n$ vlastních podprostorů. V příslušné bázi z vlastních vektorů má pak naše zobrazení diagonální tvar s vlastními čísly na diagonále.

**2.49.** Vlastní čísla a vlastní vektory mohou sloužit k názornému popisu lineárních zobrazení, zejména v $\mathbb{R}^2$ a $\mathbb{R}^3$.

(1) Uvažme zobrazení s maticí ve standardní bázi

$$f:\mathbb{R}^3\to\mathbb{R}^3,\ A=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}.$$

Pak dostáváme

$$|A-\lambda E|=\begin{vmatrix}-\lambda&0&1\\0&1-\lambda&0\\1&0&-\lambda\end{vmatrix}=-\lambda^3+\lambda^2+\lambda-1$$

s kořeny $\lambda_{1,2}=1, \lambda_3=-1$. Vlastní vektory s vlastní hodnotou $\lambda=1$ se spočtou:

$$\begin{pmatrix}-1&0&1\\0&0&0\\1&0&-1\end{pmatrix}\sim\begin{pmatrix}1&0&-1\\0&0&0\\0&0&0\end{pmatrix};$$

s bází prostoru řešení, tj. všech vlastních vektorů s touto vlastní hodnotou

$$u_1=(0,1,0),\quad u_2=(1,0,1).$$

Podobně pro $\lambda=-1$ dostáváme třetí nezávislý vlastní vektor

$$\begin{pmatrix}1&0&1\\0&2&0\\1&0&1\end{pmatrix}\sim\begin{pmatrix}1&0&1\\0&2&0\\0&0&0\end{pmatrix}\Rightarrow u_3=(-1,0,1).$$

V bázi $u_1, u_2, u_3$ (všimněte si, že $u_3$ musí být lineárně nezávislý na zbylých dvou díky větě 2.47 a $u_1, u_2$ vyšly jako dvě nezávislá řešení) má $f$ diagonální matici

$$A=\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}.$$

Celý prostor $\mathbb{R}^3$ je přímým součtem vlastních podprostorů, $\mathbb{R}^3=V_1\oplus V_2$, $\dim V_1=2$, $\dim V_2=1$. Tento rozklad je dán jednoznačně a vypovídá mnoho o geometrických vlastnostech zobrazení $f$. Vlastní podprostor $V_1$ je navíc přímým součtem jednorozměrných vlastních podprostorů, které lze však zvolit mnoha různými způsoby (takový další rozklad nemá tedy již žádný geometrický význam).

(2) Uvažme lineární zobrazení $f:\mathbb{R}_2[x]\to\mathbb{R}_2[x]$ definované derivováním polynomů, tj. $f(1)=0$, $f(x)=1$, $f(x^2)=2x$. Zobrazení $f$ má tedy v obvyklé bázi $(1,x,x^2)$ matici

$$A=\begin{pmatrix}0&1&0\\0&0&2\\0&0&0\end{pmatrix}.$$

Řešením je prostor $\left\langle\left(1, 1+\sqrt{2}, 1+\sqrt{2}\right)\right\rangle$, který je jednodimenzionální.

- $2-\sqrt{2}$: Řešíme soustavu

$$\begin{pmatrix} (\sqrt{2}-1) & 1 & 0 \\ 1 & \sqrt{2} & 1 \\ 1 & 2 & (\sqrt{2}-1) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 0.$$

Řešením je prostor vlastních vektorů $\left\langle\left(1, 1-\sqrt{2}, 1-\sqrt{2}\right)\right\rangle$.

Daná matice má vlastní čísla 0, $2+\sqrt{2}$ a $2-\sqrt{2}$, kterým přísluší po řadě jednorozměrné prostory vlastních vektorů $\langle(1,-1,1)\rangle$, $\langle(1,\ 1+\sqrt{2},\ 1+\sqrt{2})\rangle$ a $\langle(1, 1-\sqrt{2}, 1-\sqrt{2})\rangle$.

Zobrazení tedy můžeme interpretovat jako projekci podél vektoru $(1,-1,1)$ do roviny dané vektory $(1, 1+\sqrt{2}, 1+\sqrt{2})$ a $(1,\ 1-\sqrt{2},\ 1-\sqrt{2})$ složenou s lineárním zobrazením daným „natažením“ daným vlastními čísly ve směru uvedených vlastních vektorů.

Nyní jej vyjádřeme v uvedené bázi. K tomu budeme potřebovat matici přechodu $T$ od standardní báze k dané nové bázi. Tu získáme tak, že souřadnice vektorů staré báze v bázi nové napíšeme do sloupců matice $T$. My však snadněji zapíšeme matici přechodu od dané báze k bázi standardní, tedy matici $T^{-1}$. Souřadnice vektorů nové báze pouze zapíšeme do sloupců:

$$T^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Potom

$$T = T^{-1^{-1}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ -2 & 1 & 3 \end{pmatrix},$$

a pro matici $B$ zobrazení v nové bázi pak máme (viz 2.38)

$$B = TAT^{-1} = \begin{pmatrix} 0 & 5 & 2 \\ 0 & -2 & -1 \\ 0 & 14 & 6 \end{pmatrix}.$$

□

**2.68.** Pro libovolnou $n \times n$ matici $A$ je její charakteristický polynom $|A-\lambda E|$ stupně $n$ tvaru

$$|A-\lambda E| = c_n\lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_1\lambda + c_0, \quad c_n \neq 0,$$

přičemž platí

$$c_n = (-1)^n, \quad c_{n-1} = (-1)^{n-1}\operatorname{tr} A, \quad c_0 = |A|.$$

Jestliže je matice $A$ trojrozměrná, obdržíme

$$|A-\lambda E| = -\lambda^3 + (\operatorname{tr} A)\lambda^2 + c_1\lambda + |A|.$$

Volbou $\lambda = 1$ dostáváme

$$|A-E| = -1 + \operatorname{tr} A + c_1 + |A|.$$

Charakteristický polynom je $|A-\lambda\cdot E| = -\lambda^3$, existuje tedy pouze jediná vlastní hodnota $\lambda = 0$. Spočtěme vlastní vektory:

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Prostor vlastních vektorů je tedy jednorozměrný, generovaný konstantním polynomem 1.

**2.50. Ortogonální zobrazení.** Podívejme se teď na speciální případ zobrazení $f : V \to W$ mezi prostory se skalárními součiny, která zachovávají velikosti pro všechny vektory $u \in V$.



DEFINICE ORTOGONÁLNÍCH ZOBRAZENÍ

Lineární zobrazení $f : V \to W$ mezi prostory se skalárním součinem se nazývá *ortogonální zobrazení*, jestliže pro všechny $u \in V$ platí

$$\langle f(u), f(u)\rangle = \langle u, u\rangle.$$

Z linearity $f$ a ze symetrie skalárního součinu vyplývá pro všechny dvojice vektorů rovnost

$$\langle f(u+v), f(u+v)\rangle = \langle f(u), f(u)\rangle + \langle f(v), f(v)\rangle + 2\langle f(u), f(v)\rangle.$$

Proto všechny ortogonální zobrazení splňují i zdánlivě silnější požadavek, aby platilo pro všechny vektory $u, v \in V$

$$\langle f(u), f(v)\rangle = \langle u, v\rangle.$$

V úvodní diskusi o geometrii v rovině jsme ve Větě 1.33 dokázali, že lineární zobrazení $\mathbb{R}^2 \to \mathbb{R}^2$ zachovává velikosti vektorů, právě když jeho matice ve standardní bázi (a ta je ortonormální vzhledem ke standardnímu skalárnímu součinu) splňuje $A^T \cdot A = E$, tj. $A^{-1} = A^T$.

Obecně, ortogonální zobrazení $f : V \to W$ musí být vždy injektivní, protože podmínka $\langle f(u), f(u)\rangle = 0$ znamená i $\langle u, u\rangle = 0$ a tedy $u = 0$. Je tedy vždy v takovém případě dimenze oboru hodnot alespoň taková, jako je dimenze definičního oboru $f$. Pak ovšem je dimenze obrazu rovna dimenzi oboru hodnot a víme, že $f : V \to \operatorname{Im} f$ je bijekce. Pokud $\operatorname{Im} f \neq W$, doplníme ortonormální bázi na obrazu $f$ na ortonormální bázi cílového prostoru a matice zobrazení bude obsahovat čtvercovou regulární matici $A$ doplněnou nulovými řádky na potřebnou velikost. Bez újmy na obecnosti tedy předpokládejme $W = V$.

Naše podmínka pro matici ortogonálního zobrazení v ortonormální bázi pak říká pro všechny vektory $x$ a $y$ v prostoru $\mathbb{K}^n$ toto:

$$(A\cdot x)^T \cdot (A\cdot y) = x^T \cdot (A^T\cdot A)\cdot y = x^T \cdot y.$$

Speciálními volbami vektorů standardní báze za $x$ a $y$ dostaneme přímo, že $A^T \cdot A = E$, tedy tentýž výsledek jako v dimenzi dvě. Dokázali jsme tak následující tvrzení:

MATICE ORTOGONÁLNÍCH ZOBRAZENÍ

**Věta.** *Nechť $V$ je reálný vektorový prostor se skalárním součinem a $f : V \to V$ je lineární zobrazení. Pak $f$ je ortogonální, právě když v některé ortonormální bázi (a pak už ve všech) má matici $A$ splňující $A^T = A^{-1}$.*

Odsud získáváme vyjádření

$$|A-\lambda E| = -\lambda^3 + (\operatorname{tr} A)\lambda^2 + (|A-E|+1-\operatorname{tr} A - |A|)\lambda + |A|.$$

Využijte toto vyjádření k určení charakteristického polynomu a vlastních hodnot matice

$$A = \begin{pmatrix} 32 & -67 & 47 \\ 7 & -14 & 13 \\ -7 & 15 & -6 \end{pmatrix}.$$

Další základní příklady na vlastní čísla a vektory matic naleznete na straně 116

*2.69.* **Pauliho matice.** Ve fyzice se stav částice se spinem $\frac{1}{2}$ popisuje Pauliho maticemi. Jsou to následující matice $2 \times 2$ nad komplexními čísly

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Pro čtvercové matice definujeme jejich *komutátor* (značený hranatými závorkami) jako $[\sigma_1, \sigma_2] := \sigma_1\sigma_2 - \sigma_2\sigma_1$.

Ukažte, že platí $[\sigma_1, \sigma_2] = 2i\sigma_3$ a podobně $[\sigma_1, \sigma_3] = 2i\sigma_2$ a $[\sigma_2, \sigma_3] = 2i\sigma_1$. Dále ukažte, že $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = 1$ a že vlastní hodnoty matic $\sigma_1, \sigma_2, \sigma_3$ jsou $\pm 1$.

Ukažte, že pro matice popisující stav částice se spinem 1

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & -i & 0 \\ i & 0 & -i \\ 0 & i & 0 \end{pmatrix},\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

platí stejné komutační relace jako v případě Pauliho matic.

Ekvivalentně lze ukázat, že při označení

$$1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I := i\sigma_3,\ J := i\sigma_2,\ K := i\sigma_1$$

tvoří vektorový prostor s bází $(1, I, J, K)$ algebru kvaternionů (algebra je vektorový prostor s binární bilineární operací násobení; v tomto případě je toto násobení dáno násobením matic). K tomu, aby uvažovaný prostor byl skutečně algebrou kvaternionů, je nutné a stačí ukázat následující vlastnosti: $I^2 = J^2 = K^2 = -1$ a $IJ = -JI = K$, $JK = -KJ = I$ a $KI = -IK = J$.

*2.70.* Uveďte dimenze vlastních podprostorů jednotlivých vlastních hodnot $\lambda_i$ matice

$$\begin{pmatrix} 4 & 0 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 5 & 2 & 3 & 0 \\ 0 & 4 & 0 & 3 \end{pmatrix}.$$

○

*2.71.* Lze vyjádřit matici

$$B = \begin{pmatrix} 5 & 6 \\ 6 & 5 \end{pmatrix}$$

Důkaz. Skutečně, jestliže zachovává $f$ velikosti, musí mít uvedenou vlastnost v každé ortonormální bázi. Naopak, předchozí výpočet ukazuje, že vlastnost matice v jedné bázi už zaručuje zachovávání velikostí. □

Čtvercovým maticím, které splňují rovnost $A^T = A^{-1}$, říkáme *ortogonální matice*.

Důsledkem předchozí věty je také popis všech matic přechodu



$S$ mezi ortonormálními bázemi. Každá totiž musí zadávat zobrazení $\mathbb{K}^n \to \mathbb{K}^n$ zachovávající velikosti a splňují tady také právě podmínku $S^{-1} = S^T$. Při přechodu od jedné ortonormální báze ke druhé se tedy matice (libovolných) lineárních zobrazení mění podle vztahu

$$A' = S^T A\, S\,.$$

**2.51. Rozklad ortogonálního zobrazení.** Podívejme se nyní po-



drobněji na vlastní vektory a vlastní čísla ortogonálních zobrazení na reálném vektorovém prostoru $V$ se skalárním součinem.

Uvažujme pevně zvolené ortogonální zobrazení $f : V \to V$ s maticí $A$ v nějaké ortonormální bázi a zkusme postupovat obdobně jako s maticí rotace $D$ v příkladu 2.45.

Nejprve se ale podívejme obecně na invariantní podprostory ortogonálních zobrazení a jejich ortogonální doplňky. Jestliže pro libovolný podprostor $W \subseteq V$ a ortogonální zobrazení $f : V \to V$ platí $f(W) \subseteq W$, pak také platí pro všechny $v \in W^\perp$, $w \in W$

$$\langle f(v), w\rangle = \langle f(v), f \circ f^{-1}(w)\rangle = \langle v, f^{-1}(w)\rangle = 0,$$

protože i $f^{-1}(w) \in W$. To ale znamená, že také $f(W^\perp) \subseteq W^\perp$. Dokázali jsme tedy jednoduché, ale velice důležité tvrzení:

**Tvrzení.** *Ortogonální doplněk k invariantnímu podprostoru je také invariantní.*

Kdyby byla vlastní čísla ortogonálního zobrazení reálná, zaručovalo by už toto tvrzení, že bude vždy existovat báze $V$ z vlastních vektorů. Skutečně, zúžení $f$ na ortogonální doplněk invariantního podprostoru je opět ortogonální zobrazení, takže můžeme do báze přibírat jeden vlastní vektor za druhým, až dostaneme celý rozklad $V$. Nicméně většinou nejsou vlastní čísla ortogonálních zobrazení reálná. Musíme si proto pomoci opět výletem do komplexních vektorových prostorů. Zformulujeme rovnou výsledek:

Rozklad ortogonálních zobrazení

**Věta.** *Nechť $f : V \to V$ je ortogonální zobrazení na prostoru se skalárním součinem. Pak všechny kořeny charakteristického polynomu $f$ mají velikost jedna a existuje rozklad $V$ na jednorozměrné vlastní podprostory odpovídající vlastním číslům $\lambda = \pm 1$ a dvourozměrné podprostory $P_{\lambda,\bar\lambda}$, na kterých působí $f$ rotací o úhel rovný argumentu komplexního čísla $\lambda$ v kladném směru. Všechny tyto různé podprostory jsou po dvou ortogonální.*

Důkaz. Bez újmy na obecnosti můžeme pracovat s prostorem



$V = \mathbb{R}^m$ se standardním skalárním součinem. Zobrazení tedy bude dáno ortogonální maticí $A$, kterou můžeme stejně považovat za matici lineárního zobrazení na komplexním prostoru $\mathbb{C}^m$ (která je jen shodou okolností reálná). Zaručeně bude existovat právě $m$ (komplexních)

ve tvaru součinu $B = P^{-1} \cdot D \cdot P$ pro nějakou diagonální matici $D$ a invertibilní matici $P$? Pokud je to možné, udejte příklad takové dvojice matic $D$, $P$ a zjistěte, kolik takových dvojic existuje. ◯

Jak jsme viděli v ‖2.67‖, na základě vlastních hodnot a vektorů dané matice $3 \times 3$ umíme často geometricky interpretovat zobrazení, které tato matice zadává ve standardní bázi v $\mathbb{R}^3$. Umíme to zejména v těchto situacích:

Má-li matice vlastní číslo 0 a vlastní číslo 1 s geometrickou násobností 2, tak se jedná o projekci ve směru vlastního vektoru příslušného vlastní hodnotě 0 na rovinu vlastních vektorů příslušných vlastní hodnotě 1. Pokud je vlastní vektor příslušný vlastní hodnotě 0 kolmý na rovinu vlastních vektorů příslušných hodnotě 1, pak se jedná o kolmou projekci.

Má-li matice vlastní číslo $-1$ s vlastním vektorem kolmým na rovinu vlastních vektorů příslušných vlastní hodnotě 1, jde o zrcadlení podle roviny vlastních vektorů příslušných vlastní hodnotě 1.

Má-li matice vlastní číslo 1 s vlastním vektorem kolmým na rovinu vlastních vektorů příslušných vlastní hodnotě $-1$, jedná se o osovou symetrii (v prostoru) podle osy dané vlastním vektorem příslušným vlastní hodnotě 1.

**2.72.** Určete geometrický význam lineárního zobrazení $\mathbb{R}^3 \to \mathbb{R}^3$ zadaného maticí

$$\begin{pmatrix} -\frac{2}{3} & -\frac{1}{3} & -\frac{2}{3} \\ \frac{4}{3} & -\frac{7}{3} & -\frac{8}{3} \\ -1 & 1 & 1 \end{pmatrix}$$

**Řešení.** Matice má dvojnásobnou vlastní hodnotu $-1$, jí příslušný prostor vlastních vektorů je $\langle (2,0,1), (1,1,0) \rangle$. Dále má matice vlastní hodnotu 0, s vlastním vektorem $(1,4,-3)$. Zobrazení dané touto maticí ve standardní bázi je tudíž projekce podle vektoru $(1,4,3)$ následovaná středovou symetrií podle počátku. □

**2.73.** Věta 2.51 nám dává do ruky nástroje, jak poznat matici rotace v $\mathbb{R}^3$: má tři různá vlastní čísla s absolutní hodnotou 1, jedno z nich je přímo číslo 1 (jemu příslušný vlastní vektor je osa rotace). Argument zbylých dvou, tedy nutně komplexně sdružených, vlastních čísel potom udává úhel rotace v kladném smyslu v rovině určené bází $u_\lambda + \overline{u_\lambda}$, $i[u_\lambda - \overline{u_\lambda}]$.

**2.74.** Určete, jaké lineární zobrazení zadává matice

$$\begin{pmatrix} -\frac{1}{5} & \frac{3}{5} & -\frac{1}{5} \\ -\frac{8}{5} & \frac{9}{5} & \frac{2}{5} \\ \frac{8}{5} & -\frac{4}{5} & \frac{3}{5} \end{pmatrix}.$$

kořenů charakteristického polynomu, včetně jejich algebraické násobnosti (viz tzv. základní věta algebry, 11.20 na str. 663). Navíc, protože charakteristický polynom zobrazení bude mít výhradně reálné koeficienty, budou tyto kořeny buď reálné, nebo půjde o dvojice komplexně sdružených kořenů $\lambda$ a $\bar{\lambda}$. Příslušné vlastní vektory v $\mathbb{C}^m$ k takové dvojici komplexně sdružených vlastních čísel budou řešením dvou komplexně sdružených systémů homogenních lineárních rovnic, neboť příslušné matice systémů rovnic jsou celé reálné, až na samotná dosazená vlastní čísla. Evidentně proto budou také řešení těchto systémů komplexně sdružené vektory.

Nyní využijeme skutečnost, že ke každému invariantnímu podprostoru je i jeho ortogonální doplněk invariantní. Nejprve si najdeme všechny vlastní podprostory $V_{\pm 1}$ příslušné k reálným vlastním hodnotám a zúžíme naše zobrazení na ortogonální doplněk k jejich součtu. Bez újmy na obecnosti tedy můžeme předpokládat, že naše ortogonální zobrazení nemá žádná reálná vlastní čísla a že je $\dim V = 2n > 0$.

Zvolme nyní nějaké vlastní číslo $\lambda$ a označme $u_\lambda$ vlastní vektor příslušný k vlastnímu číslu $\lambda = \alpha + i\beta$, $\beta \neq 0$. Zcela stejně jako v případě rotace v rovině zadané v odstavci 2.45 maticí $D$ nás zajímá reálná část součtu dvou jednorozměrných podprostorů $\langle u_\lambda \rangle \oplus \langle \bar{u}_\lambda \rangle$, kde $\bar{u}_\lambda$ je vlastní vektor příslušný k vlastnímu číslu $\bar{\lambda}$.

Jde o průnik uvedeného součtu komplexních podprostorů s $\mathbb{R}^{2n}$, který je generovaný vektory $u_\lambda + \bar{u}_\lambda$ a $i(u_\lambda - \bar{u}_\lambda)$, tj. reálný vektorový podprostor $P_\lambda \subseteq \mathbb{R}^{2n}$ generovaný bází danou reálnou a imaginární částí $u_\lambda$

$$x_\lambda = \operatorname{re} u_\lambda, \quad -y_\lambda = -\operatorname{im} u_\lambda.$$

Protože $A \cdot (u_\lambda + \bar{u}_\lambda) = \lambda u_\lambda + \bar{\lambda}\bar{u}_\lambda$ a podobně s druhým bázovým vektorem, jde zjevně o invariantní podprostor vůči násobení maticí $A$ a dostáváme

$$A \cdot x_\lambda = \alpha x_\lambda + \beta y_\lambda, \; A \cdot y_\lambda = -\alpha y_\lambda + \beta x_\lambda.$$

Protože naše zobrazení zachovává velikosti, musí být navíc velikost vlastní hodnoty $\lambda$ rovna jedné. To ale neznamená nic jiného, než že zúžení našeho zobrazení na $P_\lambda$ je rotací o argument vlastní hodnoty $\lambda$. Všimněme si, že volba vlastního čísla $\bar{\lambda}$ místo $\lambda$ vede na stejný podprostor se stejnou rotací, pouze ji dostaneme vyjádřenou v bázi $x_\lambda$, $y_\lambda$, tj. musíme v souřadnicích rotovat o úhel s opačným znaménkem.

Důkaz celé věty je tím dokončen, protože zúžením našeho zobrazení na ortogonální doplněk a opakováním předchozí úvahy dostaneme celý rozklad po $n$ krocích. □

K myšlenkám tohoto důkazu se ještě vrátíme v kapitole třetí, když budeme studovat komplexní rozšíření euklidovských vektorových prostorů, viz 3.26.



**Poznámka.** Speciálně v dimenzi tři musí být alespoň jedno vlastní číslo $\pm 1$, protože je trojka liché číslo. Pak ovšem příslušný vlastní podprostor je osou rotace trojrozměrného prostoru o úhel daný argumentem dalších vlastních čísel. Zkuste si rozmyslet, jak poznat, kterým směrem jde rotace a také, že vlastní číslo $-1$ znamená ještě dodatečné zrcadlení podle roviny kolmé na osu rotace.

**Řešení.** Již známým postupem zjistíme, že matice má následující vlastní čísla a jim příslušné vlastní vektory: $1$, $(1,2,0)$; $\frac{3}{5}+\frac{4}{5}i$, $(1,1+i,-1-i)$; $\frac{3}{5}-\frac{4}{5}i$, $(1,1-i,-1+i)$. Přesto, že absolutní hodnoty všch vlastních hodnot jsou rovny jedné, nejedná se o rotaci, neboť daná matice není ortogonální.

Jde tedy o matici rotace (všechna vlastní čísla mají absolutní hodnotu 1 a jedna z vlastních hodnot je přímo 1). Navíc víme, že se jedná o rotaci o $\arccos\left(\frac{3}{5}\right) \doteq 0{,}295\pi$, což je argument vlastního čísla $\frac{3}{5}+\frac{4}{5}i$. Zbývá určit smysl otáčení. Nejprve je dobré si připomenout, že smysl otáčení se mění s orientací osy (nemá tedy smyslu hovořit o smyslu otáčení, pokud nemáme orientovánu jeho osu. Dle úvah v důkazu věty 2.51 působí daná matice otáčením o $\arccos\left(\frac{3}{5}\right)$) v kladném smyslu v rovině dané bází $((0,1,-1),(1,1,-1))$. První vektor báze je imaginární částí vlastního vektoru příslušného vlastní hodnotě $\frac{3}{5}+\frac{4}{5}i$, druhý pak je (společnou) reálnou částí vlastních vektorů příslušných komplexním vlastním hodnotám. Tady je důležité pořadí vektorů v bázi (prohozením vektorů se změní smysl otáčení). Osa otáčení je kolmá na uvažovanou rovinu. Pokud ji orientujeme podle pravidla pravé ruky (daný kolmý směr také dostaneme vektorovým součinem vektorů v bázi), tak bude smysl otáčení v prostoru souhlasit se smyslem otáčení v rovině s uvedenou bází. V našem případě dostaneme vektorovým součinem $(0,1,-1)\times(1,1,-1)=(0,-1,-1)$. Jedná se tedy o rotaci o $\arccos\left(\frac{3}{5}\right)$ v kladném smyslu kolem vektoru $(0,-1,-1)$, neboli o rotaci o $\arccos\left(\frac{3}{5}\right)$ v záporném smyslu kolem vektoru $(0,1,1)$. □

*2.75.* Bez počítání napište spektrum lineárního zobrazení $f:\mathbb{R}^3\to\mathbb{R}^3$ zadaného přiřazením

$$(x_1,\ x_2,\ {}_3)\mapsto(x_1+x_3,\ x_2,\ x_1+x_3).$$ ○

K diskusi vlastností matic a lineárních zobrazení se budeme vracet. Před pokračováním obecné teorie si napřed ukážeme v následující kapitole několik aplikací, ještě ale uzavřeme naši diskusi obecnou definicí:

### Spektrum lineárního zobrazení

**2.52. Definice.** *Spektrum lineárního zobrazení* $f:V\to V$ (resp. matice) je posloupnost kořenů charakteristického polynomu zobrazení $f$, včetně násobností. *Algebraickou násobností* vlastní hodnoty rozumíme její násobnost jakožto kořenu charakteristického polynomu, *geometrická násobnost* vlastní hodnoty je dimenze příslušného podprostoru vlastních vektorů.

*Spektrálním poloměrem* lineárního zobrazení (matice) je největší z absolutní hodnot vlastních čísel.

V této terminologii můžeme naše výsledky o ortogonálních zobrazeních zformulovat tak, že jejich spektra jsou vždy celá podmnožinou jednotkové kružnice v komplexní rovině. To znamená, že v reálné části spektra mohou být pouze hodnoty $\pm1$, jejichž algebraické a geometrické násobnosti jsou stejné. Komplexní hodnoty spektra pak odpovídají rotacím ve vhodných dvourozměrných podprostorech, které jsou na sebe po dvou kolmé.

### K. Doplňující příklady k celé kapitole

**2.76.** Řešte soustavu

$$\begin{array}{rcrcrcrcrcl} x_1 & + & x_2 & + & x_3 & + & x_4 & - & 2x_5 & = & 3,\\ & & 2x_2 & + & 2x_3 & + & 2x_4 & - & 4x_5 & = & 5,\\ -x_1 & - & x_2 & - & x_3 & + & x_4 & + & 2x_5 & = & 0,\\ -2x_1 & + & 3x_2 & + & 3x_3 & & & - & 6x_5 & = & 2. \end{array}$$

**Řešení.** Rozšířená matice soustavy je

$$\left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & -2 & 3\\ 0 & 2 & 2 & 2 & -4 & 5\\ -1 & -1 & -1 & 1 & 2 & 0\\ -2 & 3 & 3 & 0 & -6 & 2 \end{array}\right).$$

Přičtením prvního řádku ke třetímu a jeho dvojnásobku ke čtvrtému a poté přičtením $(-5/2)$násobku druhého řádku ke čtvrtému obdržíme

$$\left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & -2 & 3\\ 0 & 2 & 2 & 2 & -4 & 5\\ 0 & 0 & 0 & 2 & 0 & 3\\ 0 & 5 & 5 & 2 & -10 & 8 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & -2 & 3\\ 0 & 2 & 2 & 2 & -4 & 5\\ 0 & 0 & 0 & 2 & 0 & 3\\ 0 & 0 & 0 & -3 & 0 & -9/2 \end{array}\right).$$

Poslední řádek je zřejmě násobkem předposledního, a tak jej můžeme vynechat. Pivoti se nacházejí v 1., 2. a 4. sloupci, proto jsou volné proměnné $x_3$ a $x_5$, které nahradíme reálnými parametry $t$, $s$. Uvažujeme tak soustavu

$$\begin{array}{rcrcrcrcrcl} x_1 & + & x_2 & + & t & + & x_4 & - & 2s & = & 3,\\ & & 2x_2 & + & 2t & + & 2x_4 & - & 4s & = & 5,\\ & & & & & & 2x_4 & & & = & 3. \end{array}$$

Víme tedy, že $x_4 = 3/2$. Druhá rovnice dává

$$2x_2 + 2t + 3 - 4s = 5, \quad \text{tj.} \quad x_2 = 1 - t + 2s.$$

Z první potom plyne

$$x_1 + 1 - t + 2s + t + 3/2 - 2s = 3, \quad \text{tj.} \quad x_1 = 1/2.$$

Celkem máme

(2.1)

$$(x_1,\, x_2,\, x_3,\, x_4,\, x_5) = (1/2,\, 1 - t + 2s,\, t,\, 3/2,\, s), \quad t, s \in \mathbb{R}.$$

Také v tomto příkladu znovu uvažujme rozšířenou matici a převeďme ji pomocí řádkových úprav do schodovitého tvaru, kde první nenulové číslo v každém řádku je 1 a kde ve sloupci, ve kterém tato 1 je, jsou ostatní čísla 0. Ještě připomeňme, že čtvrtou rovnici, jež je kombinací prvních třech rovnic, budeme vynechávat. Po řadě vynásobením druhého a třetího řádku číslem 1/2, odečtením třetího řádku od druhého a od prvního a odečtením druhého řádku od prvního získáme

$$\left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & -2 & 3\\ 0 & 2 & 2 & 2 & -4 & 5\\ 0 & 0 & 0 & 2 & 0 & 3 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & -2 & 3\\ 0 & 1 & 1 & 1 & -2 & 5/2\\ 0 & 0 & 0 & 1 & 0 & 3/2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 0 & -2 & 3/2\\ 0 & 1 & 1 & 0 & -2 & 1\\ 0 & 0 & 0 & 1 & 0 & 3/2 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & 1/2\\ 0 & 1 & 1 & 0 & -2 & 1\\ 0 & 0 & 0 & 1 & 0 & 3/2 \end{array}\right).$$

Pokud opět zvolíme $x_3 = t$, $x_5 = s$ ($t, s \in \mathbb{R}$), dostaneme odsud obecné řešení (‖2.1‖) ve stejném tvaru, a to bezprostředně. Uvažte příslušné rovnice

$$\begin{aligned} x_1 &= 1/2, \\ x_2 + t - 2s &= 1, \\ x_4 &= 3/2. \end{aligned}$$

□

**2.77.** Najděte řešení soustavy lineárních rovnic zadané rozšířenou maticí

$$\left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 2 & 1 & 1 & 0 & 4 \\ 0 & 5 & -4 & 3 & 1 \\ 5 & 3 & 3 & -3 & 5 \end{array}\right).$$

**Řešení.** Uvedenou rozšířenou matici upravíme na schodovitý tvar. Nejprve první a třetí řádek opíšeme a do druhého řádku napíšeme součet $(-2)$násobku prvního a 3násobku druhého řádku a do čtvrtého řádku součet 5násobku prvního a $(-3)$násobku posledního řádku. Takto získáme

$$\left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 2 & 1 & 1 & 0 & 4 \\ 0 & 5 & -4 & 3 & 1 \\ 5 & 3 & 3 & -3 & 5 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 5 & -4 & 3 & 1 \\ 0 & 6 & 1 & 14 & 0 \end{array}\right).$$

Opsání prvních dvou řádků a přičtení 5násobku druhého řádku k 3násobku třetího a jeho 2násobku ke čtvrtému řádku dává

$$\left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 5 & -4 & 3 & 1 \\ 0 & 6 & 1 & 14 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 0 & -17 & -1 & 33 \\ 0 & 0 & -1 & 10 & 12 \end{array}\right).$$

Pokud první, druhý a čtvrtý řádek opíšeme a ke třetímu přičteme čtvrtý, dostaneme

$$\left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 0 & -17 & -1 & 33 \\ 0 & 0 & -1 & 10 & 12 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 0 & -18 & 9 & 45 \\ 0 & 0 & -1 & 10 & 12 \end{array}\right).$$

Dále je (řádkové úpravy jsou již „obvyklé“)

$$\left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 0 & -18 & 9 & 45 \\ 0 & 0 & -1 & 10 & 12 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 0 & 2 & -1 & -5 \\ 0 & 0 & 1 & -10 & -12 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 0 & 1 & -10 & -12 \\ 0 & 0 & 2 & -1 & -5 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 0 & 1 & -10 & -12 \\ 0 & 0 & 0 & 19 & 19 \end{array}\right).$$

Vidíme, že soustava má právě 1 řešení. Určeme ho zpětnou eliminací

$$\left(\begin{array}{cccc|c} 3 & 3 & 2 & 1 & 3 \\ 0 & -3 & -1 & -2 & 6 \\ 0 & 0 & 1 & -10 & -12 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 3 & 2 & 0 & 2 \\ 0 & -3 & -1 & 0 & 8 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 3 & 3 & 0 & 0 & 6 \\ 0 & -3 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right).$$

Výsledek je tak

$$x_1 = 4, \quad x_2 = -2, \quad x_3 = -2, \quad x_4 = 1. \qquad \square$$

**2.78.** Uveďte všechna řešení homogenního systému

$$x + y = 2z + v, \quad z + 4u + v = 0, \quad -3u = 0, \quad z = -v$$

4 lineárních rovnic 5 proměnných $x, y, z, u, v$.

**Řešení.** Systém přepíšeme do matice tak, že v prvním sloupci budou koeficienty u $x$, ve druhém sloupci koeficienty u $y$, až v pátém sloupci koeficienty u $v$, přičemž všechny členy v každé rovnici převedeme na levou stranu. Tímto způsobem přísluší systému matice

$$\begin{pmatrix} 1 & 1 & -2 & 0 & -1 \\ 0 & 0 & 1 & 4 & 1 \\ 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Přičteme-li (4/3)-násobek třetího řádku ke druhému a odečteme-li poté druhý řádek od čtvrtého, obdržíme

$$\begin{pmatrix} 1 & 1 & -2 & 0 & -1 \\ 0 & 0 & 1 & 4 & 1 \\ 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & -2 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Dále vynásobíme třetí řádek číslem $-1/3$ a přičteme 2násobek druhého řádku k prvnímu, což dává

$$\begin{pmatrix} 1 & 1 & -2 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Z poslední matice můžeme přímo vypsat všechna řešení

$$\begin{pmatrix} x \\ y \\ z \\ u \\ v \end{pmatrix} = t \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + s \begin{pmatrix} -1 \\ 0 \\ -1 \\ 0 \\ 1 \end{pmatrix}, \quad t, s \in \mathbb{R},$$

neboť máme matici ve schodovitém tvaru, přičemž první nenulové číslo v každém řádku je 1 a ve sloupci, kde se taková 1 nachází, jsou na ostatních pozicích 0. Výše uvedené řešení ve tvaru lineární kombinace dvou vektorů je určeno právě sloupci bez prvního nenulového čísla nějakého řádku, tj. druhým a pátým sloupcem, kdy volíme 1 jako druhou složku pro druhý sloupec a jako pátou složku pro pátý sloupec a kdy čísla v příslušném sloupci bereme s opačným znaménkem a umisťujeme je na pozici danou sloupcem, ve kterém je první 1 v jejich řádku. Dodejme, že výsledek je ihned možné přepsat do tvaru

$$(x,\ y,\ z,\ u,\ v) = (-t - s,\ t,\ -s,\ 0,\ s), \quad t, s \in \mathbb{R}. \qquad \square$$

**2.79.** Zjistěte počet řešení soustav

(a)

$$\begin{aligned} 12x_1 &+ \sqrt{5}x_2 + 11x_3 = -9, \\ x_1 &\quad - 5x_3 = -9, \\ x_1 &\quad + 2x_3 = -7; \end{aligned}$$

(b)

$$\begin{aligned} 4x_1 &+ 2x_2 - 12x_3 &= 0,\\ 5x_1 &+ 2x_2 - x_3 &= 0,\\ -2x_1 &- x_2 + 6x_3 &= 4; \end{aligned}$$

(c)

$$\begin{aligned} 4x_1 &+ 2x_2 - 12x_3 &= 0,\\ 5x_1 &+ 2x_2 - x_3 &= 1,\\ -2x_1 &- x_2 + 6x_3 &= 0. \end{aligned}$$

**Řešení.** Vektory $(1, 0, -5)$, $(1, 0, 2)$ jsou očividně lineárně nezávislé (jeden není násobkem druhého) a vektor $(12, \sqrt{5}, 11)$ nemůže být jejich lineární kombinací (jeho druhá složka je nenulová), a proto matice, jejímiž řádky jsou tyto tři lineárně nezávislé vektory, je invertibilní. Soustava ve variantě (a) má tedy právě jedno řešení.

U soustav ve variantách (b), (c) si stačí povšimnout, že je

$$(4, 2, -12) = -2(-2, -1, 6).$$

V případě (b) tak sečtení první rovnice s dvojnásobkem třetí dává $0 = 8$ – soustava nemá řešení; v případě (c) je třetí rovnice násobkem první – soustava má zřejmě nekonečně mnoho řešení. □

**2.80.** Najděte (libovolný) lineární systém, jehož množina řešení je právě

$$\{(t + 1,\ 2t,\ 3t,\ 4t);\ t \in \mathbb{R}\}.$$

**Řešení.** Takovým systémem je např.

$$2x_1 - x_2 = 2, \quad 2x_2 - x_4 = 0, \quad 4x_3 - 3x_4 = 0.$$

Těmto rovnicím totiž uvedené řešení vyhovuje pro každé $t \in \mathbb{R}$ a vektory

$$(2, -1, 0, 0), \quad (0, 2, 0, -1), \quad (0, 0, 4, -3)$$

zadávající levé strany rovnic jsou zřejmě lineárně nezávislé (množina řešení obsahuje jeden parametr). □

**2.81.** Stanovte hodnost matice

$$A = \begin{pmatrix} 1 & -3 & 0 & 1 \\ 1 & -2 & 2 & -4 \\ 1 & -1 & 0 & 1 \\ -2 & -1 & 1 & -2 \end{pmatrix}.$$

Poté stanovte počet řešení systému lineárních rovnic

$$\begin{aligned} x_1 &+ x_2 + x_3 - 2x_4 &= 4,\\ -3x_1 &- 2x_2 - x_3 - x_4 &= 5,\\ &+ 2x_2 \qquad + x_4 &= 1,\\ x_1 &- 4x_2 + x_3 - 2x_4 &= 3 \end{aligned}$$

a také všechna řešení systému

$$\begin{aligned} x_1 &+ x_2 + x_3 - 2x_4 &= 0,\\ -3x_1 &- 2x_2 - x_3 - x_4 &= 0,\\ &+ 2x_2 \qquad + x_4 &= 0,\\ x_1 &- 4x_2 + x_3 - 2x_4 &= 0 \end{aligned}$$

a systému

$$\begin{array}{rcrcrcr} x_1 & - & 3x_2 & & & = & 1, \\ x_1 & - & 2x_2 & + & 2x_3 & = & -4, \\ x_1 & - & x_2 & & & = & 1, \\ -2x_1 & - & x_2 & + & x_3 & = & -2. \end{array}$$

**Řešení.** Protože je $\det A = -10$, tedy nenulový, jsou sloupce matice $A$ lineárně nezávislé, a tudíž se její hodnost rovná jejímu rozměru.

První z uvedených třech systémů je zadán rozšířenou maticí

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & -2 & 4 \\ -3 & -2 & -1 & -1 & 5 \\ 0 & 2 & 0 & 1 & 1 \\ 1 & -4 & 1 & -2 & 3 \end{array}\right).$$

Ovšem levá strana je právě $A^T$ s determinantem $|A^T| = |A| \neq 0$. Existuje tedy matice $\left(A^T\right)^{-1}$ a soustava má právě 1 řešení

$$(x_1,\, x_2,\, x_3,\, x_4)^T = \left(A^T\right)^{-1} \cdot (4, 5, 1, 3)^T .$$

Druhý ze systémů má totožnou levou stranu (určenou maticí $A^T$) s prvním. Protože absolutní členy na pravé straně lineárních systémů neovlivňují počet řešení a protože každý homogenní systém má nulové řešení, dostáváme jako jediné řešení druhého systému uspořádanou čtveřici

$$(x_1,\, x_2,\, x_3,\, x_4) = (0, 0, 0, 0) .$$

Třetí systém má rozšířenou matici

$$\left(\begin{array}{ccc|c} 1 & -3 & 0 & 1 \\ 1 & -2 & 2 & -4 \\ 1 & -1 & 0 & 1 \\ -2 & -1 & 1 & -2 \end{array}\right),$$

což je matice $A$ (pouze poslední sloupec je uveden za svislou čarou). Pokud budeme tuto matici upravovat na schodovitý tvar, musíme obdržet řádek

$$\left(\begin{array}{ccc|c} 0 & 0 & 0 & a \end{array}\right), \text{ kde } a \neq 0.$$

Víme totiž, že sloupec na pravé straně není lineární kombinací sloupců na levé straně (hodnost matice je 4). Tento systém nemá řešení. □

*2.82.* Vyřešte systém homogenních lineárních rovnic zadaný maticí

$$\begin{pmatrix} 0 & \sqrt{2} & \sqrt{3} & \sqrt{6} & 0 \\ 2 & 2 & \sqrt{3} & -2 & -\sqrt{5} \\ 0 & 2 & \sqrt{5} & 2\sqrt{3} & -\sqrt{3} \\ 3 & 3 & \sqrt{3} & -3 & 0 \end{pmatrix}.$$

○

*2.83.* Určete všechna řešení systému

$$\begin{array}{rcrcrcrcr} & & x_2 & & & + & x_4 & = & 1, \\ 3x_1 & - & 2x_2 & - & 3x_3 & + & 4x_4 & = & -2, \\ x_1 & + & x_2 & - & x_3 & + & x_4 & = & 2, \\ x_1 & & & - & x_3 & & & = & 1. \end{array}$$

○

*2.84.* Vyřešte

$$\begin{array}{rcrcrcrcl} 3x & - & 5y & + & 2u & + & 4z & = & 2, \\ 5x & + & 7y & - & 4u & - & 6z & = & 3, \\ 11x & - & 3y & + & & + & 2z & = & 1. \end{array}$$

○

*2.85.* Rozhodněte o řešitelnosti soustavy lineárních rovnic

$$\begin{array}{rcrcrcl} 3x_1 & + & 3x_2 & + & x_3 & = & 1, \\ 2x_1 & + & 3x_2 & - & x_3 & = & 8, \\ 2x_1 & - & 3x_2 & + & x_3 & = & 4, \\ 3x_1 & - & 2x_2 & + & x_3 & = & 6 \end{array}$$

třech proměnných $x_1, x_2, x_3$. ○

*2.86.* Stanovte počet řešení 2 soustav 5 lineárních rovnic

$$A^T \cdot x = (1, 2, 3, 4, 5)^T, \quad A^T \cdot x = (1, 1, 1, 1, 1)^T,$$

kde

$$x = (x_1, x_2, x_3)^T \quad \text{a} \quad A = \begin{pmatrix} 3 & 1 & 7 & 5 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 2 & 1 & 4 & 3 & 0 \end{pmatrix}.$$

○

*2.87.* Určete řešení soustavy lineárních rovnic

$$\begin{array}{rcrcrcl} ax_1 & + & 4x_2 & + & 2x_3 & = & 0, \\ 2x_1 & + & 3x_2 & - & x_3 & = & 0 \end{array}$$

v závislosti na parametru $a \in \mathbb{R}$. ○

*2.88.* V závislosti na hodnotě parametru $a \in \mathbb{R}$ rozhodněte o počtu řešení soustavy

$$\begin{pmatrix} 4 & 1 & 4 & a \\ 2 & 3 & 6 & 8 \\ 3 & 2 & 5 & 4 \\ 6 & -1 & 2 & -8 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \\ 3 \\ -3 \end{pmatrix}.$$

○

*2.89.* Rozhodněte, zda existuje homogenní soustava lineárních rovnic tří proměnných, jejíž množinou řešení je

(a) $\{(0, 0, 0)\}$;

(b) $\{(0, 1, 0), (0, 0, 0), (1, 1, 0)\}$;

(c) $\{(x, 1, 0);\ x \in \mathbb{R}\}$;

(d) $\{(x, y, 2y);\ x, y \in \mathbb{R}\}$.

○

*2.90.* Řešte soustavu lineárních rovnic v závislosti na reálných parametrech $a, b$.

$$\begin{array}{rcrcrcl} x & + & 2y & + & bz & = & a, \\ x & - & y & + & 2z & = & 1, \\ 3x & - & y & & & = & 1. \end{array}$$

○

*2.91.* Najděte algebraicky adjungovanou matici $F^*$, je-li

$$F = \begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \alpha, \beta, \gamma, \delta \in \mathbb{R}.$$

○

*2.92.* Vypočítejte algebraicky adjungované matice k maticím

$$\text{(a)} \begin{pmatrix} 3 & -2 & 0 & -1 \\ 0 & 2 & 2 & 1 \\ 1 & -2 & -3 & -2 \\ 0 & 1 & 2 & 1 \end{pmatrix}, \qquad \text{(b)} \begin{pmatrix} 1+i & 2i \\ 3-2i & 6 \end{pmatrix},$$

přičemž $i$ označuje imaginární jednotku. ○

*2.93.* Rozložte na transpozice následující permutace:

i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$,

ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 2 & 5 & 8 & 3 & 7 \end{pmatrix}$,

iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 1 & 10 & 2 & 5 & 9 & 8 & 3 & 7 \end{pmatrix}$.

*2.94.* Určete paritu následujících permutací:

i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}$,

ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 1 & 2 & 3 & 8 & 4 & 5 \end{pmatrix}$,

iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 7 & 1 & 10 & 2 & 5 & 4 & 9 & 3 & 6 \end{pmatrix}$.

*2.95.* Je množina $V = \{(1, x);\ x \in \mathbb{R}\}$ s operacemi

$$\oplus : V \times V \to V,\ (1, y) \oplus (1, z) = (1, z + y),$$
$$\odot : \mathbb{R} \times V \to V,\ z \odot (1, y) = (1, y \cdot z),$$

kde $y, z \in \mathbb{R}$, vektorovým prostorem? ○

*2.96.* Vyjádřete vektor $(5, 1, 11)$ jako lineární kombinaci vektorů $(3, 2, 2)$, $(2, 3, 1)$, $(1, 1, 3)$, tj. nalezněte čísla $p, q, r \in \mathbb{R}$, pro která je

$$(5, 1, 11) = p\,(3, 2, 2) + q\,(2, 3, 1) + r\,(1, 1, 3)\ .$$ ○

*2.97.* V $\mathbb{R}^3$ určete matici rotace o 120° v kladném smyslu kolem vektoru $(1, 0, 1)$ (stačí uvést ve tvaru součinu matic). ○

*2.98.* Ve vektorovém prostoru $\mathbb{R}^3$ určete matici kolmé projekce na rovinu $x + y - 2z = 0$. ○

*2.99.* Ve vektorovém prostoru $\mathbb{R}^3$ určete matici kolmé projekce na rovinu $2x - y + 2z = 0$. ○

*2.100.* Je dána přímka

$$p : [1, 1] + (4, 1)t,\ t \in \mathbb{R}.$$

Určete parametrické vyjádření všech přímek $q$, které procházejí počátkem souřadnic a s přímkou $p$ mají odchylku 60°. ○

**2.101.** Napište nějakou bázi reálného vektorového prostoru matic $3 \times 3$ nad $\mathbb{R}$ s nulovou stopou (součet prvků na diagonále) a napište souřadnice matice

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ 1 & -2 & -3 \end{pmatrix}$$

v této bázi.

*2.102.* Zaveďte nějaký skalární součin na vektorovém prostoru matic z předchozího příkladu. Spočítejte normu matice z předchozího příkladu, která je indukovaná Vámi zavedeným součinem. ○

*2.103.* Určete, zda jsou podprostory

$$U = \langle (2, 1, 2, 2) \rangle ,$$
$$V = \langle (-1, 0, -1, 2) , \ (-1, 0, 1, 0) , \ (0, 0, 1, -1) \rangle$$

prostoru $\mathbb{R}^4$ na sebe kolmé. Pokud ano, je $\mathbb{R}^4 = U \oplus V$, tj. je $U^\perp = V$?

*2.104.* V závislosti na parametru $t \in \mathbb{R}$ stanovte dimenzi podprostoru $U$ vektorového prostoru $\mathbb{R}^3$, je-li $U$ generován vektory

(a) $u_1 = (1, 1, 1),\ u_2 = (1, t, 1),\ u_3 = (2, 2, t)$;
(b) $u_1 = (t, t, t),\ u_2 = (-4t, -4t, 4t),\ u_3 = (-2, -2, -2)$.

*2.105.* Sestrojte ortogonální bázi podprostoru

$$\langle\, (1, 1, 1, 1),\ (1, 1, 1, -1),\ (-1, 1, 1, 1) \,\rangle$$

prostoru $\mathbb{R}^4$.

*2.106.* V prostoru $\mathbb{R}^4$ nalezněte nějakou ortogonální bázi podprostoru všech lineárních kombinací vektorů $(1, 0, 1, 0)$, $(0, 1, 0, -7)$, $(4, -2, 4, 14)$ a podprostoru generovaného vektory $(1, 2, 2, -1)$, $(1, 1, -5, 3)$, $(3, 2, 8, -7)$.

*2.107.* Pro jaké hodnoty parametrů $a, b \in \mathbb{R}$ jsou vektory

$$(1, 1, 2, 0, 0),\ (1, -1, 0, 1, a),\ (1, b, 2, 3, -2)$$

v prostoru $\mathbb{R}^5$ po dvou ortogonální?

*2.108.* V prostoru $\mathbb{R}^5$ uvažujte podprostor generovaný vektory $(1, 1, -1, -1, 0)$, $(1, -1, -1, 0, -1)$, $(1, 1, 0, 1, 1)$, $(-1, 0, -1, 1, 1)$. Najděte nějakou bázi jeho ortogonálního doplňku.

*2.109.* Popište ortogonální doplněk podprostoru $V$ prostoru $\mathbb{R}^4$, je-li $V$ generován vektory $(-1, 2, 0, 1)$, $(3, 1, -2, 4)$, $(-4, 1, 2, -4)$, $(2, 3, -2, 5)$.

*2.110.* V prostoru $\mathbb{R}^5$ určete ortogonální doplněk $W^\perp$ podprostoru $W$, jestliže

(a) $W = \{(r + s + t, -r + t, r + s, -t, s + t) \mid r, s, t \in \mathbb{R}\}$;
(b) $W$ je množina řešení soustavy rovnic $x_1 - x_3 = 0$, $x_1 - x_2 + x_3 - x_4 + x_5 = 0$.

*2.111.* Nechť jsou v prostoru $\mathbb{R}^4$ dány vektory $(1, -2, 2, 1)$, $(1, 3, 2, 1)$. Doplňte tyto dva vektory libovolným způsobem na ortogonální bázi celého $\mathbb{R}^4$. (Můžete k tomu využít Gramův-Schmidtův ortogonalizační proces.) ○

**2.112.** Nalezněte vlastní čísla a jim příslušné vektorové prostory vlastních vektorů matice

$$A = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ 2 & -2 & 2 \end{pmatrix}.$$

**Řešení.** Charakteristický polynom matice je $\lambda^3 - 6\lambda^2 + 12\lambda - 8$, což je $(\lambda - 2)^3$ s trojnásobným kořenem 2. Číslo 2 je tedy vlastní hodnotou s algebraickou násobností tři. Její geometrická násobnost tedy bude jedna, dvě, nebo tři. Určeme tedy vlastní vektory příslušné této vlastní hodnotě jako řešení soustavy

$$(A - 2E)x = 0, \text{ tj. } \begin{array}{rcrcl} -x_1 & + & x_2 & = & 0, \\ -x_1 & + & x_2 & = & 0, \\ 2x_1 & - & 2x_2 & = & 0. \end{array}$$

Jejím řešením je dvojrozměrný prostor $\langle (1, -1, 0), (0, 0, 1) \rangle$. Vlastní hodnota 2 má tedy algebraickou násobnost tři, ale geometrickou pouze dva. □

*2.113.* Stanovte vlastní hodnoty matice

$$\begin{pmatrix} -13 & 5 & 4 & 2 \\ 0 & -1 & 0 & 0 \\ -30 & 12 & 9 & 5 \\ -12 & 6 & 4 & 1 \end{pmatrix}.$$

○

*2.114.* Víte-li, že čísla $1, -1$ jsou vlastní hodnoty matice

$$A = \begin{pmatrix} -11 & 5 & 4 & 1 \\ -3 & 0 & 1 & 0 \\ -21 & 11 & 8 & 2 \\ -9 & 5 & 3 & 1 \end{pmatrix},$$

uveďte všechna řešení charakteristické rovnice $|A - \lambda E| = 0$. Nápověda: Označíme-li kořeny polynomu $|A - \lambda E|$ jako $\lambda_1, \lambda_2, \lambda_3, \lambda_4$, je

$$|A| = \lambda_1 \cdot \lambda_2 \cdot \lambda_3 \cdot \lambda_4, \quad \operatorname{tr} A = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 . \qquad ○$$

*2.115.* Udejte příklad čtyřrozměrné matice s vlastními čísly $\lambda_1 = 6$ a $\lambda_2 = 7$ takové, aby násobnost $\lambda_2$ jako kořene charakteristického polynomu byla 3 a aby

(a) dimenze podprostoru vlastních vektorů $\lambda_2$ byla 3;

(b) dimenze podprostoru vlastních vektorů $\lambda_2$ byla 2;

(c) dimenze podprostoru vlastních vektorů $\lambda_2$ byla 1.

○

*2.116.* Nalezněte vlastní čísla a vlastní vektory matice:

$$\begin{pmatrix} -1 & -\frac{5}{6} & \frac{5}{3} \\ 0 & -\frac{2}{3} & -\frac{2}{3} \\ 0 & \frac{1}{6} & -\frac{4}{3} \end{pmatrix}.$$

○

*2.117.* Určete charakteristický polynom $|A - \lambda E|$, vlastní čísla a vlastní vektory matice

$$\begin{pmatrix} 4 & -1 & 6 \\ 2 & 1 & 6 \\ 2 & -1 & 8 \end{pmatrix}.$$

○

*2.118.* Určete geometrický význam zobrazení v $\mathbb{R}^3$, které je zadáno maticí

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

○

*2.119.* Rozhodněte, zda $\|A^{1000}v\| < 1$, kde $v = (3, 2, 1)$, kde $A = \begin{pmatrix} -1 & 3 & -\frac{3}{2} \\ -\frac{3}{2} & 7/2 & -\frac{3}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix}$. ○

## Řešení cvičení

*2.7.*

$$A^5 = \begin{pmatrix} 122 & -121 & 121 \\ -121 & 122 & -121 \\ 0 & 0 & 1 \end{pmatrix}, \; A^{-3} = \frac{1}{27}\begin{pmatrix} 14 & 13 & -13 \\ 13 & 14 & 13 \\ 0 & 0 & 27 \end{pmatrix}.$$

*2.12.* Taková matice $X$ existuje právě jedna, a to

$$\begin{pmatrix} 18 & -32 \\ 5 & -8 \end{pmatrix}.$$

*2.14.* $A^{-1} = \begin{pmatrix} 1 & 10 & -4 \\ 1 & 12 & -5 \\ 0 & 5 & -2 \end{pmatrix}$.

*2.15.* $\begin{pmatrix} 2 & -3 & 0 & 0 & 0 \\ -5 & 8 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -5 & 2 \\ 0 & 0 & 0 & 3 & -1 \end{pmatrix}$.

*2.16.* $C^{-1} = \frac{1}{2}\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 1 \end{pmatrix}$.

*2.17.* V prvním případě dostáváme

$$A^{-1} = \frac{1}{2} \cdot \begin{pmatrix} 3 & -i \\ i & 1 \end{pmatrix};$$

ve druhém potom

$$A^{-1} = \begin{pmatrix} 14 & 8 & 5 \\ 2 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

*2.18.* Platí

$$A^{-1} = \frac{1}{n-1}\begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{pmatrix}.$$

*2.21.* -3,17,-1

*2.27.*

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}^{-1} \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Následně lze snadno získat

$$x_1 = \frac{13}{4}, \quad x_2 = -\frac{3}{4}, \quad x_3 = -\frac{3}{4}, \quad x_4 = \frac{1}{4}.$$

*2.39.* $(2 + \frac{1}{\sqrt{3}}, 2 - \frac{1}{\sqrt{3}})$.

*2.40*. Vektory jsou závislé, je-li splněna alespoň jedna z podmínek

$$a = b = 1, \qquad a = c = 1, \qquad b = c = 1.$$

*2.41*. Vektory jsou lineárně nezávislé.

*2.42*. Stačí připojit např. polynom $x$.

*2.61*. $\cos = \frac{\sqrt{2}}{\sqrt{3}}$.

*2.68*. Je $|A - \lambda E| = -\lambda^3 + 12\lambda^2 - 47\lambda + 60$, tj. $\lambda_1 = 3$, $\lambda_2 = 4$, $\lambda_3 = 5$.

*2.70*. Dimenze je 1 pro $\lambda_1 = 4$ a 2 pro $\lambda_2 = 3$.

*2.71*. Matice $B$ má dvě různá vlastní čísla, a proto takové vyjádření existuje. Např. platí

$$\begin{pmatrix} 5 & 6 \\ 6 & 5 \end{pmatrix} = \tfrac{1}{2} \begin{pmatrix} \sqrt{2} & -\sqrt{2} \\ \sqrt{2} & \sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} 11 & 0 \\ 0 & -1 \end{pmatrix} \cdot \tfrac{1}{2} \begin{pmatrix} \sqrt{2} & \sqrt{2} \\ -\sqrt{2} & \sqrt{2} \end{pmatrix}.$$

Existují právě dvě diagonální matice $D$, a to

$$\begin{pmatrix} 11 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} -1 & 0 \\ 0 & 11 \end{pmatrix},$$

ovšem sloupce matice $P^{-1}$ můžeme nahradit za jejich libovolné nenulové skalární násobky, tedy uvažovaných dvojic $D$, $P$ je nekonečně mnoho.

*2.75*. Výsledkem je posloupnost 0, 1, 2.

*2.82*. Řešeními jsou právě všechny skalární násobky vektoru

$$\left(1 + \sqrt{3},\ -\sqrt{3},\ 0,\ 1,\ 0\right).$$

*2.83*. $x_1 = 1 + t, \quad x_2 = \frac{3}{2}, \quad x_3 = t, \quad x_4 = -\frac{1}{2}, \qquad t \in \mathbb{R}$.

*2.84*. Soustava nemá řešení.

*2.85*. Soustava má řešení, protože je

$$3 \cdot \begin{pmatrix} 3 \\ 2 \\ 2 \\ 3 \end{pmatrix} - \begin{pmatrix} 3 \\ 3 \\ -3 \\ -2 \end{pmatrix} - 5 \cdot \begin{pmatrix} 1 \\ -1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 8 \\ 4 \\ 6 \end{pmatrix}.$$

*2.86*. Systém lineárních rovnic

$$\begin{aligned} 3x_1 \quad &+ \quad 2x_3 &&= 1, \\ x_1 \quad &+ \quad x_3 &&= 2, \\ 7x_1 \quad &+ \quad 4x_3 &&= 3, \\ 5x_1 \quad &+ \quad 3x_3 &&= 4, \\ x_2 \quad & &&= 5 \end{aligned}$$

nemá řešení, zatímco systém

$$\begin{aligned} 3x_1 \quad &+ \quad 2x_3 &&= 1, \\ x_1 \quad &+ \quad x_3 &&= 1, \\ 7x_1 \quad &+ \quad 4x_3 &&= 1, \\ 5x_1 \quad &+ \quad 3x_3 &&= 1, \\ x_2 \quad & &&= 1 \end{aligned}$$

má právě jedno řešení $x_1 = -1$, $x_2 = 1$, $x_3 = 2$.

*2.87*. Množina všech řešení je

$$\{(-10t,\ (a+4)t,\ (3a-8)t)\ ;\ t \in \mathbb{R}\}.$$

*2.88*. Pro $a = 0$ nemá uvažovaný systém řešení; pro $a \neq 0$ má nekonečně mnoho řešení.

*2.89.* Při zachování pořadí jsou správné odpovědi „ano“, „ne“, „ne“ a „ano“.

*2.90.* i) Pro $b \neq -7$ je $x = z = (2+a)/(b+7)$, $y = (3a-b-1)/(b+7)$ (1b). ii) Pro $b = -7$ (1b) a $a \neq -2$ (1b) nemá řešení (1b), pro $a = -2$ je řešením $x = z$, $3z - 1$ (2b).

*2.91.* Ze znalosti inverzní matice $F^{-1}$ dostáváme

$$F^* = (\alpha\delta - \beta\gamma)\ F^{-1} = \begin{pmatrix} \delta & -\beta & 0 \\ -\gamma & \alpha & 0 \\ 0 & 0 & \alpha\delta - \beta\gamma \end{pmatrix},$$

pro libovolná $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

*2.92.* Hledanými maticemi jsou

$$\text{(a)} \begin{pmatrix} 1 & 1 & -2 & -4 \\ 0 & 1 & 0 & -1 \\ -1 & -1 & 3 & 6 \\ 2 & 1 & -6 & -10 \end{pmatrix}, \qquad \text{(b)} \begin{pmatrix} 6 & -2i \\ -3+2i & 1+i \end{pmatrix}.$$

*2.93.* i) $(1,7)(2,6)(5,3)$, ii) $(1,6)(6,8)(8,7)(7,3)(2,4)$, iii) $(1,4)(4,10)(10,7)(7,9)(9,3)(2,6)(6,5)$

*2.94.* i) 17 inverzí, lichá, ii) 12 inverzí, sudá, iii) 25 inverzí, lichá

*2.95.* Lehce se ověří, že se jedná o vektorový prostor. První souřadnice neovlivňuje výpočty součtů vektorů ani hodnoty skalárních násobků vektorů: jedná se o přeznačený prostor $(\mathbb{R}, +, \cdot)$.

*2.96.* Úloha má jediné řešení

$$p = 2, \qquad q = -2, \qquad r = 3.$$

*2.97.*

$$\begin{pmatrix} 1/4 & -\sqrt{6}/4 & 3/4 \\ \sqrt{6}/4 & -1/2 & -\sqrt{6}/4 \\ 3/4 & \sqrt{6}/4 & 1/4 \end{pmatrix}$$

*2.98.*

$$\begin{pmatrix} 5/6 & -1/6 & 1/3 \\ -1/6 & 5/6 & 1/3 \\ 1/3 & 1/3 & 1/3 \end{pmatrix}.$$

*2.99.*

$$\begin{pmatrix} 5/9 & 2/9 & -4/9 \\ 2/9 & 8/9 & 2/9 \\ -4/9 & 2/9 & 5/9 \end{pmatrix}$$

*2.100.*

$$q_1 : \left(2 - \frac{\sqrt{3}}{2}, 2\sqrt{3} + \frac{1}{2}\right) t, \quad q_2 : \left(2 + \frac{\sqrt{3}}{2}, -2\sqrt{3} + \frac{1}{2}\right) t.$$

*2.102.* Například skalární součin, který vyplývá z izomorfismu prostoru všech reálných matic $3 \times 3$ s $\mathbb{R}^9$. Použijeme-li součin z $\mathbb{R}^9$ dostáváme skalární součin, který dvěma maticím přiřadí součet součinů po dvou odpovídajících si složek. Pro danou matici dostaneme

$$\left\| \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ 1 & -2 & -3 \end{pmatrix} \right\| = \left\langle \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ 1 & -2 & -3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ 1 & -2 & -3 \end{pmatrix} \right\rangle =$$

$$= \sqrt{1^2 + 2^2 + 0^2 + 0^2 + 2^2 + 0^2 + 1^2 + (-2)^2 + (-3)^2} = \sqrt{23}.$$

*2.103.* Vektor, který zadává podprostor $U$, je kolmý na každý ze tří vektorů, které generují $V$. Podprostory jsou tak na sebe kolmé. Avšak není pravda, že $\mathbb{R}^4 = U \oplus V$. Podprostor $V$ je totiž pouze dvojdimenzionální, protože

$$(-1, 0, -1, 2) = (-1, 0, 1, 0) - 2\,(0, 0, 1, -1)\,.$$

*2.104.* V prvním případě je $\dim U = 2$ pro $t \in \{1, 2\}$, jinak je $\dim U = 3$. Ve druhém případu je $\dim U = 2$ pro $t \neq 0$ a $\dim U = 1$ pro $t = 0$.

*2.105.* Gramovým-Schmidtovým ortogonalizačním procesem lze obdržet výsledek

$$((1, 1, 1, 1),\ (1, 1, 1, -3),\ (-2, 1, 1, 0))\,.$$

*2.106.* Při zachování pořadí podprostorů ze zadání jsou ortogonálními bázemi např.

$((1, 0, 1, 0), (0, 1, 0, -7))$ a $((1, 2, 2, -1), (2, 3, -3, 2), (2, -1, -1, -2))$.

*2.107.* Výsledek je $a = 9/2$, $b = -5$, neboť musí mj. platit

$$1 + b + 4 + 0 + 0 = 0, \quad 1 - b + 0 + 3 - 2a = 0.$$

*2.108.* Hledaná báze obsahuje jediný vektor. Je jím nějaký nenulový skalární násobek vektoru

$$(3, -7, 1, -5, 9).$$

*2.109.* Ortogonální doplněk (komplement) $V^\perp$ je množina všech skalárních násobků vektoru $(4, 2, 7, 0)$.

*2.110.* (a) $W^\perp = \langle\,(1, 0, -1, 1, 0),\ (1, 3, 2, 1, -3)\,\rangle$;

(b) $W^\perp = \langle\,(1, 0, -1, 0, 0),\ (1, -1, 1, -1, 1)\,\rangle$.

*2.111.* Hledaných doplnění je pochopitelně nekonečně mnoho. Jedním (skutečně jednoduchým) je např.

$$(1, -2, 2, 1), \quad (1, 3, 2, 1), \quad (1, 0, 0, -1), \quad (1, 0, -1, 1).$$

*2.113.* Daná matice má pouze jedno vlastní číslo, a to $-1$.

*2.114.* Kořen $-1$ polynomu $|\,A - \lambda\,E\,|$ je trojnásobný.

*2.115.* Kupř.

$$\text{(a)}\ \begin{pmatrix} 6 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 \end{pmatrix}; \quad \text{(b)}\ \begin{pmatrix} 6 & 0 & 0 & 0 \\ 0 & 7 & 1 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 \end{pmatrix}; \quad \text{(c)}\ \begin{pmatrix} 6 & 0 & 0 & 0 \\ 0 & 7 & 1 & 0 \\ 0 & 0 & 7 & 1 \\ 0 & 0 & 0 & 7 \end{pmatrix}.$$

*2.116.* Trojnásobná vlastní hodnota $-1$, příslušný vektorový prostor je $\langle(1, 0, 0), (0, 2, 1)\rangle$.

*2.117.* Charakteristický polynom je $-(\lambda-2)^2(\lambda-9)$, tj. vlastní čísla jsou 2 a 9 s příslu nými (po řadě) vlastními vektory

$$(1, 2, 0)\,, (-3, 0, 1) \quad \text{a} \quad (1, 1, 1)\,.$$

*2.118.* Zrcadlení podle roviny $\langle(1, 0, 1), (0, 1, 0)\rangle$.

*2.119.* Daný vektor je vlastním vektorem dané matice s vlastní hodnotou $1/2$. Je tedy

$$\|A^{1000}v\| = \|\left(\frac{1}{2}\right)^{1000} v\| = \left(\frac{1}{2}\right)^{1000} \|v\| < 1.$$

KAPITOLA 3

# Lineární modely a maticový počet

*kde jsou matice užitečné?*
*– nakonec skoro všude...*



Otázkou počtu řešení soustavy lineárních rovnic jsme se již zabývali v příkladech na straně 83 a několika následujících.

## A. Procesy s lineárními omezeními

Ukažme si příklad velmi jednoduché lineární optimalizační úlohy, se kterými se lze setkat v praxi:

**3.1.** Firma vyrábí šroubky a matičky. Šroubky i matičky jsou lisovány – vylisování krabičky šroubků trvá 1 minutu, krabička matiček je lisována 2 minuty. Šroubky i matičky balí do krabiček, ve kterých je pak prodává – krabička šroubků se balí 1 minutu, krabička matic 4 minuty. Firma má k dispozici 2 hodiny času pro lisování a 3 hodiny času pro balení výrobků. Vzhledem k poptávce je třeba vyrobit alespoň o 90 krabiček šroubků více než krabiček matic. Z technických důvodů nelze vyrobit více než 110 krabiček šroubků. Zisk z jedné krabičky šroubků je 40 Kč a z jedné krabičky matic 60 Kč. Firma nemá potíže s odbytem výrobků. Kolik krabiček šroubků a matic má firma vyrobit, chce-li dosáhnout maximálního zisku?

**Řešení.** Zapišme si zadané údaje do tabulky:

Máme už vybudován docela slušný balíček nástrojů a tak je na čase, abychom si maticový počet zkusili použít. Na docela jednoduchých úlohách uvidíme, že teorie nám umožňuje kvalitativní i kvantitativní analýzy a někdy i překvapivě snadno vede k nečekaným výsledkům.

Jakkoliv se může zdát, že předpoklad linearity vztahů mezi veličinami je příliš omezující, v reálných úlohách naopak často právě lineární závislosti buď vystupují přímo nebo je skutečný proces výsledkem iterace mnoha lineárních kroků. I když tomu tak není, můžeme tímto způsobem skutečné procesy alespoň aproximovat.



V této kapitole proto nejprve zrekapitulujeme nejjednodušší případ, kdy celý proces je popsán jediným lineárním zobrazením. O co méně tady bude nové teorie, tím více snad bude zajímavé, jak takové modely vznikají v různých oblastech využití matematických nástrojů. Poté se vrátíme k tzv. lineárním diferenčním rovnicím, které lze chápat buď jako rekurentně definované funkce nebo také jako specifický případ lineárního iterovaného procesu. Právě takovým procesům bude věnována část třetí, kde si ukážeme, k jakým kouzlům vede pochopení vlastností vlastních hodnot matic.



Na matice (resp. lineární zobrazení) se také někdy rádi díváme jako na objekty, se kterými bychom rádi pracovali tak, jak to umíme se skaláry. K tomu ale bude třeba docela usilovná práce ve čtvrté části kapitoly. Rychlé a užitečné použití pak ukážeme na tzv. rozkladech matic, které jsou potřebné pro numerické zvládnutí maticového počtu co nejrobustnějším způsobem.

### 1. Lineární procesy

**3.1. Řešení systému lineárních rovnic.** Jednoduché lineární procesy jsou dány lineárními zobrazeními $\varphi : V \to W$ na vektorových prostorech. Jak si jistě umíme představit, vektor $v \in V$ může představovat stav nějakého námi sledovaného systému, zatímco $\varphi(v)$ pak dá výsledek po uskutečněném procesu.



Pokud chceme dosáhnout předem daného výsledku $b \in W$ takového jednorázového procesu, řešíme problém

$$\varphi(x) = b$$

pro neznámý vektor $x$ a známý vektor $b$.

V pevně zvolených souřadnicích pak máme matici $A$ zobrazení $\varphi$ a souřadné vyjádření vektoru $b$. Jak jsme si povšimli už v úvodu druhé kapitoly, množina všech řešení tzv. *homogenní úlohy*

$$A \cdot x = 0$$

| | Šroubky 1 krabička | Matičky 1 krabička | Kapacita |
|---|---|---|---|
| Lis | 1 min/kr | 2 min/kr | 2 hodiny |
| Balení | 1 min/kr | 4 min/kr | 3 hodiny |
| Zisk | 40 Kč/kr | 60 Kč/kr | |

Označme $x_1$ počet vyrobených krabiček šroubků, $x_2$ počet vyrobených krabiček matic. Z doby, po kterou má firma k dispozici lis, resp. kterou má na balení, dostáváme omezující podmínky:

$$x_1 + 2x_2 \leq 120,$$
$$x_1 + 4x_2 \leq 180,$$
$$x_1 \geq x_2 + 90,$$
$$x_1 \leq 110.$$

Účelová funkce (funkce udávající zisk při daném počtu vyrobených šroubků a matic) je $40x_1 + 60x_2$. Předchozí soustava nerovnic zadává v $\mathbb{R}^2$ určitou oblast a optimalizace zisku znamená najít v této oblasti bod (případně body), ve kterém bude mít účelová funkce nejvyšší hodnotu, tj. najít největší $k$ takové, že přímka $40x_1 + 60x_2 = k$ bude mít s danou oblastí neprázdný průnik. Graficky můžeme najít řešení například tak, že umístíme přímku $p$ do roviny tak, aby splňovala rovnici $40x_1 + 60x_2 = 0$ a začneme ji rovnoběžně posunovat „nahoru“ tak dlouho, dokud bude mít nějaký společný průnik s danou oblastí. Je zřejmé, že tímto posledním průnikem může být buď bod, nebo hraniční přímka dané oblasti (pokud by byla rovnoběžná s $p$). Dostaneme tak (viz obrázek), bod $x_1 = 110$ a $x_2 = 5$. Maximální možný zisk tedy činí $40 \cdot 110 + 60 \cdot 5 = 4700$ Kč. □

*3.2.* **Minimalizace nákladů na krmení.** Hříbárna v Nišovicích u Volyně nakupuje na zimu krmivo: seno a oves. Výživné hodnoty krmiv a požadované denní dávky pro jedno hříbě jsou v tabulce

| g/kg | Seno | Oves | POŽADAVKY |
|---|---|---|---|
| Sušina | 841 | 860 | Alespoň 6300 g |
| SNL | 53 | 123 | Nejvýše 1150 g |
| Škrob | 0,348 | 0,868 | Nejvýše 5,35 g |
| Vápník | 6 | 1,6 | Alespoň 30 g |
| Fosfor | 2,8 | 3,5 | Nejvýše 44 g |
| Sodík | 0,2 | 1,4 | Přibližně 7 g |
| CENA | 1,80 | 1,60 | |

Každé hříbě musí v krmné dávce denně dostat alespoň 2 kg ovsa. Průměrná cena včetně dopravy činí 1,80 Kč za 1 kg sena a 1,60 Kč za 1 kg ovsa. Sestavte denní dávku krmení pro jedno hříbě tak, aby náklady byly minimální. ○

Předchozí dva příklady šlo řešit pouze graficky, vyznačením oblasti v rovině $\mathbb{R}^2$, která je určena danými omezeními, a potom snadno je vektorovým podprostorem.

Pokud je dimenze $V$ konečná, řekněme $n$, a dimenze obrazu zobrazení $\varphi$ je $k$, pak řešením této soustavy pomocí převodu na řádkově schodovitý tvar (viz 2.7) zjistíme, že dimenze podprostoru všech řešení je právě $n - k$. Skutečně, protože sloupce matice zobrazení jsou právě obrazy bázových vektorů, je v matici systému právě $k$ lineárně nezávislých sloupců a tedy i stejný počet lineárně nezávislých řádků. Proto nám zůstane při převodu na řádkový schodovitý tvar právě $n - k$ nulových řádků. Při řešení systému rovnic nám tak zůstane právě $n - k$ volných parametrů. Dosazením vždy jednoho z nich s hodnotou jedna a vynulováním ostatních získáme právě $n - k$ lineárně nezávislých řešení. Všechna řešení jsou pak dána právě všemi lineárními kombinacemi těchto $n - k$ řešení. Každé takové $(n - k)$–tici řešení říkáme *fundamentální systém řešení* daného homogenního systému rovnic. Dokázali jsme:

**Věta.** *Množina všech řešení homogenního systému rovnic*

$$A \cdot x = 0$$

*pro $n$ proměnných s maticí $A$ hodnosti $k$ je vektorovým podprostorem v $\mathbb{K}^n$ dimenze $n - k$. Každá báze tohoto podprostoru tvoří fundamentální systém řešení daného homogenního systému.*

**3.2. Nehomogenní systémy rovnic.** Uvažme nyní obecný systém rovnic

$$A \cdot x = b.$$

Znovu si uvědomme, že sloupce matice $A$ jsou ve skutečnosti obrazy vektorů standardní báze v $\mathbb{K}^n$ v lineárním zobrazení $\varphi$ odpovídajícím matici $A$. Pokud má existovat řešení, musí být $b$ v obrazu $\varphi$ a tedy musí být lineární kombinací sloupců v $A$.

Jestliže tedy rozšíříme matici $A$ o sloupec $b$, můžeme, ale nemusíme, také zvětšit počet lineárně nezávislých sloupců a tedy i řádků. Pokud se tento počet zvětší, pak $b$ v obrazu není a tedy systém rovnic nemůže mít řešení. Jestliže ale naopak máme stejný počet nezávislých řádků i po přidání sloupce $b$ k matici $A$, znamená to, že sloupec $b$ musí být lineární kombinací sloupců matice $A$. Koeficienty takové kombinace jsou právě řešení našeho systému rovnic.

Uvažme nyní dvě pevně zvolená řešení $x$ a $y$ našeho systému a nějaké řešení $z$ systému homogenního se stejnou maticí. Pak zjevně

$$A \cdot (x - y) = b - b = 0$$
$$A \cdot (x + z) = 0 + b = b.$$

Můžeme proto shrnout:

**3.3. Věta.** *Řešení nehomogenního systému lineárních rovnic $A \cdot x = b$ existuje právě tehdy, když přidáním sloupce $b$ k matici $A$ nezvýšíme počet lineárně nezávislých řádků. V takovém případě je prostor všech řešení dán všemi součty jednoho pevně zvoleného partikulárního řešení systému a všech řešení systému homogenního se stejnou maticí.*

V literatuře se tomuto tvrzení často říká *Frobeniova věta* a obvyklá formulace je „systém má řešení, právě když je hodnost jeho matice rovna hodnosti matice rozšířené“.

nalezneme na její hranici bod, ve kterém nabývá zadaná funkce maxima (je to „nejvzdálenější“ bod dané oblasti ve směru největšího růstu dané funkce, tedy normály k nadrovině zadané koeficienty optimalizované funkce).

Jde vlastně o obecnější pozorování. Pokud máme zadánu nějakou lineární funkci $\mathbb{R}^n \to \mathbb{R}^n$, $f(x_1, \dots, x_n) = c_0 + c_1x_1 + \cdots + c_nx_n$ (říkejme jí dále účelová funkce), tak se její hodnota v bodech $A = [a_1, \dots, a_n]$ a $B = A+u = [a_1+u_1, \dots, a_n+u_n]$ liší díky linearitě o hodnotu $f(A-B) = f(u) = f(u_1, \dots, u_n) = c_1u_1+\cdots+c_nu_n$, což je skalární součin vektorů $(c_1, ..., c_n)$ a $(u_1, ..., u_n)$. Ze vztahu skalárního součinu a kosinu odchylky dvou vektorů vidíme, že zadaná lineární funkce definuje ve vektorovém prostoru $\mathbb{R}^n$ nadrovinu (s normálou $(c_1, \dots, c_1)$ rozdělující prostor $\mathbb{R}^n$ na dva poloprostory takové, že zkoumaná funkce ve směru libovolného vektoru z jednoho poloprostoru roste, ve směru libovolného vektoru z druhého poloprostoru klesá. Jde vlastně o stejný princip, se kterým jsme se setkali u rozhodování o viditelnosti dané úsečky v rovině (určili jsme, jestli pozorovací bod leží na napravo, či nalevo od ní, viz 1.35).

Toto pozorování pak vede k algoritmickému postupu hledání extrému účelové funkce na množině omezené lineárními nerovnostmi.

Algoritmus pracuje pro úlohu v tzv. standardním tvaru maximalizovat funkci $c_1x_1 + \cdots + c_nx_n$ na množině $Ax = b$. Do tohoto tvaru lze libovolnou úlohu o hledání extrému účelové funkce na množině $Ax \leq b$ snadno převést (násobením nerovnosti číslem (-1) můžeme měnit znaménko nerovnosti, pronásobením číslem (-1) účelové funkce rovněž můžeme změnit minimalizační problém na maximalizační, přidáním nové nezáporné proměnné k jedné nerovnici pak můžeme změnit nerovnici na rovnici).

Zápis algoritmu pomocí tabulky: mějme úlohu maximalizovat $c_1x_1+\cdots+c_nx_n$ na množině v $\mathbb{R}^n$ dané rovnicemi $Ax = b$, a nerovnicemi $x_j \geq 0$, kde $A = (a_{ij}), 1 \leq j \leq n, 1 \leq i \leq m, b = (b_1, \dots, b_m)$. Zadání přepíšeme do tabulky takto:

| | | | |
|---|---|---|---|
| $-c_1$ | $\dots$ | $-c_n$ | 0 |
| $a_{11}$ | $\dots$ | $a_{1n}$ | $b_1$ |
| $\vdots$ | | $\vdots$ | $\vdots$ |
| $a_{m1}$ | $\dots$ | $a_{mn}$ | $b_m$ |

Pokud se nám podaří v matici $A$ nalézt $m$ sloupců takových, že postupnou eliminací vůči vhodně vybraným prvkům v těchto sloupcích (v každém jeden), dosáhneme toho, že vybrané sloupce budou tvořit (ve vhodném pořadí) jednotkovou matici a pravý sloupec bude po eliminaci splňovat podmínky úlohy (např. nezápornost), můžeme zahájit

**3.4. Optimalizační lineární modely.** Ve vedlejším sloupci jsme druhou kapitolu začali problémy natěračů (‖2.1‖). Budeme v tom pokračovat. Představme si, že náš velice specializovaný natěrač v černobílém světě je ochoten natírat fasády buď malých rodinných domků nebo naopak velikých veřejných budov a že pochopitelně používá jen černou a bílou barvu. Může si zcela volně vybírat, v jakém rozsahu bude dělat $x$ jednotek plochy prvého typu nebo $y$ jednotek druhého. Předpokládejme však, že jeho maximální pracovní zátěž je ve sledovaném období $L$ jednotek plochy, jeho čistý výnos (tj. po odečtení nákladů) je na jednotku plochy $c_1$ u malých domků a $c_2$ u veřejných staveb. Zároveň má k dispozici maximálně $W$ kg bílé a $B$ kg černé barvy. Konečně na jednotku plochy rodinného domu potřebuje $w_1$ kg bílé barvy a $b_1$ kg černé, zatímco u veřejných staveb jsou to hodnoty $w_2$ a $b_2$.



Když si to celé shrneme do (ne)rovnic, dostáváme omezení

$$x_1 + x_2 \leq L, \tag{3.1}$$

$$w_1x_1 + w_2x_2 \leq W, \tag{3.2}$$

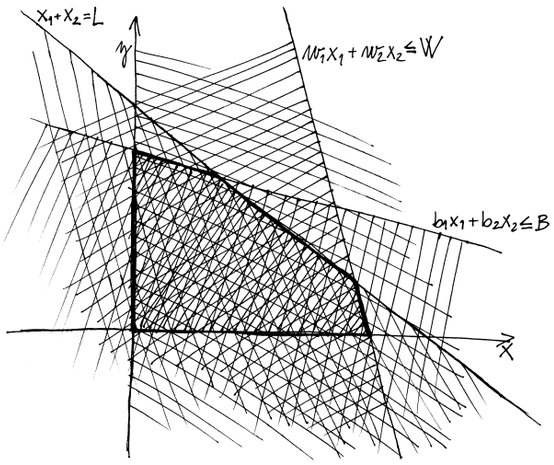
$$b_1x_1 + b_2x_2 \leq B. \tag{3.3}$$

Celkový čistý výnos natěrače

$$h(x_1, x_2) = c_1x_1 + c_2x_2$$

bychom přitom rádi měli co největší.

Každá z uvedených nerovnic samozřejmě zadává v rovině proměnných $(x_1, x_2)$ polorovinu, ohraničenou přímkou zadanou příslušnou rovnicí, a jistě musíme také předpokládat, že jak $x_1$ tak $x_2$ jsou nezáporná reálná čísla, protože záporné velikosti ploch natěrač neumí. Ve skutečnosti máme tedy omezení na hodnoty $(x_1, x_2)$, které může být buď nesplnitelné nebo je dáno jako vnitřek mnohoúhelníku s maximálně pěti vrcholy:




Obecně hovoříme o *problému lineárního programování*, jestliže hledáme buď maximum nebo minimum lineární formy $h$ na $\mathbb{R}^n$ na množině ohraničené pomocí systému lineárních nerovnic, kterým říkáme *lineární omezení*. Vektoru na pravé straně pak říkáme *vektor omezení*, lineární formě $h$ také *účelová funkce*.

Formulace s nerovnostmi $\leq$ u omezujících podmínek, nezápornými proměnnými a maximalizaci účelové funkce říkáme *standardní maximalizační problém*. Naopak, *standardní minimalizační problém* je hledání minima účelové funkce při omezujících podmínkách s nerovnostmi $\geq$, přičemž opět uvažujeme nezáporné proměnné.

výpočet (uvidíme, že při zadání úlohy ve tvaru $Ax \leq b$, kde $b$ je nezáporné, je možné matici $A$ jednoduše rozšířit tak, že toho lze snadno docílit).

Dále postupujeme v následujících krocích: Vybereme první sloupec zleva, který má na prvním řádku nekladný prvek. V tomto sloupci vybereme z kladných čísel to číslo $x$, pro které je poměr čísla ve stejném řádku a nejpravějším sloupci ku $x$ minimální. Eliminujeme celý sloupec této tabulku podle čísla $x$, říkejme mu pivot (tzn. elementárními řádkovými transformacemi dané tabulky dosáhneme toho, že ve vybraném sloupci bude číslo 1 na místě $x$, jinak samé nuly).

Ukažme si postup na konkrétním příkladu:

**3.3.** Minimalizujte funkci $-3x - y - 2z$ za podmínek $x, y, z \geq 0$ a

$$\begin{aligned} x &- y + z \geq -4, \\ 2x &\quad + z \leq 3, \\ x &+ y + 3z \leq 8. \end{aligned}$$

**Řešení.** Vynásobením účelové funkce a první nerovnice číslem $-1$ dostáváme ekvivalentní úlohu maximalizovat funkci $3x + y + 2z$ za podmínek

$$\begin{aligned} -x &+ y - z \leq 4, \\ 2x &\quad + z \leq 3, \\ x &+ y + 3z \leq 8. \end{aligned}$$

Zavedením nezáporných proměnných $u$, $v$, $w$ dostáváme již tabulku (účelová funkce je $3x + y + 2z + 0 \cdot u + 0 \cdot v + 0 \cdot w$):

| | | | | | | |
|---|---|---|---|---|---|---|
| $-3$ | $-1$ | $-2$ | 0 | 0 | 0 | 0 |
| $-1$ | 1 | $-1$ | 1 | 0 | 0 | 4 |
| (2) | 0 | 1 | 0 | 1 | 0 | 3 |
| 1 | 1 | 3 | 0 | 0 | 1 | 8 |

.

Nyní vybereme první sloupec tabulky, ve kterém je v prvním řádku záporné číslo (tedy celkově první sloupec tabulky) a v něm vybereme řádek s dvojkou (u řádků s kladnou hodnotou porovnáváme velikosti čísel $\frac{3}{2}$ a $\frac{8}{1}$, vybereme řádek odpovídající menší hodnotě). V dalším eliminujeme první sloupec podle prvku 2 (vynásobíme třetí řádek číslem $\frac{1}{2}$, a odečteme jeho vhodné násobky od ostatních tak, aby v nich zůstaly v prvním sloupci samé nuly; nezapomínáme na první řádek tabulky):

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | $-1$ | $-\frac{1}{2}$ | 0 | $\frac{3}{2}$ | 0 | $\frac{9}{2}$ |
| 0 | (1) | $-\frac{1}{2}$ | 1 | $\frac{1}{2}$ | 0 | $\frac{11}{2}$ |
| 1 | 0 | $\frac{1}{2}$ | 0 | $\frac{1}{2}$ | 0 | $\frac{3}{2}$ |
| 0 | 1 | $\frac{5}{2}$ | 0 | $-\frac{1}{2}$ | 1 | $\frac{13}{2}$ |

.

Nyní vybíráme z druhého sloupce a podle již aplikovaného pravidla vybereme první řádek ($\frac{11}{2} < \frac{13}{2}$), pivotem tedy bude jednička ve

Je snadné nahlédnout, že každý obecný problém lineárního programování lze převést na kterýkoliv ze standardních. Kromě změn znamének můžeme ještě pracovat s rozdělením případných proměnných bez omezení znaménka na rozdíl dvou kladných. Bez újmy na obecnosti se tedy budeme dále věnovat jen standardnímu maximalizačnímu problému.

Jak takový problém řešit? Hledáme maximum lineární formy $h$ na podmnožinách $M$ vektorového prostoru, které jsou zadány lineárními nerovnostmi, tj. v rovině pomocí průniku polorovin, obecně budeme v další kapitole hovořit o poloprostorech. Všimněme si, že každá lineární forma na reálném vektorovém prostoru $h : V \to \mathbb{R}$ (tj. libovolná lineární skalární funkce) v každém vybraném směru buď stále roste nebo stále klesá. Přesněji řečeno, jestliže vybereme pevný počáteční vektor $u \in V$ a „směrový“ vektor $v \in V$, pak složením naší formy $h$ s parametrizací dostaneme

$$t \mapsto h(u + t\,v) = h(u) + t\,h(v).$$

Tento výraz je skutečně s rostoucím parametrem $t$ vždy buď rostoucí nebo klesající, případně konstantní (podle toho, zda je $h(v)$ kladné nebo záporné, případně nulové).

Jistě tedy musíme očekávat, že problémy podobné tomu s natěračem budou buď nesplnitelné (když je množina zadaná omezením prázdná) nebo bude výnos neohraničený (když omezení zadají neomezenou část celého prostoru a forma $h$ v některém z neomezených směrů bude nenulová) nebo budou mít maximální řešení v alespoň jednom z „vrcholů“ množiny $M$ (přičemž zpravidla půjde o jediný vrchol, může ale jít o konstantní maximální hodnotu na části hranice oblasti $M$).

**3.5. Formulace pomocí lineárních rovnic.** Ne vždy je nalezení optima tak snadné jako v předchozím případě. Problém může zahrnovat velmi mnoho proměnných a velmi mnoho omezení a jen rozhodnout, zda je množina $M$ splnitelných bodů neprázdná, je problematické.



Nemáme tu prostor na úplnou teorii, zmíníme ale alespoň dva směry úvah, které ukazují, že ve skutečnosti bude řešení nalezitelné vždy podobně, jako tomu bylo v dvojrozměrném problému v předchozím odstavci.

Začneme srovnáním se systémy lineárních rovnic – těm už totiž rozumíme dobře. Zapišme si rovnice (3.1)–(3.3) vektorově v obecném tvaru:

$$A \cdot x \leq b,$$

kde $x$ je nyní $n$–rozměrný vektor, $b$ je $m$–rozměrný vektor a $A$ odpovídající matice a nerovností myslíme jednotlivé nerovnosti po řádcích. Maximalizovat chceme součin $c \cdot x$ pro daný řádkový vektor koeficientů lineární formy $h$. Jestliže si pro každou z rovnic přidáme jednu pomocnou proměnnou a ještě si přimyslíme proměnnou $z$ jako hodnotu lineární formy $h$, můžeme celý problém přepsat jako systém lineárních rovnic

$$\begin{pmatrix} 1 & -c & 0 \\ 0 & A & E_m \end{pmatrix} \cdot \begin{pmatrix} z \\ x \\ x_s \end{pmatrix} = \begin{pmatrix} 0 \\ b \end{pmatrix},$$

kde matice je složena z bloků o $1 + n + m$ sloupcích a $1 + m$ řádcích a tomu odpovídají jednotlivé komponenty vektorů. Dodatečně přitom požadujeme pro všechny souřadnice (proměnné) $x$ i $x_s$ nezápornost.

druhém řádku i sloupci tabulky. Eliminujeme podle ní:

$$\begin{array}{cccccc|c} 0 & 0 & -1 & 1 & 2 & 0 & 10 \\ \hline 0 & 1 & -\frac{1}{2} & 1 & \frac{1}{2} & 0 & \frac{11}{2} \\ 1 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{3}{2} \\ 0 & 0 & \textcircled{3} & -1 & -1 & 1 & 1 \end{array}.$$

Pivotem bude nyní číslo 3 ve třetím sloupci a čtvrtém řádku:

$$\begin{array}{ccccccc} 0 & 0 & 0 & \frac{2}{3} & \frac{5}{3} & \frac{1}{3} & \frac{31}{3} \\ \hline 0 & 1 & 0 & \frac{5}{6} & \frac{1}{3} & \frac{1}{6} & \frac{17}{3} \\ 1 & 0 & 0 & \frac{1}{6} & \frac{2}{3} & -\frac{1}{6} & \frac{4}{3} \\ 0 & 0 & 1 & -\frac{1}{3} & -\frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{array}.$$

Z výsledné tabulky odečteme řešení (hodnoty v pravém sloupci udávají hodnoty neznámých, zastoupených v „jednotkové podmatici“, pokud se proměnná v podmatici nevyskytuje, je její hodnota nulová – to ovšem není tento případ): $x_1 = \frac{4}{3}$, $x_2 = \frac{17}{3}$, $x_3 = \frac{1}{3}$. Maximální hodnota účelové funkce na zadané množině je pak $\frac{31}{3}$ (můžeme ji vyčíst v pravém horním rohu tabulky).

Z tabulky lze vyčíst i řešení duální úlohy, totiž minimalizovat $4u + 3v + 8w$ za podmínek

$$\begin{array}{rcrcrcl} u & + & 2v & + & w & \leq & 3, \\ -u & & & + & w & \geq & 1, \\ u & + & v & + & 3w & \geq & 2. \end{array}$$

Hodnota tohoto minima je totiž dle věty o dualitě (3.7) také $\frac{31}{3}$, odpovídající hodnoty proměnných odečteme v horním řádku tabulky ve sloupcích odpovídajících neznámým $u$, $v$, $w$, tedy ve sloupcích 4, 5 a 6: $u = \frac{2}{3}$, $v = \frac{5}{3}$, $w = \frac{1}{3}$. Není těžké si rozmyslet, že pro tři čísla $a_{14}$, $a_{15}$, $a_{16}$ v prvním řádku tabulky a zmíněných sloupcích a hodnotu $h$ v pravém horním rohu tabulky platí v průběhu výpočtu neustále $4a_{14}+3a_{15}+8a_{16} = h$. (Čísla v prvním řádku zmíněných sloupců totiž udávají, kolikrát byl řádek odpovídající doplňkové proměnné přičten k prvnímu, tedy nejpravější hodnota v prvním řádku bude odpovídající lineární kombinací nejpravějších hodnot ostatních řádků.) □

**3.4. Špetka teorie her.** Uvažme hru, kterou mezi sebou hrají dva



hráči, burzián a osud. Burzián chce investovat do zlata, stříbra, diamantů či do akcií významné softwarové firmy. Jsou známy zisky či ztráty těchto investic v posledních čtyř letech (pro jednoduchost výpočtu uvažujeme pouze poslední čtyři roky a zapišme je do matice $A = (a_{ij})$):

| | zlato | stříbro | diamanty | ovoce |
|---|---|---|---|---|
| 2001 | 2% | 1% | 4% | 3% |
| 2002 | 3% | -1% | -2% | 6% |
| 2003 | 1% | 2% | 3% | -4% |
| 2004 | -2% | 1% | 2% | 3% |

Pokud tedy má daný systém rovnic řešení, hledáme v této množině řešení takové hodnoty proměnných $z$, $x$ a $x_s$, aby všechna $x$ byla nezáporná a $z$ maximální možné. K diskusi, jak to obecně může dopadat se vrátíme z pohledu afinní geometrie v odstavci 4.11 na straně 199.

Konkrétně v našem problému černobílého natěrače bude systém lineárních rovnic vypadat takto:

$$\begin{pmatrix} 1 & -c_1 & -c_2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & w_1 & w_2 & 0 & 1 & 0 \\ 0 & b_1 & b_2 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} z \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ L \\ W \\ B \end{pmatrix}.$$

**3.6. Dualita v lineárním programování.** Uvažujme reálnou ma-



tici $A$ s $m$ řádky a $n$ sloupci, vektor omezení $b$ a řádkový vektor $c$ zadávající účelovou funkci. Z těchto dat můžeme sestavit dva problémy lineárního programování pro $x \in \mathbb{R}^n$ a $y \in \mathbb{R}^m$.

**Maximalizační problém:**
Maximalizuj $c \cdot x$ za podmínky $A \cdot x \leq b$ a zároveň $x \geq 0$.

**Minimalizační problém:**
Minimalizuj $y^T \cdot b$ za podmínky $y^T \cdot A \geq c^T$ a zároveň $y \geq 0$.

Říkáme, že tyto problémy jsou vzájemně duální. K odvození dalších vlastností problémů lineárního programování zavedeme trochu terminologie.

Řekneme, že jde o *řešitelný problém*, jestliže existuje nějaký *přípustný vektor* $x$, který vyhoví všem omezujícím podmínkám. Řešitelný maximalizační, resp. minimalizační problém je *ohraničený*, jestliže je účelová funkce na množině vyhovující omezením ohraničená shora, resp. zdola.

**Lemma.** *Je-li $x \in \mathbb{R}^n$ přípustný vektor pro standardní maximalizační problém a $y \in \mathbb{R}^m$ je přípustný vektor pro duální minimalizační problém, pak pro účelové funkce platí*

$$c \cdot x \leq y^T \cdot b$$

Důkaz. Jde vlastně jen o snadné pozorování: $x \geq 0$ a $c \leq y^T \cdot A$, ale také $y \geq 0$ a $A \cdot x \leq b$, proto musí platit

$$c \cdot x \leq y^T \cdot A \cdot x \leq y^T \cdot b,$$

což jsme měli dokázat. □

Odtud okamžitě vidíme, že jestliže jsou oba duální problémy řešitelné, pak musí být i ohraničené. Ještě zajímavější je následující postřeh přímo vycházející z nerovnosti v předchozí větě.

**Důsledek.** *Jestliže existují přípustné vektory $x$ a $y$ duálních lineárních problémů takové, že pro účelové funkce platí $c \cdot x = y^T \cdot b$, pak jde o optimální řešení obou problémů.*

**3.7. Věta** (O dualitě)**.** *Je-li standardní problém lineárního programování řešitelný a ohraničený, pak je takový i jeho duální problém, optimální hodnoty jejich účelových funkcí splývají a optimální řešení vždy existuje.*

Důkaz. Jeden směr tvrzení jsme již dokázali v předchozím důsledku. Zbývá důkaz existence optimálního řešení. Ten se nejsnadněji dokáže konstrukcí funkčního algoritmu, tomu se však teď nebudeme v podrobnostech věnovat. K chybějící části důkazu se vrátíme na straně 199 v afinní geometrii. □

Burzián chce investovat na jeden rok. Jak má rozložit svůj vklad, aby si zaručil maximální možný zisk bez ohledu na to, jak se situace na burze vyvine? (Předpokládáme, že následující rok bude nějakým pravděpodobnostním mixem čtyř předchozích let. Ve hře tedy osud zahraje nějaký pravděpodobnostní vektor $(x_1, x_2, x_3, x_4)$, burzián zvolí pravděpodobnostní vektor $(y_1, y_2, y_3, y_4)$ odpovídající rozdělení jeho vkladu. Výhra burziána je pak $\sum_{i,j=1}^{4} x_i y_j a_{ij}$.)

**Řešení.** Problém úlohy je najít pravděpodobnostní vektor $(y_1, y_2, y_3, y_4)$, který maximalizuje minimum ze všech hodnot $\sum_{i,j=1}^{4} x_i y_j a_{ij}$ pro $(y_1, y_2, y_3, y_4)$ pevné a $(x_1, x_2, x_3, x_4)$ libovolný pravděpodobnostní vektor.

Velmi bystrý čtenář si rozmyslí, že tento problém je ekvivalentní problému maximalizovat $z_1 + z_2 + z_3 + z_4$ za podmínky $A^T z \leq (1, \ldots, 1)^T$, $z \geq 0$ (hledaný pravděpodobnostní vektor $y$ pak dostaneme pravděpodobnostním normováním vektoru $z$). [1]

Řešme tedy tuto úlohu lineárního programování. Zavedeme pomocné proměnné $w_1, w_2, w_3, w_4$, převedeme úlohu do standardního tvaru

$$\max\left\{z_1 + z_2 + z_3 + z_4 \mid \left(A^T | E_4\right)(z, w) = (1, 1, 1, 1)^T\right\}$$

a zapíšeme do tabulky:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $-1$ | $-1$ | $-1$ | $-1$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $2$ | $3$ | $1$ | $-2$ | $1$ | $0$ | $0$ | $0$ | $1$ |
| $1$ | $-1$ | $2$ | $1$ | $0$ | $1$ | $0$ | $0$ | $1$ |
| $(4)$ | $-2$ | $3$ | $2$ | $0$ | $0$ | $1$ | $0$ | $1$ |
| $3$ | $6$ | $-4$ | $3$ | $0$ | $0$ | $0$ | $1$ | $1$ |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $0$ | $-\frac{3}{2}$ | $-\frac{1}{4}$ | $-\frac{1}{2}$ | $0$ | $0$ | $\frac{1}{4}$ | $0$ | $\frac{1}{4}$ |
| $0$ | $4$ | $-\frac{1}{2}$ | $-3$ | $1$ | $0$ | $-\frac{1}{2}$ | $0$ | $\frac{1}{2}$ |
| $0$ | $-\frac{1}{2}$ | $\frac{5}{4}$ | $\frac{1}{2}$ | $0$ | $1$ | $-\frac{1}{4}$ | $0$ | $\frac{3}{4}$ |
| $1$ | $-\frac{1}{2}$ | $\frac{3}{4}$ | $\frac{1}{2}$ | $0$ | $0$ | $\frac{1}{4}$ | $0$ | $\frac{1}{4}$ |
| $0$ | $\left(\frac{15}{2}\right)$ | $-\frac{25}{4}$ | $\frac{3}{2}$ | $0$ | $0$ | $-\frac{3}{4}$ | $1$ | $\frac{1}{4}$ |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $-\frac{3}{2}$ | $-\frac{1}{5}$ | $0$ | $0$ | $\frac{1}{10}$ | $\frac{1}{5}$ | $\frac{3}{10}$ |
| $0$ | $0$ | $\left(\frac{17}{6}\right)$ | $-\frac{19}{5}$ | $1$ | $0$ | $-\frac{1}{10}$ | $-\frac{8}{15}$ | $\frac{11}{30}$ |
| $0$ | $0$ | $\frac{5}{6}$ | $\frac{3}{5}$ | $0$ | $1$ | $-\frac{3}{10}$ | $\frac{1}{15}$ | $\frac{23}{30}$ |
| $1$ | $0$ | $\frac{1}{3}$ | $\frac{3}{5}$ | $0$ | $0$ | $\frac{1}{5}$ | $\frac{1}{15}$ | $\frac{4}{15}$ |
| $0$ | $1$ | $-\frac{5}{6}$ | $\frac{1}{5}$ | $0$ | $0$ | $-\frac{1}{10}$ | $\frac{2}{15}$ | $\frac{1}{30}$ |

[1] Toto je klíčová úvaha v proslulé von Neumannově větě, která říká, že pravděpodobnostní rozšíření libovolné maticové hry má rovnovážnou situaci.

Povšimněme si ještě pěkného přímého důsledku právě zformulované věty o dualitě:

**Důsledek** (Věta o ekvilibriu)**.** *Uvažme přípustné vektory $x$ a $y$ pro standardní maximalizační problém a jeho duální problém z definice 3.6. Pak jsou oba tyto vektory optimální, právě tehdy, když $y_i = 0$ pro všechny souřadnice s indexem $i$, pro které $\sum_{j=1}^{n} a_{ij} x_j < b_i$ a zároveň $x_j = 0$ pro všechny souřadnice s indexem $j$, pro které $\sum_{i=1}^{m} y_i a_{ij} > c_i$.*



Důkaz. Předpokládejme, že platí oba vztahy z předpokladu implikace ve větě. Pak tedy můžeme v následujícím výpočtu počítat s rovnostmi, protože sčítance s ostrou nerovností mají stejně u sebe nulové koeficienty:

$$\sum_{i=1}^{m} y_i b_i = \sum_{i=1}^{m} y_i \sum_{j=1}^{n} a_{ij} x_j = \sum_{i=1}^{m} \sum_{j=1}^{n} y_i a_{ij} x_j$$

a ze stejného důvodu také

$$\sum_{i=1}^{m} \sum_{j=1}^{n} y_i a_{ij} x_j = \sum_{j=1}^{n} c_j x_j.$$

Tím máme dokázánu jednu implikaci z tvrzení díky větě o dualitě.

Předpokládejme nyní, že $x$ a $y$ jsou skutečně optimální vektory. Víme tedy, že platí

$$\sum_{i=1}^{m} y_i b_i \geq \sum_{i=1}^{m} \sum_{j=1}^{n} y_i a_{ij} x_j \geq \sum_{j=1}^{n} c_j x_j,$$

ale zároveň jsou si levé a pravé strany rovny. Nastává tedy všude rovnost. Přepíšeme-li prvou rovnost jako

$$\sum_{i=1}^{m} y_i \left(b_i - \sum_{j=1}^{n} a_{ij} x_j\right) = 0,$$

vidíme, že může být naplněna jen za podmínek ve větě, protože jde o nulový součet samých nezáporných čísel. Z druhé rovnosti stejně plyne i druhé zbylé tvrzení a důkaz je ukončen. □

Věty o dualitě a ekvilibriu jsou užitečné při řešení problémů lineárního programování, protože nám ukazují souvislosti mezi nulovostí jednotlivých dodatečných proměnných a naplňování omezujících podmínek.

**3.8. Poznámky o lineárních modelech v ekonomii.** Náš velice schematický problém černobílého natěrače z odstavce 3.4 můžeme použít jako ilustraci jednoho z typických ekonomických modelů, tzv. *model plánování výroby*. Jde přitom o zachycení problému jako celku, tj. se zahrnutím vnitřních i vnějších vztahů. Levé strany rovnic (3.1), (3.2), (3.3) i účelové funkce $h(x_1, x_2)$ jsou vyjádřením různých výrobních vztahů. Podle povahy problému pak jsou požadovány na pravé straně buď přesné hodnoty (pak řešíme systém rovnic) nebo požadujeme kapacitní omezení a optimalizaci účelu (a pak dostáváme právě problémy lineárního programování).



Můžeme tak tedy obecně řešit problém alokace zdrojů při dodavatelských omezeních a přitom buď minimalizovat náklady nebo maximalizovat zisk. Z tohoto pohledu lze také nahlížet dualizaci problémů. Jestliže by náš natěrač chtěl hypoteticky nastavit svoje

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | $-\frac{188}{85}$ | $\frac{9}{17}$ | 0 | $\frac{4}{85}$ | $-\frac{7}{85}$ | $\frac{42}{85}$ |
| 0 | 0 | 1 | $-\frac{114}{85}$ | $\frac{6}{17}$ | 0 | $-\frac{3}{85}$ | $-\frac{16}{85}$ | $\frac{11}{85}$ |
| 0 | 0 | 0 | $\frac{146}{85}$ | $-\frac{5}{17}$ | 1 | $-\frac{23}{85}$ | $\frac{19}{85}$ | $\frac{56}{85}$ |
| 1 | 0 | 0 | $\frac{89}{85}$ | $-\frac{2}{17}$ | 0 | $\frac{18}{85}$ | $\frac{11}{85}$ | $\frac{19}{85}$ |
| 0 | 1 | 0 | $-\frac{78}{85}$ | $\frac{5}{17}$ | 0 | $-\frac{11}{85}$ | $-\frac{2}{85}$ | $\frac{12}{85}$ |
| $\frac{188}{89}$ | 0 | 0 | 0 | $\frac{25}{89}$ | 0 | $\frac{44}{89}$ | $\frac{17}{89}$ | $\frac{86}{89}$ |
| $\frac{114}{89}$ | 0 | 1 | 0 | $\frac{18}{89}$ | 0 | $\frac{21}{89}$ | $-\frac{2}{89}$ | $\frac{37}{89}$ |
| $-\frac{146}{89}$ | 0 | 0 | 0 | $-\frac{9}{89}$ | 1 | $-\frac{55}{89}$ | $\frac{1}{89}$ | $\frac{26}{89}$ |
| $-\frac{85}{89}$ | 0 | 0 | 1 | $-\frac{10}{89}$ | 0 | $\frac{18}{89}$ | $\frac{11}{89}$ | $\frac{19}{89}$ |
| $\frac{78}{89}$ | 1 | 0 | 0 | $\frac{17}{89}$ | 0 | $\frac{5}{89}$ | $\frac{8}{89}$ | $\frac{30}{89}$ |

Závěrečná tabulka již je optimální, neboť v prvním řádku se vyskytují jenom nezáporné hodnoty. Z tabulky odečteme optimální řešení úlohy: $z_2 = \frac{30}{89}$, $z_3 = \frac{37}{89}$, $z_4 = \frac{19}{89}$, $z_1 = 0$. Optimální hodnota (pravý horní roh) je pak $z_1 + z_2 + z_3 + z_4 = \frac{86}{89}$. Po přeškálování na pravděpodobnostní vektor (vynásobením hodnotou $\frac{89}{86}$) dostáváme řešení původní úlohy: $y_1 = 0$, $y_2 = \frac{30}{86}$, $y_3 = \frac{37}{86}$, $y_4 = \frac{19}{86}$ s optimální hodnotou $\frac{89}{86}$. Podotkněme, že závěry úlohy byly udělány bez vysvětlení s tím, že vzbudí zájem čtenáře o danou problematiku. Více viz početné zdroje na internetu. □

### B. Rekurentní rovnice

Různé lineární závislosti mohou být dobrým nástrojem pro popsání rozličných modelů růstu. Začněme s velmi populárním populačním modelem, který využívá lineární diferenční rovnici druhého řádu:

**3.5. Fibonacciho posloupnost.** Na začátku jara přinesl čáp na louku



dva čerstvě narozené zajíčky, samečka a samičku. Samička je schopná od dvou měsíců stáří povít každý měsíc dva malé zajíčky (samečka a samičku). Nově narození zajíci plodí potomky po jednom měsíci a pak každý další měsíc. Každá samička je březí jeden měsíc a pak opět porodí samečka a samičku. Kolik párů zajíců bude na louce po devíti měsících (pokud žádný neuhyne a žádný se tam „nepřistěhuje“)?

**Řešení.** Po uplynutí prvního měsíce je na louce pořád jeden pár, nicméně samička zabřezne. Po dvou měsících se narodí první potomci, takže na louce budou dva páry. Po uplynutí každého dalšího měsíce se narodí (tedy přibude) tolik zajíců, kolik zabřezlo zaječic před měsícem, což je přesně tolik, kolik bylo před měsícem párů schopných mít potomka, což je přesně tolik, kolik bylo párů před dvěma měsíci. Celkový počet $p_n$ zajíců po uplynutí $n$-tého měsíce tak je tak součtem počtů náklady spojené se svojí prací $y_L$, bílou barvou $y_W$ a černou barvou $y_B$, pak bude chtít minimalizovat účelovou funkci

$$L \cdot y_L + W y_W + B y_B$$

při omezujících podmínkách

$$y_L + w_1 y_W + b_1 y_B \geq c_1,$$
$$y_L + w_2 y_W + b_2 y_B \geq c_2.$$

To je právě duální problém k původnímu a hlavní věta 3.7 říká, že optimální stav je takový, kdy účelové funkce mají stejnou hodnotu.

V ekonomických modelech najdeme mnoho modifikací. Jednou z nich jsou *úlohy finančního plánování*, související s optimalizací portfolia. Určujeme přitom objemy investic do jednotlivých investičních variant s cílem držet se daných omezení na rizika a optimalizovat přitom zisk, resp. při očekávaném objemu minimalizovat rizika.

Dalším obvyklým modelem jsou *marketingové aplikace*, např. alokace nákladů na reklamy v různých médiích nebo umísťování reklam do časových termínů. Omezujícími podmínkami bude disponibilní rozpočet, rozložení cílových skupin apod.

Velmi obvyklé jsou modely *výživových problémů*, tj. návrh návek různých komponent výživy s daným složením a omezujícími požadavky na celkové objemy výživových látek.

Problémy lineárního programování se objevují při personálních úlohách, kdy jsou pracovníci s různými kvalifikacemi a dalšími předpoklady rozdělováni do směn. Obvyklé jsou také problémy *směšování*, problémy *dělení* a problémy *distribuce zboží*.

### 2. Diferenční rovnice

Diferenčními rovnicemi jsme se stručně zabývali již v první



kapitole, byť pouze těmi prvního řádu. Nyní si ukážeme obecnou teorii pro lineární rovnice s konstantními koeficienty, která poskytuje nejen velmi praktické nástroje, ale je také pěknou ilustrací pro koncepty vektorových podprostorů a lineárních zobrazení.

HOMOGENNÍ LINEÁRNÍ ROVNICE ŘÁDU $k$

**3.9. Definice.** *Homogenní lineární diferenční rovnice řádu $k$* je dána výrazem

$$a_0 x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = 0, \quad a_0 \neq 0, \quad a_k \neq 0,$$

kde koeficienty $a_i$, $i \in \{0, \ldots k\}$, jsou skaláry, které mohou případně i záviset na $n$.

Říkáme také, že taková rovnost zadává *homogenní lineární rekurenci* řádu $k$ a často zapisujeme hledanou posloupnost jako funkci

$$x_n = f(n) = -\frac{a_1}{a_0} f(n-1) - \cdots - \frac{a_k}{a_0} f(n-k).$$

Řešením této rovnice nazýváme posloupnost skalárů $x_i$, pro všechna $i \in \mathbb{N}$, případně $i \in \mathbb{Z}$, které vyhovují rovnici pro všechna $n$.

párů v předchozích dvou měsících. Pro počet párů zajíců na louce tedy dostáváme *homogenní lineární rekurentní formuli*

$$p_{n+2} = p_{n+1} + p_n, \quad n \in \mathbb{N}, \tag{3.1}$$

která spolu s počátečními podmínkami $p_1 = 1$ a $p_2 = 1$ jednoznačně určuje počty párů zajíců na louce v jednotlivých měsících. Linearita formule znamená, že všechny členy posloupnosti $(p_n)$ jsou ve vztahu v první mocnině, rekurence je snad jasná a homogenita značí, že v předpisu chybí absolutní člen (viz 3.14 pro nehomogenní rovnice). Pro hodnotu $n$-tého členu můžeme odvodit explicitní formuli. V hledaní formule nám pomůže pozorování, že pro jistá $r$ je funkce $r^n$ řešením diferenční rovnice bez počátečních podmínek. Tato $r$ získáme tak, že dosadíme do rekurentního vztahu:

$$r^{n+2} = r^{n+1} + r^n, \text{ a po vydělení } r^n \text{ dostaneme}$$
$$r^2 = r + 1,$$

což je tzv. *charakteristická rovnice* daného rekurentního vztahu. Naše rovnice má kořeny $\frac{1-\sqrt{5}}{2}$ a $\frac{1+\sqrt{5}}{2}$ a tedy posloupnosti $a_n = \left(\frac{1-\sqrt{5}}{2}\right)^n$ a $b_n = \left(\frac{1+\sqrt{5}}{2}\right)^n$, $n \geq 1$, vyhovují danému vztahu. Vztah také splňuje jejich libovolná tzv. lineární kombinace, tedy posloupnost $c_n = sa_n + tb_n$, $s, t \in \mathbb{R}$. Čísla $s$ a $t$ můžeme zvolit tak, aby výsledná kombinace splňovala dané počáteční podmínky, v našem případě $c_1 = 1$, $c_2 = 1$. Pro jednoduchost je vhodné navíc ještě dodefinovat nultý člen posloupnosti jako $c_0 = 0$ a spočítat $s$ a $t$ z rovnic pro $c_0$ a $c_1$. Zjistíme, že $s = -\frac{1}{\sqrt{5}}$, $t = \frac{1}{\sqrt{5}}$ a tedy

$$p_n = \frac{\left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n}{2^n\left(\sqrt{5}\right)}. \tag{3.2}$$

Takto zadaná posloupnost splňuje danou rekurentní formuli a navíc počáteční podmínky $c_0 = 0$, $c_1 = 1$, jedná se tedy o tu jedinou posloupnost, která je těmito požadavky zadána. Všimněte si, že hodnota vzorce (‖3.2‖) je celočíselná pro libovolné přirozené $n$ (zadává totiž celočíselnou Fibonacciho posloupnost), i když to tak na první pohled nevypadá. □

**3.6. Zjednodušený model chování hrubého národního produktu.** Uvažujme diferenční rovnici

$$y_{k+2} - a(1+b)y_{k+1} + aby_k = 1, \tag{3.3}$$



Libovolným zadáním $k$ po sobě jdoucích hodnot $x_i$ jsou určeny i všechny ostatní hodnoty jednoznačně. Skutečně, pracujeme nad polem skalárů, takže hodnoty $a_0$ i $a_k$ jsou invertibilní, a proto z definičního vztahu lze vždy spočíst hodnotu $x_n$ ze známých ostatních hodnot a stejně tak pro $x_{n-k}$. Indukcí tedy okamžitě dokážeme, že lze jednoznačně dopočítat všechny hodnoty jak pro kladná tak pro záporná celá $n$.

Prostor všech nekonečných posloupností $x_i$ je vektorový prostor, kde sčítání i násobení skaláry je dáno po složkách. Přímo z definice je zjevné, že součet dvou řešení homogenní lineární rovnice nebo skalární násobek řešení je opět řešení. Stejně jako u homogenních systémů lineárních tedy vidíme, že množina všech řešení je vektorový podprostor.

Počáteční podmínka na hodnoty řešení je dána jako $k$– rozměrný vektor v $\mathbb{K}^k$. Součtu počátečních podmínek odpovídá součet příslušných řešení a obdobně se skalárními násobky. Dále si všimněme, že dosazením nul a jedniček do zadávaných počátečních $k$ hodnot snadno získáme $k$ lineárně nezávislých řešení naší rovnice. Jakkoliv jsou tedy zkoumané vektory nekonečné posloupnosti skalárů, samotný prostor všech řešení je konečněrozměrný. Předem víme, že jeho dimenze bude rovna řádu rovnice $k$, a umíme snadno určit bázi všech těchto řešení. Opět hovoříme o *fundamentálním systému řešení* a všechna ostatní řešení jsou právě jejich lineárními kombinacemi.

Jak jsme si již ověřili, vybereme-li $k$ po sobě jdoucích indexů $i, i+1, \ldots, i+k-1$, zadává homogenní lineární diferenční rovnice lineární zobrazení $\mathbb{K}^k \to \mathbb{K}^\infty$ $k$–rozměrných vektorů počátečních hodnot do nekonečně rozměrných posloupností týchž skalárů. Nezávislost různých takových řešení je ekvivalentní nezávislosti počátečních hodnot, ale tu umíme snadno rozpoznat pomocí determinantu. Máme-li $k$–tici řešení $(x_n^{[1]}, \ldots, x_n^{[k]})$, pak jde o nezávislá řešení, právě když následující determinant, tzv. *Casoratián*, je nenulový pro jedno (a pak už všechna) $n$

$$C(x_n^{[1]}, \ldots, x_n^{[k]}) = \begin{vmatrix} x_n^{[1]} & \cdots & x_n^{[k]} \\ x_{n+1}^{[1]} & \cdots & x_{n+1}^{[k]} \\ \vdots & \ddots & \vdots \\ x_{n+k-1}^{[1]} & \cdots & x_{n+k-1}^{[k]} \end{vmatrix} \neq 0.$$

**3.10. Rekurence s konstantními koeficienty.** Těžko bychom hledali univerzální postup, jak hledat řešení obecných homogenních lineárních diferenčních rovnic, tj. přímo spočítatelný výraz pro obecné řešení $x_n$.



V praktických modelech ale velice často vystupují rovnice, kde jsou koeficienty konstantní. V tomto případě se daří uhodnout vhodnou formu řešení a skutečně se nám podaří najít $k$ lineárně nezávislých možností. Tím budeme mít problém vyřešený, protože všechna ostatní řešení budou jejich lineární kombinací.

Pro jednoduchost začneme rovnicemi druhého řádu. Takové potkáváme obzvlášť často v praktických problémech, kde se vyskytují vztahy závisející na dvou předchozích hodnotách. Lineární diferenční rovnicí druhého řádu s konstantními koeficienty (resp. lineární rekurencí druhého řádu s konstantními koeficienty) tedy rozumíme předpis

$$f(n+2) = a \cdot f(n+1) + b \cdot f(n) + c, \tag{3.4}$$

kde $y_k$ je národní produkt v roce $k$. Konstanta $a$ je takzvaný *mezní sklon ke spotřebě*, což je makroekonomický ukazatel, který udává jaký zlomek peněz, které mají obyvatelé k dispozici, utratí, a konstanta $b$ popisuje, jak závisí míra investic soukromého sektoru na mezním sklonu ke spotřebě.



Předpokládáme dále, že velikost národního produktu je normována tak, aby na pravé straně rovnice vyšlo číslo 1.

Spočítejte konkrétní hodnoty pro $a = \frac{3}{4}$, $b = \frac{1}{3}$, $y_0 = 1$, $y_1 = 1$.

**Řešení.** Nejprve budeme hledat řešení homogenní rovnice (pravá strana nulová) ve tvaru $r^k$. Číslo $r$ musí být řešením charakteristické rovnice

$$x^2 - a(1+b)x + ab = 0, \text{ tj. } x^2 - x + \frac{1}{4} = 0,$$

která má dvojnásobný kořen $\frac{1}{2}$. Všechna řešení homogenní rovnice jsou potom tvaru $a(\frac{1}{2})^n + bn(\frac{1}{2})^n$, viz 3.12.

Dále si všimněme, že najdeme-li nějaké řešení nehomogenní rovnice (tzv. partikulární řešení), tak pokud k němu přičteme libovolné řešení homogenní rovnice, obdržíme jiné řešení nehomogenní rovnice. Lze ukázat, že takto získáme všechna řešení nehomogenní rovnice (viz 3.14).

V našem případě (tj. pokud jsou všechny koeficienty i nehomogenní člen konstantami) je partikulárním řešením konstanta $y_n = c$. Dosazením do rovnice máme $c - c + \frac{1}{4}c = 1$, tedy $c = 4$. Všechna řešení diferenční rovnice

$$y_{k+2} - y_{k+1} + \frac{1}{4} \cdot y_k = 1$$

jsou tedy tvaru $4 + a\left(\frac{1}{2}\right)^n + bn\left(\frac{1}{2}\right)^n$. Požadujeme $y_0 = y_1 = 1$ a tyto dvě rovnice dávají $a = b = -3$, tedy řešení naší nehomogenní rovnice je

$$y_n = 4 - 3\left(\frac{1}{2}\right)^n - 3n\left(\frac{1}{2}\right)^n.$$

Opět protože víme, že posloupnost zadaná touto formulí splňuje danou diferenční rovnici a zároveň dané počáteční podmínky, jedná se vskutku o tu jedinou posloupnost, která je těmito vlastnostmi charakterizována. □

V předchozím příkladu jsme použili tzv. *metodu neurčitých koeficientů*. Ta spočívá v tom, že na základě nehomogenního členu dané diferenční rovnice „uhodneme“ tvar partikulárního řešení. Tvary partikulárních řešení jsou známy pro celou řadu nehomogenních členů. Např. rovnice

$$y_{n+k} + a_1 y_{n+k-1} + \cdots + a_k y_n = P_m(n), \tag{3.4}$$

kde $a, b, c$ jsou známé skalární koeficienty.

Např. v populačních modelech můžeme zohlednit, že jedinci v populaci dospívají a pořádně se rozmnožují až o dvě období později (tj. přispívají k hodnotě $f(n+2)$ násobkem $b \cdot f(n)$ s kladným $b > 1$), zatímco nedospělí jedinci vysílí a zničí část dospělé populace (tj. koeficient $a$ pak bude záporný). Navíc si je třeba někdo pěstuje a průběžně si ujídá konstantní počet $c < 0$ v každém jednotlivém období.

Speciálním takovým příkladem s $c = 0$ je např. Fibonacciho posloupnost čísel $y_0, y_1, \ldots$, kde $y_{n+2} = y_{n+1} + y_n$.

Jestliže při řešení matematického problému nemáme žádný nový nápad, vždy můžeme zkusit, do jaké míry funguje známé řešení podobných úloh. Zkusme proto dosadit do rovnice (3.4) s koeficientem $c = 0$ podobné řešení jako u rovnic prvního řádu, tj. $f(n) = \lambda^n$ pro nějaké skalární $\lambda$. Dosazením dostáváme

$$\lambda^{n+2} - a\lambda^{n+1} - b\lambda^n = \lambda^n\left(\lambda^2 - a\lambda - b\right) = 0.$$

Tento vztah bude platit buď pro $\lambda = 0$ nebo při volbě hodnot

$$\lambda_1 = \frac{1}{2}\left(a + \sqrt{a^2+4b}\right), \quad \lambda_2 = \frac{1}{2}\left(a - \sqrt{a^2+4b}\right).$$

Zjistili jsme tedy, že skutečně opět taková řešení fungují, jen musíme vhodně zvolit skalár $\lambda$. To nám ale nestačí, protože my chceme najít řešení pro jakékoliv počáteční hodnoty $f(0)$ a $f(1)$, a zatím jsme našli jen dvě konkrétní posloupnosti splňující danou rovnici (a nebo dokonce jen jednu, pokud je $\lambda_2 = \lambda_1$).

Jak jsme již dovodili i u zcela obecných lineárních rekurencí, součet dvou řešení $f_1(n)$ a $f_2(n)$ naší rovnice

$$f(n+2) - a \cdot f(n+1) - b \cdot f(n) = 0$$

je zjevně opět řešením téže rovnice a totéž platí pro konstantní násobky řešení. Naše dvě konkrétní řešení proto poskytují daleko obecnější řešení

$$f(n) = C_1\lambda_1^n + C_2\lambda_2^n$$

pro libovolné skaláry $C_1$ a $C_2$. Pro jednoznačné vyřešení konkrétní úlohy se zadanými počátečními hodnotami $f(0)$ a $f(1)$ nám zbývá jen najít příslušné konstanty $C_1$ a $C_2$. (A také si musíme ujasnit, zda to pro všechny počáteční hodnoty půjde).

**3.11. Volba skalárů.** Ukažme si, jak to může fungovat alespoň na jednom příkladě. Soustředíme se přitom na problém, že kořeny charakteristického polynomu nevychází obecně ve stejném oboru skalárů, jako jsou koeficienty v rovnici. Řešme tedy problém:

$$\begin{aligned} y_{n+2} &= y_{n+1} + \frac{1}{2}y_n, \\ y_0 &= 2,\ y_1 = 0. \end{aligned} \tag{3.5}$$

V našem případě je tedy $\lambda_{1,2} = \frac{1}{2}\left(1 \pm \sqrt{3}\right)$ a zjevně

$$\begin{aligned} y_0 &= C_1 + C_2 = 2, \\ y_1 &= \frac{1}{2}C_1\left(1+\sqrt{3}\right) + \frac{1}{2}C_2\left(1-\sqrt{3}\right) \end{aligned}$$

je splněno pro právě jednu volbu těchto konstant. Přímým výpočtem $C_1 = 1 - \frac{1}{3}\sqrt{3}$, $C_2 = 1 + \frac{1}{3}\sqrt{3}$ a naše úloha má jediné řešení

$$\begin{aligned} f(n) = \left(1 - \tfrac{1}{3}\sqrt{3}\right)\tfrac{1}{2^n}\left(1+\sqrt{3}\right)^n + \\ + \left(1 + \tfrac{1}{3}\sqrt{3}\right)\tfrac{1}{2^n}\left(1-\sqrt{3}\right)^n. \end{aligned}$$

kde $P_m(n)$ je polynom stupně $m$ a příslušná charakteristická rovnice má reálné kořeny, má (skoro vždy) partikulární řešení tvaru $Q_m(n)$ a kde $Q_m(n)$ je polynom stupně $m$.

Další možným způsobem řešení je tzv. *metoda variace konstant*, kdy nejprve najdeme řešení

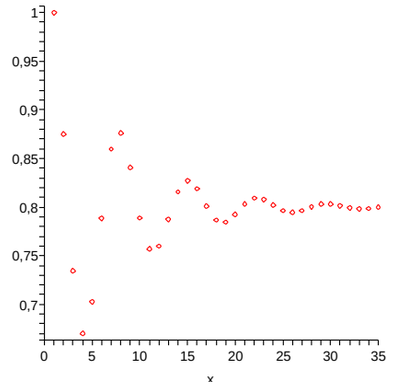
$$y(n) = \sum_{i=1}^{k} c_i f_i(n)$$

zhomogenizované rovnice a poté uvažujeme konstanty $c_i$ jako funkce $c_i(n)$ proměnné $n$ a hledáme partikulární řešení dané rovnice ve tvaru

$$y(n) = \sum_{i=1}^{k} c_i(n) f_i(n).$$

Na následujícím obrázku jsou vyneseny hodnoty $f(n)$ pro $n \leq 35$, kde $f$ vyhovuje rovnici

$$f(n) = \frac{9}{8} f(n-1) - \frac{3}{4} f(n-2) + \frac{1}{2}, \quad f(0) = f(1) = 1.$$




Dále si procvičme, jak řešit lineární diferenční rovnice druhého řádu s konstantními koeficienty. Posloupnost vyhovující dané rekurentní rovnici druhého řádu je dána jednoznačně, pokud zadáme navíc nějaké dva její sousední členy. Znovu si povšimněme dalšího využití komplexních čísel: pro určení explicitního vzorce pro $n$-tý člen posloupnosti reálných čísel můžeme potřebovat výpočty s čísly komplexními (to nastává tehdy, pokud má charakteristický polynom dané diferenční rovnice komplexní kořeny, viz též 3.14).

**3.7.** Nalezněte explicitní vzorec pro posloupnost vyhovující následující lineární diferenční rovnici s počátečními podmínkami:

$$x_{n+2} = 2x_n + n, \; x_1 = 2, x_2 = 2.$$

**Řešení.** Zhomogenizovaná rovnice je

$$x_{n+2} = 2x_n.$$

Všimněme si, že i když nalezená řešení pro rovnice s celočíselnými koeficienty vypadají složitě a jsou vyjádřena pomocí iracionálních (případně komplexních) čísel, o samotném řešení dopředu víme, že je celočíselné též. Bez tohoto „úkroku“ do většího oboru skalárů bychom ovšem obecné řešení napsat neuměli.

S podobnými jevy se budeme potkávat velice často. Obecné řešení nám také umožňuje bez přímého vyčíslování konstant diskutovat kvalitativní chování posloupnosti čísel $f(n)$, tj. zda se budou s rostoucím $n$ blížit k nějaké pevné hodnotě nebo budou oscilovat v nějakém rozsahu nebo utečou do neomezených kladných nebo záporných hodnot.

**3.12. Obecný případ homogenních rekurencí.** Zkusme nyní stejně jako v případě druhého řádu dosadit volbu $x_n = \lambda^n$ pro nějaký (zatím neznámý) skalár $\lambda$ do obecné homogenní rovnice z definice 3.9. Dostáváme pro každé $n$ podmínku



$$\lambda^{n-k}\left(a_0\lambda^k + a_1\lambda^{k-1} \cdots + a_k\right) = 0,$$

což znamená, že buď $\lambda = 0$ nebo je $\lambda$ kořenem tzv. *charakteristického polynomu* v závorce. Charakteristický polynom ale už není závislý na $n$.

Předpokládejme, že má charakteristický polynom $k$ různých kořenů $\lambda_1, \ldots, \lambda_k$. Můžeme za tímto účelem i rozšířit uvažované pole skalárů, např. $\mathbb{Q}$ na $\mathbb{R}$ nebo $\mathbb{R}$ na $\mathbb{C}$, protože výsledkem výpočtu pak stejně budou řešení, která opět zůstanou v původním poli díky samotné rovnici. Každý z kořenů nám dává jedno možné řešení

$$x_n = (\lambda_i)^n.$$

Abychom byli uspokojeni, potřebujeme $k$ lineárně nezávislých řešení.

K tomu nám postačí ověřit nezávislost dosazením $k$ hodnot pro $n = 0, \ldots, k-1$ pro $k$ možností $\lambda_i$ do Casoratiánu, viz 3.9. Dostaneme tak tzv. Vandermondovu matici a je pěkným (ale ne úplně snadným) cvičením spočíst, že pro všechna $k$ a jakékoliv $k$–tice různých $\lambda_i$ je determinant takovéto matice nenulový, viz příklad ‖2.24‖ na straně 80. To ale znamená, že zvolená řešení jsou lineárně nezávislá.

Nalezli jsme tedy fundamentální systém řešení homogenní diferenční rovnice v případě, že všechny kořeny jejího charakteristického polynomu jsou po dvou různé.

Uvažme nyní násobný kořen $\lambda$ a dosaďme do definiční rovnice předpokládané řešení $x_n = n\lambda^n$. Dostáváme podmínku

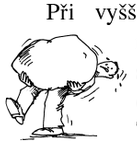
$$a_0 n\lambda^n + \cdots + a_k(n-k)\lambda^{n-k} = 0.$$

Tuto podmínku je možné přepsat pomocí tzv. derivace polynomu (viz 5.6 na straně 239), kterou značíme apostrofem:

$$\lambda(a_0\lambda^n + \cdots + a_k\lambda^{n-k})' = 0$$

a hned na začátku kapitoly páté uvidíme, že kořen polynomu $f$ je vícenásobný, právě když je kořenem i jeho derivace $f'$. Naše podmínka je tedy splněna.

Při vyšší násobnosti $\ell$ kořenu charakteristického polynomu můžeme postupovat obdobně a využijeme skutečnosti, že $\ell$–násobný kořen je kořenem všech derivací polynomu až do $(\ell-1)$-ní derivace včetně. Tuto skutečnost dokážeme na začátku páté kapitoly.



Její charakteristický polynom je $x^2-2$, jeho kořeny jsou $\pm\sqrt{2}$. Řešení zhomogenizované rovnice je tedy tvaru

$$a\left(\sqrt{2}\right)^n + b\left(-\sqrt{2}\right)^n \text{ pro libovolná } a, b \in \mathbb{R}.$$

Partikulární řešení budeme hledat metodou neurčitých koeficientů. Nehomogenní část dané rovnice je lineární polynom $n$, partikulární řešení proto budeme nejprve hledat ve tvaru lineárního polynomu v proměnné $n$, tedy $kn+l$, kde $k, l \in \mathbb{R}$. Dosazením do původní rovnice dostáváme

$$k(n+2)+l = 2(kn+l)+n.$$

Porovnáním koeficientů u proměnné $n$ na obou stranách rovnice dostáváme vztah $k = 2k+1$, tedy $k=-1$, porovnáním absolutních členů pak vztah $2k+l = 2l$, tedy $l=-2$. Celkem je tedy partikulárním řešením je posloupnost $-n-2$.

Řešení dané nehomogenní diferenční rovnice druhého řádu bez počátečních podmínek jsou tedy tvaru $a\left(\sqrt{2}\right)^n + b\left(-\sqrt{2}\right)^n - n - 2$, $a, b \in \mathbb{R}$.

Nyní dosazením do počátečních podmínek určíme neznámé $a, b \in \mathbb{R}$. Pro početní jednoduchost použijeme malého triku: z počátečních podmínek a daného rekurentního vztahu vypočteme člen $x_0 : x_0 = \frac{1}{2}(x_2 - 0) = 1$. Daný rekurentní vztah spolu s podmínkami $x_0 = 1$ a $x_1 = 1$ pak zřejmě splňuje tatáž posloupnost, která splňuje původní počáteční podmínky. Máme tedy následující vztahy pro $a, b$:

$$x_0 : a\left(\sqrt{2}\right)^0 + b\left(-\sqrt{2}\right)^0 - 2 = 1, \text{ tedy } a+b=3,$$
$$x_1 : \sqrt{2}a - \sqrt{2}b = 5,$$

jejichž řešením dostáváme $a = \frac{6+5\sqrt{2}}{4}$, $b = \frac{6-5\sqrt{2}}{4}$. Řešením je posloupnost

$$x_n = \tfrac{6+5\sqrt{2}}{4}\left(\sqrt{2}\right)^n + \tfrac{6-5\sqrt{2}}{4}\left(-\sqrt{2}\right)^n - n - 2. \qquad \square$$

**3.8.** Určete reálnou bázi prostoru řešení homogenní diferenční rovnice

$$x_{n+4} = x_{n+3} + x_{n+1} - x_n,$$

**Řešení.** Charakteristický polynom dané rovnice je $x^4 - x^3 - x + 1$. Hledáme-li jeho kořeny, řešíme *reciprokou rovnici* (to znamená, že koeficienty u $(n-k)$-té a $k$-té mocniny $x$, $k = 1, \ldots, n$, jsou shodné)

$$x^4 - x^3 - x + 1 = 0.$$

Standardním postupem nejprve vydělíme rovnici výrazem $x^2$ a poté zavedeme substituci $t = x + \frac{1}{x}$, tedy $t^2 = x^2 + \frac{1}{x^2} + 2$. Obdržíme

Derivace přitom postupně vypadají takto:

$$f(\lambda) = a_0\lambda^n + \cdots + a_k\lambda^{n-k},$$
$$f'(\lambda) = a_0 n\lambda^{n-1} + \cdots + a_k(n-k)\lambda^{n-k-1},$$
$$f''(\lambda) = a_0 n(n-1)\lambda^{n-2} + \cdots + a_k(n-k)(n-k-1)\lambda^{n-k-2},$$
$$\vdots$$
$$f^{(\ell+1)} = a_0 n\ldots(n-\ell)\lambda^{n-\ell-1} + \ldots$$
$$\cdots + a_k(n-k)\ldots(n-k-\ell)\lambda^{n-k-\ell-1}.$$

Podívejme se na případ trojnásobného kořenu $\lambda$ a hledejme řešení ve tvaru $n^2\lambda^n$. Dosazením do definiční podmínky dostaneme rovnost

$$a_0 n^2\lambda^n + \cdots + a_k(n-k)^2\lambda^{n-k} = 0.$$

Zjevně je levá strana rovna výrazu $\lambda^2 f''(\lambda) + \lambda f'(\lambda)$, a protože je $\lambda$ kořenem obou derivací, je podmínka splněna.

Indukcí snadno dokážeme, že i obecnou podmínku pro hledané řešení ve tvaru $x_n = n^\ell\lambda^n$,

$$a_0 n^\ell\lambda^n + \ldots a_k(n-k)^\ell\lambda^{n-k} = 0,$$

dostaneme jako vhodnou lineární kombinaci derivací charakteristického polynomu začínající výrazem

$$\lambda^{\ell+1} f^{(\ell+1)} + \frac{1}{2}\lambda^\ell\ell(\ell+1)f^{(\ell)} + \ldots,$$

čímž jsme téměř dokázali následující:

**Věta.** *Každá homogenní lineární diferenční rovnice řádu $k$ nad libovolným číselným oborem $\mathbb{K}$ obsaženým v komplexních číslech $\mathbb{K}$ má za množinu všech řešení $k$–rozměrný vektorový prostor generovaný posloupnostmi $x_n = n^\ell\lambda^n$, kde $\lambda$ jsou (komplexní) kořeny charakteristického polynomu, a $\ell = 0, \ldots s-1$, kde $s$ je násobnost příslušného kořenu $\lambda$.*

Důkaz. Výše použité vztahy násobnosti kořenů a derivací uvidíme později, a nebudeme tu dokazovat tvrzení, že každý komplexní polynom má právě tolik kořenů, včetně násobnosti, jaký má stupeň. Zbývá tedy ještě dokázat, že nalezená $k$–tice řešení je lineárně nezávislá. I v tomto případě lze induktivně dokázat nenulovost příslušného Casoratiánu, jako jsme odkazovali u případu Vandermondova determinantu výše.

Pro ilustraci postupu ukážeme, jak výpočet vypadá pro případ jednoduchého kořenu $\lambda_1$ a dvojnásobného kořenu $\lambda_2$ charakteristického polynomu:

$$C\left(\lambda_1^n, \lambda_2^n, n\lambda_2^n\right) = \begin{vmatrix} \lambda_1^n & \lambda_2^n & n\lambda_2^n \\ \lambda_1^{n+1} & \lambda_2^{n+1} & (n+1)\lambda_2^{n+1} \\ \lambda_1^{n+2} & \lambda_2^{n+2} & (n+2)\lambda_2^{n+2} \end{vmatrix} =$$
$$= \lambda_1^n\lambda_2^{2n}\begin{vmatrix} 1 & 1 & n \\ \lambda_1 & \lambda_2 & (n+1)\lambda_2 \\ \lambda_1^2 & \lambda_2^2 & (n+2)\lambda_2^2 \end{vmatrix} =$$
$$= \lambda_1^n\lambda_2^{2n}\begin{vmatrix} 1 & 1 & n \\ \lambda_1-\lambda_2 & 0 & \lambda_2 \\ \lambda_1(\lambda_1-\lambda_2) & 0 & \lambda_2^2 \end{vmatrix} =$$
$$= -\lambda_1^n\lambda_2^{2n}\begin{vmatrix} \lambda_1-\lambda_2 & \lambda_2 \\ \lambda_1(\lambda_1-\lambda_2) & \lambda_2^2 \end{vmatrix} =$$
$$= \lambda_1^n\lambda_2^{2n+1}(\lambda_1-\lambda_2)^2 \neq 0.$$

rovnici

$$t^2 - t - 2 = 0$$

s kořeny $t_1 = -1, t_2 = 2$. Pro obě tyto hodnoty neznámé $t$ pak řešíme zvlášť rovnici danou substitučním vztahem:

$$x + \frac{1}{x} = -1.$$

Ta má dva komplexní kořeny $x_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos(2\pi/3) + i\sin(2\pi/3)$ a $x_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = \cos(2\pi/3) - i\sin(2\pi/3)$.

Pro druhou hodnotu neznámé $t$ dostáváme rovnici

$$x + \frac{1}{x} = 2$$

s dvojnásobným kořenem 1. Celkem je tedy bází hledaného vektorového prostoru posloupností, které jsou řešením dané diferenční rovnice, následující čtveřice posloupností: $\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)_{n=1}^{\infty}$, $\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)_{n=1}^{\infty}$,$(1)_{n=1}^{\infty}$ (konstantní posloupnost) a $(n)_{n=1}^{\infty}$. Hledáme-li však reálnou bázi, musíme nahradit dva generátory (posloupnosti) z této báze s komplexními hodnotami generátory reálnými. Protože tyto generátory jsou geometrické řady, jejichž libovolné členy jsou komplexně sdružená čísla, můžeme vzít jako vhodné generátory posloupnosti dané polovinou součtu, resp. polovinou $i$-násobku rozdílu, daných komplexních generátorů. Takto dostaneme následující reálnou bázi řešení: $(1)_{n=1}^{\infty}$ (konstantní posloupnost), $(n)_{n=1}^{\infty}$, $(\cos(n \cdot 2\pi/3))_{n=1}^{\infty}$, $(\sin(n \cdot 2\pi/3))_{n=1}^{\infty}$. □

**3.9.** Najděte posloupnost, která vyhovuje nehomogenní diferenční rovnici s počátečními podmínkami:

$$x_{n+2} = x_{n+1} + 2x_n + 1, \quad x_1 = 2,\ x_2 = 2.$$

**Řešení.** Obecné řešení zhomogenizované rovnice je tvaru $a(-1)^n + b2^n$. Partikulárním řešením je konstanta $-1/2$. Obecné řešení dané nehomogenní rovnice bez počátečních podmínek je tedy

$$x_n = a(-1)^n + b2^n - \frac{1}{2}.$$

Dosazením do počátečních podmínek zjistíme konstanty $a = -5/6$, $b = 5/6$. Dané rovnici s počátečními podmínkami tedy vyhovuje posloupnost

$$x_n = -\frac{5}{6}(-1)^n + \frac{5}{3}2^{n-1} - \frac{1}{2}.$$ □

**3.10.** Řešte následující diferenční rovnici:

$$x_{n+4} = x_{n+3} - x_{n+2} + x_{n+1} - x_n.$$

**Řešení.** Z teorie víme, že prostor řešení této diferenční rovnice bude čtyřdimenzionální vektorový prostor, jehož generátory zjistíme V obecném případě vedeme podobně důkaz nenulovosti příslušného Casoratiánu indukcí. □

**3.13. Reálné báze řešení.** Pro rovnice s reálnými koeficienty povedou reálné počáteční podmínky vždy na reálná řešení. Přesto ale budou příslušná fundamentální řešení z právě odvozené věty často existovat pouze v oboru komplexním.



Zkusme proto najít jiné generátory, se kterými se nám bude pracovat lépe. Protože jsou koeficienty charakteristického polynomu reálné, každý jeho kořen bude buď také reálný nebo musí kořeny vystupovat po dvou komplexně sdružených.

Jestliže si řešení popíšeme v goniometrickém tvaru jako

$$\lambda^n = |\lambda|^n(\cos n\varphi + i\sin n\varphi),$$
$$\bar{\lambda}^n = |\lambda|^n(\cos n\varphi - i\sin n\varphi),$$

okamžitě je vidět, že jejich součtem a rozdílem dostáváme jiná dvě lineárně nezávislá řešení (nezávislost snadno ověříme pomocí Casoratiánu)

$$x_n = |\lambda|^n \cos n\varphi, \quad y_n = |\lambda|^n \sin n\varphi.$$

Diferenční rovnice se velmi často vyskytují jako model dynamiky nějakého systému. Pěkným tématem na přemýšlení je proto souvislost absolutních hodnot jednotlivých kořenů a stabilizace řešení, buď všech nebo v závislosti na počátečních podmínkách. Nepůjdeme zde do podrobností, protože teprve v páté kapitole budeme probírat pojem konvergence hodnot k nějaké hodnotě limitní apod., jistě je tu ale prostor pro zajímavé numerické experimenty např. s oscilacemi vhodných populačních nebo ekonomických modelů.

**3.14. Nehomogenní lineární diferenční rovnice.** Stejně jako u systémů lineárních rovnic můžeme dostat všechna řešení *nehomogenních lineárních diferenčních rovnic*



$$a_0(n)x_n + a_1(n)x_{n-1} + \cdots + a_k(n)x_{n-k} = b(n),$$

kde koeficienty $a_i$ a $b$ jsou skaláry, které mohou záviset na $n$, a $a_0(n) \neq 0, a_k(n) \neq 0$.

Postupujeme tak, že najdeme jedno řešení a přičteme celý vektorový prostor dimenze $k$ řešení odpovídajících systémů homogenních. Skutečně takto dostáváme řešení a protože je rozdíl dvou řešení nehomogenní rovnice zjevně řešením homogenní rovnice, dostáváme takto řešení všechna.

U systému lineárních rovnic se mohlo stát, že nemusel vůbec mít řešení. To u našich diferenčních rovnic možné není. Zato ale bývá nesnadné nalézt to jedno potřebné partikulární řešení nehomogenního systému, pokud je chování skalárních koeficientů v rovnici složité. U lineárních rekurencí je to podobné.

Omezíme se tu na jediný případ, kdy příslušný homogenní systém má koeficienty konstantní a $b(n)$ je polynom stupně $s$. Řešení pak lze hledat ve tvaru polynomu

$$x_n = \alpha_0 + \alpha_1 n + \cdots + \alpha_s n^s$$

s neznámými koeficienty $\alpha_i$, $i = 1, \ldots, s$. Dosazením do diferenční rovnice a porovnáním koeficientů u jednotlivých mocnin $n$ dostaneme systém $s + 1$ rovnic pro $s + 1$ proměnných $\alpha_i$. Pokud má tento systém řešení, našli jsme řešení našeho původního problému. Pokud řešení nemá, může stačit zvětšit stupeň $s$ hledaného polynomu.

z kořenů charakteristického polynomu dané rovnice. Charakteristická rovnice je

$$x^4 - x^3 + x^2 - x + 1 = 0.$$

Jedná se o reciprokou rovnici. Zavedeme tedy substituci $u = x + \frac{1}{x}$. Po vydělení rovnice $x^2$ (nula nemůže být kořenem) a substituci (všimněte si, že $x^2 + \frac{1}{x^2} = u^2 - 2$) dostáváme

$$x^2 - x + 1 - \frac{1}{x} + \frac{1}{x^2} = u^2 - u - 1 = 0.$$

Dostáváme tedy neznámé $u_{1,2} = \frac{1\pm\sqrt{5}}{2}$. Odtud pak z rovnice $x^2 - ux + 1 = 0$ určíme čtyři kořeny

$$x_{1,2,3,4} = \frac{1 \pm \sqrt{5} \pm \sqrt{-10 \pm 2\sqrt{5}}}{4}.$$

Nyní si všimněme, že kořeny charakteristické rovnice jsme mohli „uhodnout“ rovnou. Je totiž

$$x^5 + 1 = (x + 1)(x^4 - x^3 + x^2 - x + 1)$$

a tedy jsou kořeny polynomu $x^4 - x^3 + x^2 - x + 1$ i kořeny polynomu $x^5 + 1$, což jsou páté odmocniny z $-1$. Takto dostáváme, že řešením charakteristického polynomu jsou čísla $x_{1,2} = \cos\left(\frac{\pi}{5}\right) \pm i \sin\left(\frac{\pi}{5}\right)$ a $x_{3,4} = \cos\left(\frac{3\pi}{5}\right) \pm i \sin\left(\frac{3\pi}{5}\right)$. Tedy reálnou bází prostoru řešení dané diferenční rovnice je například báze posloupností $\cos\left(\frac{n\pi}{5}\right)$, $\sin\left(\frac{n\pi}{5}\right)$, $\cos\left(\frac{3n\pi}{5}\right)$ a $\sin\left(\frac{3n\pi}{5}\right)$, což jsou siny a kosiny argumentů příslušných mocnin kořenů charakteristického polynomu.

Všimněme si, že jsme mimochodem odvodili algebraické výrazy pro $\cos\left(\frac{\pi}{5}\right) = \frac{1+\sqrt{5}}{4}$, $\sin\left(\frac{\pi}{5}\right) = \frac{\sqrt{10-2\sqrt{5}}}{4}$, $\cos\left(\frac{3\pi}{5}\right) = \frac{\sqrt{5}-1}{4}$ a $\sin\left(\frac{3\pi}{5}\right) = \frac{\sqrt{10+2\sqrt{5}}}{4}$ (vzhledem k tomu, že všechny kořeny rovnice mají absolutní hodnotu 1, tak jsou to reálné, resp. imaginární, části příslušných kořenů). □

**3.11.** Určete explicitní vyjádření posloupnosti vyhovující diferenční rovnici $x_{n+2} = 2x_{n+1} - 2x_n$ se členy $x_1 = 2$, $x_2 = 2$.

**Řešení.** Kořeny charakteristického polynomu $x^2 - 2x + 2$ jsou $1 + i$ a $1 - i$. Báze (komplexního) vektorového prostoru řešení je tedy tvořena posloupnostmi $y_n = (1 + i)^n$ a $z_n = (1 - i)^n$. Hledanou posloupnost můžeme vyjádřit jako lineární kombinaci těchto posloupností (s komplexními koeficienty). Je tedy $x_n = a \cdot y_n + b \cdot z_n$, kde $a = a_1 + ia_2$, $b = b_1 + ib_2$. Z rekurentního vztahu dopočteme $x_0 = \frac{1}{2}(2x_1 - x_2) = 0$ a dosazením $n = 0$ a $n = 1$ do uvažovaného vyjádření $x_n$ dostáváme

$$1 = x_0 = a_1 + ia_2 + b_1 + ib_2,$$
$$2 = x_1 = (a_1 + ia_2)(1 + i) + (b_1 + ib_2)(1 - i),$$

Např. rovnice $x_n - x_{n-2} = 2$ nemůže mít konstantní řešení, ale dosazením $x_n = \alpha_0 + \alpha_1 n$ dostáváme řešení $\alpha_1 = 1$ (a koeficient $\alpha_0$ může být libovolný), a proto je obecné řešení naší rovnice

$$x_n = C_1 + C_2(-1)^n + n.$$

Všimněme si, že skutečně matice příslušného systému rovnic pro polynom nižšího stupně nula je nulová a rovnice $0 \cdot \alpha_0 = 2$ nemá řešení. Další poznámky o vhodných postupech nalézání partikulárních řešení jsou za příkladem ‖3.6‖.

**3.15. Lineární filtry.** Uvažujme nyní nekonečné posloupnosti

$$x = (\dots, x_{-n}, x_{-n+1}, \dots, x_{-1}, x_0, x_1, \dots, x_n, \dots).$$

Budeme, podobně jako u systémů lineárních rovnic, pracovat s operací $T$, která zobrazí celou posloupnost $x$ na posloupnost $z = Tx$ se členy

$$z_n = a_0 x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k}.$$



S posloupnostmi $x$ můžeme opět pracovat jako s vektory vzhledem ke sčítání i násobení skaláry po složkách. Pouze bude tento velký vektorový prostor nekonečněrozměrný. Naše zobrazení $T$ je zjevně lineárním zobrazením na takovém vektorovém prostoru.

Posloupnosti si představme jako diskrétní hodnoty nějakého signálu, odečítané zpravidla ve velmi krátkých časových jednotkách, operace $T$ pak může být filtrem, který signál zpracovává. Bude nás zajímat, jak odhadnout vlastnosti, které takový „filtr“ bude mít.

Signály jsou velice často ze své podstaty dány součtem několika částí, které jsou samy o sobě víceméně periodické. Z naší definice je ale zřejmé, že periodické posloupnosti $x_n$, tj. posloupnosti splňující pro nějaké pevné přirozené číslo $p$

$$x_{n+p} = x_n$$

budou mít i periodické obrazy $z = Tx$

$$z_{n+p} = a_0 x_{n+p} + a_1 x_{n-1+p} + \cdots + a_k x_{n-k+p} =$$
$$= a_0 x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = z_n$$

se stejnou periodou $p$.

Pro pevně zvolenou operaci $T$ nás bude zajímat, které vstupní periodické posloupnosti zůstanou přibližně stejné (případně až na násobek) a které budou utlumeny na nulové hodnoty.

Ve druhém případě tedy hledáme jádro našeho lineárního zobrazení $T$. To je ale dáno právě homogenní diferenční rovnicí

$$a_0 x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = 0, \quad a_0 \neq 0, \quad a_k \neq 0,$$

kterou jsme se už naučili řešit.

**3.16. Špatný ekvalizér.** Jako příklad uvažujme velmi jednoduchý lineární filtr zadaný rovnicí

$$z_n = (Tx)_n = x_{n+2} + x_n.$$



Výsledky takového zpracování signálu jsou naznačeny na následujících čtyřech obrázcích pro postupně se zvyšující frekvenci periodického signálu $x_n = \cos(\varphi n)$. Signály se stejnou amplitudou na všech obrázcích jsou původní signály, další jsou výsledky po zpracování filtrem. Nerovnoměrnosti křivek jsou důsledkem nepřesného kreslení, všechny signály jsou samozřejmě rovnoměrnými sinusovkami.

a porovnáním reálné a komplexní složky obou rovnic dostáváme lineární soustavu čtyř rovnic o čtyřech neznámých

$$\begin{array}{rcrcrcl} a_1 & & + & b_1 & & = & 1,\\ & a_2 & & & + \; b_2 & = & 0,\\ a_1 & - \; a_2 & + & b_1 & + \; b_2 & = & 2,\\ a_1 & + \; a_2 & - & b_1 & + \; b_2 & = & 0 \end{array}$$

s řešením $a_1 = b_1 = b_2 = \frac{1}{2}$ a $a_2 = -1/2$. Celkem můžeme hledanou posloupnost vyjádřit jako

$$x_n = \left(\frac{1}{2} - \frac{1}{2}i\right)(1+i)^n + \left(\frac{1}{2} + \frac{1}{2}i\right)(1-i)^n.$$

Posloupnost můžeme však vyjádřit i pomocí reálné báze (komplexního) vektorového prostoru řešení, totiž posloupností $u_n = \frac{1}{2}(y_n + z_n) = \left(\sqrt{2}\right)^n \cos\left(\frac{n\pi}{4}\right)$ a $v_n = \frac{1}{2}i(z_n - y_n) = \left(\sqrt{2}\right)^n \sin\left(\frac{n\pi}{4}\right)$. Matice přechodu od komplexní báze k reálné je

$$T := \begin{pmatrix} \frac{1}{2} & -\frac{1}{2}i \\ \frac{1}{2} & \frac{1}{2}i \end{pmatrix},$$

inverzní matice je $T^{-1} = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$. Pro vyjádření posloupnosti $x_n$ pomocí reálné báze, tj. souřadnice $(c, d)$ posloupnosti $x_n$ v bázi $\{u_n, v_n\}$, pak máme

$$\begin{pmatrix} c \\ d \end{pmatrix} = T^{-1} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Máme tedy alternativní vyjádření posloupnosti $x_n$, ve kterém se nevyskytují komplexní čísla (ale zase jsou v něm odmocniny):

$$x_n = \left(\sqrt{2}\right)^n \cos\left(\frac{n\pi}{4}\right) + \left(\sqrt{2}\right)^n \sin\left(\frac{n\pi}{4}\right),$$

které jsme samozřejmě mohli získat též řešením dvou lineárních rovnic o dvou neznámých $c$, $d$, totiž $1 = x_0 = c \cdot u_0 + d \cdot v_0 = c$ a $2 = x_1 = c \cdot u_1 + d \cdot v_1 = c + d$. □

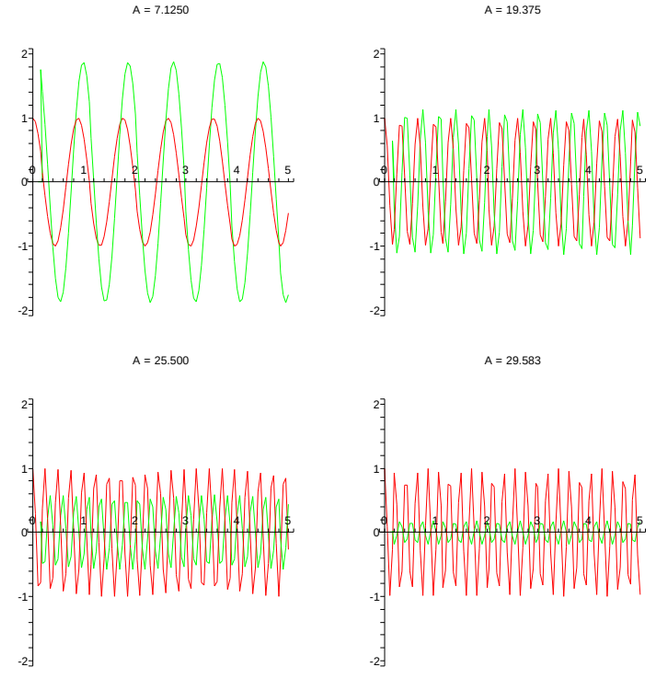
*3.12.* Dokažte, že každý člen posloupnosti zadané rekurentním vztahem

$$x_n = 2x_{n-1} + 8x_{n-2} - 9, \quad n \geq 2,$$

se členy $x_1 = 1, x_2 = 25$, je druhou mocninou přirozeného čísla. ◯

## C. Populační modely

Populační modely, kterými se budeme zabývat, budou rekurentní vztahy ve vektorových prostorech. Neznámou veličinou tedy nebude posloupnost čísel nýbrž posloupnost vektorů. Roli koeficientů pak budou hrát matice. Začneme s jednoduchým (dvourozměrným) příkladem.




Všimněme si, že v oblastech, kde je výsledný signál přibližně stejně silný jako původní, dochází k dramatickému posuvu fáze signálu. Levné ekvalizéry skutečně podobně špatně fungují.

### 3. Iterované lineární procesy

**3.17. Iterované procesy.** V praktických modelech se často setkáváme se situací, kdy je vývoj systému v jednom časovém období dán lineárním procesem, zajímáme se ale o chování systému po mnoha iteracích. Často přitom samotný lineární proces zůstává pořád stejný, z pohledu našeho matematického modelu tedy nejde o nic jiného než opakované násobení stavového vektoru stále stejnou maticí.



Zatímco pro řešení systémů lineárních rovnic jsme potřebovali jen minimum znalostí o vlastnostech lineárních zobrazení, k pochopení chování iterovaného systému budeme účelně používat znalosti vlastních čísel, vlastností vlastních vektorů a další strukturní výsledky.

V jistém smyslu se pohybujeme v podobném prostředí jako u lineárních rekurencí a skutečně můžeme náš popis filtrů v minulých odstavcích takto také popsat. Představme si, že pracujeme se zvukem a uchováváme si stavový vektor

$$Y_n = (x_n, \ldots, x_{n-k+1})$$

všech hodnot od aktuální až po poslední, kterou ještě v našem lineárních filtru zpracováváme. V jednom časovém intervalu (ve vzorkovací frekvenci audio signálu mimořádně krátkém) pak přejdeme ke stavovému vektoru

$$Y_{n+1} = (x_{n+1}, x_n, \ldots, x_{n-k+2}),$$

kde první hodnota $x_{n+1} = a_1 x_n + \cdots + a_k x_{n-k+1}$ je spočtena jako u homogenních diferenčních rovnic, ostatní si jen posunujeme o jednu pozici a poslední zapomeneme. Příslušná čtvercová matice

**3.13. Spoření.** S kamarádem spoříme na společnou dovolenou následujícím způsobem. Na začátku dám 10 EUR a on 20 EUR. Každý další měsíc pak dá každý z nás tolik, co minulý měsíc plus polovinu toho, co dal ten druhý z nás předchozí měsíc. Kolik budeme mít za rok dohromady naspořeno? Kolik peněz budu platit dvanáctý měsíc?

**Řešení.** Obnos peněz, který budu platit $n$-tý měsíc já označím $x_n$ a to, co bude platit kamarád označím $y_n$. První měsíc tedy dáme $x_1 = 10, y_1 = 20$. Pro další platby můžeme psát rekurentní rovnice:

$$x_{n+1} = x_n + \frac{1}{2}y_n, \quad y_{n+1} = y_n + \frac{1}{2}x_n.$$

Pokud označíme společný vklad $z_n = x_n + y_n$, pak sečtením uvedených rovnic dostaneme vztah $z_{n+1} = z_n + \frac{1}{2}z_n = \frac{3}{2}z_n$. To je geometrická řada a dostáváme tedy $z_n = 30 \cdot \left(\frac{3}{2}\right)^{n-1}$. Za rok budeme mít celkem naspořeno $z_1 + z_2 + \cdots + z_{12}$. Tento částečný součet umíme lehce spočítat

$$z_1\left[1 + \frac{3}{2} + \cdots + \left(\frac{3}{2}\right)^{11}\right] = 30\frac{(\frac{3}{2})^{12} - 1}{\frac{3}{2} - 1} \doteq 7725.$$

Za rok tedy dohromady naspoříme více než 7724 euro.

Rekurentní soustavu rovnic popisující systém spoření můžeme napsat pomocí matice následovně

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}.$$

Jde tedy opět o geometrickou řadu. Jejími prvky jsou teď ovšem vektory a kvocient není skalár, ale matice. Řešení lze nicméně najít obdobně

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}^{n-1} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}.$$

Mocninu matice působící na vektor $(x_1, y_1)$ můžeme nalézt, když vyjádříme tento vektor v bázi vlastních vektorů. Charakteristický polynom matice je $(1 - \lambda)^2 - \frac{1}{4}$ a vlastní čísla jsou tedy $\lambda_{1,2} = \frac{3}{2}, \frac{1}{2}$. Příslušné vlastní vektory jsou po řadě $(1, 1)$ a $(1, -1)$. Pro počáteční vektor $(x_1, y_1) = (10, 20)$ spočítáme

$$\begin{pmatrix} 10 \\ 20 \end{pmatrix} = 15\begin{pmatrix} 1 \\ 1 \end{pmatrix} - 5\begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

a proto

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = 15\left(\frac{3}{2}\right)^{n-1}\begin{pmatrix} 1 \\ 1 \end{pmatrix} - 5\left(\frac{1}{2}\right)^{n-1}\begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

To znamená, že já zaplatím 12. měsíc

$$x_{12} = 15\left(\frac{3}{2}\right)^{11} - 5\left(\frac{1}{2}\right)^{11} \doteq 1297$$

euro a můj kamarád v podstatě stejně. □

**Poznámka.** Předchozí příklad lze řešit i bez matice následujícím přepsáním rekurentní rovnice: $x_{n+1} = x_n + \frac{1}{2}y_n = \frac{1}{2}x_n + \frac{1}{2}z_n$.

řádu $k$ splňující $Y_{n+1} = A \cdot Y_n$ bude vypadat takto:

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Pro takovou jednoduchou matici jsme si odvodili explicitní postup pro úplné řešení otázky, jak vypadá formule pro řešení. Obecně to tak snadno nepůjde ani pro velice podobné systémy. Jedním z typických případů je studium dynamiky populací v různých biologických systémech.

Všimněme si také, že vcelku pochopitelně má matice $A$ za charakteristický polynom právě

$$p(\lambda) = \lambda^k - a_1\lambda^{k-1} - \cdots - a_k,$$

jak snadno dovodíme pomocí rozvoje podle posledního sloupce a rekurencí. To je vysvětlitelné i přímo, protože řešení $x_n = \lambda^n$, $\lambda \neq 0$, vlastně znamená, že matice $A$ vynásobením převede vlastní vektor $(\lambda^k, \dots, \lambda)^T$ na jeho $\lambda$–násobek. Musí být tedy takové $\lambda$ vlastním číslem matice $A$.

**3.18. Leslieho model růstu populací.** Představme si, že zkoumáme nějaký systém jednotlivců (pěstovaná zvířata, hmyz, buněčné kultury apod.) rozdělený do $m$ skupin, třeba podle stáří, fází vývoje hmyzu, apod. Stav $X_n$ je tedy dán vektorem



$$X_n = (u_1, \dots, u_m)^T$$

závisejícím na okamžiku $t_n$, ve kterém systém pozorujeme. Lineární model vývoje takového systému je dán maticí $A$ dimenze $n$, která zadává změnu vektoru $X_n$ na

$$X_{n+1} = A \cdot X_n$$

při přírůstku času z $t_n$ na $t_{n+1}$.

Uvažujme jako příklad tzv. *Leslieho model růstu*, ve kterém vystupuje matice

$$A = \begin{pmatrix} f_1 & f_2 & f_3 & \dots & f_{m-1} & f_m \\ \tau_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \tau_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & \tau_3 & \ddots & 0 & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \tau_{m-1} & 0 \end{pmatrix},$$

jejíž parametry jsou svázány s vývojem populace rozdělené do $m$ věkových skupin tak, že $f_i$ označuje relativní plodnost příslušné věkové skupiny (ve sledovaném časovém skoku vznikne z $N$ jedinců v $i$–té skupině $f_i N$ jedinců nových, tj. ve skupině první), zatímco $\tau_i$ je relativní úmrtnost $i$-té skupiny během jednoho období. Pochopitelně lze použít takový model s libovolným počtem věkových skupin.

Všechny koeficienty jsou tedy nezáporná reálná čísla a čísla $\tau_i$ jsou mezi nulou a jedničkou. Všimněme si, že pokud jsou všechna $\tau_i$ rovna jedné, jde vlastně o lineární rekurenci s konstantními koeficienty, a tedy buď exponenciálním růstem/poklesem (pro reálné kořeny $\lambda$ charakteristického polynomu) nebo oscilováním spojeným s případným růstem či poklesem (pro komplexní kořeny).

Předcházející příklad byl vlastně modelem růstu (v daném případě růstu množství naspořených peněz). Nyní přejděme k modelům růstu popisujícím primárně růst nějaké populace. Leslieho model růstu, který jsme detailně rozebrali v teorii, velmi dobře popisuje nejen populace ovcí (podle kterých byl sestaven), ale uplatňuje se například i při modelování následujících populací:

**3.14. Zajíci podruhé.** Ukažme si, jak můžeme Leslieho modelem popsat populaci zajíců na louce, kterou jsme se zaobírali v příkladu (‖3.5‖). Uvažujme, že zajíci umírají po dovršení devátého měsíce věku (v původním modelu byl věk zajíců neomezen). Označme počty zajíců (resp. zaječic) podle stáří v měsících v čase $t$ (měsíců) jako $x_1(t), x_2(t), \ldots, x_9(t)$, tak počty zajíců v jednotlivých věkových skupinách budou po jednom měsíci $x_1(t+1) = x_2(t)+x_3(t)+\cdots+x_9(t)$, $x_i(t+1) = x_{i-1}(t)$, pro $i = 2, 3, \ldots, 10$, neboli

$$\begin{pmatrix} x_1(t+1)\\ x_2(t+1)\\ x_3(t+1)\\ x_4(t+1)\\ x_5(t+1)\\ x_6(t+1)\\ x_7(t+1)\\ x_8(t+1)\\ x_9(t+1) \end{pmatrix} = \begin{pmatrix} 0&1&1&1&1&1&1&1&1\\ 1&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0\\ 0&0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1&0 \end{pmatrix} \begin{pmatrix} x_1(t)\\ x_2(t)\\ x_3(t)\\ x_4(t)\\ x_5(t)\\ x_6(t)\\ x_7(t)\\ x_8(t)\\ x_9(t) \end{pmatrix}.$$

Charakteristický polynom uvedené matice je

$$\lambda^9 - \lambda^7 - \lambda^6 - \lambda^5 - \lambda^4 - \lambda^3 - \lambda^2 - \lambda - 1.$$

Kořeny této rovnice nejsme schopni explicitně vyjádřit, jeden z nich však velmi dobře odhadnout, $\lambda_1 \doteq 1,608$ (proč musí být menší než $(\sqrt{5}+1)/2$)?). Populace bude tedy podle tohoto modelu růst přibližně s geometrickou řadou s kvocientem $1,608^t$.

Obecněji můžeme zpracovat předcházející model takto:

**3.15.** Nechť je v populačním modelu dravec-kořist určen vztah mezi počtem dravců $D_k$ a kořisti $K_k$ v daném a následujícím měsíci ($k \in \mathbb{N} \cup \{0\}$) lineárním systémem

(a)
$$\begin{aligned} D_{k+1} &= 0,6\,D_k + 0,5\,K_k,\\ K_{k+1} &= -0,16\,D_k + 1,2\,K_k; \end{aligned}$$

(b)
$$\begin{aligned} D_{k+1} &= 0,6\,D_k + 0,5\,K_k,\\ K_{k+1} &= -0,175\,D_k + 1,2\,K_k; \end{aligned}$$

(c)
$$\begin{aligned} D_{k+1} &= 0,6\,D_k + 0,5\,K_k,\\ K_{k+1} &= -0,135\,D_k + 1,2\,K_k. \end{aligned}$$

Analyzujte chování tohoto modelu po velmi dlouhé době.

**Řešení.** Všimněme si, že jednotlivé varianty se od sebe navzájem liší pouze v hodnotě koeficientu u $D_k$ ve druhé rovnici. Můžeme proto

Než se pustíme do obecnější teorie, trochu si pohrajeme s tímto konkrétním modelem.

Přímým výpočtem pomocí Laplaceova rozvoje podle posledního sloupce spočteme charakteristický polynom $p_m(\lambda)$ matice $A$ pro model s $m$ skupinami:

$$p_m(\lambda) = |A - \lambda E| = -\lambda p_{m-1}(\lambda) + (-1)^{m-1} f_m \tau_1 \ldots \tau_{m-1}.$$

Vcelku snadno dovodíme indukcí, že tento charakteristický polynom má tvar

$$p_m(\lambda) = (-1)^m(\lambda^m - a_1\lambda^{m-1} - \cdots - a_{m-1}\lambda - a_m)$$

s vesměs nezápornými koeficienty $a_1, \ldots, a_m$, pokud jsou všechny parametry $\tau_i$ a $f_i$ kladné. Např. je vždy

$$a_m = f_m \tau_1 \ldots \tau_{m-1}.$$



Zkusme kvalitativně odhadnout rozložení kořenů polynomu $p_m$. Bohužel, detaily budeme umět přesně vysvětlit a ověřit až po absolvování příslušných partií tzv. matematické analýzy v kapitole páté a později, přesto by ale postup měl být intuitivně jasný. Vyjádříme si charakteristický polynom ve tvaru

$$p_m(\lambda) = \pm\lambda^m\big(1 - q(\lambda)\big),$$

kde $q(\lambda) = a_1\lambda^{-1} + \cdots + a_m\lambda^{-m}$ je ostře klesající a nezáporná funkce pro $\lambda > 0$. Evidentně bude proto existovat právě jedno kladné $\lambda$, pro které bude $q(\lambda) = 1$ a tedy také $p_m(\lambda) = 0$. Jinými slovy, pro každou Leslieho matici existuje právě jedno kladné reálné vlastní číslo.

Pro skutečné Leslieho modely populací bývají všechny koeficienty $\tau_i$ i $f_j$ mezi nulou a jedničkou a typicky nastává situace, kdy jediné reálné vlastní číslo $\lambda_1$ je větší nebo rovno jedné, zatímco absolutní hodnoty ostatních vlastních čísel jsou ostře menší než jedna.

Jestliže začneme s libovolným stavovým vektorem $X$, který bude dán jako součet vlastních vektorů

$$X = X_1 + \cdots + X_m$$

s vlastními hodnotami $\lambda_i$, pak při iteracích dostáváme

$$A^k \cdot X = \lambda_1^k X_1 + \ldots \lambda_m^k X_m,$$

takže za předpokladu, že $|\lambda_i| < 1$ pro všechna $i \geq 2$, budou všechny komponenty ve vlastních podprostorech velmi rychle mizet, kromě komponenty $\lambda_1 X_1^k$.

Rozložení populace do věkových skupin se tak budou rychle blížit poměrům komponent vlastního vektoru k dominantnímu vlastnímu číslu $\lambda_1$.

Například pro matici (uvědomme si význam jednotlivých koeficientů, jsou převzaty z modelu pro chov ovcí, tj. hodnoty $\tau$ zahrnují jak přirozený úhyn tak případné aktivity chovatelů na jatkách)

$$A = \begin{pmatrix} 0 & 0,2 & 0,8 & 0,6 & 0\\ 0,95 & 0 & 0 & 0 & 0\\ 0 & 0,8 & 0 & 0 & 0\\ 0 & 0 & 0,7 & 0 & 0\\ 0 & 0 & 0 & 0,6 & 0 \end{pmatrix}$$

vyjdou vlastní hodnoty přibližně

$$1,03;\ 0;\ -0,5;\ -0,27 + 0,74i;\ -0,27 - 0,74i$$

všechny tři případy vyjádřit jako

$$\begin{pmatrix} D_k \\ K_k \end{pmatrix} = \begin{pmatrix} 0{,}6 & 0{,}5 \\ -a & 1{,}2 \end{pmatrix} \cdot \begin{pmatrix} D_{k-1} \\ K_{k-1} \end{pmatrix}, \quad k \in \mathbb{N},$$

kde budeme postupně klást $a = 0{,}16, a = 0{,}175, a = 0{,}135$. Hodnota koeficientu $a$ zde reprezentuje průměrný počet kusů kořisti zahubených jedním (očividně „nenáročným“) dravcem za měsíc. Při označení

$$T = \begin{pmatrix} 0{,}6 & 0{,}5 \\ -a & 1{,}2 \end{pmatrix}$$

bezprostředně dostáváme

$$\begin{pmatrix} D_k \\ K_k \end{pmatrix} = T^k \cdot \begin{pmatrix} D_0 \\ K_0 \end{pmatrix}, \quad k \in \mathbb{N}.$$

Pomocí mocnin matice $T$ tak můžeme určit vývoj populací dravce a kořisti po velmi dlouhé době.

Snadno stanovíme vlastní čísla

(a) $\lambda_1 = 1, \quad \lambda_2 = 0{,}8;$
(b) $\lambda_1 = 0{,}95, \quad \lambda_2 = 0{,}85;$
(c) $\lambda_1 = 1{,}05, \quad \lambda_2 = 0{,}75$

matice $T$ a jim (při zachování pořadí) příslušné vlastní vektory

(a) $(5,4)^T, \quad (5,2)^T;$
(b) $(10,7)^T, \quad (2,1)^T;$
(c) $(10,9)^T, \quad (10,3)^T.$

Víme, že matice $T$ má v bázi dané vlastními vektory diagonální tvar s vlastními čísly na diagonále. Vlastní vektory zapsané do sloupců pak zadávají matici přechodu od standardní báze k bázi tvořené vlastními vektory. Je tedy

$$T = \begin{pmatrix} 5 & 5 \\ 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0{,}8 \end{pmatrix} \cdot \begin{pmatrix} 5 & 5 \\ 4 & 2 \end{pmatrix}^{-1}$$

a pro $k \in \mathbb{N}$ tudíž platí

(a)

$$T^k = \begin{pmatrix} 5 & 5 \\ 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0{,}8 \end{pmatrix}^k \cdot \begin{pmatrix} 5 & 5 \\ 4 & 2 \end{pmatrix}^{-1};$$

(b)

$$T^k = \begin{pmatrix} 10 & 2 \\ 7 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0{,}95 & 0 \\ 0 & 0{,}85 \end{pmatrix}^k \cdot \begin{pmatrix} 10 & 2 \\ 7 & 1 \end{pmatrix}^{-1};$$

(c)

$$T^k = \begin{pmatrix} 10 & 10 \\ 9 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1{,}05 & 0 \\ 0 & 0{,}75 \end{pmatrix}^k \cdot \begin{pmatrix} 10 & 10 \\ 9 & 3 \end{pmatrix}^{-1}.$$

Odtud dále pro velká $k \in \mathbb{N}$ plyne

s velikostmi 1,03; 0; 0,5; 0,78; 0,78 a vlastní vektor příslušný dominantnímu vlastnímu číslu je přibližně

$$X^T = (30\ 27\ 21\ 14\ 8).$$

Zvolili jsme rovnou jediný vlastní vektor se součtem souřadnic rovným stu, zadává nám proto přímo výsledné procentní rozložení populace.

Pokud bychom chtěli místo tříprocentního celkového růstu populace setrvalý stav a předsevzali si ujídat více ovce třeba z druhé věkové skupiny, řešili bychom úlohu, o kolik máme zmenšit $\tau_2$, aby bylo dominantní vlastní číslo rovno jedné.

**3.19. Matice s nezápornými prvky.** Reálné matice, které nemají žádné záporné prvky mají velmi speciální vlastnosti. Zároveň jsou skutečně časté v praktických modelech. Naznačíme proto teď proto tzv. *Perronovu-Frobeniovu teorii*, která se právě takovým maticím věnuje.



Začneme definicí několika pojmů, abychom mohli naše úvahy vůbec formulovat.

KLADNÉ A PRIMITIVNÍ MATICE

**Definice.** Za *kladnou matici* budeme považovat takovou čtvercovou matici $A$, jejíž všechny prvky $a_{ij}$ jsou reálné a kladné. *Primitivní matice* je pak taková čtvercová matice $A$, jejíž nějaká mocnina $A^k$ je kladná.

Připomeňme, že *spektrálním poloměrem matice A* nazýváme maximum absolutních hodnot všech jejích (reálných i komplexních) vlastních čísel. Spektrálním poloměrem lineárního zobrazení na (konečněrozměrném) vektorovém prostoru rozumíme spektrální poloměr jeho matice v některé bázi. *Normou* matice $A \in \mathbb{R}^{n^2}$ nebo vektoru $x \in \mathbb{R}^n$ rozumíme součet absolutních hodnot všech jejich prvků. U vektorů $x$ píšeme pro jejich normu $|x|$.

Následující výsledek je mimořádně užitečný a snad i dobře srozumitelný. Jeho důkaz se svou náročností dosti vymyká této učebnici, uvádíme ale alespoň jeho stručný nástin. Pokud by čtenář měl problém s plynulým čtením nástinu důkazu, doporučujeme jej přeskočit.

**Věta** (Perronova)**.** *Jestliže je $A$ primitivní matice se spektrálním poloměrem $\lambda \in \mathbb{R}$, pak je $\lambda$ jednoduchým kořenem charakteristického polynomu matice $A$, který je ostře větší než absolutní hodnota kteréhokoliv jiného vlastního čísla matice $A$. K vlastnímu číslu $\lambda$ navíc existuje vlastní vektor $x$ s výhradně kladnými prvky $x_i$.*

DŮKAZ. [1] V důkazu se budeme opírat o intuici elementární geometrie. Částečně budeme použité koncepty upřesňovat už v analytické geometrii ve čtvrté kapitole, některé analytické aspekty budeme studovat podrobněji v kapitolách páté a později, přesné důkazy některých analytických kroků v této učebnici nepodáme vůbec. Snad budou následující úvahy nejen osvětlovat dokazovaný teorém, ale budou také samy o sobě motivací pro naše další studium geometrie i matematické analýzy. Začneme docela srozumitelně znějícím pomocným lemmatem:



[1] inspirováno materiálem na webu, viz http://www-users.math.umd.edu/~mmb/475/spec.pdf

(a)

$$T^k \approx \begin{pmatrix} 5 & 5 \\ 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 5 & 5 \\ 4 & 2 \end{pmatrix}^{-1} = \\ = \frac{1}{10} \begin{pmatrix} -10 & 25 \\ -8 & 20 \end{pmatrix};$$

(b)

$$T^k \approx \begin{pmatrix} 10 & 2 \\ 7 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 10 & 2 \\ 7 & 1 \end{pmatrix}^{-1} = \\ = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix};$$

(c)

$$T^k \approx \begin{pmatrix} 10 & 10 \\ 9 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1{,}05^k & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 10 & 10 \\ 9 & 3 \end{pmatrix}^{-1} = \\ = \frac{1{,}05^k}{60} \begin{pmatrix} -30 & 100 \\ -27 & 90 \end{pmatrix},$$

neboť právě pro velká $k \in \mathbb{N}$ můžeme položit

(a)

$$\begin{pmatrix} 1 & 0 \\ 0 & 0{,}8 \end{pmatrix}^k \approx \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};$$

(b)

$$\begin{pmatrix} 0{,}95 & 0 \\ 0 & 0{,}85 \end{pmatrix}^k \approx \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix};$$

(c)

$$\begin{pmatrix} 1{,}05 & 0 \\ 0 & 0{,}75 \end{pmatrix}^k \approx \begin{pmatrix} 1{,}05^k & 0 \\ 0 & 0 \end{pmatrix}.$$

Podotkněme, že ve variantě (b), tj. pro $a = 0{,}175$, nebylo nutné vlastní vektory počítat.

Obdrželi jsme tak

(a)

$$\begin{pmatrix} D_k \\ K_k \end{pmatrix} \approx \frac{1}{10} \begin{pmatrix} -10 & 25 \\ -8 & 20 \end{pmatrix} \cdot \begin{pmatrix} D_0 \\ K_0 \end{pmatrix} = \\ = \frac{1}{10} \begin{pmatrix} 5\,(-2D_0 + 5K_0) \\ 4\,(-2D_0 + 5K_0) \end{pmatrix};$$

(b)

$$\begin{pmatrix} D_k \\ K_k \end{pmatrix} \approx \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} D_0 \\ K_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix};$$

(c)

$$\begin{pmatrix} D_k \\ K_k \end{pmatrix} \approx \frac{1{,}05^k}{60} \begin{pmatrix} -30 & 100 \\ -27 & 90 \end{pmatrix} \cdot \begin{pmatrix} D_0 \\ K_0 \end{pmatrix} = \\ = \frac{1{,}05^k}{60} \begin{pmatrix} 10\,(-3D_0 + 10K_0) \\ 9\,(-3D_0 + 10K_0) \end{pmatrix}.$$

Tyto výsledky lze interpretovat následovně:

(a) Pokud $2D_0 < 5K_0$, velikosti obou populací se ustálí na nenulových hodnotách (říkáme, že jsou stabilní). Jestliže $2\,D_0 \geq 5\,K_0$, obě populace vymřou.

**Lemma.** *Uvažme libovolný mnohostěn $P$ obsahující počátek $0 \in \mathbb{R}^n$.*

*Jestliže nějaká iterace lineárního zobrazení $\psi : \mathbb{R}^n \to \mathbb{R}^n$ zobrazuje $P$ do jeho vnitřku, pak je spektrální poloměr zobrazení $\psi$ ostře menší než jedna.*

Uvažme matici $A$ zobrazení $\psi$ ve standardní bázi. Protože vlastní čísla $A^k$ jsou $k$–té mocniny vlastních čísel matice $A$, můžeme rovnou bez újmy na obecnosti předpokládat, že samotné zobrazení $\psi$ již zobrazuje $P$ do vnitřku $P$. Zjevně tedy nemůže mít $\psi$ Žádnou vlastní hodnotu s absolutní hodnotou větší než jedna.

Důkaz dále povedeme sporem. Předpokládejme, že existuje vlastní hodnota $\lambda$ s $|\lambda| = 1$. Máme tedy dvě možnosti. Buď je $\lambda^k = 1$ pro vhodné $k$ nebo takové $k$ neexistuje.

Obrazem $P$ je uzavřená množina (to znamená, že pokud se body v obrazu budou hromadit k nějakému bodu $y$ v $\mathbb{R}^n$, bude $y$ opět v obrazu) a hranici $P$ tento obraz vůbec neprotíná. Nemůže tedy mít $\psi$ pevný bod na hranici $P$ ani nemůže existovat žádný bod na hranici, ke kterému by se mohly libovolně blížit body v obrazu. První argument vylučuje, že by nějaká mocnina $\lambda$ byla jedničkou, protože to by takový pevný bod na hranici $P$ jistě existoval. Ve zbývajícím případě jistě existuje dvourozměrný podprostor $W \subseteq \mathbb{R}^n$, na nějž se $\psi$ zužuje coby rotace o iracionální argument a jistě existuje bod $y$ v průniku $W$ s hranicí $P$. Pak by ale byl bod $y$ libovolně přesně přiblížen body z množiny $\psi^n(y)$ při průchodu přes všechny iterace, a tedy by musel sám být také v obrazu. Došli jsme tedy ke sporu a lemma je ověřeno.

Nyní se dáme do důkazu Perronovy věty. Naším prvním krokem bude ověření existence vlastního vektoru, který má všechny prvky kladné. Uvažme za tím účelem tzv. standardní simplex

$$S = \{x = (x_1, \ldots, x_n)^T;\ |x| = 1, x_i \geq 0, i = 1, \ldots, n\}.$$

Protože všechny prvky v matici $A$ jsou nezáporné, obraz $A{\cdot}x$ bude mít samé nezáporné souřadnice stejně jako $x$ a alespoň jedna z nich bude vždy nenulová. Zobrazení $x \mapsto |A \cdot x|^{-1}(A \cdot x)$ proto zobrazuje $S$ do sebe, Toto zobrazení $S \to S$ splňuje všechny předpoklady tzv. Brouwerovy věty o pevném bodě a proto existuje vektor $y \in S$ takový, že je tímto zobrazením zobrazen sám na sebe. Důkaz Brouwerovy věty v této učebnici nepodáváme, zájemci snadno najdou odkazy na wikipedii. To ale znamená, že

$$A \cdot y = \lambda\, y, \quad \lambda = |A \cdot y|$$

a našli jsme vlastní vektor, který leží v $S$. Protože ale má nějaká mocnina $A^k$ podle našeho předpokladu samé kladné prvky a samozřejmě je také $A^k \cdot y = \lambda^k y$, všechny souřadnice vektoru $y$ jsou ostře kladné (tj. leží ve vnitřku $S$) a $\lambda > 0$.

Abychom dokázali zbytek věty, budeme uvažovat zobrazení zadané maticí $A$ ve výhodnější bázi a navíc ho vynásobíme konstantou $\lambda^{-1}$:

$$B = \lambda^{-1}(Y^{-1} \cdot A \cdot Y),$$

kde $Y$ je diagonální matice se souřadnicemi $y_i$ právě nalezeného vlastního vektoru $y$ na diagonále. Evidentně je $B$ také primitivní matice a navíc je vektor $z = (1, \ldots, 1)^T$ jejím vlastním vektorem, protože zjevně $Y \cdot z = y$.

Jestliže nyní dokážeme, že $\mu = 1$ je jednoduchým kořenem charakteristického polynomu matice $B$ a všechny ostatní kořeny mají absolutní hodnotu ostře menší než jedna, bude Perronova věta dokázána.

(b) Obě populace vymřou.

(c) Pro $3D_0 < 10K_0$ nastává populační exploze obou druhů. Pro $3D_0 \geq 10K_0$ obě populace vymřou.

To, že extrémně malá změna velikosti $a$ může vést ke zcela odlišnému výsledku, je zapříčiněno neměnností hodnoty $a$ v závislosti na velikosti obou populací. Poznamenejme, že toto omezení, kdy $a$ v našich modelech považujeme za konstantní, nemá oporu ve skutečnosti. Přesto získáváme odhad velikosti $a$ pro stabilní populace. □

V lineárních modelech hrají významnou roli tzv. primitivní matice (viz 3.19).

**3.16.** Které z matic

$$A = \begin{pmatrix} 0 & 1/7 \\ 1 & 6/7 \end{pmatrix}, \quad B = \begin{pmatrix} 1/2 & 0 & 1/3 \\ 0 & 1 & 1/2 \\ 1/2 & 0 & 1/6 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 0 \\ 1/4 & 0 & 1/2 \\ 3/4 & 0 & 1/2 \end{pmatrix},$$

$$D = \begin{pmatrix} 1/3 & 1/2 & 0 & 0 \\ 1/2 & 1/3 & 0 & 0 \\ 0 & 1/6 & 1/6 & 1/3 \\ 1/6 & 0 & 5/6 & 2/3 \end{pmatrix}, \quad E = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

jsou primitivní?

**Řešení.** Neboť

$$A^2 = \begin{pmatrix} 1/7 & 6/49 \\ 6/7 & 43/49 \end{pmatrix}, \quad C^3 = \begin{pmatrix} 3/8 & 1/4 & 1/4 \\ 1/4 & 3/8 & 1/4 \\ 3/8 & 3/8 & 1/2 \end{pmatrix},$$

matice $A$ a $C$ jsou primitivní. Dále platí rovnost

$$\begin{pmatrix} 1/2 & 0 & 1/3 \\ 0 & 1 & 1/2 \\ 1/2 & 0 & 1/6 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

a tak bude prostřední sloupec matice $B^n$ vždy (pro libovolné $n \in \mathbb{N}$) vektorem $(0, 1, 0)^T$, tj. matice $B$ nemůže být primitivní. Součin

$$\begin{pmatrix} 1/3 & 1/2 & 0 & 0 \\ 1/2 & 1/3 & 0 & 0 \\ 0 & 1/6 & 1/6 & 1/3 \\ 1/6 & 0 & 5/6 & 2/3 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ a/6 + b/3 \\ 5a/6 + 2b/3 \end{pmatrix}, \quad a, b \in \mathbb{R}$$

implikuje, že matice $D^2$ bude mít v pravém horním rohu nulovou dvourozměrnou (čtvercovou) submatici. Opakováním této implikace dostáváme, že stejnou vlastnost mají matice $D^3 = D \cdot D^2$, $D^4 = D \cdot D^3$, $\ldots$, $D^n = D \cdot D^{n-1}$, $\ldots$, tudíž matice $D$ není primitivní. Matice $E$ je permutační (v každém řádku a sloupci má právě jeden nenulový prvek, a to 1). Není obtížné si uvědomit, že mocniny permutační matice jsou opět permutační matice. Matice $E$ proto také není primitivní. To lze rovněž ověřit výpočtem mocnin $E^2$, $E^3$, $E^4$. Matice $E^4$ je totiž jednotková. □

Nyní uveďme poněkud obsáhlejší model.

K tomu se nám teď bude hodit dříve dokázané pomocné lemma. Uvažujme matici $B$ jako matici lineárního zobrazení, které zobrazuje řádkové vektory

$$u = (u_1, \ldots, u_n) \mapsto u \cdot B = v,$$

tj. pomocí násobení zprava. Díky tomu, že je $z = (1, \ldots, 1)^T$ vlastním vektorem matice $B$, je součet souřadnic řádkového vektoru $v$ roven

$$\sum_{i,j=1}^{n} u_i b_{ij} = \sum_{i=1}^{n} u_i = 1,$$

kdykoliv je $u \in S$. Proto toto zobrazení zobrazuje simplex $S$ na sebe a má také jistě v $S$ vlastní (řádkový) vektor $w$ s vlastní hodnotou jedna (pevný bod, opět dle Brouwerovy věty). Protože nějaká mocnina $B^k$ obsahuje samé ostře pozitivní prvky, je nutně obraz simplexu $S$ v $k$–té iteraci zobrazení daného $B$ uvnitř $S$. To už jsme blízko použití našeho lemmatu, které jsme si pro důkaz připravili.

Budeme i nadále pracovat s řádkovými vektory a označme si $P$ posunutí simplexu $S$ do počátku pomocí vlastního vektoru $w$, který jsme právě našli, tj. $P = -w + S$. Evidentně je $P$ mnohostěn obsahující počátek a vektorový podprostor $V \subseteq \mathbb{R}^n$ generovaný $P$ je invariantní vůči působení matice $B$ pomocí násobení řádkových vektorů zprava. Zúžení našeho zobrazení na $P$ tedy splňuje předpoklady pomocného lemmatu, a proto nutně musí být všechny jeho vlastní hodnoty v absolutní hodnotě menší než jedna.

Ještě se musíme vypořádat se skutečností, že právě uvažované zobrazení je dáno násobením řádkových vektorů zprava maticí $B$ (zatímco nás původně zajímalo chování zobrazení, zadaného maticí $B$ pomocí násobení sloupcových vektorů zleva). To je ale ekvivalentní násobení transponovaných sloupcových vektorů transponovanou maticí $B$ obvyklým způsobem zleva. Dokázali jsem tedy vlastně potřebné tvrzení o vlastních číslech pro matici transponovanou k naší matici $B$. Transponování ale vlastní čísla nemění.

Dimenze prostoru $V$ je přitom $n - 1$, takže důkaz věty je ukončen. □

**3.20. Jednoduché důsledky.** Následující velice užitečné tvrzení má při znalosti Perronovy věty až překvapivě jednoduchý důkaz a ukazuje, jak silná je vlastnost primitivnosti matice zobrazení.



**Důsledek.** *Jestliže $A = (a_{ij})$ je primitivní matice a $x \in \mathbb{R}^n$ její vlastní vektor se všemi souřadnicemi nezápornými a vlastní hodnotou $\lambda$, pak $\lambda > 0$ je spektrální poloměr $A$. Navíc platí*

$$\min_{j \in \{1,\ldots,n\}} \sum_{i=1}^{n} a_{ij} \leq \lambda \leq \max_{j \in \{1,\ldots,n\}} \sum_{i=1}^{n} a_{ij}.$$

Důkaz. Uvažme vlastní vektor $x$ z dokazovaného tvrzení. Protože je $A$ primitivní, můžeme zvolit pevně $k$ tak, aby $A^k$ už měla samé pozitivní prvky, a pak je samozřejmě i $A^k \cdot x = \lambda^k x$ vektor se samými ostře kladnými souřadnicemi. Nutně proto je $\lambda > 0$.

Z Perronovy věty víme, že spektrální poloměr $\mu$ je vlastním číslem a zvolme takový vlastní vektor $y$ k $\mu$, že rozdíl $x - y$ má samé kladné souřadnice. Potom nutně pro všechny mocniny $n$

$$0 < A^n \cdot (x - y) = \lambda^n x - \mu^n y,$$

ale zároveň platí $\lambda \leq \mu$. Odtud již vyplývá $\lambda = \mu$.

Zbývá odhad spektrálního poloměru pomocí minima a maxima součtů jednotlivých sloupců matice. Označme je $b_{\min}$ a $b_{\max}$,

**3.17. Model šíření jednoletých bylin.** Budeme uvažovat rostliny, které na začátku léta vykvetou, na jeho vrcholu vyprodukují semena a samy uhynou. Některá ze semen vyklíčí ještě na konci podzimu (ozimé rostliny), jiná přečkají zimu v zemi a vyklíčí na začátku jara (jarní rostliny). Ozimé rostlinky (sazenice), které přes zimu nezmrznou, jsou na jaře větší než jarní a většinou z nich vyrostou větší rostliny než z jarních sazenic. Větší rostlina vyprodukuje více semen. Pak se celý vegetační cyklus opakuje.

Rok je tedy rozdělen na čtyři vegetační období a v každém z těchto období můžeme rozlišit několik „forem“ rostliny:

| Období | stadia rostliny |
|---|---|
| začátek jara | malé a velké sazenice |
| začátek léta | malé, střední a velké kvetoucí rostliny |
| vrcholné léto | semena |
| podzim | sazenice a přezimující semena |

Označme $x_1(t)$, resp. $x_2(t)$, počet malých, resp. velkých, sazenic na začátku jara roku $t$ a $y_1(t)$, resp. $y_2(t)$, resp. $y_3(t)$, počet malých, resp. středních, resp. velkých rostlin v létě téhož roku. Z malých sazenic mohou vyrůst malé nebo střední rostliny, z velkých sazenic mohou vyrůst střední nebo velké rostliny. Kterákoliv ze sazenic samozřejmě může uhynout (uschnout, být spasena krávou a podobně) a nevyroste z ní nic. Označme $b_{ij}$ pravděpodobnost, že ze sazenice $j$-té velikosti, $j = 1, 2$, vyroste rostlina $i$-té velikosti, $i = 1, 2, 3$. Pak je

$$0 < b_{11} < 1, \quad b_{12} = 0, \quad 0 < b_{21} < 1, \quad 0 < b_{22} < 0, \quad b_{31} = 0,$$
$$0 < b_{32} < 1, \quad b_{11} + b_{21} < 1, \quad b_{22} + b_{32} < 1$$

(promyslete si, co každá z těchto nerovností vyjadřuje). Pokud pravděpodobnost považujeme za klasickou, můžeme $b_{11}$ vypočítat jako podíl příznivých výsledků (z malé vyrostla malá rostlina) a všech možných výsledků (počet malých sazenic), tj. $b_{11} = y_1(t)/x_1(t)$. Odtud

$$y_1(t) = b_{11}x_1(t).$$

Analogicky dostaneme rovnost

$$y_3(t) = b_{32}x_2(t).$$

Označíme-li na chvíli $y_{2,1}(t)$, resp. $y_{2,2}(t)$ počet středních rostlin vyrostlých z malých, resp. velkých sazenic, je $y_2(t) = y_{2,1}(t) + y_{2,2}(t)$ a $b_{21} = y_{2,1}(t)/x_1(t)$, $b_{22} = y_{2,2}(t)/x_2(t)$ a tedy

$$y_2(t) = b_{21}x_1(t) + b_{22}x_2(t).$$

Označíme

$$B = \begin{pmatrix} b_{11} & 0 \\ b_{21} & b_{22} \\ 0 & b_{32} \end{pmatrix}, \quad x(t) = \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix}, \quad y(t) = \begin{pmatrix} y_1(t) \\ y_2(t) \\ y_3(t) \end{pmatrix}$$

zvolme za $x$ vektor se součtem souřadnic jedna a počítejme:

$$\sum_{i,j=1}^{n} a_{ij}x_j = \sum_{i=1}^{n} \lambda x_i = \lambda,$$
$$\lambda = \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} a_{ij}\Big)x_j \le \sum_{j=1}^{n} b_{\max}x_j = b_{\max},$$
$$\lambda = \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} a_{ij}\Big)x_j \ge \sum_{j=1}^{n} b_{\min}x_j = b_{\min}. \qquad \square$$

Všimněme si, že např. všechny Leslieho matice z 3.18, kde jsou všechny uvažované koeficienty $f_i$ a $\tau_j$ ostře kladné, jsou primitivní a tedy na ně můžeme plně použít právě odvozené výsledky.

Perronova-Frobeniova věta je zobecněním Perronovy věty na obecnější matice, které tu nebudeme uvádět.

**3.21. Markovovy řetězce.** Velice častý a zajímavý případ lineárních procesů se samými nezápornými prvky v matici je matematický model systému, který se může nacházet v $m$ různých stavech s různou pravděpodobností. V jistém okamžiku je systém ve stavu $i$ s pravděpodobností $x_i$ a k přechodu z možného stavu $i$ do stavu $j$ dojde s pravděpodobností $t_{ij}$.



Můžeme tedy proces zapsat takto: V čase $n$ je systém popsán pravděpodobnostním vektorem

$$x_n = (u_1(n), \ldots, u_m(n))^T.$$

To znamená, že všechny komponenty vektoru $x$ jsou reálná nezáporná čísla a jejich součet je roven jedné. Komponenty udávají rozdělení pravděpodobnosti jednotlivých možností stavů systému. Rozdělení pravděpodobností pro čas $n+1$ bude dáno vynásobením pravděpodobnostní maticí přechodu $T = (t_{ij})$, tj.

$$x_{n+1} = T \cdot x_n.$$

Protože předpokládáme, že vektor $x$ zachycuje všechny možné stavy a proto s celkovou pravděpodobností jedna přejde opět do některého z nich, budou všechny sloupce matice $T$ tvořeny také pravděpodobnostními vektory. Takovému procesu říkáme (diskrétní) *Markovův proces* a výsledné posloupnosti vektorů $x_0, x_1, \ldots$ říkáme *Markovův řetězec*.

Všimněme si, že každý pravděpodobnostní vektor $x$ je skutečně Markovovým procesem zobrazen na vektor se součtem souřadnic jedna:

$$\sum_{i,j} t_{ij}x_j = \sum_{j}\Big(\sum_{i} t_{ij}\Big)x_j = \sum_{j} x_j = 1.$$

Nyní můžeme v plné síle použít Perronovu–Frobeniovu teorii. Protože je součet řádků matice $T$ vždy roven vektoru $(1, \ldots, 1)$, je zcela elementárně vidět, že matice $T - E$ je singulární a jednička proto bude zaručeně vlastním číslem matice $T$.

Pokud je navíc $T$ primitivní matice (tj. např. když jsou všechny prvky nenulové), z Důsledku 3.20 víme, že je jednička jednoduchým kořenem charakteristického polynomu a všechny ostatní mají absolutní hodnotu ostře menší než jedna.

**Věta.** *Markovovy procesy s maticí, která nemá žádné nulové prvky nebo jejíž některá mocnina má tuto vlastnost, splňují:*

- *existuje jediný vlastní vektor $x_\infty$ pro vlastní číslo 1, který je pravděpodobnostní,*

a předchozí rovnosti zapíšeme v maticovém tvaru

$$y(t) = Bx(t).$$

Označíme-li po řadě $c_{11}$, $c_{12}$ a $c_{13}$ počty semen, které vyprodukuje jedna malá, střední a velká rostlina, a $z(t)$ celkový počet vyprodukovaných semen v létě roku $t$, platí

$$z(t) = c_{11}y_1(t) + c_{12}y_2(t) + c_{13}y_3(t),$$

nebo v maticovém tvaru

$$z(t) = Cy(t)$$

při označení

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \end{pmatrix}.$$

Aby matice $C$ popisovala modelovanou realitu, budeme předpokládat, že platí nerovnosti

$$0 < c_{11} < c_{12} < c_{13}.$$

Označme nakonec $w_1(t)$ a $w_2(t)$ počet semen, které vyklíčí ještě na podzim a počet semen, která přezimují, v tomto pořadí, a $d_{11}$, resp. $d_{21}$ pravděpodobnost, že semeno vyklíčí na podzim, resp. nevyklíčí (přezimuje), a $f_{11}$, resp. $f_{22}$ pravděpodobnost, že ozimá sazenice, resp. že přezimující semeno během zimy nezmrzne. Pravděpodobnosti vyklíčení $d_{11}, d_{21}$ zřejmě musí splňovat nerovnosti

$$0 < d_{11}, \quad 0 < d_{21}, \quad d_{11} + d_{21} = 1,$$

a poněvadž rostlinka snáze zmrzne, než semeno ukryté v zemi, budeme o pravděpodobnostech $f_{11}$, $f_{22}$ přežití zimy předpokládat

$$0 < f_{11} < f_{22} < 1.$$

Při označení

$$D = \begin{pmatrix} d_{11} \\ d_{21} \end{pmatrix}, \qquad F = \begin{pmatrix} f_{11} & 0 \\ 0 & f_{22} \end{pmatrix}, \qquad w(t) = \begin{pmatrix} w_1(t) \\ w_2(t) \end{pmatrix}$$

dostaneme podobnými úvahami jako výše rovnosti

$$w(t) = Dz(t), \qquad x(t+1) = Fw(t).$$

Poněvadž násobení matic je asociativní, můžeme pro počty jednotlivých stadií rostlin v následujícím roce z předchozích rovností sestavit

- *iterace $T^k x_0$ se blíží k vektoru $x_\infty$ pro jakýkoliv počáteční pravděpodobnostní vektor $x_0$.*

Důkaz. První tvrzení vyplývá přímo z kladnosti souřadnic vlastního vektoru dovozené v Perronově větě.



Předpokládejme nejprve, že jsou algebraické a geometrické násobnosti vlastních čísel matice $T$ stejné. Pak každý pravděpodobnostní vektor $x_0$ můžeme (v komplexním rozšíření $\mathbb{C}^n$) napsat jako lineární kombinaci

$$x_0 = c_1x_\infty + c_2u_2 + \cdots + c_nu_n,$$

kde $u_2, \ldots, u_n$ doplňují $x_\infty$ na bázi z vlastních vektorů. Pak ovšem $k$–násobná iterace dává opět pravděpodobnostní vektor

$$x_k = T^k \cdot x_0 = c_1x_\infty + \lambda_2^k c_2u_2 + \cdots + \lambda_n^k c_nu_n.$$

Protože jsou všechna vlastní čísla $\lambda_2, \cdots \lambda_n$ v absolutní hodnotě ostře menší než jedna, všechny komponenty vektoru $x_k$, kromě té první, se velmi rychle blíží v normě k nule. Přitom ale je stále $x_k$ pravděpodobnostní, takže musí být $c_1 = 1$ a druhé tvrzení máme ověřeno.

Ve skutečnosti ale i při různé algebraické a geometrické násobnosti vlastních čísel dojdeme ke stejnému závěru pomocí podrobnějšího studia tzv. kořenových podprostorů pro matici $T$, ke kterým se dostaneme v souvislosti s tzv. Jordanovým rozkladem matic ještě v této kapitole, viz poznámka 3.33.

I v obecném případě totiž dostaneme k vlastnímu podprostoru $\langle x_\infty \rangle$ jednoznačně určený invariantní $(n-1)$–rozměrný komplement, na kterém už všechna vlastní čísla jsou v absolutní hodnotě menší než jedna, a proto se příslušná komponenta v $x_k$ také bude neomezeně blížit k nule jako výše. □

**3.22. Iterace stochastických matic.** Matice Markovových procesů, tj. matice jejichž všechny sloupce mají součet svých komponent roven jedné se nazývají *stochastické matice*. Standardní úlohy spojené s Markovovými procesy zahrnují odpovědi na otázky po očekávané střední době přechodu mezi předem určenými stavy systému apod. Zatím ale nejsme na řešení těchto úloh připraveni.



Přeformulujeme předchozí větu do jednoduchého, ale asi docela překvapivého důsledku. Konvergencí k limitní matici v následujícím tvrzení myslíme skutečnost, že když si předem určíme možnou chybu $\varepsilon > 0$, tak najdeme hranici na počet iterací $k$ po níž už všechny komponenty uvedené matice se od té limitní budou lišit o méně než $\varepsilon$.

**Důsledek.** *Nechť $T$ je primitivní stochastická matice z Markovova procesu a $x_\infty$ je stochastický vlastní vektor k dominantnímu číslu 1 jako ve větě výše. Pak iterace $T^k$ konvergují k limitní matici $T_\infty$, jejíž všechny sloupce jsou rovny $x_\infty$.*

Důkaz. Sloupce v matici $T^k$ jsou obrazy vektorů standardní báze v příslušném iterovaném lineárním zobrazení. To ale jsou obrazy pravděpodobnostních vektorů, a proto všechny konvergují k $x_\infty$. □

Nyní se ještě na rozlučku s Markovovými procesy zamyslíme nad problémem, zda existují pro daný systém stavy, do kterých se má systém tendenci dostat a setrvat v nich.

rekurentní formule:

$$\begin{aligned}
x(t+1) &= Fw(t) = F\big(Dz(t)\big) = (FD)z(t) = (FD)\big(Cy(t)\big) = \\
&= (FDC)y(t) = (FDC)\big(Bx(t)\big) = (FDCB)x(t), \\
y(t+1) &= Bx(t+1) = B\big(Fw(t)\big) = (BF)w(t) = \\
&= (BF)\big(Dz(t)\big) = (BFD)z(t) = (BFD)\big(Cy(t)\big) = \\
&= (BFDC)y(t), \\
z(t+1) &= Cy(t+1) = C\big(Bx(t+1)\big) = (CB)x(t+1) = \\
&= (CB)\big(Fw(t)\big) = (CBF)w(t) = (CBF)\big(Dz(t)\big) = \\
&= (CBFD)z(t), \\
w(t+1) &= Dz(t+1) = D\big(Cy(t+1)\big) = (DC)y(t+1) = \\
&= (DC)\big(Bx(t+1)\big) = (DCB)x(t+1) = \\
&= (DCB)\big(Fw(t)\big) = (DCBF)w(t).
\end{aligned}$$

Při označení

$$A_x = FDCB, \quad A_y = BFDC, \quad A_z = CBFD, \quad A_w = DCBF$$

je zjednodušíme na formule

$$\begin{aligned}
x(t+1) &= A_x x(t), & y(t+1) &= A_y y(t), \\
z(t+1) &= A_z z(t), & w(t+1) &= A_w(t).
\end{aligned}$$

Z těchto formulí již můžeme vypočítat složení populace rostlin v libovolném období libovolného roku, pokud známe složení populace v nějakém období počátečního (nultého) roku.

Nechť je například známo složení populace v létě, tj. počet $z(0)$ vysetých semen. Pak složení populace na začátku jara $t$-tého roku je

$$\begin{aligned}
x(t) &= A_x x(t-1) = A_x^2 x(t-2) = \cdots = A_x^{t-1} x(1) = \\
&= A_x^{t-1} Fw(0) = A_x^{t-1} FDz(0).
\end{aligned}$$

Povšimněme si, že matice $A_z = CBFD$ je typu $1 \times 1$. Není to tedy matice, ale skalár. Můžeme tedy označit $\lambda = A_z$, vypočítat

(3.5)

$$\begin{aligned}
\lambda = CBFD &= \begin{pmatrix} c_{11} & c_{12} & c_{13} \end{pmatrix} \begin{pmatrix} b_{11} & 0 \\ b_{21} & b_{22} \\ 0 & b_{32} \end{pmatrix} \begin{pmatrix} f_{11} & 0 \\ 0 & f_{22} \end{pmatrix} \begin{pmatrix} d_{11} \\ d_{21} \end{pmatrix} = \\
&= \begin{pmatrix} c_{11}b_{11} + c_{12}b_{21} & c_{12}b_{22} + c_{13}b_{32} \end{pmatrix} \begin{pmatrix} f_{11}d_{11} \\ f_{22}d_{21} \end{pmatrix} = \\
&= b_{11}c_{11}d_{11}f_{11} + b_{21}c_{12}d_{11}f_{11} + b_{22}c_{12}d_{21}f_{22} + b_{32}c_{13}d_{21}f_{22}
\end{aligned}$$

a předchozí výpočet uspořádat do výhodného tvaru

$$\begin{aligned}
x(t) &= (FDCB)^{t-1} FDz(0) = FD(CBFD)^{t-2} CBFDz(0) = \\
&= FD(CBFD)^{t-1} z(0) = FDA_z^{t-1} z(0) = \lambda^{t-1} FDz(0).
\end{aligned}$$

Tímto způsobem zůstanou pouze dvě násobení matic.

O stavu systému řekneme, že je *přechodový*, jestliže v něm systém setrvává s pravděpodobností ostře menší než jedna. Za *absorpční* označíme stav, ve kterém systém setrvává s pravděpodobností 1 a do kterého se lze dostat s nenulovou pravděpodobností z kteréhokoliv z přechodových stavů. Konečně, Markovův řetězec $x_n$ je *absorpční*, jestliže jsou jeho všechny jeho stavy buď absorpční nebo přechodové.

Je-li v absorpčním Markovově řetězci prvních $r$ stavů systému absorpčních, pro stochastickou matici $T$ systému to znamená, že se rozpadá na „blokově“ horní trojúhelníkový tvar

$$T = \begin{pmatrix} E & R \\ 0 & Q \end{pmatrix},$$

kde $E$ je jednotková matice, jejíž rozměr je dán počtem absorpčních stavů, zatímco $R$ je kladná matice a $Q$ nezáporná. V každém případě iteracemi této matice budeme pořád dostávat stejný blok nulových hodnot v levém dolním bloku, a tedy zcela jistě nebude primitivní, např.

$$T^2 = \begin{pmatrix} E & R + R \cdot Q \\ 0 & Q^2 \end{pmatrix}.$$

I o takových maticích lze získat hodně informací pomocí plné Perronovy–Frobeniovy teorie a se znalostí pravděpodobnosti a statistiky také odhadovat střední doby, po kterých se systém dostane do jednoho z absorpčních stavů apod.

### 4. Více maticového počtu

Na vcelku praktických příkladech jsme viděli, že porozumění vnitřní struktuře matic a jejich vlastnostem je silným nástrojem pro konkrétní výpočty nebo analýzy. Ještě více to platí pro efektivitu numerického počítání s maticemi. Proto se budeme zase chvíli věnovat abstraktní teorii.

Budeme přitom zkoumat další speciální typy lineárních zobrazení na vektorových prostorech ale také obecný případ, kdy je struktura zobrazení popsána tzv. Jordanovou větou.

**3.23. Unitární prostory a zobrazení.** Už jsme si zvykli, že je



užitečné pracovat rovnou v číselném oboru komplexních čísel a to i v případě, kdy nás zajímají jen reálné objekty. Navíc v mnohých oblastech jsou komplexní vektorové prostory nutnou součástí úvah. Jasným příkladem je například tzv. kvantové počítání, které se stalo velmi akční oblastí teoretické informatiky, přestože kvantové počítače zatím zkonstruovány ve funkční podobě nebyly.

Proto navážeme na ortogonální zobrazení a matice z konce druhé kapitoly následující definicí:

#### Unitární prostory

**Definice.** *Unitární prostor* je komplexní vektorový prostor $V$ spolu se zobrazením $V \times V \to \mathbb{C}$, $(u, v) \mapsto u \cdot v$, které splňuje pro všechny vektory $u, v, w \in V$ a skaláry $a \in \mathbb{C}$

(1) $u \cdot v = \overline{v \cdot u}$ (zde pruh značí komplexní konjugaci),
(2) $(au) \cdot v = a(u \cdot v)$,
(3) $(u + v) \cdot w = u \cdot w + v \cdot w$,
(4) je-li $u \neq 0$, pak $u \cdot u > 0$ (zejména je výraz reálný).

Toto zobrazení nazýváme *skalární součin* na $V$.

Reálné číslo $\sqrt{v \cdot v}$ nazýváme *velikostí vektoru* $v$, značíme $\|v\|$ a vektor je *normovaný*, jestliže má velikost jedna. Vektory $u$ a $v$ nazýváme *ortogonální*, jestliže je jejich skalární součin nulový,

Uvedeme konkrétní hodnoty matic $B$, $C$, $D$, $F$. Jedná se o parametry hypotetické rostliny, které ale byly inspirované skutečnou trávou *Vulpia ciliata*:

$$B = \begin{pmatrix} 0{,}3 & 0 \\ 0{,}1 & 0{,}6 \\ 0 & 0{,}2 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 10 & 100 \end{pmatrix},$$

$$D = \begin{pmatrix} 0{,}5 \\ 0{,}5 \end{pmatrix}, \quad F = \begin{pmatrix} 0{,}05 & 0 \\ 0 & 0{,}1 \end{pmatrix}.$$

Nyní můžeme vypočítat jednotlivé matice, které zobrazují vektor popisující složení populace v nějakém vegetačním období na vektor složení populace v témže období následujícího roku:

$$A_x = \begin{pmatrix} 0{,}0325 & 0{,}6500 \\ 0{,}0650 & 1{,}3000 \end{pmatrix}, \quad A_y = \begin{pmatrix} 0{,}0075 & 0{,}0750 & 0{,}7500 \\ 0{,}0325 & 0{,}3250 & 3{,}2500 \\ 0{,}0100 & 0{,}1000 & 1{,}0000 \end{pmatrix},$$

$$A_z = 1{,}3325, \qquad A_w = \begin{pmatrix} 0{,}0325 & 1{,}3000 \\ 0{,}0325 & 1{,}3000 \end{pmatrix}.$$

Hodnota $\lambda = A_z = 1{,}3325$ vyjadřuje meziroční relativní přírůstek populace. Přesvědčete se, že každá z matic $A_x$, $A_y$, $A_w$ má jedinou nenulovou vlastní hodnotu $\lambda = 1{,}3325$; ostatní vlastní hodnoty jsou rovny 0.

Ukážeme ještě jedno využití uvedeného modelu. Může nás zajímat, jak „pružně“ reaguje meziroční relativní přírůstek $\lambda$ na změnu jednotlivých „demografických parametrů“, jak např. změna pravděpodobnosti přežití semene přes zimu ovlivní meziroční přírůstek. Tuto otázku poněkud upřesníme. Za *pružnost reakce charakteristiky $\lambda$ na parametr $s$*, označenou $e(\lambda, s)$ prohlásíme relativní změnu hodnoty $\lambda$ vztaženou k relativní změně parametru $s$. Ještě přesněji: označíme $\lambda(s)$ meziroční přírůstek závislý na parametru $s$. Potom $\Delta\lambda(s) = \lambda(s + \Delta s) - \lambda(s)$ vyjadřuje absolutní změnu relativního přírůstku $\lambda$ při absolutní změně parametru $s$ o $\Delta s$. Relativní změna $\lambda$ tedy je $\Delta\lambda(s)/\lambda(s)$. Relativní změna přírůstku parametru $s$ je $\Delta s\,/s$. Hledaná pružnost je tedy podíl těchto relativních změn, tj.

$$e(\lambda, s) = \frac{\Delta\lambda(s)/\lambda(s)}{\Delta s\,/s} = \frac{s}{\lambda(s)} \frac{\lambda(s + \Delta s) - \lambda(s)}{\Delta s}.$$

Konkrétně meziroční relativní přírůstek populace závislý na přežití semen přes zimu je podle (‖3.5‖)

$$\lambda(f_{22}) = d_{21}(b_{22}c_{12} + b_{32}c_{13})f_{22} + d_{11}(b_{11}c_{11}f_{11} + b_{21}c_{12}f_{11})$$

a pro konkrétní zvolené hodnoty ostatních parametrů

$$\lambda(f_{22}) = 13 f_{22} + 0{,}0325.$$

Poněvadž $f_{22} = 0{,}1$, můžeme počítat

$$\lambda(0{,}1) = 1{,}3325, \ \lambda(0{,}1{+}\Delta s) = 1{,}3325{+}13\Delta s, \ \Delta\lambda(0{,}1) = 13\Delta s,$$

bázi sestavenou z po dvou ortogonálních a normovaných vektorů nazýváme *ortonormální báze $V$*.

Na první pohled jde o rozšíření definice euklidovských vektorových prostorů do komplexního oboru. Nadále budeme také používat alternativní značení $\langle u, v \rangle$ pro skalární součin vektorů $u$ a $v$. Zcela stejně jako v reálném oboru také okamžitě z definice vyplývají následující jednoduché vlastnosti skalárního součinu pro všechny vektory ve $V$ a skaláry v $\mathbb{C}$:

$$\begin{aligned} u \cdot u &\in \mathbb{R}, \\ u \cdot u &= 0 \text{ právě tehdy, když } u = 0, \\ u \cdot (av) &= \bar{a}(u \cdot v), \\ u \cdot (v + w) &= u \cdot v + u \cdot w, \\ u \cdot 0 &= 0 \cdot u = 0, \\ \Big(\sum_i a_i u_i\Big) \cdot \Big(\sum_j b_j v_j\Big) &= \sum_{i,j} a_i \bar{b}_j (u_i \cdot v_j), \end{aligned}$$

kde poslední rovnost platí pro všechny konečné lineární kombinace. Podrobné ověření je skutečně jednoduchým cvičením, např. první vztah plyne okamžitě z definiční vlastnosti (1).

Standardním příkladem skalárního součinu na komplexním vektorovém prostoru $\mathbb{C}^n$ je

$$(x_1, \ldots, x_n)^T \cdot (y_1, \ldots, x_n)^T = x_1\bar{y}_1 + \cdots + x_n\bar{y}_n.$$

Díky konjugování souřadnic druhého argumentu toto zobrazení splňuje všechny požadované vlastnosti. Prostor $\mathbb{C}^n$ s tímto skalárním součinem budeme nazývat *standardní unitární prostor* v dimenzi $n$. Maticově můžeme tento skalární součin psát jako $x \cdot y = \bar{y}^T \cdot x$.

Zcela obdobně jako u euklidovských prostorů a ortogonálních zobrazení budou důležitá lineární zobrazení, která respektují skalární součiny.

### Unitární zobrazení

Lineární zobrazení $\varphi : V \to W$ mezi unitárními prostory se nazývá *unitární zobrazení*, jestliže pro všechny vektory $u, v \in V$ platí

$$u \cdot v = \varphi(u) \cdot \varphi(v).$$

*Unitární isomorfismus* je bijektivní unitární zobrazení.

**3.24. Vlastnosti prostorů se skalárním součinem.** Ve stručné



diskusi euklidovských prostorů v předchozí kapitole jsme už některé jednoduché vlastnosti prostorů se skalárním součinem odvodili, důkazy v komplexním oboru jsou velmi podobné.

V dalším budeme pracovat s reálnými i komplexními prostory zároveň a budeme psát $\mathbb{K}$ pro $\mathbb{R}$ nebo $\mathbb{C}$, v reálném případě je konjugace prostě identické zobrazení (tak jak skutečně zúžení konjugace na reálnou přímku v komplexní rovině je). Stejně jako u reálných prostorů definujeme obecně pro libovolný vektorový podprostor $U \subseteq V$ v prostoru se skalárním součinem jeho *ortogonální doplněk*

$$U^\perp = \{v \in V;\ u \cdot v = 0 \text{ pro všechny } u \in U\},$$

což je zjevně také vektorový podprostor ve $V$.

takže

$$e(\lambda, 0{,}1) = \frac{0{,}1}{1{,}3325}\frac{13\Delta s}{\Delta s} \doteq 0{,}976.$$

Analogicky můžeme spočítat pružnost reakce relativního přírůstku $\lambda$ populace na ostatních „demografických parametrech“. Výsledky jsou shrnuty v tabulce:

| parametr | pružnost reakce | parametr | pružnost reakce |
|---|---|---|---|
| $b_{11}$ | 0,006 | $c_{11}$ | 0,006 |
| $b_{21}$ | 0,019 | $c_{12}$ | 0,244 |
| $b_{22}$ | 0,225 | $c_{13}$ | 0,751 |
| $b_{23}$ | 0,750 | $f_{11}$ | 0,024 |
| $d_{11}$ | 0,024 | $f_{22}$ | 0,976 |
| $d_{21}$ | 0,976 | | |

Z ní můžeme vidět, že přírůstek $\lambda$ je nejvíce ovlivňován množstvím přezimujících semen (parametr $d_{21}$) a jejich přežíváním (parametr $f_{22}$). Toto zjištění není nijak překvapivé, zemědělcům je tento fakt dobře známý již od neolitu. Výsledek však ukazuje, že matematický model skutečně nějak adekvátně realitu popisuje.

Další zajímavé a detailně popsané modely růstu nalezne čtenář v souboru příkladů za touto kapitolou.

**3.18.** Uvažujte následující Leslieho model: farmář chová ovce. Porodnost ovcí je dána pouze věkem a je průměrně 2 ovce na jednu ovci mezi jedním a dvěma lety věku, pět ovcí na ovci mezi dvěma a třemi lety věku a dvě ovce na ovci mezi třemi a čtyřmi roky věku. Ovce do jednoho roku nerodí. Z roku na rok umře vždy polovina ovcí a to rovnoměrně ve všech věkových skupinách. Po čtyřech letech posílá farmář ovce na jatka. Farmář by rád ještě prodával (živá) jehňátka do jednoho roku na kožešinu. Jakou část jehňátek může každý rok prodat, aby mu velikost stáda zůstávala z roku na rok stejná? V jakém poměru budou potom rozděleny počty ovcí v jednotlivých věkových skupinách?

**Řešení.** Matice daného modelu (bez zásahu farmáře) je

$$L = \begin{pmatrix} 0 & 2 & 5 & 2 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}.$$

Farmář může ovlivnit kolik ovcí do jednoho roku mu ve stádu zůstane do dalšího roku, může tedy ovlivnit prvek $l_{12}$ matice $L$. Zkoumáme tedy model

$$L = \begin{pmatrix} 0 & 2 & 5 & 2 \\ a & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}$$

a hledáme $a$ tak, aby daná matice měla vlastní hodnotu 1 (víme, že má pouze jednu reálnou kladnou). Charakteristický polynom této matice

Budeme v dalších odstavcích pracovat výhradně s konečněrozměrnými unitárními nebo euklidovskými prostory. Řada našich výsledků ale má přirozené rozšíření pro tzv. Hilbertovy prostory, což jsou jisté nekonečněrozměrné prostory se skalárním součinem, ke kterým se aspoň stručně vrátíme později.

**Tvrzení.** *Pro každý konečněrozměrný prostor $V$ dimenze $n$ se skalárním součinem platí:*

*(1) Ve $V$ existuje ortonormální báze.*
*(2) Každý systém nenulových ortogonálních vektorů ve $V$ je lineárně nezávislý a lze jej doplnit do ortogonální báze.*
*(3) Pro každý systém lineárně nezávislých vektorů $(u_1, \dots, u_k)$ existuje ortonormální báze $(v_1, \dots, v_n)$ taková, že její vektory postupně generují stejné podprostory jako vektory $u_j$, tzn. $\langle v_1, \dots, v_i\rangle = \langle u_1 \dots, u_i\rangle$, $1 \le i \le k$.*
*(4) Je-li $(u_1, \dots, u_n)$ ortonormální báze $V$, pak souřadnice každého vektoru $u \in V$ jsou vyjádřeny vztahem*

$$u = (u \cdot u_1)u_1 + \cdots + (u \cdot u_n)u_n.$$

*(5) V libovolné ortonormální bázi má skalární součin souřadný tvar*

$$u \cdot v = x \cdot y = x_1\bar{y}_1 + \cdots + x_n\bar{y}_n,$$

*kde $x$ a $y$ jsou sloupce souřadnic vektorů $u$ a $v$ ve zvolené bázi. Zejména je tedy každý $n$–rozměrný prostor se skalárním součinem izomorfní standardnímu euklidovskému $\mathbb{R}^n$ nebo unitárnímu $\mathbb{C}^n$.*
*(6) Ortogonální součet unitárních podprostorů $V_1 + \cdots + V_k$ ve $V$ je vždy přímý součet.*
*(7) Je-li $A \subseteq V$ libovolná podmnožina, pak $A^\perp \subseteq V$ je vektorový (tedy i unitární) podprostor a $(A^\perp)^\perp \subseteq V$ je právě podprostor generovaný $A$. Navíc platí $V = \langle A\rangle \oplus A^\perp$.*
*(8) $V$ je ortogonálním součtem $n$ jednorozměrných unitárních podprostorů.*



Důkaz. (1), (2), (3): Daný systém vektorů nejprve doplníme do libovolné báze $(u_1, \dots, u_n)$ prostoru $V$ a spustíme na ni Gramovu–Schmidtovu ortogonalizaci z 2.42. Tak získáme ortogonální bázi s vlastnostmi požadovanými v (3). Přitom ale z algoritmu Gramovy–Schmidtovy ortogonalizace vyplývá, že pokud již původních $k$ vektorů tvořilo ortogonální systém vektorů, pak v průběhu ortogonalizace zůstanou nezměněny. Dokázali jsme tedy zároveň i (2) a (1).

(4): Je-li $u = a_1u_1 + \cdots + a_nu_n$, pak

$$u \cdot u_i = a_1(u_1 \cdot u_i) + \cdots + a_n(u_n \cdot u_i) = a_i\|u_i\|^2 = a_i.$$

(5): Podobně pro libovolné vektory $u = x_1u_1 + \dots + x_nu_n$, $v = y_1u_1 + \dots + y_nu_n$:

$$u \cdot v = (x_1u_1 + \cdots + x_nu_n) \cdot (y_1u_1 + \cdots + y_nu_n) = \\ = x_1\bar{y}_1 + \cdots + x_n\bar{y}_n.$$

(6): Potřebujeme ukázat, že pro libovolnou dvojici $V_i$, $V_j$ ze zadaných podprostorů je jejich průnik triviální. Je-li však $u \in V_i$ a zároveň $u \in V_j$, pak je $u \perp u$, tj. $u \cdot u = 0$. To je ale možné pouze pro nulový vektor $u \in V$.

(7): Nechť $u, v \in A^\perp$. Pak $(au + bv) \cdot w = 0$ pro všechny $w \in A$, $a, b \in \mathbb{K}$ (z distributivity skalárního součinu). Tím jsme ověřili, že $A^\perp$ je unitární podprostor ve $V$. Nechť $(v_1, \dots, v_k)$

je

$$\lambda^4 - 2a\lambda^2 - \frac{5}{2}a\lambda - \frac{1}{2}a.$$

Požadujeme-li, aby měl kořen 1, musí být $a = \frac{1}{5}$ (dosadíme za $\lambda$ číslo 1 a položíme rovno nule). Farmář tedy může prodat $\frac{1}{2} - \frac{1}{5} = \frac{3}{10}$ ovcí, které se mu v daný rok narodí. Odpovídající vlastní vektor k vlastnímu číslu 1 dané matice je $(20, 4, 2, 1)$ a v těchto poměrech se taky ustálí populace ovcí. □

*3.19.* Uvažujme Leslieho model růstu pro populaci krys, které máme rozděleny do tří věkových skupin: do jednoho roku, od jednoho do dvou let a od dvou let do tří. Předpokládáme, že se žádná krysa nedožívá více než tří let. Průměrná porodnost v jednotlivých věkových skupinách připadajících na jednu krysu je následující: v 1. skupině je to nula a ve druhé i třetí 2 krysy. Krysy, které se dožijí jednoho roku, umírají až po druhém roce života (úmrtnost ve druhé skupině je nulová). Určete úmrtnost v první skupině, víte-li, že daná populace krys stagnuje (počet jedinců v ní se nemění). ○

Další zajímavé populační modely můžete najít počínaje stranou 170.

### D. Markovovy procesy

**3.20. Mlsný hazardér.** Hazardní hráč sází na to, která strana mince padne. Na začátku hry má tři kremrole. Na každý hod vsadí jednu kremroli a když jeho tip vyjde, tak k ní získá jednu navíc, pokud ne, tak kremroli prohrává. Hra končí, pokud všechny kremrole prohraje, nebo jich získá pět. Jaká je pravděpodobnost, že hra neskončí po čtyřech sázkách?

**Řešení.** Před $j$-tým kolem (sázkou) můžeme popsat stav, ve kterém se hráč nachází náhodným vektorem $X_j = \big(p_0(j), p_1(j), p_2(j), p_3(j), p_4(j), p_5(j)\big)$, kde $p_i$ je pravděpodobnost, že hráč má $i$ kremrolí. Pokud má hráč před $j$-tou sázkou $i$ kremrolí ($i = 2, 3, 4$), tak po sázce má s poloviční pravděpodobností $(i-1)$ kremrolí a s poloviční pravděpodobností $(i+1)$ kremrolí. Pokud dosáhne pěti kremrolí nebo všechny prohraje, už se počet kremrolí nemění. Vektor $X_{j+1}$ tak získáme podle podmínek zadání z $X_j$ vynásobením maticí

$$A := \begin{pmatrix} 1 & 0{,}5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0{,}5 & 0 & 0 & 0 \\ 0 & 0{,}5 & 0 & 0{,}5 & 0 & 0 \\ 0 & 0 & 0{,}5 & 0 & 0{,}5 & 0 \\ 0 & 0 & 0 & 0{,}5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0{,}5 & 1 \end{pmatrix}.$$

je nějaká báze $\langle A\rangle$, vybraná z prvků $A$, $(u_1, \dots, u_k)$ ortonormální báze vzniklá z Gramovy–Schmidtovy ortogonalizace vektorů $(v_1, \dots, v_k)$. Doplňme ji na ortonormální bázi celého $V$ (obojí existuje podle již dokázaných částí věty). Protože se jedná o ortogonální bázi, je nutně $\langle u_{k+1}, \dots, u_n\rangle = \langle u_1, \dots, u_k\rangle^\perp = A^\perp$ a $A \subseteq \langle u_{k+1}, \dots, u_n\rangle^\perp$ (jak plyne z vyjádření souřadnic v ortonormální bázi). Je-li $u \perp \langle u_{k+1}, \dots, u_n\rangle$, pak $u$ je nutně lineární kombinací vektorů $u_1, \dots, u_k$, to je ale právě tehdy, když je lineární kombinací vektorů $v_1, \dots, v_k$, což je ekvivalentní příslušnosti $u$ do $\langle A\rangle$.
(8): Je pouze ekvivalentní formulaci existence ortonormální báze. □

**3.25. Důležité vlastnosti velikosti.** Nyní máme vše připraveno pro základní vlastnosti spojené s naší definicí velikostí vektorů. Hovoříme také o *normě* definované skalárním součinem. Všimněme si také, že všechna tvrzení se týkají vždy konečných množin vektorů a jejich platnost proto nezávisí na dimenzi prostoru $V$, ve kterém se vše odehrává.



**Věta.** *Pro libovolné vektory $u, v$ v prostoru $V$ se skalárním součinem platí*

*(1)* $\|u+v\| \le \|u\|+\|v\|$, *přitom rovnost nastane, právě když jsou $u$ a $v$ lineárně závislé.*
*(trojúhelníková nerovnost)*
*(2)* $|u \cdot v| \le \|u\|\,\|v\|$, *přitom rovnost nastane, právě když jsou $u$ a $v$ lineárně závislé.*
*(Cauchyova nerovnost)*
*(3) Pro každý ortonormální systém vektorů $(e_1, \dots, e_k)$ platí*

$$\|u\|^2 \ge |u \cdot e_1|^2 + \cdots + |u \cdot e_k|^2.$$

*(Besselova nerovnost)*
*(4) Pro ortonormální systém vektorů $(e_1, \dots, e_k)$ patří vektor $u$ do podprostoru $\langle e_1, \dots, e_k\rangle$, právě když*

$$\|u\|^2 = |u \cdot e_1|^2 + \cdots + |u \cdot e_k|^2.$$

*(Parsevalova rovnost)*
*(5) Pro ortonormální systém vektorů $(e_1, \dots, e_k)$ a vektor $u \in V$ je vektor*

$$w = (u \cdot e_1)e_1 + \cdots + (u \cdot e_k)e_k$$

*jediným vektorem, který minimalizuje velikost $\|u - v\|$ pro všechny $v \in \langle e_1, \dots, e_k\rangle$.*

Důkaz. Všechny důkazy spočívají v přímých výpočtech:
(2): Definujme vektor $w := u - \frac{u\cdot v}{v\cdot v}v$, tzn. $w \perp v$, a počítejme

$$0 \le \|w\|^2 = \|u\|^2 - \tfrac{(\overline{u\cdot v})}{\|v\|^2}(u \cdot v) - \tfrac{u\cdot v}{\|v\|^2}(v \cdot u) + \tfrac{(u\cdot v)(\overline{u\cdot v})}{\|v\|^4}\|v\|^2,$$
$$0 \le \|w\|^2\|v\|^2 = \|u\|^2\|v\|^2 - 2(u \cdot v)(\overline{u \cdot v}) + (u \cdot v)(\overline{u \cdot v}).$$

Odtud již přímo plyne, že $\|u\|^2\|v\|^2 \ge |u \cdot v|^2$ a rovnost nastane právě tehdy, když $w = 0$, tj. když jsou $u$ a $v$ lineárně závislé.

Na začátku máme $X_1 = (0, 0, 1, 0, 0)^T$, po čtyřech sázkách bude situaci popisovat náhodný vektor

$$X_5 = A^4 X_1 = \left(\frac{1}{8}, \frac{3}{16}, 0, \frac{5}{16}, 0, \frac{3}{8}\right)^T,$$

tedy pravděpodobnost, že hra skončí do čtvrté sázky (včetně) je polovina.

Všimněme si ještě, že matice $A$ popisující vývoj pravděpodobnostního vektoru $X$ je pravděpodobnostní, tedy má součet prvků v každém sloupci 1. Nemá ale vlastnost vyžadovanou v Perronově–Frobeniově větě a snadným výpočtem zjistíte (nebo přímo uvidíte bez počítání), že existují dva lineárně nezávislé vlastní vektory příslušné k vlastnímu číslu 1 – případ, kdy hráči nezůstane žádná krémrole, tj. $x = (1, 0, 0, 0, 0, 0)^T$, nebo případ kdy získá 5 krémrolí a hra tím pádem končí a všechny mu už zůstávají, tj. $x = (0, 0, 0, 0, 0, 1)^T$. Všechna ostatní vlastní čísla (přibližně 0,8, 0,3, −0,8, −0,3) jsou v absolutní hodnotě ostře menší než jedna. Proto komponenty v příslušných vlastních podprostorech při iteraci procesu s libovolnou počáteční hodnotou vymizí a proces se blíží k limitní hodnotě pravděpodobnostního vektoru tvaru $(a, 0, 0, 0, 0, 1-a)$, kde hodnota $a$ závisí na počtu kremrolí, se kterými hráč začíná. V našem případě je to $a = 0{,}4$, kdyby začal se 4 kremrolemi, bylo by to $a = 0{,}2$ atd. □

**3.21.** Na základě teploty ve dvě hodiny odpoledne se rozdělují dny na teplé, průměrné a chladné. Dle celoročních statistik následuje po teplém dni teplý v polovině případů a průměrný ve 30 % případů, po průměrném dnu průměrný ve 40 % případů a chladný ve 30 % případů, po chladném dnu chladný v polovině případů a ve 30 % případů průměrný. Bez dalších informací zjistěte, kolik lze během roku očekávat teplých, průměrných a chladných dnů.

**Řešení.** Pro každý den musí nastav právě jeden ze stavů „teplý den“, „průměrný den“, „chladný den“. Pokud vektor $x_n$ má za složky pravděpodobnosti toho, že jistý (označený jako $n$-tý) den bude teplý, průměrný, chladný (při zachování pořadí), potom složky vektoru

$$x_{n+1} = \begin{pmatrix} 0{,}5 & 0{,}3 & 0{,}2 \\ 0{,}3 & 0{,}4 & 0{,}3 \\ 0{,}2 & 0{,}3 & 0{,}5 \end{pmatrix} \cdot x_n$$

udávají postupně pravděpodobnosti, že následující den bude teplý, průměrný, chladný. Pro ověření stačí dosadit

$$x_n = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad x_n = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad x_n = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},$$

přičemž např. pro třetí volbu musíme dostat pravděpodobnosti, že po chladném dnu bude následovat teplý, průměrný, chladný (v tomto

(1): Opět stačí počítat

$$\begin{aligned} \|u+v\|^2 &= \|u\|^2 + \|v\|^2 + u\cdot v + v\cdot u = \\ &= \|u\|^2 + \|v\|^2 + 2\,\mathrm{Re}(u\cdot v) \le \\ &\le \|u\|^2 + \|v\|^2 + 2|u\cdot v| \le \\ &\le \|u\|^2 + \|v\|^2 + 2\|u\|\|v\| = \\ &= (\|u\| + \|v\|)^2. \end{aligned}$$

Protože se přitom jedná o nezáporná reálná čísla, je opravdu $\|u+v\| \le \|u\| + \|v\|$. Navíc, při rovnosti musí nastat rovnost ve všech předchozích nerovnostech, to však je ekvivalentní podmínce, že $u$ a $v$ jsou lineárně závislé (podle předchozí části důkazu).
(3), (4): Nechť $(e_1, \dots, e_k)$ je ortonormální systém vektorů. Doplníme jej do ortonormální báze $(e_1, \dots, e_n)$ (to vždy jde podle předchozí věty). Pak, opět podle předchozí věty, je pro každý vektor $u \in V$:

$$\|u\|^2 = \sum_{i=1}^{n} (u\cdot e_i)(\overline{u\cdot e_i}) = \sum_{i=1}^{n} |u\cdot e_i|^2 \ge \sum_{i=1}^{k} |u\cdot e_i|^2.$$

To je ale právě dokazovaná Besselova nerovnost. Přitom rovnost může nastat právě tehdy, když $u\cdot e_i = 0$ pro všechny $i > k$, a to dokazuje Parsevalovu rovnost.
(5): Zvolme libovolný $v \in \langle e_1, \dots, e_k\rangle$ a doplňme daný ortonormální systém na ortonormální bázi $(e_1, \dots, e_n)$. Nechť $(u_1, \dots, u_n)$ a $(x_1, \dots, x_k, 0, \dots, 0)$ jsou souřadnice $u$ a $v$ v této bázi. Pak

$$\|u-v\|^2 = |u_1 - x_1|^2 + \cdots + |u_k - x_k|^2 + |u_{k+1}|^2 + \cdots + |u_n|^2$$

a tento výraz je zjevně minimalizován při volbě jednotlivých vektorů $x_1 = u_1, \dots, x_k = u_k$. □

**3.26. Vlastnosti unitárních zobrazení.** Vlastnosti ortogonálních zobrazení mají přímočarou obdobu v komplexním oboru. Můžeme je snadno zformulovat a dokázat společně:



**Tvrzení.** *Uvažme lineární zobrazení (endomorfismus) $\varphi : V \to V$ na prostoru se skalárním součinem. Pak jsou následující podmínky ekvivalentní:*

*(1) $\varphi$ je unitární nebo ortogonální transformace,*
*(2) $\varphi$ je lineární isomorfismus a pro každé $u, v \in V$ platí $\varphi(u)\cdot v = u\cdot\varphi^{-1}(v)$,*
*(3) matice $A$ zobrazení $\varphi$ v libovolné ortonormální bázi splňuje $A^{-1} = \bar{A}^T$ (pro euklidovské prostory to znamená $A^{-1} = A^T$),*
*(4) matice $A$ zobrazení $\varphi$ v některé ortonormální bázi splňuje $A^{-1} = \bar{A}^T$,*
*(5) řádky matice $A$ zobrazení $\varphi$ v ortonormální bázi tvoří ortonormální bázi prostoru $\mathbb{K}^n$ se standardním skalárním součinem,*
*(6) sloupce matice $A$ zobrazení $\varphi$ v ortonormální bázi tvoří ortonormální bázi prostoru $\mathbb{K}^n$ se standardním skalárním součinem.*

Důkaz. (1) ⇒ (2): Zobrazení $\varphi$ je prosté, proto musí být i na. Platí přitom $\varphi(u)\cdot v = \varphi(u)\cdot\varphi(\varphi^{-1}(v)) = u\cdot\varphi^{-1}(v)$.
(2) ⇒ (3): Standardní skalární součin je v $\mathbb{K}^n$ vždy dán pro sloupce $x, y$ skalárů výrazem $x\cdot y = x^T E\bar{y}$, kde $E$ je jednotková matice. Vlastnost (2) tedy znamená, že matice $A$ zobrazení $\varphi$ je invertibilní a platí $(Ax)^T\bar{y} = x^T\overline{A^{-1}y}$. To znamená

pořadí). Vidíme tak, že úloha je Markovovým řetězcem s pravděpodobnostní maticí přechodu

$$T = \begin{pmatrix} 0{,}5 & 0{,}3 & 0{,}2 \\ 0{,}3 & 0{,}4 & 0{,}3 \\ 0{,}2 & 0{,}3 & 0{,}5 \end{pmatrix}.$$

Neboť jsou všechny prvky této matice kladné, existuje pravděpodobnostní vektor

$$x_\infty = \left(x^1_\infty, x^2_\infty, x^3_\infty\right)^T,$$

k němuž se blíží vektor $x_n$ pro zvětšující se $n$ nezávisle na tom, jaký byl vektor $x_n$ pro mnohem menší $n$. Navíc podle důsledku Perronovy-Frobeniovy věty (viz odstavec 3.19) je $x_\infty$ vlastním vektorem matice $T$ pro vlastní číslo 1. Má tedy platit

$$\begin{aligned} x^1_\infty &= 0{,}5\,x^1_\infty + 0{,}3\,x^2_\infty + 0{,}2\,x^3_\infty, \\ x^2_\infty &= 0{,}3\,x^1_\infty + 0{,}4\,x^2_\infty + 0{,}3\,x^3_\infty, \\ x^3_\infty &= 0{,}2\,x^1_\infty + 0{,}3\,x^2_\infty + 0{,}5\,x^3_\infty, \\ 1 &= x^1_\infty + x^2_\infty + x^3_\infty, \end{aligned}$$

kde poslední podmínka znamená, že vektor $x_\infty$ je pravděpodobnostní. Snadno se vypočítá, že tato soustava má jediné řešení

$$x^1_\infty = x^2_\infty = x^3_\infty = \frac{1}{3}.$$

Lze tedy očekávat přibližně stejný počet teplých, průměrných a chladných dnů.

Zdůrazněme, že součet všech čísel z libovolného sloupce matice $T$ musel být roven 1 (jinak by se nejednalo o Markovův proces). Protože $T^T = T$ (matice je symetrická), je součet všech čísel z libovolného řádku matice také roven 1. O matici s nezápornými prvky a s vlastností, že součet čísel v každém řádku a rovněž součet čísel v každém sloupci je 1, mluvíme jako o dvojnásobně (dvojitě, dvojně) stochastické. Důležitou vlastností každé dvojnásobně stochastické primitivní matice (pro jakýkoli rozměr – počet stavů) je, že jí příslušný vektor $x_\infty$ má všechny složky stejné, tj. po dostatečně dlouhé době vyhodnocování se všechny stavy v odpovídajícím Markovově procesu jeví jako stejně časté. □

**3.22. Půjčovna aut.** Firma půjčující každý týden auta má dvě pobočky - jednu v Brně a jednu v Praze. Auto zapůjčené v Brně lze vrátit i v Praze a naopak. Po čase se zjistilo, že na konci týdne je vždy v Praze vráceno zhruba 80 % z aut vypůjčených v Praze a 90 % z aut vypůjčených v Brně.

Jak je potřeba rozdělit auta mezi pobočky, aby na obou byl na začátku týdne vždy stejný počet aut jako předchozí týden?

Jak bude vypadat situace po jisté dlouhé době, pokud jsou auta mezi pobočky na začátku náhodně rozdělena?

$\bar{x}^T\left(\bar{A}^T y - A^{-1} y\right) = 0$ pro všechny $x \in \mathbb{K}^n$. Zejména dosazením výrazu v závorce za $x$ zjistíme, že to je možné pouze při $\bar{A}^T = A^{-1}$.

(3) $\Leftrightarrow$ (4): Je-li $\bar{A}^T = A^{-1}$ v některé ortonormální bázi, pak to zaručuje platnost podmínky (2):

$$\varphi(u) \cdot v = (Ax)^T E\bar{y} = x^T E\overline{A^{-1}y} = u \cdot \varphi^{-1}(v)$$

a tedy i (3).

(4) $\Rightarrow$ (5) Dokazované tvrzení je vyjádřeno prostřednictvím matice $A$ zobrazení $\varphi$ vztahem $A\bar{A}^T = E$, to je ale zaručeno podmínkou (4).

(5) $\Rightarrow$ (6): Protože pro determinant platí $|\bar{A}^T A| = |E| = |A\bar{A}^T| = |A|\overline{|A|} = 1$, existuje inverzní matice $A^{-1}$. Přitom je $A\bar{A}^T A = A$, proto i $\bar{A}^T A = E$ což vyjadřuje právě (6).

(6) $\Rightarrow$ (1): Ve vybrané ortonormální bázi je

$$\varphi(u) \cdot \varphi(v) = (Ax)^T\overline{(Ay)} = xA^T\bar{A}\bar{y} = x^T\bar{E}\bar{y} = x^T\bar{y},$$

kde $x$ a $y$ jsou sloupce souřadnic vektorů $u$ a $v$. Tím je zaručeno zachovávání skalárního součinu. □



Charakterizace z předchozí věty si zaslouží několik poznámek. Matice $A \in \mathrm{Mat}_n(\mathbb{K})$ s vlastností $A^{-1} = \bar{A}^T$ se nazývají *unitární matice* pro komplexní skaláry (a v případě $\mathbb{R}$ jsme jim již říkali *ortogonální matice*). Z definiční vlastnosti plyne, že součin unitárních (resp. ortogonálních) matic je unitární (resp. ortogonální), stejně pro inverze. Unitární matice tedy tvoří podgrupu $U(n) \subseteq \mathrm{Gl}_n(\mathbb{C})$ v grupě všech invertibilních komplexních matic s operací součinu. Ortogonální matice tvoří podgrupu $O(n) \subseteq \mathrm{Gl}_n(\mathbb{R})$ v grupě reálných invertibilních matic. Hovoříme o *unitární grupě* a o *ortogonální grupě*.

Jednoduchý výpočet

$$1 = \det E = \det(A\bar{A}^T) = \det A\,\overline{\det A} = |\det A|^2$$

ukazuje, že determinant unitární matice má vždy velikost rovnu jedné, v případě reálných skalárů pak determinant musí být $\pm 1$. Dále, je-li $Ax = \lambda x$ pro unitární či ortogonální matici, pak $(Ax) \cdot (Ax) = x \cdot x = |\lambda|^2 (x \cdot x)$. Proto jsou reálné vlastní hodnoty ortogonálních matic v reálném oboru rovny $\pm 1$, vlastní hodnoty unitárních matic jsou vždy komplexní jednotky v komplexní rovině.

Stejně jako u ortogonálních zobrazení také docela snadno ověříme, že ortogonální doplňky k invariantním podprostorům vzhledem k unitárnímu $\varphi : V \to V$ jsou vždy také invariantní. Skutečně, je-li $\varphi(U) \subseteq U$, $u \in U$ a $v \in U^\perp$ libovolné, pak

$$\varphi(v) \cdot \varphi(\varphi^{-1}(u)) = v \cdot \varphi^{-1}(u).$$

Protože je zúžení $\varphi_{|U}$ také unitární, musí to tedy být bijekce, zejména je $\varphi^{-1}(u) \in U$. Pak ovšem $\varphi(v) \cdot u = 0$, protože $v \in U^\perp$. To znamená, že i $\varphi(v) \in U^\perp$.

Odtud ovšem v komplexním oboru okamžitě dostáváme užitečný důsledek.

**Důsledek.** *Nechť $\varphi : V \to V$ je unitární zobrazení komplexních vektorových prostorů. Pak je $V$ ortogonálním součtem jednorozměrných vlastních podprostorů.*

Důkaz. Jistě existuje alespoň jeden vlastní vektor $v \in V$. Pak je zúžení $\varphi$ na invariantní podprostor $\langle v \rangle^\perp$ opět unitární a jistě má opět nějaký vlastní vektor. Po $n$ takovýchto krocích obdržíme hledanou ortogonální bázi z vlastních vektorů. Po vynormování vektorů získáme ortonormální bázi. □

**Řešení.** Hledaný začáteční počet aut v Brně označme $x_B$ a v Praze $x_P$. Stav rozmístění aut mezi pobočkami je tedy popsán vektorem $\mathrm{x} = \begin{pmatrix} x_B \\ x_P \end{pmatrix}$. Uvážíme-li takový násobek vektoru x, že součet jeho složek je 1, pak dávají jeho složky procentuální rozmístění aut.

Na konci týdne bude podle zadání stav popsán vektorem $\begin{pmatrix} 0{,}1 & 0{,}2 \\ 0{,}9 & 0{,}8 \end{pmatrix}\begin{pmatrix} x_B \\ x_P \end{pmatrix}$. Matice $A = \begin{pmatrix} 0{,}1 & 0{,}2 \\ 0{,}9 & 0{,}8 \end{pmatrix}$ tedy popisuje náš (lineární) systém půjčování aut. Pokud má být na konci týdne v pobočkách stejně aut jako na začátku, pak hledáme takový vektor x, pro který platí $A\mathrm{x} = \mathrm{x}$. To znamená, že hledáme vlastní vektor matice $A$ příslušný vlastnímu číslu 1.

Charakteristický polynom matice $A$ je

$$(0{,}1 - \lambda)(0{,}8 - \lambda) - (0{,}9) \cdot (0{,}2) = (\lambda - 1)(\lambda + 0{,}1)$$

a 1 je tedy opravdu vlastní hodnota matice $A$. Příslušný vlastní vektor $\mathrm{x} = \begin{pmatrix} x_B \\ x_P \end{pmatrix}$ splňuje rovnici $\begin{pmatrix} -0{,}9 & 0{,}2 \\ 0{,}9 & -0{,}2 \end{pmatrix}\begin{pmatrix} x_B \\ x_P \end{pmatrix} = 0$. Je to tedy násobek vektoru $\begin{pmatrix} 0{,}2 \\ 0{,}9 \end{pmatrix}$. Pro zjištění procentuálního rozložení hledáme takový násobek, aby $x_B + x_P = 1$. To splňuje vektor $\frac{1}{1{,}1}\begin{pmatrix} 0{,}2 \\ 0{,}9 \end{pmatrix} = \begin{pmatrix} 0{,}18 \\ 0{,}82 \end{pmatrix}$. Správné rozložení aut mezi Brnem a Prahou je takové, že 18% aut bude v Brně a 82% aut v Praze.

Pokud zvolíme libovolný počáteční stav $\mathrm{x} = \begin{pmatrix} x_B \\ x_P \end{pmatrix}$, pak bude stav za $n$ týdnů popsán vektorem $\mathrm{x}_n = A^n\mathrm{x}$. Nyní je výhodné vyjádřit počáteční vektor x v bázi vlastních vektorů matice $A$. Vlastní vektor k vlastnímu číslu 1 už jsme našli a podobně se nalezne vlastní vektor k vlastnímu číslu $-0{,}1$. Tím je například vektor $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

Počáteční vektor tedy můžeme vyjádřit jako lineární kombinaci $\mathrm{x} = a\begin{pmatrix} 0{,}2 \\ 0{,}9 \end{pmatrix} + b\begin{pmatrix} -1 \\ 1 \end{pmatrix}$. Stav po $n$ týdnech je pak

$$\mathrm{x}_n = A^n\left(a\begin{pmatrix} 0{,}18 \\ 0{,}82 \end{pmatrix} + b\begin{pmatrix} -1 \\ 1 \end{pmatrix}\right) = a\begin{pmatrix} 0{,}18 \\ 0{,}82 \end{pmatrix} + b(-0{,}1)^n\begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

Druhý sčítanec se pro $n \to \infty$ blíží nule, a proto se stav ustálí na $a\begin{pmatrix} 0{,}18 \\ 0{,}82 \end{pmatrix}$, tedy složce počátečního vektoru ve směru prvního vlastního vektoru. Koeficient $a$ lze jednoduše vyjádřit pomocí počátečních počtů aut: $a = \frac{x_B + x_P}{1{,}1}$. □

**3.23. Studenti na přednášce.** Studenty můžeme rozdělit řekněme do tří skupin - na ty, co jsou přítomni na přednášce a vnímají, na ty, co jsou rovněž přítomni, ale nevnímají, a na ty, co sedí místo přednášky v hospodě. Nyní budeme hodinu po hodině sledovat, jak se mění počty studentů v těchto skupinách. Základem je vypozorovat, jaké jsou jednotlivé pravděpodobnosti změn stavu studenta. Dejme tomu, že by to mohlo být následovně:

Nyní už je možné snadno pochopit detaily důkazu spektrálního rozkladu ortogonálního zobrazení z 2.51 na konci druhé kapitoly — reálnou matici ortogonálního zobrazení interpretujeme jako matici unitárního zobrazení na komplexním rozšíření euklidovského prostoru a pečlivě sledujeme důsledky struktury kořenů reálného charakteristického polynomu nad komplexním oborem. Automaticky přitom dostáváme invariantní dvourozměrné podprostory zadané dvojicemi komplexně sdružených vlastních čísel a tedy příslušné rotace pro zúžené původní reálné zobrazení.

**3.27. Duální a adjungovaná zobrazení.** Při diskusi vektorových



prostorů a lineárních zobrazení jsme již ve druhé kapitole letmo zmínili duální vektorový prostor $V^*$ všech lineárních forem na vektorovém prostoru $V$, viz 2.39.

Pro každé lineární zobrazení mezi vektorovými prostory $\psi : V \to W$ můžeme přirozeně definovat jeho *duální zobrazení* $\psi^* : W^* \to V^*$ vztahem

$$\langle v, \psi^*(\alpha)\rangle = \langle \psi(v), \alpha\rangle, \tag{3.6}$$

kde $\langle\ ,\ \rangle$ značí vyčíslení formy (druhý argument) na vektoru (první argument), $v \in V$ a $\alpha \in W^*$ jsou libovolné.

Zvolme si báze $\underline{v}$ na $V$, $\underline{w}$ na $W$ a pišme $A$ pro matici zobrazení $\psi$ v těchto bázích. Pak snadno spočteme matici zobrazení $\psi^*$ v příslušných duálních bázích na duálních prostorech. Skutečně, definiční vztah říká, že pokud bychom reprezentovali vektory z $W^*$ v souřadnicích jako řádky skalárů, pak je zobrazení $\psi^*$ je dáno touž maticí jako $\psi$, pokud jí násobíme řádkové vektory zprava:

$$\langle \psi(v), \alpha\rangle = (\alpha_1, \ldots, \alpha_n) \cdot A \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \langle v, \psi^*(\alpha)\rangle.$$

To znamená, že maticí duálního zobrazení $\psi^*$ je transponovaná matice $A^T$, protože $\alpha \cdot A = (A^T \cdot \alpha^T)^T$.

Předpokládejme nadále, že se pohybujeme ve vektorovém prostoru se skalárním součinem. Jestliže tedy zvolíme pevně jeden vektor $v \in V$, dosazování vektorů za druhý argument ve skalárním součinu nám dává zobrazení $V \to V^* = \mathrm{Hom}(V, \mathbb{K})$

$$V \ni v \mapsto (w \mapsto \langle v, w\rangle \in \mathbb{K}).$$



Podmínka nedegenerovanosti skalárního součinu nám zaručuje, že toto zobrazení je bijekcí. Zároveň víme, že jde skutečně o lineární zobrazení nad komplexními nebo reálnými skaláry, protože jsme pevně zvolili druhý argument. Na první pohled je vidět, že vektory ortonormální báze jsou takto zobrazeny na formy tvořící bázi duální, a každý vektor můžeme prostřednictvím skalárního součinu chápat také jako lineární formu.

V případě vektorových prostorů se skalárním součinem proto převádí naše ztotožnění vektorového prostoru se svým duálem také duální zobrazení $\psi^*$ na zobrazení $\psi^* : W \to V$ zadané formulí

$$\langle \psi(u), v\ \rangle = \langle u, \psi^*(v)\rangle, \tag{3.7}$$

kde stejným značením závorek jako v definičním vztahu (3.6) nyní myslíme skalární součin. Tomuto zobrazení se říká *adjungované zobrazení* k $\psi$.

Ekvivalentně lze brát vztah (3.27) za definici adjungovaného zobrazení $\psi^*$, např. dosazením všech dvojic vektorů ortonormální

Student, který vnímá: s pravděpodobností 50% zůstane vnímat, 40% přestane vnímat a 10% odejde do hospody. Student, který je na přednášce a nevnímá: začne vnímat s pravděpodobností 10%, zůstane ve stejném stavu 50%, odejde do hospody 40%. Student, který sedí v hospodě má nulovou pravděpodobnost, že se vrátí na přednášku.

Jak se bude tento model vyvíjet v čase? Jak se situace změní, pokud budeme předpokládat aspoň desetiprocentní pravděpodobnost toho, že se student vrátí z hospody na přednášku (tu ovšem samozřejmě nevnímá)?

**Řešení.** Ze zadání se jedná o Markovův proces s maticí

$$\begin{pmatrix} 0{,}5 & 0{,}1 & 0 \\ 0{,}4 & 0{,}5 & 0 \\ 0{,}1 & 0{,}4 & 1 \end{pmatrix}.$$

Její charakteristický polynom je $(0{,}5-\lambda)^2(1-\lambda)-0{,}4(1-\lambda)$. Evidentně je tedy 1 vlastní číslo této matice (další kořeny jsou pak 0,3 a 0,7). Postupem času se tedy studenti rozdělí do skupin tak, že stav bude popsán příslušným vlastním vektorem. Ten je řešením rovnice

$$\begin{pmatrix} -0{,}5 & 0{,}1 & 0 \\ 0{,}4 & -0{,}5 & 0 \\ 0{,}1 & 0{,}4 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0,$$

což jsou právě násobky vektoru (0, 0, 1). Jinými slovy, všichni studenti po čase skončí v hospodě.

Tento výsledek je zřejmý i bez počítání - tím, že je nulová pravděpodobnost odchodu studenta do školy, se budou studenti postupně hromadit v hospodě. Přidáním desetiprocentní možnosti odchodu studenta do školy se toto změní. Příslušná matice bude

$$\begin{pmatrix} 0{,}5 & 0{,}1 & 0 \\ 0{,}4 & 0{,}5 & 0{,}1 \\ 0{,}1 & 0{,}4 & 0{,}9 \end{pmatrix}.$$

Opět platí, že se stav ustálí na vlastním vektoru příslušnému vlastnímu číslu 1. Ten je v tomto případě řešením rovnice

$$\begin{pmatrix} -0{,}5 & 0{,}1 & 0 \\ 0{,}4 & -0{,}5 & 0{,}1 \\ 0{,}1 & 0{,}4 & -0{,}1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0.$$

Řešením je například vektor (1, 5, 21). Poměrné rozložení studentů v jednotlivých skupinách pak dá násobek tohoto vektoru, který má součet složek roven 1, tj. vektor $\left(\frac{1}{27}, \frac{5}{27}, \frac{21}{27}\right)$. Opět tedy většina studentů skončí v hospodě, někteří ale ve škole budou. □

**3.24. Ruleta.** Hráč rulety má následující strategii: přišel hrát se 100 Kč. Vždy všechno, co aktuálně má, sází vždy na černou (v ruletě je 37 čísel, z toho je 18 černých, 18 červených a nula). Hráč skončí, pokud nic nemá, nebo pokud získá 800 Kč. Uvažte tuto úlohu jako Markovův proces a napište jeho matici.

báze za vektory $u$ a $v$ dostáváme přímo všechny hodnoty matice zobrazení $\psi^*$.

Předchozí výpočet pro duální zobrazení v souřadnicích nyní můžeme zopakovat, pouze musíme mít na paměti, že v ortonormálních bázích na unitárních prostorech vystupují souřadnice druhého argumentu konjugované:

$$\langle \psi(v), w\rangle = \overline{(w_1,\dots,w_n)} \cdot A \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} =$$

$$= \overline{\left(\bar{A}^T \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}\right)^T} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \langle v, \psi^*(w)\rangle.$$

Vidíme proto, že je-li $A$ matice zobrazení $\psi$ v ortonormální bázi, pak matice adjungovaného zobrazení $\psi^*$ je matice transponovaná a konjugovaná, kterou značíme $A^* = \bar{A}^T$.

Matici $A^*$ se říká *adjungovaná matice* k matici $A$. Všimněme si, že adjungované matice jsou dobře definované pro jakékoliv obdélníkové matice a nepleťme si je s maticemi algebraicky adjungovanými, které jsme u čtvercových matic používali při úvahách o determinantech.

Můžeme si tedy shrnout, že má-li jakékoliv lineární zobrazení $\psi : V \to W$ mezi unitárními prostory v ortonormálních bázích matici $A$, bude mít jeho duální zobrazení v bázích duálních matici $A^T$. Pokud přitom ztotožníme pomocí skalárního součinu vektorové prostory s jejich duálními prostory, pak nám duální zobrazení představuje adjungované zobrazení $\psi^* : W \to V$ (které je zvykem značit stejně jako to zobrazení duální), které ale má matici $A^*$. Rozdíl mezi maticemi duálního a adjungovaného zobrazení je tedy v dodatečné konjugaci, ta ale samozřejmě je důsledkem toho, že ztotožnění unitárního prostoru s jeho duálním prostorem není komplexně lineární zobrazení (neboť z druhé pozice ve skalárním součinu se skaláry vytýkají konjugované).

**3.28. Samoadjungovaná zobrazení.** Zvláštním případem lineárních zobrazení jsou tedy ta, která splývají se svým adjungovaným zobrazením: $\psi^* = \psi$. Takovým zobrazením říkáme *samoadjungovaná*. Ekvivalentně můžeme říci, že jsou to ta zobrazení, jejichž matice $A$ v jedné a tedy ve všech ortonormálních bázích splňují $A = A^*$.



V případě euklidovských prostorů jsou samoadjungovaná zobrazení tedy ta, která mají v některé ortonormální bázi (a pak už všech) symetrickou matici. Často se jim proto říká *symetrické matice* a *symetrická zobrazení*.

V komplexním oboru se maticím splňujícím $A = A^*$ říká *hermiteovské matice*. Občas se také hermiteovským maticím říká *samoadjungované matice*. Všimněme si, že hermiteovské matice tvoří reálný vektorový podprostor v prostoru všech komplexních matic, není však podprostorem v komplexním oboru.

**Poznámka.** Obzvlášť zajímavý je v této souvislosti následující postřeh. Jestliže hermiteovskou matici $A$ vynásobíme imaginární jednotkou, dostáváme matici $B = i\,A$, která má vlastnost $B^* = \bar{i}\,\bar{A}^T = -B$. Takovým maticím říkáme anti–hermiteovské. Tak jako je tedy každá reálná matice součtem své symetrické a

**Řešení.** V průběhu a na konci hry může mít hráč pouze následující peněžní obnosy (v Kč): 0, 100, 200, 400, 800. Budeme-li na danou situaci nahlížet jako na Markovův proces, toto budou jeho stavy a snadno také sestavíme jeho matici:

$$A = \begin{pmatrix} 1 & a & a & a & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 \\ 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & b & 1 \end{pmatrix},$$

kde $a = \frac{19}{37}$ a $b = \frac{18}{37}$.Všimněme si, že matice je pravděpodobnostní a singulární. Vlastní hodnota 1 je dvojnásobná. Hra nebude konvergovat k jedinému vektoru $x_\infty$, nýbrž skončí na jednom z vlastních vektorů příslušných vlastní hodnotě 1, totiž $(1, 0, 0, 0, 0)$ (hráč prohraje vše), nebo $(0, 0, 0, 0, 1)$ (hráč vyhraje 800 Kč). Navíc snadno nahlédneme, že hra skončí po třech sázkách, tedy posloupnost $\{A^n\}_{n=1}^{\infty}$, je konstantní pro $n \geq 3$:

$$A^\infty := A^3 = A^n = \begin{pmatrix} 1 & a+ab+ab^2 & a+ab & a & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & b^3 & b^2 & b & 1 \end{pmatrix}$$

a snadno zjistíme, že hra skončí s pravděpodobností $a + ab + ab^2 \doteq 0{,}885$ prohrou a s pravděpodobností cca 0,115 výhrou 800 Kč. (Maticí $A^\infty$ vynásobíme počáteční vektor $(0, 1, 0, 0, 0)$ a dostáváme vektor $(a + ab + ab^2, 0, 0, 0, b^3)$.) □

*3.25.* Uvažujme situaci z předchozího případu a předpokládejme, že pravděpodobnost výhry i prohry je 1/2. Označme matici procesu $A$. Bez použití výpočetního software určete $A^{100}$. ○

**3.26. Roztržitý profesor.** Uvažujme následující situaci: Roztržitý profesor s sebou nosí deštník, ale s pravděpodobností 1/2 jej zapomene tam, odkud odchází. Ráno odchází do práce. V práci chodí na oběd do restaurace a zpět. Po skončení práce odchází domů. Uvažujme pro jednoduchost, že nikam jinam po dostatečně dlouhou dobu profesor nechodí a že v restauraci zůstává deštník na profesorově oblíbeném místě, odkud si ho může následující den vzít (pokud nezapomene). Uvažte tuto situaci jako Markovův proces a napište jeho matici. Jaká je pravděpodobnost, že se po mnoha dnech po ránu deštník bude nalézat v restauraci? (Je vhodné za časovou jednotku vzít jeden den – od rána do rána.)

**Řešení.** Platí

$$A = \begin{pmatrix} 11/16 & 3/8 & 1/4 \\ 3/16 & 3/8 & 1/4 \\ 1/8 & 1/4 & 1/2 \end{pmatrix}.$$

antisymetrické části

$$A = \frac{1}{2}\left(A + A^T\right) + \frac{1}{2}\left(A - A^T\right),$$

je v komplexním oboru obdobně

$$A = \frac{1}{2}\left(A + A^*\right) + i\frac{1}{2i}\left(A - A^*\right),$$

a můžeme proto vyjádřit každou komplexní matici právě jedním způsobem jako součet

$$A = B + i\,C$$

s hermiteovskými maticemi $B$ a $C$. Jde o obdobu rozkladu komplexního čísla na reálnou a ryze imaginární komponentu a skutečně se často v literatuře setkáme i se značením

$$B = \operatorname{re} A = \frac{1}{2}\left(A + A^*\right),\ C = \operatorname{im} A = \frac{1}{2i}\left(A - A^*\right).$$

V řeči lineárních zobrazení to tedy znamená, že každý komplexní lineární automorfismus můžeme takto jednoznačně vyjádřit pomocí dvou samoadjungovaných zobrazení.

**3.29. Spektrální rozklad.** Uvažujme samoadjungované zobra-



zení $\psi : V \to V$ s maticí $A$ v nějaké ortonormální bázi a zkusme postupovat obdobně jako v 2.51. Opět se nejprve obecně podíváme na invariantní podprostory samoadjungovaných zobrazení a jejich ortogonální doplňky. Jestliže pro libovolný podprostor $W \subseteq V$ a samoadjungované zobrazení $\psi : V \to V$ platí $\psi(W) \subseteq W$, pak také platí pro všechny $v \in W^\perp$, $w \in W$

$$\langle \psi(v), w\rangle = \langle v, \psi(w)\rangle = 0.$$

To ale znamená, že také $\psi(W^\perp) \subseteq W^\perp$.

Uvažme nyní matici $A$ samoadjungovaného zobrazení v nějaké ortonormální bázi a nějaký vlastní vektor $x \in \mathbb{C}^n$, tj. $A \cdot x = \lambda x$. Dostáváme

$$\lambda\langle x, x\rangle = \langle Ax, x\rangle = \langle x, Ax\rangle = \langle x, \lambda x\rangle = \bar{\lambda}\langle x, x\rangle.$$

Kladným reálným číslem $\langle x, x\rangle$ můžeme krátit, a proto musí být $\bar{\lambda} = \lambda$, tj. vlastní čísla jsou vždy reálná.

Komplexních kořenů má charakteristický polynom $\det(A - \lambda E)$ tolik, kolik je dimenze čtvercové matice $A$, a všechny jsou ve skutečnosti reálné. Dokázali jsme tak důležitý obecný výsledek:

**Tvrzení.** *Ortogonální doplněk k invariantnímu podprostoru pro samoadjungované zobrazení je také invariantní. Navíc jsou všechna vlastní čísla hermiteovské matice $A$ vždy reálná.*

Ze samotné definice je zřejmé, že zúžení samoadjungovaného zobrazení na invariantní podprostor je opět samoadjungované. Předchozí tvrzení nám tedy zaručuje, že bude vždy existovat báze $V$ z vlastních vektorů. Skutečně, zúžení $\psi$ na ortogonální doplněk invariantního podprostoru je opět samoadjungované zobrazení, takže můžeme do báze přibírat jeden vlastní vektor za druhým, až dostaneme celý rozklad $V$. Vlastní vektory příslušející různým vlastním číslům jsou navíc kolmé, protože z rovností $\psi(u) = \lambda u$, $\psi(v) = \mu v$ vyplývá

$$\lambda\langle u, v\rangle = \langle \psi(u), v\rangle = \langle u, \psi(v)\rangle = \bar{\mu}\langle u, v\rangle = \mu\langle u, v\rangle.$$

Obvykle bývá náš výsledek formulován pomocí projekcí na vlastní podprostory. O projektoru $P : V \to V$ říkáme, že je *kolmý*,

Spočítejme třeba prvek $a_1^1$, tedy pravděpodobnost, že deštník začne den doma a skončí doma (bude tam i druhý den ráno): deštník může putovat třemi disjunktními cestami:

D Profesor ho hned ráno zapomene doma: $p_1 = \frac{1}{2}$.

DPD Profesor si ho vezme do práce, pak ho zapomene vzít na oběd a poté ho večer odnese domů: $p_2 = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$.

DPRPD Profesor bere deštník všude a nikde ho nezapomene: $p_3 = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{16}$.

Celkem $a_1^1 = p_1 + p_2 + p_3 = \frac{11}{16}$.

Vlastní vektor této matice příslušný dominantní vlastní hodnotě 1 je (2, 1, 1), je tedy hledaná pravděpodobnost $1/(2+1+1) = 1/4$. □

**3.27. Algoritmus na určování důležitosti stránek.** Internetové vyhledávače umí na internetu vyhledat (skoro) všechny stránky obsahující dané slovo či frázi. Jak ale setřídit vyhledané stránky tak, aby uživatel dostal pokud možno seznam seřazený podle relevance daných stránek? Jednou z možností je následující algoritmus: soubor všech nalezených stránek považujme za systém a každou z nalezených stránek za jeden z jeho možných stavů. Popíšeme náhodné procházení těchto stránek jako Markovův proces. Pravděpodobnosti přechodu mezi jednotlivými stránkami jsou dány odkazy: každý odkaz, řekněme ze stránky A na stránku B určuje pravděpodobnost (1/(celkový počet odkazů ze stránky A)), se kterou se dostaneme ze stránky A na stránku B. Pokud z některé stránky nevedou žádné odkazy, tak ji uvažujeme jako stránku, ze které vedou odkazy na všechny ostatní. Tímto dostaneme pravděpodobnostní matici $M$ (prvek $m_{ij}$ odpovídá pravděpodobnosti, se kterou se dostaneme z $i$-té stránky na $j$-tou). Bude-li tedy člověk náhodně klikat na odkazy v nalezených stránkách (pokud se dostane na stránku, ze které nevede odkaz, vybere si náhodně další), tak pravděpodobnost toho, že se v daný okamžik (dostatečně vzdálený od počátku klikání) bude nalézat na $i$-té stránce odpovídá $i$-té složce jednotkového vlastního vektoru matice M, odpovídajícího vlastnímu číslu 1. Podle velikosti těchto pravděpodobností pak určíme důležitost jednotlivých stránek.

Tento algoritmus lze modifikovat tím, že budeme předpokládat, že uživatel po nějaké době přestane klikat z odkazu na odkaz a opět začne náhodně na nějaké nové stránce. Řekněme, že s pravděpodobností $d$ vybere náhodně novou stránku a s pravděpodobností $(1-d)$ klikne na nějaký odkaz na ní. V takovéto situaci je nyní pravděpodobnost přechodu mezi libovolnými dvěma stránkami $S_i$ a $S_j$ nenulová, je to totiž $d/n + (1-d)/$(celkový počet odkazů ze stránky $S_i$), pokud je-li $\operatorname{Im} P \perp \operatorname{Ker} P$. Dva kolmé projektory $P$, $Q$ jsou *vzájemně kolmé*, je-li $\operatorname{Im} P \perp \operatorname{Im} Q$.

**Věta** (O spektrálním rozkladu)**.** *Pro každé samoadjungované zobrazení $\psi : V \to V$ na vektorovém prostoru se skalárním součinem existuje ortonormální báze z vlastních vektorů. Jsou-li $\lambda_1, \dots, \lambda_k$ všechna různá vlastní čísla $\psi$ a $P_1, \dots, P_k$ příslušné kolmé a navzájem kolmé projektory na vlastní podprostory k odpovídajícím vlastním číslům, pak*

$$\psi = \lambda_1 P_1 + \cdots + \lambda_k P_k.$$

*Dimenze obrazů těchto projektorů je přitom vždy rovna algebraické násobnosti vlastních čísel $\lambda_i$.*

**3.30. Ortogonální diagonalizace.** Zobrazení, pro která lze najít



ortonormální bázi jako v předchozí větě o spektrálním rozkladu, se nazývají *ortogonálně diagonalizovatelná*. Jsou to samozřejmě právě ta zobrazení, pro která umíme najít ortonormální bázi tak, aby v ní jejich matice zobrazení byla diagonální. Zamysleme se, jak mohou vypadat.

Pro euklidovský případ je to snadné: diagonální matice jsou zejména symetrické, jedná se tedy právě o samoadjungovaná zobrazení. Jako důsledek získáváme tvrzení, že ortogonální zobrazení euklidovského prostoru do sebe je ortogonálně diagonalizovatelné, právě když je zároveň samoadjungované (jsou to právě ta samoadjungovaná zobrazení s vlastními hodnotami $\pm 1$).

U komplexních unitárních prostorů je situace složitější. Uvažme libovolné lineární zobrazení $\varphi : V \to V$ unitárního prostoru a nechť $\varphi = \psi + i\eta$ je (jednoznačně daný) rozklad $\varphi$ na hermiteovskou a anti-hermiteovskou část. Má-li $\varphi$ ve vhodné ortonormální bázi diagonální matici $D$, pak $D = \mathrm{re}D + i\,\mathrm{im}D$, kde reálná a imaginární část jsou právě matice $\psi$ a $\eta$ (plyne z jednoznačnosti rozkladu). Zejména tedy platí $\psi \circ \eta = \eta \circ \psi$ a také $\varphi \circ \varphi^* = \varphi^* \circ \varphi$. Zobrazení $\varphi : V \to V$ s poslední uvedenou vlastností se nazývají *normální*.

Vzájemné souvislosti ukazuje následující věta (pokračujeme ve značení tohoto odstavce):

**Tvrzení.** *Následující podmínky jsou ekvivalentní:*

*(1) $\varphi$ je ortogonálně diagonalizovatelné,*
*(2) $\varphi^* \circ \varphi = \varphi \circ \varphi^*$ (tj. $\varphi$ je normální zobrazení),*
*(3) $\psi \circ \eta = \eta \circ \psi$,*
*(4) Pro matici $A = (a_{ij})$ zobrazení $\varphi$ v nějaké ortonormální bázi a jejích $m = \dim V$ vlastních čísel $\lambda_i$ platí $\sum_{i,j} |a_{ij}|^2 = \sum_{i=1}^{m} |\lambda_i|^2$.*

Důkaz. Implikaci (1) $\Rightarrow$ (2) jsme již diskutovali.

(2) $\Leftrightarrow$ (3): Stačí provést přímý výpočet

$$\varphi\varphi^* = (\psi + i\eta)(\psi - i\eta) = \psi^2 + \eta^2 + i(\eta\psi - \psi\eta),$$
$$\varphi^*\varphi = (\psi - i\eta)(\psi + i\eta) = \psi^2 + \eta^2 + i(\psi\eta - \eta\psi).$$

Odečtením dostaneme $2i(\eta\psi - \psi\eta)$.

(2) $\Rightarrow$ (1): Nechť $u \in V$ je vlastní vektor normálního zobrazení $\varphi$. Pak

$$\varphi(u) \cdot \varphi(u) = \langle \varphi^*\varphi(u), u\rangle = \langle \varphi\varphi^*(u), u\rangle = \varphi^*(u) \cdot \varphi^*(u),$$

zejména tedy $|\varphi(u)| = |\varphi^*(u)|$. Je-li $\varphi$ normální, komutuje také s $(\varphi - \lambda\,\mathrm{id}\,V)^* = (\varphi^* - \bar{\lambda}\,\mathrm{id}\,V)$ a je proto i $(\varphi - \lambda\,\mathrm{id}\,V)$ normální zobrazení. Z předešlé rovnosti tedy plyne, že je-li $\varphi(u) = \lambda u$, pak

ze stránky $S_i$ vede odkaz na $S_j$, pokud ne, tak je tato pravděpodobnost $d/n$ ($1/n$, pokud z $S_i$ nevedou žádné odkazy). Podle Frobeniovy-Perronovy věty je vlastní hodnota 1 jednonásobná a dominantní, takže jí odpovídající vlastní vektor je jediný (pokud bychom volili pravděpodobnosti přechodu pouze způsobem z předchozího odstavce, tak by tomu tak nemuselo být).

Pro názornost uvažme stránky $A$, $B$, $C$ a $D$. Odkazy vedou z $A$ na $B$ a na $C$, z $B$ na $C$ a z $C$ na $A$, z $D$ pak nikam. Uvažujme, že pravděpodobnost toho, že uživatel náhodně zvolí novou stránku je 1/5. Potom by matice $M$ vypadala následovně:

$$M = \begin{pmatrix} 1/20 & 1/20 & 17/20 & 1/4 \\ 9/20 & 1/20 & 1/20 & 1/4 \\ 9/20 & 17/20 & 1/20 & 1/4 \\ 1/20 & 1/20 & 1/20 & 1/4 \end{pmatrix}.$$

Vlastní vektor příslušný vlastní hodnotě 1 je

$$(305/53, 175/53, 315/53, 1),$$

důležitost stránek tedy bude stanovena v pořadí podle velikosti jeho odpovídajících složek, tedy $C > A > B > D$.

**3.28.** Sledujte určitou vlastnost daného živočišného druhu, která je podmíněna nezávisle na pohlaví jistým genem – dvojicí alel. Každý jedinec získává po jedné alele od obou rodičů zcela náhodně a nezávisle na sobě. Existují formy genu dané různými alelami $a$, $A$. Ty určují tři možné stavy $aa$, $aA = Aa$, $AA$ vyšetřované vlastnosti.

(a) Předpokládejte, že každý jedinec jisté populace se bude rozmnožovat výhradně s jedincem jiné populace, ve které se vyskytuje pouze vlastnost podmíněná dvojicí $aA$. Právě jeden jejich (náhodně zvolený) potomek bude ponechán na stanovišti a také on se bude rozmnožovat výhradně s jedincem té jiné populace atd. Stanovte výskyt kombinací $aa$, $aA$, $AA$ v uvažované populaci po dostatečně dlouhé době.

(b) Řešte úlohu uvedenou ve variantě (a), pokud je jiná populace tvořena pouze jedinci s dvojicí alel $AA$.

(c) Náhodně zvolené dva jedince opačného pohlaví zkřížíte. Z jejich potomstva opět náhodně vyberete dva jedince opačného pohlaví, které zkřížíte. Pokud takto budete pokračovat velmi dlouho dobu, vypočtěte pravděpodobnost, že oba křížení jedinci budou mít dvojici alel $AA$, příp. $aa$ (proces křížení skončí).

(d) Řešte úlohu uvedenou ve variantě (c) bez kladení podmínky, že křížení jedinci mají stejné rodiče. Pouze tedy křížíte jedince jisté velké populace mezi sebou, potom křížíte potomky mezi sebou atd.

$\varphi^*(u) = \bar{\lambda}u$. Tzn., že $\varphi$ a $\varphi^*$ mají stejné vlastní vektory a konjugované vlastní hodnoty.

Stejně jako u samoadjungovaných teď snadno dokážeme ortogonální diagonalizovatelnost. K tomu je nutné a stačí, aby ortogonální doplněk každého vlastního podprostoru pro normální $\varphi$ byl invariantní (je totiž zúžení normálního zobrazení na invariantní podprostor opět normální). Uvažme vlastní vektor $u \in V$ s vlastní hodnotou $\lambda$, $v \in \langle u \rangle^\perp$. Platí

$$\varphi(v) \cdot u \ = v \cdot \varphi^*(u) = \langle v, \bar{\lambda}u \rangle = \lambda u \cdot v \ = 0$$

a tedy opět $\varphi(v) \in \langle u \rangle^\perp$.

(1) $\Leftrightarrow$ (4): Výraz $\sum_{i,j} |a_{ij}|^2$ je právě stopa matice $AA^*$, to je matice zobrazení $\varphi \circ \varphi^*$. Proto nezávisí na volbě ortonormální báze. Je-li tedy $\varphi$ diagonalizovatelné, je tento výraz roven právě $\sum_i |\lambda_i|^2$.

Opačná implikace je přímým důsledkem Schurovy věty o unitární triangulovatelnosti libovolného lineárního zobrazení $V \to V$, kterou dokážeme později v 3.37. Podle ní totiž existuje pro každé lineární zobrazení $\varphi : V \to V$ ortonormální báze, ve které má $\varphi$ horní trojúhelníkovou matici. Na její diagonále pak musí být právě všechny vlastní hodnoty $\varphi$. Jak jsme již ukázali, výraz $\sum_{i,j} |a_{ij}|^2$ nezávisí na volbě ortonormální báze, proto z předpokládané rovnosti vyplývá, že všechny prvky mimo diagonálu musí být v této matici nulové. □

V termínech matic zobrazení dostáváme: zobrazení je normální právě, když jeho matice v některé ortonormální bázi (a ekvivalentně v každé) splňuje $AA^* = A^*A$. Takové matice nazýváme *normální matice*.

**Poznámka.** Všimněme si, že pro počet s lineárními zobrazeními na komplexním unitárním prostoru lze poslední větu chápat také jako zobecnění běžných počtů s komplexními čísly v goniometrickém tvaru (roli reálných čísel zde hrají samoadjungovaná zobrazení). Roli komplexních jednotek pak hrají unitární zobrazení. Zejména si všimněme analogie k vyjádření komplexních jednotek ve tvaru $\cos t + i \sin t$ s vlastností $\cos^2 t + \sin^2 t = 1$:

**Důsledek.** *Unitární zobrazení na unitárním prostoru $V$ jsou právě ta normální zobrazení, pro která výše užívaný jednoznačný rozklad $\varphi = \psi + i\eta$ splňuje $\psi^2 + \eta^2 = \mathrm{id}\, V$.*

Důkaz. Pro unitární zobrazení $\varphi$ je $\varphi\varphi^* = \mathrm{id}\, V = \varphi^*\varphi$ a tedy $\varphi\varphi^* = (\psi + i\eta)(\psi - i\eta) = \psi^2 + 0 + \eta^2 = \mathrm{id}\, V$. Naopak, pro normální zobrazení již poslední výpočet ukazuje, že opačná implikace platí také. □

**3.31. Nezáporná zobrazení a odmocniny.** Nezáporná reálná čísla jsou právě ta, která umíme psát jako druhé mocniny. Zobecnění takového chování pro matice a zobrazení lze vidět u součinů matic $B = A^* \cdot A$ (tj. složení zobrazení $\psi^* \circ \psi$):



$$\langle B \cdot x, x \rangle = \langle A^* \cdot A \cdot x, x \rangle = \langle A \cdot x, A \cdot x \rangle \geq 0$$

pro všechny vektory $x$. Navíc zjevně

$$B^* = (A^* \cdot A)^* = A^* \cdot A \ = B.$$

Hermiteovským maticím $B$ s takovou vlastností říkáme *pozitivně semidefinitní* a pokud nastane nulová hodnota pouze pro $x = 0$, pak jim říkáme *pozitivně definitní*. Obdobně hovoříme o *pozitivně definitních* a *pozitivně semidefinitních* zobrazeních $\psi : V \to V$.

**Řešení.** Případ (a). Jedná se o Markovův proces zadaný maticí

$$T = \begin{pmatrix} 1/2 & 1/4 & 0 \\ 1/2 & 1/2 & 1/2 \\ 0 & 1/4 & 1/2 \end{pmatrix},$$

přičemž pořadí stavů odpovídá pořadí dvojic alel $aa$, $aA$, $AA$. Hodnoty v prvním sloupci plynou z toho, že potomek jedince s dvojicí alel $aa$ a jedince s dvojicí alel $aA$ má s pravděpodobností $1/2$ dvojici $aa$ a s pravděpodobností $1/2$ dvojici $aA$. Analogicky postupujeme pro třetí sloupec. Hodnoty ve druhém sloupci potom vyplývají z toho, že každý ze čtyř případů dvojic alel $aa, aA, Aa, AA$ je stejně pravděpodobný u jedince, jehož oba rodiče mají dvojici alel $aA$. Uvědomme si, že na rozdíl od počítání pravděpodobností, kdy musíme rozlišovat dvojici $aA$ od $Aa$ (která z alel pochází od kterého z rodičů), vlastnosti podmíněné dvojicemi $aA$ a $Aa$ jsou samozřejmě stejné. Pro určení výsledného stavu stačí nalézt pravděpodobnostní vektor, který přísluší vlastnímu číslu 1 matice $T$, protože matice

$$T^2 = \begin{pmatrix} 3/8 & 1/4 & 1/8 \\ 1/2 & 1/2 & 1/2 \\ 1/8 & 1/4 & 3/8 \end{pmatrix}$$

splňuje podmínku Perronovy-Frobeniovy věty (všechny její prvky jsou kladné). Hledaný pravděpodobnostní vektor je

$$\left(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}\right)^T,$$

což již dává pravděpodobnosti $1/4, 1/2, 1/4$ výskytu po řadě kombinací $aa$, $aA$, $AA$ po velmi dlouhé (teoreticky nekonečné) době.

Případ (b). Pro pořadí dvojic alel $AA$, $aA$, $aa$ nyní dostáváme pravděpodobnostní matici přechodu

$$T = \begin{pmatrix} 1 & 1/2 & 0 \\ 0 & 1/2 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Ihned vidíme všechna vlastní čísla $1$, $1/2$ a $0$ (odečteme-li je od diagonály, hodnost obdržené matice nebude 3, tj. touto maticí zadaná homogenní soustava bude mít netriviální řešení). Těmto vlastním číslům přísluší po řadě vlastní vektory

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}.$$

Proto je

$$T = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}^{-1} =$$
$$= \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Pro každé pozitivně semidefinitní zobrazení $\psi : V \to V$ umíme najít jeho odmocninu, tj. zobrazení $\eta$ takové, že $\eta \circ \eta = \psi$. Nejjednodušeji to uvidíme v ortonormální bázi, ve které bude mít $\psi$ diagonální matici. Taková podle našich předchozích úvah vždy existuje a matice $A$ zobrazení $\psi$ v ní bude mít na diagonále nezáporná reálná vlastní čísla zobrazení $\psi$. Kdyby totiž bylo některé z nich záporné, nebyla by splněna podmínka nezápornosti již pro některý z bázových vektorů. Pak ovšem stačí definovat zobrazení $\eta$ pomocí matice $B$ s odmocninami příslušných vlastních čísel na diagonále. Dokázali jsme:

**Věta.** *Pro každou pozitivně semidefinitní matici $A \geq 0$ existuje její odmocnina*

$$B = \sqrt{A} = PDP^T,$$

*kde $P$ je vhodná ortogonální matice a $D$ je diagonální matice s odmocninami vlastních čísel matice $A$ na diagonále.*

**3.32. Spektra a nilpotentní zobrazení.** Na závěr této části se vrátíme k otázce, jak se mohou chovat lineární zobrazení v úplné obecnosti. Budeme i nadále pracovat s reálnými nebo komplexními vektorovými prostory.



Připomeňme, že *spektrum lineárního zobrazení* $f : V \to V$ je posloupnost kořenů charakteristického polynomu zobrazení $f$, včetně násobností. *Algebraickou násobností* vlastní hodnoty rozumíme její násobnost jako kořenu charakteristického polynomu, *geometrická násobnost* vlastní hodnoty je dimenze příslušného podprostoru vlastních vektorů.

Lineární zobrazení $f : V \to V$ se nazývá *nilpotentní*, jestliže existuje celé číslo $k \geq 1$ takové, že iterované zobrazení $f^k$ je identicky nulové. Nejmenší číslo $k$ s touto vlastností se nazývá *stupněm nilpotentnosti* zobrazení $f$. Zobrazení $f : V \to V$ se nazývá *cyklické*, jestliže existuje báze $(u_1, \ldots, u_n)$ prostoru $V$ taková, že $f(u_1) = 0$ a $f(u_i) = u_{i-1}$ pro všechna $i = 2, \ldots, n$. Jinými slovy, matice $f$ v této bázi je tvaru

$$A = \begin{pmatrix} 0 & 1 & 0 & \ldots \\ 0 & 0 & 1 & \ldots \\ \vdots & \vdots & & \ddots \end{pmatrix}.$$

Je-li $f(v) = a \cdot v$, pak pro každé přirozené $k$ je $f^k(v) = a^k \cdot v$. Zejména tedy může spektrum nilpotentního zobrazení obsahovat pouze nulový skalár (a ten tam vždy je).

Přímo z definice plyne, že každé cyklické zobrazení je nilpotentní, navíc je jeho stupeň nilpotentnosti roven dimenzi prostoru $V$. Operátor derivování na polynomech, $D(x^k) = k\,x^{k-1}$, je příkladem cyklického zobrazení na prostorech $\mathbb{K}_n[x]$ všech polynomů stupně nejvýše $n$ nad skaláry $\mathbb{K}$.

Kupodivu to platí i naopak a každé nilpotentní zobrazení je přímým součtem cyklických. Důkaz tohoto tvrzení nám dá hodně práce, proto napřed zformulujeme výsledky, ke kterým směřujeme, a pak se teprve dáme do technické práce. Ve výsledné větě o *Jordanově rozkladu* vystupují vektorové (pod)prostory a lineární zobrazení na nich s jediným vlastním číslem $\lambda$ a maticí

$$J = \begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \ldots & \lambda \end{pmatrix}.$$

Takovýmto maticím (a odpovídajícím invariantním podprostorům) se říká *Jordanův blok*.

Odsud pro libovolné $n \in \mathbb{N}$ plyne

$$T^n = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix}^n \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2^{-n} & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Zřejmě pro velká $n \in \mathbb{N}$ můžeme nahradit $2^{-n}$ za 0, což implikuje

$$T^n \approx \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Pokud tedy plodí potomky jedinci původní populace výhradně s členy populace, ve které se vyskytuje pouze dvojice alel $AA$, nutně po dostatečně velkém počtu křížení dojde k tomu, že dvojice $aA$ a $aa$ zcela vymizí (bez ohledu na jejich původní četnost).

Případ (c). Tentokráte budeme mít 6 možných stavů (v tomto pořadí)

$$AA, AA; \qquad aA, AA; \qquad aa, AA;$$
$$aA, aA; \qquad aa, aA; \qquad aa, aa,$$

přičemž tyto stavy jsou dány různými případy genotypů rodičů. Matice odpovídajícího Markovova řetězce je

$$T = \begin{pmatrix} 1 & 1/4 & 0 & 1/16 & 0 & 0 \\ 0 & 1/2 & 0 & 1/4 & 0 & 0 \\ 0 & 0 & 0 & 1/8 & 0 & 0 \\ 0 & 1/4 & 1 & 1/4 & 1/4 & 0 \\ 0 & 0 & 0 & 1/4 & 1/2 & 0 \\ 0 & 0 & 0 & 1/16 & 1/4 & 1 \end{pmatrix}.$$

Pokud budeme např. uvažovat situaci (druhý sloupce), kdy jeden z rodičů má dvojici alel $AA$ a druhý $aA$, pak zjevně může nastat každý ze čtyř případů (jde-li o dvojice alel jejich dvou náhodně zvolených potomků)

$$AA, AA; \quad AA, aA; \quad aA, AA; \quad aA, aA$$

se stejnou pravděpodobností. Pravděpodobnost setrvání ve druhém stavu je proto $1/2$ a pravděpodobnost přechodu ze druhého stavu do prvního je $1/4$ a do čtvrtého také $1/4$.

Nyní bychom měli opět určit mocniny $T^n$ pro velká $n \in \mathbb{N}$. Uvážením podoby prvního a posledního sloupce, vidíme, že

$$(1, 0, 0, 0, 0, 0)^T \quad \text{a} \quad (0, 0, 0, 0, 0, 1)^T$$

jsou vlastní vektory matice $T$ příslušné vlastnímu číslu 1. Přechodem ke čtyřrozměrné podmatici matice $T$ (vynecháním právě prvního a šestého řádku a sloupce) nalezneme poté zbylá vlastní čísla

$$\frac{1}{2}, \quad \frac{1}{4}, \quad \frac{1-\sqrt{5}}{4}, \quad \frac{1+\sqrt{5}}{4}.$$

**Věta** (Jordanova věta o kanonickém tvaru)**.** *Nechť $V$ je vektorový prostor dimenze $n$ a $f : V \to V$ je lineární zobrazení s $n$ vlastními čísly včetně algebraických násobností. Pak existuje jednoznačný rozklad prostoru $V$ na přímý součet podprostorů*

$$V = V_1 \oplus \cdots \oplus V_k$$

*takových, že $f(V_i) \subseteq V_i$, zúžení $f$ na každé $V_i$ má jediné vlastní číslo $\lambda_i$ a zúžení $f - \lambda_i \cdot \mathrm{id}$ na $V_i$ je buď cyklické nebo nulové zobrazení.*

Věta tedy říká, že ve vhodné bázi má každé lineární zobrazení blokově diagonální tvar s Jordanovými bloky podél diagonály. Celkový počet jedniček nad diagonálou v takovém tvaru je roven rozdílu mezi celkovou algebraickou a geometrickou násobností vlastních čísel.

**3.33. Poznámky.** Všimněme si, že jsme Jordanovu větu již dříve plně dokázali v případech, kdy jsou všechna vlastní čísla různá nebo když jsou geometrické a algebraické násobnosti vlastních čísel stejné. Zejména jsme ji plně dokázali pro unitární, normální a samoadjungovaná zobrazení.

Další užitečné pozorování je, že pro každé lineární zobrazení přísluší ke každému vlastnímu číslu jednoznačně určený invariantní podprostor, který odpovídá Jordanovým blokům s příslušnou vlastní hodnotou.



Také si všimněme jednoho velice užitečného důsledku Jordanovy věty (který jsme už použili u diskuse chování Markovových řetězců). Předpokládejme, že jsou vlastní hodnoty našeho zobrazení $f$ všechny v absolutní hodnotě menší než jedna. Potom opakované působení lineárního zobrazení na jakémkoliv vektoru $v \in V$ vede k rychlému zmenšování všech souřadnic $f^k(v)$ nad všechny meze. Skutečně, předpokládejme pro jednoduchost, že na celém $V$ má zobrazení $f$ jediné vlastní číslo $\lambda$ a $f - \lambda\,\mathrm{id}_V$ je cyklické (tj. omezujeme se na jediný Jordanův blok), a nechť $v_1, \ldots, v_\ell$ je příslušná báze. Pak podmínka z věty říká, že $f(v_2) = \lambda v_2 + v_1$, $f^2(v_2) = \lambda^2 v_2 + \lambda v_1 + \lambda v_1$, a podobně pro ostatní $v_i$ a vyšší mocniny. V každém případě při iterování dostáváme stále vyšší a vyšší mocniny $\lambda$ u všech nenulových komponent, přičemž nejnižší z nich může být nejvýše o stupeň nilpotentnosti nižší než násobnost iterace.

Tím je tvrzení dokázáno (a stejný argument s absolutní hodnotou vlastních čísel ostře větší než jedna vede k neomezenému růstu všech souřadnic iterací $f^k(v)$).



Zbytek této části třetí kapitoly je věnován důkazu Jordanovy věty a několika k tomu potřebným pojmům. Je výrazně obtížnější než dosavadní text a čtenář jej může případně přeskočit až do začátku 5. části této kapitoly.

**3.34. Kořenové prostory.** Na příkladech jsme viděli, že vlastní podprostory popisují dostatečně geometrické vlastnosti jen některých lineárních zobrazení. Zavedeme nyní jemnější nástroj, tzv. kořenové podprostory.

**Definice.** Nenulový vektor $u \in V$ se nazývá *kořenovým vektorem* lineárního zobrazení $\varphi : V \to V$, jestliže existuje $a \in \mathbb{K}$ a celé číslo $k > 0$ takové, že $(\varphi - a \cdot \mathrm{id}_V)^k(u) = 0$, tj. $k$–tá iterace uvedeného zobrazení zobrazuje $u$ na nulu. Množinu všech kořenových

Vzpomeneme-li si na řešení příkladu nazvaného Mlsný hazardér, nemusíme $T^n$ počítat. V tomto příkladu jsme dostali stejné vlastní vektory příslušné číslu 1 a ostatní vlastní čísla měla rovněž absolutní hodnotu ostře menší 1 (jejich přesné hodnoty jsme nevyužívali). Dostáváme tak totožný závěr, že proces se blíží k pravděpodobnostnímu vektoru

$$(a, 0, 0, 0, 0, 1-a)^T ,$$

kde $a \in [0, 1]$ je dáno výchozím stavem. Protože pouze na první a šesté pozici výsledného vektoru mohou být nenulová čísla, stavy

$$aA, AA; \quad aa, AA; \quad aA, aA; \quad aa, aA$$

po mnohonásobném křížení vymizí. Uvědomme si dále (plyne z předešlého a z příkladu Mlsný hazardér), že pravděpodobnost toho, aby proces končil $AA$, $AA$, se rovná relativní četnosti výskytu $A$ v počátečním stavu.

Případ (d). Nechť hodnoty $a, b, c \in [0, 1]$ udávají (při zachování pořadí) relativní četnosti výskytu dvojic alel $AA, aA, aa$ v dané populaci. Chceme získat vyjádření relativních četností dvojic $AA, aA, aa$ v potomstvu populace. Probíhá-li výběr dvojic pro páření náhodně, lze při velkém počtu jedinců očekávat, že relativní četnost páření jedinců s dvojicemi alel $AA$ (u obou) je $a^2$, relativní četnost páření jedinců, z nichž jeden má dvojici alel $AA$ a druhý $aA$, je $2ab$, relativní četnost páření jedinců s dvojicemi alel $aA$ (u obou) je $b^2$ atd. Potomek rodičů s dvojicemi $AA$, $AA$ musí dvojici alel $AA$ zdědit. Pravděpodobnost, že potomek rodičů s dvojicemi $AA$, $aA$ bude mít $AA$, je zřejmě $1/2$ a pravděpodobnost, že potomek rodičů s dvojicemi $aA$, $aA$ bude mít $AA$, je pak $1/4$. Jiné případy pro potomka s dvojicí alel $AA$ uvažovat nemusíme (pokud má jeden rodič dvojici alel $aa$, potomek nemůže mít dvojici $AA$). Relativní četnost výskytu dvojice alel $AA$ v potomstvu je tedy

$$a^2 \cdot 1 + 2ab \cdot \frac{1}{2} + b^2 \cdot \frac{1}{4} = a^2 + ab + \frac{b^2}{4}.$$

Analogicky stanovíme postupně relativní četnosti dvojic $aA$ a $aa$ v potomstvu ve tvarech

$$ab + bc + 2ac + \frac{b^2}{2}$$

a

$$c^2 + bc + \frac{b^2}{4}.$$

Na tento proces můžeme nahlížet jako na zobrazení $T$, které transformuje vektor $(a, b, c)^T$. Platí

$$T : \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} a^2 + ab + b^2/4 \\ ab + bc + 2ac + b^2/2 \\ c^2 + bc + b^2/4 \end{pmatrix}.$$

vektorů příslušných k pevnému skaláru $\lambda$ doplněnou o nulový vektor nazýváme *kořenovým prostorem* příslušným ke skaláru $\lambda \in \mathbb{K}$, značíme $\mathcal{R}_\lambda$.

Je-li $u$ kořenový vektor a $k$ z definice je vybráno nejmenší možné, pak $(\varphi - a \cdot \mathrm{id}_V)^{k-1}(u)$ je vlastní vektor s vlastní hodnotou $a$. Je tedy $\mathcal{R}_\lambda = \{0\}$ pro všechny skaláry $\lambda$, které neleží ve spektru zobrazení $\varphi$.

**Tvrzení.** *Pro lineární zobrazení $\varphi : V \to V$ platí:*

*(1) Pro každé $\lambda \in \mathbb{K}$ je $\mathcal{R}_\lambda \subseteq V$ vektorový podprostor.*

*(2) Pro každé $\lambda, \mu \in \mathbb{K}$ je $\mathcal{R}_\lambda$ invariantní vzhledem k lineárnímu zobrazení $(\varphi - \mu \cdot \mathrm{id}_V)$, zejména tedy je $\mathcal{R}_\lambda$ invariantní vzhledem k $\varphi$.*

*(3) Je-li $\mu \neq \lambda$, pak $(\varphi - \mu \cdot \mathrm{id}_V)|_{\mathcal{R}_\lambda}$ je invertibilní.*

*(4) Zobrazení $(\varphi - \lambda \cdot \mathrm{id}_V)|_{\mathcal{R}_\lambda}$ je nilpotentní.*

Důkaz. (1) Ověření vlastností vektorového podprostoru je jednoduché a ponecháváme jej čtenáři.

(2) Předpokládejme, že $(\varphi - \lambda \cdot \mathrm{id}_V)^k(u) = 0$ a uvažme $v = (\varphi - \mu \cdot \mathrm{id}_V)(u)$. Pak

$$\begin{aligned}(\varphi - \lambda \cdot \mathrm{id}_V)^k(v) &= \\ &= (\varphi - \lambda \cdot \mathrm{id}_V)^k((\varphi - \lambda \cdot \mathrm{id}_V) + (\lambda - \mu) \cdot \mathrm{id}_V)(u) = \\ &= (\varphi - \lambda \cdot \mathrm{id}_V)^{k+1}(u) + (\lambda - \mu) \cdot (\varphi - \lambda \cdot \mathrm{id}_V)^k(u) = \\ &= 0.\end{aligned}$$

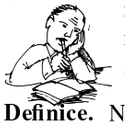
(3) Je-li $u \in \mathrm{Ker}(\varphi - \mu \cdot \mathrm{id}_V)|_{\mathcal{R}_\lambda}$, pak

$$(\varphi - \lambda \cdot \mathrm{id}_V)(u) = (\varphi - \mu \cdot \mathrm{id}_V)(u) + (\mu - \lambda) \cdot u = (\mu - \lambda) \cdot u.$$

Odtud $0 = (\varphi - \lambda \cdot \mathrm{id}_V)^k(u) = (\mu - \lambda)^k \cdot u$ a je tedy nutně $u = 0$ pro $\lambda \neq \mu$.

(4) Zvolme bázi $e_1, \ldots, e_p$ podprostoru $\mathcal{R}_\lambda$. Protože podle definice existují čísla $k_i$ taková, že $(\varphi - \lambda \cdot \mathrm{id}_V)^{k_i}(e_i) = 0$, je nutně celé zobrazení $(\varphi - \lambda \cdot \mathrm{id}_V)|_{\mathcal{R}_\lambda}$ nilpotentní. □

**3.35. Faktorové prostory.** Naším dalším cílem je ukázat, že dimenze kořenových prostorů je vždy rovna algebraické násobnosti příslušných vlastních čísel. Nejprve však zavedeme šikovné technické nástroje.



**Definice.** Nechť $U \subseteq V$ je vektorový podprostor. Na množině všech vektorů ve $V$ definujeme ekvivalenci takto: $v_1 \sim v_2$ právě tehdy, když $v_1 - v_2 \in U$. Axiomy ekvivalence jdou ověřit snadno. Množina $V/U$ tříd této ekvivalence, spolu s operacemi definovanými pomocí reprezentantů, tj. $[v]+[w] = [v+w]$, $a \cdot [u] = [a \cdot u]$, tvoří vektorový prostor, který nazýváme *faktorový vektorový prostor* prostoru $V$ podle podprostoru $U$.

Ověřte si korektnost definice operací a platnost všech axiomů vektorového prostoru!

Třídy (vektory) ve faktorovém prostoru $V/U$ budeme často označovat jako formální součet jednoho reprezentanta se všemi vektory podprostoru $U$, např. $u + U \in V/U$, $u \in V$. Nulový vektor ve $V/U$ je právě třída $0 + U$, tj. vektor $u \in V$ reprezentuje nulový vektor ve $V/U$, právě když je $u \in U$.

Jako jednoduché příklady si rozmyslete $V/\{0\} \cong V$, $V/V \cong \{0\}$ a faktorový prostor roviny $\mathbb{R}^2$ podle libovolného jednorozměrného podprostoru (zde je každý jednorozměrný podprostor $U \subseteq \mathbb{R}^2$ přímkou procházející počátkem), kde třídy ekvivalence jsou rovnoběžky s touto přímkou.

Podotkněme, že za definiční obor (a pochopitelně i obor hodnot) $T$ vlastně bereme pouze vektory

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix}, \text{ kde } a, b, c \in [0, 1],\ a + b + c = 1.$$

Chtěli bychom zadat operaci $T$ pomocí násobení vektoru $(a, b, c)^T$ jistou konstantní maticí. To však očividně není možné (zobrazení $T$ není lineární). Nejedná se tedy o Markovův proces a nelze zjednodušit určování, co se stane po velmi dlouhé době, jako v předešlých případech. Můžeme ale vypočítat, co se stane, když aplikujeme zobrazení $T$ dvakrát po sobě. Ve druhém kroku dostáváme

$$T : \begin{pmatrix} a^2 + ab + b^2/4 \\ ab + bc + 2ac + b^2/2 \\ c^2 + bc + b^2/4 \end{pmatrix} \mapsto \begin{pmatrix} t_2^1 \\ t_2^2 \\ t_2^3 \end{pmatrix},$$

kde

$$\begin{aligned}
t_2^1 &= \left(a^2 + ab + \frac{b^2}{4}\right)^2 + \left(a^2 + ab + \frac{b^2}{4}\right)\left(ab + bc + 2ac + \frac{b^2}{2}\right) + \\
&\quad + \frac{1}{4}\left(ab + bc + 2ac + \frac{b^2}{2}\right)^2, \\
t_2^2 &= \left(a^2 + ab + \frac{b^2}{4}\right)\left(ab + bc + 2ac + \frac{b^2}{2}\right) + \\
&\quad + \left(ab + bc + 2ac + \frac{b^2}{2}\right)\left(c^2 + bc + \frac{b^2}{4}\right) + \\
&\quad + 2\left(a^2 + ab + \frac{b^2}{4}\right)\left(c^2 + bc + \frac{b^2}{4}\right) + \frac{1}{2}\left(ab + bc + 2ac + \frac{b^2}{2}\right)^2, \\
t_2^3 &= \left(c^2 + bc + \frac{b^2}{4}\right)^2 + \left(ab + bc + 2ac + \frac{b^2}{2}\right)\left(c^2 + bc + \frac{b^2}{4}\right) + \\
&\quad + \frac{1}{4}\left(ab + bc + 2ac + \frac{b^2}{2}\right)^2.
\end{aligned}$$

Lze ukázat (využitím $a + b + c = 1$), že

$$t_2^1 = a^2 + ab + \frac{b^2}{4},\ t_2^2 = ab + bc + 2ac + \frac{b^2}{2},\ t_2^3 = c^2 + bc + \frac{b^2}{4},$$

tj.

$$T : \begin{pmatrix} a^2 + ab + b^2/4 \\ ab + bc + 2ac + b^2/2 \\ c^2 + bc + b^2/4 \end{pmatrix} \mapsto \begin{pmatrix} a^2 + ab + b^2/4 \\ ab + bc + 2ac + b^2/2 \\ c^2 + bc + b^2/4 \end{pmatrix}.$$

Získali jsme tak překvapivý výsledek, že dalším aplikováním transformace $T$ se vektor obdržený v prvním kroku nezmění. To znamená, že výskyt uvažovaných dvojic alel je po libovolně dlouhé době totožný jako v první generaci potomstva. Pro velkou populaci jsme tak dokázali, že evoluční vývoj by se realizoval během jediné generace, kdyby nedocházelo k mutacím nebo k selekci. □

**Tvrzení.** *Nechť $U \subseteq V$ je vektorový podprostor a $(u_1, \dots, u_n)$ je taková báze $V$, že $(u_1, \dots, u_k)$ je báze $U$. Pak* $\dim V/U = n - k$ *a vektory*

$$u_{k+1} + U, \dots, u_n + U$$

*tvoří bázi $V/U$.*

Důkaz. Protože $V = \langle u_1, \dots, u_n \rangle$, je i $V/U = \langle u_1 + U, \dots, u_n + U \rangle$. Přitom ale je prvních $k$ generátorů nulových, takže je $V/U = \langle u_{k+1} + U, \dots, u_n + U \rangle$. Předpokládejme, že $a_{k+1} \cdot (u_{k+1} + U) + \dots + a_n \cdot (u_n + U) = (a_{k+1} \cdot u_{k+1} + \dots + a_n \cdot u_n) + U = 0 \in V/U$. To je ale ekvivalentní příslušnosti lineární kombinace vektorů $u_{k+1}, \dots, u_n$ do podprostoru $U$. Protože $U$ je generováno zbylými vektory, je nutně tato kombinace nulová, tj. všechny koeficienty $a_i$ jsou nulové. □

**3.36. Indukovaná zobrazení na faktorových prostorech.**



Předpokládejme, že $U \subseteq V$ je invariantní podprostor vzhledem k lineárnímu zobrazení $\varphi : V \to V$ a zvolme takovou bázi $u_1, \dots, u_n$ prostoru $V$, že prvních $k$ vektorů této báze je bází $U$. V této bázi má $\varphi$ blokovou matici $A = \left(\begin{smallmatrix} B & C \\ 0 & D \end{smallmatrix}\right)$. Pak budeme umět dokázat následující tvrzení:

**Lemma.** *(1) Zobrazení $\varphi$ indukuje lineární zobrazení $\varphi_{V/U} : V/U \to V/U$, $\varphi_{V/U}(v + U) = \varphi(v) + U$ s maticí $D$ v indukované bázi $u_{k+1} + U, \dots, u_n + U$ na $V/U$.*
*(2) Charakteristický polynom $\varphi_{V/U}$ dělí charakteristický polynom $\varphi$.*

Důkaz. Pro $v, w \in V$, $u \in U$, $a \in \mathbb{K}$ máme $\varphi(v + u) \in \varphi(v) + U$ (protože $U$ je invariantní), $(\varphi(v) + U) + (\varphi(w) + U) = \varphi(v + w) + U$ a $a \cdot (\varphi(v) + U) = a \cdot \varphi(v) + U = \varphi(a \cdot v) + U$ (protože $\varphi$ je lineární), je tedy zobrazení $\varphi_{V/U}$ dobře definované a lineární. Navíc je přímo z definice matice zobrazení patrné, že matice $\varphi_{V/U}$ v indukované bázi na $V/U$ je právě matice $D$ (při počítání obrazů bázových prvků nám koeficienty z matice $C$ přispívají pouze do třídy $U$). Charakteristický polynom indukovaného zobrazení $\varphi_{V/U}$ je tedy $|D - \lambda \cdot E|$, zatímco charakteristický polynom původního zobrazení $\varphi$ je $|A - \lambda \cdot E| = |B - \lambda \cdot E||D - \lambda \cdot E|$. □

**Důsledek.** *Nechť $V$ je vektorový prostor nad $\mathbb{K}$ dimenze $n$ a nechť $\varphi : V \to V$ je lineární zobrazení, jehož spektrum obsahuje $n$ prvků (tj. všechny kořeny charakteristického polynomu leží v $\mathbb{K}$ a počítáme je včetně násobnosti). Pak existuje posloupnost invariantních podprostorů $\{0\} = V_0 \subseteq V_1 \subseteq \dots \subseteq V_n = V$ s dimenzemi $\dim V_i = i$. V bázi $u_1, \dots, u_n$ prostoru $V$ takové, že $V_i = \langle u_1, \dots, u_i \rangle$, má $\varphi$ horní trojúhelníkovou matici:*

$$\begin{pmatrix} \lambda_1 & \dots & * \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix},$$

*kde $\lambda_1, \dots, \lambda_n$ je posloupnost prvků spektra.*

Důkaz. Konstrukci podprostorů $V_i$ provedeme induktivně. Nechť $\lambda_1, \dots, \lambda_n$ jsou prvky ve spektru zobrazení $\varphi$, tzn. charakteristický polynom zobrazení $\varphi$ je tvaru $(\lambda - \lambda_1) \cdot \dots \cdot (\lambda - \lambda_n)$. Zvolme $V_0 = \{0\}$, $V_1 = \langle u_1 \rangle$, kde $u_1$ je libovolný vlastní vektor s vlastní hodnotou $\lambda_1$. Podle předešlé věty je charakteristický polynom zobrazení $\varphi_{V/V_1}$ tvaru $(\lambda - \lambda_2) \cdot \dots \cdot (\lambda - \lambda_n)$. Předpokládejme,

**3.29.** Nechť jsou dány dvě urny, které obsahují dohromady $n$ bílých a $n$ černých koulí. V pravidelných časových intervalech je z obou uren vylosována jedna koule a přemístěna do druhé urny, přičemž počet koulí v obou urnách je na začátku (a tedy po celou dobu) právě $n$. Zadejte tento Markovův proces pravděpodobnostní maticí přechodu $T$.

**Řešení.** Tento příklad se používá ve fyzice jako model prolínání dvou nestlačitelných kapalin (již v roce 1769 ho zavedl D. Bernoulli) nebo analogicky jako model difúze plynů. Stavy $0, 1, \ldots, n$ budou odpovídat kupř. počtu bílých koulí v jedné pevně zvolené urně. Tento údaj totiž současně zadává, kolik černých koulí je ve zvolené urně (všechny ostatní koule jsou pak ve druhé z uren). Pokud v jistém kroku dojde ke změně stavu $j \in \{1, \ldots, n\}$ na $j-1$, znamená to, že ze zvolené urny byla vytažena bílá koule a z druhé černá. To se stane s pravděpodobností

$$\frac{j}{n} \cdot \frac{j}{n} = \frac{j^2}{n^2}.$$

Přechodu ze stavu $j \in \{0, \ldots, n-1\}$ do $j+1$ odpovídá vytažení černé koule ze zvolené urny a bílé z té druhé s pravděpodobností

$$\frac{n-j}{n} \cdot \frac{n-j}{n} = \frac{(n-j)^2}{n^2}.$$

Soustava zůstane ve stavu $j \in \{1, \ldots, n-1\}$, jestliže z obou uren byly vytaženy koule stejné barvy, což má pravděpodobnost

$$\frac{j}{n} \cdot \frac{n-j}{n} + \frac{n-j}{n} \cdot \frac{j}{n} = \frac{2j\,(n-j)}{n^2}.$$

Dodejme, že ze stavu 0 se nutně (s pravděpodobností 1) přechází do stavu 1 a že ze stavu $n$ se s jistotou přechází do stavu $n-1$. Uvážením výše uvedeného dostáváme hledanou matici

$$T = \frac{1}{n^2} \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ n^2 & 2\cdot 1(n-1) & 2^2 & \ddots & 0 & 0 & 0 \\ 0 & (n-1)^2 & 2\cdot 2(n-2) & \ddots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 2\cdot(n-2)2 & (n-1)^2 & 0 \\ 0 & 0 & 0 & \ddots & 2^2 & 2\cdot(n-1)1 & n^2 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

pro pořadí stavů $0, 1, \ldots, n$.

Při užití tohoto modelu ve fyzice nás samozřejmě zajímá složení uren po uplynutí určité doby (po daném počtu výměn v závislosti na předešlém složení uren). Bude-li počáteční stav např. 0, můžeme pomocí mocnin matice $T$ sledovat, s jakou pravděpodobností přibývají ve zvolené urně bílé koule. Také lze potvrdit očekávaný výsledek, že počáteční rozdělení koulí bude ovlivňovat jejich rozdělení po delší době zanedbatelným způsobem.

že jsme již sestrojili lineárně nezávislé vektory $u_1, \ldots, u_k$ a invariantní podprostory $V_i = \langle u_1 \ldots, u_i \rangle$, $i = 1, \ldots, k < n$, takové, že charakteristický polynom $\varphi_{V/V_k}$ je tvaru $(\lambda - \lambda_{k+1}) \cdot \cdots \cdot (\lambda - \lambda_n)$ a $\varphi(u_i) \in (\lambda_i \cdot u_i + V_{i-1})$ pro všechna $i = 1, \ldots, k$.

Zejména tedy existuje vlastní vektor $u_{k+1} + V_k \in V/V_k$ zobrazení $\varphi_{V/V_k}$ s vlastní hodnotou $\lambda_{k+1}$. Uvažme nyní prostor $V_{k+1} = \langle u_1, \ldots, u_{k+1} \rangle$. Kdyby byl vektor $u_{k+1}$ lineární kombinací vektorů $u_1, \ldots, u_k$, znamenalo by to, že $u_{k+1} + V_k$ je nulová třída v $V/V_k$, to ale není možné. Je proto $\dim V_{k+1} = k+1$. Zbývá studovat indukované zobrazení $\varphi_{V/V_{k+1}}$. Charakteristický polynom tohoto zobrazení je stupně $n-k-1$ a dělí charakteristický polynom zobrazení $\varphi$. Přitom doplněním vektorů $u_1, \ldots, u_{k+1}$ do báze $V$ dostaneme blokovou matici zobrazení $\varphi$ s horní trojúhelníkovou submaticí $B$ v horním levém rohu a nulou v levém dolním rohu, jejíž diagonální prvky jsou právě skaláry $\lambda_1, \ldots, \lambda_{k+1}$. Proto mají kořeny charakteristického polynomu indukovaného zobrazení požadované vlastnosti. □

**3.37. Poznámky.** Pokud existuje rozklad celého prostoru $V$ na přímý součet vlastních podprostorů, existuje báze z vlastních podprostorů a předchozí věta vlastně neříká vůbec nic zajímavého. Její síla ovšem spočívá v tom, že jediným jejím předpokladem je existence $\dim V$ kořenů charakteristického polynomu (včetně násobností). To je ovšem zaručeno, je-li pole $\mathbb{K}$ algebraicky uzavřené, např. pro komplexní čísla $\mathbb{C}$. Přímým důsledkem pak jsou zajímavá tvrzení o determinantu a stopě zobrazení: jsou vždy součinem, resp. součtem prvků ve spektru. Tuto skutečnost můžeme použít i pro všechny reálné matice. Můžeme je totiž vždy považovat za komplexní, spočítat potřebné, a protože determinant i stopa jsou algebraické výrazy v prvcích matice, výsledkem budou právě hledané reálné hodnoty.



Když je na vektorovém prostoru $V$ zadán skalární součin, můžeme v každém induktivním kroku důkazu předchozího tvrzení využít skutečnosti, že vždy $V/V_k \simeq V_k^\perp$ a $V_k^\perp \ni u \mapsto (u + V_k) \in V/V_k$. To znamená, že v každé třídě rozkladu $V/V_k$ existuje právě jeden vektor z $V_k^\perp$. Skutečně, tuto vlastnost má faktorový prostor podle libovolného podprostoru v unitárním prostoru – pokud $u, v \in V_k^\perp$ jsou v jedné třídě, pak jejich rozdíl patří do $V_k \cap V_k^\perp$, tedy jsou stejné. Můžeme tedy jako reprezentanta $u_{k+1}$ nalezené třídy, tedy vlastního vektoru $\varphi_{V/V_k}$, zvolit právě vektor z $V_k^\perp$. Touto modifikací dojdeme k ortogonální bázi s vlastnostmi požadovanými v tvrzení o triangulovatelnosti. Proto existuje i taková ortonormální báze:

**Důsledek** (Schurova věta o ortogonální triangulovatelnosti)**.** *Nechť $\varphi : V \to V$ je libovolné lineární zobrazení (reálného nebo komplexního) unitárního prostoru s $m = \dim V$ vlastními hodnotami (včetně násobnosti). Pak existuje ortonormální báze prostoru $V$ taková, že $\varphi$ v ní má horní trojúhelníkovou matici s vlastními čísly $\lambda_1, \ldots, \lambda_m$ na diagonále.*

**3.38. Věta.** *Nechť $\varphi$ $V \to V$ je lineární zobrazení. Součet kořenových prostorů*

$$\mathcal{R}_{\lambda_1}, \ldots, \mathcal{R}_{\lambda_k}$$

*příslušných různým vlastním hodnotám $\lambda_1 \ldots, \lambda_k$ je přímý. Navíc je pro každou vlastní hodnotu $\lambda$ dimenze podprostoru $\mathcal{R}_\lambda$ rovna její algebraické násobnosti.*

Kdybychom jednotlivé koule očíslovali, místo výběru po jedné kouli z uren vylosovali nějaké z čísel $1, 2, \ldots, 2n$ a kouli, jejíž číslo bylo vytaženo, přemístili do druhé urny, obdrželi bychom Markovův proces se stavy $0, 1, \ldots, 2n$ (počet koulí ve zvolené urně), kdy se tak už nerozlišuje barva koulí. Tento Markovův řetězec je rovněž ve fyzice důležitý. (P. a T. Ehrenfestovi jej zavedli v roce 1907.) Používá se jako model výměny tepla mezi dvěma izolovanými tělesy (teplota je reprezentována počtem koulí, tělesa urnami). □

Další využití Markovových řetězců viz strana (‖3.57‖).

### E. Unitární prostory

Již v minulé kapitole jsme definovali skalární součin v reálných vektorových prostorech (viz 2.40), v této kapitole rozšiřujeme jeho definici i na komplexní vektorové prostory (viz 3.23).

**3.30. Grupy O(n) a U(n).** Uvážíme-li všechna lineární zobrazení z $\mathbb{R}^3$ do $\mathbb{R}^3$, která zachovávají daný skalární součin, tedy vzhledem k definicím délky vektorů a odchylky dvou vektorů lineární zobrazení zachovávající délky a úhly, tak tato tvoří zřejmě vzhledem ke skládání zobrazení grupu (viz 1.1; složení dvou takových zobrazení je z definice zobrazení zachovávající délky a úhly, jednotkovým prvkem je identické zobrazení, inverzním prvkem k danému zobrazení je zobrazení k němu inverzní – díky podmínce na zachovávaní velikostí existuje). Matice těchto zobrazení tedy tvoří vzhledem k násobení matic grupu (viz oddíl 11.1), říkáme jí *ortogonální grupa*, značíme $0(n)$. Je to podgrupa všech invertibilních zobrazení z $\mathbb{R}^n$ do $\mathbb{R}^n$.

Požadujeme-li navíc po maticích zobrazení, aby měly determinant roven jedné, hovoříme o speciální ortogonální grupě $SO(n)$ (obecně může být determinantem matice z $O(n)$ číslo 1 či $-1$).

Obdobně definujeme *unitární grupu U(n)* jakožto grupu všech (komplexních) matic, které odpovídají komplexně lineárním zobrazením z $\mathbb{C}^n$ do $\mathbb{C}^n$, která zachovávají daný skalární součin v unitárním prostoru. Stejně pak $SU(n)$ značí podgrupu matic v $U(n)$ s jednotkovým determinantem (obecně může být determinantem libovolná komplexní jednotka).

Následující úloha vyžaduje znalost integrování komplexně hodnotové funkce jedné reálné proměnné. S tímto pojmem se seznámíme až v šesté kapitole, počínaje odstavcem 6.18. Pokud se čtenář s integrováním doposud nesetkal, může tuto úlohu s klidným svědomím přeskočit.



**3.31.** Uvažujme vektorový prostor $V$ funkcí $\mathbb{R} \to \mathbb{C}$. Určete, zda je zobrazení $\varphi$ z unitárního prostoru $V$ lineární:



Důkaz. Důkaz provedeme indukcí přes počet $k$ kořenových prostorů. Předpokládejme, že tvrzení vždy platí pro méně než $k$ prostorů a že pro vektory $u_1 \in \mathcal{R}_{\lambda_1}, \ldots, u_k \in \mathcal{R}_{\lambda_k}$ platí $u_1 + \cdots + u_k = 0$. Pro vhodné $j$ pak $(\varphi - \lambda_k \cdot \mathrm{id}_V)^j(u_k) = 0$ a zároveň jsou $y_i = (\varphi - \lambda_k \cdot \mathrm{id}_V)^j(u_i)$ nenulové vektory v $\mathcal{R}_{\lambda_i}$, $i = 1, \ldots, k-1$, pokud $u_i$ jsou nenulové, viz věta 3.34.

Přitom ale

$$y_1 + \cdots + y_{k-1} = \sum_{i=1}^{k} (\varphi - \lambda_k \cdot \mathrm{id}_V)^j(u_i) = 0$$

a tedy podle indukčního předpokladu jsou všechny $y_i$ nulové. Pak ovšem i $u_k = 0$ a lineární nezávislost je dokázána.

Zbývá ukázat, že dimenze každého kořenového prostoru $\mathcal{R}_\lambda$ je rovna algebraické násobnosti kořenu $\lambda$ charakteristického polynomu. Nechť tedy je $\lambda$ vlastní hodnota $\varphi$, označme $\bar{\varphi}$ zúžení $\varphi|_{\mathcal{R}_\lambda}$ a $\psi : V/\mathcal{R}_\lambda \to V/\mathcal{R}_\lambda$ nechť je zobrazení indukované $\varphi$ na faktorovém prostoru. Předpokládejme, že dimenze $\mathcal{R}_\lambda$ je menší než násobnost kořenu $\lambda$ charakteristického polynomu. Podle lemmatu 3.36 to znamená, že $\lambda$ je i vlastní hodnotou zobrazení $\psi$. Nechť $(v + \mathcal{R}_\lambda) \in V/\mathcal{R}_\lambda$ je příslušný vlastní vektor, tj. $\psi(v + \mathcal{R}_\lambda) = \lambda \cdot (v + \mathcal{R}_\lambda)$ což podle definice značí $v \notin \mathcal{R}_\lambda$ a $\varphi(v) = \lambda \cdot v + w$ pro vhodné $w \in \mathcal{R}_\lambda$. Máme tedy $w = (\varphi - \lambda \cdot \mathrm{id}_V)(v)$ a $(\varphi - \lambda \cdot \mathrm{id}_V)^j(w) = 0$ pro vhodné $j$. Celkem jsme dovodili $(\varphi - \lambda \cdot \mathrm{id}_V)^{j+1}(v) = 0$, což je ve sporu s volbou $v \notin \mathcal{R}_\lambda$.

Tím jsme dokázali, že dimenze $\mathcal{R}_\lambda$ je rovna násobnosti kořene $\lambda$ charakteristického polynomu $\varphi$. □

**Důsledek.** *Pro každé lineární zobrazení $\varphi : V \to V$, jehož celé spektrum je v $\mathbb{K}$, je $V = \mathcal{R}_{\lambda_1} \oplus \cdots \oplus \mathcal{R}_{\lambda_n}$ přímým součtem kořenových podprostorů. Zvolíme-li vhodně báze těchto podprostorů, pak $\varphi$ má v této bázi blokově diagonální tvar s horními trojúhelníkovými maticemi v blocích a vlastními hodnotami $\lambda_i$ na diagonále.*

**3.39. Nilpotentní a cyklická zobrazení.** Nyní již máme skoro vše připraveno pro diskusi kanonických tvarů matic. Zbývá jen vyjasnit vztah mezi cyklickými a nilpotentními zobrazeními a poskládat dohromady již připravené výsledky.



**Věta.** *Nechť $\varphi : V \to V$ je nilpotentní lineární zobrazení. Pak existuje rozklad $V$ na přímý součet podprostorů $V = V_1 \oplus \cdots \oplus V_k$ takových, že zúžení $\varphi$ na kterýkoliv z nich je cyklické.*



Důkaz. Ověření je docela přímočaré a spočívá v konstrukci takové báze prostoru $V$, že akce zobrazení $\varphi$ na bázových vektorech přímo ukazuje rozklad na cyklická zobrazení. Postup bude ale poněkud zdlouhavý.

Nechť $k$ je stupeň nilpotentnosti zobrazení $\varphi$ a označme $P_i = \mathrm{im}(\varphi^i)$, $i = 0, \ldots, k$, tzn.

$$\{0\} = P_k \subseteq P_{k-1} \subseteq \cdots \subseteq P_1 \subseteq P_0 = V.$$

Vyberme libovolnou bázi $e_1^{k-1}, \ldots, e_{p_{k-1}}^{k-1}$ prostoru $P_{k-1}$, kde $p_{k-1} > 0$ je dimenze $P_{k-1}$. Z definice plyne, že $P_{k-1} \subseteq \mathrm{Ker}\,\varphi$, tj. vždy $\varphi(e_j^{k-1}) = 0$.

Předpokládejme, že $P_{k-1} \neq V$. Protože $P_{k-1} = \varphi(P_{k-2})$, nutně existují v $P_{k-2}$ vektory $e_j^{k-2}$, $j = 1, \ldots, p_{k-1}$, takové, že

i) $\varphi(u) = \lambda u$, kde $\lambda \in \mathbb{C}$,
ii) $\varphi(u) = u^*$,
iii) $\varphi(u) = u^2 (= u.u)$,
iv) $\varphi(u) = \frac{du}{dx}$.

$V$ je pro vhodné funkce unitární prostor nekonečné dimenze. Skalárním součin se definuje vztahem $f \cdot g = \int_{-\infty}^{\infty} \overline{f(x)}\, g(x) dx$.

**3.32.** Ukažte, že pokud je $H$ hermiteovská matice, pak je

$$U = \exp(iH) = \sum_{n=0}^{\infty} (-1)^n \tfrac{1}{n!} (iH)^n$$

unitární matice a spočtěte její determinant.

**Řešení.** Z definice exp lze ukázat, že platí

$$\exp(A + B) = \exp(A) \cdot \exp(B)$$

tak, jak jsme zvyklí u exponenciálního zobrazení v oboru čísel. Vzhledem k tomu, že obecně platí $(u + v)^* = u^* + v^*$ a $(cv)^* = \bar{c} v^*$, tak dostáváme

$$U^* = \left( \sum_{n=0}^{\infty} (-1)^n \frac{1}{n!} (iH)^n \right)^* = \sum_{n=0}^{\infty} (-1)^n \frac{1}{n!} (-iH^*)^n,$$

a protože $H^* = H$, tak

$$U^* = - \sum_{n=0}^{\infty} (-1)^n \frac{1}{n!} (-iH)^n = \exp(-iH),$$

a proto

$$U^* U = \exp(iH) \exp(-iH) = \exp(0) = 1. \qquad \square$$

**3.33.** Hermiteovské matice $A, B, C$ splňují $[A, C] = [B, C] = 0$ a $[A, B] \neq 0$, kde $[,]$ je komutátor matic definovaný vztahem $[A, B] = AB - BA$. Ukažte, že aspoň jeden vlastní podprostor matice $C$ musí mít dimenzi větší než 1..

**Řešení.** Budeme dokazovat sporem. Předpokládáme tedy, že všechny vlastní podprostory operátoru $C$ mají dim $= 1$. Pak můžeme pro libovolný vektor $u$ psát $u = \sum_k c_k u_k$, kde $u_k$ jsou lineárně nezávislé normované vlastní vektory operátoru $C$ vlastním číslem $\lambda_k$ (a $c_k = u \cdot u_k$) Pro tyto vlastní vektory pak zjevně platí

$$0 = [A, C] u_k = ACu_k - CAu_k = \lambda_k Au_k - C(Au_k).$$

Odtud vidíme, že $Au_k$ je vlastním vektorem matice $C$ s vlastní hodnotou $\lambda_k$. To ovšem znamená, že $Au_k = \lambda_k^A u_k$ pro nějaké číslo $\lambda_k^A$. Stejně tak odvodíme $Bu_k = \lambda_k^B u_k$ pro nějaké číslo $\lambda_k^B$. Pro komutátor matic $A$ a $B$ pak dostáváme

$$[A, B] u_k = ABu_k - BAu_k = \lambda_k^A \lambda_k^B u_k - \lambda_k^B \lambda_k^A u_k = 0.$$

To ovšem znamená

$$[A, B] u = [A, B] \sum_k c_k u_k - \sum_k c_k [A, B] u_k = 0,$$

a protože $u$ bylo libovolné, znamená to, že $[A, B] = 0$, což je spor. $\square$

$\varphi(e_j^{k-2}) = e_j^{k-1}$. Předpokládejme

$$a_1 e_1^{k-1} + \cdots + a_{p_{k-1}} e_{p_{k-1}}^{k-1} + b_1 e_1^{k-2} + \cdots + b_{p_{k-1}} e_{p_{k-1}}^{k-2} = 0.$$

Aplikací zobrazení $\varphi$ na tuto lineární kombinaci získáme

$$b_1 e_1^{k-1} + \cdots + b_{p_{k-1}} e_{p_{k-1}}^{k-1} = 0,$$

proto jsou všechny $b_j = 0$. Pak ale i $a_j = 0$, protože se jedná o kombinaci bázových vektorů. Celkem jsme tedy ověřili lineární nezávislost všech $2p_{k-1}$ zvolených vektorů. Doplňme je do báze

$$e_1^{k-1}, \ldots, e_{p_{k-1}}^{k-1},$$
$$e_1^{k-2}, \ldots, e_{p_{k-1}}^{k-2}, e_{p_{k-1}+1}^{k-2}, \ldots, e_{p_{k-2}}^{k-2}$$

prostoru $P_{k-2}$. Navíc jsou obrazy přidaných bázových prvků v $P_{k-1}$, nutně tedy musejí být lineárními kombinacemi bázových prvků $e_1^{k-1}, \ldots, e_{p_{k-1}}^{k-1}$. Můžeme proto zaměnit zvolené vektory $e_{p_{k-1}+1}^{k-2}, \ldots, e_{p_{k-2}}^{k-2}$ vektory $e_j^{k-2} - \varphi(e_j^{k-2})$. Tím docílíme, že doplněné vektory do báze $P_{k-2}$ patří do jádra zobrazení $\varphi$. Předpokládejme to přímo o zvolené bázi.

Předpokládejme dále, že již máme sestrojenu bázi podprostoru $P_{k-\ell}$ takovou, že ji můžeme poskládat do schématu

$$\begin{array}{l}
e_1^{k-1}, \ldots, e_{p_{k-1}}^{k-1}, \\
e_1^{k-2}, \ldots, e_{p_{k-1}}^{k-2}, e_{p_{k-1}+1}^{k-2}, \ldots, e_{p_{k-2}}^{k-2}, \\
e_1^{k-3}, \ldots, e_{p_{k-1}}^{k-3}, e_{p_{k-1}+1}^{k-3}, \ldots, e_{p_{k-2}}^{k-3}, e_{p_{k-2}+1}^{k-3}, \ldots, e_{p_{k-3}}^{k-3}, \\
\vdots \\
e_1^{k-\ell}, \ldots, e_{p_{k-1}}^{k-\ell}, e_{p_{k-1}+1}^{k-\ell}, \ldots, e_{p_{k-2}}^{k-\ell}, e_{p_{k-2}+1}^{k-\ell}, \ldots, e_{p_{k-3}}^{k-\ell}, \ldots e_{p_{k-\ell}}^{k-\ell},
\end{array}$$

kde hodnota zobrazení $\varphi$ na libovolném bázovém vektoru se nachází nad ním, nebo je nulová, pokud nad zvoleným vektorem báze již nic není. Pokud je $P_{k-\ell} \neq V$, opět musí existovat vektory $e_1^{k-\ell-1}, \ldots, e_{p_{k-\ell}}^{k-\ell-1}$, které se zobrazují na $e_1^{k-\ell}, \ldots, e_{p_{k-\ell}}^{k-\ell}$ a můžeme je doplnit do báze $P_{k-l-1}$, řekněme vektory

$$e_{p_{k-\ell}+1}^{k-\ell-1}, \ldots, e_{p_{k-\ell-1}}^{k-\ell-1}.$$

Přitom postupným odečítáním hodnot iterací zobrazení $\varphi$ na těchto vektorech dosáhneme opět toho, že doplněné vektory do báze $P_{k-\ell-1}$ budou ležet v jádru $\varphi$ a analogicky jako výše ověříme, že skutečně dostaneme bázi $P_{k-\ell-1}$.

Po $k$ krocích získáme bázi celého $V$, která má vlastnosti uvedené pro bázi prostoru $P_{k-\ell}$. Jednotlivé sloupce výsledného schématu pak generují hledané podprostory $V_i$ a navíc jsme přímo našli báze těchto podprostorů ukazující, že příslušná zúžení $\varphi$ jsou cyklická zobrazení. $\square$

**3.40. Důkaz Jordanovy věty.** Nechť $\lambda_1, \ldots, \lambda_k$ jsou všechny různé vlastní hodnoty zobrazení $\varphi$. Z předpokladů Jordanovy věty plyne (viz 3.32, že $V = \mathcal{R}_{\lambda_1} \oplus \cdots \oplus \mathcal{R}_{\lambda_k}$. Zobrazení $\varphi_i = (\varphi|_{\mathcal{R}_{\lambda_i}} - \lambda_i \cdot \mathrm{id}_{\mathcal{R}_{\lambda_i}})$ jsou nilpotentní, a proto je každý z kořenových prostorů přímým součtem



$$\mathcal{R}_{\lambda_i} = P_{1,\lambda_i} \oplus \cdots \oplus P_{j_i,\lambda_i}$$

prostorů, na nichž je zúžení zobrazení $\varphi - \lambda_i \cdot \mathrm{id}_V$ cyklické. Matice těchto zúžených zobrazení na $P_{r,s}$ jsou Jordanovy bloky příslušné k nulové vlastní hodnotě, zúžené zobrazení $\varphi|_{P_{r,s}}$ má proto za matici Jordanův blok s vlastní hodnotou $\lambda_i$.

Pro důkaz Jordanovy věty zbývá dokázat tvrzení o jednoznačnosti. Protože diagonální hodnoty $\lambda_i$ jsou dány jako kořeny

**3.34. Použití v kvantové fyzice.** V kvantové fyzice se fyzikální veličině nepřiřazuje číselná hodnota, tak jak tomu je v klasické fyzice, nýbrž hermiteovský operátor. To není nic jiného, než hermiteovské zobrazení, které ovšem může vést, a často taky vede, mezi unitárními prostory nekonečné dimenze (můžeme si to představit třeba jako matici nekonečného rozměru). Vektory v tomto unitárním prostoru potom reprezentují stavy daného fyzikálního systému. Při měření dané fyzikální veličiny můžeme dostat jen hodnoty, které jsou vlastními hodnotami příslušného operátoru.

Například místo souřadnice $x$ máme operátor souřadnice $\hat{x}$. Je-li stav systému popsán vektorem $v$, pak platí $\hat{x}(v) = xv$, tzn. je to násobení vektoru reálným číslem $x$. Na první pohled je tento hermiteovský operátor jiný než naše příklady z konečné dimenze. Evidentně je totiž každé reálné číslo vlastním číslem ($\hat{x}$ má tzv. spojité spektrum). Podobně, místo rychlosti (přesněji hybnosti) máme operátor $\hat{p} = -i\frac{d}{dx}$. Vlastní vektory jsou řešení diferenciální rovnice $-i\frac{dv}{dx} = \lambda v$. I v tomto případě je spektrum spojité. To je vyjádřením faktu, že příslušná fyzikální veličina je spojitá (může nabývat libovolné reálné hodnoty). Naproti tomu máme fyzikální veličiny. např. energie, které mohou nabývat jen diskrétní hodnoty (energie je kvantována). Příslušné operátory jsou pak opravdu podobné hermiteovským maticím, jen mají nekonečný počet vlastních čísel.

**3.35.** Ukažte, že $\hat{x}$ a $\hat{p}$ jsou hermiteovské a že

$$[\hat{x}, \hat{p}] = i.$$

**Řešení.** Pro libovolný vektor $v$ platí

$$[\hat{x}, \hat{p}]v = \hat{x}\hat{p}v - \hat{p}\hat{x}v = x(-i\frac{dv}{dx}) + i\frac{d(xv)}{dx} - = iv$$

a odtud už přímo vyplývá naše tvrzení. □

**3.36.** Ukažte

$$[\hat{x} - \hat{p}, \hat{x} + \hat{p}] = 2i.$$

**Řešení.** Evidentně platí $[\hat{x}, \hat{x}] = 0$ a $[\hat{p}, \hat{p}] = 0$ a zbytek vyplývá z linearity komutátoru a z minulého příkladu. □

**3.37. Jordanův tvar.** Najděte Jordanův tvar matice $A$ a napište příslušný rozklad. Jaká je geometrická interpretace rozkladu této matice?

i) $A = \begin{pmatrix} -1 & 1 \\ -6 & 4 \end{pmatrix}$,

ii) $A = \begin{pmatrix} -1 & 1 \\ -4 & 3 \end{pmatrix}$.

charakteristického polynomu, je jejich jednoznačnost zřejmá. Vyjádříme rozměry jednotlivých Jordanových bloků prostřednictvím hodností $r_k(\lambda_i)$ zobrazení $(\varphi - \lambda_i \cdot \mathrm{id}_V)^k$. Tím bude jasné, že až na pořadí jsou bloky jednoznačně určeny. Naopak, přehození bloků odpovídá přečíslování vektorů báze, lze je tedy získat v libovolném pořadí.

Je-li $\psi$ cyklický operátor na $n$-rozměrném prostoru, pak defekt iterovaného zobrazení $\psi^k$ je $k$ pro $0 \leq k \leq n$ a je $n$ pro všechna $k \geq n$. Odtud plyne, že pokud matice $J$ zobrazení $\varphi$ obsahuje $d_k(\lambda)$ Jordanových bloků řádu $k$ s vlastní hodnotou $\lambda$, pak defekt matice $(J - \lambda \cdot E)^\ell$ je

$$d_1(\lambda) + 2d_2(\lambda) + \ldots \ell d_\ell(\lambda) + \ell d_{\ell+1}(\lambda) + \ldots.$$

Odtud spočítáme

$$\begin{aligned} n - r_\ell(\lambda) = d_1(\lambda) + 2d_2(\lambda) + \cdots + \ell d_\ell(\lambda) + \\ + \ell d_{\ell+1}(\lambda) + \cdots + d_k(\lambda) = \\ = r_{k-1}(\lambda) - 2r_k(\lambda) + r_{k+1}(\lambda) \end{aligned}$$

(kde poslední řádek vznikne kombinací předchozího pro hodnoty $\ell = k-1, k, k+1$).

**3.41. Poznámka.** Důkaz věty o existenci Jordanova kanonického tvaru byl sice konstruktivní, nedává nám ale dokonale efektivní algoritmický postup pro jejich hledání. Nyní shrneme již odvozený postup explicitního výpočtu báze, v níž má dané zobrazení $\varphi : V \to V$ matici v kanonickém Jordanově tvaru.

(1) Najdeme kořeny charakteristického polynomu.
(2) Jestliže jich je méně než $n = \dim V$, včetně násobností, kanonický tvar neexistuje.
(3) Je-li $n$ lineárně nezávislých vlastních vektorů, získáme bázi $V$ z vlastních vektorů a v ní má $\varphi$ diagonální matici.
(4) Nechť $\lambda$ je vlastní hodnota s geometrickou násobností menší než algebraickou a $v_1, \ldots, v_k$ nechť jsou příslušné vlastní vektory. To by měly být vektory na horním okraji schématu z důkazu věty 3.39, je ovšem nutné najít vhodnou bázi aplikacemi iterací $\varphi - \lambda \cdot \mathrm{id}_V$. Zároveň přitom zjistíme, ve kterém řádku se vektory nacházejí, a najdeme lineárně nezávislá řešení $w_i$ rovnic $(\varphi - \lambda\,\mathrm{id})(x) = v_i$ z řádků pod nimi. Postup opakujeme iterativně (tj. pro $w_i$ atd.). Najdeme tak „řetízky“ bázových vektorů zadávajících podprostory, kde $\varphi - \lambda\,\mathrm{id}$ je cyklické.

Postup je praktický pro matice, kde násobnosti vlastních hodnot jsou malé, nebo aspoň diskutované stupně nilpotentnosti jsou malé. Např. pro matici

$$A = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

dostaneme dvourozměrný podprostor vlastních vektorů

$$\langle (1,0,0), (0,1,0) \rangle.$$

Potřebujeme proto najít řešení rovnic $(A - 2E)x = (a, b, 0)^T$ pro vhodné konstanty $a, b$. Tento systém je ovšem řešitelný pouze pro $a = b$ a jedno z možných řešení je $v = (0,0,1)$, $a = b = 1$. Celá hledaná báze pak je $(1,1,0)$, $(0,0,1)$, $(1,0,0)$. Všimněme si, že jsme měli spoustu voleb a bází s požadovanými vlastnostmi je tedy mnoho.

**Řešení.** i) Nejprve spočítáme charakteristický polynom matice $A$

$$|A-\lambda E| = \begin{vmatrix} -1-\lambda & 1 \\ -6 & 4-\lambda \end{vmatrix} = \lambda^2 - 3\lambda + 2.$$

Vlastní čísla matice $A$ jsou kořeny tohoto polynomu, to znamená $\lambda_{1,2} = 1, 2$. Protože matice je řádu dva a máme dvě různé vlastní hodnoty, je Jordanův tvar diagonální matice $J = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Vlastní vektor $(x, y)$ příslušný vlastní hodnotě 1 splňuje $0 = (A - E)x = \begin{pmatrix} -2 & 1 \\ -6 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$, tj. $-2x + y = 0$. To jsou právě násobky vektoru $(1, 2)$. Podobně zjistíme, že vlastním vektorem k vlastní hodnotě 2 je $(1, 3)$. Jordanův tvar nám říká, že matice $A$ určuje takové lineární zobrazení, které má v bázi vlastních vektorů $(1, 2)$, $(1, 3)$ výše uvedený diagonální tvar. To znamená, že ve směru $(1, 2)$ se nic neděje a ve směru $(1, 3)$ se každý vektor protáhne na svůj dvojnásobek.

Matici $P$ takovou, že $A = P \cdot J \cdot P^{-1}$, pak dostaneme napsáním těchto vlastních vektorů do sloupců, tj. $P = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$. Pro matici $A$ pak máme $A = P \cdot J \cdot P^{-1}$. Inverzní matice k $P$ má tvar $P^{-1} = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$ a dohromady pak dostáváme

$$\begin{pmatrix} -1 & 1 \\ -6 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}.$$

ii) Charakteristický polynom matice $A$ je v tomto případě

$$|A-\lambda E| = \begin{vmatrix} -1-\lambda & 1 \\ -4 & 3-\lambda \end{vmatrix} = \lambda^2 - 2\lambda + 1 = 0.$$

Dostáváme tedy dvojnásobný kořen $\lambda = 1$ a příslušný vlastní vektor $(x, y)$ splňuje

$$0 = (A - E)x = \begin{pmatrix} -2 & 1 \\ -4 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

To jsou, opět jako v minulém příkladu, násobky vektoru $(1, 2)$. To, že řešením této rovnice nejsou dva lineárně nezávislé vektory, říká, že Jordanův tvar v tomto případě nebude diagonální, ale bude to matice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Bázi, ve které má matice $A$ tento tvar, tvoří vlastní vektor $(1, 2)$ a vektor, který se na tento vektor zobrazí zobrazením $A - E$. Je tedy řešením soustavy rovnic

$$\left(\begin{array}{cc|c} -2 & 1 & 1 \\ -4 & 2 & 2 \end{array}\right) \sim \left(\begin{array}{cc|c} -2 & 1 & 1 \\ 0 & 0 & 0 \end{array}\right).$$

To jsou násobky vektoru $(1, 3)$. Dostáváme tedy stejnou bázi jako v minulém příkladu a můžeme psát

$$\begin{pmatrix} -1 & 1 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}.$$

Zobrazení teď působí na vektor tak, že složka ve směru $(1, 3)$ zůstává stejná a ke složka ve směru $(1, 2)$ se bude násobit součtem koeficientů, které určují složky ve směrech $(1, 3)$ a $(1, 2)$. □

## 5. Rozklady matic a pseudoinverze



V minulé části jsme s soustředili na geometrický popis struktury zobrazení. Teď naše výsledky přeložíme do jazyku tzv. rozkladů matic, což je obzvlášť důležité téma pro numerické postupy a maticový počet obecně.

I při počítání s reálnými čísly užíváme pro zjednodušení rozklady na součiny. Nejjednodušším je vyjádření každého reálného čísla jednoznačně ve tvaru

$$a = \operatorname{sgn}(a) \cdot |a|,$$

tj. jako součin znaménka a absolutní hodnoty. V dalším textu si uvedeme stručně přehled několika takových rozkladů pro různé typy matic, které bývají nesmírně užitečné při numerických výpočtech s maticemi. Například jsme vhodný rozklad pro pozitivně semidefinitní symetrické matice využili v odstavci 3.31 pro konstrukci odmocniny z matice.



**3.42. LU–rozklad.** Začneme přeformulováním několika výsledků, které jsme už dávno odvodili. V odstavcích 2.7 a 2.8 jsme upravovali matice nad skaláry z libovolného pole na řádkový schodovitý tvar. K tomu jsme používali elementární úpravy, které spočívaly v postupném násobení naší matice invertibilními dolními trojúhelníkovými maticemi $P_i$, které postihovaly přičítání násobků řádků pod právě zpracovávaným řádkem.

Předpokládejme pro jednoduchost, že naše matice $A$ je čtvercová a že při Gaussově eliminaci nejsme nuceni přehazovat řádky, a proto všechny naše matice $P_i$ mohou být dolní trojúhelníkové s jedničkami na diagonálách. Konečně, stačí si povšimnout, že inverzní matice k takovýmto $P_i$ jsou opět dolní trojúhelníkové s jedničkami na diagonálách a dostáváme

$$U = P \cdot A = P_k \cdots P_1 \cdot A,$$

kde $U$ je horní trojúhelníková matice a tedy

$$A = L \cdot U,$$

kde $L$ je dolní trojúhelníková matice s jedničkami na diagonále a $U$ je horní trojúhelníková. Tomuto rozkladu se říká *LU–rozklad* matice $A$.

V případě obecné matice můžeme při Gaussově eliminaci na řádkově schodovitý tvar potřebovat navíc permutace řádků, někdy i sloupců matice. Pak dostáváme obecněji:

**Věta.** *Pro každou matici $A$ existují permutační matice $P$, $Q$, dolní trojúhelníková matice $L$ a horní trojúhelníková matice $U$ tak, že*

$$A = P \cdot L \cdot U \cdot Q.$$



**3.43. Poznámky.** Přímým důsledkem Gaussovy eliminace bylo také zjištění, že až na volbu vhodných bází na definičním oboru a oboru hodnot je každé zobrazení $f : V \to W$ zadáno maticí v blokově diagonálním tvaru s jednotkovou maticí, s rozměrem daným dimenzí obrazu $f$ a s nulovými bloky všude kolem. To lze přeformulovat takto: Každou matici $A$ typu $m/n$ nad polem skalárů $\mathbb{K}$ lze rozložit na součin

$$A = P \cdot \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix} \cdot Q,$$

kde $P$ a $Q$ jsou vhodné invertibilní matice.

**3.38.** Najděte Jordanův tvar matice $A$ a napište příslušný rozklad. Jaká je geometrická interpretace rozkladu této matice? $A_1 = \frac{1}{3}\begin{pmatrix} 5 & -1 \\ -2 & 4 \end{pmatrix}$ a $A_2 = \frac{1}{3}\begin{pmatrix} 5 & -1 \\ 4 & 1 \end{pmatrix}$ a nakreslete (narýsujte), jak se vektory $v = (3, 0)$, $A_1 v$ a $A_2 v$ rozkládají vzhledem k bázi vlastních vektorů matice $A_1$, resp. $A_2$.

**Řešení.** Matice mají stejné Jordanovy tvary jako matice v minulém příkladu a obě je mají v bázi tvořenou vektory $(1, 2)$ a $(1, -1)$, tj.

$$\frac{1}{3}\begin{pmatrix} 5 & -1 \\ -2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}^{-1}$$

a

$$\frac{1}{3}\begin{pmatrix} 5 & -1 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}^{-1}.$$

Pro vektor $v = (3, 0)$ dostáváme $v = (1, 2) + 2(1, -1)$ a pro jeho obrazy $A_1 v = (5, -2) = (1, 2) + 2 \cdot 2 \cdot (1, -1)$ a $A_2 v = (5, 4) = (2 + 1) \cdot (1, 2) + 2 \cdot (1, -1)$. □

### F. Rozklady matic

**3.39.** Vyvraťte nebo dokažte:

- Nechť $A$ je čtvercová matice $n \times n$. Pak je matice $A^T A$ je symetrická.
- Nechť čtvercová matice $A$ má pouze kladné reálné vlastní hodnoty. Pak je $A$ symetrická.

**3.40.** Nalezněte LU-rozklad následující matice:

$$\begin{pmatrix} -2 & 1 & 0 \\ -4 & 4 & 2 \\ -6 & 1 & -1 \end{pmatrix}.$$

**Řešení.** Rozklad je roven

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & -1 & 1 \end{pmatrix}\begin{pmatrix} -2 & 1 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Nejprve vynásobíme matice odpovídající Gaussově eliminaci, dostáváme tak pro původní matici $A$, $XA = U$, kde $X$ je dolní trojúhelníková daná zmíněným součinem, $U$ horní trojúhelníková. Z této rovnosti máme $A = X^{-1}U$, což je hledaný rozklad (musíme tedy spočítat inverzi k $X$). □

*3.41.* Nalezněte $LU$-rozklad matice $\begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 2 \\ - & 1 & -1 \end{pmatrix}$. ○

Pro čtvercové matice jsme v 3.32 ukázali při diskusi vlastností lineárních zobrazení $f : V \to V$ na komplexních vektorových prostorech, že každou čtvercovou matici $A$ dimenze $m$ umíme rozložit na součin

$$A = P \cdot B \cdot P^{-1},$$

kde $B$ je blokově diagonální s Jordanovými bloky příslušnými k vlastním číslům na diagonále. Skutečně jde o pouhé přepsání Jordanovy věty, protože násobení maticí $P$ a její inverzí z opačných stran odpovídá v tomto případě právě změně báze na vektorovém prostoru $V$ a citovaná věta říká, že ve vhodné bázi má každé zobrazení Jordanův kanonický tvar.

Obdobně jsme také při diskusi samoadjungovaných zobrazení dokázali, že pro reálné symetrické nebo komplexní hermiteovské matice existuje vždy rozklad na součin

$$A = P \cdot B \cdot P^*,$$

kde $B$ je diagonální matice se všemi (vždy reálnými) vlastními čísly na diagonále, včetně násobností. Skutečně, jde opět o součin s maticemi vystihující změnu báze, nicméně připouštíme nyní pouze změny mezi mezi ortonormálními bázemi a proto i matice přechodu $P$ musí být ortogonální. Odtud $P^{-1} = P^*$.

Pro reálná ortogonální zobrazení jsme odvodili obdobné vyjádření jako u symetrických, pouze naše $B$ bude blokově diagonální s bloky rozměru dva nebo jedna vyjadřujícími buď rotaci nebo zrcadlení nebo identitu vzhledem k příslušným podprostorům.

**3.44. Věta o singulárním rozkladu.** Nyní se vrátíme k obecným



lineárním zobrazením mezi (obecně různými) vektorovými prostory. Jestliže na nich je definován skalární součin a omezíme se přitom na ortonormální báze, musíme postupovat o hodně rafinovaněji, než v případě bází libovolných:

**Věta.** *Nechť $A$ je libovolná matice typu $m/n$ nad reálnými nebo komplexními skaláry. Pak existují čtvercové unitární matice $U$ a $V$ dimenzí $m$ a $n$, a reálná diagonální matice $D$ s nezápornými prvky, dimenze $r$, $r \leq \min\{m, n\}$, takové, že*

$$A = USV^*, \quad S = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

*a $r$ je hodnost matice $AA^*$. Přitom je $S$ určena jednoznačně až na pořadí prvků a prvky diagonální matice $D$ jsou druhé odmocniny vlastních čísel $d_i$ matice $AA^*$. Pokud je $A$ reálná matice, pak i matice $U$ a $V$ jsou ortogonální.*



Důkaz. Předpokládejme nejprve $m \leq n$ a označme $\varphi : \mathbb{K}^n \to \mathbb{K}^m$ zobrazení mezi reálnými nebo komplexními prostory se standardními skalárními součiny, zadané maticí $A$ ve standardních bázích.

Tvrzení věty můžeme přeformulovat tak, že existují ortonormální báze na $\mathbb{K}^n$ a $\mathbb{K}^m$, ve kterých bude mít $\varphi$ matici $S$ z tvrzení věty.

Jak jsme viděli dříve, matice $A^*A$ je pozitivně semidefinitní. Proto má pouze reálná nezáporná vlastní čísla a existuje ortonormální báze $\underline{w}$ v $\mathbb{K}^n$, ve které má příslušné zobrazení $\varphi^* \circ \varphi$ diagonální matici s vlastními čísly na diagonále. Jinými slovy, existuje unitární matice $V$ taková, že $A^*A = VBV^*$ pro reálnou diagonální

**3.42. Ray-tracing.** V počítačové 3D-grafice se obraz zobrazuje pomocí algoritmu Ray-tracing. Základem tohoto algoritmu je aproximace světelných vln paprskem (přímka) a aproximace zobrazovaných objektů mnohostěny. Ty jsou tedy ohraničeny rovinami a je potřeba spočítat, kam se na těchto rovinách odráží světelné paprsky. Z fyziky přitom víme, jak se paprsky odráží - úhel odrazu je roven úhlu dopadu. Z touto problematikou v rovině jsme se již potkali v příkladu ‖1.58‖.

Paprsek světla ve směru $v = (1, 2, 3)$ dopadá na rovinu určenou rovnicí $x + y + z = 1$. V jakém směru se paprsek odrazí?

**Řešení.** Jednotkový normálový vektor k rovině je $n = \frac{1}{\sqrt{3}}(1, 1, 1)$. Vektor určující směr odraženého paprsku $v_R$ bude ležet v rovině určené vektory $v, n$. Můžeme jej tedy vyjádřit jako lineární kombinaci těchto vektorů. Zároveň nám pravidlo úhel odrazu je roven úhlu dopadu jinými slovy říká, že $\langle v, n\rangle = -\langle v_R, n\rangle$. Odtud dostaneme kvadratickou rovnici pro koeficienty lineární kombinace.

Příklad můžeme vyřešit i jednodušším, geometrickým způsobem. Z obrázku můžeme přímo odvodit,že

$$v_R = v - 2\langle v, n\rangle n$$

a v našem případě dostáváme $v_R = (-3, -2, -1)$. □

**3.43. Singulární rozklad, polární rozklad, pseudoinverze.** Spočítejte singulární rozklad matice $A = \begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Následně spočítejte její polární rozklad a najděte její pseudoinverzi.

**Řešení.** Nejprve spočítáme $A^TA$:

$$A^TA = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 0 \\ -\frac{1}{2} & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \frac{1}{4} \end{pmatrix}$$

a dostáváme diagonální matici. Potřebujeme ale najít takovou ortonormální bázi, ve které je matice diagonální a nulový řádek je až poslední. Toho zjevně docílíme otočením o pravý úhel kolem osy $x$ (souřadnice $y$ přejde na $z$ a $z$ přejde na $-y$). Toto otočení je ortogonální transformace daná maticí $V = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$. Tím jsme bez počítání našli rozklad $A^TA = VBV^T$, kde $B$ je diagonální s vlastními čísly $(1, \frac{1}{4}, 0)$ na diagonále. Protože teď máme $B = (AV)^T(AV)$, tvoří sloupce matice

$$AV = \begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{2} & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

ortogonální systém vektorů, který znormalizujeme a doplníme do báze. Ta má pak tvar $(0, -1, 0)$, $(1, 0, 0)$, $(0, 0, 1)$. Matice přechodu od této matici s nezápornými vlastními čísly $(d_1, d_2, \ldots, d_r, 0, \ldots, 0)$ na diagonále, $d_i \neq 0$ pro všechny $i = 1, \ldots, r$. Odtud

$$B = V^*A^*AV = (AV)^*(AV).$$

To je ale je ekvivalentní tvrzení, že prvních $r$ sloupců matice $AV$ je ortogonálních a zbývající jsou nulové, protože mají nulovou velikost.

Označme nyní prvních $r$ sloupců $v_1, \ldots, v_r \in \mathbb{R}^m$. Platí tedy $\langle v_i, v_i\rangle = d_i, i = 1, \ldots, r$, a normované vektory $u_i = \frac{1}{\sqrt{d_i}}v_i$ tvoří ortonormální systém nenulových vektorů. Doplňme je na ortonormální bázi $\underline{u} = u_1, \ldots, u_n$ celého $\mathbb{K}^m$. Vyjádříme-li naše původní zobrazení $\varphi$ v bázích $\underline{w}$ na $\mathbb{K}^n$ a $\underline{u}$ na $\mathbb{K}^m$, dostáváme matici $\sqrt{B}$. Přechody od standardních bází k nově vybraným odpovídají násobení zleva ortogonálními maticemi $U$ a zprava $V^{-1} = V^*$.

Pokud je $m > n$, můžeme aplikovat předchozí část důkazu na matici $A^*$. Odtud pak přímo plyne požadované tvrzení.

Pokud pracujeme nad reálnými skaláry, jsou všechny naše kroky v důkazu výše také realizovány v reálném oboru. □

Tento důkaz věty o singulárním rozkladu je konstruktivní a můžeme jej opravdu použít pro výpočet unitárních, resp. ortogonálních, matic $U$, $V$ a diagonálních nenulových prvků matice $S$.

**3.45. Geometrická interpretace.** Diagonálním hodnotám matice $D$ z předchozí věty se říká *singulární hodnoty matice* $A$. Přeformulujme si tuto větu v reálném případě geometričtěji.



Pro příslušné lineární zobrazení $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ mají singulární hodnoty skutečně jednoduchý geometrický význam: Nechť $K \subseteq \mathbb{R}^n$ je jednotková sféra pro standardní skalární součin. Obrazem $\varphi(K)$ pak vždy bude (případně degenerovaný) $m$-rozměrný elipsoid. Singulární čísla matice $A$ jsou přitom velikosti hlavních poloos a věta navíc říká, že původní sféra vždy připouští ortogonální sdružené průměry, jejichž obrazem budou právě všechny poloosy tohoto elipsoidu.

Pro čtvercové matice je vidět, že $A$ je invertibilní, právě když všechna singulární čísla jsou nenulová. Poměr největšího a nejmenšího singulárního čísla je důležitým parametrem pro robustnost řady numerických výpočtů s maticemi, např. pro výpočet inverzní matice. Poznamenejme také, že existují rychlé metody výpočtů, resp. odhadů, vlastních čísel, proto lze se singulárním rozkladem velmi efektivně pracovat.

**3.46. Věta o polárním rozkladu.** Věta o singulárním rozkladu



je východiskem pro mnoho mimořádně užitečných nástrojů. Uvažujme nyní nad několika přímými důsledky (které samy o sobě jsou dosti netriviální). Tvrzení věty říká pro libovolnou matici $A$, ať už reálnou nebo komplexní, $A = USW^*$ s diagonální $S$ s nezápornými reálnými čísly na diagonále a unitárními $U, W$. Pak ovšem také $A = USU^*UW^*$ a pojmenujme si matice $P = USU^*$, $V = UW^*$. První z nich, $P$, je hermiteovská (v reálném případě symetrická) a pozitivně semidefinitní, protože jde jen o zápis zobrazení s reálnou diagonální maticí $S$ v jiné ortonormální bázi, zatímco $V$ je coby součin dvou unitárních matic opět unitární (v reálném případě ortogonální). Navíc $A^* = WSU^*$ a tedy $AA^* = USSU^* = P^2$ a naše matice $P$ je vlastně odmocninou ze snadno spočítatelné hermiteovské matice $AA^*$.

báze ke standardní je pak $U = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Dohromady tak dostáváme rozklad $A = U\sqrt{B}V^T$:

$$\begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Geometricky lze rozklad zobrazení interpretovat tak, že nejprve se vše otočí o pravý úhel kolem osy x, pak následuje projekce do roviny xy taková, že jednotková koule se zobrazí do elipsy s hlavními poloosami 1 a $\frac{1}{2}$ a výsledek se otočí o pravý úhel kolem osy z.

Polární rozklad $A = P \cdot W$ dostaneme ze singulárního jednoduše: $P := U\sqrt{B}U^T$ a $W := UV^T$, tj.

$$P = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

a

$$W = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

a z toho plyne

$$\begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Pseudoinverzní matice je dána výrazem $A^\dagger := VS'U^T$, kde $S' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Máme tedy

$$A^\dagger = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{pmatrix}.$$

□

**3.44. QR rozklad.** QR rozklad matice $A$ se dobře hodí v případě, když je dán systém lineárních rovnic $Ax = b$, který sice nemá řešení, ale my potřebujeme najít jeho co nejlepší přiblížení. Chceme tedy minimalizovat $\|Ax - b\|$. Podle Pythagorovy věty máme $\|Ax - b\|^2 = \|Ax - b_\parallel\|^2 + \|b_\perp\|^2$, kde $b$ jsme rozložili na $b_\parallel$, které patří do obrazu matice $A$ a na $b_\perp$, které je k tomuto obrazu kolmé. Projekci na obraz matice $A$ můžeme psát ve tvaru $QQ^T$ pro vhodnou ortogonální matici $Q$. Konkrétně tuto matici získáme Gram-Schmidtovou ortonormalizací sloupců matice $A$. Potom máme $b_\parallel = QQ^Tb$ a proto $Ax - b_\parallel = Q(Q^TAx - Q^Tb)$. Soustava v závorce už má řešení, pro které potom dostáváme $\|Ax - b\| = \|b_\perp\|$, což je minimální hodnota. Navíc matice $R := Q^TA$ je horní trojúhelníková a proto požadované přibližné řešení najdeme velmi lehce.

Předpokládejme, že $A = PV = QU$ jsou dva takové rozklady matice $A$ na součin pozitivně semidefinitní hermiteovské a unitární matice a předpokládejme, že $A$ je invertibilní. Pak ovšem je

$$AA^* = PVV^*P = P^2 = QUU^*Q = Q^2$$

pozitivně definitní, a proto jsou matice $Q = P = \sqrt{AA^*}$ jednoznačně určené a invertibilní. Pak ovšem také $U = V = P^{-1}A$.

Beze zbytku jsme tedy odvodili velice užitečnou analogii rozkladu reálného čísla na znaménko (ortogonální matice v případě dimenze jedna jsou právě $\pm 1$) a absolutní hodnotu (matice $P$, ke které umíme odmocninu).

**Věta** (Věta o polárním rozkladu)**.** *Každou čtvercovou komplexní matici $A$ dimenze $n$ lze vždy vyjádřit ve tvaru $A = P \cdot V$, kde $P$ je hermiteovská a pozitivně definitní čtvercová matice téže dimenze a $V$ je unitární. Přitom $P = \sqrt{AA^*}$. Je-li $A$ invertibilní, je rozklad jednoznačný a $V = (\sqrt{AA^*})^{-1}A$.*

*Pokud pracujeme nad reálnými skaláry, je $P$ symetrická a $V$ ortogonální.*

Když budeme tutéž větu aplikovat na $A^*$ místo $A$, dostaneme tentýž výsledek, ovšem s obráceným pořadím hermiteovských a unitárních matic. Matice v příslušných pravých a levých rozkladech budou samozřejmě obecně různé.

V komplexním případě je analogie s rozkladem čísel ještě zábavnější — pozitivně semidefinitní $P$ hraje opět roli absolutní hodnoty komplexního čísla, unitární matice $V$ pak má jednoznačné vyjádření jako součet $V = \mathrm{re}\,V + i\,\mathrm{im}\,V$ s hermiteovskými reálnými a imaginárními částmi a s vlastností $(\mathrm{re}\,V)^2 + (\mathrm{im}\,V)^2 = E$, tj. dostáváme plnou analogii goniometrického tvaru komplexních čísel (viz závěrečná poznámka v 3.30). Všimněme si ale, že ve vícerozměrném případě je podstatné, v jakém pořadí tento „goniometrický tvar“ matice píšeme. Jde to oběma způsoby, výsledky jsou ale obecně různé.



Pro řadu praktických aplikací bývá rychlejší použití tzv. *QR rozkladu* matic, který je obdobou Schurovy věty o ortogonální triangulaci:

**3.47. Věta.** *Pro každou komplexní matici $A$ typu $m/n$ existuje unitární matice $Q$ a horní trojúhelníková matice $R$ takové, že $A = Q^TR$.*

*Pokud pracujeme nad reálnými skaláry, jsou $Q$ i $R$ reálné.*

Důkaz. V geometrické formulaci potřebujeme dokázat, že pro každé zobrazení $\varphi : \mathbb{K}^n \to \mathbb{K}^m$ s maticí $A$ ve standardních bázích můžeme zvolit novou ortonormální bázi na $\mathbb{K}^m$ tak, aby potom $\varphi$ mělo horní trojúhelníkovou matici.



Uvažme obrazy $\varphi(e_1), \ldots, \varphi(e_n) \in \mathbb{K}^m$ vektorů standardní ortonormální báze, vyberme z nich maximální lineárně nezávislý systém $v_1, \ldots, v_k$ takovým způsobem, že vypouštěné závislé vektory jsou vždy lineární kombinací předchozích vektorů, a doplňme jej do báze $v_1, \ldots, v_m$. Nechť $u_1, \ldots, u_m$ je ortonormální báze $\mathbb{K}^m$ vzniklá Gramovou-Schmidtovou ortogonalizací tohoto systému vektorů.

Nyní pro každé $e_i$ je $\varphi(e_i)$ buď jedno z $v_j$, $j \leq i$, nebo je lineární kombinací $v_1, \ldots, v_{i-1}$, proto ve vyjádření $\varphi(e_i)$ v bázi $\underline{u}$ vystupují pouze vektory $u_1, \ldots, u_i$. Zobrazení $\varphi$ má proto ve

Najděte přibližné řešení soustavy rovnic

$$\begin{aligned} x &+ 2y &&= 1,\\ 2x &+ 4y &&= 4. \end{aligned}$$

**Řešení.** Máme tedy soustavu $Ax = b$ s $A = \begin{pmatrix}1&2\\2&4\end{pmatrix}$ a $b = \begin{pmatrix}1\\4\end{pmatrix}$ (která evidentně nemá řešení). Uděláme tedy ortonormalizaci sloupců matice $A$. Vezmeme první z nich a vydělíme ho jeho velikostí. Tím dostaneme první vektor ortonormální báze $\frac{1}{\sqrt5}\begin{pmatrix}1\\2\end{pmatrix}$. Druhý dostaneme tak, že od druhého sloupce odečteme jeho komponentu ve směru už nalezeného prvního vektoru ortonormální báze. Druhý vektor je ovšem dvojnásobek prvního a proto v ortonormalizaci nulový. Máme proto $Q = \frac{1}{\sqrt5}\begin{pmatrix}1\\2\end{pmatrix}$. Projektor na obraz matice $A$ je pak $QQ^T = \frac15\begin{pmatrix}1&2\\2&4\end{pmatrix}$, dále spočítáme

$$Q^Tb = \frac{1}{\sqrt5}\begin{pmatrix}1&2\end{pmatrix}\begin{pmatrix}1\\4\end{pmatrix} = \frac{9}{\sqrt5}$$

a

$$R = \frac{1}{\sqrt5}\begin{pmatrix}1&2\end{pmatrix}\begin{pmatrix}1&2\\2&4\end{pmatrix} = \frac{1}{\sqrt5}\begin{pmatrix}5&9\end{pmatrix}.$$

Přibližné řešení pak splňuje $Rx = Q^Tb$ a to v našem případě znamená $5x + 9y = 9$ (přibližné řešení tedy není jednoznačné). QR rozklad matice $A$ je

$$\begin{pmatrix}1&2\\2&4\end{pmatrix} = \tfrac{1}{\sqrt5}\begin{pmatrix}1\\2\end{pmatrix}\tfrac{1}{\sqrt5}\begin{pmatrix}5&9\end{pmatrix}. \qquad \square$$

**3.45.** Minimalizujte $\|Ax - b\|$ pro $A = \begin{pmatrix}2&-1&-1\\-1&2&-1\\-1&-1&2\end{pmatrix}$ a $b = \begin{pmatrix}1\\0\\0\end{pmatrix}$ a napište QR rozklad matice $A$.

**Řešení.** Normalizovaný první sloupec matice $A$ je $e_1 = \frac{1}{\sqrt6}\begin{pmatrix}2\\-1\\-1\end{pmatrix}$. Z druhého sloupce odečteme jeho složku ve směru $e_1$. Máme

$$\left\langle\begin{pmatrix}-1\\2\\-1\end{pmatrix}, \frac{1}{\sqrt6}\begin{pmatrix}2\\-1\\-1\end{pmatrix}\right\rangle = -\frac{3}{\sqrt6},$$

a proto dostaneme

$$\begin{pmatrix}-1\\2\\-1\end{pmatrix} - \left\langle\begin{pmatrix}-1\\2\\-1\end{pmatrix}, \frac{1}{\sqrt6}\begin{pmatrix}2\\-1\\-1\end{pmatrix}\right\rangle\frac{1}{\sqrt6}\begin{pmatrix}2\\-1\\-1\end{pmatrix} = \frac12\begin{pmatrix}0\\3\\3\end{pmatrix}.$$

Tím jsme vyrobili ortogonální vektor, který normujeme a dostaneme $e_2 = \frac{1}{\sqrt2}\begin{pmatrix}0\\1\\-1\end{pmatrix}$. Třetí sloupec matice $A$ je už lineárně závislý standardní bázi na $\mathbb{K}^n$ a ortonormální bázi $\underline{u}$ na $\mathbb{K}^m$ horní trojúhelníkovou matici $R$. Přechod k bázi $\underline{u}$ na $\mathbb{R}^m$ odpovídá násobení unitární maticí $Q$ zleva, tj. $R = QA$, ekvivalentně $A = Q^TR$.

Poslední tvrzení je z naší konstrukce zřejmé. $\square$



Závěrem této části textu si všimněme mimořádně užitečné a důležité aplikace našich výsledků pro přibližné numerické výpočty. Půjde přitom o docela přímočarou aplikaci singulárních rozkladů matic, jak je vidět už z následující:

**3.48. Definice.** Nechť $A$ je reálná matice typu $m/n$ a nechť

$$A = USV^*, \quad S = \begin{pmatrix}D&0\\0&0\end{pmatrix}$$

je její singulární rozklad (zejména $D$ je invertibilní). Matici

$$A^\dagger := VS'U^*, \quad S' = \begin{pmatrix}D^{-1}&0\\0&0\end{pmatrix}$$

nazýváme *pseudoinverzní matice* k matici $A$.

Jak ukazuje následující věta, je pseudoinverze důležité zobecnění pojmu inverzní matice, včetně přímočarých aplikací.

**3.49. Věta.** *Nechť $A$ je reálná nebo komplexní matice typu $m/n$. Pak pro její pseudoinverzní matici platí:*

*(1) Je-li $A$ invertibilní (zejména tedy čtvercová), pak*

$$A^\dagger = A^{-1}.$$

*(2) Pro pseudoinverzi $A^\dagger$ platí, že $A^\dagger A$ i $AA^\dagger$ jsou hermiteovské (v reálném případě symetrické) a*

$$AA^\dagger A = A, \quad A^\dagger AA^\dagger = A^\dagger.$$

*(3) Pseudoinverzní matice $A^\dagger$ je čtyřmi vlastnostmi z předchozího bodu určena jednoznačně. Pokud tedy nějaká matice $B$ typu $n \times m$ splňuje, že $BA$ i $AB$ jsou hermiteovské, $ABA = A$ a $BAB = B$, pak $B = A^\dagger$.*

*(4) Je-li $A$ matice systému lineárních rovnic $Ax = b$ s pravou stranou $b \in \mathbb{K}^m$, pak vektor $y = A^\dagger b \in \mathbb{K}^n$ minimalizuje velikost $\|Ax - b\|$ pro všechny vektory $x \in \mathbb{K}^n$.*

*(5) Systém lineárních rovnic $Ax = b$ s $b \in \mathbb{K}^m$ je řešitelný, právě když platí $AA^\dagger b = b$. V tomto případě jsou všechna řešení dána výrazem*

$$x = A^\dagger b + (E - A^\dagger A)u,$$

*kde $u \in \mathbb{K}^n$ je libovolné.*



Důkaz. (1): Je-li $A$ invertibilní, pak je matice $S = U^*AV$ také invertibilní a přímo z definice je $S' = S^{-1}$. Odtud vyplývá $A^\dagger A = AA^\dagger = E$.

(2): Přímým výpočtem dostáváme $SS'S = S$ a $S'SS' = S'$, proto

$$AA^\dagger A = USV^*VS'U^*USV^* = USS'SV^* = USV^* = A$$

a analogicky pro druhou rovnost. Dále

$$\begin{aligned}(AA^\dagger)^* &= (USS'U^*)^* = U(S')^*S^*U^* =\\ &= U(SS')^*U^* = USS'U^* = AA^\dagger\end{aligned}$$

a podobně se ukáže $(A^\dagger A)^* = A^\dagger A$.

(3) Tvrzení dokážeme přímým výpočtem. Uvažme na chvíli zobrazení $\varphi$ dané ve standardních bázích maticí $A$ vyjádřeme

(můžeme ověřit spočítáním determinantu). Hledaná sloupcově ortogonální matice je tedy

$$Q = \frac{1}{\sqrt{6}} \begin{pmatrix} 2 & 0 \\ -1 & \sqrt{3} \\ -1 & -\sqrt{3} \end{pmatrix}.$$

Dále spočítáme

$$R = Q^T A = \frac{1}{\sqrt{6}} \begin{pmatrix} 2 & -1 & -1 \\ 0 & \sqrt{3} & -\sqrt{3} \end{pmatrix} \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} = \\ = \frac{1}{\sqrt{6}} \begin{pmatrix} 6 & -3 & -3 \\ 0 & 3\sqrt{3} & -3\sqrt{3} \end{pmatrix}$$

a

$$Q^T b = \frac{1}{\sqrt{6}} \begin{pmatrix} 2 & -1 & -1 \\ 0 & \sqrt{3} & -\sqrt{3} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{6}} \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Řešením rovnice $Rx = Q^T b$ je $x = y = z$. Násobky vektoru $(1, 1, 1)$ tedy minimalizují $\|Ax - b\|$.

Zobrazení určené maticí $A$ je projekce na rovinu s normálovým vektorem $(1, 1, 1)$. □

**3.46. Lineární regrese.** Znalosti, které jsme se v této kapitole naučili, lze s výhodou použít v praxi při řešení problémů pomocí lineární regrese. Jde o to nalézt nejlepší přiblížení nějaké funkční závislosti pomocí lineární funkce.

Máme tedy zadánu funkční závislost v několika bodech (například zkoumáme hodnotu majetku $y_i$ lidí v závislosti na jejich inteligenci $(a_1)$, na majetku rodičů $(a_2)$ , počtu společných známých s panem Kalouskem $(a_3), \ldots)$, tj. $f(a_1^1, \ldots, a_n^1) = y_1, \ldots, f(a_1^k, a_2^k, \ldots, a_n^k) = y_k$, $k > n$ (máme tedy více rovnic než neznámých) a chceme tuto závislost „co nejlépe“ odhadnout pomocí lineární funkce, tj. vyjádřit hodnotu majetku jakožto lineární funkci $f(x_1, \ldots, x_n) = b_1 x_1 + b_2 x_2 + \ldots + b_n x_n + c$. Definujeme tedy „co nejlépe“ tím, že chceme minimalizovat

$$\sum_{i=1}^{k} \left( y_i - \sum_{j=1}^{n} (b_j x_j + c) \right)^2$$

v závislosti na reálných konstantách $b_1, \ldots, b_n$, $c$. Naším cílem je najít takovou lineární kombinaci sloupců matice $A = (a_j^i)$ (s koeficienty $b_1, \ldots, b_n$), která bude mít co nejmenší vzdálenost od vektoru $(y_1, \ldots, y_k)$ v $\mathbb{R}^k$, tedy vlastně najít kolmou projekci vektoru $(y_1, \ldots, y_k)$ na podprostor generovaný sloupci matice $A$. Podle věty 3.49 je touto projekcí vektor $(b_1, \ldots, b_n)^T = A^\dagger (y_1, \ldots, b_n)$. Tuto metodu už jsme také použili na výpočet vzdálenosti bodu od podprostoru v příkladu $\|4.75\|$.

$\varphi$ v bázi z věty o singulárním rozkladu, tj. v této bázi bude mít $\varphi$ matici $S$ z definice pseudoinverze $A^\dagger$. Bez újmy na obecnosti nyní budeme pracovat v této bázi, tj. můžeme předpokládat, že v blokovém tvaru

$$A = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}, \; A^\dagger = \begin{pmatrix} D^{-1} & 0 \\ 0 & 0 \end{pmatrix}$$

s diagonální maticí $D$ všech nenulových singulárních čísel, a $B$ je matice splňující předpoklady. Zjevně

$$A^\dagger A = \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix},$$

a tedy dostáváme

$$A^\dagger = A^\dagger A B A A^\dagger = \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix} B \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} D^{-1} & 0 \\ 0 & 0 \end{pmatrix}.$$

Odtud vidíme, že

$$B = \begin{pmatrix} D^{-1} & P \\ Q & R \end{pmatrix}$$

pro vhodné matice $P$, $Q$ a $R$. Nyní však

$$BA = \begin{pmatrix} D^{-1} & P \\ Q & R \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} E & 0 \\ QD & 0 \end{pmatrix}$$

má být hermiteovská, proto je $QD = 0$ a tedy i $Q = 0$ (matice $D$ je diagonální a invertibilní). Obdobně požadavek na hermiteovskost $AB$ vede na nulovost $P$. Zároveň ještě platí

$$B = BAB = \begin{pmatrix} D^{-1} & 0 \\ 0 & R \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} D^{-1} & 0 \\ 0 & R \end{pmatrix}.$$

Na pravé straně ale je v pravém dolním rohu nula, proto také $R = 0$ a tvrzení je dokázáno.

(4): Uvažme zobrazení $\varphi : \mathbb{K}^n \to \mathbb{K}^m$, $x \mapsto Ax$, a přímé součty $\mathbb{K}^n = (\operatorname{Ker}\varphi)^\perp \oplus \operatorname{Ker}\varphi$, $\mathbb{K}^m = \operatorname{Im}\varphi \oplus (\operatorname{Im}\varphi)^\perp$. Zúžené zobrazení $\tilde{\varphi} := \varphi_{|(\operatorname{Ker}\varphi)^\perp} : (\operatorname{Ker}\varphi)^\perp \to \operatorname{Im}\varphi$ je lineární isomorfismus. Zvolíme-li vhodně ortonormální báze na $(\operatorname{Ker}\varphi)^\perp$ a $\operatorname{Im}\varphi$ a doplníme je na ortonormální báze na celých prostorech, bude mít $\varphi$ matici $S$ a $\tilde{\varphi}$ matici $D$ z věty o singulárním rozkladu. Pro dané $b \in \mathbb{K}^m$ je bod $z \in \operatorname{Im}\varphi$ minimalizující vzdálenost $\|b - z\|$ (tj. realizující vzdálenost od afinního podprostoru $\rho(b, \operatorname{Im}\varphi)$, viz další kapitola) právě komponenta $z = b_1$ rozkladu $b = b_1 + b_2$, $b_1 \in \operatorname{Im}\varphi$, $b_2 \in (\operatorname{Im}\varphi)^\perp$. Přitom ale ve zvolené bázi je zobrazení $\varphi^\dagger$, původně zadané ve standardních bázích pseudoinverzí $A^\dagger$, dáno maticí $S'$ z věty o singulárním rozkladu, zejména je $\varphi^\dagger(\operatorname{Im}\varphi) = (\operatorname{Ker}\varphi)^\perp$ a $D^{-1}$ maticí zúžení $\varphi^\dagger_{|\operatorname{Im}\varphi}$ a $\varphi^\dagger_{|(\operatorname{Im}\varphi)^\perp}$ je nulové. Je tedy skutečně

$$\varphi \circ \varphi^\dagger(b) = \varphi(\varphi^\dagger(z)) = z$$

a důkaz je ukončen.

(5) Evidentně, z rovnosti $Ax = b$ pro pevně zvolené $x \in \mathbb{K}^n$ plyne

$$b = AA^\dagger A\, x = AA^\dagger b.$$

Jde proto o podmínku nutnou. Na druhou stranu, jestliže tato podmínka platí, pak můžeme pro uvedený výraz $x$ spočíst

$$Ax = A(A^\dagger b + (E - A^\dagger A)u) = b + (A - AA^\dagger A)u = b.$$

Hodnost matice $A - A^\dagger A$ přitom dává správně velký obraz příslušného zobrazení podle Frobeniovy věty o řešení systému lineárních rovnic, proto takto dostáváme řešení všechna. □

**3.47.** Metodou nejmenších čtverců řešte soustavu

$$\begin{aligned} 2x &+ y &+ 2z &= 1,\\ x &+ y &+ 3z &= 2,\\ 2x &+ y &+ z &= 0,\\ x & &+ z &= -1. \end{aligned}$$

**Řešení.** Naše soustava nemá řešení, neboť její matice má hodnost 3, rozšířená matice soustavy pak hodnost 4. Nejlepším přiblížením vektoru $b = (1, 2, 0, -1)$ tvořeném pravými stranami rovnic soustavy můžeme tedy dle věty 3.49 dosáhnout pomocí vektoru $A^\dagger b$ ($AA^\dagger b$ je pak ono nejlepší přiblížení, neboli kolmá projekce vektoru $b$ na prostor generovaný sloupci matice $A$).

Protože sloupce matice $A$ jsou lineárně nezávislé, je její pseudoinverzní matice určena vztahem $(A^TA)^{-1}A^T$. Je tedy

$$\begin{aligned} A^\dagger &= \left(\begin{pmatrix}2&1&2\\1&1&3\\2&1&1\\1&0&1\end{pmatrix}\begin{pmatrix}2&1&2&1\\1&1&1&0\\2&3&1&1\end{pmatrix}\right)^{-1}\begin{pmatrix}2&1&2&1\\1&1&1&0\\2&3&1&1\end{pmatrix} =\\ &= \left(\begin{pmatrix}10&5&10\\5&3&6\\10&6&15\end{pmatrix}\right)^{-1}\begin{pmatrix}2&1&2&1\\1&1&1&0\\2&3&1&1\end{pmatrix} =\\ &= \begin{pmatrix}3/5&-1&0\\-1&10/3&-2/3\\0&-2/3&1/3\end{pmatrix}\begin{pmatrix}2&1&2&1\\1&1&1&0\\2&3&1&1\end{pmatrix} =\\ &= \begin{pmatrix}1/5&-2/5&1/5&3/5\\0&1/3&2/3&-5/3\\0&1/3&-1/3&1/3\end{pmatrix}. \end{aligned}$$

Je tedy hledané $\mathbf{x}$ rovno

$$A^\dagger b = (-6/5, 7/3, 1/3)^T.$$

Projekce (nejlepší přiblížení k sloupci pravých stran) je pak vektor $(3/5, 32/15, 4/15, -13/15)$. □

**Poznámka.** Lze také ukázat, že matice $A^\dagger$ minimalizuje výraz

$$\|AA^\dagger - E\|^2,$$

tj. součet kvadrátů všech prvků uvedené matice.

Z bodu (4) předchozí věty plyne, že matice $AA^\dagger$ je maticí kolmé projekce z vektorového prostoru $\mathbb{R}^n$, kde $n$ je počet řádků matice $A$ na podprostor generovaný sloupci matice $A$ (tato interpretace má samozřejmě smysl pouze pro matice mající více řádků než sloupců).

Dále pro matice $A$, jejichž sloupce tvoří nezávislé vektory, má smysl výraz $(A^TA)^{-1}A^T$ a není těžké ověřit, že tato matice splňuje všechny vlastnosti z (1) a (2) z předchozí věty, jedná se tedy o pseudoinverzi k matici $A$.

Z úvah v důkazu předcházející věty vyplývají také následující vlastnosti pseudoinverze:

**Důsledek.**
- *Pro všechny matice $A$ platí $(A^\dagger)^\dagger = A$,*
- *pokud má matice $A$, typu $m \times n$, plnou řádkovou hodnost $m$, pak $A^\dagger = A^*(AA^T)^{-1}$,*
- *pokud má matice $A$, typu $m \times n$, plnou sloupcovou hodnost $n$, pak $A^\dagger = (AA^T)^{-1}A^*$.*

**3.50. Lineární regrese.** Aproximační vlastnost (3) předchozí



věty je velice užitečná v případech, kdy máme najít co nejlepší přiblížení (neexistujícího) řešení přeurčeného systému $Ax = b$, kde $A$ je reálná matice typu $m/n$ a $m > n$.

Např. máme experimentem dáno mnoho naměřených reálných hodnot $b_j$ a chceme najít lineární kombinaci několika funkcí $f_i$, která bude co nejlépe aproximovat hodnoty $b_j$. Skutečné hodnoty zvolených funkcí v bodech $y_j \in \mathbb{R}$ zadají matici $a_{ij} = f_j(y_i)$, jejíž sloupce jsou dány hodnotami jednotlivých funkcí $f_j$ v uvažovaných bodech, a naším úkolem je tedy určit koeficienty $x_j \in \mathbb{R}$ tak, aby součet kvadrátů odchylek od skutečných hodnot

$$\sum_{i=1}^{m}\left(b_i - \left(\sum_{j=1}^{n} x_j f_j(y_i)\right)\right)^2 = \sum_{i=1}^{m}\left(b_i - \left(\sum_{j=1}^{n} a_{ij}x_j\right)\right)^2$$

byl minimální. Jinými slovy, hledáme lineární kombinaci funkcí $f_i$ takovou, abychom „dobře“ proložili zadané hodnoty $b_i$. Díky předchozí větě jsou hledané optimální koeficienty $A^\dagger b$.

Abychom měli konkrétnější představu, uvažujme pouze dvě funkce $f_1(x) = x$, $f_2(x) = x^2$ a předpokládejme, že „naměřené hodnoty“ jejich neznámé kombinace $g(x) = y_1x + y_2x^2$ v celočíselných hodnotách pro $x$ mezi 1 a 10 jsou $b^T = (1{,}44\ 10{,}64\ 4{,}48\ 14{,}56\ 31{,}12\ 39{,}20\ 54{,}88\ 71{,}28\ 85{,}92\ 104{,}16)$. Tento vektor vznikl výpočtem hodnot $x + x^2$ v daných bodech posunutých o náhodné hodnoty v rozmezí $\pm 8$. Matice $A = (b_{ij})$ je tedy v našem případě rovna

$$A^T = \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\1&4&9&16&25&36&49&64&81&100\end{pmatrix}$$

a hledané koeficienty v kombinaci jsou

$$y = A^\dagger \cdot b = \begin{pmatrix}0{,}61\\0{,}99\end{pmatrix}.$$

Výsledné proložení je nejlépe vidět v grafickém zobrazení Pokud jste spřáteleni s Maplem nebo Matlabem (nebo jiným podobným softwarem), zkuste si zaexperimentovat s podobnými úlohami a výslednými obrázky.

## G. Doplňující příklady k celé kapitole

**3.48.** Určete posloupnost reálných čísel, která vyhovuje následující nehomogenní diferenční rovnici s počátečními podmínkami:

$$2x_{n+2} = -x_{n+1} + x_n + 2, \quad x_1 = 2,\ x_2 = 3.$$

**Řešení.** Obecné řešení zhomogenizované rovnice je tvaru $a(-1)^n + b(1/2)^n$. Partikulárním řešením je konstanta 1. Obecné řešení dané nehomogenní rovnice bez počátečních podmínek je tedy

$$x_n = a(-1)^n + b\left(\frac{1}{2}\right)^n + 1.$$

Dosazením do počátečních podmínek zjistíme konstanty $a = 1, b = 4$. Dané rovnici s počátečními podmínkami tedy vyhovuje posloupnost

$$x_n = (-1)^n + 4\left(\tfrac{1}{2}\right)^n + 1. \qquad \square$$

*3.49.* Určete jedinou posloupnost vyhovující rekurentnímu vztahu

$$x_n = 7x_{n-1} - 10x_{n-2} + 8n - 22$$

s počátečními členy $x_1 = 6, x_2 = 8$. ○

*3.50.* Určete explicitní vyjádření posloupnosti vyhovující diferenční rovnici $x_{n+2} = 3x_{n+1} + 3x_n$ se členy $x_1 = 1$ a $x_2 = 3$. ○

*3.51.* Určete explicitní vzorec pro $n$-tý člen jediné posloupnosti $\{x_n\}_{n=1}^{\infty}$ vyhovující následujícím podmínkám:

$$x_{n+2} = x_{n+1} - x_n, \quad x_1 = 1,\ x_2 = 5. \qquad ○$$

*3.52.* Určete explicitní vzorec pro $n$-tý člen jediné posloupnosti $\{x_n\}_{n=1}^{\infty}$ vyhovující následujícím podmínkám:

$$-x_{n+3} = 2x_{n+2} + 2x_{n+1} + x_n, \quad x_1 = 1,\ x_2 = 1,\ x_3 = 1. \qquad ○$$

*3.53.* Určete explicitní vzorec pro $n$-tý člen jediné posloupnosti $\{x_n\}_{n=1}^{\infty}$ vyhovující následujícím podmínkám:

$$-x_{n+3} = 3x_{n+2} + 3x_{n+1} + x_n, \quad x_1 = 1,\ x_2 = 1,\ x_3 = 1. \qquad ○$$

**3.54. Jezírko.** Mějme jednoduchý model jezírka, ve kterém žije populace bílé ryby (plotice, ouklej, podoustev, ostroretka atd.). Předpokládáme, že druhého roku se dožije 20 % rybího plůdku a od tohoto stáří už jsou ryby schopny se reprodukovat. Z mladých ryb přežije z druhého do třetího roku přibližně 60 % a v dalších letech je už úmrtnost zanedbatelná. Dále předpokládáme, že roční přírustek nových plůdků je třikrát větší než počet ryb (schopných reprodukce).

Tato populace by evidentně jezírko brzy přeplnila. Rovnováhu chceme dosáhnout nasazením dravé ryby, např. štiky. Předpokládejme, že jedna štika sní ročně asi 500 dospělých bílých ryb. Kolik štik pak musíme do jezírka nasadit, aby populace stagnovala?

**Řešení.** Pokud označíme $p$ počet plůdku, $m$ počet mladých ryb a $r$ počet dospělých ryb, pak je stav populace v dalším roce popsán následovně:

$$\begin{pmatrix} p \\ m \\ r \end{pmatrix} \mapsto \begin{pmatrix} 3m + 3r \\ 0{,}2p \\ 0{,}6m + \tau r \end{pmatrix},$$

kde $1-\tau$ je relativní úmrtnost dospělé ryby způsobená štikou. Příslušná matice popisující tento model je tedy

$$\begin{pmatrix} 0 & 3 & 3 \\ 0{,}2 & 0 & 0 \\ 0 & 0{,}6 & \tau \end{pmatrix}.$$

Pokud má populace stagnovat, pak musí mít tato matice vlastní hodnotu 1. Jinými slovy, jednička musí být kořenem charakteristického polynomu této matice. Ten je tvaru $\lambda^2(\tau-\lambda)+0{,}36-0{,}6.(\tau-\lambda)=0$. To znamená, že $\tau$ musí splňovat

$$\begin{aligned} \tau - 1 + 0{,}36 - 0{,}6(\tau - 1) &= 0, \\ 0{,}4\tau - 0{,}04 &= 0. \end{aligned}$$

Do dalšího roku tedy může přežít jen 10 % z dospělých ryb a zbytek by měla sníst štika. Označíme-li hledaný počet štik $x$, pak dohromady sní $500x$ ryb, což by mělo odpovídat podle předchozího výpočtu $0{,}9r$. Poměr počtu bílé ryby ku počtu štik by tedy měl být $\frac{r}{x} = \frac{500}{09}$. To je přibližně jedna štika na 556 kusů bílé ryby. □

**3.55. Model vývoje populace velryb.** Pro vývoj populace jsou podstatné samice a u nich není důležitý věk, ale plodnost. Z tohoto hlediska můžeme samice rozdělit na novorozené neboli juvenilní, tj. dosud neplodné samice, mladé plodné samice, dospělé samice s největší plodností a samice postmenopauzní, které již plodné nejsou, ale mají velký význam při ochraně mláďat nebo vyhledávání zdrojů potravy.

Budeme modelovat vývoj takové populace v čase. Za časovou jednotku zvolíme dobu dosažení dospělosti. Novorozená samice, která tuto dobu přežije, dospěje k plodnosti. Vývoj mladé samice do plné plodnosti a vývoj dospělé samice k menopauze závisí na podmínkách prostředí. Přechod do další plodnostní kategorie je tedy náhodný jev. Stejně je náhodným jevem i úmrtí samice. Mladá plodná samice má za jednotku času průměrně méně mláďat, než samice plodná. Tyto poznatky vyjádříme formalizovaně.

Označme $x_1(t)$, resp. $x_2(t)$, resp. $x_3(t)$, resp. $x_4(t)$, množství juvenilních, resp. mladých, resp. plně plodných, resp. postmenopauzních, samic v čase $t$. Množství může vyjadřovat počet jedinců, ale také počet jedinců vztažených na jednotkový areál (tzv. populační hustotu), případně také celkovou biomasu a podobně. Dále označme $p_1$ pravděpodobnost, že juvenilní samice přežije jednotkový časový interval a tedy během něho dospěje, a $p_2$, resp. $p_3$, pravděpodobnost, že během jednotkové doby mladá, resp. plně plodná, samice, která neuhyne, dospěje do následující kategorie, tj. mladá do plné plodnosti a plně plodná k menopauze. Dalším náhodným jevem je umírání (pozitivně řečeno: přežívání) samic, které nedospějí do další kategorie; označme pravděpodobnosti přežití po řadě $q_2$, $q_3$ a $q_4$ pro mladé, plně plodné a postmenopauzní samice. Každé z čísel $p_1$, $p_2$, $p_3$, $q_2$, $q_3$, $q_4$ jakožto pravděpodobnost je z intervalu $[0, 1]$. Mladá samice může přežít, dospět do plné plodnosti nebo uhynout; tyto jevy jsou neslučitelné, společně tvoří jev jistý a možnost úmrtí nelze vyloučit. Platí tedy $p_2 + q_2 < 1$. Z podobných důvodů platí $p_3 + q_3 < 1$. Nakonec ještě označíme $f_2$, resp. $f_3$ průměrný počet dcer mladé, resp. plně plodné, samice. Tyto parametry splňují nerovnost $0 < f_2 < f_3$.

Očekávaný počet novorozených samic v následujícím časovém období je součtem dcer mladých a plně plodných samic, tj.

$$x_1(t+1) = f_2 x_2(t) + f_3 x_3(t).$$

Označme na okamžik $x_{2,1}(t+1)$ množství mladých samic v čase $t+1$, které byly v předchozím období, tj. v čase $t$ juvenilními, a $x_{2,2}(t+1)$ množství mladých samic, které již v čase $t$ byly plodné, jednotkový časový interval přežily, ale nedosáhly plné plodnosti. Pravděpodobnost $p_1$, že juvenilní samice přežije jednotkový časový interval, můžeme vyjádřit jako klasickou, tj. jako poměr $x_{2,1}(t+1)/x_1(t)$, a podobně můžeme vyjádřit pravděpodobnost $q_2$ jako poměr $x_{2,2}(t+1)/x_2(t)$. Poněvadž mladé samice v čase $t+1$ jsou právě ty, které dospěly z juvenilního stádia, a ty, které již plodné byly, přežily a nedospěly k plné plodnosti, platí

$$x_2(t+1) = x_{2,1}(t+1) + x_{2,2}(t+1) = p_1 x_1(t) + q_2 x_2(t).$$

Analogicky odvodíme očekávaný počet plně plodných samic jako

$$x_3(t+1) = p_2 x_2(t) + q_3 x_3(t)$$

a očekávaný počet postmenopauzních samic

$$x_4(t+1) = p_3 x_3(t) + q_4 x_4(t).$$

Nyní můžeme označit

$$A = \begin{pmatrix} 0 & f_2 & f_3 & 0 \\ p_1 & q_2 & 0 & 0 \\ 0 & p_2 & q_3 & 0 \\ 0 & 0 & p_3 & q_4 \end{pmatrix}, \qquad x(t) = \begin{pmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ x_4(t) \end{pmatrix}$$

a předchozí rekurentní formule přepsat v maticovém tvaru

$$x(t+1) = Ax(t).$$

Pomocí této maticové diferenční rovnice snadno spočítáme očekávané množství velrybích samic v jednotlivých plodnostních kategoriích, pokud známe složení populace v nějakém počátečním čase.

Konkrétně pro populaci kosatek dravých byly odpozorovány populační parametry

$$\begin{aligned} p_1 &= 0{,}9775, \quad q_2 = 0{,}9111, \quad f_2 = 0{,}0043, \\ p_2 &= 0{,}0736, \quad q_3 = 0{,}9534. \quad f_3 = 0{,}1132, \\ p_3 &= 0{,}0452, \quad q_4 = 0{,}9804; \end{aligned}$$

časovou jednotkou je v tomto případě jeden rok.

Začneme-li v čase $t = 0$ s jednotkovým množstvím mladých samic v nějakém neobsazeném areálu, tj. s vektorem $x(0) = (0, 1, 0, 0)^T$, můžeme spočítat

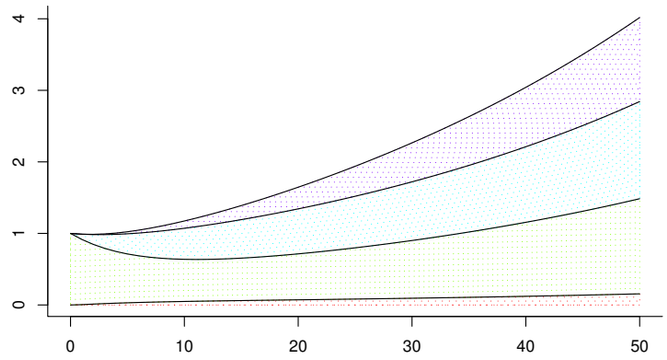
$$x(1) = \begin{pmatrix} 0 & 0{,}0043 & 0{,}1132 & 0 \\ 0{,}9775 & 0{,}9111 & 0 & 0 \\ 0 & 0{,}0736 & 0{,}9534 & 0 \\ 0 & 0 & 0{,}0452 & 0{,}9804 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0{,}0043 \\ 0{,}9111 \\ 0{,}0736 \\ 0 \end{pmatrix},$$

$$x(2) = \begin{pmatrix} 0 & 0{,}0043 & 0{,}1132 & 0 \\ 0{,}9775 & 0{,}9111 & 0 & 0 \\ 0 & 0{,}0736 & 0{,}9534 & 0 \\ 0 & 0 & 0{,}0452 & 0{,}9804 \end{pmatrix} \begin{pmatrix} 0{,}0043 \\ 0{,}9111 \\ 0{,}0736 \\ 0 \end{pmatrix} = \begin{pmatrix} 0{,}01224925 \\ 0{,}83430646 \\ 0{,}13722720 \\ 0{,}00332672 \end{pmatrix},$$

a tak můžeme pokračovat dále. Výsledky výpočtu můžeme také znázornit graficky; to je provedeno na obrázku. Vyzkoušejte si výpočet a grafické znázornění jeho výsledků i pro jiné počáteční složení populace. Výsledkem by mělo být pozorování, že celková velikost populace roste jako exponenciální funkce, poměry velikostí jednotlivých plodnostních tříd se postupně ustálí na konstantních hodnotách.

Matice $A$ má vlastní hodnoty $\lambda_1 = 1{,}025441326$, $\lambda_2 = 0{,}980400000$, $\lambda_3 = 0{,}834222976$, $\lambda_4 = 0{,}004835698$, vlastní vektor příslušný k největší vlastní hodnotě $\lambda_1$ je

$$w = (0{,}03697187,\ 0{,}31607121,\ 0{,}32290968,\ 0{,}32404724).$$




OBRÁZEK 1. Vývoj populace kosatky dravé. Na vodorovné ose je čas v letech, na svislé velikost populace. Jednotlivé plochy zobrazují množství juvenilních, mladých, plně plodných a postmenopauzních samic v tomto pořadí zdola.

Tento vektor je normován tak, aby součet jednotlivých složek byl roven 1.

Porovnejte vývoj velikosti populace s exponenciální funkcí $F(t) = \lambda_1^t x_0$, kde $x_0$ je celková velikost počáteční populace. Vypočítejte také relativní zastoupení jednotlivých plodnostních kategorií v populaci po jisté době vývoje a porovnejte ho se složkami vlastního vektoru $w$. Shoda je způsobena pouze tím, že matice $A$ má jednu vlastní hodnotu, která má absolutní hodnotu největší z absolutních hodnot všech vlastních hodnot matice $A$, a tím, že vektorový podprostor generovaný vlastními vektory příslušnými k vlastním hodnotám $\lambda_2$, $\lambda_3$, $\lambda_4$ má s nezáporným orthantem jednoprvkový průnik (pouze nulový vektor). Struktura matice $A$ však sama nezaručuje takto jednoduše předvídatelný vývoj, je totiž tzv. reducibilní.

**3.56. Model růstu populace bodláků *Dipsacus sylvestris*.** Tuto rostlinu můžeme vidět ve čtyřech podobách. Buď jako kvetoucí rostlinu nebo jako růžici listů, přičemž u růžic můžeme rozlišit trojí velikost – malé, střední a velké. Životní cyklus této jednodomé víceleté byliny můžeme popsat následovně.

Kvetoucí rostlina vyprodukuje v pozdním létě větší množství semen a uhyne. Ze semen některá vyklíčí ještě v témže roce a vyroste z nich růžice listů, nejčastěji střední velikosti. Jiná semena zůstanou v zemi a přezimují. Některá z přezimujících semen na jaře vyklíčí a vyroste z nich růžice listů; poněvadž jsou ale přezimováním oslabena, bude tato růžice s nejvyšší pravděpodobností malá. Většina z přezimujících semen zůstane v zemi, a ta z nich, která přežijí, na jaře vyklíčí a vyrostou z nich malé růžice. Po třech nebo více zimách „spící“ (odborně řečeno dormantní) semena hynou, ztrácí schopnost vyklíčit. Podle podmínek prostředí, kde rostlina roste, může malá nebo střední růžice listů do dalšího roku vyrůst, kterákoliv z růžic může zůstat ve své velikostní kategorii nebo uhynout – uschnout, být sežrána nějakým hmyzem a podobně. Střední nebo velká růžice může v následujícím roce vykvést. Kvetoucí rostlina produkuje semena a celý cyklus se opakuje.

Abychom mohli předpovídat, jak rychle se bude populace uvažovaných bodláků v krajině šířit, potřebujeme popsané procesy nějak kvantifikovat. Botanici zjistili, že kvetoucí rostlina vyprodukuje průměrně 431 semen. Pravděpodobnosti klíčení různých semen, růstu růžic listů a vykvetení jsou shrnuty v tabulce:

| jev | pravděpodobnost |
|---|---|
| semeno vyprodukované rostlinou uhyne | 0,172 |
| ze semene vyroste malá růžice v témže roce | 0,008 |
| ze semene vyroste střední růžice v témže roce | 0,070 |
| ze semene vyroste velká růžice v témže roce | 0,002 |
| ze semene přezimujícího rok vyroste malá růžice | 0,013 |
| ze semene přezimujícího rok vyroste střední růžice | 0,007 |
| ze semene přezimujícího rok vyroste velká růžice | 0,001 |
| ze semene přezimujícího dva roky vyroste malá růžice | 0,001 |
| semeno po prvním přezimování uhyne | 0,013 |
| malá růžice přežije a nevyroste | 0,125 |
| střední růžice přežije a nevyroste | 0,238 |
| velká růžice přežije a nevyroste | 0,167 |
| z malé růžice vyroste střední | 0,125 |
| z malé růžice vyroste velká | 0,036 |
| ze střední růžice vyroste velká | 0,245 |
| střední růžice vykvete | 0,023 |
| velká růžice vykvete | 0,750 |

Povšimněme si, že všechny relevantní jevy v životním cyklu rostliny mají pravděpodobnost přiřazenu a že se jedná o jevy neslučitelné.

Budeme si představovat, že populaci pozorujeme vždycky na začátku vegetačního roku, řekněme v březnu, a že ke všem uvažovaným jevům dochází ve zbytku času, dejme tomu od dubna do února. V populaci se vyskytují kvetoucí rostliny, růžice tří velikostí, vyprodukovaná semena a semena dormantní jeden nebo dva roky. Toto pozorování by mohlo svádět k tomu, že populaci rozdělíme do sedmi tříd – semena čerstvá, dormantní první rok a dormantní druhý rok, růžice malé střední a velké, kvetoucí rostliny. Avšak z vyprodukovaných semen se v témže roce vyvinou buď růžice nebo semena přezimují. Čerstvá semena tedy netvoří samostatnou třídu, jejíž velikost bychom na začátku roku mohli určit. Označme tedy:

$x_1(t)$ — počet semen dormantních první rok na jaře roku $t$,
$x_2(t)$ — počet semen dormantních druhý rok na jaře roku $t$,
$x_3(t)$ — počet malých růžic na jaře roku $t$,
$x_4(t)$ — počet středních růžic na jaře roku $t$,
$x_5(t)$ — počet velkých růžic na jaře roku $t$,
$x_6(t)$ — počet kvetoucích rostlin na jaře roku $t$.

Počet vyprodukovaných semen v roce $t$ je $431x_6(t)$. Pravděpodobnost, že semeno zůstane jako dormantní první rok, je rovna pravděpodobnosti, že ze semena nevyroste žádná růžice a že neuhyne, tedy $1 - (0{,}008 + 0{,}070 + 0{,}002 + 0{,}172) = 0{,}748$. Očekávaný počet semen dormantních jednu zimu v následujícím roce tedy je

$$x_1(t+1) = 0{,}748 \cdot 431x_6(t) = 322{,}388x_6(t).$$

Pravděpodobnost, že semeno, které již jeden rok bylo dormantní, zůstane dormantním i druhý rok je rovna pravděpodobnosti, že ze semena dormantního jeden rok nevyroste žádná růžice a že neuhyne, tedy $1 - 0{,}013 - 0{,}007 - 0{,}001 - 0{,}013 = 0{,}966$. Očekávaný počet semen dormantních dvě zimy v následujícím roce tedy bude

$$x_2(t+1) = 0{,}966x_1(t).$$

Malá růžice může vyrůst ze semena bezprostředně, ze semena dormantního jeden rok nebo dormantního dva roky. Očekávaný počet malých růžic vyrostlých bezprostředně v roce $t$ je roven

$0{,}008 \cdot 431 x_6(t) = 3{,}448 x_6(t)$. Očekávaný počet malých růžic vyrostlých ze semen dormantních jeden a dva roky je $0{,}013 x_1(t)$ a $0{,}010 x_2(t)$. S těmito nově vyrostlými malými růžicemi jsou v populaci rostlin také malé růžice starší, které nevyrostly; těch je $0{,}125 x_3(t)$. Celkový očekávaný počet malých růžic tedy je

$$x_3(t+1) = 0{,}013 x_1(t) + 0{,}010 x_2(t) + 0{,}125 x_3(t) + 3{,}448 x_6(t).$$

Analogicky určíme očekávaný počet středních a velkých růžic

$$\begin{aligned} x_4(t+1) &= 0{,}007 x_1(t) + 0{,}125 x_3(t) + 0{,}238 x_4(t) + 0{,}070 \cdot 431 x_6(t) = \\ &= 0{,}007 x_1(t) + 0{,}125 x_3(t) + 0{,}238 x_4(t) + 30{,}170 x_6, \\ x_5(t+1) &= 0{,}245 x_4(t) + 0{,}167 x_5(t) + 0{,}002 \cdot 431 x_6(t) = \\ &= 0{,}245 x_4(t) + 0{,}167 x_5(t) + 0{,}862 x_6(t). \end{aligned}$$

Kvetoucí rostlina může vyrůst ze střední nebo velké růžice. Očekávaný počet kvetoucích rostlin tedy bude

$$x_6(t+1) = 0{,}023 x_4(t) + 0{,}750 x_5(t).$$

Dospěli jsme tedy k šesti rekurentním formulím pro jednotlivé složky populace studované rostliny. Označíme nyní

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 322{,}388 \\ 0{,}966 & 0 & 0 & 0 & 0 & 0 \\ 0{,}013 & 0{,}010 & 0{,}125 & 0 & 0 & 3{,}448 \\ 0{,}007 & 0 & 0{,}125 & 0{,}238 & 0 & 30{,}170 \\ 0{,}008 & 0 & 0{,}038 & 0{,}245 & 0{,}167 & 0{,}862 \\ 0 & 0 & 0 & 0{,}023 & 0{,}750 & 0 \end{pmatrix}, \quad x(t) = \begin{pmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ x_4(t) \\ x_5(t) \\ x_6(t) \end{pmatrix}$$

a předchozí rovnosti zapíšeme v maticovém tvaru vhodném pro výpočet

$$x(t+1) = Ax(t).$$

Pokud známe počty jednotlivých složek populace v nějakém počátečním roce $t = 0$, můžeme vypočítat očekávané počty rostlin a semen v letech následujících. Můžeme také počítat celkový počet jedinců $n(t)$ v čase $t$, $n(t) = \sum_{i=1}^{6} x_i(t)$, relativní zastoupení jednotlivých složek $x_i(t)/n(t)$, $i = 1, 2, 3, 4, 5, 6$ a meziroční relativní změnu populace $n(t+1)/n(t)$. Výsledky takového výpočtu pro patnáct let a případ, že na nějakou lokalitu jsme přesadili jednu kvetoucí rostlinu, jsou uvedeny v tabulce ‖1‖. Na rozdíl od populace velryb by nyní obrázek nebyl příliš přehledný, počty rostlin jsou oproti počtům semen zanedbatelné, v obrázku by splynuly.

Matice $A$ má vlastní hodnoty

$$\begin{aligned} \lambda_1 &= 2{,}3339, & \lambda_4 &= 0{,}1187 + 0{,}1953\mathrm{i}, \\ \lambda_2 &= -0{,}9569 + 1{,}4942\mathrm{i}, & \lambda_5 &= 0{,}1187 - 0{,}1953\mathrm{i}, \\ \lambda_3 &= -0{,}9569 - 1{,}4942\mathrm{i}, & \lambda_6 &= -0{,}1274. \end{aligned}$$

Vlastní vektor příslušný k vlastní hodnotě $\lambda_1$ je

$$w = (0{,}6377,\ 0{,}2640,\ 0{,}0122,\ 0{,}0693,\ 0{,}0122,\ 0{,}0046).$$

Tento vektor je normován tak, aby součet jeho složek byl roven jedné. Vidíme, že s rostoucím časem $t$ se relativní změna velikosti populace přibližuje vlastní hodnotě $\lambda_1$, relativní zastoupení jednotlivých složek populace se přibližují složkám normovaného vlastního vektoru příslušného k vlastní hodnotě $\lambda_1$. Každá nezáporná matice, která má nenulové prvky na stejných pozicích jako matice $A$, je primitivní. Vývoj populace tedy zákonitě spěje ke stabilizované struktuře.

| $t$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $n(t)$ |
|---|---|---|---|---|---|---|---|
| 0 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 1,00 | 1,00 |
| 1 | 322,39 | 0,00 | 3,45 | 30,17 | 0,86 | 0,00 | 356,87 |
| 2 | 0,00 | 311,43 | 4,62 | 9,87 | 10,25 | 1,34 | 337,50 |
| 3 | 432,13 | 0,00 | 8,31 | 43,37 | 5,46 | 7,91 | 497,18 |
| 4 | 2 550,50 | 417,44 | 33,93 | 253,07 | 22,13 | 5,09 | 3 282,16 |
| 5 | 1 641,69 | 2 463,78 | 59,13 | 235,96 | 91,78 | 22,42 | 4 514,76 |
| 6 | 7 227,10 | 1 585,88 | 130,67 | 751,37 | 107,84 | 74,26 | 9 877,12 |
| 7 | 23 941,29 | 6 981,37 | 382,20 | 2 486,25 | 328,89 | 98,16 | 34 218,17 |
| 8 | 31 646,56 | 23 127,29 | 767,29 | 3 768,67 | 954,73 | 303,85 | 60 568,39 |
| 9 | 97 958,56 | 30 570,58 | 1 786,27 | 10 381,63 | 1 627,01 | 802,72 | 143 126,78 |
| 10 | 258 788,42 | 94 627,97 | 4 570,24 | 27 597,99 | 4 358,70 | 1 459,04 | 391 402,36 |
| 11 | 470 376,19 | 249 989,61 | 9 912,57 | 52 970,28 | 10 991,08 | 3 903,78 | 798 143,52 |
| 12 | 1 258 532,41 | 454 383,40 | 23 314,10 | 134 915,73 | 22 317,98 | 9 461,62 | 1 902 925,24 |
| 13 | 3 050 314,29 | 1 215 742,31 | 56 442,70 | 329 291,15 | 55 891,57 | 19 841,54 | 4 727 523,56 |
| 14 | 6 396 675,73 | 2 946 603,60 | 127 280,49 | 705 398,22 | 133 660,97 | 49 492,37 | 10 359 111,38 |
| 15 | 15 955 747,76 | 6 179 188,75 | 299 182,59 | 1 721 756,52 | 293 816,44 | 116 469,89 | 24 566 161,94 |

| $t$ | $\frac{x_1(t)}{n(t)}$ | $\frac{x_2(t)}{n(t)}$ | $\frac{x_3(t)}{n(t)}$ | $\frac{x_4(t)}{n(t)}$ | $\frac{x_5(t)}{n(t)}$ | $\frac{x_6(t)}{n(t)}$ | $\frac{n(t+1)}{n(t)}$ |
|---|---|---|---|---|---|---|---|
| 0 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 1,000 | 356,868 |
| 1 | 0,903 | 0,000 | 0,010 | 0,085 | 0,002 | 0,000 | 0,946 |
| 2 | 0,000 | 0,923 | 0,014 | 0,029 | 0,030 | 0,004 | 1,473 |
| 3 | 0,869 | 0,000 | 0,017 | 0,087 | 0,011 | 0,016 | 6,602 |
| 4 | 0,777 | 0,127 | 0,010 | 0,077 | 0,007 | 0,002 | 1,376 |
| 5 | 0,364 | 0,546 | 0,013 | 0,052 | 0,020 | 0,005 | 2,188 |
| 6 | 0,732 | 0,161 | 0,013 | 0,076 | 0,011 | 0,008 | 3,464 |
| 7 | 0,700 | 0,204 | 0,011 | 0,073 | 0,010 | 0,003 | 1,770 |
| 8 | 0,522 | 0,382 | 0,013 | 0,062 | 0,016 | 0,005 | 2,363 |
| 9 | 0,684 | 0,214 | 0,012 | 0,073 | 0,011 | 0,006 | 2,735 |
| 10 | 0,661 | 0,242 | 0,012 | 0,071 | 0,011 | 0,004 | 2,039 |
| 11 | 0,589 | 0,313 | 0,012 | 0,066 | 0,014 | 0,005 | 2,384 |
| 12 | 0,661 | 0,239 | 0,012 | 0,071 | 0,012 | 0,005 | 2,484 |
| 13 | 0,645 | 0,257 | 0,012 | 0,070 | 0,012 | 0,004 | 2,191 |
| 14 | 0,617 | 0,284 | 0,012 | 0,068 | 0,013 | 0,005 | 2,371 |
| 15 | 0,650 | 0,252 | 0,012 | 0,070 | 0,012 | 0,005 | |

TABULKA 1. Modelovaný vývoj populace bodláku *Dipsacus sylvestris*. Velikosti jednotlivých složek populace, celková velikost populace, relativní zastoupení jednotlivých složek a relativní přírůstky velikosti.

**3.57. Nelineární model populace.** Prozkoumejte podrobně vývoj populace pro nelineární model 1.12 z první kapitoly a hodnoty $K = 1$ a

i) míru růstu $r = 1$ a počáteční stav $p(1) = 0{,}2$,
ii) míru růstu $r = 1$ a počáteční stav $p(1) = 2$,
iii) míru růstu $r = 1$ a počáteční stav $p(1) = 3$,
iv) míru růstu $r = 2{,}2$ a počáteční stav $p(1) = 0{,}2$,

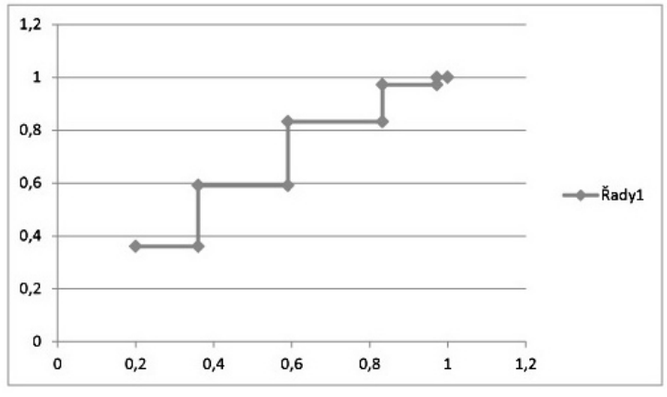
v) míru růstu $r = 3$ a počáteční stav $p(1) = 0{,}2$.

Spočítejte několik prvních členů a odhadněte, jak bude populace dále růst.

**Řešení.** (i) Prvních deset členů posloupnosti $p(n)$ je v následující tabulce. Odtud je vidět, že velikost populace konverguje k hodnotě 1.

| $n$ | $p(n)$ |
|---|---|
| 1 | 0,2 |
| 2 | 0,36 |
| 3 | 0,5904 |
| 4 | 0,83222784 |
| 5 | 0,971852502 |
| 6 | 0,999207718 |
| 7 | 0,999999372 |

Graf vývoje populace pro $r = 1$ a $p(1) = 0,2$:



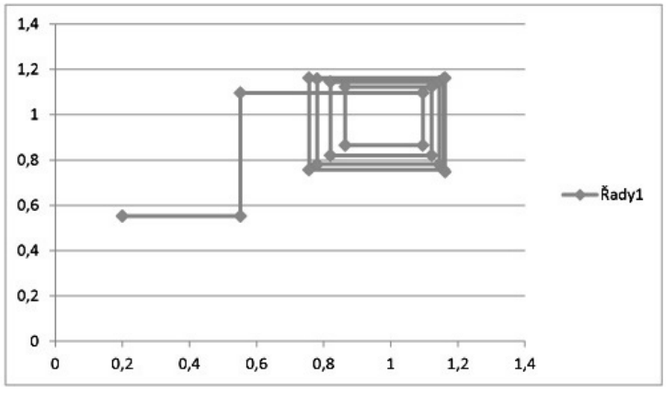

(ii) Pro počáteční hodnotu $p(1) = 2$ dostaneme $p(2) = 0$ a dál už se populace měnit nebude.
(iii) Pro $p(1) = 3$ dostáváme

| $n$ | $p(n)$ |
|---|---|
| 1 | 3 |
| 2 | -15 |
| 3 | -255 |
| 4 | -65535 |

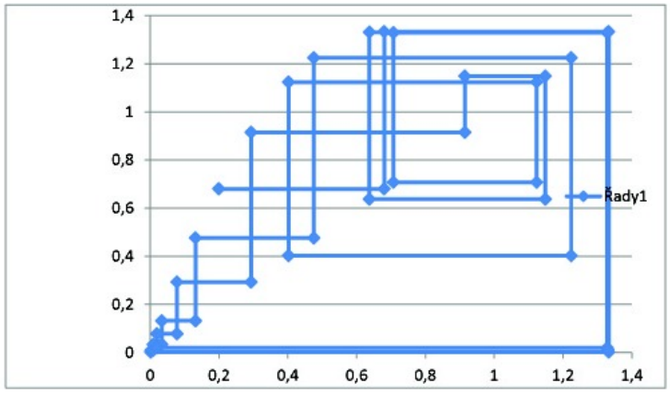
a odtud je vidět, že populace bude klesat pode všechny meze.
(iv) Pro míru růstu $r = 2,2$ a počáteční stav $p(1) = 0,2$ dostáváme

| $n$ | $p(n)$ |
|---|---|
| 1 | 0,2 |
| 2 | 0,552 |
| 3 | 1,0960512 |
| 4 | 0,864441727 |
| 5 | 1,122242628 |
| 6 | 0,820433675 |
| 7 | 1,144542647 |
| 8 | 0,780585155 |
| 9 | 1,157383491 |
| 10 | 0,756646772 |
| 11 | 1,161738128 |
| 12 | 0,748363958 |
| 13 | 1,162657716 |
| 14 | 0,74660417 |

Vidíme, že místo konvergence dostáváme v tomto případě oscilaci–po nějaké době bude populace přeskakovat mezi hodnotami 1,16 a 0,74. Graf vývoje populace pro $r = 2{,}2$ a $p(1) = 0{,}2$ pak vypadá následovně:




(v) Pro míru růstu $r = 3$ a počáteční stav $p(1) = 0,2$ je už situace složitější–populace začne oscilovat mezi více hodnotami. Abychom lépe viděli mezi kterými, bylo by potřeba spočítat ještě víc členů.




Tabulka vývoje populace:

| $n$ | $p(n)$ |
|---|---|
| 1 | 0,2 |
| 2 | 0,68 |
| 3 | 1,3328 |
| 4 | 0,00213248 |
| 5 | 0,008516278 |
| 6 | 0,033847529 |
| 7 | 0,131953152 |
| 8 | 0,475577705 |
| 9 | 1,223788359 |
| 10 | 0,402179593 |
| 11 | 1,123473097 |
| 12 | 0,707316989 |
| 13 | 1,328375987 |
| 14 | 0,019755658 |
| 15 | 0,077851775 |
| 16 | 0,293224403 |
| 17 | 0,91495596 |
| 18 | 1,148390614 |
| 19 | 0,63715945 |
| 20 | 1,330721306 |
| 21 | 0,010427642 |
| 22 | 0,041384361 |
| 23 | 0,160399447 |

□

*3.58.* **Sledovanost televizí.** V jisté zemi vysílají jisté dvě televizní stanice. Z veřejného výzkumu vyplynulo, že po jednom roce přejde 1/6 diváků první stanice ke druhé stanici, 1/5 diváků druhé stanice přejde k první stanici. Popište časový vývoj počtu diváků sledujících dané stanice jako Markovův proces, napište jeho matici, nalezněte její vlastní čísla a vlastní vektory. ○

**3.59.** Výrobní linka nefunguje spolehlivě: jednotlivé výrobky se od sebe co do kvality nezanedbatelně liší. Navíc jistý pracovník ve snaze zvýšit kvalitu neustále zasahuje do výrobního procesu. Při rozdělení výrobků do tříd I, II, III podle kvality se zjistilo, že po výrobku třídy I následuje výrobek stejné kvality v 80 % případů a třídy II v 10 % případů, po výrobku třídy II se nezmění kvalita v 60 % případů a změní se na třídu I ve 20 % případů a že po výrobku třídy III následuje výrobek stejné kvality v polovině případů a se stejnou četností pak výrobky tříd I, II. Spočtěte pravděpodobnost, že 18. výrobek je třídy I, pokud 16. výrobek v pořadí náležel do třídy III.

**Řešení.** Nejprve úlohu vyřešme bez uvážení Markovova řetězce. Sledovanému jevu vyhovují případy (16. výrobek je třídy III)

- 17. výrobek byl zařazen do třídy I a 18. do třídy I;
- 17. výrobek byl zařazen do třídy II a 18. do třídy I;
- 17. výrobek byl zařazen do třídy III a 18. do třídy I

po řadě s pravděpodobnostmi

- $0{,}25 \cdot 0{,}8 = 0{,}2$;
- $0{,}25 \cdot 0{,}2 = 0{,}05$;
- $0{,}5 \cdot 0{,}25 = 0{,}125$.

Lehce tak získáváme výsledek

$$0{,}375 = 0{,}2 + 0{,}05 + 0{,}125.$$

Nyní na úlohu nahlížejme jako na Markovův proces. Ze zadání plyne, že pořadí možných stavů „výrobek je třídy I“, „výrobek je třídy II“, „výrobek je třídy III“ odpovídá pravděpodobnostní matice přechodu

$$\begin{pmatrix} 0{,}8 & 0{,}2 & 0{,}25 \\ 0{,}1 & 0{,}6 & 0{,}25 \\ 0{,}1 & 0{,}2 & 0{,}5 \end{pmatrix}.$$

Situaci, kdy výrobek patří do třídy III, zadává pravděpodobnostní vektor $(0, 0, 1)^T$. Pro následující výrobek dostáváme pravděpodobnostní vektor

$$\begin{pmatrix} 0{,}25 \\ 0{,}25 \\ 0{,}5 \end{pmatrix} = \begin{pmatrix} 0{,}8 & 0{,}2 & 0{,}25 \\ 0{,}1 & 0{,}6 & 0{,}25 \\ 0{,}1 & 0{,}2 & 0{,}5 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

a pro další výrobek v pořadí potom vektor

$$\begin{pmatrix} 0{,}375 \\ 0{,}3 \\ 0{,}325 \end{pmatrix} = \begin{pmatrix} 0{,}8 & 0{,}2 & 0{,}25 \\ 0{,}1 & 0{,}6 & 0{,}25 \\ 0{,}1 & 0{,}2 & 0{,}5 \end{pmatrix} \cdot \begin{pmatrix} 0{,}25 \\ 0{,}25 \\ 0{,}5 \end{pmatrix},$$

jehož první složka je hledanou pravděpodobností.

Doplňme, že první metoda řešení (bez zavedení Markovova procesu) vedla k výsledku zřejmě rychleji. Uvědomme si, jak výrazně by se však první metoda znepřehlednila, kdybychom např. místo 18. výrobku uvažovali 20., 22. nebo až 30. výrobek v pořadí. Ve druhé metodě se lze omezit na do jisté míry „bezmyšlenkovité“ násobení (umocňování) matic. Při zavedení Markovova procesu jsme také současně vyšetřovali situace, kdy 18. výrobek náleží do tříd II a III. □

*3.60.* Jistá populace malých hlodavců se množí následujícím způsobem: hlodavci stáří do jednoho měsíce splodí v průměru jednoho hlodavce, na jednoho hlodavce stáří mezi jedním a dvěma měsíci připadá v průměru 12 nově narozených hlodavců. Starší hlodavci neplodí. Umírá polovina hlodavců stáří do jednoho jednoho měsíce i polovina hlodavců stáří mezi měsícem a dvěma měsíci. Více než tří měsíců se nedožije žádný. Na jakém poměru se ustálí počet hlodavců stáří do jednoho měsíce ku počtu hlodavců stáří mezi jedním a dvěma měsíci ku počtu hlodavců stáří mezi dvěma a třemi měsíci.

○

**3.61.** Opakovaně házíme hrací kostkou. Napište pravděpodobnostní matici přechodu $T$ pro Markovův řetězec „maximální počet ok dosažených do $n$-tého hodu včetně“ pro pořadí stavů $1, \ldots, 6$. Poté určete $T^n$ pro každé $n \in \mathbb{N}$.

**Řešení.** Ihned můžeme uvést

$$T = \begin{pmatrix} 1/6 & 0 & 0 & 0 & 0 & 0 \\ 1/6 & 2/6 & 0 & 0 & 0 & 0 \\ 1/6 & 1/6 & 3/6 & 0 & 0 & 0 \\ 1/6 & 1/6 & 1/6 & 4/6 & 0 & 0 \\ 1/6 & 1/6 & 1/6 & 1/6 & 5/6 & 0 \\ 1/6 & 1/6 & 1/6 & 1/6 & 1/6 & 1 \end{pmatrix},$$

kde první sloupec je určen stavem 1 a pravděpodobností 1/6 pro jeho zachování (v dalším hodu padne 1) a pravděpodobností 1/6 jeho přechodu do libovolného ze stavů $2, \ldots, 6$ (po řadě padne $2, \ldots, 6$), druhý sloupec je zadán stavem 2 a pravděpodobností 2/6 pro jeho zachování (v dalším hodu padne 1 nebo 2) a pravděpodobností 1/6 pro přechod do jakéhokoli ze stavů $3, \ldots, 6$ (padne

3, . . . , 6), až poslední sloupce získáme ze skutečnosti, že stav 6 je trvalý (pokud již padla šestka, nemůže padnout vyšší počet ok).

Rovněž pro $n \in \mathbb{N}$ lze přímo určit

$$T^n = \begin{pmatrix} \left(\frac{1}{6}\right)^n & 0 & 0 & 0 & 0 & 0 \\ \left(\frac{2}{6}\right)^n - \left(\frac{1}{6}\right)^n & \left(\frac{2}{6}\right)^n & 0 & 0 & 0 & 0 \\ \left(\frac{3}{6}\right)^n - \left(\frac{2}{6}\right)^n & \left(\frac{3}{6}\right)^n - \left(\frac{2}{6}\right)^n & \left(\frac{3}{6}\right)^n & 0 & 0 & 0 \\ \left(\frac{4}{6}\right)^n - \left(\frac{3}{6}\right)^n & \left(\frac{4}{6}\right)^n - \left(\frac{3}{6}\right)^n & \left(\frac{4}{6}\right)^n - \left(\frac{3}{6}\right)^n & \left(\frac{4}{6}\right)^n & 0 & 0 \\ \left(\frac{5}{6}\right)^n - \left(\frac{4}{6}\right)^n & \left(\frac{5}{6}\right)^n - \left(\frac{4}{6}\right)^n & \left(\frac{5}{6}\right)^n - \left(\frac{4}{6}\right)^n & \left(\frac{5}{6}\right)^n - \left(\frac{4}{6}\right)^n & \left(\frac{5}{6}\right)^n & 0 \\ 1 - \left(\frac{5}{6}\right)^n & 1 - \left(\frac{5}{6}\right)^n & 1 - \left(\frac{5}{6}\right)^n & 1 - \left(\frac{5}{6}\right)^n & 1 - \left(\frac{5}{6}\right)^n & 1 \end{pmatrix}.$$

Hodnoty v prvním sloupci totiž odpovídají postupně pravděpodobnostem, že $n$-krát po sobě padne 1, $n$-krát po sobě padne 1 nebo 2 a alespoň jednou 2 (odečítáme proto pravděpodobnost uvedenou v prvním řádku), $n$-krát po sobě padne 1, 2 nebo 3 a alespoň jednou padne 3, až v posledním řádku je pravděpodobnost, že aspoň jednou během $n$ hodů padne 6 (tu lze snadno určit z pravděpodobnosti opačného jevu). Podobně např. ve čtvrtém sloupci jsou postupně nenulové pravděpodobnosti jevů „$n$-krát po sobě padne 1, 2, 3 nebo 4“, „$n$-krát po sobě padne 1, 2, 3, 4 nebo 5 a alespoň jednou 5“ a „alespoň jednou během $n$ hodů padne 6“. Interpretace matice $T$ jako matice přechodu jistého Markovova procesu tak umožňuje rychlé vyjádření mocnin $T^n$, $n \in \mathbb{N}$. □

**3.62.** V laboratoři je prováděn pokus se stejnou pravděpodobností úspěchu i neúspěchu. Pokud se pokus podaří, bude pravděpodobnost úspěchu druhého pokusu 0,7. Jestliže skončí první pokus neúspěchem, bude pravděpodobnost úspěchu druhého pokusu pouze 0,6. Dále se bude pokračovat v provádění pokusů, kdy úspěšnost předešlého znamená, že pravděpodobnost úspěchu následujícího bude 0,7, a jeho neúspěšnost způsobí, že pravděpodobnost úspěchu následujícího bude 0,6. Pro libovolné $n \in \mathbb{N}$ stanovte pravděpodobnost, že $n$-tý pokus se podaří.

**Řešení.** Zaveďme pravděpodobnostní vektor

$$x_n = \left(x_n^1,\, x_n^2\right)^T, \quad n \in \mathbb{N},$$

kde $x_n^1$ je pravděpodobnost úspěchu $n$-tého pokusu a $x_n^2 = 1 - x_n^1$ je pravděpodobnost jeho neúspěchu. Podle zadání je

$$x_1 = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$$

a zřejmě také

$$x_2 = \begin{pmatrix} 0{,}7 & 0{,}6 \\ 0{,}3 & 0{,}4 \end{pmatrix} \cdot \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} = \begin{pmatrix} 13/20 \\ 7/20 \end{pmatrix}.$$

Při označení

$$T = \begin{pmatrix} 7/10 & 3/5 \\ 3/10 & 2/5 \end{pmatrix}$$

platí

$$x_{n+1} = T \cdot x_n, \quad n \in \mathbb{N}, \tag{3.6}$$

neboť pravděpodobnostní vektor $x_{n+1}$ závisí pouze na $x_n$ a tato závislost je totožná jako pro $x_2$ a $x_1$. Ze vztahu (‖3.6‖) bezprostředně plyne

$$x_{n+1} = T \cdot T \cdot x_{n-1} = \cdots = T^n \cdot x_1, \quad n \geq 2,\ n \in \mathbb{N}. \tag{3.7}$$

Proto vyjádříme $T^n$, $n \in \mathbb{N}$. Jedná se o Markovův proces, a tudíž je 1 vlastní číslo matice $T$. Druhé vlastní číslo 0,1 můžeme snadno získat, pokud si všimneme, že stopa (součet prvků na diagonále)

je rovna součtu všech vlastních čísel (každé vlastní číslo bereme tolikrát, jaká je jeho algebraická násobnost). Těmto vlastním číslům pak přísluší vlastní vektory

$$\begin{pmatrix}2\\1\end{pmatrix}, \quad \begin{pmatrix}1\\-1\end{pmatrix}.$$

Dostáváme tak

$$T = \begin{pmatrix}2 & 1\\1 & -1\end{pmatrix} \cdot \begin{pmatrix}1 & 0\\0 & 1/10\end{pmatrix} \cdot \begin{pmatrix}2 & 1\\1 & -1\end{pmatrix}^{-1},$$

tj. pro $n \in \mathbb{N}$ je

$$\begin{aligned} T^n &= \begin{pmatrix}2 & 1\\1 & -1\end{pmatrix} \cdot \begin{pmatrix}1 & 0\\0 & 1/10\end{pmatrix}^n \cdot \begin{pmatrix}2 & 1\\1 & -1\end{pmatrix}^{-1} = \\ &= \begin{pmatrix}2 & 1\\1 & -1\end{pmatrix} \cdot \begin{pmatrix}1^n & 0\\0 & 10^{-n}\end{pmatrix} \cdot \begin{pmatrix}2 & 1\\1 & -1\end{pmatrix}^{-1}. \end{aligned}$$

Dosazení

$$\begin{pmatrix}2 & 1\\1 & -1\end{pmatrix}^{-1} = \frac{1}{3}\begin{pmatrix}1 & 1\\1 & -2\end{pmatrix}$$

a roznásobení dává

$$T^n = \frac{1}{3}\begin{pmatrix}2+10^{-n} & 2-2\cdot 10^{-n}\\1-10^{-n} & 1+2\cdot 10^{-n}\end{pmatrix}, \quad n \in \mathbb{N}.$$

Odtud z (‖3.6‖) a (‖3.7‖) plyne

$$x_{n+1} = \left(\frac{2}{3} - \frac{1}{6\cdot 10^n}, \frac{1}{3} + \frac{1}{6\cdot 10^n}\right)^T, \quad n \in \mathbb{N}.$$

Zvláště vidíme, že pro velká $n$ je pravděpodobnost úspěchu $n$-tého pokusu blízká $2/3$. □

**3.63.** Dva hráči $A$, $B$ hrají o peníze opakovaně jistou hru, která může skončit pouze vítězstvím jednoho z hráčů. Pravděpodobnost výhry hráče $A$ je v každé jednotlivé hře $p \in [0, 1/2)$ a oba sází vždy (v libovolné hře) jen 1 Kč, tj. po každé hře s pravděpodobností $p$ dá 1 Kč hráč $B$ hráči $A$ a s pravděpodobností $1-p$ naopak 1 Kč dá hráč $A$ hráči $B$. Hrají ovšem tak dlouho, dokud jeden z nich nepřijde o všechny peníze. Jestliže má hráč $A$ na začátku $x$ Kč a hráč $B$ má $y$ Kč, určete pravděpodobnost, že hráč $A$ vše prohraje.

**Řešení.** Tato úloha se nazývá Ruinování hráče. Jedná se o speciální Markovův řetězec (viz také příklad Mlsný hazardér) s mnoha důležitými aplikacemi. Hledaná pravděpodobnost činí

$$\frac{1-\left(\frac{p}{1-p}\right)^y}{1-\left(\frac{p}{1-p}\right)^{x+y}}. \tag{3.8}$$

Povšimněme si, jaká je tato hodnota pro konkrétní volby $p$, $x$, $y$. Kdyby hráč $B$ chtěl mít téměř jistotu a požadoval, aby pravděpodobnost, že hráč $A$ s ním prohraje 1 000 000 Kč, byla alespoň 0,999, potom stačí, aby měl 346 Kč, je-li $p = 0{,}495$ (či 1 727 Kč, je-li $p = 0{,}499$). Proto je ve velkých kasinech možné, aby „vášniví“ hráči mohli hrát téměř spravedlivé hry. □

**3.64.** Jirka má ve zvyku si každý večer zaběhat. Má tři trasy – krátkou, střední a dlouhou. Pokud si někdy zvolí krátkou trasu, následující den si to vyčítá a rozhodne se libovolně (tj. se stejnou pravděpodobností) pro dlouhou, nebo střední. Jestliže si v některý den zvolí dlouhou trasu, v následujícím dnu volí zcela libovolně jednu z tras. Pokud běžel středně dlouhou trasu, cítí se dobře a druhý den si se stejnou pravděpodobností vybere buď střední, nebo dlouhou. Předpokládejte, že takto běhá každý večer už velmi dlouhou dobu. Jak často volí krátkou a jak často dlouhou trasu? Jaká je pravděpodobnost, že si zvolí dlouhou trasu, když si ji zvolil přesně před týdnem?

**Řešení.** Zřejmě se jedná o Markovův proces se třemi možnými stavy, a to volbami krátké, střední a dlouhé trasy. Toto pořadí stavů dává pravděpodobnostní matici přechodu

$$T = \begin{pmatrix} 0 & 0 & 1/3 \\ 1/2 & 1/2 & 1/3 \\ 1/2 & 1/2 & 1/3 \end{pmatrix}.$$

Stačí si uvědomit, že např. druhý sloupec odpovídá volbě střední trasy v minulém dnu, která znamená, že s pravděpodobností $1/2$ bude opět zvolena střední trasa (druhý řádek) a s pravděpodobností $1/2$ bude zvolena dlouhá trasa (třetí řádek). Neboť je

$$T^2 = \begin{pmatrix} 1/6 & 1/6 & 1/9 \\ 5/12 & 5/12 & 4/9 \\ 5/12 & 5/12 & 4/9 \end{pmatrix},$$

můžeme využít důsledků Perronovy-Frobeniovy věty pro Markovovy procesy. Není obtížné vypočítat, že vlastním vektorem, který přísluší vlastnímu číslu 1 a který je pravděpodobnostní, je právě

$$\left(\frac{1}{7}, \frac{3}{7}, \frac{3}{7}\right)^T.$$

Hodnoty $1/7, 3/7, 3/7$ pak udávají po řadě pravděpodobnosti, že v náhodně určeném dnu volí trasu krátkou, střední, dlouhou.

Nechť si Jirka v jistý den (v čase $n \in \mathbb{N}$) vybere dlouhou trasu. Tomuto rozhodnutí odpovídá pravděpodobnostní vektor

$$x_n = (0,\ 0,\ 1)^T.$$

Pro následující den tedy platí

$$x_{n+1} = \begin{pmatrix} 0 & 0 & 1/3 \\ 1/2 & 1/2 & 1/3 \\ 1/2 & 1/2 & 1/3 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/3 \\ 1/3 \\ 1/3 \end{pmatrix},$$

až po sedmi dnech je

$$x_{n+7} = T^7 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = T^6 \cdot \begin{pmatrix} 1/3 \\ 1/3 \\ 1/3 \end{pmatrix}.$$

Vyčíslením dostáváme jako složky $x_{n+7}$ hodnoty

$$0{,}142\,861\,225\ldots;\quad 0{,}428\,569\,387\ldots;\quad 0{,}428\,569\,387\ldots.$$

Tedy pravděpodobnost, že zvolí dlouhou trasu za podmínky, že si ji zvolil před sedmi dny, činí přibližně $0{,}428\,569 \approx 3/7 \doteq 0{,}428\,571$. □

*3.65.* V rámci jisté společnosti fungují dvě navzájem si konkurující oddělení. Vedení společnosti se rozhodlo, že každý týden bude poměřovat relativní (vzhledem k počtu zaměstnanců) zisky dosažené těmito dvěma odděleními. Do oddělení, které bude úspěšnější, pak budou přeřazeni dva pracovníci

z druhého oddělení. Tento proces má probíhat tak dlouho, až jedno z oddělení zanikne. Získali jste zaměstnání v této společnosti a můžete si vybrat jedno z těchto dvou oddělení, kde budete pracovat. Chcete si zvolit to, které nebude v důsledku vnitropodnikové konkurence zrušeno. Jaká bude Vaše volba, když jedno oddělení má nyní 40 zaměstnanců, druhé 10 a když odhadujete, že to v současnosti menší z nich bude mít větší relativní zisky v 54 % případů? ○

*3.66.* Student na koleji je značně společensky unaven (v důsledku toho není schopen plně vnímat smyslové podněty a koordinovat své pohyby). V tomto stavu se přesto rozhodne, že na právě probíhající večírek pozve známou, která má pokoj na jednom konci chodby. Na opačném konci chodby však bydlí někdo, koho pozvat rozhodně nehodlá. Je ovšem natolik „unaven“, že rozhodnutí udělat krok zvoleným směrem se mu podaří realizovat pouze v 53 ze 100 pokusů (ve zbylých 47 jde přesně na opačnou stranu). Za předpokladů, že vyjde v polovině chodby a že vzdálenost k oběma dveřím na koncích chodby odpovídá jeho 20 krokům, stanovte pravděpodobnost, že nejdříve dorazí ke správným dveřím. ○

**3.67.** Nechť $n \in \mathbb{N}$ osob hraje tzv. tichou poštu. Pro jednoduchost předpokládejte, že první osoba zašeptá druhé právě jedno (libovolně zvolené) ze slov „ano“, „ne“. Druhá osoba pak potichu řekne třetí osobě to ze slov „ano“, „ne“, o kterém si myslí, že ho řekla první osoba. Takto to pokračuje až k $n$-té osobě. Jestliže pravděpodobnost toho, že při libovolném předání se zamění (nechtě, úmyslně) šířené slovo na to druhé, je $p \in (0, 1)$, stanovte pro velká $n \in \mathbb{N}$ pravděpodobnost, že $n$-tá osoba určí správně slovo zvolené první osobou.

**Řešení.** Na tuto úlohu lze nahlížet jako na Markovův řetězec se dvěma stavy nazvanými Ano a Ne, kdy řekneme, že proces je ve stavu Ano v čase $m \in \mathbb{N}$, pokud si $m$-tá osoba bude myslet, že předávané slovo je „ano“. Pro pořadí stavů Ano, Ne je pravděpodobnostní matice přechodu

$$T = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}.$$

Součin matice $T^{m-1}$ a pravděpodobnostního vektoru počáteční volby první osoby potom udává pravděpodobnosti toho, co si bude myslet $m$-tá osoba. Mocniny této matice ovšem počítat nemusíme, neboť všechny prvky matice $T$ jsou kladná čísla. Navíc tato matice je dvojnásobně stochastická. Víme tudíž, že pro velká $n \in \mathbb{N}$ bude pravděpodobnostní vektor blízký vektoru $(1/2, 1/2)^T$. Pravděpodobnost, že $n$-tá osoba řekne „ano“, je proto přibližně stejná jako pravděpodobnost, že řekne „ne“, a to nezávisle na tom, pro které slovo se rozhodla první osoba. Pro velký počet zúčastněných tak platí, že zhruba polovina z nich uslyší „ano“ (zopakujme, že nezávisle na tom, které slovo bylo na začátku vybráno).

Pro úplnost zjistěme, jak by úloha dopadla, kdybychom předpokládali, že pravděpodobnost záměny „ano“ na „ne“ je u libovolné osoby $p \in (0, 1)$ a pravděpodobnost záměny „ne“ na „ano“ je obecně odlišné $q \in (0, 1)$. V tomto případě pro stejné pořadí stavů dostáváme pravděpodobnostní matici přechodu

$$T = \begin{pmatrix} 1-p & q \\ p & 1-q \end{pmatrix},$$

která vede (pro velká $n \in \mathbb{N}$) k pravděpodobnostnímu vektoru blízkému vektoru

$$\left( \frac{q}{p+q}, \frac{p}{p+q} \right)^T,$$

což kupř. plyne z vyjádření matice

$$T^n = \frac{1}{p+q}\left[\begin{pmatrix} q & q \\ p & p \end{pmatrix} + (1-p-q)^n \begin{pmatrix} p & -q \\ -p & q \end{pmatrix}\right].$$

Rovněž tentokrát při dostatečném počtu lidí nezáleželo na volbě slova, kterou učinila první osoba. Stručně řečeno, v tomto modelu platí, že nezáleží na původním rozhodnutí, protože o tom, jakou informaci si lidé předávají, rozhodují oni sami; přesněji řečeno, lidé sami rozhodují o četnosti výskytu „ano“ a „ne“, pokud je jich dostatečný počet (a chybí-li jakékoli ověřování).

Doplňme ještě, že výše uvedený závěr byl experimentálně ověřen. V psychologických pokusech byl mj. jedinec opakovaně vystaven vjemu, který šlo vnímat dvěma různými způsoby, a to v časových intervalech zaručujících, aby si subjekt pamatoval předešlý vjem. Viz např. „T. Havránek a kol.: *Matematika pro biologické a lékařské vědy*, Praha, Academia 1981“, kde je uveden experiment, v němž je zábleskem osvětlován v pevných časových odstupech nejednoznačný obraz (třeba náčrt krychle vnímatelný jako nadhled i podhled). Takový proces je totiž Markovovým řetězcem s maticí přechodu

$$\begin{pmatrix} 1-p & q \\ p & 1-q \end{pmatrix},$$

kde $p, q \in (0, 1)$. □

**3.68.** V jisté hře si můžete vybrat jednoho ze dvou soupeřů. Pravděpodobnost, že porazíte lepšího, je 1/4, zatímco horšího ze soupeřů porazíte s pravděpodobností 1/2. Soupeři ale nejsou rozlišeni, a tak nevíte, který z nich je ten lepší. Čeká Vás velké množství her (pro každou můžete zvolit jiného soupeře) a samozřejmě chcete dosáhnout celkově co největšího podílu vítězných her. Uvažte tyto dvě strategie:

1. Pro první hru si vyberete soupeře náhodně. Pokud nějakou hru vyhrajete, pokračujete se stejným soupeřem; jestliže ji prohrajete, změníte pro další hru soupeře.
2. Pro první dvě hry si vyberete (jednoho) soupeře náhodně. Dále se řídíte výsledkem předchozích dvou her, kdy na další dvě hry změníte soupeře, právě když obě předchozí prohrajete.

Kterou ze strategií (moudře) zvolíte?

**Řešení.** Obě strategie jsou vlastně Markovovým řetězcem. Pro jednoduchost horšího ze soupeřů označujme jako osobu $A$ a lepšího ze soupeřů jako osobu $B$. V prvním případě pro stavy „hra s osobou $A$“, „hra s osobou $B$“ (a toto jejich pořadí) dostáváme pravděpodobnostní matici přechodu

$$\begin{pmatrix} 1/2 & 3/4 \\ 1/2 & 1/4 \end{pmatrix}.$$

Tato matice má všechny prvky kladné, a proto stačí najít pravděpodobnostní vektor $x_\infty$, který přísluší vlastnímu číslu 1. Platí

$$x_\infty = \left(\frac{3}{5}, \frac{2}{5}\right)^T.$$

Jeho složky odpovídají pravděpodobnostem, že po dlouhé řadě her bude soupeřem osoba $A$, resp. $B$. Lze tedy očekávat, že 60 % her bude hráno proti horšímu ze soupeřů. Neboť

$$\frac{2}{5} = \frac{3}{5} \cdot \frac{1}{2} + \frac{2}{5} \cdot \frac{1}{4},$$

vítězných her bude kolem 40 %.

Pro druhou strategii zaveďme stavy „dvě hry po sobě s osobou $A$“ a „dvě hry po sobě s osobou $B$“, které vedou na pravděpodobnostní matici přechodu

$$\begin{pmatrix} 3/4 & 9/16 \\ 1/4 & 7/16 \end{pmatrix}.$$

Snadno určíme, že nyní je

$$x_\infty = \left(\frac{9}{13}, \frac{4}{13}\right)^T.$$

Proti horšímu ze soupeřů by se tak hrálo (9/4)-krát častěji než proti lepšímu z nich. Připomeňme, že pro první strategii to bylo (3/2)-krát častěji. Druhá strategie je proto výhodnější. Ještě poznamenejme, že při druhé strategii bude přibližně 42,3 % her vítězných. Stačí totiž vyčíslit

$$0{,}423 \doteq \tfrac{11}{26} = \tfrac{9}{13} \cdot \tfrac{1}{2} + \tfrac{4}{13} \cdot \tfrac{1}{4}. \qquad \square$$

**3.69.** Petr se pravidelně setkává se svým kamarádem. Je ovšem „proslulý“ svou nedochvilností. Snaží se ale změnit, a proto platí, že v polovině případů přijde včas a v jedné desetině případů dokonce ještě dříve, pokud na minulé setkání přišel pozdě. Jestliže minule přišel včas nebo dříve, než měl přijít, vrátí se ke své „bezstarostnosti“ a s pravděpodobností 0,8 dorazí pozdě a pouze s pravděpodobností 0,2 včas. Jaké je pravděpodobnost, že na dvacáté setkání přijde pozdě, když na jedenácté přišel včas?

**Řešení.** Zřejmě se jedná o Markovův proces se stavy „Petr přijde pozdě“, „Petr přijde včas“, „Petr přijde dříve“ a s pravděpodobnostní maticí přechodu (pro uvedené pořadí stavů)

$$T = \begin{pmatrix} 0{,}4 & 0{,}8 & 0{,}8 \\ 0{,}5 & 0{,}2 & 0{,}2 \\ 0{,}1 & 0 & 0 \end{pmatrix}.$$

Jedenácté setkání je určeno pravděpodobnostním vektorem $(0, 1, 0)^T$ (s jistotou víme, že Petr přišel včas). Dvacátému setkání pak odpovídá pravděpodobnostní vektor

$$T^9 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0{,}571\,578\,368 \\ 0{,}371\,316\,224 \\ 0{,}057\,105\,408 \end{pmatrix}.$$

Hledaná pravděpodobnost je tudíž 0,571 578 368 (přesně). Dodejme, že je

$$T^9 = \begin{pmatrix} 0{,}571\,316\,224 & 0{,}571\,578\,368 & 0{,}571\,578\,368 \\ 0{,}371\,512\,832 & 0{,}371\,316\,224 & 0{,}371\,316\,224 \\ 0{,}057\,170\,944 & 0{,}057\,105\,408 & 0{,}057\,105\,408 \end{pmatrix}.$$

Odtud vidíme, jak málo záleží na tom, zda přišel na jedenácté setkáni pozdě (první sloupec), včas nebo dříve (druhý a současně třetí sloupec). $\square$

**3.70.** Dva studenti $A$ a $B$ tráví každé pondělní odpoledne hraním jisté počítačové hry o to, kdo z nich večer zaplatí společnou útratu v restauraci. Hra může rovněž skončit remízou, kdy večer oba platí právě polovinu útraty. Výsledek předešlé hry částečně ovlivňuje hru následující. Pokud tedy před týdnem vyhrál student $A$, potom s pravděpodobností 3/4 vyhraje opět a s pravděpodobností 1/4 skončí hra remízou. Remíza se opakuje s pravděpodobností 2/3 a s pravděpodobností 1/3 vyhraje ve hře následující po remíze student $B$. Pokud před týdnem vyhrál student $B$, pak s pravděpodobností 1/2 své vítězství zopakuje a s pravděpodobností 1/4 vyhraje student $A$. Nalezněte pravděpodobnost, že dnes bude každý platit polovinu útraty, jestliže první hru před velmi dlouhou dobou vyhrál student $A$.

**Řešení.** Vlastně je zadán Markovův proces se stavy „vyhraje student $A$“, „hra skončí remízou“, „vyhraje student $B$“ (v tomto pořadí) pravděpodobnostní maticí přechodu

$$T = \begin{pmatrix} 3/4 & 0 & 1/4 \\ 1/4 & 2/3 & 1/4 \\ 0 & 1/3 & 1/2 \end{pmatrix}.$$

Chceme najít pravděpodobnost přechodu z prvního stavu do druhého po velkém počtu $n \in \mathbb{N}$ kroků (týdnů). Matice $T$ je primitivní, protože

$$T^2 = \begin{pmatrix} 9/16 & 1/12 & 5/16 \\ 17/48 & 19/36 & 17/48 \\ 1/12 & 7/18 & 1/3 \end{pmatrix}.$$

Stačí tak najít vlastní pravděpodobnostní vektor $x_\infty$ matice $T$ příslušný vlastnímu číslu 1. Snadno lze spočítat, že

$$x_\infty = \left(\frac{2}{7}, \frac{3}{7}, \frac{2}{7}\right)^T.$$

Víme, že vektor $x_\infty$ se jen velmi málo liší od pravděpodobnostního vektoru pro velká $n$ a téměř nezávisí na počátečním stavu, tj. pro velká $n \in \mathbb{N}$ můžeme klást

$$T^n \approx \begin{pmatrix} 2/7 & 2/7 & 2/7 \\ 3/7 & 3/7 & 3/7 \\ 2/7 & 2/7 & 2/7 \end{pmatrix}.$$

Hledaná pravděpodobnost je prvkem této matice na druhé pozici v prvním sloupci (je druhou složkou vektoru $x_\infty$). Poměrně rychle jsme nalezli výsledek 3/7. □

*3.71.* Adam, Bedřich a Čeněk si házejí balónem. Adam jej s pravděpodobností $\frac{1}{2}$ hodí Čeňkovi, s pravděpodobností $\frac{1}{2}$ Bedřichovi. Bedřich jej s pravděpodobností $\frac{1}{3}$ hodí Adamovi a s pravděpodobností $\frac{2}{3}$ Čeňkovi. Konečně Čeněk jej hodí s pravděpodobností $\frac{4}{5}$ Adamovi a s pravděpodobností $\frac{1}{5}$ Bedřichovi. Sestavte matici tohoto Markovova procesu a určete, s jakou pravděpodobností se míč bude nacházet po velkém počtu hodů u Bedřicha (každý potřebuje stejný čas na odhození balónu).

○

*3.72.* Sheldon a Leonard si házejí balónem přes síť. Pravděpodobnost, že Sheldon dokáže přehodit síť jsou 3/5 (s pravděpodobností 2/5 zůstane míč na jeho straně). Pravděpodobnost, že Leonard přehodí síť jsou 4/5 (s pravděpodobností 1/5 zůstane míč na jeho straně). Jaká je pravděpodobnost, že po velkém počtu pokusů obou pánů bude míč na Sheldonově straně? Formulujte úlohu jako Markovův proces a uveďte jeho matici. ○

**3.73.** Ukažte, že symetrická matice

$$\tfrac{1}{2}\begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

má vlastní hodnoty $\lambda_l = \cos\varphi_l$, kde $\varphi_l = \frac{l\pi}{n+1}$ s $1 \le l \le n$ a že příslušné vlastní vektory $\sqrt{\frac{2}{n+1}}(\sin\varphi_l, \sin 2\varphi_l, \vdots \sin n\varphi_l)$ tvoří ortonormální bázi.

**Řešení.** Nejprve spočítáme, čemu je rovna k-tá složka vektoru

$$\frac{1}{2}\sqrt{\frac{2}{n+1}}\begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}\begin{pmatrix} \sin\varphi_l \\ \sin 2\varphi_l \\ \vdots \\ \sin n\varphi_l \end{pmatrix}$$

Použitím součtového vzorce pro sinus dostáváme

$$\frac{1}{2}\sqrt{\frac{2}{n+1}}(\sin(k-1)\varphi_l + \sin(k+1)\varphi_l) = \sqrt{\frac{2}{n+1}}\sin k\varphi_l \cos\varphi_l,$$

takže daný vektor je opravdu vlastní vektor s vlastní hodnotou $\cos\varphi_l$. Protože máme n různých vlastních čísel (což je dimenze), tvoří tyto vlastní vektory bázi. Nyní zbývá ověřit, že vlastní vektory jsou ortogonální a normované. □

## Řešení cvičení

*3.2.* Denní dávka by měla sestávat z 3,9 kg sena a 4,3 kg ovsa. Náklady na dávku potom budou 13,82 Kč.

*3.12.* $x_n = 4^n + 2 \cdot (-2)^n + 1 = (2^n + (-1)^n)^2$.

*3.19.* Leslieho matice daného modelu je (úmrtnost v první skupině označíme $a$)

$$\begin{pmatrix} 0 & 2 & 2 \\ a & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Podmínka stagnace populace odpovídá tomu, že matice má vlastní hodnotu 1, neboli polynom $\lambda^3 - 2a\lambda - 2a$ má mít kořen 1, t.j $a = 1/4$.

*3.25.* Stejně jako v (‖3.24‖) skončí hra po třech sázkách. Jsou tedy opět všechny mocniny $A$, počínaje $A^3$ shodné.

$$A^{100} = A^3 = \begin{pmatrix} 1 & 7/8 & 3/4 & 1/2 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1/8 & 1/4 & 1/2 & 1 \end{pmatrix}.$$

*3.31.* Je, není, není, je.

*3.39.*

- Tvrzení je pravdivé. ($B := A^T A$, $b_{ij}$ = ($i$-tý řádek $A^T$) $\cdot$ ($j$-tý sloupec $A$)= $b_{ji}$ = ($j$-tý řádek $A^T$) $\cdot$ ($i$-tý sloupec $A$)=($j$-tý sloupec $A$) $\cdot$ ($i$-tý řádek $A^T$).
- Tvrzení zřejmě neplatí. Uvažte např. $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

*3.41.*

$$\begin{pmatrix} 1 & 0 & 0 & \\ & 1 & -2 & 0 \\ 0 & 1 & 1 & \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}.$$

*3.49.* $x_n = 2^{n+1} - 5^{n-1} + 2n + 1$.

*3.50.*

$$x_n = \frac{1}{\sqrt{21}} \left( \frac{3 + \sqrt{21}}{2} \right)^n - \frac{1}{\sqrt{21}} \left( \frac{3 - \sqrt{21}}{2} \right)^n.$$

*3.51.* $x_n = 2\sqrt{3} \sin(n \cdot (\pi/6)) - 4 \cos(n \cdot (\pi/6))$.

*3.52.* $x_n = -3(-1)^n - 2 \cos(n \cdot (2\pi/3)) - 2\sqrt{3} \sin(n \cdot ((2\pi/3))$.

*3.53.* $x_n = (-1)^n(-2n^2 + 8n - 7)$.

*3.58.*

$$\begin{pmatrix} \frac{5}{6} & \frac{1}{5} \\ \frac{1}{6} & \frac{4}{5} \end{pmatrix}.$$

Matice má dominantní vlastní hodnotu 1, příslušný vlastní vektor je $(\frac{6}{5}, 1)$. Protože je vlastní hodnota dominantní, tak se poměr diváků se ustálí na poměru 6 : 5.

*3.60.* 36 : 6 : 1.

*3.65.* Můžeme využít výsledku úlohy označované jako Ruinování hráče. Pravděpodobnost, že zanikne to oddělení, které má nyní 40 zaměstnanců, je podle tohoto příkladu rovna

$$\frac{1 - \left( \frac{0{,}46}{1-0{,}46} \right)^5}{1 - \left( \frac{0{,}46}{1-0{,}46} \right)^{25}} \doteq 0, 56.$$

Stačilo dosadit $p = 1 - 0,54$, $y = 10/2$ a $x = 40/2$ do (‖3.8‖). Prozíravější je tedy zvolit v tuto chvíli menší oddělení.

*3.66.* Znovu se jedná o speciální případ Ruinování hráče. Stačí zadání vhodně přeformulovat. Pro $p = 0,47$, $y = 20$ a $x = 20$ z (‖3.8‖) plyne výsledek

$$0,917 \doteq \frac{1 - \left(\frac{0,47}{1-0,47}\right)^{20}}{1 - \left(\frac{0,47}{1-0,47}\right)^{40}}.$$

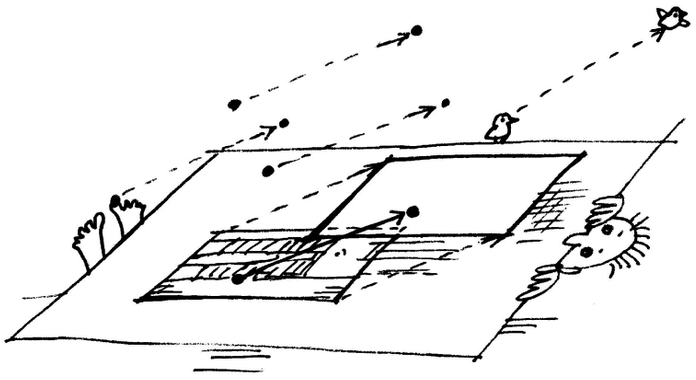
*3.71.* Matice procesu je $\begin{pmatrix} 0 & \frac{1}{3} & \frac{4}{5} \\ \frac{1}{2} & 0 & \frac{1}{5} \\ \frac{1}{2} & \frac{2}{3} & 0 \end{pmatrix}$, vlastní vektor příslušný vlastní hodnotě 1 je $(\frac{13}{9}, 1, \frac{25}{18})$, hledaná pravděpodobnost pak $\dfrac{1}{13/9 + 1 + 25/18} = \dfrac{6}{23}$.

*3.72.* $\begin{pmatrix} \frac{1}{5} & \frac{3}{5} \\ \frac{4}{5} & \frac{2}{5} \end{pmatrix}$, resp. $\begin{pmatrix} \frac{2}{5} & \frac{4}{5} \\ \frac{3}{5} & \frac{1}{5} \end{pmatrix}$, vlastní vektor příslušný vlastní hodnotě 1 je $(1, 4/3)$, resp. $(4/3, 1)$, hledaná pravděpodobnost $4/7$.

KAPITOLA 4

# Analytická geometrie

*poloha, incidence, projekce?*
*– a zase skončíme u matic...*



## A. Afinní geometrie

**4.1.** Napište parametrické vyjádření přímky určené v $\mathbb{R}^3$ rovnicemi

$$\begin{aligned} x &- 2y + z = 2,\\ 2x &+ y - z = 5. \end{aligned}$$



**Řešení.** Zřejmě postačuje vyřešit uvedenou soustavu rovnic. Jde o dvě lineární rovnice o třech neznámých. Jejím řešením je jednoparametrický systém $(x, y, z) = (t, 3t - 7, 5t - 12)$, což je již hledané parametrické vyjádření.

Můžeme ale postupovat také odlišně. Potřebujeme totiž najít nenulový (směrový) vektor, který bude kolmý na (normálové) vektory $(1, -2, 1), (2, 1, -1)$. Ten můžeme najít jednak vyřešením soustavy rovnic

$$\begin{aligned} x_1 &- 2x_2 + x_3 = 0,\\ 2x_1 &+ x_2 - x_3 = 0 \end{aligned}$$

vystihující, že skalární součin hledaného vektoru $(x_1, x_2, x_3)$ s vektory $(1, -2, 1)$ i $(2, 1, -1)$ bude nulový (jde o zhomogenizovaný původní systém). Řešením je jednoparametrický systém kolmých vektorů $(t, 3t, 5t)$. Vektor $(x_1, x_2, x_3)$ můžeme také určit přímo, pomocí

Vrátíme se teď k našemu pohledu na geometrii, když jsme zkoumali polohy bodů v rovině v 5. části první kapitoly, viz 1.23. Budeme se nejprve zajímat o vlastnosti prostorových objektů vymezených pomocí bodů, přímek, rovin apod. Podstatné přitom bude vyjasnění, jak jejich vlastnosti souvisí s pojmem vektorů a zda závisí na pojmu velikosti vektorů.

V další části pak použijeme lineární algebru pro studium objektů, které už lineárně definované nejsou. Opět přitom budeme potřebovat trochu více maticového počtu. Výsledky budou důležité později při diskusi technik pro optimalizace, tj. hledání extrémů funkčních hodnot.

Projektivní rozšíření afinních prostorů nám v závěru kapitoly ukáže, jak lze překvapivě snadno dosáhnout zjednodušení i stability algoritmických postupů typických pro práci s počítačovou grafikou.

### 1. Afinní a euklidovská geometrie



Když jsme si ujasňovali strukturu řešení systémů lineárních rovnic v první části předchozí kapitoly, zjistili jsme v odstavci 3.1, že všechna řešení nehomogenních systémů rovnic sice netvoří vektorové podprostory, vždy ale vznikají tak, že k jednomu jedinému řešení přičteme celý vektorový prostor řešení příslušné homogenní soustavy. Naopak, rozdíl dvou řešení nehomogenní soustavy je vždy řešením soustavy homogenní. Obdobně se chovají lineární diferenční rovnice, jak jsme již viděli v odstavci 3.14.

**4.1. Afinní prostory.** Návod na teoretické uchopení takové situace dává již diskuse geometrie roviny, viz odstavec 1.25 a dále. Tam jsme totiž popisovali přímky a body jako množiny řešení systémů lineárních rovnic. Přímka pro nás pak byla „jednorozměrným“ prostorem, přestože její body byly popisovány dvěma souřadnicemi. Parametricky jsme ji zadávali tak, že k jednomu bodu (tj. dvojici souřadnic) jsme přičítali násobky pevně zvoleného směrového vektoru. Stejně budeme postupovat i teď v libovolné dimenzi.

STANDARDNÍ AFINNÍ PROSTOR

*Standardní afinní prostor* $\mathcal{A}_n$ je množina všech bodů v $\mathbb{R}^n = \mathcal{A}_n$ spolu s operací, kterou k bodu $A = (a_1, \dots, a_n) \in \mathcal{A}_n$ a vektoru $v = (v_1, \dots, v_n) \in \mathbb{R}^n = V$ přiřadíme bod

$$A + v = (a_1 + v_1, \dots, a_n + v_n) \in \mathbb{R}^n = \mathcal{A}_n.$$

Tyto operace splňují následující tři vlastnosti:

(1) $A + 0 = A$ pro všechny body $A \in \mathcal{A}_n$ a nulový vektor $0 \in V$,
(2) $A + (v + w) = (A + v) + w$ pro všechny vektory $v, w \in V$ a body $A \in \mathcal{A}_n$,

tzv. vektorového součinu (viz 4.24):

$$(1, -2, 1) \times (2, 1, -1) = (1, 3, 5).$$

Všimneme-li si navíc, že např. uspořádaná trojice

$$(x, y, z) = (2, -1, -2)$$

vyhovuje dané soustavě, dostaneme výsledek

$$[2, -1, -2] + t\,(1, 3, 5)\,, \quad t \in \mathbb{R}.$$

Čtenář jistě postřehl, že alternativní postup pouze geometricky interpretoval řešení nehomogenní lineární soustavy rovnic. □

**4.2.** V $\mathbb{R}^4$ je parametricky dána rovina

$$\varrho : [0, 3, 2, 5] + t\,(1, 0, 1, 0) + s\;(2, -1, -2, 2)\,, \quad t, s \in \mathbb{R}.$$

Vyjádřete tuto rovinu implicitně.

**Řešení.** Úkolem je najít soustavu lineárních rovnic čtyř proměnných $x, y, z, u$ (čtyři proměnné jsou dány dimenzí prostoru), jíž budou vyhovovat právě souřadnice bodů uvedené roviny. Poznamenejme, že hledaná soustava bude obsahovat $2 = 4 - 2$ lineárně nezávislé rovnice. Příklad vyřešíme tzv. eliminací parametrů. Body $[x, y, z, u] \in \varrho$ splňují

$$\begin{array}{rcrcrcr} x &=& & & t &+& 2s, \\ y &=& 3 & & &-& s, \\ z &=& 2 &+& t &-& 2s, \\ u &=& 5 & & &+& 2s, \end{array}$$

přičemž $t, s \in \mathbb{R}$. Odtud můžeme ihned přejít k maticovému zápisu

$$\left(\begin{array}{cc|cccc|c} 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 0 & 3 \\ 1 & -2 & 0 & 0 & -1 & 0 & 2 \\ 0 & 2 & 0 & 0 & 0 & -1 & 5 \end{array}\right),$$

kde první dva sloupce jsou směrové vektory roviny, za svislou čarou následuje záporně vzatá jednotková matice a za druhou svislou čarou jsou souřadnice bodu $[0, 3, 2, 5]$. Tento přepis vzniká tak, že na výše uvedenou soustavu rovnic nahlížíme jako na soustavu rovnic pro neznámé $t, s, x, y, z, u$ a všechny členy přitom převádíme na jednu stranu rovnic. Získanou matici převedeme pomocí elementárních řádkových transformací do tvaru, kdy před první svislou čarou bude maximální možný počet nulových řádků. Přičtením $(-1)$-násobku prvního

(3) pro každé dva body $A, B \in \mathcal{A}_n$ existuje právě jeden vektor $v \in V$ takový, že $A + v = B$. Značíme jej $v = B - A$, někdy také $\vec{AB}$.

Vektorový prostor $\mathbb{R}^n$ nazýváme *zaměření* standardního afinního prostoru $\mathcal{A}_n$.



Všimněme si několika formálních nebezpečí. Používáme stejný symbol „+“ pro dvě různé operace: přičtení vektoru ze zaměření k bodu v afinním prostoru, ale také sčítání vektorů v zaměření $V = \mathbb{R}^n$. Také nezavádíme zvláštní písmena pro samotnou množinu bodů afinního prostoru, tj. $\mathcal{A}_n$ pro nás představuje jak samotnou množinu bodů, tak i celou strukturu definující afinní prostor.

Proč vlastně chceme rozlišovat množinu bodů prostoru $\mathcal{A}_n$ od jeho zaměření $V$, když se jedná jakoby o stejné $\mathbb{R}^n$? Jde o velice podstatný formální krok k pochopení geometrie v $\mathbb{R}^n$: Geometrické objekty jako přímky, body, roviny apod. nejsou totiž přímo závislé na vektorové struktuře na množině $\mathbb{R}^n$ a už vůbec ne na tom, že pracujeme s $n$–ticemi skalárů. Potřebujeme jen umět říci, co to znamená pohybovat se „rovně v daném směru“. K tomu právě potřebujeme na jedné straně vnímat třeba rovinu jako neohraničenou desku bez zvolených souřadnic, ale s možností posunout se o zadaný vektor. Když přejdeme navíc k takovému abstraktnímu pohledu, budeme umět diskutovat „rovinnou geometrii“ pro dvourozměrné podprostory, tj. roviny ve vícerozměrných prostorech, „prostorovou“ pro třírozměrné atd., aniž bychom museli přímo manipulovat $k$–ticemi souřadnic.

Tento pohled je zachycen v následující definici:

**4.2. Definice.** Afinním prostorem $\mathcal{A}$ se zaměřením $V$ rozumíme množinu *bodů* $\mathcal{P}$, spolu se zobrazením

$$\mathcal{P} \times V \to \mathcal{P}, \quad (A, v) \mapsto A + v,$$

kde $V$ je vektorový prostor a naše zobrazení splňuje vlastnosti (1)–(3) z definice standardního afinního prostoru.

Pro libovolný pevně zvolený vektor $v \in V$ je tak definováno *posunutí* $\tau_v : \mathcal{A} \to \mathcal{A}$ jako zúžené zobrazení

$$\tau_v : \mathcal{P} \simeq \mathcal{P} \times \{v\} \to \mathcal{P}, \quad A \mapsto A + v.$$

*Dimenzí* afinního prostoru $\mathcal{A}$ rozumíme dimenzi jeho zaměření.

Nadále nebudeme rozlišovat ve značení důsledně množinu bodů $\mathcal{A}$ a množinu vektorů $\mathcal{P}$, budeme místo toho hovořit o bodech a vektorech afinního prostoru $\mathcal{A}$.

Z axiomů okamžitě plyne pro libovolné body $A, B, C$ v afinním prostoru $\mathcal{A}$

$$A - A = 0 \in V, \tag{4.1}$$

$$B - A = -(A - B), \tag{4.2}$$

$$(C - B) + (B - A) = C - A. \tag{4.3}$$

Skutečně, (4.1) vyplývá z toho, že $A + 0 = 0$ a takový vektor musí být jednoznačný (první a třetí definiční vlastnost). Postupným přičtením $B - A$ a $A - B$ k $A$ (v uvedeném pořadí), zjevně dostaneme podle druhé definiční vlastnosti opět $A$, tedy jsme přičetli nulový vektor a to dokazuje (4.2). Obdobně z definiční vlastnosti 4.1 (2) a jednoznačnosti vyplývá (4.3).

a současně $(-4)$-násobku druhého řádku ke třetímu řádku a dvojnásobku druhého ke čtvrtému řádku dostáváme

$$\left(\begin{array}{cccc|c} 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 0 & 3 \\ 1 & -2 & 0 & 0 & -1 & 0 & 2 \\ 0 & 2 & 0 & 0 & 0 & -1 & 5 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 4 & -1 & 0 & -10 \\ 0 & 0 & 0 & -2 & 0 & -1 & 11 \end{array}\right).$$

Odkud plyne výsledek

$$\begin{array}{rcrcrcrcl} x & + & 4y & - & z & & - & 10 = & 0, \\ & & -2y & & & - & u & + 11 = & 0. \end{array}$$

Koeficienty za první svislou čarou v řádcích, které jsou před touto svislou čarou nulové, určují totiž koeficienty obecných rovnic roviny.

Upozorněme, že kdybychom např. přepsali soustavu rovnic do matice

$$\left(\begin{array}{cccc|cc|c} 1 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 1 & 0 & 1 & -2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 2 & 5 \end{array}\right),$$

která odpovídá situaci, kdy proměnné $x$, $y$, $z$, $u$ zůstávají na levé straně rovnic, totožná úprava

$$\left(\begin{array}{cccc|cc|c} 1 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 1 & 0 & 1 & -2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 2 & 5 \end{array}\right) \sim \left(\begin{array}{cccc|cc|c} 1 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 3 \\ -1 & -4 & 1 & 0 & 0 & 0 & -10 \\ 0 & 2 & 0 & 1 & 0 & 0 & 11 \end{array}\right)$$

dává výsledek ve tvaru

$$\begin{array}{rcrcrcrcl} -x & - & 4y & + & z & & = & -10, \\ & & 2y & & & + & u & = & 11. \end{array}$$

Při přepisování soustavy do matice je tudíž nutné zohledňovat, zda svislá čára odděluje levou stranu rovnic od pravé (či nikoliv). Jak jsme částečně viděli v tomto příkladu, metoda eliminace parametrů může být zdlouhavá a při jejím použití se lze snadno dopustit chyb.

**Jiné řešení.** Řešení můžeme do značné míry urychlit naší „šikovností“. Pokud si všimneme, že dva lineárně nezávislé normálové vektory, tj. vektory kolmé na vektory $(1, 0, 1, 0)$, $(2, -1, -2, 2)$. jsou např. $(0, 2, 0, 1)$, $(-1, 0, 1, 2)$, dosazením $x = 0$, $y = 3$, $z = 2$, $u = 5$ do rovnic

$$\begin{array}{rcrcrcl} & & 2y & & + & u & = a, \\ -x & & & + & z & + 2u & = b \end{array}$$

bychom obdrželi $a = 11$, $b = 12$, následně hledané implicitní vyjádření

$$\begin{array}{rcrcrcl} & & 2y & & + & u & = 11, \\ -x & & & + & z & + 2u & = 12. \end{array}$$

□

Všimněme si, že volba jednoho pevného bodu $A_0 \in \mathcal{A}$ nám určuje bijekci mezi $V$ a $\mathcal{A}$. Při volbě pevné báze $\underline{u}$ ve $V$ tak dostáváme pro každý bod $A \in \mathcal{A}$ jednoznačné vyjádření

$$A = A_0 + x_1 u_1 + \cdots + x_n u_n.$$

Hovoříme o *afinní soustavě souřadnic* $(A_0; u_1, \ldots, u_n)$ zadané *počátkem afinní souřadné soustavy* $A_0$ a bází zaměření $\underline{u}$ nebo také o *afinním repéru* $(A_0, \underline{u})$.

Slovy můžeme shrnout situaci takto: Afinní souřadnice bodu $A$ v soustavě $(A_0, \underline{u})$ jsou souřadnicemi vektoru $A - A_0$ v bázi $\underline{u}$ zaměření $V$.

Volba afinního souřadného systému ztotožňuje jakýkoliv $n$-rozměrný afinní prostor $\mathcal{A}$ se standardním afinním prostorem $\mathcal{A}_n$.

**4.3. Afinní podprostory.** Jestliže si vybereme v $\mathcal{A}$ jen body, které budou mít některé předem vybrané souřadnice nulové (třeba poslední jednu). Dostaneme opět množinu, která se bude chovat jako afinní prostor. Takto budeme skutečně parametricky popisovat tzv. afinní podprostory ve smyslu následující definice.



### Podprostory afinního prostoru

**Definice.** Neprázdná podmnožina $\mathcal{Q} \subseteq \mathcal{A}$ afinního prostoru $\mathcal{A}$ se zaměřením $V$ se nazývá *afinní podprostor* v $\mathcal{A}$, je-li podmnožina $W = \{B - A;\, A, B \in \mathcal{Q}\} \subseteq V$ vektorovým podprostorem a pro libovolné $A \in \mathcal{Q}$, $v \in W$ je $A + v \in \mathcal{Q}$.

Je podstatné mít obě podmínky zahrnuty v definici, protože je snadné najít příklady podmnožin, které budou splňovat první, ale nikoliv druhou podmínku. Přemýšlejte např. o přímce v rovině s vyjmutým jedním bodem.

Pro libovolnou množinu bodů $M \subseteq \mathcal{A}$ v afinním prostoru se zaměřením $V$ definujeme vektorový podprostor

$$Z(M) = \langle \{B - A;\, B, A \in M\} \rangle \subseteq V$$

všech vektorů generovaných rozdíly bodů z $M$.

Zejména je $V = Z(\mathcal{A})$ a každý afinní podprostor $\mathcal{Q} \subseteq \mathcal{A}$ splňuje sám axiomy afinního prostoru se zaměřením $Z(\mathcal{Q})$.

Přímo z definic je také zřejmé, že průnik libovolné množiny afinních podprostorů je buď opět afinní podprostor nebo prázdná množina.

Afinní podprostor $\langle M \rangle$ v $\mathcal{A}$ *generovaný* neprázdnou podmnožinou $M \subseteq \mathcal{A}$ je průnikem všech afinních podprostorů, které obsahují všechny body podmnožiny $M$.

### Afinní obal a parametrický popis podprostoru

Afinní podprostory si můžeme pěkně popsat pomocí jejich zaměření, jakmile si zvolíme jeden jejich bod $A_0 \in M$ v generující množině bodů $M$. Skutečně, dostáváme $\langle M \rangle = \{A_0 + v; v \in Z(M) \subseteq Z(\mathcal{A})\}$, tj. pro generování afinního podprostoru vezmeme vektorový podprostor $Z(M)$ v zaměření generovaný všemi rozdíly bodů z $M$ a ten pak přičteme k libovolnému z nich. Hovoříme také o *afinním obalu* množiny bodů $M$ v $\mathcal{A}$.

Naopak, kdykoliv zvolíme podprostor $U$ v zaměření $Z(\mathcal{A})$ a jeden pevný bod $A \in \mathcal{A}$, pak podmnožina $A + U$ vzniklá všemi možnými součty jediného bodu $A$ se všemi vektory v $U$ je afinní

**4.3.** Nalezněte parametrické vyjádření roviny procházející body

$$A = [2, 1, 1], \quad B = [3, 4, 5], \quad C = [4, -2, 3].$$

Poté parametricky vyjádřete otevřenou polorovinu obsahující bod $C$ a vymezenou přímkou zadanou body $A$, $B$.

**Řešení.** K parametrickému vyjádření roviny potřebujeme jeden bod ležící v této rovině a dva směrové (lineárně nezávislé) vektory. Stačí zvolit bod $A$ a vektory $B - A = (1, 3, 4)$ a $C - A = (2, -3, 2)$, které jsou očividně lineárně nezávislé. Bod $[x, y, z]$ náleží do dané roviny právě tehdy, když existují čísla $t, s \in \mathbb{R}$, pro která je

$$x = 2 + 1 \cdot t + 2 \cdot s, \quad y = 1 + 3 \cdot t - 3 \cdot s, \quad z = 1 + 4 \cdot t + 2 \cdot s;$$

tj. hledané parametrické vyjádření roviny je

$$[2, 1, 1] + t\,(1, 3, 4) + s\,(2, -3, 2), \quad t, s \in \mathbb{R}.$$

Volba $s = 0$ zjevně dává přímku, která prochází body $A$, $B$. Pro $t = 0, s \geq 0$ dostáváme polopřímku začínající v bodě $A$ a procházející bodem $C$. Libovolně pevně zvolené $t \in \mathbb{R}$ a měnné $s \geq 0$ pak zadávají polopřímku s počátkem na hraniční přímce a s body v polorovině, ve které se nachází bod $C$. To znamená, že hledanou otevřenou polorovinu můžeme vyjádřit parametricky takto

$$[2, 1, 1] + t\,(1, 3, 4) + s\,(2, -3, 2), \quad t \in \mathbb{R},\ s > 0. \qquad \square$$

**4.4.** Určete vzájemnou polohu přímek

$$p : [1, 0, 3] + t\,(2, -1, -3), \quad t \in \mathbb{R},$$
$$q : [1, 1, 3] + s\,(1, -1, -2), \quad s \in \mathbb{R}.$$

**Řešení.** Hledejme společné body zadaných přímek (průnik podprostorů). Dostáváme soustavu

$$\begin{array}{rcrcrcl} 1 & + & 2t & = & 1 & + & s, \\ 0 & - & t & = & 1 & - & s, \\ 3 & - & 3t & = & 3 & - & 2s. \end{array}$$

Vyřešením prvních dvou rovnic vzhledem k neznámým $s$ a $t$ získáme hodnoty $t = 1, s = 2$. Ty ovšem nevyhovují třetí rovnici. Soustava tak nemá řešení. Protože směrový vektor $(2, -1, -3)$ přímky $p$ není násobkem směrového vektoru $(1, -1, -2)$ přímky $q$, přímky nejsou rovnoběžné. Jedná se proto o mimoběžky. $\square$

**4.5.** Pro jaká čísla $a \in \mathbb{R}$ jsou přímky

$$p : [4, -4, 8] + t\,(2, 1, -4), \quad t \in \mathbb{R},$$
$$q : [a, 6, -5] + s\,(1, -3, 3), \quad s \in \mathbb{R},$$

různoběžné?

podprostor. Takový postup vede k pojmu parametrizace podprostorů:

Nechť $\mathcal{Q} = A + Z(\mathcal{Q})$ je afinní podprostor v $\mathcal{A}_n$ a $(u_1, \ldots, u_k)$ je báze $Z(\mathcal{Q}) \subseteq \mathbb{R}^n$. Pak vyjádření podprostoru

$$\mathcal{Q} = \{A + t_1 u_1 + \cdots + t_k u_k;\, t_1, \ldots, t_k \in \mathbb{R}\}$$

nazýváme *parametrický popis* podprostoru $\mathcal{Q}$.

Již jsme viděli jinou možnost zadávání afinních podprostorů: Jestliže máme zvoleny afinní souřadnice, pak lze zaměření podprostoru popsat pomocí homogenního systému lineárních rovnic v těchto souřadnicích. Dosazením souřadnic jednoho bodu našeho podprostoru $\mathcal{Q}$ do získaného systému rovnic dostaneme pravou stranu nehomogenního systému se stejnou maticí a celý podprostor $\mathcal{Q}$ je pak právě množinou řešení tohoto systému. Zadání podprostoru $\mathcal{Q}$ systémem rovnic v daných souřadnicích nazýváme *implicitní popis* podprostoru $\mathcal{Q}$.

Následující obecná věta říká, že takto umíme ve skutečnosti zadat všechny afinní podprostory a tím také ukazuje geometrickou podstatu vlastností množiny všech řešení systémů lineárních rovnic.

**4.4. Věta.** *Nechť $(A_0; \underline{u})$ je afinní souřadný systém v $n$-rozměrném afinním prostoru $\mathcal{A}$. Afinní podprostory dimenze $k$ v $\mathcal{A}$, vyjádřené v daných souřadnicích, jsou právě množiny řešení řešitelných systémů $n - k$ lineárně nezávislých lineárních rovnic v $n$ proměnných.*

Důkaz. Uvažujme libovolný řešitelný systém $n - k$ lineárně nezávislých rovnic $\alpha_i(x) = b_i$, $b_i \in \mathbb{R}$, $i = 1, \ldots, n - k$. Je-li $A = (a_1, \ldots, a_n)^T \in \mathbb{R}^n$ libovolné pevně zvolené řešení tohoto (nehomogenního) systému rovnic a je-li $U \subseteq \mathbb{R}^n$ vektorový podprostor všech řešení zhomogenizovaného systému $\alpha_i(x) = 0$, pak dimenze $U$ je $k$ a podmnožina všech řešení daného systému je tvaru $\{B;\, B = A + (y_1, \ldots, y_n)^T,\, y = (y_1 \ldots, y_n)^T \in U\} \subseteq \mathbb{R}^n$, viz 3.1. Příslušný afinní podprostor je tím popsán parametricky ve výchozích souřadnicích $(A_0; \underline{u})$.

Naopak, uvažme libovolný afinní podprostor $\mathcal{Q} \subseteq \mathcal{A}_n$ a zvolme nějaký jeho bod $B$ za počátek afinního souřadného systému $(B, \underline{v})$ pro afinní prostor $\mathcal{A}$. Protože $\mathcal{Q} = B + Z(\mathcal{Q})$, potřebujeme popsat zaměření podprostoru $\mathcal{Q}$ jako podprostor řešení homogenního systému rovnic. Zvolme tedy bázi $\underline{v}$ na $Z(\mathcal{A})$ tak, aby prvních $k$ vektorů tvořilo bázi $Z(\mathcal{Q})$. Pak v těchto souřadnicích jsou vektory $v \in Z(\mathcal{Q})$ dány rovnostmi

$$\alpha_j(v) = 0, \quad j = k + 1, \ldots, n,$$

kde $\alpha_i$ jsou lineární formy z tzv. duální báze k $\underline{v}$, tj. funkce přiřazení jednotlivých souřadnic v naší bázi $\underline{v}$.

Náš vektorový podprostor $Z(\mathcal{Q})$ dimenze $k$ v $n$-rozměrném prostoru $\mathbb{R}^n$ je tedy skutečně dán jako řešení homogenního systému $n - k$ nezávislých rovnic. Popis zvoleného afinního podprostoru v námi nově vybraném souřadném systému $(B; \underline{v})$ je proto dán systémem homogenních lineárních rovnic.

Zbývá nám se vypořádat důsledky přechodu z původního zadaného souřadného systému $(A; \underline{u})$ do našeho přizpůsobeného $(B; \underline{v})$. Z obecné úvahy o transformacích souřadnic v následujícím odstavci vyplyne, že výsledný popis podprostoru bude opět pomocí systému rovnic, tentokrát ale už obecně nehomogenních. $\square$

**Řešení.** Přímky jsou různoběžné tehdy a jenom tehdy, když má soustava

$$\begin{array}{rcrcrcl} 4 & + & 2t & = & a & + & s, \\ -4 & + & t & = & 6 & - & 3s, \\ 8 & - & 4t & = & -5 & + & 3s \end{array}$$

právě 1 řešení. V maticovém zápisu řešíme (první sloupec odpovídá proměnné $t$, druhý pak $s$)

$$\left(\begin{array}{cc|c} 2 & -1 & a-4 \\ 1 & 3 & 10 \\ -4 & -3 & -13 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 10 \\ 2 & -1 & a-4 \\ -4 & -3 & -13 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cc|c} 1 & 3 & 10 \\ 0 & -7 & a-24 \\ 0 & 1 & 3 \end{array}\right).$$

Vidíme, že soustava má právě 1 řešení tehdy a jenom tehdy, když je druhý řádek násobkem třetího. To je splněno pouze pro $a = 3$. Dodejme, že průsečíkem je v tomto případě bod $[6, -3, 4]$. □

**4.6.** V $\mathbb{R}^3$ stanovte vzájemnou polohu přímky $p$ zadané implicitně rovnicemi

$$\begin{array}{rcrcrcl} x & + & y & - & z & = & 4, \\ x & - & 2y & + & z & = & -3 \end{array}$$

a roviny $\varrho : y = 2x - 1$.

**Řešení.** Normálový vektor $\varrho$ je $(2, -1, 0)$ (uvažte zápis $\varrho : \; 2x \; - \; y \; + \; 0z \; = \; 1$). Lze postřehnout, že platí

$$(1, 1, -1) + (1, -2, 1) = (2, -1, 0),$$

tj. že normálový vektor roviny $\varrho$ je lineární kombinací normálových vektorů $p$. Zaměření přímky (zadané nenulovým směrovým vektorem kolmým na uvedené dva normálové vektory) je proto podprostorem zaměření roviny $\varrho$ (směrový vektor přímky je nutně kolmý na vektor $(2, -1, 0)$). Lehce jsme zjistili, že přímka $p$ je rovnoběžná s rovinou $\varrho$. Zajímá nás, zda se protínají (zda $p$ leží v $\varrho$). Soustava rovnic

$$\begin{array}{rcrcrcl} x & + & y & - & z & = & 4, \\ x & - & 2y & + & z & = & -3, \\ 2x & - & y & & & = & 1 \end{array}$$

má nekonečně mnoho řešení, neboť sečtením prvních dvou rovnic dostaneme právě třetí z rovnic. Přímka $p$ tak musí ležet v rovině $\varrho$. □

Následuje standardní příklad na průnik vektorových prostorů.



Čtenář by měl být schopen následující příklad vyřešit. Doporučujeme nepokračovat ve čtení této učebnice, dokud tomu tak nebude.

**4.5. Transformace souřadnic.** Dvě libovolně zvolené afinní soustavy souřadnic $(A_0, \underline{u})$, $(B_0, \underline{v})$ se obecně liší posunutím počátku o vektor $(B_0 - A_0)$ a jinou bází zaměření. Transformační rovnice mezi příslušnými souřadnicemi tedy vyčteme ze vztahu pro obecný bod $X \in \mathcal{A}$



$$\begin{aligned} X &= B_0 + x'_1 v_1 + \cdots + x'_n v_n = \\ &= B_0 + (A_0 - B_0) + x_1 u_1 + \cdots + x_n u_n. \end{aligned}$$

Označme $y = (y_1, \ldots, y_n)^T$ sloupec souřadnic vektoru $(A_0 - B_0)$ v bázi $\underline{v}$ a $M = (a_{ij})$ buď matice vyjadřující bázi $\underline{u}$ prostřednictvím báze $\underline{v}$. Potom

$$\begin{aligned} x'_1 &= y_1 + a_{11}x_1 + \cdots + a_{1n}x_n, \\ &\vdots \\ x'_n &= y_n + a_{n1}x_1 + \cdots + a_{nn}x_n, \end{aligned}$$

tj. maticově

$$x' = y + M \cdot x.$$

Jako příklad si můžeme vyjádřit dopad takové změny báze na



souřadné vyjádření podmnožin pomocí systémů lineárních rovnic. Nechť má v souřadnicích $(A_0; \underline{u})$ náš systém rovnic tvar

$$S \cdot x = b$$

s maticí systému $S$. Potom

$$S \cdot x = S \cdot M^{-1} \cdot (y + M \cdot x) - S \cdot M^{-1} \cdot y = b.$$

Proto v nových výše uvažovaných souřadnicích $(B_0; \underline{v})$ bude mít náš systém rovnic tvar

$$(S \cdot M^{-1}) \cdot x' = b' = b + (S \cdot M^{-1}) \cdot y.$$

Pokud tedy máme nějakou podmnožinu popsánu systémem lineárních rovnic v jednom afinním repéru, pak tomu tak bude i ve všech ostatních afinních souřadných systémech. To plně dokončuje důkaz předchozí věty.

**4.6. Příklady afinních podprostorů.** (1) Jednorozměrný (standardní) afinní prostor je množina všech bodů reálné



přímky $\mathcal{A}_1$. Její zaměření je jednorozměrný vektorový prostor $\mathbb{R}$ (a nosná množina také $\mathbb{R}$). Afinní souřadnice dostaneme volbou počátku a měřítka (tj. báze ve vektorovém prostoru $\mathbb{R}$). Všechny vlastní afinní podprostory jsou 0-rozměrné, jsou to právě všechny body reálné přímky $\mathbb{R}$.

(2) Dvourozměrný (standardní) afinní prostor je množina všech bodů prostoru $\mathcal{A}_2$ se zaměřením $\mathbb{R}^2$. (Nosnou množinou je $\mathbb{R}^2$.) Afinní souřadnice dostaneme volbou počátku a dvou nezávislých vektorů (směrů a měřítek). Vlastní afinní podprostory jsou pak všechny body a přímky v rovině (0-rozměrné a 1-rozměrné). Přímky přitom jednoznačně zadáme jejich jedním bodem a jedním generátorem zaměření (tzv. parametrický popis přímky).

(3) Trojrozměrný (standardní) afinní prostor je množina všech bodů prostoru $\mathcal{A}_3$ se zaměřením $\mathbb{R}^3$. Afinní souřadnice dostaneme volbou počátku a tří nezávislých vektorů (směrů a měřítek). Vlastní afinní podprostory jsou pak všechny body, přímky a roviny (0-rozměrné, 1-rozměrné a 2-rozměrné).

(4) Podprostor všech řešení jedné lineární rovnice $a \cdot x = b$ pro

**4.7.** Nalezněte průnik podprostorů $Q_1$ a $Q_2$, je-li

$$Q_1 : [4,-5,1,-2] + t_1\,(3,5,4,2) + t_2\,(2,4,5,1) + t_3\,(0,3,1,2)\,,$$
$$Q_2 : [4,4,4,4] + s_1\,(0,-6,-2,-4) + s_2\,(-1,-5,-3,-3)\,,$$

kde $t_1, t_2, t_3, s_1, s_2 \in \mathbb{R}$.

**Řešení.** Bod $X = [x_1, x_2, x_3, x_4] \in \mathbb{R}^4$ náleží do $Q_1 \cap Q_2$ právě tehdy, když je

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 4 \\ -5 \\ 1 \\ -2 \end{bmatrix} + t_1 \begin{pmatrix} 3 \\ 5 \\ 4 \\ 2 \end{pmatrix} + t_2 \begin{pmatrix} 2 \\ 4 \\ 5 \\ 1 \end{pmatrix} + t_3 \begin{pmatrix} 0 \\ 3 \\ 1 \\ 2 \end{pmatrix}$$

pro nějaká čísla $t_1, t_2, t_3 \in \mathbb{R}$ a současně, když je

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 4 \\ 4 \\ 4 \\ 4 \end{bmatrix} + s_1 \begin{pmatrix} 0 \\ -6 \\ -2 \\ -4 \end{pmatrix} + s_2 \begin{pmatrix} -1 \\ -5 \\ -3 \\ -3 \end{pmatrix}$$

pro nějaká $s_1, s_2 \in \mathbb{R}$. Porovnáním získáváme

$$t_1 \begin{pmatrix} 3 \\ 5 \\ 4 \\ 2 \end{pmatrix} + t_2 \begin{pmatrix} 2 \\ 4 \\ 5 \\ 1 \end{pmatrix} + t_3 \begin{pmatrix} 0 \\ 3 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 4-4 \\ 4+5 \\ 4-1 \\ 4+2 \end{pmatrix} + s_1 \begin{pmatrix} 0 \\ -6 \\ -2 \\ -4 \end{pmatrix} + s_2 \begin{pmatrix} -1 \\ -5 \\ -3 \\ -3 \end{pmatrix}.$$

Při maticovém zápisu (pro pořadí proměnných $t_1, t_2, t_3, s_1, s_2$ a po převodu vektorů u $s_1$ a $s_2$ na levou stranu) řešme pomocí řádkových operací

$$\left(\begin{array}{ccccc|c} 3 & 2 & 0 & 0 & 1 & 0 \\ 5 & 4 & 3 & 6 & 5 & 9 \\ 4 & 5 & 1 & 2 & 3 & 3 \\ 2 & 1 & 2 & 4 & 3 & 6 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 3 & 2 & 0 & 0 & 1 & 0 \\ 0 & 2 & 9 & 18 & 10 & 27 \\ 0 & 7 & 3 & 6 & 5 & 9 \\ 0 & -1 & 6 & 12 & 7 & 18 \end{array}\right) \sim \dots$$

$$\dots \sim \left(\begin{array}{ccccc|c} 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right).$$

Odtud vidíme, že $t_1 = t_2 = s_2 = 0$ a pro $s_1 = t \in \mathbb{R}$ je $t_3 = 3 - 2t$. Podotkněme, že k určení $Q_1 \cap Q_2$ stačilo znát buď $t_1, t_2, t_3$ nebo $s_1, s_2$. Vraťme se nyní k vyjádření

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 4 \\ 4 \\ 4 \\ 4 \end{bmatrix} + s_1 \begin{pmatrix} 0 \\ -6 \\ -2 \\ -4 \end{pmatrix} + s_2 \begin{pmatrix} -1 \\ -5 \\ -3 \\ -3 \end{pmatrix} = \begin{bmatrix} 4 \\ 4 \\ 4 \\ 4 \end{bmatrix} + t \begin{pmatrix} 0 \\ -6 \\ -2 \\ -4 \end{pmatrix}.$$

Průnikem zadaných podprostorů je tedy přímka ($s = -2t$)

$$[4,4,4,4] + s\ (0,3,1,2)\,, \quad s \in \mathbb{R}.$$

neznámý bod $[x_1, \dots, x_n] \in \mathcal{A}_n$, známý nenulový vektor koeficientů $(a_1, \dots, a_n)$ a skalár $b \in \mathbb{R}$ je afinní podprostor dimenze $n-1$ (říkáme také, že je jeho kodimenze 1), tj. tzv. *nadrovina v* $A_n$.

**4.7. Afinní kombinace bodů.** Zavedeme nyní obdobu lineárních kombinací vektorů. Nechť $A_0, \dots, A_k$ jsou body v afinním prostoru $\mathcal{A}$. Jejich afinní obal $\langle\{A_0 \dots, A_k\}\rangle$ můžeme zapsat jako



$$\{A_0 + t_1(A_1 - A_0) + \dots + t_k(A_k - A_0);\, t_1, \dots, t_k \in \mathbb{R}\}$$

a v libovolných afinních souřadnicích (tj. každý bod $A_i$ je vyjádřen sloupcem skalárů) můžeme tutéž množinu zapsat jako

$$\langle A_0, \dots, A_k\rangle = \left\{ t_0A_0 + t_1A_1 + \dots + t_kA_k;\, t_i \in \mathbb{R}, \sum_{i=0}^{k} t_i = 1 \right\}.$$

AFINNÍ KOMBINACE BODŮ

Obecně výrazy $t_0A_0 + t_1A_1 + \dots + t_kA_k$ s koeficienty splňujícími $\sum_{i=0}^{k} t_i = 1$ rozumíme body $A_0 + \sum_{i=1}^{k} t_i(A_i - A_0)$ a nazýváme je *afinní kombinace bodů*.

Body $A_0 \dots, A_k$ jsou v *obecné poloze*, jestliže generují $k$-rozměrný afinní podprostor. Z našich definic je vidět, že to nastane, právě když pro kterýkoliv bod $A_i$ z nich platí, že vektory vzniklé pomocí rozdílů tohoto bodu $A_i$ a ostatních bodů $A_j$ jsou lineárně nezávislé vektory. Všimněme si také, že zadání posloupnosti $(\dim \mathcal{A}) + 1$ bodů v obecné poloze je ekvivalentní zadání afinního repéru s počátkem v prvním z nich.

**4.8. Simplexy.** Afinní kombinace je obdobná konstrukce pro body afinního prostoru jako byla lineární kombinace pro vektorové prostory. Skutečně, afinní podprostor generovaný body $A_0, \dots, A_k$ je roven množině všech afinních kombinací svých generátorů. Můžeme však nyní dobře zobecnit i pojem „mezi dvěma body na přímce“. V dvojrozměrném případě tomu dopovídá vnitřek trojúhelníku. Obecně budeme postupovat takto:

$k$–ROZMĚRNÉ SIMPLEXY

Nechť $A_0, \dots, A_k$ je $k+1$ bodů afinního prostoru $\mathcal{A}$ v obecné poloze. Množina $\Delta = \Delta(A_0, \dots, A_k)$ definovaná jako množina všech afinních kombinací bodů $A_i$ s pouze nezápornými koeficienty, tj.

$$\Delta = \left\{ t_0A_0 + t_1A_1 + \dots + t_kA_k;\, t_i \in [0,1] \subseteq \mathbb{R}, \sum_{i=0}^{k} t_i = 1 \right\},$$

se nazývá $k$–rozměrný *simplex* generovaný body $A_i$.

Jednorozměrný simplex je *úsečka*, dvourozměrný *trojúhelník*, nula–rozměrný simplex je bod.

Všimněme si, že každý $k$–rozměrný simplex má právě $k+1$ *stěn*, které jsou postupně zadány rovnicemi $t_i = 0$, $i = 0, \dots, k$. Přímo z definice je vidět, že jde opět o simplexy, a to s dimenzí $k-1$. Hovoříme o *hranici simplexu*. Např. trojúhelník má za svou hranici tři hrany, každá z nich pak dva body.

Zadání podprostoru jako množiny afinních kombinací bodů v obecné poloze je ekvivalentní parametrickému popisu. Obdobně pracujeme s parametrickými popisy simplexů.

Pro kontrolu rovněž dosaďme

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 4 \\ -5 \\ 1 \\ -2 \end{bmatrix} + t_1 \begin{pmatrix} 3 \\ 5 \\ 4 \\ 2 \end{pmatrix} + t_2 \begin{pmatrix} 2 \\ 4 \\ 5 \\ 1 \end{pmatrix} + t_3 \begin{pmatrix} 0 \\ 3 \\ 1 \\ 2 \end{pmatrix} =$$

$$= \begin{bmatrix} 4 \\ -5 \\ 1 \\ -2 \end{bmatrix} + (3 - 2t) \begin{pmatrix} 0 \\ 3 \\ 1 \\ 2 \end{pmatrix} = \begin{bmatrix} 4 \\ 4 \\ 4 \\ 4 \end{bmatrix} + t \begin{pmatrix} 0 \\ -6 \\ -2 \\ -4 \end{pmatrix}.$$

□

**4.8.** Zjistěte, zda leží body $[0, 2, 1]$, $[-1, 2, 0]$, $[-2, 5, 2]$ a $[0, 5, 4]$ z $\mathbb{R}^3$ v jedné rovině.

**Řešení.** Libovolná dvojice zadaných bodů z afinního prostoru $\mathbb{R}^3$ určuje vektor (viz definice afinního prostoru; jeho souřadnice jsou dány po složkách rozdíly souřadnic daných dvou bodů). To, že dané čtyři body leží v rovině je ekvivalentní tomu, že jsou tři vektory dané jedním vybraným bodem a vždy jedním ze tří zbylých lineárně závislé. Vybereme např. bod $[0, 2, 1]$ (na výběru nezáleží), pak uvažujeme vektory $[0, 2, 1]-[-1, 2, 0] = (1, 0, 1)$, $[0, 2, 1]-[-2, 5, 2] = (2, -3, -1)$ a $[0, 2, 1]-[0, 5, 4] = (0, -3, -3)$. Vidíme, že součet dvojnásobku prvního vektoru a třetího vektoru je roven druhému vektoru, vektory jsou tedy lineárně závislé (jinak má taky matice, jejíž řádky jsou tvořeny souřadnicemi daných vektorů, hodnost nižší než tři; v tomto případě se tedy jedná o matici

$$\begin{pmatrix} 1 & 0 & 1 \\ 2 & -3 & -1 \\ 0 & -3 & -3 \end{pmatrix},$$

která má hodnost dva). Dané body tedy leží v rovině. □

*4.9.* Na kolik částí mohou dělit prostor ($\mathbb{R}^3$) tři roviny? Pro každou možnost popište odpovídající případ. ○

**4.10.** Rozhodněte, zda leží bod $[2, 1, 0]$ uvnitř konvexního obalu bodů $[0, 2, 1]$, $[1, 0, 1]$, $[3, -2, -1]$, $[-1, 0, 1]$.

**Řešení.** Sestavíme nehomogenní lineární soustavu, pro koeficienty $t_1$, $t_2$, $t_3$, $t_4$, afinní kombinace daných bodů, která dává první bod (jsou určeny jednoznačně, pokud dané body neleží v rovině).

$$\begin{pmatrix} 0 & 1 & 3 & -1 \\ 2 & 0 & -2 & 0 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

Poslední rovnice udává, že jde o afinní kombinaci. Řešením této soustavy je čtveřice $(t_1, t_2, t_3, t_4) = (1, 0, 1/2, -1/2)$, jediná afinní kombinace, kterou je bod $[2, 1, 0]$ pomocí čtyř zadaných bodů určen tedy

**4.9. Konvexní množiny.** Podmnožina $M$ afinního prostoru se nazývá *konvexní*, jestliže s každými svými dvěma body $A$, $B$ obsahuje i celou úsečku $\Delta(A, B)$. Přímo z definice je vidět, že každá konvexní množina obsahuje s každými $k+1$ body v obecné poloze i celý jimi definovaný simplex (formální ověření je také obsaženo v důkazu následující věty).

Konvexními množinami jsou např.

(1) prázdná podmnožina,
(2) afinní podprostory,
(3) úsečky, *polopřímky* $p = \{P + t \cdot v;\ t \geq 0\}$,
(4) obecněji $k$– rozměrné *poloprostory*

$$\alpha = \{P + t_1 \cdot v_1 + \cdots + t_k \cdot v_k;\ t_1, \ldots, t_k \in \mathbb{R}, t_k \geq 0\},$$

(5) *úhly* v dvojrozměrných podprostorech

$$\beta = \{P + t_1 \cdot v_1 + t_2 \cdot v_2;\ t_1 \geq 0, t_2 \geq 0\}.$$

Přímo z definice také plyne, že průnik libovolného systému konvexních množin je opět konvexní. Průnik všech konvexních množin obsahujících danou množinu $M$ nazýváme *konvexní obal* $\mathcal{K}(M)$ množiny $M$.

**Věta.** *Konvexní obal libovolné neprázdné podmnožiny $M \subseteq \mathcal{A}$ je*

$$\mathcal{K}(M) = \left\{ t_1 A_1 + \cdots + t_s A_s;\ \sum_{i=1}^{s} t_i = 1,\ t_i \geq 0,\ A_i \in M \right\}$$

Důkaz. Označme $S$ množinu všech afinních kombinací na pravé straně dokazované rovnosti. Nejprve ověříme, že je $S$ konvexní. Zvolme tedy dvě sady parametrů $t_i$, $i = 1, .., s_1$, $t'_j$, $j = 1, \ldots, s_2$ s požadovanými vlastnosti.



Bez újmy na obecnosti můžeme předpokládat, že $s_1 = s_2$ a že v obou kombinacích vystupují stejné body z $M$ (jinak prostě přidáme sčítance s nulovými koeficienty). Uvažme libovolný bod úsečky zadané takto získanými body:

$$\varepsilon(t_1 A_1 + \cdots + t_s A_s) + (1 - \varepsilon)(t'_1 A_1 + \cdots + t'_s A_s),\ 0 \leq \varepsilon \leq 1.$$

Zřejmě jsou opět všechny v $S$.

Zbývá ukázat, že konvexní obal bodů $A_1, \ldots, A_s$ nemůže být menší než $S$. Samotné body $A_i$ odpovídají volbě parametrů $t_j = 0$ pro všechny $j \neq i$ a $t_i = 1$. Předpokládejme, že tvrzení platí pro všechny množiny s nejvýše $s - 1$ body. To znamená, že konvexní obal bodů $A_1, \ldots, A_{s-1}$ je (podle předpokladu) tvořen právě těmi kombinacemi z pravé strany dokazované rovnosti, kde $t_s = 0$. Uvažme nyní libovolný bod $A = t_1 A_1 + \cdots + t_s A_s \in S, t_s < 1$, a afinní kombinace

$$\varepsilon(t_1 A_1 + \cdots + t_{s-1} A_{s-1}) + (1 - \varepsilon(1 - t_s)) A_s,\ 0 \leq \varepsilon \leq \tfrac{1}{1-t_s}.$$

Jde o úsečku s krajními body určenými parametry $\varepsilon = 0$ (bod $A_s$) a $\varepsilon = 1/(1 - t_s)$ (bod v konvexním obalu bodů $A_1, \ldots, A_{s-1}$). Bod $A$ je vnitřním bodem této úsečky s parametrem $\varepsilon = 1$. □

Konvexní obaly konečných množin bodů se nazývají *konvexní mnohostěny*. Jsou-li definující body $A_0, \ldots, A_k$ konvexního mnohostěnu v obecné poloze, dostáváme právě $k$-rozměrný *simplex*. V případě simplexu je vyjádření jeho bodů ve tvaru afinní kombinace definujících vrcholů jednoznačné.

Zvláštním příkladem jsou konvexní mnohostěny generované jedním bodem a konečně mnoha vektory: Nechť $u_1, \ldots, u_k$, jsou

není konvexní kombinací, a tedy bod nemůže ležet v jejich konvexním obalu. □

**4.11.** V $\mathbb{R}^3$ je dán čtyřstěn $ABCD$, kde $A = [4, 0, 2]$, $B = [-2, -3, 1]$, $C = [1, -1, -3]$, $D = [2, 4, -2]$. Rozhodněte, zda leží bod $X = [0, -3, 0]$ uvnitř tohoto čtyřstěnu.

**Řešení.** Daný bod uvnitř daného čtyřstěnu neleží. Vyjádříme-li $X$ jakožto afinní kombinaci jeho vrcholů (řešením soustavy čtyř lineárních rovnic o čtyřech neznámých $a$, $b$, $c$ a $d$ dané rovností $X = aA + bB + cC + dD$), obdržíme $X = \frac{1}{4}A + \frac{1}{2}B + \frac{1}{2}C - \frac{1}{4}D$. To znamená, že $X$ neleží v daném čtyřstěnu, tj. v konvexním obalu bodů $A$, $B$, $C$ a $D$ ($a$, $b$, $c$ i $d$ by musela být v intervalu $\langle 0, 1\rangle$). □

**4.12. Afinní transformace souřadnic bodů**



V afinní bázi $\{[1, 2, 3], (1, 1, 1), (1, -1, 2), (2, 1, 1)\}$ v $\mathbb{R}^3$ jsou vyjádřeny souřadnice bodu $X$ jako $[2, 2, 3]$. Určete jeho souřadnice ve standardní bázi, tj. v bázi $\{[0, 0, 0], (1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.

**Řešení.** Souřadnice $[2, 2, 3]$ v bázi $\{[1, 2, 3], (1, 1, 1), (1, -1, 2), (2, 1, 1)\}$ určují předpisem $[1, 2, 3] + 2 \cdot (1, 1, 1) + 2 \cdot (1, -1, 2) + 3 \cdot (2, 1, 1) = [11, 5, 12]$ souřadnice bodu $X$ ve standardní bázi. □

**4.13. Afinní transformace předpisu zobrazení.** Nalezněte předpis afinního zobrazení $f$ v souřadné soustavě dané bází $\underline{u} = \{(1, 1), (-1, 1)\}$ a počátkem $[2, 0]$, které je ve standardní bázi v $\mathbb{R}^2$ dáno jako

$$f(x_1, x_2) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

**Řešení.** Matice přechodu od dané báze $\underline{u}$ ke standardní bázi k je

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Matici zobrazení v bázi $([2, 0], \underline{u})$ získáme tak, že nejprve transformujeme souřadnice v bázi $([2, 0], \underline{u})$ na souřadnice ve standardní bázi, tedy v bázi $([0, 0], (1, 0), (0, 1))$, poté aplikujeme matici zobrazení $f$ ve standardní bázi a na závěr výsledek transformujeme zpět do souřadnic v bázi $([2, 0], \underline{u})$. Transformační rovnice přechodu od souřadnic $y_1$, $y_2$ v bázi $([2, 0], \underline{u})$ k souřadnicím $x_1$, $x_2$ v standardní bázi jsou

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Odtud máme, že

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}^{-1} \left( \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} - \begin{pmatrix} 2 \\ 0 \end{pmatrix}. \right) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

libovolné vektory v zaměření $\mathbb{R}^n$, $A \in \mathcal{A}_n$ je libovolný bod. *Rovnoběžnostěn* $\mathcal{P}_k(A; u_1, \ldots, u_k) \subseteq \mathcal{A}_n$ je množina

$$\mathcal{P}_k(A; u_1, \ldots, u_k) = \{A + c_1u_1 + \cdots + c_ku_k;\ 0 \le c_i \le 1\}.$$

Jsou-li vektory $u_1, \ldots, u_k$ nezávislé, hovoříme o $k$-rozměrném rovnoběžnostěnu $\mathcal{P}_k(A; u_1, \ldots, u_k) \subseteq \mathcal{A}_n$. Z definice je zřejmé, že rovnoběžnostěny jsou konvexní. Ve skutečnosti jde o konvexní obaly jejich vrcholů.

**4.10. Příklady standardních afinních úloh.** (1) *K podprostoru zadanému implicitně nalézt parametrický popis a naopak:*



Nalezením partikulárního řešení nehomogenního systému a fundamentálního řešení zhomogenizovaného systému rovnic získáme (v souřadnicích, ve kterých byly rovnice zadány) právě hledaný parametrický popis. Naopak, zapíšeme-li parametrický popis v souřadnicích, můžeme volné parametry $t_1, \ldots, t_k$ vyeliminovat a získáme právě rovnice zadávající daný podprostor implicitně.

(2) *Nalézt podprostor generovaný několika podprostory $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$ (obecně různých dimenzí, např. v $R_3$ nalézt rovinu danou bodem a přímkou, třemi body apod.) a zadat jej implicitně či parametricky:*

Výsledný podprostor $\mathcal{Q}$ je vždy určen jedním pevně zvoleným bodem $A_i$ v každém z nich a součtem všech zaměření. Např.

$$\mathcal{Q} = A_1 + (Z(\{A_1, \ldots, A_k\}) + Z(\mathcal{Q}_1) + \cdots + Z(\mathcal{Q}_s)).$$

Pokud jsou podprostory zadány implicitně, je možné je nejdříve převést na parametrický tvar. V konkrétních situacích bývají funkční i jiné postupy. Všimněme si, že obecně je skutečně nutné využít jednoho bodu z každého podprostoru. Např. dvě paralelní přímky v rovině vygenerují celou rovinu, ale sdílí totéž jednorozměrné zaměření.

(3) *Nalézt průnik podprostorů $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$:*

Pokud jsou zadány v implicitním tvaru, stačí sjednotit všechny rovnice do jednoho systému (a případně vynechat lineárně závislé). Pokud je vzniklý systém neřešitelný, je průnik prázdný. V opačném případě získáme implicitní popis afinního podprostoru, který je hledaným průnikem.

Pokud máme dány parametrické tvary, můžeme také hledat přímo společné body jako řešení vhodných rovnic, podobně jako při hledání průniků vektorových podprostorů. Získáme tak přímo opět parametrický popis. Pokud je podprostorů více než dva, musíme průnik hledat postupně.

Máme-li jeden prostor zadaný parametricky a ostatní implicitně, stačí dosadit parametrizované souřadnice a řešit výsledný systém rovnic.

(4) *Nalezení příčky mimoběžek $p$, $q$ v $\mathcal{A}_3$ procházející daným bodem nebo mající předem daný směr (tj. zaměření):*



*Příčkou* rozumíme přímku, která má neprázdný průnik s oběma mimoběžkami. Výsledná příčka $r$ tedy bude jednorozměrným afinním podprostorem. Pokud máme zadán jeho bod $A \in r$, pak afinní podprostor generovaný $p$ a $A$ je buď přímka ($A \in p$) nebo rovina ($A \notin p$). V prvém případě máme nekonečně mnoho řešení, jedno pro každý bod z $q$, v druhém stačí najít průnik $B$ roviny $\langle p \cup A\rangle$ s $q$ a $r = \langle\{A, B\}\rangle$. Pokud je průnik prázdný, úloha nemá řešení, v případě že $q \subseteq \langle p \cup A\rangle$, máme opět nekonečně mnoho řešení, a pokud je průnik jednoprvkový, dostáváme právě jedno řešení.

Pro předpis zobrazení pak dostáváme

$$f(y_1,y_2) = \\ = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \left[ \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \left( \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right) + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] + \\ + \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} 2 \\ -1 \end{pmatrix}.$$

□

**4.14.** Mějme dánu standardní souřadnou soustavu v prostoru $\mathbb{R}^3$. Agent K sídlí v bodě $S$ o souřadnicích $[0,1,2]$ a ústředí mu přidělilo pro používání souřadnou soustavu s počátkem $S$ a bází $\{(1,1,0),(-1,0,1),(0,1,2)\}$. Agent Sokol bydlí domě $D$ na kótě $[1,1,1]$ a používá souřadnou soustavu s bází $\{(0,0,1),(-1,1,2),(1,0,1)\}$. Agent K žádá Sokola o schůzku v cihelně, která leží podle jeho souřadné soustavy v bodě $[1,1,0]$. Kam má přijít Sokol (podle jeho souřadnic)?

**Řešení.** Matice přechodu od báze agenta K k Sokolově bázi (při stejných počátcích) je

$$T = \begin{pmatrix} -4 & 2 & -1 \\ 1 & 0 & 1 \\ 2 & -1 & 1 \end{pmatrix}.$$

Vektor $(0,1,2)$ má tedy souřadnice $T \cdot (0,1,2)^T = (0,2,1)^T$, posunutím počátku (přičteme vektor $(-1,0,1)$) dostáváme výsledek $(-1,2,2)$. □

**4.15.** Najděte příčku přímek (úsečku, jejíž jeden koncový bod leží na



jedné z přímek, druhý pak na druhé z nich)

$$p: [1,1,1] + t(2,1,0),$$
$$q: [2,2,0] + t(1,1,1),$$

takovou, že přímka jí určená prochází bodem $[1,0,0]$.

**Řešení.** Nalezneme průsečík hledané příčky s přímkou $q$ (nazveme jej $Q$). Hledaná příčka obsahuje nějaký bod na přímce $p$ a bod $[1,0,0]$, nutně tedy leží v rovině $\rho$ určené tímto bodem a přímkou $p$, tedy v rovině

$$[1,1,1] + t(2,1,0) + s(0,1,1).$$

Bod $Q$ je pak průnikem této roviny s přímkou $q$. Ten nalezneme vyřešením soustavy

$$\begin{array}{rcrcrcl} 1 & & & + & 2t & = & 2 + u, \\ 1 & + & s & + & t & = & 2 + u, \\ 1 & + & s & & & = & u. \end{array}$$

Levé strany rovnic reprezentují postupně všechny tři souřadnice libovolného bodu roviny $\rho$, pravé pak souřadnice libovolného bodu na

Máme-li místo bodu dán směr $u \in \mathbb{R}^n$, tj. zaměření $r$, pak uvažujeme opět podprostor $\mathcal{Q}$ generovaný $p$ a zaměřením $Z(p) + \langle u \rangle \subseteq \mathbb{R}^n$. Opět, pokud $q \subseteq \mathcal{Q}$, máme nekonečně mnoho řešení, jinak uvážíme průnik $\mathcal{Q}$ s $q$ a úlohu dokončíme stejně jako v předchozím případě.

Řešení mnoha dalších praktických geometrických úloh vesměs spočívá v systematickém používání výše uvedených kroků.

**4.11. Poznámky k lineárnímu programování.** Na začátku třetí



kapitoly jsme se zastavili v odstavcích 3.4–3.8 u praktických problémů, které jsou zadány pomocí systémů lineárních nerovnic. Snadno ověříme, že každá taková jednotlivá nerovnice

$$a_1x_1 + \cdots + a_nx_n \leq b$$

zadává v standardním afinním prostoru $\mathbb{R}^n$ poloprostor ohraničený nadrovinou, kterou zadává příslušná rovnice (srovnej s definicí v odstavci 4.9(4)). Skutečně, jestliže zvolíme parametrický popis příslušné nadroviny

$$\{P + t_1v_1 + \cdots + t_{n-1}v_{n-1}\}$$

s vektory zaměření $v_1, \ldots, v_{n-1}$, pak doplněním těchto vektorů do báze celého $\mathbb{R}^n$ vektorem $v$, nutně musí být hodnota

$$a_1x_1 + \cdots + a_nx_n - b$$

na lineární kombinaci $t_1v_1 + \cdots + t_{n-1}v_{n-1} + t_nv$ vždy kladná pro všechny vektory buď s kladným nebo záporným $t_n$.

Zároveň tedy vidíme, že množina všech přípustných vektorů pro problém lineárního programování je vždy průnikem konečně mnoha konvexních množin a tedy je sama buď konvexní nebo prázdná.

Pokud je zároveň průnik neprázdný a omezený, pak jde zřejmě o konvexní mnohostěn. Jak jsme zdůvodnili již v 3.4, každá lineární forma je podél každé (parametrizované) přímky v afinním prostoru buď stále rostoucí nebo stále klesající nebo konstantní. Pokud je tedy daný problém lineárního programování řešitelný a omezený, pak musí mít optimální řešení v jednom z vrcholů příslušného konvexního mnohostěnu. Čtenář by si měl umět toto tvrzení bez problémů představit v případě dvourozměrného nebo třírozměrného problému. Přímočaré zdůvodnění z těchto malých dimenzí však platí pro všechny konečněrozměrné případy.

Tím jsme podali „geometrický důkaz“ existenční části základní věty 3.7. Také jsme tak původní problém převedli k diskrétní (tj. konečné) úvaze o hodnotách dané cenové funkce v konečně mnoha bodech prostoru. K příkladu praktického algoritmu, jak příslušné vrcholy konvexního mnohostěnu co nejsnáze najít a vyhodnotit, se vrátíme ještě v kapitole o diskrétní matematice.

**4.12. Afinní zobrazení.** Zobrazení $f : \mathcal{A} \to \mathcal{B}$ mezi afin-



ními prostory nazýváme *afinní zobrazení*, jestliže mezi jejich zaměřeními existuje lineární zobrazení $\varphi : Z(\mathcal{A}) \to Z(\mathcal{B})$ takové, že pro všechny $A \in \mathcal{A}$, $v \in Z(\mathcal{A})$ platí

$$f(A + v) = f(A) + \varphi(v).$$

Zobrazení $f$ a $\varphi$ jsou jednoznačně zadána touto vlastností a libovolně zvolenými obrazy $(\dim \mathcal{A} + 1)$ bodů v obecné poloze.

$q$ (volný parametr ve vyjádření přímky jsme nazvali $u$, abychom zamezili duplicitě proměnných). Vyřešením této soustavy získáme $s = 2$, $t = 2, u = 3$ a dosazením například $u = 3$ do rovnice přímky $q$ dostaneme $Q = [5, 5, 3]$ (stejný bod dostaneme i pokud dosadíme $s = 2$, $t = 2$, do parametrického vyjádření roviny $\rho$). Hledaná příčka je tedy dána bodem $Q$ a bodem $[1, 0, 0]$. Snadno již dopočteme její průnik s přímkou $p$, bod $P = [7/3, 5/3, 1]$. □

**4.16.** Určete osu mimoběžek

$$p : [3, 0, 3] + (0, 1, 2)t, \quad t \in \mathbb{R},$$
$$q : [0, -1, -2] + (1, 2, 3)s, \quad s \in \mathbb{R}.$$

**Řešení.** Jde o problém najít příčku se směrem kolmým jak na směrový vektor přímky $p$, tak na směrový vektor přímky $q$. Tento směr můžeme najít například vektorovým součinem těchto dvou vektorů, je to směr $(1, -2, 1)$. Nyní sestavíme soustavu lineárních rovnic reflektující požadavek, aby vektor určený nějakými dvěma body, jeden na přímce $p$, druhý na $q$, byl rovnoběžný se směrem $(1, -2, 1)$. Symbolicky tedy dostáváme soustavu $P - Q = k(1, -2, 1)$, neboli $\underbrace{[3, 0, 3] + (0, 1, 2)t}_{P} - \underbrace{([0, -1, -2] + (1, 2, 3)s)}_{Q} = k(1, -2, 1)$.
Rozepsáním této rovnosti po souřadnicích, dostaneme

$$\begin{array}{rcrcrcr} 3 & & & - & s & = & k, \\ 1 & + & t & - & 2s & = & -2k, \\ 5 & + & 2t & - & 3s & = & k \end{array}$$

s řešeními $t = 1, s = 2, k = 1$. Dosazením $t = 1$ do parametrického vyjádření přímky $p$ dostáváme jeden bod osy, bod $[3, 1, 5]$, dosazením parametru $s = 2$ do vyjádření přímky $q$ pak bod $[2, 3, 4]$). Těmito dvěma body je určena hledaná osa. □

## B. Eukleidovská geometrie

**4.17. Pata kolmice.** Určete patu kolmice spuštěné z bodu $[0, 0, 6]$ na rovinu

$$\rho : [2, 1, 4] + (1, 2, 2)t + (-2, 1, 1)s.$$

**Řešení.** V příkladech ‖2.56‖ a ‖2.57‖ jsme se naučili určovat matici kolmé projekce v $\mathbb{R}^3$ na rovinu procházející počátkem souřadnic, tedy kolmou projekci ve vektorovém prostoru $\mathbb{R}^3$. Toho nyní využijeme. Posuneme projekční rovinu (a s ní i zobrazovaný bod) tak, aby procházela počátkem souřadnic. Dle toho, jak je rovina zadána, se nabízí posunutí o vektor $(-2, -1, -4)$. Určeme nyní kolmý průmět bodu (vektoru $u$) $[0, 0, 6] - (2, 1, 4) = [-2, -1, 2]$ do roviny (vektorového podprostoru) $\rho : [0, 0, 0] + (1, 2, 2)t + (-2, 1, 1)$ tak jako v příkladu viz

Pro libovolnou afinní kombinaci bodů $t_0A_0 + \cdots + t_sA_s \in \mathcal{A}$ pak dostaneme

$$\begin{aligned} f(t_0A_0 + \cdots + t_sA_s) &= \\ &= f(A_0 + t_1(A_1 - A_0) + \cdots + t_s(A_s - A_0)) = \\ &= f(A_0) + t_1\varphi(A_1 - A_0) + \cdots + t_s\varphi(A_s - A_0) = \\ &= t_0 f(A_0) + t_1 f(A_1) + \cdots + t_s f(A_s). \end{aligned}$$

Naopak, pokud pro nějaké zobrazení platí, že zachovává afinní kombinace, můžeme použít speciální případ kombinace $n + 1$ pevně zvolených vektorů zadávajících afinní repér. Postupně pak volbou koeficientů $t_0 = 0$ a $t_i = 1$ definujeme hodnotu zobrazení $\varphi$ mezi zaměřeními vztahem $\varphi(A_i - A_0) = f(A_1)$. Pak lze číst předchozí výpočet v opačném pořadí a ověřit korektnost i linearitu $\varphi$. Skutečně, z předpokladu, že se první a poslední řádek rovnají dovodíme, že jsou si rovny také řádky druhý a třetí. Tím jsme zjistili, že se skutečně jedná o afinní zobrazení s lineárním zobrazením $\varphi$ na zaměření, které jsme uvedeným postupem popsali ve zvoleném afinním repéru. Platí proto:

**Věta.** *Afinní zobrazení jsou právě ta zobrazení, která zachovávají afinní kombinace bodů.*

Ve skutečnosti stačí ověřit zachovávání afinní kombinace pro všechny dvojice bodů, protože z nich už vytvoříme i libovolnou konečnou afinní kombinaci. Skutečně, afinní kombinaci $k+2$ bodů $A_0, A_{k+1}$ vždycky můžeme vyjádřit takto:

$$r(t_0A_0 + \cdots + t_kA_k) + sA_{k+1},$$

kde $\sum_{i=0}^{k} t_k = 1$ a $r + s = 1$. Prostě napřed si vybereme nějaký bod, který je afinní kombinací $k + 1$ bodů a pak děláme jeho kombinace s posledním. Takto můžeme postupně skutečně jakoukoliv konečnou afinní kombinaci vyrobit z kombinací dvojic.

**4.13. Poměr bodů na přímce.** Afinní kombinace dvojice bodů můžeme také dobře vyjádřit pomocí tzv. *poměru bodů* na přímce. Jeli bod $C$ afinní kombinací bodů $A$ a $B \neq C$, $C = rA + sB$, pak řekneme, že číslo



$$\lambda = (C; A, B) = -\frac{s}{r}$$

je poměrem bodu $C$ vzhledem k daným bodům $A$ a $B$. Protože bod $C$ můžeme vyjádřit jako

$$C = A + s(B - A) = B + r(A - B),$$

je poměr $\lambda$ ve skutečnosti poměrem velikostí orientovaných vektorů $C - A$ a $C - B$. Zejména je $\lambda = -1$ právě, když je $C$ středem úsečky dané body $A$ a $B$ (tj. v naší afinní kombinaci bude $r = s = \frac{1}{2}$).

Naše charakterizace afinních zobrazení prostřednictvím afinních kombinací tedy má velice srozumitelně znějící důsledek:

**Důsledek.** *Afinní zobrazení jsou právě ta zobrazení, která zachovávají poměry.*

**4.14. Změny souřadnic.** Volbou afinních souřadnic $(A_0, \underline{u})$ na $\mathcal{A}$ a $(B_0, \underline{v})$ na $\mathcal{B}$ dostáváme souřadné vyjádření afinního zobrazení $f : \mathcal{A} \to \mathcal{B}$. Přímo z definice je zřejmé, že stačí vyjádřit obraz $f(A_0)$ počátku souřadnic v $\mathcal{A}$ v souřadnicích na $\mathcal{B}$, tj. vyjádřit vektor $f(A_0) - B_0$ v bázi $\underline{v}$ jako sloupec souřadnic $y_0$ a vše ostatní je pak určeno násobením maticí zobrazení $\varphi$ ve zvolených bázích

‖2.57‖: snadno nalezneme nějaký kolmý vektor k rovině $\rho$ (viz ‖4.1‖, například vektor $(0, 1, -1)$. Kolmá projekce je potom dána jako

$$u - \frac{u \cdot (0,1,-1)}{(0,1,-1)\cdot(0,1,-1)}(0,1,-1) = \left(-2, \frac{1}{2}, \frac{1}{2}\right).$$

Projekci pak dostaneme zpětným posunutím o vektor $(2, 1, 4)$, je tedy rovna $\left[-2, \frac{1}{2}, \frac{1}{2}\right] + (2, 1, 4) = \left[0, -\frac{3}{2}, -\frac{3}{2}\right]$. □

**4.18. Zrcadlení.** Určete obraz bodu $[3, 2, 2]$ v zrcadlení podle roviny $x + y + z = 1$.

**Řešení.** Podobně jako v předchozím příkladu ‖4.17‖ posuneme rovinu zrcadlení tak, aby procházela počátkem souřadné soustavy. Toho dosáhneme například posunutím o $-1$ ve směru osy $z$, neboli uvážíme nové souřadnice $(x', y', z') = (x, y, z-1)$. Rovnice dané roviny je pak $x' + y' + z' = 0$. Nyní zobrazíme posunutý bod ($[3, 2, 1]$) známým způsobem (získáme bod $X'$) a obraz posuneme zpět (získáme bod $X''$). Je tedy

$$X' = [3,2,1] - 2 \cdot \frac{(3,2,1)\cdot(1,1,1)}{3}(1,1,1) = [-1,-2,-3].$$

Souřadnice hledaného obrazu $X''$ jsou $X'' = X' + (0, 0, 1) = [-1, -2, -2]$. Při zrcadlení bodu $[3, 2, 1]$ jsme samozřejmě mohli použít přímo matice získané v příkladu ‖2.58‖. □

**4.19.** Určete vzdálenost přímek v $\mathbb{R}^3$:

$$p : [1,-1,0] + t(-1,2,3) \quad \text{a} \quad q : [2,5,-1] + t(-1,-2,1).$$

**Řešení.** Vzdálenost je dána jako velikost kolmého průmětu libovolné příčky (spojnice) daných přímek do ortogonálního doplňku vektorového podprostoru generovaného jejich zaměřeními. Tento ortogonální doplněk zjistíme například pomocí vektorového součinu:

$$\langle(-1,2,3),(-1,-2,1)\rangle^\perp = \langle(-1,2,3)\times(-1,-2,1)\rangle = \\ = \langle(8,-2,4)\rangle = \langle(4,-1,2)\rangle.$$

Spojnicí daných přímek je například úsečka $[1, -1, 0][2, 5, -1]$, promítneme tedy vektor $[1, -1, 0] - [2, 5, -1] = (-1, -6, 1)$. Pro vzdálenost přímek pak dostáváme:

$$\rho(p,q) = \frac{|(-1,-6,1)\cdot(4,-1,2)|}{\|(4,-1,2)\|} = \frac{4}{\sqrt{21}}.$$ □

**4.20.** Jarda stojí v bodě $[2, 1, 2]$ a má tyč délky 4. Může se touto tyčí současně dotknout přímek $p$ a $q$, kde

$$p : [-1,4,1] + t(-1,2,0),$$
$$q : [4,4,-1] + s(1,2,-4)?$$

(Tyč musí procházet bodem $[2, 1, 2]$.)

a přičtením výsledku. Každé afinní zobrazení tedy v souřadnicích vypadá takto:

$$x \mapsto y_0 + Y \cdot x,$$

kde $y_0$ je jako výše a $Y$ je matice zobrazení $\varphi$.

Transformace afinních souřadnic odpovídá, obdobně jako u lineárních zobrazení, vyjádření identického zobrazení ve zvolených afinních repérech. Změna souřadného vyjádření afinního zobrazení v důsledku změny bází se snadno spočte pomocí násobení a sčítání matic a vektorů. Skutečně, při změně báze na definičním oboru daném posunutím $w$ a maticí $M$, přičemž staré souřadnice pomocí nových jsou

$$x = w + M \cdot x',$$

a změně na oboru hodnot s posunutím $z$ a maticí $N$, přičemž nové souřadnice jsou pomocí starých

$$y' = z + N \cdot y,$$

dostáváme pro zobrazení dané v původních bázích vektorem posunutí $y_0$ a maticí $Y$ přímým výpočtem

$$y' = z + N \cdot y = z + N \cdot (y_0 + Y \cdot x) = \\ = (z + N \cdot y_0 + N \cdot Y \cdot w) + (N \cdot Y \cdot M) \cdot x'.$$

Je tedy afinní zobrazení v nových bázích dáno vektorem posunutí $z + N \cdot y_0 + N \cdot Y \cdot w$ a maticí $N \cdot Y \cdot M$.

**4.15. Euklidovské bodové prostory.** Zatím jsme pro naše



elementární geometrické úvahy nepotřebovali pojem vzdálenosti nebo velikosti. V mnoha praktických úlohách ale velikost vektorů a odchylka vektorů, tak jak jsme je zavedli na samém konci třetí části druhé kapitoly (viz 2.40 a dále), hrají podstatnou roli. Ve skutečnosti se ale dodatečné informace týkají opravdu jen vektorů v zaměření, takže nám nezbývá mnoho práce:

EUKLIDOVSKÉ PROSTORY

Standardní *bodový euklidovský prostor* $\mathcal{E}_n$ je afinní prostor $\mathcal{A}_n$, jehož zaměřením je standardní euklidovský prostor $\mathbb{R}^n$ se skalárním součinem

$$\langle x, y\rangle = y^T \cdot x.$$

*Kartézská souřadná soustava* je afinní souřadná soustava $(A_0; \underline{u})$ s ortonormální bází $\underline{u}$.

*Vzdálenost bodů* $A, B \in \mathcal{E}_n$ definujeme jako velikost vektoru $\|B - A\|$, budeme ji značit $\rho(A, B)$.

*Euklidovské podprostory* v $\mathcal{E}_n$ jsou afinní podprostory, jejichž zaměření uvažujeme spolu se zúženými skalárními součiny.

*Bodovým euklidovským prostorem* $\mathcal{E}$ dimenze $n$ pak obecně rozumíme afinní prostor, jehož zaměření je reálný $n$–rozměrný euklidovský vektorový prostor. Pojem kartézské souřadné soustavy má opět jasný smysl. Každá volba takové souřadné soustavy ovšem zadává ztotožnění $\mathcal{E}$ se standardním prostorem $\mathcal{E}_n$. Proto se budeme v dalším, bez újmy na obecnosti, zabývat hlavně standardními euklidovskými prostory a jejich podprostory.

Z geometrického pohledu mají jednoduché vlastnosti skalárního součinu, jako jsou trojúhelníková nerovnost,



Cauchyova nerovnost, Besselova nerovnost apod., odvozené ve čtvrté části předchozí kapitoly, viz 3.25, velmi užitečné přímé důsledky:

**4.16. Věta.** *Pro body* $A, B, C \in \mathcal{E}_n$ *platí:*

**Řešení.** Již známým způsobem spočítáme příčku daných přímek procházející bodem [2, 1, 2]. Je jí úsečka [1, 0, 1][3, 2, 3], její délka je potom $\sqrt{12}$, což je méně než 4. Jarda se tedy danou tyčí dotknout přímek současně může. □

**4.21.** Nalezněte bod $A$ přímky

$$p : x + 2y + z - 1 = 0, \quad 3x - y + 4z - 29 = 0,$$

který má stejnou vzdálenost od bodů $B = [3, 11, 4]$ a $C = [-5, -13, -2]$.

**Řešení.** Nejprve vyjádříme přímku $p$ parametricky tak, že vyřešíme soustavu rovnic

$$\begin{array}{rcrcrcl} x & + & 2y & + & z & = & 1, \\ 3x & - & y & + & 4z & = & 29. \end{array}$$

Soustavu zapíšeme rozšířenou maticí a upravíme

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 3 & -1 & 4 & 29 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & -7 & 1 & 26 \end{array}\right) \sim$$
$$\sim \left(\begin{array}{ccc|c} 1 & 0 & 9/7 & 59/7 \\ 0 & 1 & -1/7 & -26/7 \end{array}\right).$$

Tím dostáváme vyjádření

$$p : \left[\frac{59}{7}, -\frac{26}{7}, 0\right] + t\left(-\frac{9}{7}, \frac{1}{7}, 1\right), \quad t \in \mathbb{R}.$$

Odkud substitucí $t = 7s + 26$ plyne

$$p : [-25, 0, 26] + s\ (-9, 1, 7), \quad s \in \mathbb{R}.$$

Bod $A$ obdržíme volbou jistého $s \in \mathbb{R}$. Přitom vektory

$$A - B = (-28 - 9s, -11 + s, 22 + 7s),$$
$$A - C = (-20 - 9s, 13 + s, 28 + 7s)$$

mají mít stejnou délku, tj. má platit

$$\sqrt{(-28 - 9s)^2 + (-11 + s)^2 + (22 + 7s)^2} =$$
$$= \sqrt{(-20 - 9s)^2 + (13 + s)^2 + (28 + 7s)^2},$$

resp.

$$(-28 - 9s)^2 + (-11 + s)^2 + (22 + 7s)^2 =$$
$$= (-20 - 9s)^2 + (13 + s)^2 + (28 + 7s)^2.$$

Úpravou poslední rovnice získáme $s = -3$. Je tak

$$A = [-25, 0, 26] - 3\,(-9, 1, 7) = [2, -3, 5].$$ □

*(1)* $\rho(A, B) = \rho(B, A)$.
*(2)* $\rho(A, B) = 0$, *právě když* $A = B$.
*(3)* $\rho(A, B) + \rho(B, C) \geq \rho(A, C)$.
*(4) V každé kartézské souřadné soustavě* $(A_0; \underline{e})$ *mají body* $A = A_0 + a_1e_1 + \ldots + a_ne_n$, $B = A_0 + b_1e_1 + \cdots + b_ne_n$ *vzdálenost* $\sqrt{\sum_{i=1}^{n}(a_i - b_i)^2}$.
*(5) Je-li dán bod* $A$ *a podprostor* $\mathcal{Q}$ *v* $\mathcal{E}_n$, *pak existuje bod* $P \in \mathcal{Q}$ *minimalizující vzdálenosti bodů* $\mathcal{Q}$ *od* $A$. *Vzdálenost bodů* $A$ *a* $P$ *je rovna velikosti kolmého průmětu vektoru* $A - B$ *do* $Z(\mathcal{Q})^\perp$ *pro libovolný* $B \in \mathcal{Q}$.
*(6) Obecněji, pro podprostory* $\mathcal{Q}$ *a* $\mathcal{R}$ *v* $\mathcal{E}_n$ *existují body* $P \in \mathcal{Q}$ *a* $Q \in \mathcal{R}$ *minimalizující vzdálenosti bodů* $B \in \mathcal{Q}$ *a* $A \in \mathcal{R}$. *Vzdálenost bodů* $Q$ *a* $P$ *je rovna velikosti kolmého průmětu vektoru* $A-B$ *do* $(Z(\mathcal{Q})+Z(\mathcal{R}))^\perp$ *pro libovolné body* $B \in \mathcal{Q}$ *a* $A \in \mathcal{R}$.

Důkaz. První tři vlastnosti vyplývají přímo z vlastností velikosti vektorů v prostorech se skalárním součinem, čtvrtá plyne přímo z vyjádření skalárního součinu v libovolné ortonormální bázi.



Podívejme se na vztah pro minimalizaci vzdálenosti $\rho(A, B)$ pro $B \in \mathcal{Q}$. Vektor $A - B$ se jednoznačně rozkládá na $A - B = u_1 + u_2$, $u_1 \in Z(\mathcal{Q})$, $u_2 \in Z(\mathcal{Q})^\perp$. Přitom $u_2$ nezávisí na volbě $B \in \mathcal{Q}$, protože případná změna bodu $B$ se projeví přičtením vektoru ze $Z(\mathcal{Q})$.

Nyní zvolme $P = A + (-u_2) = B + u_1 \in \mathcal{Q}$. Dostáváme

$$\|A - B\|^2 = \|u_1\|^2 + \|u_2\|^2 \geq \|u_2\|^2 = \|A - P\|^2.$$

Odtud již vyplývá, že nejmenší možné vzdálenosti je skutečně dosaženo, a to právě pro náš bod $P$. Vypočtená vzdálenost je skutečně $\|u_2\|$.

Obdobně ukážeme obecný výsledek. Pro volbu libovolných bodů $A \in \mathcal{R}$ a $B \in \mathcal{Q}$ je jejich rozdíl dán jako součet vektorů $u_1 \in Z(\mathcal{R}) + Z(\mathcal{Q})$ a $u_2 \in (Z(\mathcal{R}) + Z(\mathcal{Q}))^\perp$, přičemž komponenta $u_2$ nezávisí na volbě bodů. Přičtením vhodných vektorů ze zaměření $\mathcal{R}$ a $\mathcal{Q}$ zjevně obdržíme body $A'$ a $B'$, jejichž vzdálenost je právě $\|u_2\|$. □

Rozšíříme nyní náš stručný přehled elementárních úloh v analytické geometrii.

**4.17. Příklady standardních úloh.** (1) *Najděte vzdálenost bodu* $A \in \mathcal{E}_n$ *od podprostoru* $\mathcal{Q} \subseteq \mathcal{E}_n$:



Postup při řešení je dán ve větě 4.16.

(2) *V* $\mathcal{E}_2$ *veďte bodem* $A$ *přímku* $q$ *svírající s danou přímkou* $p$ *daný úhel:*

Připomeňme, že na úrovni rovinné geometrie jsme s odchylkami vektorů již pracovali (viz např. 2.43). Najdeme vektor $u \in \mathbb{R}^2$ ležící v zaměření přímky $q$ a zvolíme vektor $v$ mající od $u$ zadanou odchylku. Hledaná přímka je dána bodem $A$ a zaměřením $\langle v \rangle$. Úloha má dvě nebo jedno řešení.

(3) *Spočtěte patu kolmice vedené bodem na danou přímku:*

Postup je uveden v důkazu předposledního bodu věty 4.16.

(4) *V* $\mathcal{E}_3$ *určete vzdálenost dvou přímek* $p$, $q$:

Zvolíme libovolně jeden bod z každé přímky, $A \in p$, $B \in q$. Komponenta vektoru $A - B$ v ortogonálním doplňku $(Z(p) + Z(q))^\perp$ má velikost rovnu vzdálenosti $p$ a $q$.

(5) *V* $\mathcal{E}_3$ *najděte osu dvou mimoběžek* $p$ *a* $q$:

Osou zde rozumíme příčku, která realizuje nejmenší možnou vzdálenost daných mimoběžek pomocí bodů průniku. Opět

**4.22.** V euklidovském prostoru $\mathbb{R}^4$ stanovte vzdálenost bodu $A = [2, -5, 1, 4]$ od podprostoru daného rovnicemi

$$U : 4x_1 - 2x_2 - 3x_3 - 2x_4 + 12 = 0, \quad 2x_1 - x_2 - 2x_3 - 2x_4 + 9 = 0.$$

**Řešení.** Nejdříve nalezneme parametrické vyjádření podprostoru $U$. Např. je

$$B = [0, 3, 0, 3] \in U.$$

Víme, že vzdálenost $A$ od $U$ se rovná velikosti kolmého průmětu vektoru $A - B$ do ortogonálního doplňku zaměření podprostoru $U$. Ortogonální doplněk zaměření $U$ ovšem známe (zadává tento podprostor) – jako množinu (lineárních kombinací normálových vektorů)

$$V := \{t\,(4, -2, -3, -2) + s\,(2, -1, -2, -2)\,;\, t, s \in \mathbb{R}\}.$$

Potřebujeme najít kolmý průmět $P_{A-B}$ vektoru $A - B$ do $V$, který náleží do $V$, a proto je

$$P_{A-B} = a\,(4, -2, -3, -2) + b\,(2, -1, -2, -2)$$

pro jisté hodnoty $a, b \in \mathbb{R}$. Zjevně musí platit $(A - B - P_{A-B}) \perp V$, tedy

$$((A - B) - P_{A-B}) \perp (4, -2, -3, -2)\,,$$
$$((A - B) - P_{A-B}) \perp (2, -1, -2, -2)\,.$$

Dosazením za $A - B$ a $P_{A-B}$ odsud vyplývá

$$\begin{aligned}((2, -8, 1, 1) - a(4, -2, -3, -2) - b(2, -1, -2, -2))\cdot\\ \cdot(4, -2, -3, -2) = 0,\\ ((2, -8, 1, 1) - a(4, -2, -3, -2) - b(2, -1, -2, -2))\cdot\\ \cdot(2, -1, -2, -2)) = 0,\end{aligned}$$

tj.

$$\begin{aligned}(2, -8, 1, 1)\cdot(4, -2, -3, -2) -\\ -a(4, -2, -3, -2)\cdot(4, -2, -3, -2) -\\ -b(2, -1, -2, -2)\cdot(4, -2, -3, -2) = 0,\\ ((2, -8, 1, 1)\cdot(2, -1, -2, -2)) -\\ -a(4, -2, -3, -2)\cdot(2, -1, -2, -2) -\\ -b(2, -1, -2, -2)\cdot(2, -1, -2, -2 = 0.\end{aligned}$$

Vyčíslíme-li tyto skalární součiny, obdržíme soustavu

$$\begin{aligned}19 &- 33a - 20b = 0,\\ 8 &- 20a - 13b = 0,\end{aligned}$$

která má jediné řešení $a = 3, b = -4$. Je tudíž

$$P_{A-B} = 3\,(4, -2, -3, -2) - 4\,(2, -1, -2, -2) = (4, -2, -1, 2)\,,$$

lze postup dovodit z důkazu věty 4.16 (poslední bod). Nechť $\eta$ je podprostor generovaný jedním bodem $A \in p$ a součtem $Z(p) + (Z(p) + Z(q))^\perp$. Pokud nejsou přímky $p$ a $q$ rovnoběžné, půjde o rovinu. Pak průnik $\eta \cap q$ spolu se zaměřením $(Z(p) + Z(q))^\perp$ dávají parametrický popis hledané osy. Pokud jsou přímky rovnoběžné, bude mít úloha nekonečně mnoho řešení.

**4.18. Odchylky.** Stejně jako vzdálenost, i řada dalších geometrických pojmů jako odchylky, orientace, objem apod. je v bodových prostorech $\mathcal{E}_n$ zaváděna prostřednictvím vhodných pojmů ve vektorových euklidovských prostorech. Připomeňme, že odchylku dvou vektorů jsme definovali na konci třetí části druhé kapitoly, viz 2.43.



Skutečně, z Cauchyovy nerovnosti plyne $0 \le \frac{|u\cdot v|}{\|u\|\|v\|} \le 1$, má tedy smysl definice *odchylky* $\varphi(u, v)$ *vektorů* $u, v \in V$ v reálném vektorovém prostoru se skalárním součinem vztahem

$$\cos\varphi(u, v) = \frac{u \cdot v}{\|u\|\|v\|}, \quad 0 \le \varphi(u, v) \le 2\pi.$$

To je zcela v souladu s praxí v dvourozměrném euklidovském prostoru $\mathbb{R}^2$ a naší filozofií, že pojem týkající se dvou vektorů je ve své podstatě záležitostí dvourozměrné geometrie.

V euklidovské rovině jsme také již používali goniometrické funkce cos a sin, které jsme definovali pouze geometrickou úvahou, ke které se vrátíme na začátku kapitoly páté, kdy také budeme moci precizně ověřit geometrický názor, že je funkce cos na intervalu $[0, \pi]$ klesající. Ve vícerozměrných prostorech je proto odchylka dvou vektorů vždy měřena v rovině, kterou tyto vektory generují (nebo je nula) a náš definiční vztah odpovídá zvyklostem ve všech dimenzích.

V libovolném reálném vektorovém prostoru se skalárním součinem přímo z definic plyne

$$\begin{aligned}\|u - v\|^2 &= \|u\|^2 + \|v\|^2 - 2(u \cdot v) =\\ &= \|u\|^2 + \|v\|^2 - 2\|u\|\|v\|\cos\varphi(u, v).\end{aligned}$$

To je patrně dobře známá *kosinová věta* z rovinné geometrie.

Dále platí pro každou ortonormální bázi $\underline{e}$ zaměření $V$ a nenulový vektor $u \in V$ vztah

$$\|u\|^2 = \sum_i |u \cdot e_i|^2.$$

Podělením této rovnice číslem $\|u\|^2$ dostáváme vztah

$$1 = \sum_i (\cos\varphi(u, e_i))^2,$$

který je větou o směrových kosinech $\varphi(u, e_i)$ vektoru $u$.

Z definice odchylek vektorů nyní můžeme dovodit rozumné definice pro odchylky obecných podprostorů v libovolném euklidovském vektorovém prostoru. Je přitom třeba rozhodnutí, jak se stavět k případům, kdy podprostory mají netriviální průnik. Za odchylku dvou přímek budeme chtít patrně brát menší ze dvou možných úhlů, u dvou nerovnoběžných rovin v $\mathbb{R}^3$ nebudeme chtít slyšet, že mají odchylku nula, protože mají společný alespoň jeden směr:

### Odchylky podprostorů

**4.19. Definice.** Uvažujme konečněrozměrné podprostory $U_1, U_2$ v euklidovském vektorovém prostoru $V$ libovolné dimenze.

*Odchylka podprostorů* $U_1$, $U_2$ je reálné číslo $\alpha = \varphi(U_1, U_2) \in [0, \frac{\pi}{2}]$ splňující:

přičemž

$$|| P_{A-B} || = \sqrt{4^2 + (-2)^2 + (-1)^2 + 2^2} = 5.$$

Připomeňme, že vzdálenost $A$ od $U$ je rovna $|| P_{A-B} || = 5$. □

Další příklady na Eukleidovské prostory naleznete na straně 227, zejména je zde poprvé demonstrována technika používaná při řešení problému nejmenších čtverců.

**4.23.** V euklidovském prostoru $\mathbb{R}^5$ stanovte vzdálenost rovin

$$\varrho_1 : [7, 2, 7, -1, 1] + t_1\,(1, 0, -1, 0, 0) + s_1\,(0, 1, 0, 0, -1)\,,$$
$$\varrho_2 : [2, 4, 7, -4, 2] + t_2\,(1, 1, 1, 0, 1) + s_2\,(0, -2, 0, 0, 3)\,,$$

kde $t_1, s_1, t_2, s_2 \in \mathbb{R}$, a poté vzdálenost rovin

$$\sigma_1 : [0, 1, 2, 0, 0] + p_1\,(2, 1, 0, 0, 1) + q_1\,(-2, 0, 1, 1, 0)\,,$$
$$\sigma_2 : [3, -1, 7, 7, 3] + p_2\,(2, 2, 4, 0, 3) + q_2\,(2, 0, 0, -2, -1)\,,$$

kde $p_1, q_1, p_2, q_2 \in \mathbb{R}$.

**Řešení.** Případ $\varrho_1$, $\varrho_2$. Nejprve určíme ortogonální doplněk součtu zaměření zadaných dvou rovin tak, že směrové vektory rovin napíšeme do řádků matice a tuto matici pomocí elementárních řádkových transformací převedeme na schodovitý tvar. Tím dostaneme

$$\begin{pmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & -2 & 0 & 0 & 3 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Hledaný ortogonální doplněk tak je $\langle(0, 0, 0, 1, 0)\rangle$. (Pochopitelně bylo očividné, že vektor $(0, 0, 0, 1, 0)$ náleží do uvažovaného ortogonálního doplňku. Úpravou na schodovitý tvar jsme však zjistili, že ortogonální doplněk je jednodimenzionální.) Vzdálenost rovin je rovna velikosti kolmého průmětu vektoru $A_1 - A_2$ do podprostoru $\langle(0, 0, 0, 1, 0)\rangle$ pro libovolné body $A_1 \in \varrho_1$, $A_2 \in \varrho_2$. Zvolme kupř. $A_1 = [7, 2, 7, -1, 1]$, $A_2 = [2, 4, 7, -4, 2]$. Zřejmě je kolmý průmět $A_1 - A_2 = (5, -2, 0, 3, -1)$ do $\langle(0, 0, 0, 1, 0)\rangle$ roven $(0, 0, 0, 3, 0)$. Velikost vektoru $(0, 0, 0, 3, 0)$ dává výslednou vzdálenost 3.

Případ $\sigma_1$, $\sigma_2$. Součet zaměření rovin $\sigma_1$, $\sigma_2$ je generován směrovými vektory. Označme je

$$u_1 = (2, 1, 0, 0, 1)\,, \qquad u_2 = (-2, 0, 1, 1, 0)\,,$$
$$v_1 = (2, 2, 4, 0, 3)\,, \qquad v_2 = (2, 0, 0, -2, -1)\,.$$

(1) Je-li $\dim U_1 = \dim U_2 = 1$, $U_1 = \langle u\rangle$, $U_2 = \langle v\rangle$, pak

$$\cos\alpha = \frac{|u.v|}{\|u\|\|v\|}.$$

(2) Jsou-li dimenze $U_1$, $U_2$ kladné a $U_1 \cap U_2 = \{0\}$, pak je odchylka minimem všech odchylek jednorozměrných podprostorů

$$\alpha = \min\{\varphi(\langle u\rangle, \langle v\rangle);\, 0 \neq u \in U_1, 0 \neq v \in U_2\}.$$

Ukážeme vzápětí, že takové minimum skutečně vždy existuje.

(3) Je-li $U_1 \subseteq U_2$ nebo $U_2 \subseteq U_1$ (zejména je-li jeden z nich nulový), je $\alpha = 0$.

(4) Je-li $U_1 \cap U_2 \neq \{0\}$ a $U_1 \neq U_1 \cap U_2 \neq U_2$, pak

$$\alpha = \varphi(U_1 \cap (U_1 \cap U_2)^\perp, U_2 \cap (U_1 \cap U_2)^\perp).$$

*Odchylka podprostorů* $\mathcal{Q}_1$, $\mathcal{Q}_2$ v bodovém euklidovském prostoru $\mathcal{E}_n$ se definuje jako odchylka jejich zaměření $Z(\mathcal{Q}_1)$, $Z(\mathcal{Q}_2)$.

Všimněme si, že odchylka je vždy dobře definována, zejména v posledním případě je

$$(U_1 \cap (U_1 \cap U_2)^\perp) \cap (U_2 \cap (U_1 \cap U_2)^\perp) = \{0\}.$$

Můžeme tedy opravdu odchylku určit podle bodu (2). Všimněme si také, že v případě $U_1 \cap U_2 = \{0\}$, jsou $U_1$ a $U_2$ kolmé podle našich dřívějších definic, právě když jejich odchylka je $\pi/2$. Pokud však mají netriviální průnik, nemohou být kolmé v dřívějším smyslu.

Ke korektnosti definice zbývá ukázat, že ve skutečnosti vždy existují vektory $u \in U_1$, $v \in U_2$, pro které nabývá výraz pro odchylku požadovaného minima. Nejdříve speciální případ:

**4.20. Lemma.** *Nechť $v$ je vektor v euklidovském prostoru $V$ a $U \subseteq V$ libovolný podprostor. Označme $v_1 \in U$, $v_2 \in U^\perp$ (jednoznačně určené) komponenty vektoru $v$, tj. $v = v_1 + v_2$. Pak pro odchylku $\varphi$ podprostoru generovaného $v$ od $U$ platí*

$$\cos\varphi(\langle v\rangle, U) = \cos\varphi(\langle v\rangle, \langle v_1\rangle) = \frac{\|v_1\|}{\|v\|}.$$

Důkaz. Pro všechny vektory $u \in U$ platí díky Cauchyově nerovnosti

$$\frac{|u \cdot v|}{\|u\|\|v\|} = \frac{|u \cdot (v_1 + v_2)|}{\|u\|\|v\|} = \frac{|u \cdot v_1|}{\|u\|\|v\|} \leq$$
$$\leq \frac{\|u\|\|v_1\|}{\|u\|\|v\|} = \frac{\|v_1\|}{\|v\|} = \frac{\|v_1\|^2}{\|v\|\|v_1\|} = \frac{|v_1 \cdot v|}{\|v\|\|v_1\|}.$$

Odtud plyne

$$\cos\varphi(\langle v\rangle, \langle u\rangle) \leq \cos\varphi(\langle v\rangle, \langle v_1\rangle) = \frac{\|v_1\|}{\|v\|}$$

a námi nalezený vektor $v_1$ tedy představuje největší možnou hodnotu pro kosinus úhlu mezi všemi volbami vektorů z $U$. Protože je funkce cos na intervalu $[0, \frac{\pi}{2}]$ klesající, dostáváme tak nejmenší možný úhel a tvrzení je dokázané. □

**4.21. Výpočet odchylek.** Postupu v předchozím lemmatu



můžeme rozumět tak, že jednorozměrný podprostor generovaný vektorem $v$ kolmo promítneme do podprostoru $U$ a podíváme se, jak moc se obrazy zmenšují. Podle toho pak poznáme odchylku. Podobný postup použijeme ve vyšších dimenzích také. Potíž je přitom ale s rozpoznáním, které směry nám svými průměty odchylku skutečně prozradí. V našem předchozím případě to můžeme dobře vidět, pokud nešikovně

Nalezněme body $X_1 \in \sigma_1$, $X_2 \in \sigma_2$, ve kterých se vzdálenost rovin $\sigma_1$, $\sigma_2$ realizuje. Víme, že je

$$\begin{aligned} X_1 - X_2 &= [0,1,2,0,0] - [3,-1,7,7,3] + \\ &\quad + p_1u_1 + q_1u_2 - p_2v_1 - q_2v_2 = \\ &= (-3,2,-5,-7,-3) + p_1u_1 + q_1u_2 - p_2v_1 - q_2v_2 \end{aligned}$$

a že má platit

$$\begin{aligned} \langle X_1 - X_2, u_1 \rangle &= 0, & \langle X_1 - X_2, u_2 \rangle &= 0, \\ \langle X_1 - X_2, v_1 \rangle &= 0, & \langle X_1 - X_2, v_2 \rangle &= 0, \end{aligned}$$

tj.

$$\begin{aligned} \langle (-3,2,-5,-7,-3), u_1 \rangle + p_1 \langle u_1, u_1 \rangle + q_1 \langle u_2, u_1 \rangle - \\ - p_2 \langle v_1, u_1 \rangle - q_2 \langle v_2, u_1 \rangle = 0, \\ \langle (-3,2,-5,-7,-3), u_2 \rangle + p_1 \langle u_1, u_2 \rangle + q_1 \langle u_2, u_2 \rangle - \\ - p_2 \langle v_1, u_2 \rangle - q_2 \langle v_2, u_2 \rangle = 0, \\ \langle (-3,2,-5,-7,-3), v_1 \rangle + p_1 \langle u_1, v_1 \rangle + q_1 \langle u_2, v_1 \rangle - \\ - p_2 \langle v_1, v_1 \rangle - q_2 \langle v_2, v_1 \rangle = 0, \\ \langle (-3,2,-5,-7,-3), v_2 \rangle + p_1 \langle u_1, v_2 \rangle + q_1 \langle u_2, v_2 \rangle - \\ - p_2 \langle v_1, v_2 \rangle - q_2 \langle v_2, v_2 \rangle = 0. \end{aligned}$$

Vyčíslením těchto skalárních součinů získáváme soustavu lineárních rovnic

$$\begin{array}{rcrcrcrcr} 6p_1 & - & 4q_1 & - & 9p_2 & - & 3q_2 & = & 7, \\ -4p_1 & + & 6q_1 & & & + & 6q_2 & = & 6, \\ 9p_1 & & & - & 33p_2 & - & q_2 & = & 31, \\ 3p_1 & - & 6q_1 & - & p_2 & - & 9q_2 & = & -11, \end{array}$$

kterou vyřešíme pomocí řádkových transformací v maticovém zápisu

$$\left(\begin{array}{cccc|c} 6 & -4 & -9 & -3 & 7 \\ -4 & 6 & 0 & 6 & 6 \\ 9 & 0 & -33 & -1 & 31 \\ 3 & -6 & -1 & -9 & -11 \end{array}\right) \sim \ldots \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{array}\right).$$

Řešením této soustavy je tedy čtveřice $(p_1, q_1, p_2, q_2) = (0, -1, -1, 2)$. Určili jsme

$$X_1 - X_2 = (-3,2,-5,-7,-3) - u_2 + v_1 - 2v_2 = (-3,4,-2,-4,2).$$

Velikost vektoru $(-3,4,-2,-4,2)$ a současně vzdálenost rovin $\sigma_1$, $\sigma_2$ činí

$$7 = \sqrt{(-3)^2 + 4^2 + (-2)^2 + (-4)^2 + 2^2}.$$

Vzdálenost $\varrho_1$ od $\varrho_2$ jsme určovali odlišným způsobem ne vzdálenost $\sigma_1$ od $\sigma_2$. Uvedené metody jsme samozřejmě mohli použít v obou případech. Zkusme znovu vypočítat vzdálenost rovin $\sigma_1, \sigma_2$ postupem budeme promítat větší prostor $U$ do jednorozměrného $\langle v \rangle$ a pak kolmo zpět do $U$. Zjistíme, že odchylku poznáme podle směru vlastního vektoru takového zobrazení, jeho vlastní číslo bude kvadrátem příslušného kosinu úhlu.

Uvažujme tedy dva obecné podprostory $U_1$, $U_2$ v euklidovském vektorovém prostoru $V$, předpokládejme $U_1 \cap U_2 = \{0\}$, a zvolme pevně ortonormální báze $\underline{e}$, a $\underline{e}'$ celého prostoru $V$ tak, aby $U_1 = \langle e_1, \ldots, e_k \rangle$, $U_2 = \langle e'_1, \ldots, e'_l \rangle$.

Uvažujme kolmý průmět $\varphi$ prostoru $V$ na $U_2$, jeho zúžení na $U_1$ budeme opět značit $\varphi : U_1 \to U_2$. Zobrazení $\psi : U_2 \to U_1$ nechť vznikne podobně z kolmého průmětu na $U_1$. Tato zobrazení mají v bázích $(e_1, \ldots, e_k)$ a $(e'_1, \ldots, e'_l)$ matice

$$A = \begin{pmatrix} e_1 \cdot e'_1 & \ldots & e_k \cdot e'_1 \\ \vdots & & \vdots \\ e_1 \cdot e'_l & \ldots & e_k \cdot e'_l \end{pmatrix}, \quad B = \begin{pmatrix} e'_1 \cdot e_1 & \ldots & e'_l \cdot e_1 \\ \vdots & & \vdots \\ e'_1 \cdot e_k & \ldots & e'_l \cdot e_k \end{pmatrix}.$$

Protože jde o skalární součiny na reálném vektorovém prostoru, platí $e_i \cdot e'_j = e'_j \cdot e_i$ pro všechny indexy $i, j$ a proto zejména platí $B = A^T$.

Složené zobrazení $\psi \circ \varphi : U_1 \to U_1$ má tedy symetrickou pozitivně semidefinitní matici $A^T A$ a $\psi$ je zobrazení adjungované k $\varphi$. Viděli jsme, že každé takové zobrazení má pouze nezáporná reálná vlastní čísla a že má ve vhodné ortonormální bázi diagonální matici s těmito vlastními čísly na diagonále, viz 3.29 a 3.31.

Nyní můžeme odvodit obecný postup pro výpočet odchylky $\alpha = \varphi(U_1, U_2)$.

**Věta.** *V předchozím označení nechť je $\lambda$ největší vlastní hodnota matice $A^T A$. Pak $(\cos\alpha)^2 = \lambda$.*



Důkaz. Nechť $u \in U_1$ je vlastní vektor zobrazení $\psi \circ \varphi$ příslušný největší vlastní hodnotě $\lambda$. Uvažme všechna vlastní čísla $\lambda_1, \ldots, \lambda_k$ (včetně násobnosti) a nechť $\underline{u} = (u_1, \ldots, u_n)$ je příslušná ortonormální báze $U_1$ z vlastních vektorů. Můžeme přímo předpokládat, že $\lambda = \lambda_1$, $u = u_1$.

Potřebujeme ukázat, že odchylka libovolného $v \in U_1$ od $U_2$ je nejméně tak velká jako odchylka $u$ od $U_2$. Tzn. že kosinus příslušného úhlu nesmí být větší. Podle předchozího lemmatu stačí diskutovat odchylku $u$ a $\varphi(u) \in U_2$ a přitom víme, že $\|u\| = 1$. Zvolme tedy $v \in U_1$, $v = a_1u_1 + \cdots + a_ku_k$, $\sum_{i=1}^k a_i^2 = \|v\|^2 = 1$. Pak

$$\begin{aligned} \|\varphi(v)\|^2 = \varphi(v) \cdot \varphi(v) = (\psi \circ \varphi(v)) \cdot v \le \\ \le \|\psi \circ \varphi(v)\| \|v\| = \|\psi \circ \varphi(v)\|. \end{aligned}$$

Předchozí lemma navíc dává i vzorec pro odchylku $\alpha$ vektoru $v$ od podprostoru $U_2$

$$\cos\alpha = \frac{\|\varphi(v)\|}{\|v\|} = \|\varphi(v)\|.$$

Protože jsme zvolili za $\lambda_1$ největší z vlastních hodnot a součet kvadrátů souřadnic $a_i^2$ je jedna, dostáváme

$$\begin{aligned} (\cos\alpha)^2 = \|\varphi(v)\|^2 \le \|\psi \circ \varphi(v)\| = \left( \sum_{i=1}^k (\lambda_i a_i)^2 \right)^{\frac{1}{2}} = \\ = \left( \lambda_1^2 + \sum_{i=1}^k a_i^2 (\lambda_i^2 - \lambda_1^2) \right)^{\frac{1}{2}} \le \sqrt{\lambda_1^2}. \end{aligned}$$

použitým k vyčíslení vzdálenosti rovin $\varrho_1, \varrho_2$. Hledejme tedy ortogonální doplněk vektorového podprostoru generovaného vektory

$$(2,1,0,0,1)\,,\ (-2,0,1,1,0)\,,\ (2,2,4,0,3)\,,\ (2,0,0,-2,-1)\,.$$

Snadno získáme

$$\begin{pmatrix} 2 & 1 & 0 & 0 & 1 \\ -2 & 0 & 1 & 1 & 0 \\ 2 & 2 & 4 & 0 & 3 \\ 2 & 0 & 0 & -2 & -1 \end{pmatrix} \sim \ldots \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 3/2 \\ 0 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix},$$

odkud dostáváme ortogonální doplněk $\langle(-3/2, 2, -1, -2, 1)\rangle$, příp. jej raději zapišme jako $\langle(3, -4, 2, 4, -2)\rangle$. Připomeňme, e vzdálenost $\sigma_1$ vůči $\sigma_2$ se rovná velikosti kolmého průmětu vektoru (rozdílu libovolného bodu $\sigma_1$ a libovolného bodu $\sigma_2$)

$$u\ = (3,-2,5,7,3) = [3,-1,7,7,3] - [0,1,2,0,0]$$

do tohoto ortogonálního doplňku. Označme zmíněný kolmý průmět $u$ symbolem $p_u$ a položme $v\ = (3,-4,2,4,-2)$. Zřejmě je $p_u = a \cdot v$ pro nějaké $a \in \mathbb{R}$ a má platit

$$\langle u\ - p_u,\ v\ \rangle = 0, \quad \text{tj.} \quad \langle u,\ v\ \rangle - a\,\langle v,\ v\ \rangle = 0.$$

Vyčíslení dává $49 - a \cdot 49 = 0$. Je proto $p_u = 1 \cdot v\ = v$ a vzdálenost rovin $\sigma_1, \sigma_2$ je rovna

$$||\ p_u\ || = \sqrt{3^2 + (-4)^2 + 2^2 + 4^2 + (-2)^2} = 7.$$

Ukázalo se, že výpočet vzdálenosti pomocí ortogonálního doplňku součtu zaměření byl v předešlém příkladu „rychlejší cestou k výsledku“. Pro roviny $\varrho_1$ a $\varrho_2$ tomu bude nepochybně stejně. Druhá metoda ovšem dává body, ve kterých se vzdálenost realizuje (body, kde si jsou roviny nejblíže). Nalezněme proto s její pomocí takové body v případě rovin $\varrho_1, \varrho_2$. Označme

$$u_1 = (1,0,-1,0,0)\,, \qquad u_2 = (0,1,0,0,-1)\,,$$
$$v_1 = (1,1,1,0,1)\,, \qquad v_2 = (0,-2,0,0,3)\,.$$

Body $X_1 \in \varrho_1$, $X_2 \in \varrho_2$, ve kterých se vzdálenost rovin realizuje, můžeme vyjádřit jako

$$X_1 = [7,2,7,-1,1] + t_1u_1 + s_1u_2,$$
$$X_2 = [2,4,7,-4,2] + t_2v_1 + s_2v_2,$$

a tedy

$$X_1 - X_2 = [7,2,7,-1,1] - [2,4,7,-4,2] + \\ + t_1u_1 + s_1u_2 - t_2v_1 - s_2v_2 = \\ = (5,-2,0,3,-1) + t_1u_1 + s_1u_2 - t_2v_1 - s_2v_2.$$

Při $v = u$ dostáváme ovšem přesně $\|\varphi(v)\|^2 = \lambda_1^2\|v\|^2 = \lambda^2$ a tedy odchylka dosahuje pro tento vektor minimální možné hodnoty. Tím je věta dokázána. □

**4.22. Počítání objemu.** S náznakem počítání objemu jsme se již



setkali v rovinné geometrii v konci páté části první kapitoly (viz 1.34). Zjistili jsme přitom, že podstatným pojmem je přitom tzv. orientace, kterou jsme si mohli představit jako rozhodnutí, zda se na naši rovinu $\mathbb{R}^2$ díváme shora či zezdola. Rozdíl je přitom v pořadí standardních bázových vektorů $e_1$ a $e_2$ na jednotkové kružnici. Stejně postupujeme obecně:

ORIENTACE VEKTOROVÉHO PROSTORU

Říkáme, že dvě báze $\underline{u}$ a $\underline{v}$ reálného vektorového prostoru $V$ určují stejnou *orientaci*, jestliže má matice přechodu mezi nimi kladný determinant. Formálněji vzato, orientací reálného vektorového prostoru $V$ tedy rozumíme třídu ekvivalence bází $\underline{u}$ vzhledem k ekvivalenci, kterou jsme pomocí znaménka determinantu právě zavedli. Ekvivalentním bazím v tomto smyslu také říkáme souhlasné se zvolenou orientací.

Přímo z definice pak vyplývá, že na každém vektorovém prostoru jsou právě dvě orientace. Z každé souhlasné báze získáme snadno nesouhlasnou pomocí libovolné matice přechodu se záporným determinantem.

Vektorový prostor se zvolenou orientací nazýváme *orientovaný vektorový prostor*.

*Orientovaný (bodový) euklidovský prostor* je euklidovský bodový prostor, jehož zaměření je orientované. V dalším budeme uvažovat standardní euklidovský prostor $\mathcal{E}_n$ spolu s orientací zadanou standardní bází $\mathbb{R}^n$.

Nechť $u_1, \ldots, u_k$, jsou libovolné vektory v zaměření $\mathbb{R}^n$, $A \in \mathcal{E}_n$ je libovolný bod. Rovnoběžnostěn $\mathcal{P}_k(A; u_1, \ldots, u_k) \subseteq \mathcal{E}_n$ jsme definovali jako příklad konvexní množiny

$$\mathcal{P}_k(A; u_1, \ldots, u_k) = \{A + c_1u_1 + \cdots + c_ku_k;\, 0 \le c_i \le 1\}.$$

Jsou-li vektory $u_1, \ldots, u_k$ nezávislé, hovoříme o $k$–rozměrném rovnoběžnostěnu $\mathcal{P}_k(A; u_1 \ldots, u_k) \subseteq \mathcal{E}_n$. Pro dané vektory $u_1, \ldots, u_k$ máme k dispozici také rovnoběžnostěny menších dimenzí

$$\mathcal{P}_1(A; u_1), \ldots, \mathcal{P}_k(A; u_1, \ldots, u_k)$$

v euklidovských podprostorech $A + \langle u_1\rangle, \ldots, A + \langle u_1, \ldots, u_k\rangle$.

Jsou-li $u_1, \ldots, u_k$ lineárně závislé, definujeme objem

$$\operatorname{Vol} P_k = 0.$$

Jinak uvažujeme jako při Gramově–Schmidtově ortogonalizaci

$$\langle u_1, \ldots, u_k\rangle = \langle u_1, \ldots, u_{k-1}\rangle \oplus \langle u_1, \ldots, u_{k-1}\rangle^\perp \cap \langle u_1, \ldots, u_k\rangle.$$

V tomto rozkladu se $u_k$ jednoznačně vyjádří jako

$$u_k = u_k' + e_k,$$

kde $e_k \perp \langle u_1, \ldots, u_{k-1}\rangle$.

Absolutní hodnotu objemu rovnoběžnostěnu definujeme



induktivně tak, abychom naplnili představu, že jde o součin objemu „základny“ a „výšky“:

$$|\operatorname{Vol}|\mathcal{P}_1(A; u_1) = \|u_1\|,$$
$$|\operatorname{Vol}|\mathcal{P}_k(A; u_1, \ldots, u_k) = \|e_k\|\,|\operatorname{Vol}|\mathcal{P}_{k-1}(A; u_1, \ldots, u_{k-1}).$$

Skalární součiny

$$\langle X_1 - X_2, u_1 \rangle = 0, \qquad \langle X_1 - X_2, u_2 \rangle = 0,$$
$$\langle X_1 - X_2, v_1 \rangle = 0, \qquad \langle X_1 - X_2, v_2 \rangle = 0$$

pak vedou na soustavu lineárních rovnic

$$\begin{array}{rrrrrrr} 2t_1 & & & & & = & -5, \\ & 2s_1 & & + & 5s_2 & = & 1, \\ & & - \ 4t_2 & - & s_2 & = & -2, \\ - & 5s_1 & - \ t_2 & - & 13s_2 & = & -1 \end{array}$$

s jediným řešením $t_1 = -5/2, s_1 = 41/2, t_2 = 5/2, s_2 = -8$. Získali jsem tak

$$X_1 = [7, 2, 7, -1, 1] - \frac{5}{2}u_1 + \frac{41}{2}u_2 = \left[\frac{9}{2}, \frac{45}{2}, \frac{19}{2}, -1, -\frac{39}{2}\right],$$
$$X_2 = [2, 4, 7, -4, 2] + \frac{5}{2}v_1 - 8v_2 = \left[\frac{9}{2}, \frac{45}{2}, \frac{19}{2}, -4, -\frac{39}{2}\right].$$

Nyní ji snadno ověříme, že vzdálenost bodů $X_1, X_2$ (a současně vzdálenost rovin $\varrho_1, \varrho_2$) je $|| X_1 - X_2 || = || (0, 0, 0, 3, 0) || = 3$. □

**4.24.** Najděte průnik kolmé roviny spuštěné z bodu $A = [1, 2, 3, 4] \in \mathbb{R}^4$ na rovinu

$$\varrho : [1, 0, 1, 0] + (1, 2, -1, -2)s + (1, 0, 0, 1)t, \quad s, t \in \mathbb{R}.$$

**Řešení.** Nalezněme nejprve kolmou rovinu k $\varrho$. Její zaměření bude kolmé na zaměření $\varrho$, pro vektory $(a, b, c, d)$ patřící do jejího zaměření dostáváme tedy soustavu rovnic

$$(a, b, c, d) \cdot (1, 2, -1, -2) = 0 \equiv a + 2b - c - 2d = 0,$$
$$(a, b, c, d) \cdot (1, 0, 0, 1) = 0 \equiv a + d = 0.$$

Jejím řešením je dvoudimenzionální vektorový prostor $\langle (0, 1, 2, 0), (-1, 0, -3, 1) \rangle$. Rovina $\tau$ kolmá k rovině $\varrho$ procházející bodem $A$ má tedy parametrické vyjádření

$$\tau : [1, 2, 3, 4] + (0, 1, 2, 0)u + (-1, 0, -3, 1)v, \quad u, v \in \mathbb{R}.$$

Průnik rovin potom můžeme získat pomocí obou parametrických vyjádření. Pro parametry popisující průnik tedy dostáváme soustavu rovnic

$$\begin{array}{rrrrrrrrr} 1 & + & s & + & t & = & 1 & - & v, \\ & & 2s & & & = & 2 & + \ u, & \\ 1 & - & s & & & = & 3 & + \ 2u & - \ 3v, \\ & - & 2s & + & t & = & 4 & + & v, \end{array}$$

která má jediné řešení (musí tomu tak být, protože sloupce matice soustavy jsou dány lineárně nezávislými vektory zaměření obou rovin) $s = -8/19, t = 34/19, u = -54/19, v = -26/19$. Dosazením hodnot parametrů $s$ a $t$ do parametrického vyjádření roviny $\varrho$ pak dostaneme souřadnice průniku $[45/19, -16/19, 11/19, 18/19]$

Je-li $u_1, \ldots, u_n$ báze souhlasná s orientací $V$, definujeme (orientovaný) objem rovnoběžnostěnu

$$\operatorname{Vol} \mathcal{P}_k(A; u_1, \ldots, u_n) = |\operatorname{Vol}| \mathcal{P}_k(A; u_1, \ldots, u_n),$$

v případě nesouhlasné báze klademe

$$\operatorname{Vol} \mathcal{P}_k(A; u_1, \ldots, u_n) = -|\operatorname{Vol}| \mathcal{P}_k(A; u_1, \ldots, u_n).$$

Následující tvrzení objasňuje naše dřívější poznámky, že determinant je v jistém smyslu nástroj vyjadřující objem. První tvrzení totiž říká právě, že na $k$–rozměrném prostoru dostaneme objem rovnoběžnostěnu nataženého na $k$ vektorů tak, že jejich souřadnice (v ortonormální bázi) napíšeme do sloupců matice a spočteme determinant.

Výrazu ve druhém tvrzení se říká *Gramův determinant*. Jeho výhoda je, že je zcela nezávislý na volbě báze a zejména se s ním proto lépe pracuje v případě $k$ menšího než je dimenze celého prostoru.



**Věta.** *Nechť $\mathcal{Q} \subseteq \mathcal{E}_n$ je euklidovský podprostor a nechť $(e_1, \ldots, e_k)$ je jeho ortonormální báze. Pak pro libovolné vektory $u_1, \ldots, u_k \in Z(\mathcal{Q})$ a $A \in \mathcal{Q}$ platí*

*(1)* $$\operatorname{Vol} \mathcal{P}_k(A; u_1, \ldots, u_k) = \begin{vmatrix} u_1 \cdot e_1 & \ldots & u_k \cdot e_1 \\ \vdots & & \vdots \\ u_1 \cdot e_k & \ldots & u_k \cdot e_k \end{vmatrix},$$

*(2)* $$(\operatorname{Vol} \mathcal{P}_k(A; u_1, \ldots, u_k))^2 = \begin{vmatrix} u_1 \cdot u_1 & \ldots & u_k \cdot u_1 \\ \vdots & & \vdots \\ u_1 \cdot u_k & \ldots & u_k \cdot u_k \end{vmatrix}$$

Důkaz. Matice

$$A = \begin{pmatrix} u_1 \cdot e_1 & \ldots & u_k \cdot e_1 \\ \vdots & & \vdots \\ u_1 \cdot e_k & \ldots & u_k \cdot e_k \end{pmatrix}$$

má ve sloupcích souřadnice vektorů $u_1, \ldots, u_k$ ve zvolené ortonormální bázi. Platí

$$|A|^2 = |A||A| = |A^T||A| = |A^T A| = \begin{vmatrix} u_1 \cdot u_1 & \ldots & u_k \cdot u_1 \\ \vdots & & \vdots \\ u_1 \cdot u_k & \ldots & u_k \cdot u_k \end{vmatrix}.$$

Vidíme tedy, že pokud platí (1), platí i (2).

Přímo z definice je neorientovaný objem roven součinu

$$|\operatorname{Vol}| \mathcal{P}_k(A; u_1, \ldots, u_k) = \|v_1\| \|v_2\| \ldots \|v_k\|,$$

kde $v_1 = u_1, v_2 = u_2 + a_1^2 v_1, \ldots, v_k = u_k + a_1^k v_1 + \cdots + a_{k-1}^k v_{k-1}$ je výsledek Gramova-Schmidtova ortogonalizačního procesu. Je tedy

$$(\operatorname{Vol} \mathcal{P}_k(A; u_1, \ldots, u_k))^2 = \begin{vmatrix} v_1 \cdot v_1 & 0 & \ldots & 0 \\ \vdots & \ddots & & \\ 0 & 0 & \ldots & v_k \cdot v_k \end{vmatrix} = \begin{vmatrix} v_1 \cdot v_1 & \ldots & v_k \cdot v_1 \\ \vdots & & \vdots \\ v_1 \cdot v_k & \ldots & v_k \cdot v_k \end{vmatrix}.$$

(stejný výsledek pochopitelně obdržíme, dosadíme-li hodnoty parametrů $u$ a $v$ do parametrického vyjádření roviny $\tau$). □

**4.25.** Nechť je dána krychle $ABCDEFGH$ (při obvyklém významu zápisu, tedy vektory $E-A, F-B, G-C, H-D$ jsou kolmé na rovinu určenou vrcholy $A$, $B$, $C$, $D$) v euklidovském prostoru $\mathbb{R}^3$. Vypočtěte odchylku $\varphi$ vektorů $F-A$ a $H-A$.

**Řešení.** Uvažované body $A$, $F$, $H$ jsou vrcholy trojúhelníku, jehož všechny strany jsou úhlopříčkami stěn krychle. Jedná se tudíž o rovnostranný trojúhelník. Odtud plyne, že $\varphi = \pi/3$. □

**4.26.** Označme $S$ střed hrany $AB$ krychle $ABCDEFGH$ (v obvyklém označení). Určete kosinus odchylky přímek $ES$ a $BG$.

**Řešení.** Vzhledem k tomu, že homotetie (stejnolehlost) je podobným zobrazením, tj. zachovává úhly, můžeme předpokládat, že krychle má hranu velikosti 1. Umístíme-li navíc bod $A$ do počátku souřadné soustavy a body $B$, resp. $E$ do bodů o souřadnicích $[1,0,0]$, resp. $[0,0,1]$, pak mají zbylé uvažované body následující souřadnice: $S = [1/2,0,0]$, $G = [1,1,1]$, tedy vektor $ES = (1/2,0,-1)$ a $BG = (0,1,1)$. Pro hledaný kosinus odchylky $\varphi$ tedy máme

$$\cos(\varphi) = \left| \frac{(1/2,0,-1)\cdot(0,1,1)}{\|(1/2,0,-1)\|\cdot\|(0,1,1)\|} \right| = \frac{\sqrt{2}}{\sqrt{5}}. \qquad \square$$

**4.27.** Určete odchylku přímky $p$ zadané implicitně rovnicemi

$$\begin{aligned} x &+ 3y &+ z &= 0,\\ -x &- y &+ z &= 0 \end{aligned}$$

od roviny $\varrho : x + y + 2z + 1 = 0$.

**Řešení.** Vidíme, že normálový vektor roviny $\varrho$ je $(1,1,2)$. Sečtení rovnic zadávajících přímku $p$ při opsání první z nich dává

$$\begin{aligned} x &+ 3y &+ z &= 0,\\ &2y &+ 2z &= 0. \end{aligned}$$

Odsud plyne, že $y = -z$ a $x = 2z$. Vektor $(2,-1,1)$ je proto směrovým vektorem přímky $p$; jinak řečeno, můžeme zapsat ($p$ očividně prochází počátkem)

$$p : [0,0,0] + t\,(2,-1,1)\,, \quad t \in \mathbb{R}.$$

Pro úhel $\varphi$ vektorů $(1,1,2)$, $(2,-1,1)$ platí

$$\cos\varphi = \frac{2-1+2}{\sqrt{6}\cdot\sqrt{6}} = \frac{1}{2}.$$

Je tedy $\varphi = 60\,^\circ$. To je ovšem velikost úhlu, který svírá směrový vektor $p$ s normálovým vektorem $\varrho$. Hledaný úhel je doplňkem tohoto úhlu, a tak je výsledek $30\,^\circ = 90\,^\circ - 60\,^\circ$. □



Označme $B$ matici jejíž sloupce jsou souřadnice vektorů $v_1, \ldots, v_k$ v ortonormální bázi $\underline{e}$. Protože $v_1, \ldots, v_k$ vznikly z $u_1, \ldots, u_k$ jako obrazy v lineární transformaci s horní trojúhelníkovou maticí $C$ s jedničkami na diagonále, je $B = CA$ a $|B| = |C||A| = |A|$. Pak ovšem $|A|^2 = |B|^2 = |A||A|$, proto $\mathrm{Vol}\,\mathcal{P}_k(A; u_1, \ldots, u_k) = \pm|A|$. Přitom pokud jsou vektory $u_1, \ldots, u_k$ závislé vyjde objem nulový, pokud jsou nezávislé, pak znaménko determinantu je kladné, právě když je báze $u_1, \ldots, u_k$ zadává stejnou orientací jako báze $\underline{e}$. □

V geometrické formulaci dostáváme jako velice důležitý důsledek následující tvrzení:

**4.23. Důsledek.** *Pro každé lineární zobrazení $\varphi : V \to V$ euklidovského vektorového prostoru $V$ je* $\det\varphi$ *roven (orientovanému) objemu obrazu rovnoběžnostěnu určeného vektory ortonormální báze. Obecněji, obraz rovnoběžnostěnu $\mathcal{P}$ určeného libovolnými* $\dim V$ *vektory má objem roven* $\det\varphi$*–násobku původního objemu.*

**4.24. Vnější a vektorový součin vektorů.** Předchozí úvahy úzce souvisí s tzv. vnějším tensorovým součinem vektorů. Nebudeme zacházet podrobně do této technicky poněkud nepřehledné oblasti, ale zmíníme alespoň případ vnějšího součinu $n = \dim V$ vektorů $u_1, \ldots, u_n \in V$.



Nechť $(u_{1j}, \ldots, u_{nj})^T$ jsou souřadná vyjádření vektorů $u_j$ v nějaké pevně zvolené ortonormální bázi $V$ a $M$ nechť je matice s prvky $(u_{ij})$. Pak determinant $|M|$ nezávisí na volbě báze a jeho hodnotu nazýváme *vnějším součinem vektorů* $u_1, \ldots, u_n$ a značíme $[u_1, \ldots, u_n]$. Vnější součin je tedy právě orientovaný objem příslušného rovnoběžnostěnu, viz 4.22.

Přímo z definice nyní vyplývají užitečné vlastnosti vnějšího součinu:

(1) Zobrazení $(u_1, \ldots, u_n) \mapsto [u_1, \ldots, u_n]$ je antisymetrické $n$–lineární zobrazení, tzn. že je lineární ve všech argumentech a výměna dvou argumentů se vždy projeví změnou znaménka výsledku.

(2) Vnější součin je nulový, právě když jsou vektory $u_1, \ldots, u_n$ lineárně závislé.

(3) Vektory $u_1, \ldots, u_n$ tvoří kladnou bázi, právě když je jejich vnější součin kladný.

V technických aplikacích v prostoru $\mathbb{R}^3$ se často používá velmi úzce související operace, tzv. vektorový součin, který dvojici vektorů přiřazuje vektor třetí.

Uvažme obecný euklidovský vektorový prostor $V$ dimenze $n \geq 2$ a vektory $u_1, \ldots, u_{n-1} \in V$. Dosadíme-li těchto $n-1$ vektorů jako prvních $n-1$ argumentů $n$–lineárního zobrazení definovaného pomocí determinantu při výpočtu objemu výše, pak nám zbude jeden volný argument, tj. lineární forma na $V$. Protože však máme k dispozici skalární součin, odpovídá každá lineární forma právě jednomu vektoru. Tento vektor $v \in V$ nazveme *vektorový součin* vektorů $u_1, \ldots, u_{n-1}$, tj. pro každý vektor $w \in V$ platí

$$\langle v, w\rangle = [u_1, \ldots, u_{n-1}, w].$$

Značíme $v = u_1 \times \ldots \times u_{n-1}$.

Jsou-li v nějaké ortonormální bázi souřadnice našich vektorů $v = (y_1, \ldots, y_n)^T$, $w = (x_1, \ldots, x_n)^T$ a $u_j = (u_{1j}, \ldots u_{nj})^T$,

**4.28.** V reálné rovině nalezněte přímku, která prochází bodem $[-3, 0]$ a s přímkou

$$p : \sqrt{3}x + 3y + 5 = 0$$

svírá úhel $60\,^\circ$.

**Řešení.** Nejprve si uvědomme, že podmínkám úlohy musí vyhovovat právě dvě přímky. Obecná rovnice přímky v rovině má tvar

$$ax + by + c = 0, \quad \text{přičemž lze volit} \quad a^2 + b^2 = 1.$$

Nalezněme tedy taková čísla $a, b, c \in \mathbb{R}$, aby byly splněny uvedené podmínky. Dosadíme-li $x = -3$, $y = 0$ do této rovnice (přímka má procházet bodem $[-3, 0]$), dostaneme $c = 3a$. Podmínka, že přímka má svírat úhel $60\,^\circ$ s přímkou $p$, potom dává

$$\frac{1}{2} = \cos 60\,^\circ = \frac{\left|\sqrt{3}a + 3b\right|}{\sqrt{12}}, \quad \text{tj.} \quad \sqrt{3} = \left|\sqrt{3}a + 3b\right|.$$

Další úpravou obdržíme

$$\pm 1 = a + \sqrt{3}b \quad \text{a umocněním} \quad 1 = a^2 + 3b^2 + 2\sqrt{3}ab.$$

Využijeme-li $a^2 + b^2 = 1$, získáme

$$0 = 2b^2 + 2\sqrt{3}ab, \quad \text{tj.} \quad 0 = b\left(b + \sqrt{3}a\right).$$

Celkem tak máme možnosti (připomeňme, že $c = 3a$ a $a^2 + b^2 = 1$)

$$a = \pm 1,\ b = 0,\ c = \pm 3; \quad a = \pm\frac{1}{2},\ b = \mp\frac{\sqrt{3}}{2},\ c = \pm\frac{3}{2}.$$

Snadno se ověří, že těmito koeficienty určené přímky

$$x + 3 = 0, \qquad \frac{1}{2}x - \frac{\sqrt{3}}{2}y + \frac{3}{2} = 0$$

zadání skutečně vyhovují. □

Jiný přístup k řešení téhož problému jako v předchozím příkladě, ukazuje řešení příkladu následujícího:

**4.29.** Bodem $[1, 2] \in \mathbb{R}^2$ veďte přímku, která má odchylku $30°$ od přímky

$$p : [0, 1] + t(1, 1).$$

**Řešení.** Odchylka dvou přímek je dána úhlem, který svírají jejich směrové vektory. Stačí tedy najít směrový vektor $v$ hledané přímky. Ten získáme například rotací směrového vektoru přímky $p$ o $30°$. Matice rotace o $30°$ je

$$\begin{pmatrix} \cos 30° & -\sin 30° \\ \sin 30° & \cos 30° \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

Hledaný vektor $v$ je tedy

$$v = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} - \frac{1}{2} \\ \frac{\sqrt{3}}{2} + \frac{1}{2} \end{pmatrix}.$$

naše definice má vyjádření

$$y_1x_1 + \cdots + y_nx_n = \begin{vmatrix} u_{11} & \dots & u_{1(n-1)} & x_1 \\ \vdots & & \vdots & \vdots \\ u_{n1} & \dots & u_{n(n-1)} & x_n \end{vmatrix}.$$

Odtud je přímo vidět, že vektor $v$ je zadán jednoznačně a jeho souřadnice spočteme formálním rozvojem tohoto determinantu podle posledního sloupce. Zároveň jsou přímo z definice očekávatelné následující vlastnosti vektorového součinu:

**Věta.** *Pro vektorový součin $v = u_1 \times \ldots \times u_{n-1}$ platí*

*(1) $v \in \langle u_1, \ldots, u_{n-1}\rangle^\perp$,*
*(2) $v$ je nenulový vektor, právě když jsou vektory $u_1, \ldots, u_{n-1}$ lineárně nezávislé,*
*(3) velikost $\|v\|$ vektorového součinu je rovna absolutní hodnotě objemu rovnoběžnostěnu $\mathcal{P}(0; u_1, \ldots, u_{n-1})$,*
*(4) $(u_1, \ldots, u_{n-1}, v)$ je souhlasná báze orientovaného euklidovského prostoru $V$.*

Důkaz. První tvrzení plyne přímo z definičního vztahu pro $v$, protože dosazením libovolného vektoru $u_j$ za $w$ máme nalevo skalární součin $v \cdot u_j$ a napravo determinant s dvěma shodnými sloupci.



Hodnost matice s $n-1$ sloupci $u_j$ je dána maximální velikostí nenulového minoru. Minory, které zadávají souřadnice vektorového součinu jsou stupně $n-1$ a tím je dokázáno tvrzení (2).

Jsou-li vektory $u_1, \ldots, u_{n-1}$ závislé, pak platí i (3). Nechť jsou tedy nezávislé, $v$ je jejich vektorový součin a zvolme libovolnou ortonormální bázi $(e_1, \ldots, e_{n-1})$ prostoru $\langle u_1, \ldots, u_{n-1}\rangle$. Z již dokázaného vyplývá, že existuje nějaký násobek $(1/\alpha)v$, $0 \neq \alpha \in \mathbb{R}$, takový, že $(e_1, \ldots, e_k, (1/\alpha)v)$ je ortonormální báze celého $V$. Souřadnice našich vektorů v této bázi jsou

$$u_j = (u_{1j}, \ldots, u_{(n-1)j}, 0)^T, \quad v = (0, \ldots, 0, \alpha)^T.$$

Proto je vnější součin $[u_1, \ldots, u_{n-1}, v]$ roven (viz definice vektorového součinu)

$$[u_1, \ldots, u_{n-1}, v] = \begin{vmatrix} u_{11} & \dots & u_{1(n-1)} & 0 \\ \vdots & & \vdots & \vdots \\ u_{(n-1)1} & \dots & u_{(n-1)(n-1)} & 0 \\ 0 & \dots & 0 & \alpha \end{vmatrix} =$$

$$= \langle v, v\rangle = \alpha^2.$$

Rozvojem determinantu podle posledního sloupce zároveň obdržíme

$$\alpha^2 = \alpha \operatorname{Vol}\mathcal{P}(0; u_1, \ldots, i_{n-1}).$$

Odtud už vyplývají obě zbylá tvrzení věty. □

**4.25. Afinní a euklidovské vlastnosti.** Nyní se můžeme zamyslet nad tím, které vlastnosti jsou vlastní už afinním prostorům a zobrazením a na co skutečně teprve potřebujeme v zaměření skalární součin.



Je samozřejmé, že všechny euklidovské transformace, tj. bijektivní afinní zobrazení euklidovských prostorů, které zachovává vzdálenosti bodů, zachovávají všechny výše studované objekty. Tj. zachovávají kromě vzdáleností také neorientované úhly, neorientované objemy, odchylky podprostorů apod. Pokud chceme, aby zachovávaly i orientované úhly, vektorové součiny, objemy, pak musíme navíc předpokládat, že naše transformace zachovávají orientaci.

Rotovat jsme mohli i v opačném smyslu. Hledaná přímka (jedna ze dvou možných) má tedy parametrické vyjádření

$$[1,2]+\left(\tfrac{\sqrt{3}}{2}-\tfrac{1}{2},\tfrac{\sqrt{3}}{2}+\tfrac{1}{2}\right)t. \qquad \square$$

*4.30.* Určete obecnou rovnici všech rovin, které svírají odchylku 60° s rovinou $x+y+z-1=0$ a obsahují přímku $p:\ [1,0,0]+t\,(1,1,0)$. ○

**4.31.** Určete odchylku rovin

$$\sigma:\qquad [1,0,2]+(1,-1,1)t+(0,1,-2)s,$$
$$\rho:\qquad [3,3,3]+(1,-2,0)t+(0,1,1)s.$$

**Řešení.** Průsečnice má směrový vektor $(1,-1,1)$, kolmá rovina na ni má pak s danými rovinami průniky generované vektory $(1,0,-1)$ a $(0,1,1)$. Tyto jednorozměrné podprostory svírají úhel 60°. □

**4.32.** Je dána krychle $ABCDA'B'C'D'$ (ve standardním označení, tj. $ABCD$ a $A'B'C'D'$ jsou stěny, $AA'$ pak hrana). Určete odchylku vektorů $AB'$ a $AD'$.

**Řešení.** Uvažujme krychli o hraně 1 a umístěme ji v $\mathbb{R}^3$ tak, že bod $A$ bude mít ve standardní bázi souřadnice $[0,0,0]$, bod $B$ pak souřadnice $[1,0,0]$ a bod $C$ souřadnice $[1,1,0]$. Potom má bod $B'$ souřadnice $[1,0,1]$ a bod $D'$ souřadnice $[0,1,1]$. Pro vyšetřované vektory tedy můžeme psát $AB'=B'-A=[1,0,1]-[0,0,0]=(1,0,1)$, $AD'=D'-A=[0,1,1]-[0,0,0]=(0,1,1)$. Podle definice odchylky $\varphi$ těchto vektorů je pak

$$\cos(\varphi)=\frac{(1,0,1)\cdot(0,1,1)}{\|\,(1,0,1)\,\|\cdot\|\,(0,1,1)\,\|}=\frac{1}{2},$$

tedy $\varphi=60°$. □

Další příklady na odchylky viz ‖4.76‖.

**4.33.** Určete $\cos\alpha$, kde $\alpha$ je odchylka dvou sousedních stěn pravidelného osmistěnu (těleso, jehož stěny tvoří osm rovnostranných trojúhelníků).

**Řešení.** Odchylky libovolných dvou sousedních stěn jsou ze symetrie osmistěnu shodné. Rovněž tak nezáleží na jeho velikosti. Uvažujme osmistěn s délkou hrany 1, který je umístěn do standardní kartézské souřadné soustavy v $\mathbb{R}^3$ tak, že jeho těžiště je v bodě $[0,0,0]$. Jeho vrcholy jsou pak v bodech $A=\left[\frac{\sqrt{2}}{2},0,0\right]$, $B=\left[0,\frac{\sqrt{2}}{2},0\right]$, $C=\left[-\frac{\sqrt{2}}{2},0,0\right]$, $D=\left[0,-\frac{\sqrt{2}}{2},0\right]$, $E=\left[0,0,-\frac{\sqrt{2}}{2}\right]$ a $F=\left[0,0,\frac{\sqrt{2}}{2}\right]$.

Určeme odchylku stěn $CDF$ a $BCF$. Ta je dána odchylkou vektorů kolmých na jejich průnik a ležících v daných stěnách, tedy vektorů kolmých na $CF$. Těmi jsou vektory dané výškami z bodů $D$, resp.

Naši otázku také můžeme přeformulovat takto: *Které koncepty euklidovské geometrie zůstávají zachovány při afinních transformacích?*

Připomeňme nejprve, že afinní transformace na $n$–rozměrném prostoru $\mathcal{A}$ je jednoznačně zadána zobrazením $n+1$ bodů v obecné poloze, tj. zobrazením jednoho $n$–rozměrného simplexu. V rovině to znamená volbu obrazu jediného (nedegenerovaného) trojúhelníku, který ale můžeme zobrazit na jakýkoliv (nedegenerovaný) trojúhelník. Zachovány přitom zůstanou zejména příslušnosti k podprostorům, tj. vlastnosti typu „přímka prochází bodem“ nebo „rovina obsahuje přímku“ apod. Zároveň zůstává zachována kolinearita vektorů a pro každé dva kolineární vektory zůstává samozřejmě zachován poměr jejich velikostí (a to nezávisle, jakým skalárním součinem jejich velikost definujeme). Stejně jsme již viděli, že poměr objemů dvou $n$-rozměrných rovnoběžnostěnů zůstane po transformaci zachován (protože se zobrazením změní o stejný násobek determinantem příslušné matice).

V rovině lze tyto afinní vlastnosti velmi elegantně používat k důkazům geometrických tvrzení. Např. skutečnost, že se těžnice trojúhelníku všechny protínají v jednom bodě a zároveň v jedné třetině svých délek stačí ověřit na pravoúhlém rovnoramenném trojúhelníku nebo pouze na rovnostranném trojúhelníku a odtud už nutně vlastnost vyplývá pro všechny trojúhelníky. Promyslete si tuto argumentaci podrobně!

### 2. Geometrie kvadratických forem



V analytické geometrii roviny jsou po přímkách jako další nejjednodušší křivky na řadě tzv. kuželosečky. Jsou v kartézských souřadnicích zadány kvadratickými rovnicemi a podle koeficientů poznáme, zda jde o kružnici, elipsu, parabolu nebo hyperbolu, případně ještě může jít o dvě přímky nebo bod (degenerované případy).

Uvidíme, že naše nástroje umožní vcelku účinnou klasifikaci takovýchto objektů v libovolných konečných dimenzích i práci s nimi. Je přitom zřejmé, že v afinní geometrii nemůžeme odlišit kružnici od elipsy, proto začneme v geometrii euklidovské.

**4.26. Kvadriky v $\mathcal{E}_n$.** V analogii k rovnicím kuželoseček v rovině začneme poznámkami o objektech v euklidovských bodových prostorech, které jsou v dané ortonormální bázi zadány kvadratickými rovnicemi, hovoříme o *kvadrikách.*



Zvolme v $\mathcal{E}_n$ pevně kartézskou souřadnou soustavu (tj. bod a ortonormální bázi zaměření) a uvažme obecnou kvadratickou rovnici pro souřadnice $(x_1,\dots,x_n)^T$ bodů $A\in\mathcal{E}_n$

$$\sum_{i,j=1}^{n} a_{ij}x_ix_j+\sum_{i=1}^{n}2a_ix_i+a=0, \tag{4.4}$$

kde bez újmy na obecnosti můžeme rovnou předpokládat symetrii $a_{ij}=a_{ji}$. Tuto rovnici můžeme zapsat jako

$$f(u)+g(u)+a=0$$

pro kvadratickou formu $f$ (tj. zúžení symetrické bilineární formy $F$ na dvojice stejných argumentů), lineární formu $g$ a skalár $a\in\mathbb{R}$ a předpokládáme že alespoň jeden z koeficientů $a_{ij}$ je nenulový

$F$ na stranu $CF$ v trojúhelnících $CDF$, resp. $BCF$. Výšky v rovnostranném trojúhelníku splývají s těžnicemi, jedná se tedy o úsečky $SD$ a $SB$, kde $S$ je střed strany $CF$. Protože známe souřadnice bodů $C$ a $F$, má bod $S$ souřadnice $\left[-\frac{\sqrt{2}}{4}, 0, \frac{\sqrt{2}}{4}\right]$ a pro vektory máme $SD = \left(\frac{\sqrt{2}}{4}, -\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4}\right)$ a $SB = \left(\frac{\sqrt{2}}{4}, \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4}\right)$. Celkem

$$\cos\alpha = \frac{\left(\frac{\sqrt{2}}{4}, -\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4}\right) \cdot \left(\frac{\sqrt{2}}{4}, \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4}\right)}{\left\|\left(\frac{\sqrt{2}}{4}, -\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4}\right)\right\| \cdot \left\|\left(\frac{\sqrt{2}}{4}, \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4}\right)\right\|} = -\frac{1}{3}.$$

Je tedy $\alpha \doteq 132°$. □

**4.34.** Nyní ukážeme jednoduché využití Cauchyovy nerovnosti. Dokažte, že pro každé $n \in \mathbb{N}$ a pro libovolná kladná čísla $x_1, x_2, \ldots, x_n \in \mathbb{R}$ platí

$$n^2 \leq \left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}\right) \cdot (x_1 + x_2 + \cdots + x_n)\,.$$

Poté uveďte, kdy nastává rovnost.

**Řešení.** Postačuje uvážit Cauchyovu nerovnost

$$|\,u \cdot v\,| \leq ||\,u\,||\,||\,v\,||$$

v euklidovském prostoru $\mathbb{R}^n$ pro vektory

$$u = \left(\frac{1}{\sqrt{x_1}}, \frac{1}{\sqrt{x_2}}, \ldots, \frac{1}{\sqrt{x_n}}\right), \quad v = \left(\sqrt{x_1}, \sqrt{x_2}, \ldots, \sqrt{x_n}\right).$$

Takto dostaneme

$$n \leq \sqrt{\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}} \cdot \sqrt{x_1 + x_2 + \cdots + x_n}. \tag{4.1}$$

Dokazovanou nerovnost potom obdržíme umocněním (‖4.1‖). Dále víme, že Cauchyova nerovnost přejde v rovnost, právě když bude vektor $u$ násobkem vektoru $v$, což již implikuje $x_1 = x_2 = \cdots = x_n$.

□

**4.35.** Spočtěte objem rovnoběžnostěnu v $\mathbb{R}^3$ s podstavou v rovině $z = 0$ a s hranami zadanými dvojicemi vrcholů $[0, 0, 0]$, $[-2, 3, 0]$; $[0, 0, 0]$, $[4, 1, 0]$ a $[0, 0, 0]$, $[5, 7, 3]$.

**Řešení.** Rovnoběžnostěn je zadán vektory $(4, 1, 0)$, $(-2, 3, 0)$, $(5, 7, 3)$. Víme, že jeho objem je roven determinantu

$$\begin{vmatrix} 4 & -2 & 5 \\ 1 & 3 & 7 \\ 0 & 0 & 3 \end{vmatrix} = 3 \begin{vmatrix} 4 & -2 \\ 1 & 3 \end{vmatrix} = 3 \cdot 14 = 42.$$

Doplňme, že při změnách pořadí vektorů bychom obdrželi výsledek $\pm 42$, neboť determinant udává *orientovaný* objem rovnoběžnostěnu. Ještě poznamenejme, že objem rovnoběžnostěnu by se dle výpočtu determinantu nezměnil, pokud by třetí vektor byl $[a, b, 3]$ pro libovolná čísla $a, b \in \mathbb{R}$. Jeho objem pochopitelně závisí pouze (jinak by se jednalo o lineární rovnici popisující euklidovský podprostor).

Všimněme si také, že jakákoliv euklidovská (nebo i afinní) transformace souřadnic převede rovnici (4.4) opět na stejný tvar s kvadratickou, lineární a konstantní částí.

**4.27. Kvadratické formy.** Začněme naši diskusi rovnice (4.4) její kvadratickou částí, tj. bilineární symetrickou formou $F : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$. Stejně dobře můžeme přemýšlet o obecné symetrické bilineární formě na libovolném vektorovém prostoru.

Pro libovolnou bázi na tomto vektorovém prostoru bude hodnota $f(x)$ na vektoru $x = x_1 e_1 + \cdots + x_n e_n$ dána vztahem

$$f(x) = F(x, x) = \sum_{i,j} x_i x_j F(e_i, e_j) = x^T \cdot A \cdot x,$$

kde $A = (a_{ij})$ je symetrická matice s prvky $a_{ij} = F(e_i, e_j)$. Takovýmto zobrazením $f$ říkáme *kvadratické formy* a výše uvedený vzorec pro hodnotu formy s použitím zvolených souřadnic se nazývá *analytický tvar* formy.

Obecně rozumíme kvadratickou formou zúžení $f(x)$ jakékoliv symetrické bilineární formy $F(x, y)$ na argumenty tvaru $(x, x)$. Evidentně umíme z hodnot $f(x)$ zrekonstruovat celou bilineární formu $F$, protože

$$f(x + y) = F(x + y, x + y) = f(x) + f(y) + 2F(x, y).$$

Jestliže změníme bázi $e_i$ na jinou bázi $e'_1, \ldots, e'_n$, dostaneme pro stejný vektor jiné souřadnice $x = S \cdot x'$ (zde $S$ je příslušná matice přechodu) a tedy

$$f(x) = (S \cdot x')^T \cdot A \cdot (S \cdot x') = (x')^T \cdot (S^T \cdot A \cdot S) \cdot x'\,.$$

Předpokládejme opět, že je na našem vektorovém prostoru zadán skalární součin. Předchozí výpočet pak můžeme shrnout slovy, že matice bilineární formy $F$ a tedy i kvadratické formy $f$ se transformuje při změně souřadnic způsobem, který pro ortogonální změny souřadnic splývá s transformací matic zobrazení (skutečně, pak je $S^{-1} = S^T$). Tento výsledek můžeme interpretovat také jako následující pozorování:

**Tvrzení.** *Nechť $V$ je reálný vektorový prostor se skalárním součinem. Pak vztah*

$$\varphi \mapsto F, \quad F(u, u) = \langle \varphi(u), u \rangle$$

*zadává bijekci mezi symetrickými lineárními zobrazeními a kvadratickými formami na $V$.*



Důkaz. Skutečně, bilineární forma s pevně zadaným druhým argumentem je lineární formou $\alpha_u(\,) = F(\,, u)$ a v přítomnosti skalárního součinu je nutně dána vztahem $\alpha(u)(v) = v \cdot w$ pro vhodný vektor $w$. Klademe $\varphi(u) = w$. Přímo ze vztahu v souřadnicích výše pak vyplývá, že $\varphi$ je lineární zobrazení s maticí $A$. Je tedy samoadjungované.

Naopak, každé symetrické zobrazení $\varphi$ zadává vztahem $F(u, v) = \langle \varphi(u), v \rangle = \langle u, \varphi(v) \rangle$ symetrickou bilineární formu a jejím zúžením kvadratickou formu. □

Z tohoto tvrzení vyplývá okamžitý důsledek, že pro každou kvadratickou formu $f$ existuje ortonormální báze zaměření, ve které má $f$ diagonální matici (a diagonální hodnoty jsou jednoznačně určeny až na pořadí).

Díky ztotožnění kvadratických forem se zobrazeními můžeme také korektně zavést *hodnost kvadratické formy* jakožto hodnost

na kolmé vzdálenosti rovin dolní a horní podstavy a jejich obsahu

$$\begin{vmatrix} 4 & -2 \\ 1 & 3 \end{vmatrix} = 14. \qquad \square$$

**4.36.** V $\mathbb{R}^3$ je dán čtyřstěn $ABCD$, kde $A = [4, 0, 2]$, $B = [-2, -3, 1]$, $C = [1, -1, -3]$, $D = [2, 4, -2]$. Rozhodněte, zda leží bod $X = [0, -3, 0]$ uvnitř tohoto čtyřstěnu.

**Řešení.** Objem čtyřstěnu je šestina objemu rovnoběžnostěnu, jehož tři hrany z bodu $A$ jsou $B - A = (-6, -3, -1)$, $C - A = (-3, -1, -5)$ a $D - A = (-2, 4, -4)$ a ten je dán absolutní hodnotou determinantu

$$\begin{vmatrix} -6 & -3 & -1 \\ -3 & -1 & -5 \\ -2 & 4 & -4 \end{vmatrix} = -124.$$

Celkem je tedy objem čtyřstěnu $\frac{124}{6}$. $\square$

**4.37.** Je dán rovnoběžník $[0, 0, 1], [2, 1, 1], [3, 3, 1], [1, 2, 1]$. Určete bod $X$ na přímce $p : [0, 0, 1] + (1, 1, 1)t$ tak, aby rovnoběžnostěn určený daným rovnoběžníkem a bodem $X$ měl objem 1.

**Řešení.** Sestavíme determinant, jehož absolutní hodnota udává objem rovnoběžnostěnu při pohyblivém bodu $X$:

$$\begin{vmatrix} t & t & t \\ 2 & 1 & 0 \\ 1 & 2 & 0 \end{vmatrix} = 3t.$$

Požadujeme, aby byl roven 1, či $-1$, tedy $t = 1/3$ nebo $t = -1/3$. $\square$

**4.38.** Jsou dány vektory $\underline{u} = (u_1, u_2, u_3)$ a $\underline{v} = (v_1, v_2, v_3)$. Doplňte je třetím jednotkovým vektorem tak, aby rovnoběžnostěn daný těmito třemi vektory měl co největší objem.

**Řešení.** Označme hledaný jednotkový vektor jako $\underline{t} = (t_1, t_2, t_3)$. Podle 4.22 je objem rovnoběžnostěnu $\mathcal{P}_3(0; \underline{u}, \underline{v}, \underline{t})$ dán jako absolutní hodnota determinantu

$$\begin{vmatrix} u_1 & v_1 & t_1 \\ u_2 & v_2 & t_2 \\ u_3 & v_3 & t_3 \end{vmatrix} = \begin{vmatrix} t_1 & t_2 & t_3 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix} = \underline{t} \cdot (\underline{u} \times \underline{v}) \leq \|\underline{t}\| \|\underline{u} \times \underline{v}\| = \|\underline{u} \times \underline{v}\|.$$

Použité znaménko nerovnosti vyplývá z Cauchyovy nerovnosti, přičemž víme, že rovnost nastává právě pro $\underline{t} = c(\underline{u} \times \underline{v})$, $c \in \mathbb{R}$. Velikost objemu hledaného rovnoběžnostěnu tedy může být maximálně rovna velikosti obsahu rovnoběžníku daného vektory $\underline{u}, \underline{v}$ (tj. velikosti vektoru $(\underline{u} \times \underline{v})$). Rovnost nastane, právě když

$$\underline{t} = \pm \frac{(\underline{u} \times \underline{v})}{\|(\underline{u} \times \underline{v})\|}. \qquad \square$$

její matice v kterékoliv bázi (tj. hodnost je rovna dimenzi obrazu příslušného zobrazení $\varphi$).

**4.28. Klasifikace kvadrik.** Vraťme se k naší rovnici (4.4). Naše výsledky o kvadratických formách nám umožňují dosáhnout rovnice ve tvaru

$$\sum_{i=1}^{n} \lambda_i x_i^2 + \sum_{i=1}^{n} b_i x_i + b = 0.$$

Můžeme tedy přímo předpokládat, že ji v takovém tvaru máme a v dalším kroku pro souřadnice $x_i$ s $\lambda_i \neq 0$ provedeme doplnění do čtverců, které „pohltí“ kvadráty i lineární členy týchž neznámých (tzv. Lagrangeův algoritmus, kterému se budeme obecněji věnovat níže) . Tak nám zůstanou nejvýše ty neznámé, pro které byl jejich koeficient u kvadrátu nulový, a získáme tvar

$$\sum_{i=1}^{n} \lambda_i (x_i - p_i)^2 + \sum_{j \text{ splňující } \lambda_j = 0}^{n} b_j x_j + c = 0.$$

To odpovídá posunutí počátku souřadnic o vektor se souřadnicemi $p_i$ a zároveň volbě báze zaměření tak, abychom dostali požadovaný diagonální tvar v kvadratické části. Ve výše odvozeném ztotožnění forem se symetrickými zobrazeními to znamená, že $\varphi$ je diagonální na ortogonálním doplňku svého jádra. Pokud nám opravdu zůstaly nějaké lineární členy, můžeme upravit ortonormální bázi zaměření na jádru zobrazení $\varphi$ tak, aby odpovídající lineární forma byla násobkem prvního prvku duální báze. Umíme tedy již dosáhnout výsledného tvaru

$$\sum_{i=1}^{k} \lambda_i y_i^2 + b y_{k+1} + c = 0,$$

kde $k$ je hodnost matice kvadratické formy $f$. Pokud je $b \neq 0$, můžeme ještě další změnou počátku dosáhnout vynulování konstanty $c$ v rovnici.

Celkem si tedy shrňme, že lineární člen se může (ale nemusí) objevit jen pokud je hodnost $f$ menší než $n$, $c \in \mathbb{R}$ může být nenulové pouze když je $b = 0$. Výsledné rovnice nazýváme *kanonickými analytickými tvary* kvadrik.

**4.29. Případ $\mathcal{E}_2$.** Pro ilustraci předchozího postupu projděme celou diskusi ještě jednou pro nejjednodušší případ netriviální dimenze. Původní rovnice má tvar



$$a_{11}x^2 + a_{22}y^2 + 2a_{12}xy + a_1x + a_2y + a = 0.$$

Volbou vhodné báze zaměření a následným doplněním čtverců dosáhneme tvaru (opět používáme stejného značení $x, y$ pro nové souřadnice):

$$a_{11}x^2 + a_{22}y^2 + a_1x + a_2y + a = 0,$$

kde $a_i$ může být nenulové pouze v případě, že $a_{ii}$ je nulové. Posledním krokem obecného postupu, tj. v dimenzi $n = 2$ jen případnou volbou posunutí, dosáhneme právě jedné z rovnic:

### C. Geometrie kvadratických forem

**4.39.** Určete polární bázi formy:
$f : \mathbb{R}^3 \to \mathbb{R}$, $f(x_1, x_2, x_3) = 3x_1^2 + 2x_1x_2 + x_2^2 + 4x_2x_3 + 6x_3^2$.

**Řešení.** Její matice je

$$A = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 6 \end{pmatrix}.$$

Podle bodu (1) Lagrangeova algoritmu (viz věta 4.30) provedeme úpravy

$$\begin{aligned} f(x_1, x_2, x_3) &= \frac{1}{3}(3x_1 + x_2)^2 + \frac{2}{3}x_2^2 + 4x_2x_3 + 6x_3^2 = \\ &= \frac{1}{3}y_1^2 + \frac{3}{2}(\frac{2}{3}y_2 + 2y_3)^2 = \\ &= \frac{1}{3}z_1^2 + \frac{3}{2}z_2^2 \end{aligned}$$

a vidíme, že forma má hodnost 2 a matice přechodu do příslušné polární báze $\underline{w}$ se získá posbíráním provedených transformací:

$$z_3 = y_3 = x_3,\ z_2 = \frac{2}{3}y_2 + 2y_3 = \frac{2}{3}x_2 + 2x_3,\ z_1 = y_1 = 3x_1 + x_2,$$

tedy matice přechodu od standardní báze k polární bázi je

$$T = \begin{pmatrix} 3 & 1 & 0 \\ 0 & \frac{2}{3} & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Matici jsme získali tak, že jsme odvozené vyjádření souřadnic v polární bázi pomocí souřadnic ve standardní bázi napsali do řádků uvažované matice (čtenář si rozmyslí, že sloupce této matice jsou souřadnice vektorů standardní báze v polární bázi). Souřadnice vektorů polární báze pak snadno odečteme z matice $T^{-1}$ (jsou to její sloupce).

$$T^{-1} = \begin{pmatrix} \frac{1}{3} & -\frac{1}{2} & 1 \\ 0 & \frac{3}{2} & -3 \\ 0 & 0 & 1 \end{pmatrix},$$

hledaná polární báze tedy je $\left(\left(\frac{1}{3}, 0, 0\right), \left(-\frac{1}{2}, \frac{3}{2}, 0\right), (1, -3, 1)\right)$. □

**4.40.** Určete polární bázi formy:

$$f : \mathbb{R}^3 \to \mathbb{R}^3.\ f(x_1, x_2, x_3) = 2x_1x_3 + x_2^2.$$

**Řešení.** Matice dané formy je

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Hned v prvním kroku můžeme přehodit proměnné: $y_1 = x_2$, $y_2 = x_1$, $y_3 = x_3$. Aplikace bodu (1) Lagrangeova algoritmu je pak triviální (nejsou tu žádné společné členy), pro další krok ale nastane situace

| | |
|---|---|
| $0 = x^2/a^2 + y^2/b^2 + 1$ | prázdná množina |
| $0 = x^2/a^2 + y^2/b^2 - 1$ | elipsa |
| $0 = x^2/a^2 - y^2/b^2 - 1$ | hyperbola |
| $0 = x^2/a^2 - 2py$ | parabola |
| $0 = x^2/a^2 + y^2/b^2$ | bod |
| $0 = x^2/a^2 - y^2/b^2$ | dvě různoběžné přímky |
| $0 = x^2 - a^2$ | dvě rovnoběžné přímky |
| $0 = x^2$ | dvě splývající přímky |
| $0 = x^2 + a^2$ | prázdná množina |

Počátek kartézských souřadnic je *středem* zkoumané kuželosečky, nalezená ortonormální báze zaměření zadává směr *poloos*, výsledné koeficienty $a, b$ pak dávají velikosti poloos v nedegenerovaných směrech.

O typu kuželosečky můžeme rozhodnout i bez úpravy na některý z tvarů uvedený v seznamu 4.29. Jak již víme, každou kuželosečku můžeme napsat ve tvaru

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2a_{13}x + 2a_{23}y + a_{33} = 0.$$

Determinanty

$$\Delta = \det A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{32} & a_{33} \end{vmatrix}, \quad \delta = \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix}$$

jsou tzv. invarianty kuželosečky, což znamená, že se nemění při euklidovské transformaci souřadnic (rotace a posunutí) navíc různé typy kuželoseček mají různá znaménka těchto determinantů.

- $\Delta \neq 0$ vlastní (regulární) kuželosečky:
  elipsa pro $\delta > 0$, hyperbola pro $\delta < 0$ a parabola pro $\delta = 0$
  Aby šlo o reálnou elipsu, nikoliv imaginární, musí být navíc $(a_{11} + a_{22})\Delta < 0$.
- $\Delta = 0$ nevlastní kuželosečky (singulární, degenerované), přímky

Snadno se přesvědčíme, že znaménka, resp. nulovost, uvedených determinantů jsou skutečně invariantní vůči změně souřadnic. (Čtenář se může ještě k těmto úvahám vrátit po pročtení následující diskuse o projektivní geometrii, se tyto invarianty také úzce souvisí.)

Označme $X = \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$ a $A$ je matice kvadratické formy. Pak příslušná kuželosečka má tvar $X^T A X = 0$. Kuželosečku ve středovém základním tvaru dostaneme otočením a posunutím, tedy transformací do nových souřadnic $x'$, $y'$, pro které platí

$$\begin{aligned} x &= x' \cos\alpha - y' \sin\alpha + c_1, \\ y &= x' \sin\alpha + y' \cos\alpha + c_2, \end{aligned}$$

tedy maticově pro nové souřadnice $X' = \begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix}$ platí

$$X = \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha & c_1 \\ \sin\alpha & \cos\alpha & c_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = MX'. \tag{4.5}$$

z bodu (4). Zavedeme tedy transformaci $z_1 = y_1, z_2 = y_2, z_3 = y_3 - y_2$. Pak

$$f(x_1, x_2, x_3) = z_1^2 + 2z_2(z_3 + z_2) = z_1^2 + \frac{1}{2}(2z_2 + z_3)^2 - \frac{1}{2}z_3^2.$$

Celkem dostáváme $z_1 = y_1 = x_2, z_2 = y_2 = x_1, z_3 = y_3 - y_2 = x_3 - x_1$. Matice přechodu $T$ do příslušné polární báze je tedy

$$T = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix} \quad \text{a} \quad T^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix},$$

polární báze je tedy $((0, 1, 0),\ (1, 0, 1)\ (0, 1, 1))$. □

**4.41.** Nalezněte polární bázi kvadratické formy $f : \mathbb{R}^3 \to \mathbb{R}$, která je ve standardní bázi dána předpisem

$$f(x_1, x_2, x_3) = x_1x_2 + x_1x_3.$$

**Řešení.** Aplikací uvedeného Lagrangeova algoritmu dostáváme:

$f(x_1, x_2, x_3) = 2x_1x_2 + x_2x_3 =$

substituce podle bodu (4) algoritmu $y_2 = x_2 - x_1$, $y_1 = x_1$

$y_3 = x_3$:

$= 2x_1(x_1 + y_2) + (x_1 + y_2)x_3 = 2x_1^2 + 2x_1y_2 + x_1x_3 + y_2x_3 =$

$= \frac{1}{2}(2x_1 + y_2 + \frac{1}{2}x_3)^2 - \frac{1}{2}y_2^2 - \frac{1}{8}x_3^2 + y_2x_3 =$

substituce $y_1 = 2x_1 + y_2 + \frac{1}{2}x_3$:

$= \frac{1}{2}y_1^2 - \frac{1}{2}y_2^2 - \frac{1}{8}x_3^2 + y_2x_3 = \frac{1}{2}y_1^2 - 2(\frac{1}{2}y_2 - \frac{1}{2}x_3)^2 + \frac{3}{8}x_3^2 =$

substituce $y_3 = \frac{1}{2}y_2 - \frac{1}{2}x_3$:

$= \frac{1}{2}y_1^2 - 2y_3^2 + \frac{3}{8}x_3^2.$

V souřadnicích $y_1, y_3, x_3$ má tedy daná kvadratická forma diagonální tvar, to znamená že báze příslušná těmto souřadnicím je polární bází dané kvadratické formy. Pokud ji máme vyjádřit musíme získat matici přechodu od této polární báze ke standardní bázi. Z definice matice přechodu jsou pak její sloupce bázovými vektory polární bázi. Matici přechodu získáme tak, že buď vyjádříme staré proměnné $(x_1, x_2, x_3)$ pomocí nových proměnných $(y_1, y_3, x_3)$, nebo ekvivalentně vyjádříme nové proměnné pomocí starých (což jde jednodušeji), pak ale musíme spočítat inverzní matici.

Máme $y_1 = 2x_1 + y_2 + \frac{1}{2}x_3 = 2x_1 + (x_2 - x_1) + \frac{1}{2}x_3$ a $y_3 = \frac{1}{2}y_2 - \frac{1}{2}x_3 = -\frac{1}{2}x_1 + \frac{1}{2}x_3 - \frac{1}{2}x_3$. Matice přechodu od zvolené polární báze ke standardní bázi je

$$T = \begin{pmatrix} 2 & 1 & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}.$$

Dosazením vztahu $X = MX'$ do rovnice kuželosečky, pak dostáváme rovnici kuželosečky v nových souřadnicích, tj.

$$X^T AX = 0,$$
$$(MX')^T A(MX') = 0,$$
$$X'^T M^T A\, MX' = 0.$$

Označme $A'$ matici kvadratické formy kuželosečky v nových souřadnicích. Pak tedy $A' = M^T A\ M$, kde matice $M = \begin{pmatrix} \cos\alpha & -\sin\alpha & c_1 \\ \sin\alpha & \cos\alpha & c_2 \\ 0 & 0 & 1 \end{pmatrix}$ má jednotkový determinant, tedy

$$\det A' = \det M^T\ \det A\ \det M = \det A\ = \Delta.$$

Nutně také determinant $A_{33}$, který je algebraickým doplňkem prvku $a_{33}$ je nezávislý na změně souřadnic, protože pro nulové posunutí - tedy pouze otočení - je vztah $\det A' = \det M^T\ \det A\ \det M$ také platný. V tom případě matice $M = \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}$ a $\det A'_{33} = \det A_{33} = \delta$. Pro samotné posunutí je matice $M = \begin{pmatrix} 1 & 0 & c_1 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix}$ a tento subdeterminant neovlivňuje.



**4.30. Afinní pohled.** V předchozích dvou odstavcích jsme hledali podstatné vlastnosti a standardizované analytické popisy objektů zadávaných v euklidovských prostorech kvadratickými rovnicemi. Hledali jsme přitom co nejjednodušší rovnice v mezích daných volností výběru kartézských souřadnic. Geometrická formulace našeho výsledku pak může být taková, že pro dva různé objekty – kvadriky, zadané v obecně různých kartézských souřadnicích, existuje *euklidovská transformace* na $\mathcal{E}_n$ (tj. afinní bijektivní zobrazení zachovávající velikosti) tehdy a jen tehdy, pokud výše uvedený algoritmus vede na stejný analytický tvar, až na pořadí souřadnic. Navíc můžeme při našem postupu přímo získat kartézské souřadnice, ve kterých jsou naše objekty dány výslednými kanonickými tvary, a tím i explicitní vyjádření euklidovské transformace, která naše objekty na sebe převádí (jak víme bude vždy složena z operací posunutí, otočení a zrcadlení vůči nadrovině).

Pochopitelně se můžeme ptát, do jaké míry umíme podobnou věc v afinních prostorech s volností výběru jakékoliv afinní souřadné soustavy. Např. v rovině to bude znamenat, že neumíme rozlišit kružnici od elipsy, samozřejmě bychom přitom měli odlišit hyperbolu a všechny ostatní typy kuželoseček. Hlavně ale splynou mezi sebou všechny hyperboly atd.

Ukážeme si hlavní rozdíl postupu na kvadratických formách a k záležitosti se pak ještě vrátíme ve třetí části této kapitoly.

Uvažme nějakou kvadratickou formu $f$ na vektorovém prostoru $V$ a její analytické vyjádření $f(u) = x^T Ax$ vzhledem ke zvolené bázi na $V$. Pro vektor $u = x_1u_1 + \cdots + x_nu_n$ pak také zapisujeme formu $f$ ve tvaru

$$f(x_1, \ldots, x_n) = \sum_{ij} a_{ij}x_ix_j.$$

V předchozích odstavcích jsme již s využitím skalárního součinu ukázali, že pro vhodnou bázi bude matice $A$ diagonální, tj. že pro příslušnou symetrickou formu $F$ bude platit $F(u_i, u_j) = 0$ při

Pro inverzní matici pak máme

$$T^{-1}\begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & -\frac{1}{2} \\ \frac{1}{3} & \frac{4}{3} & \frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}.$$

Jedna z polárních bází dané kvadratické formy (polární báze není určena jednoznačně) je tedy například báze (je dána sloupci poslední matice) $((1/3, 1/3, 0), (-2/3, 4/3, 0), (-1/2, 1/2, 1))$. □

**4.42.** Určete typ kuželosečky dané rovnicí:

$$3x_1^2 - 3x_1x_2 + x_2 - 1 = 0.$$

**Řešení.** Pomocí algoritmu úpravy na čtverec postupně dostáváme:

$$\begin{aligned} 3x_1^2 - 3x_1x_2 + x_2 - 1 &= \frac{1}{3}\left(3x_1 - \frac{3}{2}x_2\right)^2 - \frac{3}{4}x_2^2 + x_2 - 1 = \\ &= \frac{1}{3}y_1^2 - \frac{4}{3}\left(\frac{3}{4}x_2 - \frac{1}{2}\right)^2 + \frac{1}{3} - 1 = \\ &= \frac{1}{2}y_1^2 - \frac{4}{3}y_2^2 - \frac{2}{3}. \end{aligned}$$

Podle seznamu kuželoseček 4.29 se tedy jedná o hyperbolu. □

**4.43.** Pomocí doplnění na čtverce vyjádřete kvadriku

$$-x^2 + 3y^2 + z^2 + 6xy - 4z = 0$$

ve tvaru, ze kterého lze vyčíst její typ.

**Řešení.** Všechny členy obsahující $x$ připojíme k $-x^2$ a provedeme doplnění na čtverec. Tím získáme

$$-(x - 3y)^2 + 9y^2 + 3y^2 + z^2 - 4z = 0.$$

Žádné „nežádoucí" členy obsahující $y$ nemáme, a proto postup opakujeme pro proměnnou $z$, což dává

$$-(x - 3y)^2 + 12y^2 + (z - 2)^2 - 4 = 0.$$

Odtud plyne, že existuje transformace proměnných, při které obdržíme (rovnici můžeme nejdříve vydělit 4) rovnici

$$-\bar{x}^2 + \bar{y}^2 + \bar{z}^2 - 1 = 0.$$ □

**4.44.** Určete typ kuželosečky $2x^2 - 2xy + 3y^2 - x + y - 1 = 0$.

**Řešení.** Determinant je $\Delta = \begin{vmatrix} 2 & -1 & -\frac{1}{2} \\ -1 & 3 & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & -1 \end{vmatrix} = -\frac{23}{4} \neq 0$. Jde tedy o regulární kuželosečku. Navíc je $\delta = 5 > 0$, tedy jde o elipsu. Dále $(a_{11} + a_{22})\Delta = (2 + 3) \cdot \left(-\frac{23}{4}\right) < 0$, jde tedy o reálnou elipsu. □

**4.45.** Určete typ kuželosečky $x^2 - 4xy - 5y^2 + 2x + 4y + 3 = 0$.

**Řešení.** Determinant je $\Delta = \begin{vmatrix} 1 & -2 & 1 \\ -2 & -5 & 2 \\ 1 & 2 & 3 \end{vmatrix} = -34 \neq 0$,

dále je $\delta = \begin{vmatrix} 1 & -2 \\ -2 & -5 \end{vmatrix} = -9 < 0$, jde tedy o hyperbolu. □

$i \neq j$. Každou takovou bázi nazýváme *polární báze* kvadratické formy $f$. Samozřejmě si pro takový účel můžeme vždy skalární součin vybrat. Dokážeme si ale toto tvrzení znovu bez využití skalárních součinů tak, že získáme daleko jednodušší algoritmus na to, jak takovou polární bázi najít mezi všemi bázemi. Tím se zároveň dovíme podstatné informace o afinních vlastnostech kvadratických forem. Následující věta bývá v literatuře uváděna pod názvem *Lagrangeův algoritmus*.

**Věta.** *Nechť $V$ je reálný vektorový prostor dimenze $n$, $f : V \to \mathbb{R}$ kvadratická forma. Pak na $V$ existuje polární báze pro $f$.*

Důkaz. (1) Nechť $A$ je matice $f$ v bázi $\underline{u} = (u_1, \ldots, u_n)$ na $V$ a předpokládejme $a_{11} \neq 0$. Pak můžeme psát

$$\begin{aligned} f(x_1, \ldots, x_n) &= a_{11}x_1^2 + 2a_{12}x_1x_2 + \cdots + a_{22}x_2^2 + \cdots = \\ &= a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n)^2 + \\ &\quad + \text{členy neobsahující } x_1. \end{aligned}$$

Provedeme tedy transformaci souřadnic (tj. změnu báze) tak, aby v nových souřadnicích bylo

$$x_1' = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n,\ x_2' = x_2, \ldots, x_n' = x_n.$$

To odpovídá nové bázi (spočtěte si jako cvičení příslušnou matici přechodu!)

$$v_1 = a_{11}^{-1}u_1,\ v_2 = u_2 - a_{11}^{-1}a_{12}u_1, \ldots, v_n = u_n - a_{11}^{-1}a_{1n}u_1$$

a tak, jak lze očekávat, v nové bázi bude příslušná symetrická bilineární forma splňovat $g(v_1, v_i) = 0$ pro všechny $i > 0$ (přepočtěte!). Má tedy $f$ v nových souřadnicích analytický tvar $a_{11}^{-1}x_1'^2 + h$, kde $h$ je kvadratická forma nezávislá na proměnné $x_1$.

Z technických důvodů bývá lepší zvolit v nové bázi $v_1 = u_1$, opět dostaneme výraz $f = f_1 + h$, kde $f_1$ závisí pouze na $x_1'$, zatímco v $h$ se $x_1'$ nevyskytuje. Přitom pak $g(v_1, v_1) = a_{11}$.

(2) Předpokládejme, že po provedení kroku (1) dostaneme pro $h$ matici (řádu o jedničku menšího) s koeficientem u $x_2'^2$ různým od nuly. Pak můžeme zopakovat přesně stejný postup a získáme vyjádření $f = f_1 + f_2 + h$, kde v $h$ vystupují pouze proměnné s indexem větším než dvě. Tak můžeme postupovat tak dlouho, až buď provedeme $n - 1$ kroků a získáme diagonální tvar, nebo v řekněme $i$-tém kroku bude prvek $a_{ii}$ právě získané matice nulový.

(3) Nastane-li poslední možnost, ale přitom existuje jiný prvek $a_{jj} \neq 0$ s $j > i$, pak stačí přehodit $i$-tý prvek báze s $j$-tým a pokračovat podle předešlého postupu.

(4) Předpokládejme, že jsme narazili na situaci $a_{jj} = 0$ pro všechny $j \geq i$. Pokud přitom neexistuje ani žádný jiný prvek $a_{jk} \neq 0$ s $j \geq i$, $k \geq i$, pak jsme již úplně hotovi, neboť jsme již dosáhli diagonální matici. Předpokládejme, že $a_{jk} \neq 0$. Použijeme pak transformaci $v_j = u_j + u_k$, ostatní vektory báze ponecháme (tj. $x_k' = x_k - x_j$, ostatní zůstávají). Pak $h(v_j, v_j) = h(u_j, u_j) + h(u_k, u_k) + 2h(u_k, u_j) = 2a_{jk} \neq 0$ a můžeme pokračovat podle postupu v (1). □

**4.31. Afinní klasifikace kvadratických forem.** Po výpočtu polární báze Lagrangeovým algoritmem můžeme ještě vylepšit bázové vektory pomocí násobení skalárem tak, aby v příslušném analytickém vyjádření naší formy vystupovaly v roli koeficientů u kvadrátů jednotlivých souřadnic pouze skaláry 1, $-1$ a 0. Následující *věta o setrvačnosti* říká navíc, že počet jedniček a mínus jedniček nezávisí



**4.46.** Určete rovnici kuželosečky (a poté její typ), která prochází body

$$[-2,-4],\quad [8,-4],\quad [0,-2]\,,\quad [0,-6]\,,\quad [6,-2]\,.$$

**Řešení.** Do obecné rovnice kuželosečky

$$a_{11}x^2+a_{22}y^2+2a_{12}xy+a_1x+a_2y+a=0$$

postupně dosadíme souřadnice zadaných bodů. Takto obdržíme soustavu

$$\begin{array}{rcrcrcrcrcl}
4a_{11} & + & 16a_{22} & + & 16a_{12} & - & 2a_1 & - & 4a_2 & + & a & = & 0,\\
64a_{11} & + & 16a_{22} & - & 64a_{12} & + & 8a_1 & - & 4a_2 & + & a & = & 0,\\
 & & 4a_{22} & & & & & - & 2a_2 & + & a & = & 0,\\
 & & 36a_{22} & & & & & - & 6a_2 & + & a & = & 0,\\
36a_{11} & + & 4a_{22} & - & 24a_{12} & + & 6a_1 & - & 2a_2 & + & a & = & 0.
\end{array}$$

V maticovém zápisu provedeme úpravy

$$\begin{pmatrix} 4 & 16 & 16 & -2 & -4 & 1\\ 64 & 16 & -64 & 8 & -4 & 1\\ 0 & 4 & 0 & 0 & -2 & 1\\ 0 & 36 & 0 & 0 & -6 & 1\\ 36 & 4 & -24 & 6 & -2 & 1 \end{pmatrix}\sim\dots$$

$$\dots\sim\begin{pmatrix} 4 & 16 & 16 & -2 & -4 & 1\\ 0 & 4 & 0 & 0 & -2 & 1\\ 0 & 0 & 64 & -8 & 12 & -9\\ 0 & 0 & 0 & 24 & -36 & 27\\ 0 & 0 & 0 & 0 & 3 & -2 \end{pmatrix}\sim\dots$$

$$\dots\sim\begin{pmatrix} 48 & 0 & 0 & 0 & 0 & -1\\ 0 & 12 & 0 & 0 & 0 & -1\\ 0 & 0 & 64 & 0 & 0 & 0\\ 0 & 0 & 0 & 24 & 0 & 3\\ 0 & 0 & 0 & 0 & 3 & -2 \end{pmatrix}.$$

Hodnotu $a$ můžeme zvolit. Zvolíme-li $a=48$, dostaneme

$$a_{11}=1,\quad a_{22}=4,\quad a_{12}=0,\quad a_1=-6,\quad a_2=32.$$

Kuželosečka má tudíž rovnici

$$x^2+4y^2-6x+32y+48=0.$$

V této rovnici doplníme výrazy $x^2-6x$, $4y^2+32y$ na druhé mocniny dvojčlenů, což dává

$$(x-3)^2+4(y+4)^2-25=0,$$

resp.

$$\frac{(x-3)^2}{5^2}+\frac{(y+4)^2}{\left(\frac{5}{2}\right)^2}-1=0.$$

Vidíme, že se jedná o elipsu se středem v bodě $[3,-4]$. □

na našich volbách v průběhu algoritmu. Tyto počty nazýváme *signaturou kvadratické formy*. Opět tedy dostáváme úplný popis kvadratických forem ve smyslu, že dvě takové formy jsou převoditelná jedna na druhou pomocí afinní transformace tehdy a jen tehdy, když mají stejnou signaturu.

**Věta.** *Pro každou nenulovou kvadratickou formu hodnosti $r$ na reálném vektorovém prostoru $V$ existuje celé číslo $0\le p\le r$ a $r$ nezávislých lineárních forem $\varphi_1,\dots,\varphi_r\in V^*$ takových, že*

$$f(u)=(\varphi_1(u))^2+\dots+(\varphi_p(u))^2-(\varphi_{p+1}(u))^2-\dots-(\varphi_r(u))^2.$$

*Jinak řečeno, existuje polární báze, ve které má $f$ analytické vyjádření*

$$f(x_1,\dots,x_n)=x_1^2+\dots+x_p^2-x_{p+1}^2-\dots-x_r^2.$$

*Počet $p$ kladných diagonálních koeficientů v matici dané kvadratické formy (a tedy i počet $r-p$ záporných koeficientů) nezávisí na volbě polární báze.*

*Dvě symetrické matice $A$, $B$ dimenze $n$ jsou maticemi téže kvadratické formy v různých bázích, právě když mají stejnou hodnost a když matice příslušných forem v polární bázi mají stejný počet kladných koeficientů.*

Důkaz. Lagrangeovým algoritmem obdržíme $f(x_1,\dots,x_n)=\lambda_1x_1^2+\dots+\lambda_rx_r^2$, $\lambda_i\neq0$, v jisté bázi na $V$. Předpokládejme navíc, že právě prvních $p$ koeficientů $\lambda_i$ je kladných. Pak transformace $y_1=\sqrt{\lambda_1}x_1,\dots,y_p=\sqrt{\lambda_p}x_p$, $y_{p+1}=\sqrt{-\lambda_{p+1}}x_{p+1},\dots,y_r=\sqrt{-\lambda_r}x_r$, $y_{r+1}=x_{r+1},\dots,y_n=x_n$ již vede na požadovaný tvar. Formy $\varphi_i$ pak jsou právě formy z duální báze ve $V^*$ k získané polární bázi. Musíme ale ještě ukázat, že $p$ nezávisí na našem postupu. Předpokládejme, že se nám podařilo najít vyjádření téže formy $f$ v polárních bázích $\underline{u}$, $\underline{v}$, tj.

$$f(x_1,\dots,x_n)=x_1^2+\dots+x_p^2-x_{p+1}^2-\dots-x_r^2,$$
$$f(y_1,\dots,y_n)=y_1^2+\dots+y_q^2-y_{q+1}^2-\dots-y_r^2$$

a označme podprostor generovaný prvními $p$ vektory prvé báze $P=\langle u_1,\dots,u_p\rangle$, a obdobně $Q=\langle v_{q+1},\dots,v_n\rangle$. Pak pro každý $u\in P$ je $f(u)>0$ zatímco pro $v\in Q$ je $f(v)\le0$. Nutně tedy platí $P\cap Q=\{0\}$, a proto $\dim P+\dim Q\le n$. Odtud plyne $p+(n-q)\le n$, tj. $p\le q$. Opačnou volbou podprostorů však získáme i $q\le p$.

Je tedy $p$ nezávislé na volbě polární báze. Pak ovšem pro dvě matice se stejnou hodností a stejným počtem kladných koeficientů v diagonálním tvaru příslušné kvadratické formy získáme stejný analytický tvar. □

Při diskusi symetrických zobrazení jsme hovořili o definitních a semidefinitních zobrazeních. Tatáž diskuse má jasný smysl i pro symetrické bilineární formy a kvadratické formy. Kvadratickou formu $f$ forma na reálném vektorovém prostoru $V$ nazýváme

(1) *pozitivně definitní*, je-li $f(u)>0$ pro všechny vektory $u\neq0$,
(2) *pozitivně semidefinitní*, je-li $f(u)\ge0$ pro všechny vektory $u\in V$,
(3) *negativně definitní*, je-li $f(u)<0$ pro všechny vektory $u\neq0$,
(4) *negativně semidefinitní*, je-li $f(u)\le0$ pro všechny vektory $u\in V$,
(5) *indefinitní*, je-li $f(u)>0$ a $f(v)<0$ pro vhodné vektory $u,v\in V$.

**4.47. Další charakteristiky kuželoseček.** Zabývejme se ještě podrobněji některými dalšími pojmy, které se pojí s kuželosečkami. *Osa kuželosečky* je přímka, podle které je kuželosečka osově souměrná. Z kanonického vyjádření kuželosečky v polární bázi (4.29) plyne, že elipsa má dvě osy ($x = 0$ a $y = 0$), parabola má jenu osu ($x = 0$) a hyperbola má dvě osy ($x = 0$ a $y = 0$). Průniky os se samotnou kuželosečkou se nazývají *vrcholy kuželosečky*. Čísla $a, b$ z kanonického vyjádření kuželosečky (které udávají vzdálenost vrcholů od počátku) se nazývají *délky poloos*. V případě elipsy a hyperboly se osy navzájem protínají v počátku. Podle tohoto bodu je pak kuželosečka zřejmě středově souměrná. Takový bod se nazývá *středem kuželosečky*. Kromě vrcholů a středů existují ještě další význačné body ležící na ose kuželosečky. Pro elipsu jsou to *ohniska elipsy* $E, F$ charakterizované vlastností $|EX| + |FX| = 2a$ pro libovolný bod $X$ ležící na elipse. Následující příklad ukazuje, že takové body $E$ a $F$ skutečně existují.

**4.48. Existence ohnisek.** Pro elipsu o velikostech poloos $a > b$ jsou body $E = [-e, 0]$ a $F = [e, 0]$, kde $e = \sqrt{a^2 - b^2}$ jejími ohnisky (v polárních souřadnicích).

**Řešení.** Uvažujme body $X = [x, y]$, které splňují podmínku $|EX| + |FX| = 2a$ a ukážeme, že to jsou právě body elipsy. V souřadnicích má tato rovnice tvar

$$\sqrt{(x+e)^2 + y^2} + \sqrt{(x-e)^2 + y^2} = 2a.$$

Umocněním rovnice a její úpravou dostaneme ekvivalentní rovnici

$$(a^2 - e^2)x^2 + a^2y^2 = a^2(a^2 - e^2).$$

Dosazením $e^2 = a^2 - b^2$ a vydělením $a^2b^2$ dostaneme kanonickou rovnici elipsy

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1. \qquad \square$$

**Poznámka.** Číslo $e$ z předchozího příkladu se nazývá *excentricita (výstřednost)* elipsy. Podobně definujeme *ohniska hyperboly* jako body $E, F$, které splňují $||EX| - |FX|| = 2a$ pro libovolný bod $X$ ležící na hyperbole. Můžete si ověřit, že tuto vlastnost splňují v polární bázi body $[-e, 0]$ a $[e, 0]$, kde $e = \sqrt{a^2 + b^2}$. *Ohnisko paraboly* je bod $F$, který má v polární bázi souřadnice $F = \left[0, \frac{p}{2}\right]$ a je charakterizován tím, že jeho vzdálenost od libovolného bodu $X$ paraboly je stejná jako jako vzdálenost $X$ od přímky $y = -\frac{p}{2}$.

**4.49.** Určete ohniska elipsy $x^2 + 2y^2 = 2$.

**Řešení.** Z rovnice přímo odečteme, že velikosti poloos jsou $a = \sqrt{2}$ a $b = 1$. Poté již snadno dopočítáme z předchozího příkladu (‖4.48‖): $e = \sqrt{a^2 - b^2} = 1$, souřadnice ohnisek jsou tedy $[-1, 0]$ a $[1, 0]$. $\square$

Stejné názvy používáme i pro symetrické reálné matice, jsou-li maticemi patřičných kvadratických forem. Signaturou symetrické matice pak rozumíme signaturu příslušné kvadratické formy.

**4.32. Věta** (Sylvestrovo kritérium)**.** *Symetrická reálná matice $A$ je pozitivně definitní, právě když jsou všechny její vedoucí hlavní minory kladné.*

*Symetrická reálná matice $A$ je negativně definitní, právě když $(-1)^i|A_i| > 0$ pro všechny vedoucí hlavní submatice $A_i$.*

Důkaz.  Budeme si muset podrobněji rozebrat, jak vypadají transformace použité v Lagrangeově algoritmu pro konstrukci polární báze. Transformace použité v prvním kroku tohoto algoritmu mají vždy horní trojúhelníkovou matici $T$ a navíc, při použití technické modifikace zmíněné v důkazu věty 4.30, má tato matice jedničky na diagonále:

$$T = \begin{pmatrix} 1 & -\frac{a_{12}}{a_{11}} & \dots & -\frac{a_{n2}}{a_{11}} \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \end{pmatrix}.$$

Taková matice přechodu od báze $\underline{u}$ k bázi $\underline{v}$ má několik pěkných vlastností. Zejména její vedoucí hlavní submatice $T_k$ tvořené prvními $k$ řádky a sloupci jsou matice přechodu podprostorů $P_k = \langle u_1, \dots, u_k \rangle$ od báze $(u_1, \dots, u_k)$ k bázi $(v_1 \dots, v_k)$. Hlavní submatice $A_k$ matice $A$ formy $f$ jsou maticemi zúžení formy $f$ na $P_k$. Při přechodu od $\underline{u}$ k $\underline{v}$ daném maticí přechodu $T$ jsou tedy matice $A_k$ a $A'_k$ zúžení na podprostory $P_k$ ve vztahu $A_k = T_k^T A'_k (T_k)^{-1}$. Inverzní matice k horní trojúhelníkové matici s jedničkami na diagonále je přitom opět horní trojúhelníková matice s jedničkami na diagonále, můžeme tedy podobně vyjádřit i $A'$ pomocí $A$. Podle Cauchyovy věty jsou tedy determinanty matic $A_k$ a $A'_k$ stejné. Celkem jsme tak dokázali velice užitečné pomocné tvrzení:

*Nechť je $f$ kvadratická forma na $V$, $\dim V = n$, a nechť je $\underline{u}$ báze $V$ taková, že při hledání polární báze Lagrangeovým algoritmem není nikdy potřebné použít body (3) a (4). Pak je výsledkem analytické vyjádření*

$$f(x_1, \dots, x_n) = \lambda_1 x_1^2 + \lambda_2 x_2^2 + \dots + \lambda_r x_r^2,$$

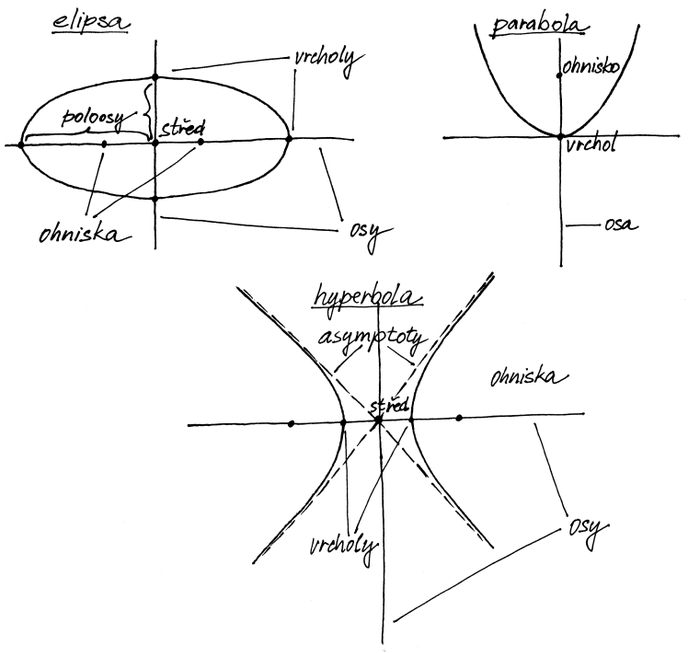
*kde $r$ je hodnost formy $f$, $\lambda_1, \dots, \lambda_r \neq 0$ a pro vedoucí hlavní submatice (původní) matice $A$ kvadratické formy $f$ platí $|A_k| = \lambda_1 \lambda_2 \dots \lambda_k$, $k \leq r$.*

V námi uvažovaném postupu se při každé postupné transformaci vždy další sloupec pod diagonálou v matici $A$ vynuluje. Odtud je již jasné, že případná nenulovost vedoucích hlavních minorů v matici $A$ zaručí nenulovost dalšího diagonálního členu v $A$. Touto úvahou jsme dokázali tzv. *Jacobiho větu*:

**Důsledek.** *Nechť $f$ je kvadratická forma hodnosti $r$ na vektorovém prostoru $V$ s maticí $A$ v bázi $\underline{u}$. V Lagrangeově algoritmu není zapotřebí jiného kroku než doplnění čtverců, právě když pro vedoucí hlavní submatice v $A$ platí $|A_1| \neq 0, \dots, |A_r| \neq 0$. Pak existuje polární báze (a obdržíme ji výše odvozeným algoritmem), ve které má $f$ analytické vyjádření*

$$f(x_1, \dots, x_n) = |A_1| x_1^2 + \frac{|A_2|}{|A_1|} x_2^2 + \dots + \frac{|A_r|}{|A_{r-1}|} x_r^2.$$

Jsou-li tedy všechny vedoucí hlavní minory kladné, pak podle právě dokázané Jacobiho věty je jistě $f$ pozitivně definitní.




**4.50.** Dokažte, že součin vzdáleností ohnisek elipsy od její libovolné tečny je konstantní a zjistěte velikost této konstanty.

**Řešení.** Uvažme polární bázi. V ní má matice elipsy diagonální tvar $\operatorname{diag}\left(\frac{1}{a^2}, \frac{1}{b^2}, -1\right)$ a rovnice poláry (tečny) v bodě X=$[x_0, y_0]$ má tvar $\frac{x_0}{a^2}x + \frac{y_0}{b^2}y = 1$. Vzdálenost ohnisek E,F= $[\mp e, 0]$ od této přímky je rovna

$$\frac{1 \pm e\frac{x_0}{a^2}}{\sqrt{\frac{x_0^2}{a^4} + \frac{y_0^2}{b^4}}}$$

a jejich součin je tedy

$$\frac{1 - e^2\frac{x_0^2}{a^4}}{\frac{x_0^2}{a^4} + \frac{y_0^2}{b^4}}.$$

Dosadíme-li $e^2 = a^2 - b^2$ a $\frac{y_0^2}{b^2} = 1 - \frac{x_0^2}{a^2}$ (bod X leží na elipse), zjistíme, že předchozí výraz je roven $b^2$. □

**4.51.** Jakou velikost mají poloosy elipsy, když je součet jejich velikostí roven vzdálenosti mezi ohnisky a ta je rovna 1.

**Řešení.** Řešíme soustavu

$$\begin{aligned} a + b &= 1, \\ 2e = \ 2\sqrt{a^2 - b^2} &= 1 \end{aligned}$$

a najdeme řešení $a = \frac{5}{8}, b = \frac{3}{8}$. □

**4.52.** Pro jaké směrnice $k$ jsou přímky vedené z bodu $[-4, 2]$ sečnami a kdy tečnami elipsy dané rovnicí

$$\frac{x^2}{9} + \frac{y^2}{4} = 1.$$

Předpokládejme naopak, že forma $f$ je pozitivně definitní. Pak pro vhodnou regulární matici $P$ platí $A = P^T E P = P^T P$. Je tedy $|A| = |P|^2 > 0$. Nechť $\underline{u}$ je zvolená báze, ve které má forma $f$ matici $A$. Zúžení $f$ na podprostory $V_k = \langle u_1, \ldots, u_k \rangle$ je opět pozitivně definitní forma $f_k$, jejíž maticí v bázi $u_1, \ldots, u_k$ je vedoucí hlavní submatice $A_k$. Proto je podle předchozí části důkazu také $|A_k| > 0$.

Tvrzení o negativně definitních vyplývá z předchozího a skutečnosti, že $A$ je pozitivně definitní právě, když $-A$ je negativně definitní. □

### 3. Projektivní geometrie



V mnoha elementárních textech o analytické geometrii autoři končí afinními a euklidovskými objekty popsanými výše. Na spoustu praktických úloh euklidovská nebo afinní geometrie stačí, na jiné bohužel ale nikoliv.

Tak třeba při zpracovávání obrazu z kamery nejsou zachovávány úhly a rovnoběžné přímky se mohou (ale nemusí) protínat. Dalším dobrým důvodem pro hledání širšího rámce geometrických úloh a úvah je požadovaná robustnost a jednoduchost numerických operací. Daleko jednodušší jsou totiž operace prováděné prostým násobením matic a velice těžko se od sebe odlišují malinké úhly od nulových, proto je lepší mít nástroje, které takové odlišení nevyžadují.

Základní ideou projektivní geometrie je rozšíření afinních prostorů o body v nekonečnu způsobem, který bude dobře umožňovat manipulace s lineárními objekty typu bodů, přímek, rovin, projekcí, apod.

**4.33. Projektivní rozšíření afinní roviny.** Začneme tím nejjednodušším zajímavým případem, geometrií v rovině. Jestliže si body roviny $\mathcal{A}_2$ představíme jako rovinu $z = 1$ v $\mathcal{R}^3$, pak každý bod $P$ naší afinní roviny představuje vektor $u = (x, y, 1) \in \mathbb{R}^3$ a tím i jednorozměrný podprostor $\langle u \rangle \subset \mathbb{R}^3$. Naopak, skoro každý jednorozměrný podprostor v $\mathbb{R}^3$ protíná naši rovinu v právě jednom bodě $P$ a jednotlivé vektory takového podprostoru jsou dány souřadnicemi $(x, y, z)$ jednoznačně, až na společný skalární násobek. Žádný průnik s naší rovinou nebudou mít pouze podprostory s body o souřadnicích $(x, y, 0)$.

PROJEKTIVNÍ ROVINA

**Definice.** *Projektivní rovina* $\mathcal{P}_2$ je množina všech jednorozměrných podprostorů v $\mathbb{R}^3$. *Homogenní souřadnice* bodu $P = (x : y : z)$ v projektivní rovině jsou trojice reálných čísel určené až na společný skalární násobek, přičemž alespoň jedno z nich musí být nenulové. Přímka v projektivní rovině je definována jako množina jednorozměrných podprostorů (tj. bodů v $\mathcal{P}_2$), které vyplní dvourozměrný podprostor (tj. rovinu) v $\mathbb{R}^3$.

Abychom měli před očima konkrétní příklad, podívejme se v afinní rovině $\mathbb{R}^2$ na dvě rovnoběžné přímky

$$L_1 : y - x - 1 = 0, \quad L_2 : y - x + 1 = 0.$$

Jestliže budeme body přímek $L_1$ a $L_2$ chápat jako konečné body v projektivním prostoru $\mathcal{P}_2$, budou zjevně jejich homogenní souřadnice $(x : y : z)$ splňovat rovnice

$$L_1 : y - x - z = 0, \quad L_2 : y - x + z = 0.$$

**Řešení.** Směrový vektor přímky je $(1, k)$ a proto je parametrické vyjádření přímky $x = -4+t$, $y = 2+kt$. Průsečík s elipsou pak splňuje

$$\frac{(-4+t)^2}{9} + \frac{(2+kt)^2}{4} = 1.$$

Tato kvadratická rovnice má diskriminant roven

$$D = -\frac{k}{-}9(7k+16).$$

To znamená, že v intervalu $k \in \left(-\frac{16}{7}, 0\right)$ má dvě řešení, tj. přímka je sečna, a pro směrnici $k = -\frac{16}{7}$ a $k = 0$ jediné řešení, tj. přímka je tečna. □

**4.53.** Najděte rovnici tečny k elipse $3x^2+7y^2 = 30$, jejíž vzdálenost od středu elipsy je rovna 3.

**Řešení.** Střed elipsy je v počátku souřadnic a pro vzdálenost $d$ přímky $ax + by + c = 0$ od počátku se odvodí $d = \frac{|c|}{\sqrt{a^2+b^2}}$. Tečna ze zadání tedy splňuje $a^2 + b^2 = \frac{c^2}{9}$. Rovnice tečny v bodě $[x_T, y_T]$ je $3xx_T + 7yy_T - 30 = 0$. Pro souřadnice bodu dotyku tak dostáváme soustavu

$$\begin{aligned} (3x_T)^2 &+ (7y_T)^2 &&= 100, \\ 3x_T^2 &+ 7y_T^2 &&= 30. \end{aligned}$$

Jejím řešením je $x_T = \pm\sqrt{\frac{55}{6}}$, $y_T = \pm\sqrt{\frac{5}{14}}$. Vzhledem k symetrii elipsy dostáváme čtyři řešení $\pm 3\sqrt{\frac{55}{6}}x \pm 7\sqrt{\frac{5}{14}}y - 30 = 0$. □

**4.54.** Je dána hyperbola $x^2 - y^2 = 2$. Určete rovnici hyperboly, která má stejná ohniska a prochází bodem $[-2, 3]$.

**Řešení.** Výstřednost zadané hyperboly je $e = \sqrt{2+2} = 2$. Rovnice hledané hyperboly bude $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ a její výstřednost bude splňovat $e^2 = a^2 + b^2 = 4$. Podmínka, že bod $[-2, 3]$ leží na hyperbole dává $\frac{4}{a^2} - \frac{9}{b^2} = 1$. Řešením této soustavy je $a^2 = 1$, $b^2 = 3$. Hledaná hyperbola je tedy $x^2 - \frac{y^2}{3} = 1$. □

**4.55.** Určete rovnice tečen hyperboly $4x^2 - 9y^2 = 1$, kolmých na přímku $x - 2y + 7 = 0$.

**Řešení.** Všechny přímky kolmé na zadanou přímku mají tvar $2x + y + c = 0$ pro nějaké $c$. Hledaná přímka má mít právě jeden průnik se zadanou hyperbolou, tj. rovnice $4x^2 - 9(-2x - c)^2 = 1$ má mít jedno řešení. To nestane tehdy, když $D = (36c)^2 - 4.32.(9c^2 + 1) = 0$. Odtud $c = \pm\frac{2\sqrt{2}}{3}$. □

Je vidět, že průnikem $L_1 \cap L_2$ bude v tomto kontextu bod $(-1 : 1 : 0) \in \mathcal{P}_2$, tj. nevlastní bod odpovídající společnému zaměření obou přímek.

**4.34. Afinní souřadnice v projektivní rovině.** Pokud začneme naopak projektivní rovinou $\mathcal{P}_2$ a budeme v ní chtít uvidět afinní rovinu jako její „konečnou“ část, pak můžeme místo roviny $z = 1$ vzít v $\mathbb{R}^3$ jakoukoliv jinou rovinu $\sigma$ neprocházející počátkem $0 \in \mathbb{R}^3$. Konečné body pak budou ty jednorozměrné podprostory, které mají neprázdný průnik s rovinou $\sigma$.



Pokračujme v našem příkladu rovnoběžných přímek z předchozího odstavce a podívejme se, jak budou jejich rovnice vypadat v souřadnicích v afinní rovině, která bude dána jako $y = 1$. Za tím účelem stačí dosadit $y = 1$ do předchozích rovnic:

$$L_1' : 1 - x - z = 0, \quad L_2' : 1 - x + z = 0.$$

Nyní jsou „nekonečné“ body naší původní afinní roviny dány vztahem $z = 0$ a vidíme, že naše přímky $L_1'$ a $L_2'$ se protínají v bodě $(1, 1, 0)$. To odpovídá geometrické představě, že rovnoběžné přímky $L_1, L_2$ v afinní rovině se protínají v nekonečnu a to v bodě $(1 : 1 : 0)$.

**4.35. Projektivní prostory a transformace.** Náš postup v afinní rovině se přirozeným způsobem zobecňuje na každou konečnou dimenzi.



Volbou libovolné afinní nadroviny $\mathcal{A}_n$ ve vektorovém prostoru $\mathbb{R}^{n+1}$, která neprochází počátkem, můžeme ztotožnit body $P \in \mathcal{A}_n$ s jednorozměrnými podprostory, které tyto body generují. Zbylé jednorozměrné podprostory vyplní nadrovinu rovnoběžnou s $\mathcal{A}_n$ a říkáme jim *nekonečné body* nebo také *nevlastní body* v projektivním rozšíření $\mathcal{P}_n$ afinní roviny $\mathcal{A}_n$.

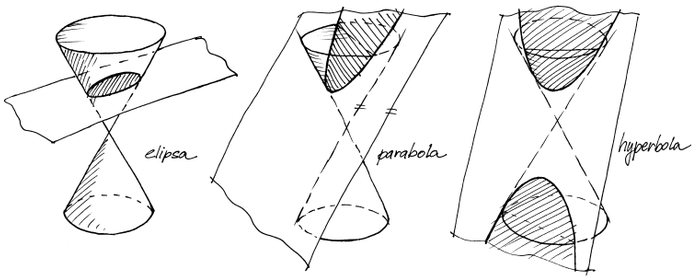
Zjevně je vždy množina nevlastních bodů v $\mathcal{P}_n$ projektivním prostorem dimenze o jedničku nižším. Afinní přímka má ve svém projektivním rozšíření pouze jediný nevlastní bod (oba konce přímky se „potkají“ v nekonečnu a projektivní přímka proto vypadá jako kružnice), projektivní rovina má projektivní přímku nevlastních bodů, trojrozměrný projektivní prostor má projektivní rovinu nevlastních bodů atd.

Ještě obecněji zavádíme *projektivizaci vektorového prostoru*: pro libovolný vektorový prostor $V$ dimenze $n+1$ definujeme

$$\mathcal{P}(V) = \{P \subseteq V;\ P \subseteq V, \dim V = 1\}.$$

Volbou libovolné báze $\underline{u}$ ve $V$ dostáváme tzv. *homogenní souřadnice* na $\mathcal{P}(V)$ tak, že pro $P \in \mathcal{P}(V)$ použijeme jeho libovolný nenulový vektor $u \in V$ a souřadnice tohoto vektoru v bázi $\underline{u}$. Bodům projektivního prostoru $\mathcal{P}(V)$ říkáme *geometrické body*, zatímco jejich nenulové generátory ve $V$ nazýváme říkáme *aritmetické reprezentanty*.

Při zvolených homogenních souřadnicích je možné jednu z jejich hodnot zafixovat na jedničku (tj. vyloučíme všechny body projektivního prostoru s touto souřadnicí nulovou) a získáme tak vložení $n$–rozměrného afinního prostoru $\mathcal{A}_n \subset \mathcal{P}(V)$. To je přesně konstrukce, kterou jsme použili v našem příkladu projektivní roviny.




**4.56. Projektivní pohled na kuželosečky.** Pojem projektivního prostoru nám také umožňuje se novým pohledem podívat na již známé kuželosečky (srovnej s 4.42). Kuželosečku v $\mathcal{E}_2$ zadanou kvadratickou formou

$$f(x, y) = a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2a_{13}x + 2a_{23}y + a_{33}$$

můžeme chápat jako množinu bodů v projektivní rovině $\mathcal{P}_2$ s homogenními souřadnicemi $(x : y : z)$, které jsou nulové body homogenní kvadratické formy

$$f(x, y, z) = a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2a_{13}xz + 2a_{23}yz + a_{33}z^2.$$

Tu můžeme jednoduše psát jako $f(v) = v^T A v$, kde $v$ je sloupcový vektor o souřadnicích $(x, y, z)$ a matice $A$ je symetrická matice $(a_{ij})$. Podle věty 4.31 existuje báze, ve které má tato kvadratická forma jeden z následujících tvarů

$$f(x, y, z) = x^2 + y^2 + z^2, \quad f(x, y, z) = x^2 + y^2 - z^2.$$

V prvním případě je řešením $f(x, y, z) = 0$ jediný (nevlastní) bod a proto původní forma nezadávala reálnou kuželosečku. Druhá kvadratická forma zadává kužel v $\mathbb{R}^3$. Příslušnou kuželosečku dostaneme přechodem zpět k nehomogenním souřadnicím. To znamená řezem tohoto kužele rovinou, která měla v původní bázi rovnici $z = 1$. Odtud dostaneme ihned klasifikaci kuželoseček z 4.29., která odpovídá řezům kužele v $\mathbb{R}^3$ různými rovinami. Řezy, které dávají vlastní kuželosečky jsou znázorněny na obrázku. Nevlastní kuželosečky odpovídají řezům rovinami, které prochází vrcholem kužele.

Pro kuželosečku v projektivní rovině definujeme následující užitečné pojmy:

Body $P, Q \in \mathcal{P}_2$ příslušné jednorozměrným podprostorům $\langle p\rangle, \langle q\rangle$ (generovanými vektory $p, q \in \mathbb{R}^3$) se nazývají *polárně sdružené* vzhledem ke kuželosečce $f$, pokud platí $F(p, q) = 0$, tj. $p^T A q = 0$.

Bod $P = \langle p\rangle$ se nazývá *singulárním bodem* kuželosečky $f$, jestliže je polárně sdružený vzhledem k $f$ se všemi body roviny, tj. $F(p, x) = 0$ pro všechna $x \in \mathcal{P}_2$. To jinými slovy znamená $Ap = 0$. Tím pádem matice $A$ kuželosečky se singulárním bodem

**4.36. Perspektivní projekce.** Velmi dobře jsou výhody projektivní geometrie vidět na perspektivní projekci $\mathbb{R}^3 \to \mathbb{R}^2$. Přestavme si, že pozorovatel sedící v počátku pozoruje „polovinu světa“, tj. body $(X, Y, Z) \in \mathbb{R}^3$ se $Z > 0$ a obraz vidí „promítnutý“ na plátně daném rovinou $Z = f > 0$.



Bod $(X, Y, Z)$ „reálného světa“ se mu tedy promítá na bod $(x, y)$ na průmětně takto:

$$x = f\frac{X}{Z}, \quad y = f\frac{Y}{Z}.$$

To je nejen nelineární formule, ale navíc při $Z$ malém bude velice problematická přesnost výpočtů.

Při rozšíření této transformace na zobrazení $\mathcal{P}_3 \to \mathcal{P}_2$ dostáváme zobrazení

$$(X : Y : Z : W) \mapsto (x : y : z) = (fX : fY : Z),$$

tj. popsané prostým lineárním vztahem

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} f & 0 & 0 & 0 \\ 0 & f & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix}.$$

Tento jednoduchý výraz zadává perspektivní projekci pro konečné body v $\mathbb{R}^3 \subset \mathcal{P}_3$, které dosazujeme jako výrazy s $W = 1$. Přitom jsem elegantně odstranili problémy s body, jejichž obraz utíká do nekonečna. Skutečně, je–li $Z$-ová souřadnice skutečného bodu scény blízká nule, bude hodnota třetí homogenní souřadnice obrazu mít souřadnici blízkou nule, tj. bude představovat bod blízký nekonečnu.

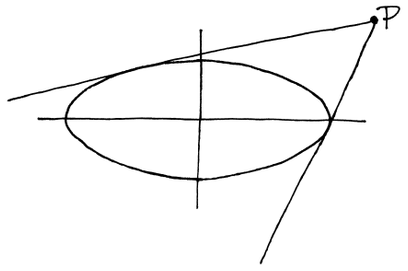
**4.37. Afinní a projektivní transformace.** Každé prosté lineární zobrazení $\varphi : V_1 \to V_2$ mezi vektorovými prostory samozřejmě zobrazuje jednorozměrné podprostory na jednorozměrné podprostory. Tím vzniká zobrazení na projektivizacích $T : \mathcal{P}(V_1) \to \mathcal{P}(V_2)$. Takovým zobrazením říkáme *projektivní zobrazení*, v literatuře je používán také pojem *kolineace*, pokud je toto zobrazení invertibilní.



Jinak řečeno, projektivní zobrazení je takové zobrazení mezi projektivními prostory, že v každé soustavě homogenních souřadnic na definičním oboru i obrazu je toto zobrazení zadáno násobením vhodnou maticí. Obecněji, pokud naše pomocné lineární zobrazení není prosté, definuje projektivní zobrazení pouze mimo svoje jádro, tj. na bodech, jejichž homogenní souřadnice se nezobrazují na nulu.

Prostá zobrazení $V \to V$ vektorového prostoru na sebe jsou invertibilní, všechna projektivní zobrazení projektivního prostoru $\mathcal{P}_n$ na sebe jsou tedy invertibilní též. Říká se jim také *regulární kolineace* nebo *projektivní transformace*. Odpovídají v homogenních souřadnicích invertibilním maticím dimenze $n+1$. Dvě takové matice zadávají stejnou projektivní transformaci, právě když se liší o konstantní násobek.

Jestliže si zvolíme první souřadnici jako tu, jejíž nulovost určuje nevlastní body, budou transformace, které zachovávají nevlastní body, dány maticemi, jejichž první řádek musí být až na první člen nulový. Jestliže budeme chtít přejít do afinních souřadnic konečných bodů, tj. zafixujeme si hodnotu první souřadnice na jedničku, musí být první prvek na prvním řádku být také rovný




nemá maximální hodnost a tak zadává nevlastní kuželosečku. Vlastní kuželosečky tedy neobsahují singulární body.

Množinu všech bodů $X = \langle x \rangle$ polárně sdružených s bodem $P = \langle p \rangle$ nazýváme *polárou* bodu $P$ vzhledem ke kuželosečce $f$. Je to tedy množina bodů, pro které platí $F(p, x) = p^T A x = 0$. Protože je polára zadaná lineární kombinací souřadnic, je to vždy (v nesingulárním případě) přímka. Geometrický význam poláry vysvětluje následující věta.

**4.57. Charakterizace polár.** Uvažme vlastní kuželosečku $f$ Polárou bodu $P \in f$ vzhledem k projektivní kuželosečce $f$ je tečna k $f$ s bodem dotyku $P$. Polárou bodu $P \notin f$ je přímka daná body dotyku tečen sestrojených z bodu $P$ ke kuželosečce $f$.

**Řešení.** Nejprve uvažujme $P \in f$ a ukážeme sporem, že polára má s kuželosečkou právě jeden společný bod (bod dotyku). Předpokládejme tedy, že polára bodu $P$, určená rovnicí $F(p, x) = 0$, protne vlastní kuželosečku $f$ v bodě $Q = \langle q \rangle \neq P$. Pak zřejmě platí $F(p, q) = 0$ a $f(q) = F(q, q) = 0$. Pro libovolný bod $X = \langle x \rangle$ ležící na přímce určené body $P$ a $Q$ pak máme $x = \alpha p + \beta q$ pro nějaké $\alpha, \beta \in \mathbb{R}$. Díky bilinearitě a symetrii $F$ pak dostáváme

$$f(x) = F(x, x) = \alpha^2 F(p, p) + 2\alpha\beta F(p, q) + \beta^2 F(q, q) = 0$$

a to znamená, že každý bod $X$ přímky leží na kuželosečce $f$. Když ale kuželosečka obsahuje přímku, pak musí být nevlastní, což je spor s předpokladem. Zároveň vidíme, že v případě nevlastní kuželosečky je polárou samotná (tzv. tvořící) přímka kuželosečky.

Tvrzení pro případ $P \notin f$ vyplývá z následujícího důsledku symetrie bilineární formy $F$. Pokud bod $Q$ leží na poláře bodu $P$, pak bod $P$ leží na poláře bodu $Q$. □

Pomocí polárně sdružených bodů můžeme také nalézt bez použití Lagrangeova algoritmu rovnice os kuželoseček i střed kuželosečky.

Napišme matici kuželosečky jako blokovou matici

$$A = \begin{pmatrix} \bar{A} & a \\ a^T & \alpha \end{pmatrix},$$

jedné. Matice kolineací zachovávajících konečné body našeho afinního prostoru tedy mají tvar:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_1 & a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots & \\ b_n & a_{n1} & \cdots & a_{nn} \end{pmatrix},$$

kde $b = (b_1, \ldots, b_n)^T \in \mathbb{R}^n$ a $A = (a_{ij})$ je invertibilní matice dimenze $n$. Působení takové matice na vektoru $(1, x_1, \ldots, x_n)$ je právě obecná afinní transformace, kde $b$ zadává posunutí a $A$ její lineární část. Jsou tedy afinní zobrazení právě ty kolineace, které zachovávají nadrovinu nevlastních bodů.

**4.38. Určení kolineací.** K zadání afinního zobrazení je nutné a stačí libovolně zadat obraz afinního repéru. V právě uvedeném popisu afinních transformací jako speciálního případu projektivních zobrazení to odpovídá vhodné volbě obrazu vhodné aritmetické báze vektorového prostoru $V$.



Obecně ale neplatí, že obraz aritmetické báze $V$ jednoznačně určí kolineaci. Ukažme si podstatu problému na jednoduchém příkladu afinní roviny. Jestliže si zvolíme v rovině čtyři body $A$, $B$, $C$, $D$ tak, aby každá z nich utvořená trojice byla v obecné poloze (tj. žádné tři z nich neleží na jedné přímce), můžeme si libovolně zvolit jejich obraz v kolineaci následujícím způsobem:

Zvolme jakkoliv jejich čtyři obrazy $A'$, $B'$, $C'$, $D'$ se stejnou vlastností a zvolme si jejich homogenní souřadnice $u$, $v$, $w$, $z$, $u'$, $v'$, $w'$, $z'$ v $\mathbb{R}^3$. Vektory $z$ a $z'$ pak můžeme jistě zapsat pomocí lineárních kombinací

$$z = c_1 u + c_2 v + c_3 w, \quad z' = c_1' u' + c_2' v' + c_3' w',$$

přičemž všech šest koeficientů musí být nenulových, neboť jinak by některá trojice z našich bodů nebyla v obecné poloze.

Nyní si zvolíme nové aritmetické reprezentanty bodů $A$, $B$ a $C$ po řadě jako $\tilde{u} = c_1 u$, $\tilde{v} = c_2 v$ a $\tilde{w} = c_3 w$ a stejně $\tilde{u}' = c_1 u'$, $\tilde{v}' = c_2 v'$ a $\tilde{w}' = c_3 w'$ pro body $A'$, $B'$ a $C'$. Tato volba zadává jediné lineární zobrazení $\varphi$ zobrazující postupně

$$\varphi(\tilde{u}) = \tilde{u}', \quad \varphi(v') = \tilde{v}', \quad \varphi(\tilde{w}) = \tilde{w}'.$$

Zároveň však platí

$$\varphi(z) = \varphi(\tilde{u} + \tilde{v} + \tilde{w}) = \tilde{u}' + \tilde{v}' + \tilde{w}' = z',$$

a tedy námi zkonstruovaná kolineace skutečně zobrazuje body tak, jak jsme si předem zvolili. Lineární zobrazení $\varphi$ přitom bylo dáno naší konstrukcí jednoznačně, takže je kolineace dána naší volbou jednoznačně.

Naše argumentace zůstává v platnosti, i když jsou některé ze zvolených bodů nevlastní (tj. jeden nebo dva). Ještě jednodušeji bychom viděli ilustraci téhož jevu na regulárních kolineacích projektivní přímky, které jsou zadány po dvou různými obrazy třech po dvou různých bodů.

Postup, který jsme použili zjevně funguje pro libovolné dimenze. O $n + 2$ bodech projektivního prostoru řekneme, že jsou v *obecné poloze*, jestliže žádných $n+1$ z nich neleží v stejné nadrovině. Říkáme také, že jde o lineárně nezávislé body, které tvoří *geometrickou bázi* projektivního prostoru.

**Věta.** *Regulární kolineace na $n$–rozměrném projektivním prostoru je jednoznačně určena libovolným zobrazením $n+2$ bodů v obecné poloze, jejichž obrazy jsou opět body v obecné poloze.*

kde $\bar{A} = (a_{ij})$ pro $i, j = 1, 2$, $a$ je vektor o souřadnicích $(a_{13}, a_{23})$ a $\alpha = a_{33}$. To znamená, že kuželosečka je zadaná rovnicí

$$u^T \bar{A} u + 2a^T u + \alpha = 0$$

pro vektor $u = (x, y)$. Nyní ukážeme:

**4.58.** Osy kuželosečky jsou poláry nevlastních bodů určených vlastními vektory matice $\bar{A}$.

**Řešení.** Protože je matice $\bar{A}$ symetrická, má v bázi svých vlastních vektorů diagonální tvar $D = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, kde $\lambda, \mu \in \mathbb{R}$ a tato báze je ortogonální. Označíme-li matici přechodu k této bázi $U$ (sloupce jsou jednotkové vlastní vektory), pak má matice kuželosečky bázi vlastních vektorů tvar

$$\begin{pmatrix} U^T & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \bar{A} & a \\ a^T & \alpha \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} D & U^T a \\ a^T U & \alpha \end{pmatrix}.$$

V této bázi má tedy kanonické vyjádření až na posunutí dané vektorem $U^T a$. Konkrétně, označíme-li jednotkové vlastní vektory $v_\lambda, v_\mu$, máme

$$\lambda \left( x + \frac{a^T v_\lambda}{\lambda} \right)^2 + \mu \left( y + \frac{a^T v_\mu}{\mu} \right)^2 = \frac{(a^T v_\lambda)^2}{\lambda} + \frac{(a^T v_\mu)^2}{\mu} - \alpha.$$

To znamená, že vlastní vektory jsou směrové vektory os kuželosečky (tzv. hlavní směry) a rovnice os v této bázi jsou $x = -\frac{a^T v_\lambda}{\lambda}$ a $y = -\frac{a^T v_\mu}{\mu}$. Souřadnice os $u_\lambda$ a $u_\mu$ ve standardní bázi proto splňují $v_\lambda^T u_\lambda = -\frac{a^T v_\lambda}{\lambda}$ a $v_\mu^T u_\mu = -\frac{a^T v_\mu}{\mu}$, neboli $v_\lambda^T(\lambda u_\lambda + a) = 0$ a $v_\mu^T(\mu u_\mu + a) = 0$. Tyto rovnice jsou ekvivalentní rovnicím $v_\lambda^T(\bar{A} u_\lambda + a) = 0$ a $v_\mu^T(\bar{A} u_\mu + a) = 0$ a to jsou rovnice polár nevlastních bodů určených vektory $v_\lambda$ a $v_\mu$. □

**4.59. Poznámka.** Důsledkem tvrzení z předchozího příkladu je fakt, že střed kuželosečky je polárně sdružený se všemi nevlastními body. Souřadnice $s$ středu pak splňují rovnici $\bar{A}s + a = 0$.

Pokud $\det(A) \neq 0$, pak má rovnice $\bar{A}s + a = 0$ pro souřadnice středu kuželosečky pro $\delta = \det(\bar{A}) \neq 0$ právě jedno řešení a pro $\delta = 0$ žádné řešení. To znamená, že z vlastních kuželoseček má elipsa a hyperbola jeden vlastní střed a parabola žádný (střed paraboly je v nevlastním bodě).

**4.60.** Dokažte, že tečna paraboly v libovolném bode svírá stejný úhel s osou paraboly, jako se spojnicí ohniska a bodu dotyku.

**Řešení.** Polárou (tj. tečnou) bodu $X = [x_0, y_0]$ k parabole zadané kanonickou rovnicí v polární bázi je přímka splňující

$$(x_0, y_0, 1) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -p \\ 0 & -p & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = x_0 x - p y - p y_0 = 0.$$

Důkaz. Důkaz se provede zcela stejně, jak jsme postupovali v dimenzi dvě. Doporučujeme rozepsat podrobně jako cvičení. □

**4.39. Dvojpoměry.** 
Připomeňme, že afinní zobrazení zachovávají poměry velikostí úseček na každé přímce. Technicky jsme definovali tento poměr pro tři body $A$, $B$ a $C \neq B, C = rA + sB$ jako $\lambda = (C; A, B) = -\frac{s}{r}$. Je zřejmé, že ale třeba středové promítání takové poměry nezachovávají, dokonce nemusí být zachována ani poloha bodů na přímce vůči sobě. Naopak jsme si uváděli, že můžeme na projektivní přímce libovolně určit obrazy tří po dvou různých bodů a tím jednoznačně zadat projektivní transformaci. Celkem snadno ale lze dovodit, že se zachovává poměr takovýchto poměrů pro dva různé body $C$:

Uvažme v projektivním prostoru čtveřici různých bodů $A$,$B$, $C$, $D$ na jedné projektivní přímce, která je generována body $A$ a $B$, a po řadě i jejich aritmetické souřadnice $x$, $y$, $w$, $z$. Protože tyto čtyři vektory leží v podprostoru $\langle x, y \rangle$, můžeme ostatní napsat jako lineární kombinace

$$w = t_1 x + s_1 y, \quad z = t_2 x + s_2 y$$

a definujeme tzv. *dvojpoměr čtveřice bodů* $(A, B, C, D)$ jako

$$\rho = \frac{s_1}{t_1} \frac{t_2}{s_2}.$$

To je korektní definice, protože jsou sice vektory $x$ a $y$ určeny každý až na skalární násobek, tyto násobky se ovšem v definici pokrátí.

Stejně tak je přímo z definice je zřejmé, že každá projektivní transformace zachovává dvojpoměry, protože když ji zadáme v našich aritmetických souřadnicích pomocí matice $A$, dostaneme obrazy $A \cdot w = t_1 A \cdot x + t_2 A \cdot y$ a podobně pro $Az$, a proto i čtveřice obrazů našich bodů bude mít stejný dvojpoměr.

Zastavme se ještě u charakterizace projektivních transformací. Opět platí, že jsou to právě ta zobrazení, která zachovávají dvojpoměry. Ve skutečnosti to ale není příliš praktická charakterizace, protože implicitně obsahuje i tvrzení, že taková zobrazení musí zobrazovat projektivní přímky na projektivní přímky.

Lze ale dokázat daleko silnější tvrzení, že zobrazení jakkoliv malé otevřené oblasti v afinním prostoru $\mathbb{R}^n$ (např. koule bez hranice), do téhož afinního prostoru, které zobrazuje přímky na přímky, je ve skutečnosti zúžením jednoznačně určené projektivní transformace projektivního rozšíření $\mathcal{P}\mathbb{R}^{n+1}$ původního afinního prostoru $\mathbb{R}^n$. A tyto transformace tedy nutně zachovávají i dvojpoměry.

**4.40. Dualita.** 
Projektivní nadroviny jsou definovány projektivním prostoru $\mathcal{P}(V)$ dimenze $n$ jako projektivizace $n$–rozměrných vektorových podprostorů ve vektorovém prostoru $V$. Jsou tedy v homogenních souřadnicích definovány jako jádra lineárních forem $\alpha \in V^*$, které jsou opět určeny až na skalární násobek.

Ve zvolené aritmetické bázi jsou tedy projektivní nadroviny dány řádkovým vektorem $\alpha = (\alpha_0, \ldots, \alpha_n)$. Přitom ale jsou formy $\alpha$ dány jednoznačně, až na skalární násobek. Každá nadrovina ve $V$ tedy je identifikována s právě jedním geometrickým bodem v projektivizaci duálního prostoru $\mathcal{P}(V^*)$. Hovoříme o *duálním projektivním prostoru* a dualitě mezi body a nadrovinami.

Kosinus úhlu, který tečna svírá s osou paraboly ($x = 0$) je daný skalárním součinem příslušných jednotkových směrových vektorů. Jednotkový směrový vektor tečny je $\frac{1}{\sqrt{p^2+x_0^2}}(p, x_0)$, a proto pro kosinus platí

$$\frac{1}{\sqrt{p^2+x_0^2}}(p, x_0) \cdot (0, 1) = \frac{x_0}{\sqrt{p^2+x_0^2}}.$$

Nyní ukážeme, že kosinus úhlu, který tečna svírá se spojnicí ohniska F=[0, $\frac{p}{2}$] a bodem dotyku X je stejný. Jednotkový směrový vektor spojnice je

$$\frac{1}{\sqrt{x_0^2 + \left(y_0 - \frac{p}{2}\right)^2}} \left(x_0, y_0 - \frac{p}{2}\right).$$

Pro kosinus úhlu pak máme

$$\frac{1}{\sqrt{p^2+x_0^2}} \frac{1}{\sqrt{x_0^2 + \left(y_0 - \frac{p}{2}\right)^2}} \left(x_0 y_0 + \frac{p x_0}{2}\right).$$

Dosazením $y_0 = \frac{x_0^2}{2p}$ a úpravou výrazu dostaneme $\frac{x_0}{\sqrt{p^2+x_0^2}}$.

Tento příklad ukazuje, že paprsky světla dopadající rovnoběžně s osou na parabolické zrcadlo, se odrážejí do ohniska a naopak, paprsky světla vyzařovaného z ohniska se odráží stejným směrem (rovnoběžně s osou). To je principem mnoha zařízení, např. parabolický reflektor, parabolická anténa. □

**4.61.** Najděte rovnici tečny v bodě $P = [1, 1]$ ke kuželosečce

$$4x^2 + 5y^2 - 8xy + 2y - 3 = 0.$$

**Řešení.** Projektivizací dostaneme kuželosečku zadanou kvadratickou formou $(x, y, z)A(x, y, z)^T$ s maticí

$$A = \begin{pmatrix} 4 & -4 & 0 \\ -4 & 5 & 1 \\ 0 & 1 & -3 \end{pmatrix}.$$

Podle předchozí věty je tečna polárou bodu P, který má homogenní souřadnice (1 : 1 : 1). Ta je dána rovnicí $(1, 1, 1)A(x, y, z)^T = 0$, což v našem případě dává rovnici

$$2y - 2z = 0.$$

Přechodem zpět k nehomogenním souřadnicím dostaneme rovnici tečny $y = 1$. □

**4.62.** Určete souřadnice bodu dotyku osy $y$ s kuželosečkou zadanou rovnicí

$$5x^2 + 2xy + y^2 - 8x = 0.$$

**Řešení.** Osa $y$, tj. přímka $x = 0$, je polárou hledaného bodu P s homogenními souřadnicemi $\langle p \rangle = (p_1 : p_2 : p_3)$. To znamená, že rovnice

Na formách působí lineární zobrazení zadávající danou kolineací pomocí násobení řádkových vektorů zprava toutéž maticí

$$\alpha = (\alpha_0, \ldots, \alpha_n) \mapsto \alpha \cdot A\,,$$

tj. matice duálních zobrazení je $A^T$. Duální zobrazení ovšem zobrazuje formy opačným směrem z „cílového prostoru“ ne „počáteční“, proto potřebujeme pro současné studium vlivu regulární kolineace na body a jejich duální nadroviny zobrazení inverzní ke kolineaci $f$. To je dáno maticí $A^{-1}$. Matice příslušného působení kolineace na formách je proto $(A^T)^{-1}$. Protože je přitom inverzní matice rovna algebraicky adjungované matici $A^*_{\text{alg}}$, až na násobek inverzí determinantu, viz vztah (2.2) na str. 83, můžeme rovnou pracovat s projektivní transformací prostoru $\mathcal{P}(V*)$ zadanou maticí $(A^*_{\text{alg}})^T$ (nebo bez transponování, pokud násobíme řádkové vektory zprava).

Okamžitě z definic je vidět, že projektivní bod $X$ patří nadrovině $\alpha$, když pro jejich aritmetické souřadnice platí $\alpha \cdot x = 0$. To samozřejmě zůstává v platnosti i po působení libovolnou kolineací, protože opět

$$(\alpha \cdot A^{-1}) \cdot (A \cdot x) = \alpha \cdot x = 0.$$

**4.41. Samodružné body, středy a osy.** Uvažujme regulární kolineaci $f$ zadanou v nějaké aritmetické bázi projektivního prostoru $\mathcal{P}(V)$ pomocí matice $A$.



*Samodružným bodem* kolineace $f$ rozumíme bod $A$, který je zobrazen na sebe, tj. $f(A) = A$, *samodružnou nadrovinou kolineace* $f$ rozumíme nadrovinu $\alpha$, která je zobrazována na sebe, tj. $f(\alpha) \subseteq \alpha$.

Přímo z definice tedy vidíme, že samodružné body mají za aritmetické reprezentanty právě vlastní vektory matice $A$.

V geometrii roviny jsme se s mnoha typy kolineací již jistě setkali: symetrie podle středu, zrcadlení podle přímky, posunutí, stejnolehlost atd. Možná vzpomeneme i na různé typy promítání, např. promítání jedné roviny v $\mathbb{R}^3$ na druhou z nějakého středu $S \in \mathbb{R}^3$.

Všimněme si, že kromě samodružných bodů se u všech takových afinních zobrazení objevovaly také samodružné přímky. Např. u symetrie podle středu se zachovávají také všechny přímky tímto středem procházející, u posunutí se (obdobně) zachovávají nevlastní body roviny.

Zastavíme se u tohoto jevu v obecné dimenzi. Nejprve zavedeme velmi klasický pojem související s incidencí bodů a nadrovin.

*Trs nadrovin procházejí bodem* $A \in \mathcal{P}(V)$ je množina všech nadrovin, které obsahují bod $A$. Z definice je zřejmé, že pro každý bod $A$ je příslušný trs nadrovin sám nadrovinou v duálním prostoru $\mathcal{P}(V^*)$ (je zadán jednou homogenní lineární rovnicí v aritmetických souřadnicích).

Pro kolineaci $f : \mathcal{P}(V) \to \mathcal{P}(V)$ řekneme, že bod $S \in \mathcal{P}(V)$ je *středem kolineace* $f$ jestliže všechny nadroviny v trsu nadrovin určeném bodem $S$ jsou samodružné. Řekneme, že nadrovina $\alpha$ je *osou kolineace* $f$, jestliže jsou všechny její body samodružné.

Přímo z definice je zřejmé, že osa kolineace je středem kolineace duální, zatímco trs nadrovin zadávajících střed kolineace je sám osou kolineace duální.

Protože matice kolineace na původním a duálním prostoru se liší pouze transpozicí, jejich vlastní čísla splývají (vlastní vektory

$x = 0$ je ekvivalentní rovnici poláry $F(p, v) = p^T A v = 0$, kde $v = (x, y, z)^T$.To je splněno právě v případě, když $Ap = (\alpha, 0, 0)^T$ pro nějaké $\alpha \in \mathbb{R}$. Tato podmínka dává pro matici naší kuželosečky

$$A = \begin{pmatrix} 5 & 1 & -4 \\ 1 & 1 & 0 \\ -4 & 0 & 0 \end{pmatrix}$$

soustavu rovnic

$$\begin{aligned} 5p_1 + p_2 - 4p_3 &= \alpha, \\ p_1 + p_2 &= 0, \\ -4p_1 &= 0. \end{aligned}$$

Buď můžeme najít souřadnice bodu P pomocí inverzní matice, $p = A^{-1}(\alpha, 0, 0)^T$, nebo vyřešit tuto soustavu rovnic přímo, zpětným dosazováním. V tomto případě takto dostaneme lehce řešení $p = \left(0, 0, -\frac{1}{4}\alpha\right)$. Osa $y$ se tedy dotýká kuželosečky v počátku. □

**4.63.** Určete bod dotyku přímky $x = 2$ s kuželosečkou z předchozího příkladu.

**Řešení.** Přímka má v projektivním rozšíření rovnici $x - 2z = 0$, a proto v tomto případě dostaneme pro bod dotyku P podmínku $Ap = (\alpha, 0, -2\alpha)$, což dává soustavu

$$\begin{aligned} 5p_1 + p_2 - 4p_3 &= \alpha, \\ p_1 + p_2 &= 0, \\ -4p_1 &= -2\alpha. \end{aligned}$$

Jejím řešením je $p = \left(\frac{1}{2}\alpha, -\frac{1}{2}\alpha, \frac{1}{4}\alpha\right)$. Tyto homogenní souřadnice jsou ekvivalentní souřadnicím $(2, -2, 1)$ a proto proto má bod dotyku souřadnice $[2, -2]$. □

**4.64.** Najděte rovnice tečen sestrojených z bodu $P = [3, 4]$ ke kuželosečce zadané rovnicí

$$2x^2 - 4xy + y^2 - 2x + 6y - 3 = 0.$$

**Řešení.** Předpokládejme, že bod dotyku T hledané tečny má homogenní souřadnice dané násobky vektoru $t = (t_1, t_2, t_3)$. Podmínka, že T leží na kuželosečce je $t^T A t = 0$, což dává

$$2t_1^2 - 4t_1t_2 + t_2^2 - 2t_1t_3 + 6t_2t_3 - 3t_3^2 = 0.$$

Podmínka, že bod P leží na poláře bodu T je $p^T A t = 0$, kde $p = (3, 4, 1)$ jsou homogenní souřadnice bodu P. Tato rovnice v našem případě dává

$$(3, 4, 1) \begin{pmatrix} 2 & -2 & -1 \\ -2 & 1 & 3 \\ -1 & 3 & -3 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix} = -3t_1 + t_2 + 6t_3 = 0.$$

jsou sloupcové, resp. řádkové, k týmž vlastním číslům). Např. v projektivní rovině (a ze stejného důvodu v každém reálném projektivním prostoru sudé dimenze) má každá kolineace alespoň jeden samodružný bod, protože charakteristické polynomy příslušných lineárních zobrazení jsou lichého stupně a tedy mají alespoň jeden reálný kořen.

Nebudeme se již zde dále věnovat obecné teorii, ale budeme aspoň krátce ilustrovat její užitečnost na několika výsledcích pro projektivní roviny.

**Tvrzení.** *Projektivní transformace roviny různá od identity má buď právě jeden střed a právě jednu osu, nebo nemá ani střed ani osu.*

Důkaz. Uvažme kolineaci $f$ na $\mathcal{P}\mathbb{R}^3$ a uvažme, že by měla dva různé středy $A$ a $B$. Označme $\ell$ přímku zadanou těmito středy a zvolme bod $X$ v projektivní rovině mimo $\ell$. Jsou-li $p$ a $q$ po řadě přímky procházející dvojicemi bodů $(A, X)$ a $(B, X)$, pak také $f(p) = p$ a $f(q) = q$ a tedy zejména je i bod $X$ samodružný. To ale znamená, že všechny body roviny mimo $L$ jsou samodružné. Každá přímka různá od $\ell$ má tedy všechny body mimo $\ell$ samodružné a proto je i její průnik s $\ell$ samodružný. Je tedy $f$ identické zobrazení a dokázali jsme, že neidentická projektivní transformace může mít nejvýše jeden střed. Tatáž úvaha pro duální projektivní rovinu nám dává výsledek o nejvýše jediné ose.

Jestliže má $f$ střed $A$, pak všechny přímky procházející $A$ jsou samodružné a odpovídají proto dvourozměrnému podprostoru vlastních řádkových vektorů příslušné matice pro transformaci $f$. Proto bude existovat dvourozměrný prostor sloupcových vlastních vektorů ke stejnému vlastnímu číslu a ten bude reprezentovat právě přímku samodružných bodů, tedy osu. Tatáž úvaha v obráceném pořadí dokazuje i opačné tvrzení — jestliže má projektivní transformace roviny osu, má i střed. □

Pro praktické problémy je užitečné i pro reálnou rovinu pracovat v jejím komplexním projektivním rozšíření a geometrické chování transformací je pak velmi dobře čitelné z případné existence reálných či imaginárních středů a os.

**4.42. Projektivní klasifikace kvadrik.** Závěrem se ještě vrátíme



ke kuželosečkám a kvadrikám. V $n$–rozměrném afinním prostoru $\mathbb{R}^n$ zadáváme kvadriku $Q$ v afinních souřadnicích pomocí obecné kvadratické rovnice (4.4), viz str. 210. Pohlížíme-li na afinní prostor $\mathbb{R}^n$ jako na afinní souřadnice v projektivním prostoru $\mathcal{P}\mathbb{R}^{n+1}$, můžeme chtít tutéž množinu $Q$ popsat pomocí homogenních souřadnic v projektivním prostoru. V nich by mělo jít o výraz, jehož všechny členy jsou druhého řádu, protože pouze vynulování takového homogenního výrazu bude mít pro homogenní souřadnice bodu smysl nezávisle na zvoleném konstantním násobku souřadnic $(x_0, x_1, \ldots, x_n)$. Hledáme tedy takový výraz, jehož zúžením na afinní souřadnice, tj. dosazením $x_0 = 1$, získáme původní výraz z (4.4).

To je ale mimořádně jednoduché, prostě dopíšeme dostatek $x_0$ ke všem výrazům – žádný ke kvadratickým členům, jedno k lineárním a $x_0^2$ ke konstantnímu členu v původní afinní rovnici pro $Q$.

Získáme tak dobře definovanou kvadratickou formu $f$ na vektorovém prostoru $\mathbb{R}^{n+1}$, jejíž nulové body korektně definují tzv. *projektivní kvadriku* $\tilde{Q}$.

Průnik „kužele“ $\tilde{Q} \subset \mathbb{R}^{n+1}$ nulových bodů této formy s afinní rovinou $x_0 = 1$ je původní kvadrika $Q$, jejíž body označujeme jako

Nyní můžeme dosadit například $t_2 = 3t_1 - 6t_3$ do předchozí (kvadratické) rovnice. Potom dostaneme

$$-t_1^2 + 4t_1t_3 - 3t_3^2 = 0.$$

Protože pro $t_3 = 0$ rovnice není splněna, můžeme přejít k nehomogenním souřadnicím $\left(\frac{t_1}{t_3}, \frac{t_2}{t_3}, 1\right)$, pro které dostáváme

$$-\left(\frac{t_1}{t_3}\right)^2 + 4\left(\frac{t_1}{t_3}\right) - 3 = 0 \quad \text{a} \quad \frac{t_2}{t_3} = 3\left(\frac{t_1}{t_3}\right) - 6,$$

tj. $\frac{t_1}{t_3} = 1$ a $\frac{t_2}{t_3} = -3$, nebo $\frac{t_1}{t_3} = 3$ a $\frac{t_2}{t_3} = 3$. Body dotyku tedy mají homogenní souřadnice $(1 : -3 : 1)$ a $(3 : 3 : 1)$. Rovnice tečen dostaneme jako poláry těchto bodů. Výsledné rovnice tečen jsou $7x - 2y - 13 = 0$ a $x = -3$. □

**4.65.** Napište rovnici tečny vedené počátkem ke kružnici zadané rovnicí

$$x^2 + y^2 - 10x - 4y + 25 = 0.$$

**Řešení.** Bod dotyku $(t_1 : t_2 : t_3)$ splňuje

$$(0, 0, 1)\begin{pmatrix} 1 & 0 & -5 \\ 0 & 1 & -2 \\ -5 & -2 & 25 \end{pmatrix}\begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix} = -5t_1 - 2t_2 + 25 = 0.$$

Odtud vyjádříme např. $t_2$ a dosadíme do rovnice kuželosečky (kružnice), kterou musí bod $(t_1 : t_2 : t_3)$ také splňovat. Dostaneme kvadratickou rovnici $29t_1^2 - 250t_1 + 525 = 0$, která má řešení $t_1 = 5$ a $t_1 = \frac{105}{29}$. Souřadnici $t_2$ dopočítáme a získáme body dotyku $[5, 0]$ a $\left[\frac{105}{29}, \frac{100}{29}\right]$. Hledané tečny jsou pak poláry těchto bodů. Ty mají rovnice $y = 0$ a $20x - 21y = 0$. □

**4.66.** Najděte rovnice tečen ke kružnici $x^2 + y^2 = 5$ rovnoběžných s přímkou $2x + y + 2 = 0$.

**Řešení.** V projektivním rozšíření se tyto tečny protínají v nevlastním bodě splňujícím $2x + y + z = 0$ tj. v bodě s homogenními souřadnicemi $(1 : -2 : 0)$. Jsou to tedy tečny spuštěné z tohoto bodu ke kružnici a postupovat můžeme stejně jako v předchozím příkladě. Matice kuželosečky (kružnice) je diagonální s diagonálou $(1, 1, -5)$, a proto bod dotyku $(t_1 : t_2 : t_3)$ hledaných tečen splňuje $t_1 - 2t_2 = 0$. Dosazením do rovnice kružnice dostaneme $5t_2^2 = 5$. Odtud máme $t_2 = \pm 1$ a body dotyku proto jsou $[2, 1]$ a $[-2, -1]$. □

Tečna v nevlastním bodě kuželosečky se nazývá *asymptota* kuželosečky. Počet asymptot kuželosečky se tedy rovná počtu průsečíků kuželosečky s přímkou nevlastních bodů, tj. elipsa nemá žádnou reálnou asymptotu, parabola má jednu (která je ovšem nevlastní přímkou) a hyperbola dvě.

vlastní body kvadriky, zatímco další body $\bar{Q} \setminus Q$ v projektivním rozšíření jsou body nevlastní.

Klasifikace reálných či komplexních projektivních kvadrik, až na projektivní transformace, je úlohou, kterou jsme již zvládli — jde prostě o nalezení kanonické polární báze, viz odstavec 4.29. Z této klasifikace dané v reálném případě signaturou formy, v komplexním pouze hodností, vcelku snadno můžeme dovodit i klasifikace kvadrik afinních. Stačí si všímat množiny nekonečných bodů v projektivním rozšíření naší afinní kvadriky. Ukážeme si podstatu postupu na případu kuželoseček v afinní a projektivní rovině.

Projektivní klasifikace dává následující možnosti, popsané v homogenních souřadnicích $(x : y : z)$ v projektivní rovině $\mathcal{P}\mathbb{R}^3$:

- imaginární regulární kuželosečka zadaná $x^2 + y^2 + z^2 = 0$,
- reálná regulární kuželosečka s rovnicí $x^2 + y^2 - z^2 = 0$,
- dvojice imaginárních přímek s rovnicí $x^2 + y^2 = 0$,
- dvojice reálných přímek s rovnicí $x^2 - y^2 = 0$,
- dvojnásobná přímka $x^2 = 0$.

Klasifikaci uvažujeme jako reálnou, tj. klasifikace kvadratických forem je dána nejen hodností, ale i signaturou, nicméně body kvadrik pak uvažujeme i v komplexním rozšíření. Tak je třeba chápat uvedené názvy, např. imaginární kuželosečka nemá žádné reálné body.

**4.43. Afinní klasifikace kvadrik.** Pro afinní klasifikaci musíme omezit projektivní transformace na ty, které zachovávají přímku nevlastních bodů. To ale můžeme také realizovat opačným postupem — pro zvolený projektivní typ kuželosečky $Q$, tj. její kužel $\tilde{Q} \subseteq \mathbb{R}^3$ budeme postupně různě volit afinní rovinu $\alpha \subseteq \mathbb{R}^3$ neprocházející počátkem a sledovat, jak se mění množina bodů $\tilde{Q} \cap \alpha$, které jsou v afinních souřadnicích realizovaných pomocí roviny $\alpha$ vlastními body $Q$.

V případě reálné regulární kuželosečky tedy máme k dispozici skutečný kužel $\tilde{Q}$ zadaný rovnicí $z^2 = x^2 + y^2$ a za rovinu $\alpha$ berme třebas tečné roviny jednotkové sféry. Začneme-li s rovinou $z = 1$, dostaneme jako průnik samé konečné body v ní ležící jednotkové kružnice $Q$. Postupným nakláněním $\alpha$ budeme dostávat protaženější a protaženější elipsy, až dosáhneme náklonu $\alpha$ rovnoběžného s jednou z přímek kužele. V tom okamžiku se již objeví jeden (dvojnásobný) nekonečný bod naší kuželosečky, jejíž konečné body ale stále tvoří jednu souvislou komponentu, a dostáváme parabolu parabola. Pokračováním nakláněni vzniknou nekonečné body dva a množina konečných bodů přestane být souvislá a tak dostáváme poslední regulární kvadriku v afinní klasifikaci, hyperbolu.

Z uvedeného postupu si můžeme vzít poučení, které nám snadno umožní pokračovat do vyšších dimenzí. Předně, si všimněme, že průnikem naší kuželosečky s projektivní přímkou nevlastních bodů je vždy opět kvadrika v dimenzi o jedničku nižší, tj. v našem případě šlo o prázdnou množinu nebo dvojnásobný bod nebo dva body jakožto typy kvadrik na projektivní přímce. Dále jsme zjistili, že afinní transformaci převádějící jednu z možných realizací zvoleného projektivního typu na druhou jsme našli jen tehdy, když příslušné kvadriky v nevlastní přímce byly projektivně ekvivalentní. Takovýmto způsobem lze pokračovat v klasifikaci kvadrik v dimenzi tři a dále.

**4.67.** Určete nevlastní body a asymptoty kuželosečky zadané rovnicí

$$4x^2 - 8xy + 3y^2 - 2y - 5 = 0.$$

**Řešení.** Nejprve napíšeme rovnici kuželosečky v homogenních souřadnicích:

$$4x^2 - 8xy + 3y^2 - 2yz - 5z^2 = 0.$$

Nevlastní body kuželosečky jsou pak body určené homogenními souřadnicemi $(x : y : 0)$ splňující tuto rovnici, to znamená

$$4x^2 - 8xy + 3y^2 = 0.$$

Pro podíl $\frac{x}{y}$ dostaneme dvě řešení: $\frac{x}{y} = -\frac{1}{2}$ a $\frac{x}{y} = -\frac{3}{2}$. Zadaná kuželosečka je tedy hyperbola s nevlastními body $P = (-1 : 2 : 0)$ a $Q = (-3 : 2 : 0)$. Asymptoty jsou potom poláry bodů $P$ a $Q$, tj.

$$(-1, 2, 0) \begin{pmatrix} 4 & -4 & 0 \\ -4 & 3 & -1 \\ 0 & -1 & -5 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = -12x + 10y - 2 = 0$$

a

$$(-3, 2, 0) \begin{pmatrix} 4 & -4 & 0 \\ -4 & 3 & -1 \\ 0 & -1 & -5 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = -20x + 18y - 2 = 0.$$

□

Další příklady na kuželosečky naleznete na straně 231.

**4.68. Harmonický dvojpoměr.** Je-li dvojpoměr čtyř bodů ležících na přímce roven $-1$, hovoříme o tzv. *harmonické čtveřici*. Harmonickou čtveřici lze snadno zkonstruovat: mějme čtyřúhelník $ABCD$. Označme $K$ průsečík přímek $AB$ a $CD$, $M$ průsečík přímek $AD$ a $BC$. Dále nechť $L$, resp. $N$, je průsečík přímky $KM$ s přímkou $AC$, resp. $BD$. Potom body $K$, $L$, $M$, $N$ tvoří harmonickou čtveřici.

### D. Doplňující příklady k celé kapitole

*4.69.* Parametricky vyjádřete průnik následujících rovin v $\mathbb{R}^3$:

$$\sigma : 2x + 3y - z + 1 = 0 \quad \text{a} \quad \rho : x - 2y + 5 = 0.$$ ○

*4.70.* Nalezněte osu mimoběžek:

$$p : [1, 1, 1] + t(2, 1, 0), \quad \text{a} \quad q : [2, 2, 0] + t(1, 1, 1).$$ ○

*4.71.* Určete příčku mimoběžek $p : [0, 1, 1] + t(1, 2, 3)$, $q : [0, 5, 5] + s(2, 1, 0)$, tj. body $P$ a $Q$, kde $P \in p$ a $Q \in q$, takové, že přímka $PQ$ prochází bodem $[-7, 7, 12]$. ○

*4.72.* Jarda stojí v bodě $[-1, 1, 0]$ a má tyč délky 4. Může se touto tyčí současně dotknout přímek $p$ a $q$, kde

$$\begin{aligned} p &: [0, -1, 0] + t(1, 2, 1), \\ q &: [3, 4, 8] + s(2, 1, 3)? \end{aligned}$$

(Tyč musí procházet bodem $[-1, 1, 0]$.) ○

*4.73.* Rozhodněte, za existuje úsečka $PQ$, kde $P \in p$, $Q \in q$, přičemž přímky $p$ a $q$ jsou dány vztahy

$$\begin{aligned} p &: [1, -1, 2] + t(1, 0, 1), \ t \in \mathbb{R}, \\ q &: [2, -3, 1] + s(-1, -1, 1), \ s \in \mathbb{R} \end{aligned}$$

a navíc bod $[0, 1, 3]$ leží na úsečce $PQ$. ○

*4.74.* V prostoru $\mathbb{R}^3$ je dána zrcadlová rovina $y = 0$. Určete délku dráhy, kterou urazí světelný paprsek při cestě z bodu $[1, 2, 3]$ odrazem o zrcadlovou rovinu do bodu $[2, 1, 2]$. ○

**4.75.** Ve vektorovém prostoru $\mathbb{R}^4$ spočtěte vzdálenost $v$ bodu $[0, 0, 6, 0]$ od vektorového podprostoru

$$U : [0, 0, 0, 0] + t_1 (1, 0, 1, 1) + t_2 (2, 1, 1, 0) + t_3 (1, -1, 2, 3) ,$$

$t_1, t_2, t_3 \in \mathbb{R}$

**Řešení.** Úlohu budeme řešit postupem založeným na tzv. problému nejmenších čtverců. Vektory generující $U$ napíšeme do sloupců matice

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & -1 \\ 1 & 1 & 2 \\ 1 & 0 & 3 \end{pmatrix}$$

a bod $[0, 0, 6, 0]$ nahradíme jemu odpovídajícím vektorem $b = (0, 0, 6, 0)^T$. Budeme řešit soustavu $A \cdot x = b$, tj. soustavu lineárních rovnic

$$\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & x_3 & = & 0, \\ & & x_2 & - & x_3 & = & 0, \\ x_1 & + & x_2 & + & 2x_3 & = & 6, \\ x_1 & & & + & 3x_3 & = & 0 \end{array}$$

právě metodou nejmenších čtverců. (Upozorněme, že tato soustava nemá řešení – jinak by vzdálenost byla rovna 0.) Systém $A \cdot x = b$ vynásobíme zleva maticí $A^T$. Rozšířená matice soustavy

$A^T \cdot A \cdot x = A^T \cdot b$ pak je

$$\left(\begin{array}{ccc|c} 3 & 3 & 6 & 6 \\ 3 & 6 & 3 & 6 \\ 6 & 3 & 15 & 12 \end{array}\right).$$

Pomocí elementárních řádkových transformací ji postupně převedeme na schodovitý tvar

$$\left(\begin{array}{ccc|c} 3 & 3 & 6 & 6 \\ 3 & 6 & 3 & 6 \\ 6 & 3 & 15 & 12 \end{array}\right) \sim \left(\begin{array}{ccc|c} 3 & 3 & 6 & 6 \\ 0 & 3 & -3 & 0 \\ 0 & -3 & 3 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 2 & 2 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Provedeme-li ještě zpětnou eliminaci

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & 2 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 3 & 2 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right),$$

můžeme ihned napsat řešení

$$x = (2 - 3t,\ t,\ t)^T, \quad t \in \mathbb{R}.$$

Dodejme, že existence nekonečně mnoha řešení je zapříčiněna nadbytečností třetího ze zadávajících vektorů podprostoru $U$, neboť je

$$3\,(1, 0, 1, 1) - (2, 1, 1, 0) = (1, -1, 2, 3)\,.$$

Libovolná ($t \in \mathbb{R}$) lineární kombinace

$$(2 - 3t)\,(1, 0, 1, 1) + t\,(2, 1, 1, 0) + t\,(1, -1, 2, 3) = (2, 0, 2, 2)$$

však odpovídá bodu $[2, 0, 2, 2]$ podprostoru $U$, který je nejblíže bodu $[0, 0, 6, 0]$. Pro hledanou vzdálenost proto platí
$v = ||\,[2, 0, 2, 2] - [0, 0, 6, 0]\,|| = \sqrt{2^2 + 0 + (-4)^2 + 2^2} = 2\sqrt{6}.$ □

**4.76.** V euklidovském prostoru $\mathbb{R}^5$ vypočtěte odchylku $\varphi$ podprostorů $U$, $V$, jestliže je

(a) $U : [3, 5, 1, 7, 2] + t\,(1, 0, 2, -2, 1)\,,\ t \in \mathbb{R}$,
$V : [0, 1, 0, 0, 0] + s\,(2, 0, -2, 1, -1)\,,\ s \in \mathbb{R}$;

(b) $U : [4, 1, 1, 0, 1] + t\,(2, 0, 0, 2, 1)\,,\ t \in \mathbb{R}$,
$V : x_1 + x_2 + x_3 + x_5 = 7$;

(c) $U : 2x_1 - x_2 + 2x_3 + x_5 = 3$,
$V : x_1 + 2x_2 + 2x_3 + x_5 = -1$;

(d) $U : [0, 1, 1, 0, 0] + t\,(0, 0, 0, 1, -1)\,,\ t \in \mathbb{R}$,
$V : [1, 0, 1, 1, 1] + r\,(1, -1, 2, 1, 0) + s\,(0, 1, 3, 2, 0) +$
$+ p\,(1, 0, 0, 1, 0) + q\,(1, 3, 1, 0, 0)\,,\ r, s, p, q \in \mathbb{R}$;

(e) $U : [0, 2, 5, 0, 0] + t\,(2, 1, 3, 5, 3) + s\,(0, 3, 1, 4, -2) +$
$+ r\,(1, 2, 4, 0, 3)\,,\ t, s, r \in \mathbb{R}$,
$V : [0, 0, 0, 0, 0] + p\,(-1, 1, 1, -5, 0) +$
$+ q\,(1, 5, 1, 13, -4)\,,\ p, q \in \mathbb{R}$;

(f) $U : [1, 1, 1, 1, 1] + t\,(1, 0, 1, 1, 1) + s\,(1, 0, 0, 1, 1)\,,\ t, s \in \mathbb{R}$,
$V : [1, 1, 1, 1, 1] + p\,(1, 1, 1, 1, 1) + q\,(1, 1, 0, 1, 1) +$
$+ r\,(1, 1, 0, 1, 0)\,,\ p, q, r \in \mathbb{R}$.

**Řešení.** Nejdříve připomeňme, že odchylka afinních podprostorů je definována jako odchylka jejich zaměření, a proto při počítání $\varphi$ nezohledňujeme posunutí vyjádřená přičtením bodu (příp. pravé strany soustav rovnic).

Varianta (a). Neboť oba podprostory $U$ a $V$ jsou jednodimenzionální, odchylka $\varphi \in [0, \pi/2]$ je dána vzorcem

$$\cos\varphi = \frac{|\,(1,0,2,-2,1)\cdot(2,0,-2,1,-1)\,|}{||\,(1,0,2,-2,1)\,||\cdot||\,(2,0,-2,1,-1)\,||} = \frac{5}{\sqrt{10}\cdot\sqrt{10}}.$$

Je tedy $\cos\varphi = 1/2$, tj. $\varphi = \pi/3$.

Varianta (b). Známe směrový vektor $(2, 0, 0, 2, 1)$ podprostoru $U$ a normálový vektor $(1, 1, 1, 0, 1)$ podprostoru $V$. Snadno můžeme stanovit úhel $\psi = \pi/3$, který svírají, a to ze vztahu

$$\cos\psi = \frac{(2,0,0,2,1)\cdot(1,1,1,0,1)}{||\,(2,0,0,2,1)\,||\cdot||\,(1,1,1,0,1)\,||} = \frac{3}{3\cdot 2}.$$

Nyní si stačí uvědomit, že je $\varphi = \pi/2 - \psi = \pi/6$ (odchylka $\varphi$ je doplňkem úhlu $\psi$).

Varianta (c). Nadroviny $U$ a $V$ jsou zadány pomocí normálových vektorů $u = (2, -1, 2, 0, 1)$ a $v = (1, 2, 2, 0, 1)$. Zřejmě je odchylka $\varphi$ rovna úhlu, který svírají přímky se směrovými vektory $u$ a $v$. Platí tudí (viz variantu (a))

$$\cos\varphi = \frac{|\,(2,-1,2,0,1)\cdot(1,2,2,0,1)\,|}{||\,(2,-1,2,0,1)\,||\cdot||\,(1,2,2,0,1)\,||} = \frac{1}{2}, \quad \text{tj.} \quad \varphi = \frac{\pi}{3}.$$

Varianta (d). Označme

$$u = (0, 0, 0, 1, -1)\,, \quad v_1 = (1, -1, 2, 1, 0)\,,$$
$$v_2 = (0, 1, 3, 2, 0)\,, \quad v_3 = (1, 0, 0, 1, 0)\,, \quad v_4 = (1, 3, 1, 0, 0)$$

a jako $p_u$ označme ortogonální projekci (kolmý průmět) vektoru $u$ do zaměření podprostoru $V$ (do vektorového podprostoru generovaného vektory $v_1, v_2, v_3, v_4$). Určíme-li $p_u$, ze vzorce

$$\cos\varphi = \frac{||\,p_u\,||}{||\,u\,||} \tag{4.2}$$

pak totiž obdržíme $\varphi \in [0, \pi/2]$. Víme, že

$$p_u = av_1 + bv_2 + cv_3 + dv_4 \quad \text{pro jisté hodnoty } a, b, c, d \in \mathbb{R}$$

a že má být

$$\langle\, p_u - u, v_1 \,\rangle = 0, \quad \langle\, p_u - u, v_2 \,\rangle = 0,$$
$$\langle\, p_u - u, v_3 \,\rangle = 0, \quad \langle\, p_u - u, v_4 \,\rangle = 0.$$

Odtud (dosazením za $p_u$) dostáváme systém lineárních rovnic

$$\begin{array}{rcrcrcrcl} 7a & + & 7b & + & 2c & & & = & 1, \\ 7a & + & 14b & + & 2c & + & 6d & = & 2, \\ 2a & + & 2b & + & 2c & + & d & = & 1, \\ & & 6b & + & c & + & 11d & = & 0. \end{array}$$

Řešením této soustavy je $(a, b, c, d) = (-8/19, 7/19, 13/19, -5/19)$, a tak

$$p_u = -\frac{8}{19}v_1 + \frac{7}{19}v_2 + \frac{13}{19}v_3 - \frac{5}{19}v_4 = (0, 0, 0, 1, 0)\,,$$
$$\cos\varphi = \frac{||\,(0, 0, 0, 1, 0)\,||}{||\,(0, 0, 0, 1, -1)\,||} = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}.$$

Je tedy $\varphi = \pi/4$.

Varianta (e). Stanovme průnik zaměření uvedených podprostorů. Vektor $(x_1, x_2, x_3, x_4, x_5)$ náleží do zaměření $U$, právě když je

$$(x_1, x_2, x_3, x_4, x_5) = t\,(2, 1, 3, 5, 3) + s\,(0, 3, 1, 4, -2) + r\,(1, 2, 4, 0, 3)$$

pro jistá $t, s, r \in \mathbb{R}$, a současně $(x_1, x_2, x_3, x_4, x_5) \in V$ (V je svým zaměřením) tehdy a jenom tehdy, když je

$$(x_1, x_2, x_3, x_4, x_5) = p\,(-1, 1, 1, -5, 0) + q\,(1, 5, 1, 13, -4)$$

pro jistá $p, q \in \mathbb{R}$. Hledejme proto taková $t, s, r, p, q \in \mathbb{R}$, aby platilo

$$\begin{aligned} &t\,(2, 1, 3, 5, 3) + s\,(0, 3, 1, 4, -2) + r\,(1, 2, 4, 0, 3) = \\ &= p\,(-1, 1, 1, -5, 0) + q\,(1, 5, 1, 13, -4) \qquad . \end{aligned}$$

Jedná se o homogenní soustavu rovnic, kterou můžeme řešit v maticovém zápisu její levé strany (při pořadí proměnných $t, s, r, p, q$)

$$\begin{pmatrix} 2 & 0 & 1 & 1 & -1 \\ 1 & 3 & 2 & -1 & -5 \\ 3 & 1 & 4 & -1 & -1 \\ 5 & 4 & 0 & 5 & -13 \\ 3 & -2 & 3 & 0 & 4 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 1 & 3 & 2 & -1 & -5 \\ 0 & 2 & 1 & -1 & -3 \\ 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Ukázalo se, že vektory zadávající podprostor $V$ jsou lineární kombinací vektorů ze zaměření podprostoru $U$. To ovšem znamená, že $V$ je podmnožinou zaměření $U$, a tudíž je $\varphi = 0$.

Varianta (f). Opět nalezněme průnik zaměření $U$ a $V$. Analogicky jako v předešlé variantě hledejme čísla $t, s, p, q, r \in \mathbb{R}$, pro která je

$$\begin{aligned} &t\,(1, 0, 1, 1, 1) + s\,(1, 0, 0, 1, 1) = \\ =&p\,(1, 1, 1, 1, 1) + q\,(1, 1, 0, 1, 1) + r\,(1, 1, 0, 1, 0)\,. \end{aligned}$$

Řešením této soustavy je $(t, s, p, q, r) = (-a, a, -a, a, 0)$, $a \in \mathbb{R}$. Do průniku $Z(U) \cap Z(V)$ zaměření $U$ a $V$ tak náleží právě vektory

$$\begin{aligned} (0, 0, -a, 0, 0) &= -a\,(1, 0, 1, 1, 1) + a\,(1, 0, 0, 1, 1) = \\ &= -a\,(1, 1, 1, 1, 1) + a\,(1, 1, 0, 1, 1) + 0\,(1, 1, 0, 1, 0)\,, \end{aligned}$$

kde $a \in \mathbb{R}$, tj. $Z(U) \cap Z(V)$ je podprostorem generovaným vektorem $(0, 0, 1, 0, 0)$ a jeho ortogonální doplněk $(Z(U) \cap Z(V))^\perp$ je zjevně generován vektory

$$(1, 0, 0, 0, 0)\,, \quad (0, 1, 0, 0, 0)\,, \quad (0, 0, 0, 1, 0)\,, \quad (0, 0, 0, 0, 1)\,.$$

Zvláště dostáváme

$$Z(U) \cap Z(V) \neq \{0\}, \quad Z(U) \cap Z(V) \neq Z(U), \quad Z(U) \cap Z(V) \neq Z(V).$$

Odchylka $\varphi$ je tedy definována jako odchylka podprostorů

$$Z(U) \cap (Z(U) \cap Z(V))^\perp \quad \text{a} \quad Z(V) \cap (Z(U) \cap Z(V))^\perp.$$

Dále je vidět, že je

$$\begin{aligned} &Z(U) \cap (Z(U) \cap Z(V))^\perp = \langle\,(1, 0, 0, 1, 1)\,\rangle\,, \\ &Z(V) \cap (Z(U) \cap Z(V))^\perp = \langle\,(1, 1, 0, 1, 1)\,, (1, 1, 0, 1, 0)\,\rangle\,. \end{aligned}$$

Postačuje totiž vyjádřit $Z(U)$ jako lineární kombinaci vektorů

$$(0, 0, 1, 0, 0)\,, \quad (1, 0, 0, 1, 1)$$

a podprostor $Z(V)$ pomocí vektorů

$$(0, 0, 1, 0, 0)\,, \quad (1, 1, 0, 1, 1)\,, \quad (1, 1, 0, 1, 0)\,.$$

Protože dimenze prostoru $Z(U) \cap (Z(U) \cap Z(V))^{\perp}$ je 1, můžeme použít vzorec (‖4.2‖), kde $u = (1,0,0,1,1)$ a $p_u$ je kolmá projekce $u$ do $Z(V) \cap (Z(U) \cap Z(V))^{\perp}$. Má být

$$p_u = a\,(1,1,0,1,1) + b\,(1,1,0,1,0)$$

a má platit

$$\langle\, p_u - u, (1,1,0,1,1)\,\rangle = 0, \quad \langle\, p_u - u, (1,1,0,1,0)\,\rangle = 0,$$

což vede na soustavu rovnic

$$\begin{array}{rcrcl} 4a & + & 3b & = & 3, \\ 3a & + & 3b & = & 2 \end{array}$$

s jediným řešením $a = 1, b = -1/3$. Tímto jsme určili

$$p_u = \left(\tfrac{2}{3}, \tfrac{2}{3}, 0, \tfrac{2}{3}, 1\right)$$

a z (‖4.2‖) již plyne

$$\cos\varphi = \frac{\|\,(2/3,2/3,0,2/3,1)\,\|}{\|\,(1,0,0,1,1)\,\|} = \frac{\sqrt{7}}{3}, \quad \text{tj.} \quad \varphi \doteq 0,49 \ \ (\approx 28\,^\circ). \qquad \square$$

*4.77.* Je dána krychle $ABCDEFGH$. Nechť bod $T$ leží na hraně $BF$, $|BT| = \frac{1}{4}|BF|$. Určete kosinus odchylky rovin $ATC$ a $BDE$. ◯

*4.78.* Je dána krychle $ABCDEFGH$. Nechť bod $T$ leží na hraně $AE$, $|AT| = \frac{1}{4}|AE|$ a $S$ je střed strany $AD$. Určete kosinus odchylky rovin $BDT$ a $SCH$. ◯

*4.79.* Je dána krychle $ABCDEFGH$. Nechť bod $T$ leží na hraně $BF$, $|BT| = \frac{1}{3}|BF|$. Určete kosinus odchylky rovin $ATC$ a $BDE$. ◯

**4.80.** Určete tečnu k elipse $\frac{x^2}{16} + \frac{y^2}{9} = 1$ rovnoběžnou s přímkou $x + y - 7 = 0$.

**Řešení.** Rovnoběžky s danou přímkou se s ní protínají v nevklastním bodě $(1 : -1 : 0)$. Z tohoto bodu spustíme tečny k dané elipse. Bod dotyku T$= (t_1 : t_2 : t_3)$ leží na jeho poláře, a proto splňuje $\frac{t_1}{16} - \frac{t_2}{9} = 0$, tj. $t_2 = \frac{9}{16}t_1$. Dosazením do rovnice elipsy pak dostáváme $t_1 = \pm\frac{16}{5}$. Body dotyku hledaných tečen tak jou $\left[\frac{16}{5}, \frac{9}{5}\right]$ a $\left[-\frac{16}{5}, -\frac{9}{5}\right]$. Tečny jsou pak poláry těchto bodů. Ty mají rovnice $x + y = 5$ a $x + y = -5$. $\square$

**4.81.** Určete nevlastní body a asymptoty kuželosečky zadané rovnicí

$$2x^2 + 4xy + 2y^2 - y + 1 = 0.$$

**Řešení.** Rovnice nevlastních bodů $2x^2 + 4xy + 2y^2 = 0$, tj. $2(x + y)^2 = 0$ má řešení $x = -y$. Jediným nevlastním bodem je tedy $(1 : -1 : 0)$ (daná kuželosečka je parabola). Asymptota je polára tohoto bodu a tou je nevlastní přímka $z = 0$ (jedná se tedy o parabolu). $\square$

**4.82.** Dokažte, že součin vzdáleností bodu libovolného bodu hyperboly od jejích asymptot je konstantní a určete velikost této konsatnty.

**Řešení.** Označme bod na hyperbole $P$. Rovnice asymptot hyperboly v kanonickém tvaru je $bx \pm ay = 0$. Jejich normály jsou tedy $(b, \pm a)$ a odtud určíme průměty $P_1, P_2$ bodu $P$ na asymptoty. Pro vzdálenost bodu $P$ od asymptot pak dostáváme $|PP_{1,2}| = \frac{|aq \pm bp|}{\sqrt{a^2+b^2}}$. Hledaný součin je tedy roven $\frac{a^2q^2 - b^2p^2}{a^2+b^2} = \frac{a^2b^2}{a^2+b^2}$, protože bod $P$ leží na hyperbole. $\square$

**4.83.** Určete úhel asymptot hyperboly $3x^2 - y^2 = 3$.

**Řešení.** Pro kosinus úhlu, který svírají asymptoty hyperboly v kanonickém tvaru lze odvodir $\cos\alpha = \frac{b^2-a^2}{b^2+a^2}$. V našem případě tak dostáváme úhel 60°. $\square$

**4.84.** Určete středy kuželoseček:

(a) $9x^2 + 6xy - 2y - 2 = 0$,

(b) $x^2 + 2xy + y^2 + 2x + y + 2 = 0$,

(c) $x^2 - 4xy + 4y^2 + 2x - 4y - 3 = 0$,

(d) $\frac{(x-\alpha)^2}{a^2} + \frac{(y-\beta)^2}{b^2} = 1$.

**Řešení.** (a) Soustava $\bar{A}s + a = 0$ pro výpočet vlastních středů má tvar

$$\begin{array}{rcrcrcl} 9s_1 & + & 3s_2 & & & = & 0, \\ 3s_1 & & & - & 2 & = & 0 \end{array}$$

a jejím vyřešením dostaneme střed $\left[\frac{2}{3}, -2\right]$.

(b) V tomto případě máme

$$\begin{array}{rcrcrcl} s_1 & + & s_2 & + & 1 & = & 0, \\ s_1 & + & s_2 & + & \frac{1}{2} & = & 0, \end{array}$$

a proto žádný vlastní střed neexistuje (kuželosečka je parabola). Pokud přejdeme do homogenních souřadnic, dostaneme nevlastní střed $(1 : -1 : 0)$.

(c) Souřadnice středu v tomto případě splňují

$$\begin{array}{rcrcrcl} s_1 & - & 2s_2 & + & 1 & = & 0, \\ -2s_1 & + & 4s_2 & - & 2 & = & 0 \end{array}$$

a řešením je tedy celá přímka středů. Je to proto, že kuželosečka je degenerovaná do dvojice rovnoběžných přímek.

(d) Z rovnic pro výpočet středu okamžitě plyne, že středem je $(\alpha, \beta)$. Souřadnice středu tedy udávájí posunutí počátku souřadnic k repéru, ve kterém má elipsa základní tvar. □

**4.85.** Určete rovnice os kuželosečky dané rovnicí $6xy + 8y^2 + 4y + 2x - 13 = 0$.

**Řešení.** Hlavní směry kuželosečky (směrové vektory os) jsou vlastní vektory matice $\begin{pmatrix} 0 & 3 \\ 3 & 8 \end{pmatrix}$. Charakteristická rovnice má tvar $\lambda^2 - 8\lambda - 9 = 0$ a vlastní čísla jsou proto $\lambda_1 = -1, \lambda_2 = 9$. Příslušné vlastní vektory jsou pak $(3, -1)$ a $(1, -3)$. Osy jsou polárami nevlastních bodů určených těmito směry. Pro $(3, -1)$ tak dostáváme rovnici osy $-3x + y + 1 = 0$ a pro $(1, -3)$ osu $-9x - 21y - 5 = 0$. □

**4.86.** Určete rovnice os kuželosečky dané rovnicí $4x^2 + 4xy + y^2 + 2x + 6y + 5 = 0$.

**Řešení.** Vlastní čísla matice $\begin{pmatrix} 4 & 2 \\ 2 & 1 \end{pmatrix}$ jsou $\lambda_1 = 0, \lambda_2 = 5$ a příslušné vlastní vektory $(-1, 2)$ a $(2, 1)$. Pro osy pak dostáváme rovnice $5 = 0$ a $2x + y + 1 = 0$. První z nich očividně není splněna pro žádný bod. Existuje tedy jen jedna osa (zadaná kuželosečka je parabola). □

## Řešení cvičení

*4.9.* 2, 3, 4, 6, 7, 8. Polohy rovin, které realizují dané počty si rozmyslete samostatně.

*4.30.* Pro normálový vektor $(a, b, c)$ hledaných rovin máme rovnice $a + b = 0$ (kolmost na $p$) a volbou $a = -b = 1$ (vektor $(0, 0, 1)$ nevyhovuje podmínkám, takže vhodným pronásobením můžeme dosáhnout podmínky $a = -b = 1$) pak dostáváme z podmínky pro odchylku $\left|\frac{c}{\sqrt{3}\sqrt{2+c^2}}\right| = \frac{1}{2}$, celkem pak hledané rovnice přímek jsou $x - y \pm \sqrt{6} - 1 = 0$.

*4.69.* Přímka $(2t, t, 7t) + [-5, 0, -9]$.

*4.70.* $[3, 2, 1][8/3, 8/3, 2/3]$.

*4.71.* $P = [-1, -1, -2]$, $Q = [-4, 3, 5]$.

*4.72.* Příčka $[1, 1, 1][-3, 1, -1]$, délky $\sqrt{20}$, tyč stačit nebude.

*4.73.* Neexistuje. Přímka procházející daným bodem a protínající jak $p$ tak $q$ je daná body $P = [1, -1, 2]$ $(\in p)$ a $Q = [2, -3, 1]$ $(\in q)$. Daný bod však na úsečce $PQ$ neleží.

*4.74.* $\sqrt{11}$.

*4.77.* $\frac{2\sqrt{6}}{9}$.

*4.78.* $\frac{\sqrt{3}}{6}$.

*4.79.* $\frac{\sqrt{3}}{\sqrt{11}}$.

KAPITOLA 5

# Zřízení ZOO funkcí

*jaké funkce potřebujeme pro naše modely?*
*– pořádný zvěřinec...*



## A. Interpolace polynomy

Na úvod této kapitoly se budeme snažit odhadnout funkce pomocí polynomů. Předpokládejme, že o neznámé funkci máme pouze kusé informace, totiž její hodnoty v několika bodech, popřípadě i hodnoty její první či druhé derivace v těchto bodech. Budeme se snažit najít polynom (co nejmenšího stupně) splňující tyto závislosti.

**5.1.** Nalezněte polynom $P$ splňující následující podmínky:



$$P(2) = 1,\ P(3) = 0,\ P(4) = -1,\ P(5) = 6$$

.

**Řešení.** Řešme příklad nejprve sestavením soustavy čtyř lineárních rovnic o čtyřech neznámých. Předpokládáme polynom ve tvaru $a_3x^3 + + a_2x^2 + a_1x_1 + a_0$. Víme, že polynom stupně nejvýše tři splňující

V této kapitole začneme budovat nástroje umožňujících modelování závislostí, které nejsou ani lineární ani diskrétní. S takovou potřebou se často setkáme, když popisujeme systém vyvíjející se v čase a to ne jen v několika vybraných okamžicích, ale „souvisle“, tj. pro všechny možné okamžiky. Někdy je to přímo záměr či potřeba (třeba ve fyzikálních modelech klasické mechaniky), jindy je to vhodné přiblížení diskrétního modelu (třeba u ekonomických, chemických nebo biologických modelů).

Klíčovým pojmem budou stále funkce. Čím větší třídu funkcí připustíme, tím obtížnější bude vybudovat nástroje pro naši práci. Když ale bude různých typů funkcí málo, nebudeme patrně umět budovat dobré modely pro reálné situace vůbec. Cílem následujících dvou kapitol bude proto explicitně zavést několik typů elementárních funkcí, implicitně popsat daleko více funkcí a vybudovat standardní nástroje pro práci s nimi. Souhrnně se tomu říká diferenciální a integrální počet jedné proměnné. Zatímco dosud jsme se spíše pohybovali v oblasti matematiky nazývané *algebra*, nyní se budeme postupně blížit k tzv. *matematické analýze*.

## 1. Interpolace polynomy

V předchozích kapitolách jsme pracovali často s posloupnostmi hodnot reálných nebo komplexních čísel, tj. se skalárními funkcemi $\mathbb{N} \to \mathbb{K}$ nebo $\mathbb{Z} \to \mathbb{K}$, kde $\mathbb{K}$ byl zvolený číselný obor. Případně jsme pracovali s posloupnostmi vektorů nad reálnými nebo komplexními čísly.

Připomeňme si diskusi z odstavce 1.4, kde jsme přemýšleli nad způsoby, jak pracovat se skalárními funkcemi. Na této diskusi není třeba nic doplňovat a rádi bychom (pro začátek) uměli pracovat s funkcemi $\mathbb{R} \to \mathbb{R}$ (*reálné funkce reálné proměnné*) nebo $\mathbb{R} \to \mathbb{C}$ (*komplexní funkce reálné proměnné*), případně funkcemi $\mathbb{Q} \to \mathbb{Q}$ (funkce jedné racionální proměnné s racionálními hodnotami) apod. Většinou půjdou naše závěry snadno rozšířit na případy s vektorovými hodnotami nad stejnými skaláry, ve výkladu se ale zpravidla omezíme jen na případ reálných a komplexních čísel.

Začneme od nejednodušších funkcí, které umíme zadat explicitně pomocí konečně mnoha algebraických operací se skaláry.

**5.1. Polynomy.** Skaláry umíme sčítat a násobit a tyto operace



splňují řadu vlastností, které jsme vyjmenovali už v odstavcích 1.1 a 1.3. Když připustíme konečný počet těchto operací, přičemž jednu proměnnou ponecháme jako neznámou a další vstupující skaláry budou pevně zvolené, dostáváme tzv. polynomy:

podmínky v zadání je dán jednoznačně.

$$\begin{array}{rcrcrcrcr} a_0 & + & 2a_1 & + & 4a_2 & + & 8a_3 & = & 1, \\ a_0 & + & 3a_1 & + & 9a_2 & + & 27a_3 & = & 0, \\ a_0 & + & 4a_1 & + & 16a_2 & + & 64a_3 & = & -1, \\ a_0 & + & 5a_1 & + & 25a_2 & + & 125a_3 & = & 6. \end{array}$$

Každá rovnice vznikla z jedné z podmínek v zadání.

Druhou možností řešení je vytvořit hledaný polynom pomocí fundamentálních Lagrangeových polynomů (viz 5.4):

$$\begin{aligned} P(x) &= 1 \cdot \frac{(x-3)(x-4)(x-5)}{(2-3)(2-4)(2-5)} + 0 \cdot (\dots) + \\ &\quad + (-1) \cdot \frac{(x-2)(x-3)(x-5)}{(4-2)(4-3)(4-5)} + \\ &\quad + 6 \cdot \frac{(x-2)(x-3)(x-4)}{(5-2)(5-3)(5-4)} = \\ &= \frac{4}{3}x^3 - 12x^2 + \frac{101}{3}x - 29. \end{aligned}$$

Koeficienty tohoto polynomu jsou samozřejmě jediným řešením výše sestavené soustavy lineárních rovnic. □

*5.2.* Nalezněte polynom $P$ splňující následující podmínky:

$$P(1+i) = i,\ P(2) = 1,\ P(3) = -i.$$ ○

**5.3.** Pro navzájem různé body $x_0, \dots, x_n \in \mathbb{R}$ uvažme elementární Lagrangeovy polynomy (5.4)

$$l_i(x) := \frac{(x-x_0)\cdots(x-x_{i-1})\,(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_0)\cdots(x_i-x_{i-1})\,(x_i-x_{i+1})\cdots(x_i-x_n)},$$

kde $x \in \mathbb{R}$, $i = 0, \dots, n$. Dokažte, že platí

$$\sum_{i=0}^{n} l_i(x) = 1 \text{ pro všechna } x \in \mathbb{R}.$$

**Řešení.** Zřejmě je

$$\begin{aligned} \sum_{i=0}^{n} l_i(x_0) &= 1 + 0 + \dots + 0 = 1, \\ \sum_{i=0}^{n} l_i(x_1) &= 0 + 1 + \dots + 0 = 1, \\ &\vdots \\ \sum_{i=0}^{n} l_i(x_n) &= 0 + 0 + \dots + 1 = 1. \end{aligned}$$

To znamená, že polynom $\sum_{i=0}^{n} l_i(x)$ stupně nejvýše $n$ nabývá v $n+1$ bodech $x_0, \dots, x_n$ stejné hodnoty 1. Takový polynom (stupně nejvýše $n$) však existuje právě jeden, a to konstantní polynom $y \equiv 1$. □

### Polynomy

*Polynomem* nad okruhem skalárů $\mathbb{K}$ rozumíme zobrazení $f : \mathbb{K} \to \mathbb{K}$ dané výrazem

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0,$$

kde $a_i$, $i = 0, \dots, n$, jsou pevně zadané skaláry, násobení je znázorněno prostým zřetězením symbolů a „+“ označuje sčítání. Pokud je $a_n \neq 0$, říkáme, že polynom $f$ je *stupně* $n$. Stupeň nulového polynomu není definován. Skaláry $a_i$ označujeme jako *koeficienty polynomu* $f$.

Polynomy stupně nula jsou právě konstantní nenulová zobrazení $x \mapsto a_0$. V algebře jsou častěji polynomy definovány jako formální výrazy uvedeného tvaru $f(x)$, tj. jako posloupnosti koeficientů $a_0, a_1, \dots$ s konečně mnoha nenulovými prvky. Vzápětí si ale ukážeme, že v analýze budou oba přístupy ekvivalentní.

Je snadné ověřit, že polynomy nad okruhem skalárů tvoří opět okruh, kde násobení a sčítání je dáno operacemi v původním okruhu $\mathbb{K}$ pomocí hodnot polynomů, tzn.

$$(f \cdot g)(x) = f(x) \cdot g(x), \quad (f+g)(x) = f(x) + g(x),$$

kde nalevo a napravo musíme správně interpretovat příslušné operace v okruhu polynomů a v samotném okruhu skalárů.

**5.2. Dělení polynomů se zbytkem.** Jak jsme již zmínili, budeme v dalším pracovat výhradně s poli skalárů $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$. Pro všechna pole skalárů však platí

**Tvrzení** (O dělení polynomů se zbytkem)**.** *Pro libovolné polynomy $f$ stupně $n$ a $g$ stupně $m$, existují jednoznačně určené polynomy $q$ a $r$ takové, že $f = q \cdot g + r$ a přitom je stupeň $r$ menší než $m$ nebo je $r = 0$.*



Důkaz. Začněme jednoznačností. Předpokládejme, že máme dvě požadovaná vyjádření polynomu $f$ s polynomy $g$, $g'$, $r$ a $r'$, tj. platí

$$f = q \cdot g + r = q' \cdot g + r'.$$

Pak také odečtením dostaneme $0 = (q - q') \cdot g + (r - r')$.

Jestliže $q = q'$, pak také $r = r'$. Je-li $q \neq q'$, pak člen s nejvyšším stupněm v $(q - q') \cdot g$ nemůže být vykompenzován $r - r'$, což vede na spor. Dokázali jsme tedy jednoznačnost výsledku dělení, pokud existuje.

Zbývá dokázat, že umíme polynom $f$ vždy napsat požadovaným způsobem. Pokud by stupeň $g$ byl větší než stupeň $f$, pak můžeme rovnou psát $f = 0 \cdot g + f$. Předpokládejme proto $n \geq m$ a dokažme tvrzení indukcí přes stupeň $f$.

Pokud je $f$ polynom stupně nula, je tvrzení zřejmé. Předpokládejme tedy, že tvrzení platí pro stupně menší než $n > 0$ a uvažme výraz $h(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$. Buď je $h(x)$ přímo nulový polynom a pak máme, co jsme hledali, nebo jde o polynom nižšího stupně a tedy jej již umíme napsat potřebným způsobem $h(x) = q \cdot g + r$ a tedy také

$$f(x) = h(x) + \frac{a_n}{b_m} x^{n-m} g(x) = (q + \frac{a_n}{b_m} x^{n-m}) g(x) + r$$

a tvrzení je dokázáno. □

Je-li pro nějaký prvek $b \in \mathbb{K}$ hodnota $f(b) = 0$, pak to znamená, že v podílu $f(x) = q(x)(x-b) + r$ musí být $r = 0$. Jinak by totiž nebylo možné dosáhnout $f(b) = q(b) \cdot 0 + r$, kde stupeň $r$ je

**5.4.** Nalezněte polynom $P$ splňující následující podmínky:

$$P(1) = 0,\ P'(1) = 1,\ P(2) = 3,\ P'(2) = 3.$$

**Řešení.** Opět ukážeme dvě možnosti řešení.

Dané podmínky určují čtyři lineární rovnice pro koeficienty hledaného polynomu. Budeme-li hledat polynom třetího stupně, dostáváme tedy přesně tolik rovnic, kolik je neznámých koeficientů polynomu (nechť např. $P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$):

$$\begin{array}{rcrcrcrcl} P(1) &=& a_3 &+& a_2 &+& a_1 &+& a_0 &=& 0,\\ P'(1) &=& 3a_3 &+& 2a_2 &+& a_1 & & &=& 1,\\ P(2) &=& 8a_3 &+& 4a_2 &+& 2a_1 &+& a_0 &=& 3,\\ P'(2) &=& 12a_3 &+& 4a_2 &+& a_1 & & &=& 3. \end{array}$$

Vyřešením tohoto systému obdržíme polynom:

$$P(x) = -2x^3 + 10x^2 - 13x + 5.$$

**Jiné řešení**. Použijeme fundamentální Hermiteovy polynomy:

$$\begin{aligned} h_1^1(x) &= \left(1 - \frac{2}{0+(-1)}(x-1)\right)(2-x)^2 = (2x-1)(x-2)^2,\\ h_2^1(x) &= (5-2x)(x-1)^2,\\ h_1^2(x) &= (x-1)(x-2)^2,\\ h_2^2(x) &= (x-2)(x-1)^2. \end{aligned}$$

Celkem

$$\begin{aligned} P(x) &= 0\cdot h_1^1(x) + 3\cdot h_2^1(x) + 1\cdot h_1^2(x) + 3\cdot h_2^2(x) =\\ &= -2x^3 + 10x^2 - 13x + 5. \end{aligned}$$

□

**5.5.** Pomocí Lagrangeovy interpolace spočítejte přibližnou hodnotu $\cos^2 1$. Použijte k tomu hodnoty funkce v bodech $\frac{\pi}{4}$, $\frac{\pi}{3}$ a $\frac{\pi}{2}$.

**Řešení.** Nejprve určíme funkční hodnoty v zadaných bodech: $\cos^2(\frac{\pi}{4}) = 1/2$, $\cos^2(\frac{\pi}{3}) = 1/4$, $\cos^2(\frac{\pi}{2}) = 0$. Dále určíme elementární Lagrangeovy polynomy, přitom můžeme spočítat hodnoty přímo v zadaném bodě:

$$\begin{aligned} l_0(1) &= \frac{\left(1-\frac{\pi}{3}\right)\left(1-\frac{\pi}{2}\right)}{\left(\frac{\pi}{4}-\frac{\pi}{3}\right)\left(\frac{\pi}{4}-\frac{\pi}{2}\right)} = 8\frac{(\pi-3)(\pi-2)}{\pi^2},\\ l_1(1) &= \frac{\left(1-\frac{\pi}{4}\right)\left(1-\frac{\pi}{2}\right)}{\left(\frac{\pi}{3}-\frac{\pi}{4}\right)\left(\frac{\pi}{3}-\frac{\pi}{2}\right)} = -9\frac{(\pi-4)(\pi-2)}{\pi^2},\\ l_2(1) &= \frac{\left(1-\frac{\pi}{4}\right)\left(1-\frac{\pi}{3}\right)}{\left(\frac{\pi}{2}-\frac{\pi}{4}\right)\left(\frac{\pi}{2}-\frac{\pi}{3}\right)} = 2\frac{(\pi-4)(\pi-3)}{\pi^2}. \end{aligned}$$

Celkem tedy

$$\begin{aligned} P(1) &= \frac{1}{2}\cdot 8\frac{(\pi-3)(\pi-2)}{\pi^2} - \frac{1}{4}\cdot 9\frac{(\pi-4)(\pi-2)}{\pi^2} + 0 =\\ &= \frac{(7\pi-12)(\pi-2)}{4\pi^2} \doteq 0{,}288913. \end{aligned}$$

nulový. Říkáme, že $b$ je *kořen polynomu* $f$. Stupeň $q$ je pak právě $n-1$. Pokud má $q$ opět kořen, můžeme pokračovat a po nejvýše $n$ krocích dojdeme ke konstantnímu polynomu. Dokázali jsme tedy, že každý nenulový polynom nad polem $\mathbb{K}$ má nejvýše tolik kořenů, kolik je jeho stupeň. Odtud již snadno dovodíme i následující pozorování:

**Důsledek.** *Je-li $\mathbb{K}$ pole s nekonečně mnoha prvky, pak dva polynomy $f$ a $g$ jsou si rovny jako zobrazení, právě když mají shodné koeficienty.*

Důkaz. Předpokládejme $f = g$, tj. $f - g = 0$, jako zobrazení. Polynom $(f-g)(x)$ tedy má nekonečně mnoho kořenů, což je možné pouze tehdy, je-li nulovým polynomem. □

Uvědomme si, že u konečných polí samozřejmě takové tvrzení neplatí. Jednoduchým příkladem je např. polynom $x^2 + x$ nad $\mathbb{Z}_2$, který představuje nulové zobrazení.

**5.3. Interpolační polynom.** Často je užitečné zadat snadno počítatelný vztah pro funkci, pro kterou máme zadány hodnoty v předem daných bodech $x_0, \ldots, x_n$. Pokud by šlo o nulové hodnoty, umíme přímo zadat polynom stupně $n+1$



$$f(x) = (x-x_0)(x-x_1)\ldots(x-x_n),$$

který bude mít nulové hodnoty právě v těchto bodech a nikde jinde. To ale není jediná polynomiální odpověď, protože požadovanou vlastnost má i nulový polynom. Ten je přitom jediný s touto vlastností ve vektorovém prostoru polynomů stupně nejvýše $n$. Obdobně to dopadne i v obecném případě:

Interpolační polynomy

Nechť $\mathbb{K}$ je nekonečné pole skalárů. *Interpolační polynom* $f$ pro množinu po dvou různých bodů $x_0, \ldots, x_n \in \mathbb{K}$ a předepsaných hodnot $y_0, \ldots, y_n \in \mathbb{K}$ je polynom stupně nejvýše $n$ nebo nulový polynom, který splňuje $f(x_i) = y_i$ pro všechna $i = 0, 1, \ldots, n$.

**Věta.** *Pro každou množinu $n+1$ po dvou různých bodů $x_0, \ldots, x_n \in \mathbb{K}$ a předepsaných hodnot $y_0, \ldots, y_n \in \mathbb{K}$ existuje právě jeden interpolační polynom $f$.*

Důkaz. Začněme jednodušší částí, tj. jednoznačností. Jsou-li $f$ a $g$ dva interpolační polynomy se stejnými definičními hodnotami, pak je jejich rozdíl polynomem stupně $n$, který má $n+1$ kořenů, a proto je $f - g = 0$.



Zbývá existence. Označme si prozatím neznámé koeficienty polynomu $f$ stupně $n$

$$f = a_nx^n + \cdots + a_1x + a_0.$$

Dosazením požadovaných hodnot dostaneme systém $n+1$ rovnic pro stejný počet neznámých koeficientů $a_i$

$$\begin{aligned} a_0 + x_0a_1 + \cdots + (x_0)^n a_n &= y_0,\\ &\vdots\\ a_0 + x_na_1 + \cdots + (x_n)^n a_n &= y_n. \end{aligned}$$

Vidíme, že při výpočtu třetí elementární polynom nebyl potřeba. Skutečná hodnota je $\cos^2 1 \doteq 0{,}291927$. □

**5.6.** Franta potřebuje počítat hodnoty funkce sin, ale má k dispozici jen mobilní telefon s jednoduchou kalkulačkou, která umí základní operace. Protože si pamatuje hodnoty funkce sin v bodech 0, $\frac{\pi}{6}$, $\frac{\pi}{4}$ $\frac{\pi}{3}$ a $\frac{\pi}{2}$ a ví, že přibližné hodnoty $\pi$, $\sqrt{2}$ a $\sqrt{3}$ jsou 3,1416, 1,4142 a 1,7321, rozhodl se, že použije k přibližnému výpočtu interpolaci. Pomozte mu sestrojit přibližný vztah s využitím všech hodnot.

**Řešení.** Sestrojíme elementární Lagrangeovy polynomy:

$$\begin{aligned}
l_0(x) &= \frac{\left(x-\frac{\pi}{6}\right)\left(x-\frac{\pi}{4}\right)\left(x-\frac{\pi}{3}\right)\left(x-\frac{\pi}{2}\right)}{\left(0-\frac{\pi}{6}\right)\left(0-\frac{\pi}{4}\right)\left(0-\frac{\pi}{3}\right)\left(0-\frac{\pi}{2}\right)} \doteq \\
&\doteq 1{,}4783x^4 - 5{,}8052x^3 + 8{,}1057x^2 - 4{,}7746x + 1, \\
l_1(x) &= \frac{(x-0)\left(x-\frac{\pi}{4}\right)\left(x-\frac{\pi}{3}\right)\left(x-\frac{\pi}{2}\right)}{\left(\frac{\pi}{6}-0\right)\left(\frac{\pi}{6}-\frac{\pi}{4}\right)\left(\frac{\pi}{6}-\frac{\pi}{3}\right)\left(\frac{\pi}{6}-\frac{\pi}{2}\right)} \doteq \\
&\doteq -13{,}3046x^4 + 45{,}2808x^3 - 49{,}2419x^2 + 17{,}1887x, \\
l_2(x) &= \frac{(x-0)\left(x-\frac{\pi}{6}\right)\left(x-\frac{\pi}{3}\right)\left(x-\frac{\pi}{2}\right)}{\left(\frac{\pi}{4}-0\right)\left(\frac{\pi}{4}-\frac{\pi}{6}\right)\left(\frac{\pi}{4}-\frac{\pi}{3}\right)\left(\frac{\pi}{4}-\frac{\pi}{2}\right)} \doteq \\
&\doteq 23{,}6526x^4 - 74{,}3070x^3 + 71{,}3298x^2 - 20{,}3718x, \\
l_3(x) &= \frac{(x-0)\left(x-\frac{\pi}{6}\right)\left(x-\frac{\pi}{4}\right)\left(x-\frac{\pi}{2}\right)}{\left(\frac{\pi}{3}-0\right)\left(\frac{\pi}{3}-\frac{\pi}{6}\right)\left(\frac{\pi}{3}-\frac{\pi}{4}\right)\left(\frac{\pi}{3}-\frac{\pi}{2}\right)} \doteq \\
&\doteq -13{,}3046x^4 + 38{,}3146x^3 - 32{,}8279x^2 + 8{,}5943x, \\
l_4(x) &= \frac{(x-0)\left(x-\frac{\pi}{6}\right)\left(x-\frac{\pi}{4}\right)\left(x-\frac{\pi}{3}\right)}{\left(\frac{\pi}{2}-0\right)\left(\frac{\pi}{2}-\frac{\pi}{6}\right)\left(\frac{\pi}{2}-\frac{\pi}{4}\right)\left(\frac{\pi}{2}-\frac{\pi}{3}\right)} \doteq \\
&\doteq 1{,}4783x^4 - 3{,}4831x^3 + 2{,}6343x^2 - 0{,}6366x.
\end{aligned}$$

Hodnota interpolačního polynomu je pak

$$\begin{aligned}
P(x) &= 0 \cdot {}_0(x) + \tfrac{1}{2}l_1(x) + \tfrac{\sqrt{2}}{2}l_2(x) + \tfrac{\sqrt{3}}{2}l_3(x) + l_4(x) \doteq \\
&\doteq 0{,}0288x^4 - 0{,}2043x^3 + 0{,}0214x^2 + 0{,}9956x\ .
\end{aligned}$$ □

**Doplňující otázky:** Může Franta tento přibližný výsledek použít i pro výpočet funkce sin na intervalu $\left[\frac{\pi}{2}, \pi\right]$? A pokud ne, jak by měl postupovat?

Jak by vypadaly přibližné vztahy, pokud by Franta nepoužil všechny uzly, ale pro každý bod jen tři uzly nejbližší?

**5.7.** Další den potřeboval Franta spočítat dvojkový logaritmus 25.



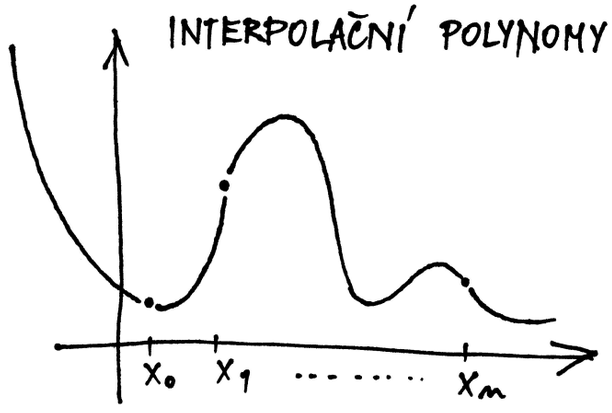
(Ve skutečnosti potřeboval přirozený logaritmus, ale protože ví, že $\ln 2$ je zhruba 0,6931, vystačí si i s dvojkovým.) Nejprve tedy vzal uzly 16 a 32 s funkčními hodnotami 4 a 5 a sestrojil interpolační polynom (přímku) $P(x) = \frac{1}{16}x + 3$, takže $P(25) = \frac{73}{16} = 4{,}5625$. Kvůli zpřesnění výsledku přidal další uzel 8 s funkční hodnotou 3. V tomto případě vyšel interpolační polynom

Existenci řešení tohoto systému rovnic můžeme snadno ukázat přímou konstrukcí patřičného polynomu pomocí tzv. Lagrangeových polynomů pro dané body $x_0, \ldots, x_n$, viz další odstavec textu níže.

Nyní ale důkaz dokončíme pomocí jednoduchých znalostí z lineární algebry. Tento systém lineárních rovnic má totiž právě jedno řešení pokud je determinant jeho matice invertibilní skalár, tj. pokud je nenulový (viz 3.1 a 2.23). Jde o tzv. *Vandermondův determinant*, který jsme již diskutovali v příkladu ‖2.24‖ na straně 80.

Protože jsme ale už ověřili, že pro nulové pravé strany existuje řešení právě jedno, víme, že tento determinant nenulový být musí.

Protože polynomy jsou jako zobrazení stejné, právě když mají stejné koeficienty, věta je dokázána. □




**5.4. Užití interpolací.** Na první pohled se může zdát, že reálné



nebo případně racionální polynomy, tj. polynomiálně zadané funkce $\mathbb{R} \to \mathbb{R}$ nebo $\mathbb{Q} \to \mathbb{Q}$, tvoří hezkou velikou třídu funkcí jedné proměnné. Můžeme jimi proložit jakékoliv sady předem zadaných hodnot. Navíc se zdají být snadno vyjádřitelné, takže by s jejich pomocí mělo být dobře možné počítat i hodnoty těchto funkcí pro jakoukoliv hodnotu proměnné. Při pokusu o praktické využití v tomto směru ovšem narazíme hned na několik problémů.

Prvním z nich je potřeba rychle vyjádřit polynom, kterým zadaná data proložíme. Pro řešení výše diskutovaného systému rovnic totiž budeme obecně potřebovat čas úměrný třetí mocnině počtu bodů, což při objemnějších datech je jistě těžko přijatelné. Podobným problémem je pomalé vyčíslení hodnoty polynomu vysokého stupně v zadaném bodě. Obojí lze částečně obejít tak, že zvolíme vhodné vyjádření interpolačního polynomu (tj. vybereme lepší bázi příslušného vektorového prostoru všech polynomů stupně nejvýše $k$, než je ta nejobvyklejší $1, x, x^2, \ldots, x^n$).

Ukážeme si pouze jediný příklad takového postupu:

### Lagrangeovy interpolační polynomy

*Lagrangeův interpolační polynom* snadno zapíšeme pomocí tzv. elementárních Lagrangeových polynomů $\ell_i$ stupně $n$ s vlastnostmi

$$\ell_i(x_j) = \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}$$

roven $P(x) = -\frac{1}{384}x^2 + \frac{3}{16}x + \frac{5}{3}$, což dává $P(25) \doteq 4{,}7266$. Franta chtěl výsledek ještě zpřesnit, přidal tedy rovnou dva uzly, a to 2 a 4 s funkčními hodnotami 1 a 2. Jaké však bylo jeho překvapení, když mu vyšla hodnota $P(25) \doteq 5{,}892$, která je určitě nesprávná vzhledem k tomu, že logaritmus je rostoucí funkce. Dokážete vysvětlit, kde se vzala taková chyba?

**Řešení.** Franta trochu pátral na internetu a zjistil, že chyba při interpolaci se dá vyjádřit ve tvaru

$$f(x) - P_n(x) = \frac{(x-x_0)(x-x_1)\dots(x-x_n)}{(n+1)!} f^{(n+1)}(\xi),$$

kde bod $\xi$ není znám, ale leží v intervalu daném nejmenším a největším uzlem. Člen v čitateli zlomku způsobuje, že přidávání dalších vzdálených uzlů přesnost spíše zhoršuje. □

**5.8.** O týden později potřeboval Franta určit $\sqrt{7}$. Napadlo ho problém otočit a použít tzv. inverzní interpolaci, tedy zaměnit roli uzlů a funkčních hodnot a určit přibližnou hodnotu vhodné funkce v nule. Jak postupoval?

**Řešení.** $\sqrt{7}$ je nulový bod funkce $x^2 - 7$. Franta vzal uzly $x_0 = 2$, $x_1 = 2{,}5$, $x_2 = 3$, příslušné funkční hodnoty jsou $-3$, $-0{,}75$ a 2. Pak prohodil úlohu uzlů a funkčních hodnot a získal elementární Lagrangeovy polynomy

$$l_0(x) = \frac{(x+0{,}75)(x-2)}{(-3+0{,}75)(-3-2)} = \frac{4}{45}x^2 - \frac{1}{9}x - \frac{2}{15},$$
$$l_1(x) = -\frac{16}{99}x^2 - \frac{16}{99}x + \frac{32}{33},$$
$$l_2(x) = \frac{6}{55}x^2 + \frac{3}{11}x + \frac{9}{55}.$$

Pro $\sqrt{7}$ tak dostal přibližnou hodnotu

$$2 \cdot l_0(0) + 2.5 \cdot l_1(0) + 3 \cdot l_2(0) = \tfrac{437}{165} \doteq 2{,}6485.$$

**Doplňující otázky:** Frantovi se do výpočtu jednoho elementárního polynomu vloudila chyba, pokuste se ji vypátrat. Má tato chyba vliv na výslednou hodnotou?

Jak bychom mohli využít také hodnotu derivace v bodě 2,5? □

**5.9.** Nalezněte přirozený splajn $S$, který splňuje podmínky



$$S(-1) = 0,\ S(0) = 1,\ S(1) = 0.$$

**Řešení.** Hledaný přirozený splajn bude složen ze dvou kubických polynomů, jednoho, řekněme $S_1$, pro interval $[-1, 0]$, druhého, řekněme $S_2$, pro interval $[0, 1]$. Slůvko „přirozený“ navíc určuje, že hodnoty druhých derivací polynomů $S_1$, resp. $S_2$, budou nulové v bodě $-1$, resp. 1. Díky předepsané společné hodnotě v bodě 0 víme že absolutní člen obou polynomů je 1, ze symetrie úlohy plyne, že

Zřejmě musí být tyto polynomy až na konstantu rovny výrazům $(x-x_0)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)$, a proto

$$\ell_i(x) = \frac{\prod_{j\neq i}(x-x_j)}{\prod_{j\neq i}(x_i-x_j)}.$$

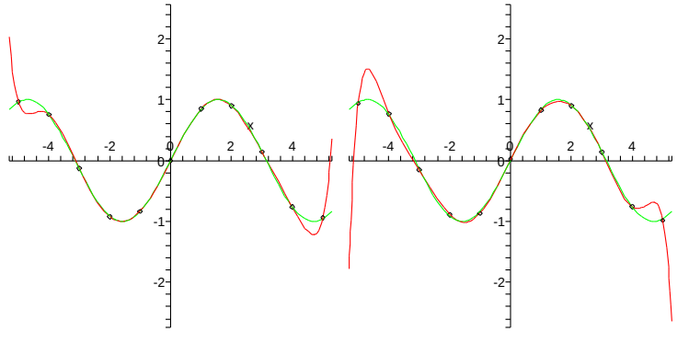
Hledaný Lagrangeův interpolační polynom je pak dán vztahem

$$f(x) = y_0\ell_0(x) + y_1\ell_1(x) + \dots + y_n\ell_n(x).$$

Použití Lagrangeových polynomů je obzvlášť efektivní, když opakovaně prokládáme zadané hodnoty závislé proměnné $y_i$ pro stále stejné hodnoty nezávislé proměnné $x_i$. Pak totiž máme elementární polynomy $\ell_i$ předem připraveny.

Toto vyjádření má nevýhodu ve velké citlivosti na nepřesnosti výpočtu při malých rozdílech zadaných hodnot $x_i$, protože se v něm těmito rozdíly dělí.

Další nepříjemností je velice špatná stabilita hodnot reálných nebo racionálních polynomů při zvětšující se hodnotě proměnné. Brzy budeme mít nástroje na přesný popis kvalitativního chování funkcí, nicméně i bez nich je zřejmé, že podle znaménka koeficientu u nejvyšší mocniny polynomu se hodnoty velice rychle při rostoucím $x$ vydají buď do plus nebo mínus nekonečna. Ani toto znaménko koeficientu u nejvyššího stupně se ale u interpolačního polynomu při malých změnách prokládaných hodnot nechová stabilně. Názorně to vidíme na dvou obrázcích, kde je proloženo jedenáct hodnot funkce $\sin(x)$ s různými malými náhodnými změnami hodnot. Je na nich vynesena aproximovaná funkce, kolečka jsou malinko posunuté hodnoty a jimi proložený jednoznačně zadaný interpolační polynom. Zatímco uvnitř intervalu je aproximace vcelku dobrá, stabilita na okrajích je otřesná.




Kolem interpolačních polynomů existuje bohatá teorie, zájemce odkazujeme na speciální literaturu.

**5.5. Poznámka.** Numerická nestabilita způsobená případnou blízkostí (některých) z bodů $x_i$ je dobře viditelná i na systému rovnic z důkazu Věty 5.3. Při řešení systémů lineárních rovnic totiž nestabilita do značné míry souvisí s velikostí determinantu matice systému, tj. v našem případě Vandermondova determinantu. Ten umíme vcelku snadno přímo spočíst:

**Lemma.** *Pro posloupnost po dvou různých skalárů* $x_0, \dots, x_n \in \mathbb{K}$ *platí*

$$V(x_0, \dots, x_n) = \prod_{i>k=0}^{n} (x_i - x_k).$$

společná hodnota první derivace v bodě 0 je nulová. Můžeme tedy psát $S_1(x) = ax^3 + bx^2 + 1$ a $S_2(x) = cx^3 + dx^2 + 1$, pro neznámé reálné parametry $a, b, c$ a $d$. Dosazením těchto tvarů do čtyř podmínek $S_1(-1) = 0$, $S_1"(-1) = 0$, $S_2(1) = 0$a $S_2"(1) = 0$ dostáváme čtyři lineární rovnice pro tyto parametry:

$$\begin{aligned} -a + b + 1 &= 0,\\ -6a + 2b &= 0,\\ c + d + 1 &= 0,\\ 6c + 2d &= 0. \end{aligned}$$

Jejich vyřešením pak $S_1(x) = -\frac{1}{2}x^3 - \frac{3}{2}x^2 + 1$, $S_2(x) = \frac{1}{2}x^3 - \frac{3}{2}x^2 + 1$. Celkem tedy

$$S(x) = \begin{cases} -\frac{1}{2}x^3 - \frac{3}{2}x^2 + 1 & \text{pro } x \in [-1, 0],\\ \frac{1}{2}x^3 - \frac{3}{2}x^2 + 1 & \text{pro } x \in [0, 1]. \end{cases}$$

□

**5.10.** Nalezněte splajn $S$, který splňuje podmínky

$$S(-1) = 0,\ S(0) = 1,\ S(1) = 0,\ S'(-1) = 1,\ S'(1) = 1.$$

**Řešení.** Hledaný splajn se od splajnu z předchozí úlohy liší pouze hodnotami derivací v bodech $-1$ a 1. Obdobně jako v předchozí úloze tak dostáváme části $S_1$ a $S_2$ splajnu ve tvaru $S_1(x) = ax^3 + bx^2 + 1$ a $S_2(x) = cx^3 + dx^2 + 1$, pro neznámé reálné parametry $a$, $b$, $c$ a $d$. Dosazením do podmínek $S_1(-1) = 0$, $S_1'(-1) = 1$, $S_2(1) = 0$ a $S_2'(1) = 1$ dostáváme nyní soustavu

$$\begin{aligned} -a + b + 1 &= 0,\\ 3a - 2b &= 1,\\ c + d + 1 &= 0,\\ 3c + 2d &= 1 \end{aligned}$$

s řešením $a = -1$, $b = -2$, $c = 3$ a $d = -4$, tedy hledaný splajn je funkce

$$S(x) = \begin{cases} -x^3 - 2x^2 + 1 & \text{pro } x \in [-1, 0],\\ 3x^3 - 4x^2 + 1 & \text{pro } x \in [0, 1]. \end{cases}$$

□

*5.11.* Nalezněte polynom nejvýše druhého stupně, který v bodech

$$x_0 = -1, \quad x_1 = 1, \quad x_2 = 2$$

nabývá po řadě hodnot

$$y_0 = 1, \quad y_1 = -3, \quad y_2 = 4.$$

○

*5.12.* Sestrojte Lagrangeův interpolační polynom pro

| $x_i$ | $-2$ | $-1$ | 1 | 2 |
|---|---|---|---|---|
| $y_i$ | 1 | $-1$ | $-1$ | 1 |

.

DŮKAZ. Vztah dokážeme indukcí přes počet bodů $x_i$. Evidentně je správný pro $n = 1$ (a pro $n = 0$ je úloha nezajímavá). Předpokládejme, že výsledek je správný pro $n - 1$, tj.

$$V(x_0, \ldots, x_{n-1}) = \prod_{i>k=0}^{n-1} (x_i - x_k).$$

Nyní považujme hodnoty $x_0, \ldots, x_{n-1}$ za pevné a hodnotu $x_n$ ponechme jako volnou proměnnou. Rozvojem determinantu podle posledního řádku (viz 2.21) obdržíme hledaný determinant jako polynom

$$V(x_0, \ldots, x_n) = (x_n)^n V(x_0, \ldots, x_{n-1}) - (x_n)^{n-1} \cdots . \tag{5.1}$$

Toto je polynom stupně $n$, protože víme, že jeho koeficient u $(x_n)^n$ je nenulový dle indukčního předpokladu. Přitom bude zjevně nulový při dosazení kterékoliv hodnoty $x_n = x_i$ pro $i < n$, protože bude v takovém případě obsahovat původní determinant dva stejné řádky. Náš polynom tedy bude dělitelný výrazem

$$(x_n - x_0)(x_n - x_1) \cdots (x_n - x_{n-1}),$$

který má sám již stupeň $n$. Odtud vyplývá, že celý Vandermondův determinant coby polynom v proměnné $x_n$ musí být tomuto výrazu roven až na konstantní násobek, tj.

$$V(x_0, \ldots, x_n) = c \cdot (x_n - x_0)(x_n - x_1) \cdots (x_n - x_{n-1}).$$

Porovnáním koeficientů u nejvyšší mocniny v (5.1) a tomto výrazu dostáváme

$$c = V(x_0, \ldots, x_{n-1})$$

a tím je důkaz lemmatu ukončen. □

Opět tedy vidíme, že determinant bude velmi malý, pokud jsou malé vzdálenosti bodů $x_i$.

**5.6. Derivace polynomů.** Zjistili jsme, že hodnoty polynomů s rostoucí proměnnou rychle míří k nekonečným hodnotám (viz také obrázky). Proto je zřejmé, že polynomy nemohou nikdy vhodně popisovat jakékoliv periodicky se opakující děje (jako jsou např. hodnoty goniometrických funkcí). Mohlo by se ale zdát, že podstatně lepší výsledky budeme alespoň mezi body $x_i$ dosahovat, když si budeme kromě hodnot funkce hlídat, jak rychle naše funkce v daných bodech rostou.



Za tímto účelem zavedeme (prozatím spíše intuitivně) pojem *derivace* pro polynomy. Můžeme přitom pracovat opět s reálnými, komplexními nebo racionálními polynomy. Rychlost růstu v bodě $x \in \mathbb{R}$ pro reálný polynom $f(x)$ dobře vyjadřují podíly

$$\frac{f(x + \Delta x) - f(x)}{\Delta x}, \tag{5.2}$$

a protože umíme spočíst (nad libovolným okruhem)

$$(x + \Delta x)^k = x^k + kx^{k-1}\,\Delta x + \cdots + \binom{k}{l} x^l (\Delta x)^{k-l} + \cdots + (\Delta x)^k,$$

dostaneme pro polynom $f(x) = a_n x^n + \cdots + a_0$ výše vedený podíl ve tvaru

$$\begin{aligned} \frac{f(x+\Delta x)-f(x)}{\Delta x} &= a_n \frac{nx^{n-1}\,\Delta x + \cdots + (\Delta x)^k}{\Delta x} + \cdots + a_1 \frac{\Delta x}{\Delta x} =\\ &= na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 + \Delta x(\ldots), \end{aligned}$$

kde výraz v závorce je polynomiálně závislý na $\Delta x$. Evidentně pro hodnoty $\Delta x$ velice blízké nule dostaneme hodnotu libovolně blízkou následujícímu výrazu:

Pak uveďte libovolný polynom vyššího než třetího stupně, jenž vyhovuje podmínkám uvedeným v tabulce. ○

*5.13.* Nalezněte polynom $p(x) = ax^3 + bx^2 + cx + d$, pro který platí
$$p(0) = 1, \quad p(1) = 0, \quad p(2) = 1, \quad p(3) = 10\,.$$ ○

*5.14.* Určete polynom $p$ nejvýše třetího stupně splňující
$$p(0) = 2, \quad p(1) = 3, \quad p(2) = 12, \quad p(5) = 147\,.$$ ○

*5.15.* Nechť jsou libovolně zvoleny hodnoty $y_0, \ldots, y_n \in \mathbb{R}$ v navzájem různých bodech $x_0, \ldots, x_n \in \mathbb{R}$. Kolik existuje polynomů stupně právě $n+1$, které nabývají v uvedených bodech zadaných hodnot? ○

*5.16.* Stanovte Hermiteovy interpolační polynomy $P$, $Q$, jestliže má být
$$P(-1) = -11, \quad P(1) = 1, \quad P'(-1) = 12, \quad P'(1) = 4;$$
$$Q(-1) = -9, \quad Q(1) = -1, \quad Q'(-1) = 10, \quad Q'(1) = 2.$$ ○

*5.17.* Nahraďte funkci $f$ Hermiteovým polynomem, víte-li

| $x_i$ | $-1$ | $1$ | $2$ |
|---|---|---|---|
| $f(x_i)$ | $4$ | $-4$ | $-8$ |
| $f'(x_i)$ | $8$ | $-8$ | $11$ |

. ○

*5.18.* Bez počítání uveďte Hermiteův interpolační polynom, je-li požadováno, aby
$$x_0 = 0, \quad x_1 = 2, \quad x_2 = 1,$$
$$y_0 = 0, \quad y_1 = 4, \quad y_2 = 1,$$
$$y'_0 = 0, \quad y'_1 = 4, \quad y'_2 = 2.$$ ○

*5.19.* Nalezněte polynom nejvýše třetího stupně, který v bodě $x = 1$ nabývá hodnoty $y = 4$, v bodě $x = 2$ hodnoty $y = 9$ a který má v bodě $x = 0$ derivaci rovnu $-2$, zatímco v bodě $x = 1$ je jeho derivace rovna 1. Poté určete polynom nejvýše třetího stupně, jenž v bodech $x = 1$ a $x = -1$ nabývá hodnoty $y = 6$ a jenž má v bodě $x = 1$ a zároveň v bodě $x = -1$ derivaci rovnu 2. ○

*5.20.* Kolik existuje navzájem různých polynomů stupně nejvýše 4, které v bodech $x_0 = 5$, $x_1 = 55$ nabývají po řadě hodnot $y_0 = 55$, $y_1 = 5$ a jejichž první a druhá derivace v bodě $x_0$ je nulová? ○

*5.21.* Napište libovolný polynom $P$ vyhovující těmto podmínkám:
$$P(0) = 6, \quad P(1) = 4, \quad P(2) = 4, \quad P'(2) = 1\,.$$ ○

### Derivace polynomů

Derivací polynomu $f(x) = a_n x^n + \cdots + a_0$ podle proměnné $x$ rozumíme polynom
$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

Z definice je jasné, že právě hodnota $f'(x_0)$ derivace polynomu nám dává dobré přiblížení jeho chování v okolí bodu $x_0$. Přesněji řečeno přímky
$$y = \frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x}(x - x_0) + f(x_0),$$
tj. sečny grafu polynomu procházející body $[x_0,\ f(x_0)]$ a $[x_0 + \Delta x,\ f(x_0 + \Delta x)]$, se, se zmenšujícím se $\Delta x$, přibližují přímce
$$y = f'(x_0)(x - x_0) + f(x_0),$$
což tedy musí být tečna grafu polynomu $f$. Hovoříme o *lineárním přiblížení* polynomu $f$ jeho *tečnou*.

Derivace polynomů je lineární zobrazení, které přiřazuje polynomům stupně nejvýše $n$ polynomy stupně nejvýše $n-1$.

Iterací této operace dostáváme druhé derivace $f''$, třetí derivace $f^{(3)}$ a obecně po $k$–násobném opakování polynom $f^{(k)}$ stupně $n-k$. Po $n+1$ derivacích je výsledkem nulový polynom. Toto lineárním zobrazení je příkladem tzv. cyklického nilpotentního zobrazení, která jsou podrobněji rozebírána v odstavci 3.32 o nilpotentních zobrazeních.

**5.7. Hermiteův interpolační problém.** Uvažme opět $m+1$ po dvou různých reálných hodnot $x_0, \ldots, x_m$, tj. $x_i \neq x_j$ pro všechna $i \neq j$. Budeme chtít zase prokládat pomocí polynomů předem dané hodnoty, tentokrát ale budeme vedle hodnot předepisovat i první derivace. Tj. předepíšeme $y_i$ a $y'_i$ pro všechna i. Hledáme polynom $f$, který bude nabývat těchto předepsaných hodnot a derivací.



Zcela analogicky jako u interpolace pouhých hodnot obdržíme pro neznámé koeficienty polynomu $f(x) = a_n x^n + \cdots + a_0$ systém $2(m+1)$ rovnic
$$\begin{aligned}
a_0 + x_0 a_1 + \cdots + (x_0)^n a_n &= y_0,\\
&\vdots\\
a_0 + x_m a_1 + \cdots + (x_m)^n a_n &= y_m,\\
a_1 + 2x_0 a_2 + \cdots + n(x_0)^{n-1} a_n &= y'_0,\\
&\vdots\\
a_1 + 2x_m a_2 + \cdots + n(x_m)^{n-1} a_n &= y'_m.
\end{aligned}$$
Opět bychom mohli ověřit, že při volbě $n = 2m+1$ bude determinant tohoto systému rovnic nenulový a tudíž bude existovat právě jedno řešení. Nicméně, obdobně ke konstrukci Lagrangeova polynomu lze zkonstruovat takový polynom $f$ přímo. Prostě si vytvoříme jednu sadu polynomů s hodnotami nula nebo jedna jak u derivací tak u hodnot, abychom jejich jednoduchou lineární kombinací uměli dosáhnout potřebné hodnoty. Ověření následující definice a tvrzení necháme na čtenáři:

*5.22.* Sestrojte přirozený kubický interpolační splajn pro body $x_0 = -1, x_1 = 0, x_2 = 1$ a hodnoty $y_0 = 1, y_1 = 0, y_2 = 1$ v těchto bodech. ○

*5.23.* Zkonstruujte přirozený kubický interpolační splajn pro funkci

$$f(x) = |x|, \quad x \in [-1, 1],$$

pokud jsou zvoleny body $x_0 = -1, x_1 = 0, x_2 = 1$. ○

*5.24.* Napište přirozený kubický interpolační splajn pro body

$$x_0 = -3, \quad x_1 = 0, \quad x_2 = 3$$

a hodnoty $y_0 = -3, y_1 = 0, y_2 = 3$. ○

*5.25.* Bez počítání uveďte přirozený kubický interpolační splajn pro body $x_0 = -1, x_1 = 0$ a $x_2 = 2$ a hodnotu $y_0 = y_1 = y_2 = 1$ v těchto bodech. ○

*5.26.* Určete

$$x_0 = -3, \quad x_1 = -2, \quad x_2 = -1$$

a pro hodnoty

$$y_0 = 0, \quad y_1 = 1, \quad y_2 = 2, \quad y_0' = 1, \quad y_2' = 1.$$

○

*5.27.* Sestrojte přirozený kubický interpolační splajn pro funkci

$$y = \frac{1}{1 + x^2}$$

při volbě bodů

$$x_0 = 0, \quad x_1 = 1, \quad x_2 = 3.$$

○

Více příkladů k interpolačním polynomům najdete na straně 288.

## B. Topologie komplexních čísel a jejich podmnožin

**5.28.** Nalezněte hromadné, izolované, hraniční a vnitřní body množin $\mathbb{N}, \mathbb{Q}, X = \{x \in \mathbb{R};\ 0 \le x < 1\}$ v $\mathbb{R}$.



**Řešení.** Množina $\mathbb{N}$. Pro libovolné $n \in \mathbb{N}$ očividně platí

$$\mathcal{O}_1(n) \cap \mathbb{N} = (n-1, n+1) \cap \mathbb{N} = \{n\}.$$

Existuje tedy okolí bodu $n \in \mathbb{N}$ v $\mathbb{R}$, které obsahuje pouze jeden prvek množiny $\mathbb{N}$ (pochopitelně právě uvažované $n$), tj. každý bod $n \in \mathbb{N}$ je izolovaný. Množina vnitřních bodů je proto prázdná (je-li bod izolovaný, nemůže být vnitřní). Bod $a \in \mathbb{R}$ je pak hromadným bodem $A$ právě tehdy, když každé jeho okolí obsahuje nekonečně mnoho bodů $A$. Ovšem množina

$$\mathcal{O}_1(a) \cap \mathbb{N} = (a-1, a+1) \cap \mathbb{N}, \text{ přičemž } a \in \mathbb{R},$$

### Hermiteův interpolační polynom

*Hermiteův interpolační polynom* definujeme pomocí fundamentálních Hermiteových polynomů:

$$h_i^1(x) = \left[1 - \frac{\ell''(x_i)}{\ell'(x_i)}(x - x_i)\right](\ell_i(x))^2,$$
$$h_i^2(x) = (x - x_i)(\ell_i(x))^2,$$

kde $\ell(x) = \prod_{i=1}^{n}(x - x_i)$. Tyto polynomy splňují:

$$h_i^1(x_j) = \delta_i^j = \begin{cases} 1 & \text{pro } i = j, \\ 0 & \text{pro } i \neq j, \end{cases}$$
$$(h_i^1)'(x_j) = 0,$$
$$h_i^2(x_j) = 0,$$
$$(h_i^2)'(x_j) = \delta_i^j,$$

a proto je Hermiteův interpolační polynom dán výrazem

$$f(x) = \sum_{i=1}^{k} \left( y_i h_i^1(x_i) + y_i' h_i^2(x_i) \right).$$

**5.8. Příklady Hermiteových polynomů.** Úplně nejjednodušší případ je zadání hodnoty a derivace v jediném bodě. Tím určíme beze zbytku polynom stupně jedna

$$f(x) = f(x_0) + f'(x_0)(x - x_0),$$

tj. právě rovnici přímky zadané hodnotou a směrnicí v bodě $x_0$. Když zadáme hodnotu a derivaci ve dvou bodech, tj. $y_0 = f(x_0)$, $y_0' = f'(x_0)$, $y_1 = f(x_1)$, $y_1' = f'(x_1)$ pro dva různé body $x_i$, dostaneme ještě pořád snadno počítatelný problém.

Ukažme si jej ve zjednodušeném provedení, kdy $x_0 = 0$, $x_1 = 1$. Pak matice systému a její inverze budou

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} 2 & -2 & 1 & 1 \\ -3 & 3 & -2 & -1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Přímým vynásobením $A \cdot (y_0, y_1, y_0', y_1')^T$ pak vyjde vektor koeficientů $(a_3, a_2, a_1, a_0)^T$ polynomu $f$, tj.

$$f(x) = (2y_0 - 2y_1 + y_0' + y_1')x^3 + \\ + (-3y_0 + 3y_1 - 2y_0' - y_1')x^2 + y_0' x + y_0.$$

**5.9. Interpolace splajny.** Obdobně můžeme předepisovat libovolný konečný počet derivací v jednotlivých bodech a vhodnou volbou stupně polynomu obdržíme vždy jednoznačné interpolace. Nebudeme zde uvádět podrobnosti. Bohužel, u všech těchto interpolací pořád zůstávají problémy zmíněné už v případě jednoduchých interpolací hodnot – složitost výpočtů a nestabilita. Použití derivací však podbízí jednoduché vylepšení metodiky:



Jak jsme viděli na obrázcích demonstrujících nestabilitu interpolace jedním polynomem dostatečně vysokého stupně, malé lokální změny hodnot zapříčiňovaly dramatické celkové změny chování výsledného polynomu. Nabízí se tedy využití malých polynomiálních kousků nízkých stupňů, které ale musíme umět rozumně navazovat.

je konečná, z čehož plyne, že $\mathbb{N}$ hromadné body nemá. To, že tato množina je konečná, dále implikuje

$$\delta_b := \inf_{n\in\mathbb{N}} |\, b-n\,| = \inf_{n\in\mathcal{O}_1(b)\cap\mathbb{N}} |\, b-n\,| > 0 \quad \text{pro } b \in \mathbb{R}\setminus\mathbb{N}.$$

Odsud máme $\mathcal{O}_{\delta_b}(b)\cap\mathbb{N} = \emptyset$, tj. žádné $b \in \mathbb{R}\setminus\mathbb{N}$ není hraničním bodem $\mathbb{N}$. Současně víme, že každý bod dané množiny, který není vnitřním bodem, je nutně jejím hraničním bodem. Množina hraničních bodů tak obsahuje $\mathbb{N}$. Shrneme-li to, množina hraničních bodů $\mathbb{N}$ je $\mathbb{N}$.

Množina $\mathbb{Q}$. Racionální čísla tvoří tzv. hustou podmnožinu množiny všech reálných čísel. To znamená, že ke každému reálnému číslu konverguje posloupnost racionálních čísel (představme si např. nekonečný desetinný rozvoj reálného čísla a jemu odpovídající posloupnost, kdy v následujícím členu přidáváme další cifru rozvoje). O této posloupnosti lze navíc předpokládat, že všechny její členy jsou navzájem různé (na poslední pozici konečného desetinného rozvoje se můžeme záměrně dopouštět chyby nebo kupř. číslu 1 přiřadíme desetinný rozvoj $0{,}999\ldots$ apod.). Množina hromadných bodů $\mathbb{Q}$ v $\mathbb{R}$ je proto celé $\mathbb{R}$ a každý bod $x \in \mathbb{R}\setminus\mathbb{Q}$ je hraniční. Zvláště dostáváme, že libovolné $\delta$-okolí

$$\mathcal{O}_\delta\left(\frac{p}{q}\right) = \left(\frac{p}{q}-\delta,\ \frac{p}{q}+\delta\right),\ \text{kde } p,q\in\mathbb{Z},\ q\neq 0,$$

racionálního čísla $p/q$ musí obsahovat nekonečně mnoho racionálních čísel, což dává neexistenci izolovaných bodů. Číslo $\sqrt{2}/10^n$ není racionální pro žádné $n \in \mathbb{N}$. Předpokladem opaku (opět $p,q\in\mathbb{Z}$, $q\neq 0$)

$$\frac{\sqrt{2}}{10^n} = \frac{p}{q}, \quad \text{tj.} \quad \sqrt{2} = \frac{10^n\, p}{q},$$

totiž okamžitě obdržíme spor – o číslu $\sqrt{2}$ víme, že není racionální. Libovolné okolí racionálního čísla $p/q$ tak zároveň obsahuje nekonečně mnoho reálných čísel $p/q + \sqrt{2}/10^n$ ($n \in \mathbb{N}$), která nejsou racionální (množina $\mathbb{Q}$ jako těleso je uzavřená vzhledem k odečítání). Všechny body $p/q \in \mathbb{Q}$ jsou tudíž rovněž hraniční a vnitřní body množina $\mathbb{Q}$ nemá.

Množina $X = [0,1)$. Nechť $a \in [0,1)$ je zvoleno libovolně. Posloupnosti $\left\{a+\frac{1}{n}\right\}_{n=1}^{\infty}$, $\left\{1-\frac{1}{n}\right\}_{n=1}^{\infty}$ zjevně konvergují po řadě k hodnotám $a$, 1. Snadno jsme tak ukázali, že množina hromadných bodů obsahuje interval $[0,1]$. Jiné hromadné body neexistují: pro jakékoli $b \notin [0,1]$ existuje $\delta > 0$ takové, že $\mathcal{O}_\delta(b)\cap[0,1] = \emptyset$ (pro $b<0$ postačuje položit $\delta = -b$ a pro $b>1$ potom $\delta = b-1$). Protože každý bod intervalu $[0,1)$ je hromadným bodem, množina izolovaných bodů je prázdná. Pro $a \in (0,1)$ označme menší z kladných čísel $a$, $1-a$ jako $\delta_a$. Uvážíme-li

$$\mathcal{O}_{\delta_a}(a) = (a-\delta_a,\ a+\delta_a) \subseteq (0,1), \quad a\in(0,1),$$

Nejjednodušší je propojení vždy dvou sousedních bodů polynomem stupně nejvýše jedna. Tak se nejčastěji zobrazují data. Z pohledu derivací to znamená, že budou na jednotlivých úsecích konstantní a pak se skokem změní.

O něco sofistikovanější možností je předepsat v každém bodě hodnotu a derivaci, tj. pro dva body budeme mít 4 hodnoty a jednoznačně tím určíme Hermiteův polynom 3. stupně, viz výše. Tento polynom pak můžeme použít pro všechny hodnoty nezávislé proměnné mezi krajními hodnotami $x_0 < x_1$. Hovoříme o *intervalu* $[x_0, x_1]$. Takové polynomiální přiblíženi po kouskách už bude mít tu vlastnost, že první derivace na sebe budou navazovat.

V praxi ale není pouhé navazování první derivace dostatečné a navíc při naměřených datech nemíváme hodnoty derivací k dispozici. Přímo se proto vnucuje pokus využívat pouze zadané hodnoty ve dvou sousedních bodech, ale požadovat zároveň rovnost prvních i druhých derivací u sousedních kousků polynomů třetího stupně. To totiž bude znamenat stejné množství rovnic a neznámých a pravděpodobně tedy i obdobnou praktickou řešitelnost problému:

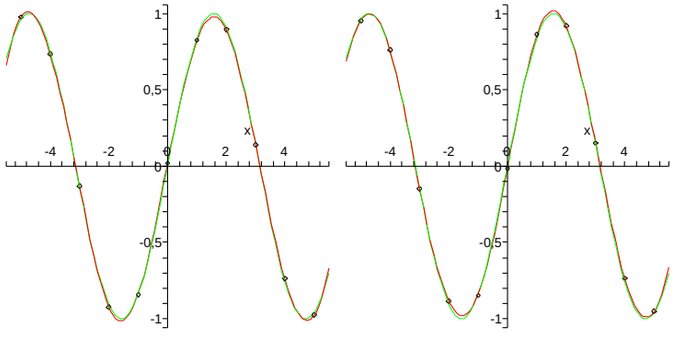
### Kubické splajny

Nechť $x_0 < x_1 < \cdots < x_n$ jsou reálné hodnoty, ve kterých jsou zadány požadované hodnoty $y_0, \ldots, y_n$. *Kubickým interpolačním splajnem* pro toto zadání je funkce $S : \mathbb{R} \to \mathbb{R}$, která splňuje následující podmínky:

- zúžení $S$ na interval $[x_{i-1}, x_i]$ je polynom $S_i$ nejvýše třetího stupně, $i = 1, \ldots, n$,
- $S_i(x_{i-1}) = y_{i-1}$ a $S_i(x_i) = y_i$ pro všechna $i = 1, \ldots n$,
- $S_i'(x_i) = S_{i+1}'(x_i)$ pro všechna $i = 1, \ldots, n-1$,
- $S_i''(x_i) = S_{i+1}''(x_i)$ pro všechna $i = 1, \ldots, n-1$.

Kubický splajn[1] pro $n+1$ bodů sestává z $n$ kubických polynomů, tj. máme k dispozici $4n$ volných parametrů (první definiční podmínka). Další podmínky přitom zadávají $2n+(n-1)+(n-1)$ rovností, tj. dva parametry zůstávají volné. Při praktickém použití se dodávají předpisy pro derivace v krajních bodech, tzv. *úplný splajn*, nebo jsou tyto zadány jako nula, tzv. *přirozený splajn*.

Pro srovnání se podívejme na interpolaci stejných dat jako v případě Lagrangeova polynomu, nyní pomocí splajnů:




[1] Ošklivé české slovo „splajn“ vzniklo fonetickým přepisem anglického ekvivalentu „spline“, který znamenal tvárné pravítko užívané inženýry pro kreslení křivek.

vidíme, že libovolný bod intervalu $(0,1)$ je vnitřním bodem intervalu $[0,1)$. Pro každé $\delta \in (0,1)$ je

$$\mathcal{O}_\delta(0) \cap [0,1) = (-\delta,\ \delta) \cap [0,1) = [0,\delta),$$
$$\mathcal{O}_\delta(1) \cap [0,1) = (1-\delta,\ 1+\delta) \cap [0,1) = (1-\delta,\ 1),$$

tj. každé $\delta$-okolí bodu 0 obsahuje jisté body intervalu $[0,1)$ a hodnoty z intervalu $(-\delta, 0)$ a každé $\delta$-okolí bodu 1 má neprázdný průnik s intervaly $[0,1)$, $[1, 1+\delta)$. Body 0 a 1 jsou tedy hraničními body. Celkem jsme zjistili, že množina všech vnitřních bodů odpovídá intervalu $(0,1)$ a množina hraničních bodů je $\{0,1\}$. Stačí si uvědomit, že bod nemůže být současně vnitřní a hraniční a že hraniční bod musí být izolovaný, nebo hromadný. □

*5.29.* Určete suprema a infima množin v $\mathbb{R}$:

$$A = (-3,0] \cup (1,\pi) \cup \{6\};\ B = \left\{ \frac{(-1)^n}{n^2};\ n \in \mathbb{N} \right\};$$
$$C = (-9,9) \cap \mathbb{Q}.$$

○

*5.30.* Nalezněte $\sup A$ a $\inf A$ pro

$$A = \left\{ \frac{n+(-1)^n}{n};\ n \in \mathbb{N} \right\} \subseteq \mathbb{R}.$$

○

*5.31.* Jsou dány následující množiny:

$$\mathbb{N} = \{1,2,\ldots,n,\ \ldots\},$$
$$\mathcal{M} = \left\{ -\frac{1}{n};\ n \in \mathbb{N} \right\},$$
$$\mathcal{J} = (0,2] \cup [3,5] \setminus \{4\}.$$

Určete $\inf \mathbb{N}$, $\sup \mathcal{M}$, $\inf \mathcal{J}$ a $\sup \mathcal{J}$ v $\mathbb{R}$. ○

*5.32.* Napište příklad množiny $M \subseteq \mathbb{R}$, která nemá v $\mathbb{R}$ infimum, ale má zde supremum; a udejte příklad množiny $N \subset \mathbb{R}$, která nemá v $\mathbb{R}$ supremum, ale má zde infimum. ○

*5.33.* Uveďte podmnožinu $X$ množiny $\mathbb{R}$, pro kterou je $\sup X \leq \inf X$. ○

*5.34.* Udejte příklad množin $A, B, C \subseteq \mathbb{R}$ takových, aby platilo

$$A \cap B = \emptyset,\ A \cap C = \emptyset,\ B \cap C = \emptyset,\ \sup A = \inf B = \inf C = \sup C.$$

○

Obrázek naznačuje, že je aproximace daleko stabilnější než tomu bylo u aproximace polynomy.

Výpočet celého splajnu už není bohužel tak jednoduchý jako u nezávislých výpočtů Hermiteových polynomů třetího stupně, protože data se prolínají vždy mezi sousedními intervaly. Při vhodném uspořádání se však dosáhne matice systému, která má nenulové prvky prakticky jen ve třech diagonálách, a pro takové existují vhodné numerické postupy, které umožní splajn počítat také v čase úměrném počtu bodů.

### 2. Reálná čísla a limitní procesy

Je důležité mít dostatečně velkou zásobu funkcí, se kterými bude možné možné vyjadřovat všechny běžné závislosti, zároveň ale musí být výběr šikovně omezen, abychom uměli vybudovat nějaké univerzální a hlavně účinné nástroje pro práci s nimi.

Ve skutečnosti se budeme muset hned z kraje soustředit na to, jak vůbec hodnoty funkcí definovat, když pomocí konečně mnoha násobení a sčítání dostáváme jen polynomy a navíc skutečně počítat umíme jen s čísly racionálními. S těmi ale nevystačíme ani při počítání odmocnin, protože už $\sqrt{2}$ racionální číslo není.

Prvním naším krokem tedy musí být pořádné zavedení tzv. limitních procesů, tj. dáme přesný obsah tvrzením, že se nějaké hodnoty blíží jejich hodnotě limitní.

Všimněme si také, že výraznou vlastností polynomů je jejich „spojitá“ závislost hodnot na nezávislé proměnné. Intuitivně řečeno, když dostatečně málo změníme $x$, určitě se nám moc nezmění ani hodnota $f(x)$. Takové chování naopak nemáme u po částech konstantních funkcí $f : \mathbb{R} \to \mathbb{R}$ v okolí „skoků“. Např. u tzv. *Heavisideovy funkce* [2]

$$f(x) = \begin{cases} 0 & \text{pro všechna } x < 0, \\ 1/2 & \text{pro } x = 0, \\ 1 & \text{pro všechna } x > 0 \end{cases}$$

taková „nespojitost“ nastane pro $x = 0$.

Začneme formalizací takovýchto intuitivních výroků.

**5.10. Reálná čísla.** Prozatím jsme docela dobře vystačili s algebraickými vlastnostmi reálných čísel, které říkaly, že $\mathbb{R}$ je pole. Už jsme ale používali i relaci uspořádání reálných čísel, kterou značíme „$\leq$“ (viz odstavec 1.38). Vlastnosti (axiomy) reálných čísel, včetně souvislostí uspořádání a ostatních relací, jsou shrnuty v následující tabulce.



Formálně vzato, pracujeme se čtveřicí $(\mathbb{R}, +, \cdot, \leq)$ s nosnou množinou $\mathbb{R}$, s binárními operacemi $+$ a $\cdot$ a s relací uspořádání $\leq$. Dělící čáry v tabulce naznačují, jak axiomy postupně zaručují, že jsou reálná čísla komutativní grupou vůči sčítání, že $\mathbb{R} \setminus \{0\}$ je komutativní grupa vůči násobení, $\mathbb{R}$ je pole, množina $\mathbb{R}$ spolu s operacemi $+, \cdot$ a s relací uspořádání je tzv. *uspořádané pole* a konečně poslednímu axiomu můžeme rozumět tak, že $\mathbb{R}$ je „dostatečně husté“, tj. nechybí nám tam body, jako např. chybí $\sqrt{2}$ v číslech racionálních.

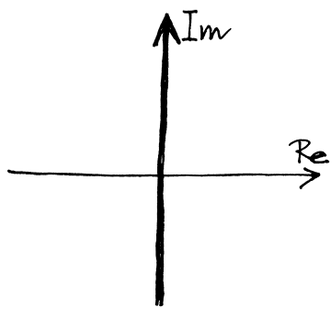
[2] Často také bývá Heavisideova funkce definována s hodnotami $-1$ pro záporné argumenty, $+1$ pro kladné a s nulovou hodnotou v nule. I my ji tak použijeme v kapitole sedmé.

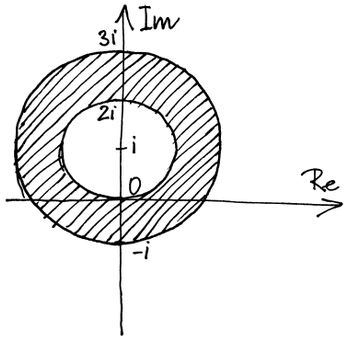
**5.35.** Vyznačte v komplexní rovině následující množiny:



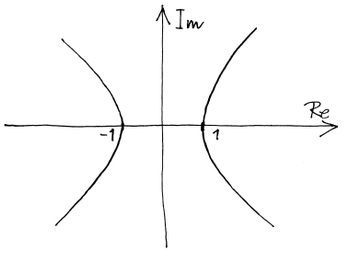
i) $\{z \in \mathbb{C} |\, |z-1| = |z+1|\}$,
ii) $\{z \in \mathbb{C} |\, 1 \le |z-i| \le 2\}$,
iii) $\{z \in \mathbb{C} |\, \mathrm{Re}(z^2) = 1\}$,
iv) $\{z \in \mathbb{C} |\, \mathrm{Re}(\frac{1}{z}) < \frac{1}{2}\}$.

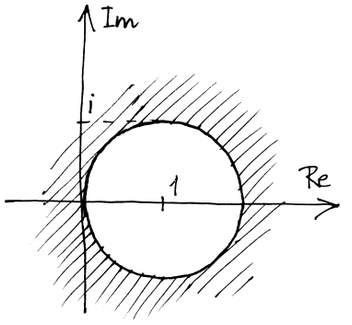
**Řešení.** (i) imaginární osa, (ii) mezikruží okolo $i$,




(iii) hyperbola $a^2 - b^2 = 1$,(iv) vnějšek jednotkového kruhu, střed v 1.




□

## C. Limity

V následujících příkladech se budeme zabývat výpočtem limit posloupností, tedy tím, jak posloupnosti „vypadají v nekonečnu“. Tj. pokud bychom chtěli předepsat $n$-tý člen posloupnosti pro hodně velké $n$, tak nám jej limita posloupnosti (pokud existuje) velmi dobře přiblíží. Limitám posloupností a posléze funkcí věnujeme v příkladovém sloupci hodně prostoru, proto s nimi začínáme dříve (a končíme později), než ve sloupci teorie.

Začněme s limitami posloupností. Potřebné definice nalezne čtenář v oddílu 5.12.

**5.36.** Spočítejte následující limity posloupností:



i) $\lim\limits_{n\to\infty} \frac{2n^2+3n+1}{n+1}$,
ii) $\lim\limits_{n\to\infty} \frac{2n^2+3n+1}{3n^2+n+1}$,
iii) $\lim\limits_{n\to\infty} \frac{n+1}{2n^2+3n+1}$,
iv) $\lim_{n\to-\infty} \frac{2^n-2^{-n}}{2^n+2^{-n}}$,

### Axiomy reálných čísel

| | |
|---|---|
| (R1) | $(a+b)+c = a+(b+c)$ pro všechna $a, b, c \in \mathbb{R}$, |
| (R2) | $a+b = b+a$ pro všechna $a, b \in \mathbb{R}$, |
| (R3) | existuje prvek $0 \in \mathbb{R}$ takový, že pro všechna $a \in \mathbb{R}$ platí $a+0 = a$, |
| (R4) | pro každé $a \in \mathbb{R}$ existuje opačný prvek $(-a) \in \mathbb{R}$ takový, že platí $a+(-a) = 0$, |
| (R5) | $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ pro všechna $a, b, c \in \mathbb{R}$, |
| (R6) | $a \cdot b = b \cdot a$ pro všechna $a, b \in \mathbb{R}$, |
| (R7) | existuje prvek $1 \in \mathbb{R}$ takový, že pro všechna $a \in \mathbb{R}$ platí $1 \cdot a = a$, |
| (R8) | pro každé $a \in \mathbb{R}$, $a \neq 0$, existuje inverzní prvek $a^{-1} \in \mathbb{R}$ takový, že platí $a \cdot a^{-1} = 1$, |
| (R9) | $a \cdot (b+c) = a \cdot b + a \cdot c$ pro všechna $a, b, c \in \mathbb{R}$, |
| (R10) | relace $\le$ je úplné uspořádání, tj. reflexivní, antisymetrická, tranzitivní a úplná relace na $\mathbb{R}$, |
| (R11) | pro všechna $a, b, c \in \mathbb{R}$ platí, že z $a \le b$ vyplývá také $a+c \le b+c$, |
| (R12) | pro všechna $a, b \in \mathbb{R}$, $a > 0$, $b > 0$, platí také $a \cdot b > 0$, |
| (R13) | každá neprázdná shora ohraničená množina $A \subseteq \mathbb{R}$ má supremum. |

Pojem *supremum* musíme ale také zavést pořádně. Má smysl pro každou uspořádanou množinu, tj. množinu s pevně zadanou relací uspořádání, a budeme se s ním takto i později setkávat ve více algebraických souvislostech. Připomeňme, že v obecné úrovni je uspořádáním jakákoliv binární relace na množině, která má vlastnosti reflexivity, antisymetrie a tranzitivity, viz odstavec 1.38.

### Supremum a infimum

**Definice.** Uvažme podmnožinu $A \subseteq B$ v uspořádané množině $B$. *Horní závorou* množiny $A$ je každý prvek $b \in B$, pro který platí, že $b \ge a$ pro všechna $a \in A$. Obdobně definujeme *dolní závory* množiny $A$ jako prvky $b \in A$ takové, že $b \le a$ pro všechna $a \in A$.

Nejmenší horní závora podmnožiny $A$, pokud existuje, se nazývá *supremum* této podmnožiny a značíme ji $\sup A$. Obdobně, největší dolní závora, pokud existuje, se nazývá *infimum*, píšeme $\inf A$.

Posledním axiomem v naší tabulce vlastností reálných čísel tedy předpokládáme, že pro každou množinu reálných čísel $A$ platí, že pokud existuje nějaké číslo $a$ větší nebo rovno než všechna $x \in A$, pak existuje také nejmenší takové číslo $a$. Např. volbou $A = \{x \in \mathbb{Q},\ x^2 < 2\}$ dostaneme jako její supremum $\sup A$ právě číslo $\sqrt{2}$.

Okamžitým důsledkem je také existence infim pro každou zdola ohraničenou neprázdnou množinu reálných čísel (stačí si všimnout, že obrácením znaménka všech čísel zaměníme suprema a infima).

Pro formální výstavbu další teorie ale potřebujeme vědět, zda námi požadované vlastnosti reálných čísel lze realizovat, tj. zda existuje taková uspořádaná čtveřice $(\mathbb{R}, +, \cdot, \le)$ s nosnou množinou $\mathbb{R}$ s binárními operacemi $+$ a $\cdot$ a s relací uspořádání, které všech třináct axiomů skutečně splňují. Zatím jsem zkonstruovali korektně jen čísla racionální, která tvoří uspořádané pole, tj. splňují axiomy (R1) – (R12), což si čtenář jistě snadno ověří.

v) $\lim\limits_{n\to\infty} \frac{\sqrt{4n^2+n}}{n}$,

vi) $\lim\limits_{n\to\infty} \sqrt{4n^2+n} - 2n$.

**Řešení.**

i) $\lim\limits_{n\to\infty} \frac{2n^2+3n+1}{n+1} = \lim\limits_{n\to\infty} \frac{2n+3+\frac{1}{n}}{1+\frac{1}{n}} = \infty$.

ii) $\lim\limits_{n\to\infty} \frac{2n^2+3n+1}{3n^2+n+1} = \lim\limits_{n\to\infty} \frac{2+\frac{3}{n}+\frac{1}{n^2}}{3+\frac{1}{n}+\frac{1}{n^2}} = \frac{2}{3}$.

iii) $\lim\limits_{n\to\infty} \frac{n+1}{2n^2+3n+1} = \lim\limits_{n\to\infty} \frac{1+\frac{1}{n}}{2n+3+\frac{1}{n}} = \frac{1}{\infty} = 0$.

iv) $\lim_{n\to-\infty} \frac{2^n-2^{-n}}{2^n+2^{-n}} = \lim\limits_{n\to-\infty} \frac{\frac{2^n}{2^{-n}}-1}{\frac{2^n}{2^{-n}}+1} = -1$.

v) Podle věty o třech limitách (5.21): $\forall n \in \mathbb{N}: \frac{\sqrt{4n^2}}{n} < \frac{\sqrt{4n^2+n}}{n} < \frac{\sqrt{4n^2+n+\frac{1}{16}}}{n}$. Dále pak $\lim\limits_{n\to\infty} \frac{\sqrt{4n^2}}{n} = \lim\limits_{n\to\infty} \frac{2n}{n} = 2$, $\lim\limits_{n\to\infty} \frac{\sqrt{4n^2+n+\frac{1}{16}}}{n} = \lim\limits_{n\to\infty} \frac{2n+\frac{1}{4}}{n} = 2$. Tedy i $\lim\limits_{n\to\infty} \frac{\sqrt{4n^2+n}}{n} = 2$.

vi) $\lim\limits_{n\to\infty} \sqrt{4n^2+n} - 2n = \lim\limits_{n\to\infty} \frac{(\sqrt{4n^2+n}-2n)(\sqrt{4n^2+n}+2n)}{\sqrt{4n^2+n}+2n} = \lim\limits_{n\to\infty} \frac{n}{\sqrt{4n^2+n}+2n} = \lim\limits_{n\to\infty} \frac{1}{\frac{\sqrt{4n^2+n}}{n}+2} = \frac{1}{4}$. □

**5.37.** Buď $c \in \mathbb{R}^+$ (kladné reálné číslo). Ukážeme, že $\lim\limits_{n\to\infty} \sqrt[n]{c} = 1$.

**Řešení.** Uvažme nejprve $c > 1$. Funkce $\sqrt[n]{c}$ je vzhledem k $n$ klesající a její hodnoty jsou stále větší než 1 a proto musí mít posloupnost $\sqrt[n]{c}$ limitu a tou je infimum jejich členů. Předpokládejme, že by tato limita byla větší než 1, řekněme $1+\varepsilon$, kde $\varepsilon > 0$. Pak by podle definice limity byly všechny hodnoty dané posloupnosti od jistého $m$ menší než $1+\varepsilon+\frac{\varepsilon^2}{4}$, tj. zejména $\sqrt[m]{c} < 1+\varepsilon+\frac{\varepsilon^2}{4}$. Potom by však

$$\sqrt[2m]{c} = \sqrt{\sqrt[m]{c}} < \sqrt{1+\varepsilon+\frac{\varepsilon^2}{4}} = 1+\frac{\varepsilon}{2} < 1+\varepsilon,$$

což je spor s tím, že $1+\varepsilon$ je infimem dané posloupnosti.

Pro $c = 1$ je tvrzení triviální a pro číslo $c \in (0,1)$ plyne z předchozího, uvážíme-li tvrzení pro číslo $1/c$. □

**5.38.** Stanovte



$$\lim_{n\to\infty} \sqrt[n]{n}.$$

**Řešení.** Zřejmě je $\sqrt[n]{n} \geq 1$, $n \in \mathbb{N}$. Můžeme tedy položit

$$\sqrt[n]{n} = 1 + a_n \quad \text{pro jistá čísla} \quad a_n \geq 0,\ n \in \mathbb{N}.$$

Užitím binomické věty získáváme

$$n = (1+a_n)^n = 1 + \binom{n}{1} a_n + \binom{n}{2} a_n^2 + \cdots + a_n^n, \quad n \geq 2\,(n \in \mathbb{N}).$$

Odsud plyne odhad (všechna čísla $a_n$ jsou nezáporná)

$$n \geq \binom{n}{2} a_n^2 = \frac{n\,(n-1)}{2}\, a_n^2, \quad n \geq 2\,(n \in \mathbb{N}),$$

Ve skutečnosti lze reálná čísla nejen zkonstruovat, ale také lze ukázat, že až na izomorfismus to jde jediným způsobem. Pro naši potřebu vystačíme s intuitivní představou reálné přímky. Jednoznačnosti i existenci se ještě budeme věnovat později.

**5.11. Komplexní rovina.** Připomeňme, že komplexní čísla jsou dána jako dvojice reálných čísel, které jsme zvyklí zapisovat jako $z = \operatorname{re} z + i \operatorname{im} z$. Dobrou představou o komplexních číslech je proto rovina $\mathbb{C} = \mathbb{R}^2$.



Se sčítáním a násobením splňuje pole komplexních čísel axiomy (R1)–(R9), není na nich ale žádným rozumným způsobem definováno uspořádání, které by naplnilo axiomy (R10)–R(13). Nicméně s nimi budeme také pracovat a již dříve jsme viděli, že rozšíření skalárů na komplexní čísla je často pro výpočty mimořádně užitečné nebo dokonce nutné.

Důležitou operací na komplexních číslech je tzv. *konjugace*. Je to zrcadlení podle přímky reálných čísel, tj. obrácení znaménka u imaginární složky. Značíme ji pruhem nad daným číslem $z \in \mathbb{C}$,

$$\bar{z} = \operatorname{re} z - i \operatorname{im} z.$$

Protože je pro $z = x + iy$

$$z \cdot \bar{z} = (x+iy)(x-iy) = x^2 + y^2,$$

zadává nám tento výraz právě kvadrát vzdálenosti komplexního čísla od nuly. Odmocněně z tohoto reálného nezáporného čísla říkáme absolutní hodnota komplexního čísla $z$, píšeme

$$|z|^2 = z \cdot \bar{z}\,. \tag{5.3}$$

Absolutní hodnotu máme definovánu také na každém uspořádaném poli skalárů $\mathbb{K}$, prostě definujeme *absolutní hodnotu* $|a|$ takto

$$|a| = \begin{cases} a & \text{je-li } a \geq 0, \\ -a & \text{je-li } a < 0. \end{cases}$$

Samozřejmě platí pro každá dvě čísla $a, b \in \mathbb{K}$

$$|a+b| \leq |a| + |b|. \tag{5.4}$$

Této vlastnosti říkáme trojúhelníková nerovnost a splňuje ji také absolutní hodnota komplexních čísel definovaná výše.

Zejména pro pole racionálních a reálných čísel, která jsou podmnožinami v komplexní rovině, zjevně obě definice absolutní hodnoty splývají.

**5.12. Konvergence posloupností.** V dalších odstavcích budeme pracovat s některým z číselných oborů $\mathbb{K}$ racionálních, reálných nebo komplexních čísel. V tomto kontextu je tedy třeba chápat absolutní hodnotu a skutečnost, že ve všech případech platí trojúhelníková nerovnost.



Budeme chtít formalizovat představu, že se hodnota nějakých čísel blíží dané limitě. Základním objektem pro nás proto budou posloupnosti čísel $a_i$, kde index $i$ bude zpravidla probíhat všechna přirozená čísla. Posloupnosti budeme zapisovat buď volně jako $a_0$, $a_1, \ldots$, nebo jako nekonečné vektory $(a_0, a_1, \ldots)$, případně v obdobě k zápisu matic jako $(a_i)_{i=1}^{\infty}$.

tj. po úpravě máme

$$0 \le a_n \le \sqrt{\frac{2}{n-1}}, \quad n \ge 2\,(n \in \mathbb{N}).$$

Podle Věty o třech limitách je

$$0 = \lim_{n\to\infty} 0 \le \lim_{n\to\infty} a_n \le \lim_{n\to\infty} \sqrt{\frac{2}{n-1}} = 0.$$

Obdrželi jsme tak výsledek

$$\lim_{n\to\infty} \sqrt[n]{n} = \lim_{n\to\infty} (1 + a_n) = 1 + 0 = 1.$$

Poznamenejme, že další užití Věty o třech limitách mj. dává

$$1 = \lim_{n\to\infty} 1 \le \lim_{n\to\infty} \sqrt[n]{c} \le \lim_{n\to\infty} \sqrt[n]{n} = 1$$

pro libovolné reálné číslo $c \ge 1$. □

**5.39.** Určete limitu

$$\lim_{n\to\infty} \left(\sqrt{2}\cdot\sqrt[4]{2}\cdot\sqrt[8]{2}\cdots\sqrt[2^n]{2}\right).$$

**Řešení.** Ke stanovení limity postačuje její členy vyjádřit ve tvaru

$$2^{\frac12}\cdot 2^{\frac14}\cdot 2^{\frac18}\cdots 2^{\frac{1}{2^n}} = 2^{\frac12+\frac14+\frac18+\cdots+\frac{1}{2^n}}.$$

Dostáváme tak

$$\lim_{n\to\infty} \left(\sqrt{2}\cdot\sqrt[4]{2}\cdot\sqrt[8]{2}\cdots\sqrt[2^n]{2}\right) = \lim_{n\to\infty} 2^{\frac12+\frac14+\frac18+\cdots+\frac{1}{2^n}} = \\ = 2^{\lim_{n\to\infty}\left(\frac12+\frac14+\frac18+\cdots+\frac{1}{2^n}\right)} = 2^{\sum_{n=1}^{\infty}\frac{1}{2^n}}.$$

Pomocí známého vzorce pro součet geometrické řady je

$$\sum_{n=1}^{\infty}\left(\frac12\right)^n = \frac{\frac12}{1-\frac12} = 1,$$

odkud plyne

$\lim_{n\to\infty}\left(\sqrt{2}\cdot\sqrt[4]{2}\cdot\sqrt[8]{2}\cdots\sqrt[2^n]{2}\right) = 2^1 = 2$. □

*5.40.* Stanovte

$$\lim_{n\to\infty}\left(\frac{1}{n^2}+\frac{2}{n^2}+\cdots+\frac{n-2}{n^2}+\frac{n-1}{n^2}\right).$$

○

*5.41.* Vypočítejte

$$\lim_{n\to\infty}\frac{\sqrt{n^3-11n^2+2}+\sqrt[5]{n^7-2n^5-n^3}-n+\sin^2 n}{2-\sqrt[3]{5n^4+2n^3+5}}.$$

○

*5.42.* Určete limitu

$$\lim_{n\to\infty}\frac{n!+(n-2)!-(n-4)!}{n^{50}+n!-(n-1)!}.$$

○

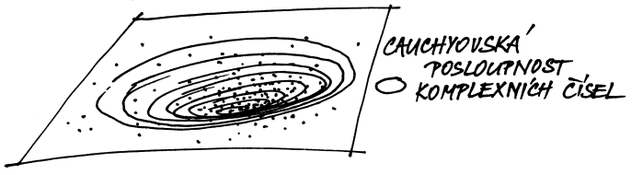
### Cauchyovské posloupnosti

Uvažme libovolnou posloupnost čísel $(a_0, a_1, \dots)$ v $\mathbb{K}$ takovou, že pro libovolné pevně zvolené kladné číslo $\varepsilon > 0$ platí pro všechny dvojice prvků $a_i$, $a_j$ posloupnosti, až na konečně mnoho výjimek (které závisí na volbě $\varepsilon$),

$$|a_i - a_j| < \varepsilon.$$

Jinak řečeno, pro každé pevné $\varepsilon > 0$ existuje index $N$ takový, že předcházející nerovnost platí pro všechna $i, j > N$. Takové posloupnosti prvků se říká *cauchyovská posloupnost*.

Intuitivně jistě cítíme, že buď jsou v takové posloupnosti všechny prvky stejné až na konečně mnoho z nich (pak bude od určitého indexu $N$ počínaje vždy $|a_i - a_j| = 0$) nebo se taková posloupnost „hromadí“ k nějaké hodnotě. Dobře je to představitelné v komplexní rovině: ať vybereme jakkoliv malý kruh (o poloměru $\varepsilon$), tak se nám jej u cauchyovské posloupnosti vždy musí podařit položit do komplexní roviny tak, že zakryje všechny body nekonečné posloupnosti $a_i$, až na konečně mnoho z nich. Můžeme si pak představit, že postupným zmenšováním se kruh smršťí až do jediné hodnoty $a$, viz obrázek.




Pokud by taková hodnota $a \in \mathbb{K}$ pro cauchyovskou posloupnost skutečně existovala, očekávali bychom od ní patrně následující vlastnost *konvergence*:

### Konvergující posloupnost

Jestliže pro posloupnost čísel $(a_0, a_1, \dots)$ v $\mathbb{K}$, pevně zvolené číslo $a \in \mathbb{K}$ a pro libovolné kladné reálné číslo $\varepsilon$ platí pro všechna $i$, až na konečně mnoho výjimek (závisejících na volbě $\varepsilon$),

$$|a_i - a| < \varepsilon,$$

říkáme, že posloupnost $(a_i)_{i=0}^{\infty}$ *konverguje* k hodnotě $a$. Číslu $a$ říkáme *limita* posloupnosti $(a_i)_{i=0}^{\infty}$.

Jestliže nějaká posloupnost čísel $a_i \in \mathbb{K}$, $i = 0, 1, \dots$, konverguje k číslu $a \in \mathbb{K}$, pak pro každé pevně zvolené kladné $\varepsilon$ víme, že $|a_i - a| < \varepsilon$ pro všechna $i$ větší než vhodné $N \in \mathbb{N}$. Pak ovšem, díky trojúhelníkové nerovnosti, pro každou dvojici indexů $i, j \ge N$ dostáváme

$$|a_i - a_j| = |a_i - a_N + a_N - a_j| < |a_i - a_N| + |a_N - a_j| < 2\varepsilon.$$

Dokázali jsme tedy:

**Lemma.** *Každá konvergující posloupnost čísel je cauchyovská.*

V poli racionálních čísel se ovšem může snadno stát, že pro cauchyovské posloupnosti příslušná hodnota $a$ neexistuje. Např. číslo $\sqrt{2}$ můžeme libovolně přesně přiblížit racionálními čísly $a_i$, dostaneme tedy konvergentní posloupnost s limitou $\sqrt{2}$, ale samotná limita již není racionální.

Uspořádaná pole skalárů, ve kterém všechny cauchyovské posloupnosti konvergují, se nazývají *úplná*. Následující tvrzení říká, že axiom (R13) takové chování reálných čísel zaručuje:

*5.43.* Udejte příklad posloupností majících nevlastní limity se členy $x_n$, $y_n$, $n \in \mathbb{N}$, pro které je

$$\lim_{n\to\infty}(x_n + y_n) = 1, \qquad \lim_{n\to\infty}\left(x_n\, y_n^2\right) = +\infty.$$

○

*5.44.* Napište všechny hromadné body posloupnosti dané členy

$$a_n = \frac{(-1)^n\, 2n}{\sqrt{4n^2+5n+3}}, \quad n \in \mathbb{N}.$$

○

*5.45.* Spočtěte

$$\limsup_{n\to\infty} a_n \quad \text{a} \quad \liminf_{n\to\infty} a_n,$$

je-li

$$a_n = \frac{n^2+4n-5}{n^2+9}\,\sin^2\frac{n\pi}{4}, \quad n \in \mathbb{N}.$$

○

*5.46.* Určete

$$\liminf_{n\to\infty}\left((-1)^n\left(1+\frac{1}{n}\right)^n + \sin\frac{n\pi}{4}\right).$$

○

**5.47.** Nyní přejděme k určování limit funkcí. Definice viz strana 252.

Určete

(a)
$$\lim_{x\to\pi/3}\sin x;$$

(b)
$$\lim_{x\to 2}\frac{x^2+x-6}{x^2-3x+2};$$

(c)
$$\lim_{x\to+\infty}\left(\arccos\frac{1}{x+1}\right)^3;$$

(d)
$$\lim_{x\to-\infty}\operatorname{arctg}\frac{1}{x}, \quad \lim_{x\to-\infty}\operatorname{arctg} x^4, \quad \lim_{x\to-\infty}\operatorname{arctg}\,(\sin x)\,.$$

**Řešení.** Případ (a). Připomeňme, že funkce je spojitá v jistém bodě, když je v tomto bodě její limita rovna funkční hodnotě. O funkci $y = \sin x$ však víme, že je spojitá na $\mathbb{R}$. Dostáváme tak

$$\lim_{x\to\pi/3}\sin x = \sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}.$$

Případ (b). Přímé dosazení $x = 2$ dává nulový čitatel i jmenovatel. Přesto je příklad velmi snadno řešitelný. Jednoduché krácení

$$\lim_{x\to 2}\frac{x^2+x-6}{x^2-3x+2} = \lim_{x\to 2}\frac{(x-2)\,(x+3)}{(x-2)\,(x-1)} = \lim_{x\to 2}\frac{x+3}{x-1} = \frac{2+3}{2-1} = 5$$

totiž vedlo ke správnému výsledku (díky spojitosti obdržené funkce v bodě $x_0 = 2$). Uvědomme si zde, že limitu můžeme počítat pouze

**Věta.** *Každá cauchyovská posloupnost reálných čísel $a_i$ konverguje k reálné hodnotě $a \in \mathbb{R}$.*



Důkaz. Každá cauchyovská posloupnost je zjevně ohraničená množina, protože pro libovolnou volbu $\varepsilon$ ohraničíme všechny členy posloupnosti až na konečně mnoho z nich. Definujme si množinu $B$ všech reálných čísel $x$, pro které platí $x < a_j$ pro všechny prvky $a_j$ posloupnosti, až na konečně mnoho z nich.

Zřejmě má $B$ horní závoru, tudíž podle axiomu (R13) má i supremum. Definujme $a = \sup B$. Nyní pro nějaké pevně zvolené $\varepsilon > 0$ zvolme $N$ takové, aby $|a_i - a_j| < \varepsilon$ pro všechna $i, j \geq N$. Zejména tedy $a_j > a_N - \varepsilon$ a $a_j < a_N + \varepsilon$ pro všechny indexy $j > N$, takže $a_N - \varepsilon$ patří do $B$, zatímco $a_N + \varepsilon$ už nikoliv. Souhrnně z toho dostáváme, že $|a - a_N| \leq \varepsilon$, a proto také

$$|a - a_j| \leq |a - a_N| + |a_N - a_j| \leq 2\varepsilon$$

pro všechna $j > N$. To ale značí právě, že $a$ je limitou uvažované posloupnosti. □

**Důsledek.** *Každá cauchyovská posloupnost komplexních čísel $z_i$ konverguje k nějakému komplexnímu číslu $z$.*

Důkaz. Pišme $z_i = a_i + i\,b_i$. Protože je $|a_i - a_j|^2 \leq |z_i - z_j|^2$ a podobně i pro hodnoty $b_i$, jsou obě posloupnosti reálných čísel $a_i$ a $b_i$ cauchyovské. Existují tedy jejich limity $a$ resp. $b$ a snadno ověříme, že $z = a + i\,b$ je limitou pro posloupnost $z_i$. □

**5.13. Poznámka.** Předchozí diskuse nám dává návod na jeden z možných postupů, jak korektně vybudovat reálná čísla. Postupujeme podobně jako při zúplňování přirozených čísel na celá (abychom přidali opačné hodnoty) a celých na racionální (abychom přidali podíly nenulových čísel). Tentokrát k racionálním číslům „přidáme“ limity všech cauchyovských posloupností.

Skutečně se podbízí zavést vhodně relaci ekvivalence na množině všech cauchyovských posloupností racionálních čísel tak, že dvě cauchyovské posloupnosti $(a_i)_{i=0}^{\infty}$ a $(b_i)_{i=0}^{\infty}$ jsou ekvivalentní, když vzdálenosti $|a_i - b_i|$ konvergují k nule (to je totéž jako požadavek, že jejich sloučením do jediné posloupnosti tak, že první posloupnost bude představovat liché, zatímco druhá sudé členy výsledné posloupnosti obdržíme opět posloupnost cauchyovskou).



Nebudeme zde teď podrobně ověřovat, že jde o ekvivalenci, ani zavádět operace násobení a sčítání, ani dokazovat, že všechny požadované axiomy skutečně dojdou naplnění. Mohou se o to ale pokusit čtenáři samostatně, protože to není složité počínání. Všechny uvedené definice lze opřít o již existující sčítání a násobení jednotlivých členů posloupností, stejně jako definici vzdálenosti čísel. Jediný náročnější bod je v důkazu, že takto definovaných „nových“ reálných čísel již bude dost, tj. že již bude platit axiom (R13) o existenci suprema. Tady je asi nejjednodušší ukázat, že každé úplné pole splňuje tento axiom, tj. že stačí ověřit, že cauchyovské posloupnosti vždy konvergují (a to v našem případě již není složité). Stejně tak je docela snadné dokázat, že axiomy (R1)–(R13) definují reálné čísla jednoznačně až na izomorfismus, tj. až na bijektivní zobrazení, která zachovávají jak algebraické operace, tak uspořádání.

Ještě se k těmto poznámkám později vrátíme v souvislosti se zúplněním metrických prostorů, která budeme diskutovat ve druhé části 7. kapitoly na straně 414.

z funkčních hodnot v libovolně malém okolí daného bodu $x_0$ a že přitom limita nezávisí na hodnotě přímo v tomto bodě. Při počítání limit tedy můžeme využívat krácení a rozšiřování výrazů, které nemění hodnoty uvažované funkce v libovolně zvoleném ryzím okolí bodu $x_0$.

Případ (c). Dvojnásobná záměna pořadí limity a vnější funkce převádí původní limitu na

$$\left(\arccos\left(\lim_{x\to+\infty}\frac{1}{x+1}\right)\right)^3.$$

Lehce určíme, že

$$\lim_{x\to+\infty}\frac{1}{x+1}=0.$$

Neboť je funkce $y=\arccos x$ spojitá v bodě 0, ve kterém nabývá hodnoty $\pi/2$, a funkce $y=x^3$ je spojitá v bodě $\pi/2$, platí

$$\lim_{x\to+\infty}\left(\arccos\frac{1}{x+1}\right)^3=\left(\arccos\left(\lim_{x\to+\infty}\frac{1}{x+1}\right)\right)^3=\left(\frac{\pi}{2}\right)^3.$$

Případ (d). Funkce $y=\operatorname{arctg} x$ má vlastnosti „užitečné při počítání limit" – je spojitá a prostá (rostoucí) na celé reálné ose. Tyto vlastnosti vždy (bez dalších podmínek či omezení) umožňují vnořit vyšetřovanou limitu do argumentu takové reálné funkce. Proto uvažujme

$$\operatorname{arctg}\left(\lim_{x\to-\infty}\frac{1}{x}\right),\quad \operatorname{arctg}\left(\lim_{x\to-\infty}x^4\right),\quad \operatorname{arctg}\left(\lim_{x\to-\infty}\sin x\right).$$

Zřejmě je

$$\lim_{x\to-\infty}\frac{1}{x}=0,\qquad \lim_{x\to-\infty}x^4=+\infty$$

a limita $\lim_{x\to-\infty}\sin x$ neexistuje, což již implikuje

$$\lim_{x\to-\infty}\operatorname{arctg}\frac{1}{x}=\operatorname{arctg}0=0,\qquad \lim_{x\to-\infty}\operatorname{arctg}x^4=\lim_{y\to+\infty}\operatorname{arctg}y=\frac{\pi}{2}$$

a neexistenci poslední limity. □

**5.48.** Určete limitu

$$\lim_{x\to0}\frac{1-\cos x}{x^2\sin(x^2)}.$$

**Řešení.**

$$\begin{aligned}\lim_{x\to0}\frac{1-\cos x}{x^2\sin(x^2)}&=\lim_{x\to0}\frac{2\sin^2\left(\frac{x}{2}\right)}{x^2\sin(x^2)}=\\&=\lim_{x\to0}\frac{\frac{1}{2}\sin^2\left(\frac{x}{2}\right)}{\left(\frac{x}{2}\right)^2\sin(x^2)}=\\&=\frac{1}{2}\left(\lim_{x\to0}\frac{\sin\left(\frac{x}{2}\right)}{\frac{x}{2}}\right)^2\cdot\lim_{x\to0}\frac{1}{\sin^2(x^2)}=\frac{1}{2}\cdot\infty=\\&=\infty.\end{aligned}$$

Předchozí výpočet je nutné chápat „odzadu". Protože existují limity na pravé straně (ať už vlastní či nevlastní) a výraz $\frac{1}{2}\cdot\infty$ má smysl

**5.14. Uzavřené množiny.** Pro další práci s reálnými nebo komplexními čísly budeme potřebovat podrobnější pochopení pojmů jako blízkost, omezenost, konvergence apod. Pro jakoukoliv podmnožinu $A$ bodů v $\mathbb{K}$ nás budou zajímat nejen její body $a\in A$ ale také body, ke kterým se umíme dostat limitně, tj. pomocí limit posloupností.



HROMADNÉ BODY MNOŽINY

Uvažme jakoukoliv množinu $A$ bodů v $\mathbb{K}$. Bod $x\in\mathbb{K}$ nazýváme *hromadný bod množiny* $A$, jestliže existuje posloupnost $a_0, a_1, \ldots$ vybraná z prvků $A$, jejíž všechny členy jsou různé od $x$ a která konverguje k hodnotě $x$.

Hromadné body podmnožiny $A$ racionálních, reálných nebo komplexních čísel jsou tedy ta čísla $x$, která jsou limitami takových posloupností čísel z $A$, které samotný bod $x$ neobsahují. Všimněme si, že hromadný bod množiny do ní může, ale nemusí, patřit.

Pro každou neprázdnou množinu $A\subset\mathbb{K}$ a pevný bod $x\in\mathbb{K}$ je množina všech vzdáleností $|x-a|$, $a\in A$, zdola ohraničená množina reálných čísel, má tedy infimum $d(x,A)$, kterému říkáme *vzdálenost bodu $x$ od množiny $A$*. Všimněme si, že $d(x,A)=0$, právě když buď $x\in A$ nebo je $x$ aspoň hromadným bodem $A$ (dokažte si podrobně z definic).

UZAVŘENÉ MNOŽINY

*Uzávěr* $\bar{A}$ množiny $A\subseteq\mathbb{K}$ je množina všech bodů, které mají od $A$ vzdálenost nulovou (všimněme si, že pro prázdnou množinu není vzdálenost bodů od ní definována, je tedy automaticky $\bar{\emptyset}=\emptyset$).

*Uzavřená podmnožina* v $\mathbb{K}$ je taková, která splývá se svým uzávěrem. Jsou to tedy právě množiny, které obsahují i všechny své hromadné body. Typickou uzavřenou množinou je tzv. *uzavřený interval*

$$[a,b]=\{x\in\mathbb{R},\ a\le x\le b\}$$

reálných čísel, kde $a$ a $b$ jsou daná reálná číslo.

Pokud některá z hraničních hodnot intervalu chybí, píšeme $a=-\infty$ (mínus nekonečno) nebo podobně $b=+\infty$, a takové uzavřené intervaly značíme $(-\infty,b]$, $[a,\infty)$ a $(-\infty,\infty)$.

Uzavřené množiny jsou tedy ty, které v sobě mají i vše, k čemu umí „dokonvergovat". Uzavřenou množinu bude tvořit např. posloupnost reálných čísel bez hromadného bodu nebo posloupnost s konečným počtem hromadných bodů spolu s těmito body. Uzavřený je také např. jednotkový kruh v rovině komplexních čísel včetně hraniční kružnice.

Snadno ověříme, že libovolný průnik a libovolné konečné sjednocení uzavřených množin opět uzavřená množina. Skutečně, pokud všechny body nějaké posloupnosti patří do průniku našeho systému množin, pak jistě patří do každé z nich, a proto do každé z nich patří i všechny hromadné body. Pokud bychom ale chtěli totéž říci o obecném sjednocení systému množin $A_i$, pak bychom neuspěli, protože např. jednobodové množiny jsou zjevně uzavřené, ale z nich utvořená posloupnost bodů už uzavřená nebývá. Pokud ale jde o konečné sjednocení množin a hromadný bod nějaké posloupnosti ležící v tomto sjednocení, pak takový hromadný bod musí být hromadným bodem i vybrané podposloupnosti, která ale už bude celá v jedné z našich množin. Každá je ale uzavřená, takže i hromadný bod do ní a tedy i celého sjednocení patří.

(viz Poznámka za větou 5.22), existuje i původní limita. Kdybychom původní limitu rozdělili na součin limit

$$\lim_{x\to 0}(1-\cos x)\cdot\lim_{x\to 0}\frac{1}{x^2\sin(x^2)},$$

jednalo by se o součin typu $0\cdot\infty$, tedy nedefinovaný výraz, ale tento fakt nevypovídá nic o existenci původní limity. □

**5.49.** Určete následující limity:

i) $\lim_{x\to 2}\frac{x-2}{\sqrt{x^2-4}}$, ii) $\lim_{x\to 0}\frac{\sin(\sin x)}{x}$,
iii) $\lim_{x\to 0}\frac{\sin^2 x}{x}$, iv) $\lim_{x\to 0} e^{\frac{1}{x}}$.

**Řešení.** i) $\lim_{x\to 2}\frac{x-2}{\sqrt{x^2-4}}=\lim_{x\to 2}\frac{x-2}{\sqrt{(x-2)(x+2)}}=\lim_{x\to 2}\frac{\sqrt{x-2}}{\sqrt{x+2}}=$
$=\frac{0}{4}=0.$

ii) $\lim_{x\to 2}\frac{x-2}{\sqrt{x^2-4}}\overset{(5.27)}{=}\lim_{y\to 0}\frac{\sin y}{y}=1$, kde jsme využili toho, že $\lim_{x\to 0}\sin x=0$.

iii) $\lim_{x\to 0}\frac{\sin^2 x}{x}=\lim_{x\to 0}\sin x\cdot\lim_{x\to 0}\frac{\sin x}{x}=0\cdot 1=0$. Opět původní limita existuje, protože existují obě limity na pravé straně rovnosti a jejich součin je definován.

iv) Při výpočtu této limity musíme být obezřetní, protože obě jednostranné limity v bodě nula existují, jejich hodnoty se však liší, zkoumaná limita tedy neexistuje:

$$\lim_{x\to 0_+} e^{\frac{1}{x}}=e^{\lim_{x\to 0_+}\frac{1}{x}}=e^{\infty}=\infty,$$
$$\lim_{x\to 0_-} e^{\frac{1}{x}}=e^{\lim_{x\to 0_-}\frac{1}{x}}=e^{-\infty}=0\,.$$ □

**5.50.** Určete

(a) $\lim_{x\to 2}\frac{x+2}{(x-2)^6}$, (b) $\lim_{x\to 2}\frac{x+2}{(x-2)^5}$,
(c) $\lim_{x\to+\infty}\left(2+\frac{1}{x}\right)^{\frac{1}{x}}$, (d) $\lim_{x\to+\infty} x^{-x}$.

**Řešení.**

V tomto příkladu se budeme věnovat tzv. neurčitým výrazům.



Přesněji řečeno, budeme se zabývat situacemi, kdy se o ně nejedná. Čtenáři doporučujeme, aby neurčité výrazy vnímal jako pojem pomocný, který mu má pouze usnadnit orientování se při prvním počítání limit, neboť obdržený neurčitý výraz pouze znamená, že jsme „nic nezjistili“. Víme, že limita součtu je součet limit, limita součinu je součin limit a že limita podílu je podíl limit, pokud jednotlivé limity existují a nezískáme-li některý z výrazů $\infty-\infty$, $0\cdot\infty$, $0/0$, $\infty/\infty$, o kterých právě hovoříme jako o neurčitých. Pro úplnost dodejme, že tato pravidla můžeme kombinovat (pro limity všech složek určené současně) a že za neurčitý výraz pak považujeme také ten, jenž obsahuje alespoň jeden neurčitý výraz. Např. tedy výrazy

**5.15. Otevřené množiny.** Dalším užitečným příkladem podmnožin jsou *otevřené intervaly* reálných čísel

$$(a,b)=\{x\in\mathbb{R};\ a<x<b\},$$

kde opět $a$ i $b$ jsou pevná reálná čísla nebo nekonečné hodnoty $\pm\infty$. Jde o typickou otevřenou množinu v následujícím smyslu:

OTEVŘENÉ MNOŽINY A OKOLÍ BODŮ

*Otevřená množina* v $\mathbb{K}$ je taková množina, jejíž doplněk je uzavřenou množinou.

*Okolím bodu* $a\in\mathbb{K}$ nazýváme libovolnou otevřenou množinu $\mathcal{O}$, která $a$ obsahuje. Je-li okolí definované jako

$$\mathcal{O}_\delta(a)=\{x\in\mathbb{K},\ |x-a|<\delta\}$$

pro kladné číslo $\delta$, hovoříme o *$\delta$-okolí* bodu $a$.

Všimněme si, že pro libovolnou množinu $A$ je $a\in\mathbb{K}$ hromadným bodem $A$, právě když v libovolném okolí $a$ leží také alespoň jeden bod $b\in A$, $b\neq a$.

**Lemma.** *Množina čísel $A\subseteq\mathbb{K}$ je otevřená, právě když každý její bod $a\in A$ do ní patří i s nějakým svým okolím.*

DŮKAZ. Nechť je $A$ otevřená a $a\in A$. Kdyby neexistovalo žádné okolí bodu $a$ uvnitř $A$, musela by existovat posloupnost $a_n\notin A$, $|a-a_n|\le 1/n$. Pak je ovšem $a\in A$ hromadným bodem množiny $\mathbb{K}\setminus A$, což není možné, protože doplněk $A$ je uzavřený.

Naopak předpokládejme, že každé $a\in A$ leží v $A$ i s nějakým svým okolím. To přirozeně zabraňuje, aby nějaký hromadný bod $b$ pro množinu $\mathbb{K}\setminus A$ ležel v $A$. Je proto $\mathbb{K}\setminus A$ uzavřená a tedy je $A$ otevřená. □

Z právě dokázaného lemmatu okamžitě vyplývá, že je libovolné sjednocení otevřených množin opět otevřenou množinou a že každý konečný průnik otevřených množin je opět otevřená množina.

V případě reálných čísel jsou $\delta$–okolí právě otevřené intervaly o délce $2\delta$ s $a$ uprostřed. V komplexní rovině je $\delta$–okolí kruh o poloměru $\delta$ se středem v $a$.

**5.16. Ohraničené a kompaktní množiny čísel.** Uzavřené a otevřené množiny představují základní pojmy tzv. *topologie*. Aniž bychom zacházeli do hlubších podrobností a souvislostí, seznámili jsme se právě s *topologií reálné přímky* a *topologií komplexní roviny*. Velice užitečné budou i následující pojmy:



OHRANIČENÉ A KOMPAKTNÍ MNOŽINY

Množina $A$ racionálních, reálných nebo komplexních čísel se nazývá *ohraničená*, jestliže existuje kladné reálné číslo $r$ takové, že $|z|\le r$ pro všechna čísla $z\in A$. V opačném případě je *neohraničená*.

Ohraničená a uzavřená množina se nazývá *kompaktní*.

Uzavřené konečné intervaly reálných čísel jsou typickým příkladem množin kompaktních.

Pro podmnožiny $A$ reálných čísel definujeme jejich *průměr* $d(A)=\sup\{|x-y|,\ x,y\in A\}$. Zjevně platí, že $A$ je ohraničená, právě když $d(A)<\infty$, a $A$ je neohraničená, právě když $d(A)=\infty$.

Přidejme ještě několik topologických pojmů, které nám umožní účinné vyjadřování:

$$-\infty+\infty=\infty-\infty,\quad \frac{-\infty}{3+\infty}=-\frac{\infty}{\infty},$$
$$\frac{0}{(-\infty)^3+\infty}=0\cdot(\infty-\infty)^{-1}$$

označujeme jako neurčité a o výrazech

$$-\infty-\infty,\quad \frac{0}{3+\infty},\quad \frac{0}{(-\infty)^3-\infty}$$

můžeme říci, že jsou „určité“ (pro ně jsme schopni ihned příslušnou limitu stanovit – výrazy odpovídají po řadě hodnotám $-\infty, 0, 0$).

V případě (a) podíl limit čitatele a jmenovatele dává výraz $4/0$. Zápis, ve kterém dělíme nulou, je sám o sobě přinejmenším nežádoucí (později bychom se mu měli být schopni vyvarovat). Přesto nám umožní stanovit výsledek: nejedná se o neurčitý výraz. Všimněme si, že jmenovatel se blíží k nule zprava (pro $x\neq 2$ je $(x-2)^6>0$). To zapisujeme jako $4/+0$. Čitatel a jmenovatel tak mají stejné znaménko v jistém ryzím okolí bodu $x_0=2$ a lze říci, že jmenovatel je v limitě „nekonečněkrát menší“ než čitatel, tj.

$$\lim_{x\to 2}\frac{x+2}{(x-2)^6}=+\infty,$$

což odpovídá položení $4/+0=+\infty$ (podobně se klade $4/-0=-\infty$).

Při určování druhé limity lze postupovat analogicky. Protože čísla $a\in\mathbb{R}$ a $a^5$ mají stejná znaménka, dostáváme

$$\lim_{x\to 2+}\frac{x+2}{(x-2)^5}=+\infty\neq-\infty=\lim_{x\to 2-}\frac{x+2}{(x-2)^5},$$

tj. oboustranná limita neexistuje. Tomu odpovídá zápis $4/\pm 0$ (nebo obecnější $a/\pm 0$, $a\neq 0$, $a\in\mathbb{R}^*$), který je „určitým výrazem“. Při důsledném oddělování symbolů $+0$ a $-0$ od $\pm 0$ vždy $a/\pm 0$ pro $a\neq 0$ znamená, že limita neexistuje.

Případy (c), (d). Je-li $f(x)>0$ pro všechna uvažovaná $x\in\mathbb{R}$, platí

$$f(x)^{g(x)}=\mathrm{e}^{\ln\left(f(x)^{g(x)}\right)}=\mathrm{e}^{g(x)\cdot\ln f(x)}.$$

Využijeme-li toho, že exponenciální funkce je spojitá a prostá na reálné přímce, můžeme nahradit limitu

$$\lim_{x\to x_0} f(x)^{g(x)}$$

za

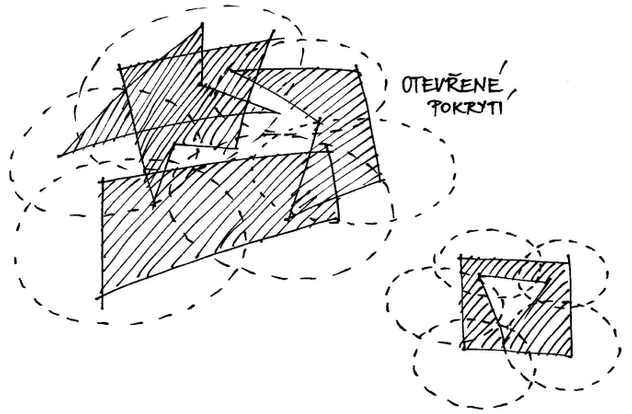
$$\mathrm{e}^{\lim\limits_{x\to x_0}(g(x)\cdot\ln f(x))}.$$

*Vnitřním bodem množiny* $A$ reálných nebo komplexních čísel nazveme takový bod, který do $A$ patří i s nějakým svým okolím.

*Hraniční bodem* množiny $A$ rozumíme takový bod, jehož každé okolí má neprázdný průnik jak s $A$ tak s doplňkem $\mathbb{K}\setminus A$. Hraniční bod tedy může, ale nemusí patřit do samotné množiny $A$.

*Otevřené pokrytí* množiny $A$ je takový systém otevřených množin $U_i$, $i\in I$, že jejich sjednocení obsahuje celé $A$.

*Izolovaným bodem* množiny $A$ rozumíme bod $a\in A$, který má okolí, jehož průnik s $A$ je právě jednobodová množina $\{a\}$.




**5.17. Věta.** *Pro podmnožiny $A$ reálných čísel platí:*

*(1) neprázdná množina $A$ je otevřená, právě když je sjednocením nejvýše spočetného systému otevřených intervalů,*
*(2) každý bod $a\in A$ je buď vnitřní nebo hraniční,*
*(3) každý hraniční bod množiny $A$ je buď izolovaným nebo hromadným bodem $A$,*
*(4) $A$ je kompaktní, právě když každá v ní obsažená nekonečná posloupnost má podposloupnost konvergující k bodu v $A$,*
*(5) $A$ je kompaktní, právě když každé její otevřené pokrytí obsahuje konečné podpokrytí.*

Důkaz. (1) Zjevně je každá otevřená množina sjednocením nějakých okolí svých bodů, tj. otevřených intervalů. Jde tedy pouze o to, jestli nám jich vždy stačí spočetně mnoho. Zkusme tedy najít „co největší“ intervaly. Řekneme, že body $a,b\in A$ jsou v relaci, jestliže celý otevřený interval $(\min\{a,b\},\max\{a,b\})$ je podmnožinou v $A$. To je zjevně relace ekvivalence (otevřený interval $(a,a)$ je prázdná množina a ta je podmnožinou, symetrie relace i tranzitivita jsou zřejmé). Třídy této ekvivalence budou zjevně intervaly, které budou navíc po dvou disjunktní. Každý z těchto intervalů jistě musí obsahovat nějaké racionální číslo a tyto musí být různé. Všech racionálních čísel je ale spočetně mnoho, proto máme tvrzení dokázané.

(2) Přímo z definic vyplývá, že bod nemůže být vnitřní a hraniční zároveň. Nechť tedy $a\in A$ není vnitřní. Pak ovšem existuje posloupnost bodů $a_i\notin A$ s hromadným bodem $a$. Zároveň $a$ patří do každého svého okolí. Proto je $a$ hraniční.

(3) Předpokládejme, že $a\in A$ je hraniční a není izolovaný. Pak stejně jako v argumentaci předchozího odstavce existují body $a_i$, tentokrát uvnitř $A$, jejichž hromadným bodem je $a$.

(4) Předpokládejme, že je $A$ kompaktní, tj. uzavřená a ohraničená, a uvažme nějakou nekonečnou posloupnost bodů $a_i\in A$. Tato podmnožina má jistě supremum $b$ i infimum

Připomeňme, že jedna z těchto limit existuje právě tehdy, když existuje druhá; a doplňme

$$\begin{aligned}
\lim_{x\to x_0}(g(x)\cdot\ln f(x)) &= a\in\mathbb{R} \quad\Longrightarrow\quad \lim_{x\to x_0} f(x)^{g(x)} = \mathrm{e}^a,\\
\lim_{x\to x_0}(g(x)\cdot\ln f(x)) &= +\infty \quad\Longrightarrow\quad \lim_{x\to x_0} f(x)^{g(x)} = +\infty,\\
\lim_{x\to x_0}(g(x)\cdot\ln f(x)) &= -\infty \quad\Longrightarrow\quad \lim_{x\to x_0} f(x)^{g(x)} = 0.
\end{aligned}$$

Můžeme tudíž psát

$$\lim_{x\to x_0} f(x)^{g(x)} = \mathrm{e}^{\lim\limits_{x\to x_0} g(x)\cdot\lim\limits_{x\to x_0}\ln f(x)},$$

jestliže obě limity vpravo existují a neobdržíme-li neurčitý výraz $0\cdot\infty$. Není obtížné si uvědomit, že tento neurčitý výraz lze získat pouze ve třech případech odpovídajících zbylým neurčitým výrazům $0^0$, $\infty^0$, $1^\infty$, kdy postupně je

$$\begin{aligned}
\lim_{x\to x_0} f(x) = 0 \quad &\text{a} \quad \lim_{x\to x_0} g(x) = 0,\\
\lim_{x\to x_0} f(x) = +\infty \quad &\text{a} \quad \lim_{x\to x_0} g(x) = 0,\\
\lim_{x\to x_0} f(x) = 1 \quad &\text{a} \quad \lim_{x\to x_0} g(x) = \pm\infty.
\end{aligned}$$

V ostatních případech nám tedy znalost (a pochopitelně existence) limit

$$\lim_{x\to x_0} f(x), \qquad \lim_{x\to x_0} g(x)$$

umožňuje uvést výsledek (při dodefinování některých zápisů)

$$\lim_{x\to x_0} f(x)^{g(x)} = \left(\lim_{x\to x_0} f(x)\right)^{\lim\limits_{x\to x_0} g(x)}.$$

Protože

$$\lim_{x\to+\infty}\left(2+\frac{1}{x}\right) = 2, \quad \lim_{x\to+\infty}\frac{1}{x} = 0, \quad \lim_{x\to+\infty} x = +\infty,$$

je

$$\lim_{x\to+\infty}\left(2+\frac{1}{x}\right)^{\frac{1}{x}} = 2^0 = 1,$$

$$\lim_{x\to+\infty} x^{-x} = \lim_{x\to+\infty}\left(\frac{1}{x}\right)^x = 0$$

nebo

$$\lim_{x\to+\infty} x^{-x} = \lim_{x\to+\infty}\left(x^x\right)^{-1} = 0.$$

Poslední výsledek pak bychom mohli vyjádřit zápisem $0^\infty = 0$ či $\infty^\infty = \infty$, $\infty^{-1} = 0$ (zdůrazněme, že se nejedná o neurčité výrazy).

Přestože jsme kladli důraz na to, aby čtenář raději upřednostňoval úvahy o limitním chování funkcí před škatulkováním výrazů na určité a neurčité (a tyto pojmy vnímal jen jako pomocné), je snad dobře patrný důvod, proč se budeme nadále zabývat především neurčitými výrazy. □

$a$ (nebo můžeme zvolit libovolnou horní a dolní závoru množiny $A$). Rozdělme nyní interval $[a,b]$ přesně na dvě poloviny $\left[a,\frac{1}{2}(b-a)\right]$ a $\left[\frac{1}{2}(b-a),b\right]$. V alespoň jedné z nich musí být nekonečně mnoho prvků $a_i$. Vyberme takovou polovinu, jeden z prvků v ní obsažených a následně tento vybraný interval opět rozdělme na poloviny. Pak znovu vybereme tu polovinu, kde je nekonečně mnoho prvků posloupnosti a vybereme si jeden z nich. Tímto způsobem dostaneme posloupnost, která bude cauchyovská (dokažte si detailně – vyžaduje to jen pozorné hraní si s odhady, podobně jako výše). O cauchyovských posloupnostech ovšem už víme, že mají vždy hromadné body nebo jsou konstantní až na konečně mnoho výjimek. Existuje tedy podposloupnost s námi hledanou limitou. Z uzavřenosti $A$ zase vyplývá, že námi nalezený bod musí opět ležet v $A$.

Opačně, jestliže každá v $A$ obsažená nekonečná podmnožina má hromadný bod v $A$, znamená to, že všechny hromadné body jsou v $A$ a tedy je $A$ uzavřená. Pokud by nebyla množina $A$ zároveň ohraničená, uměli bychom najít posloupnost stále rostoucí nebo klesající s rozdíly dvou po sobě jdoucích čísel třeba alespoň 1. Taková posloupnost bodů z $A$ ale nemůže mít hromadný bod vůbec.

(5) Nejprve se věnujme snadnější implikaci, tj. předpokládejme, že z každého otevřeného pokrytí lze vybrat konečné a dokazujme, že pak $A$ je uzavřená i ohraničená. Jistě lze $A$ pokrýt spočetným systémem intervalů $I_n = (n-2, n+2)$, $n\in\mathbb{Z}$, a jakýkoliv výběr konečného podpokrytí z nich říká, že je množina $A$ ohraničená.



Předpokládejme nyní, že $a\in\mathbb{R}\setminus A$ je hromadným bodem posloupnosti $a_i\in A$ a předpokládejme rovnou, že $|a-a_n|<\frac{1}{n}$ (jinak bychom mohli vybrat takovou podposloupnost). Množiny

$$J_n = \mathbb{R}\setminus\left[a-\frac{1}{n}, a+\frac{1}{n}\right]$$

pro všechna $n\in\mathbb{N}$, $n>0$, jsou sjednocení dvou otevřených intervalů a jistě také pokrývají naši množinu $A$. Protože je možné vybrat konečné pokrytí $A$, bod $a$ je uvnitř doplňku $\mathbb{R}\setminus A$ včetně nějakého svého okolí a není tedy hromadným bodem. Proto musí být všechny hromadné body $A$ opět v $A$ a tato množina je i uzavřená.

Opačný směr důkazu je založený na existenci a vlastnostech suprema. Předpokládejme, že je $A$ kompaktní a že je dáno nějaké její otevřené pokrytí $\mathcal{C}$. Z předchozího je zjevné, že v $A$ existují největší a nejmenší prvek, které jsou zároveň rovny $b=\sup A$ a $a=\inf A$. Označme si teď „nejzazší mez“, pro kterou ještě půjde konečné pokrytí z $\mathcal{C}$ vybrat, tj. definujeme množinu

$$B = \{x\in[a,b];\ \text{existuje konečné podpokrytí } [a,x]\cap A\}.$$

Evidentně $a\in B$, jde tedy o neprázdnou shora ohraničenou množinu a existuje proto $c=\sup B$. Jde nám o to dokázat, že ve skutečnosti musí být $c=b$.

Argumentace je trochu nepřehledná, dokud si ji nenačrtneme na obrázku, podstata je ale snadná: Víme, že $a\le c\le b$, předpokládejme tedy chvíli, že $c<b$ a $c\notin A$. Protože je $\mathbb{R}\setminus A$ otevřená, pro $c\notin A$ existuje okolí bodu $c$ obsažené v $[a,b]$ a zároveň disjunktní s $A$. To by ale vylučovalo možnost $c=\sup B$.

Zbývá tedy v takovém případě $c<b$ a $c\in A$ a tedy je i nějaké okolí $\mathcal{O}$ bodu $c$ v otevřeném pokrytí $\mathcal{C}$. Zvolme si body $p<c<q$ v $\mathcal{O}$. Opět nyní bude existovat konečné pokrytí pro $[a,q]\cap A$. To

**5.51.** Vypočítejte

$$\lim_{x\to+\infty}\frac{\sin x+\pi x^2}{2\cos x-1-x^2};$$
$$\lim_{x\to+\infty}\frac{3^{x+1}+x^5-4x}{3^x+2^x+x^2};$$
$$\lim_{x\to+\infty}\frac{4^x-8x^6-2^x-167}{3^x-45x-\sqrt{11}\pi^{x+12}};$$
$$\lim_{x\to+\infty}\frac{\sqrt{x}-\sin^3 x+x\operatorname{arctg} x}{\sqrt{1+2x+x^2}}.$$

**Řešení.** Vydělíme-li v případě první z limit čitatele i jmenovatele polynomem $x^2$, obdržíme

$$\lim_{x\to+\infty}\frac{\sin x+\pi x^2}{2\cos x-1-x^2}=\lim_{x\to+\infty}\frac{\frac{\sin x}{x^2}+\pi}{\frac{2\cos x-1}{x^2}-1}.$$

Ohraničenost výrazů

$$|\sin x|\le 1,\quad |2\cos x-1|\le 3\quad\text{pro}\quad x\in\mathbb{R}$$

a $x^2\to+\infty$ pro $x\to+\infty$ pak dávají výsledek

$$\lim_{x\to+\infty}\frac{\frac{\sin x}{x^2}+\pi}{\frac{2\cos x-1}{x^2}-1}=\frac{0+\pi}{0-1}=-\pi.$$

V předešlé úvaze jsme vlastně použili Větu o třech limitách a zápis $c/\infty=0$ platný pro $c\in\mathbb{R}$ (nebo přímo ohr./$\infty=0$, kde „ohr.“ značí ohraničenou funkci).

Tento postup lze zobecnit. Pro limitu tvaru

$$\lim_{x\to x_0}\frac{f_1(x)+f_2(x)+\cdots+f_m(x)}{g_1(x)+g_2(x)+\cdots+g_n(x)},$$

přičemž

$$\lim_{x\to x_0}\frac{f_i(x)}{f_1(x)}=0,\quad i\in\{2,\dots,m\},$$
$$\lim_{x\to x_0}\frac{g_i(x)}{g_1(x)}=0,\quad i\in\{2,\dots,n\},$$

platí

$$\lim_{x\to x_0}\frac{f_1(x)+f_2(x)+\cdots+f_m(x)}{g_1(x)+g_2(x)+\cdots+g_n(x)}=\lim_{x\to x_0}\frac{f_1(x)}{g_1(x)},$$

pokud limita na pravé straně existuje. Je přitom výhodné si uvědomit (třetí z limit lze určit např. pomocí l'Hospitalova pravidla, se kterým se seznámíme později), že

$$\lim_{x\to+\infty}\frac{c}{x^\alpha}=0,\ \lim_{x\to+\infty}\frac{x^\alpha}{x^\beta}=0,\ \lim_{x\to+\infty}\frac{x^\beta}{a^x}=0,\ \lim_{x\to+\infty}\frac{a^x}{b^x}=0$$

pro

$$c\in\mathbb{R},\quad 0<\alpha<\beta,\quad 1<a<b.$$

ale značí, že $q>c$ leží v $B$, což není možné. Původní volba $c<b$ tedy vedla ke sporu, což dokazuje požadovanou rovnost $b=c$. Nyní ale s pomocí okolí $b$, které patří do $\mathcal{C}$ umíme najít konečné pokrytí v $\mathcal{C}$ pro celé $A$. □

**5.18. Limity funkcí a posloupností.** Pro diskusi limit je vhodné rozšířit množinu reálných čísel $\mathbb{R}$ o dvě nekonečné hodnoty $\pm\infty$, tak jak jsme to už dělali při označování intervalů.



Okolím nekonečna rozumíme interval $(a,\infty)$, resp. $(-\infty,a)$ je okolí $-\infty$. Pojem hromadného bodu množin rozšiřujeme tak, že $\infty$ je hromadným bodem množiny $A\subseteq\mathbb{R}$ jestliže každé okolí $\infty$ s ní má neprázdný průnik, tj. jestliže je $A$ shora neohraničená. Obdobně pro $-\infty$. Hovoříme o *nevlastních hromadných bodech* množiny $A$.

### „POČÍTÁNÍ S NEKONEČNY“

Zavádíme i pravidla pro počítání s formálně přidanými hodnotami $\pm\infty$ a pro libovolná „konečná“ čísla $a\in\mathbb{R}$:

$$a+\infty=\infty,$$
$$a-\infty=-\infty,$$
$$a\cdot\infty=\infty,\ \text{je-li } a>0,$$
$$a\cdot\infty=-\infty,\ \text{je-li } a<0,$$
$$a\cdot(-\infty)=-\infty,\ \text{je-li } a>0,$$
$$a\cdot(-\infty)=\infty,\ \text{je-li } a<0,$$
$$\frac{a}{\pm\infty}=0\ \text{pro všechna } a\neq 0.$$

Následující definice pokrývá mnoho případů limitních procesů a bude třeba ji zvládnout dokonale. Jednotlivými případy se budeme podrobně zabývat vzápětí.

### REÁLNÉ A KOMPLEXNÍ LIMITY

**Definice.** Uvažme libovolnou podmnožinu $A\subseteq\mathbb{R}$ a reálnou funkci $f:A\to\mathbb{R}$, případně komplexní funkci $f:A\to\mathbb{C}$, definovanou na $A$. Uvažme dále hromadný bod $x_0$ množiny $A$ (tj. buď reálné číslo nebo případně $\pm\infty$).



Říkáme, že $f$ má v $x_0$ *limitu* $a\in\mathbb{R}$, případně komplexní limitu $a\in\mathbb{C}$, a píšeme

$$\lim_{x\to x_0}f(x)=a,$$

jestliže pro každé okolí $\mathcal{O}(a)$ bodu $a$ lze najít okolí $\mathcal{O}(x_0)$ bodu $x_0$ takové, že pro všechna $x\in A\cap(\mathcal{O}(x_0)\setminus\{x_0\})$ je $f(x)\in\mathcal{O}(a)$.

V případě reálné funkce může také být limitní hodnotou $a=\pm\infty$ a v takovém případě se limita $a$ reálné funkce nazývá *nevlastní*. V případě $a\in\mathbb{R}$ je o limitu *vlastní*.

Je důležité si všimnout, že hodnota $f$ v bodě $x_0$ v definici nevystupuje a $f$ v tomto hromadném bodě vůbec nemusí být definována (a v případě nevlastního hromadného bodu ani nemůže)! Často také hovoříme o *ryzím okolí* $\mathcal{O}(x_0)\setminus\{x_0\}$, ve kterém nás funkční hodnoty zajímají.

Nevlastní limity komplexních funkcí zatím definovat nebudeme.

Odtud ihned plyne

$$\lim_{x\to+\infty}\frac{3^{x+1}+x^5-4x}{3^x+2^x+x^2}=\lim_{x\to+\infty}\frac{3\cdot 3^x}{3^x}=3;$$

$$\lim_{x\to+\infty}\frac{4^x-8x^6-2^x-167}{3^x-45x-\sqrt{11}\pi^{x+12}}=\lim_{x\to+\infty}\frac{4^x}{-\sqrt{11}\pi^{12}\cdot\pi^x}=-\infty.$$

Uvědomíme-li si, že je

$$\lim_{x\to+\infty}\operatorname{arctg} x=\frac{\pi}{2}\geq 1,$$

stejně snadno dostaneme

$$\lim_{x\to+\infty}\frac{\sqrt{x}-\sin^3 x+x\operatorname{arctg} x}{\sqrt{1+2x+x^2}}=\lim_{x\to+\infty}\frac{x\operatorname{arctg} x}{\sqrt{x^2}}=$$
$$=\lim_{x\to+\infty}\operatorname{arctg} x=\frac{\pi}{2}.$$

□

**5.52.** Určete limity

$$\lim_{n\to\infty}\left(\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{(n-1)\cdot n}\right);$$

$$\lim_{n\to\infty}\left(\frac{1}{\sqrt{n^2+1}}+\frac{1}{\sqrt{n^2+2}}+\cdots+\frac{1}{\sqrt{n^2+n}}\right).$$

**Řešení.** Neboť pro každé přirozené číslo $k\geq 2$ je (provádíme tzv. rozklad na parciální zlomky – budeme jej probírat u integrování racionálních lomených funkcí viz 6.23)

$$\frac{1}{(k-1)\,k}=\frac{1}{k-1}-\frac{1}{k},$$

platí

$$\lim_{n\to\infty}\left(\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{(n-1)\cdot n}\right)=$$
$$=\lim_{n\to\infty}\left(\frac{1}{1}-\frac{1}{2}+\frac{1}{2}-\frac{1}{3}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{n-1}-\frac{1}{n}\right)=$$
$$=\lim_{n\to\infty}\left(1-\frac{1}{n}\right)=1.$$

Poznamenejme, že stanovení této limity je důležité: určuje součet jedné z tzv. teleskopických řad (se kterou pracoval již Johann I. Bernoulli).

Ke stanovení druhé limity využijeme Větu o třech limitách. Odhady

$$\frac{1}{\sqrt{n^2+1}}+\cdots+\frac{1}{\sqrt{n^2+n}}\geq\frac{1}{\sqrt{n^2+n}}+\cdots+\frac{1}{\sqrt{n^2+n}}=$$
$$=\frac{n}{\sqrt{n^2+n}},$$

$$\frac{1}{\sqrt{n^2+1}}+\cdots+\frac{1}{\sqrt{n^2+n}}\leq\frac{1}{\sqrt{n^2+1}}+\cdots+\frac{1}{\sqrt{n^2+1}}=$$
$$=\frac{n}{\sqrt{n^2+1}}$$

**5.19. Nejčastější varianty definičních oborů.** Naše definice limity pokrývá zdánlivě velice rozdílné koncepty:

(1) **Limity posloupností.** Jestliže je $A=\mathbb{N}$, tj. funkce $f$ je definována pouze pro přirozená čísla, hovoříme o limitách posloupností reálných nebo komplexních čísel. Jediným hromadným bodem definičního oboru $A$ je pak $\infty$ a zpravidla píšeme hodnoty posloupnosti $f(n)=a_n$ a limitu ve tvaru

$$\lim_{n\to\infty}a_n=a.$$

Podle definice to pak znamená, že pro každé okolí $\mathcal{O}(a)$ limitní hodnoty $a$ existuje index $N\in\mathbb{N}$ takový, že $a_n\in\mathcal{O}(a)$ pro všechna $n\geq N$. Ve skutečnosti jsme tedy v tomto speciálním případě přeformulovali definici konvergence posloupnosti (viz 5.12). Přidali jsme pouze možnost nevlastních limit. Říkáme také, že *posloupnost $a_n$ konverguje k $a$*.[3]

Přímo z naší definice pro komplexní hodnoty je opět vidět, že komplexní posloupnost má limitu $a$, právě když reálné části $a_i$ konvergují k $\operatorname{re} a$ a zároveň imaginární části konvergují k $\operatorname{im} a$.

(2) **Limita funkce ve vnitřním bodě intervalu.** Jestliže je $f$ definována na intervalu $A=(a,b)$ a $x_0$ je vnitřním bodem tohoto intervalu, hovoříme o limitě funkce ve vnitřním bodě jejího definičního oboru. Většinou v tomto případě píšeme

$$\lim_{x\to x_0}f(x)=a.$$

Podívejme se, proč je důležité v definici požadovat $f(x)\in\mathcal{O}(a)$ pouze pro body $x\neq x_0$ i v tomto případě. Vezměme jako příklad funkci $f:\mathbb{R}\to\mathbb{R}$

$$f(x)=\begin{cases}0 & \text{je-li } x\neq 0,\\ 1 & \text{je-li } x=0.\end{cases}$$

Pak zjevně limita v nule je dobře definována a v souladu s naším očekáváním bude $\lim_{x\to 0}f(x)=0$, přestože hodnota $f(0)=1$ do malých okolí limitní hodnoty 0 nepatří.

(3) **Limity funkce zprava a zleva.** Je-li $A=[a,b]$ ohraničený interval a $x_0=a$ nebo $x_0=b$, hovoříme o limitě zprava, resp. zleva, funkce $f$ v bodě $x_0$.

Jestliže je bod $x_0$ vnitřním bodem definičního oboru funkce $f$, můžeme pro účely výpočtu limity definiční obor zúžit na $[x_0,b]$ nebo $[a,x_0]$. Výsledným limitám pak také říkáme *limita zprava*, resp. *limita zleva* pro funkci $f$ v bodě $x_0$. Označujeme je výrazy $\lim_{x\to x_0^+}f(x)$, resp. $\lim_{x\to x_0^-}f(x)$. Jako příklad nám může sloužit limita zprava a zleva v $x_0=0$ pro Heavisideovu funkci $h$ z úvodu této části. Evidentně je

$$\lim_{x\to 0^+}h(x)=1,\qquad\lim_{x\to 0^-}h(x)=0.$$

Limita $\lim_{x\to 0}f(x)$ přitom neexistuje.

Přímo z našich definic je zjevné, že limita ve vnitřním bodu definičního oboru libovolné reálné funkce $f$ existuje, právě když existují limity zprava i zleva a jsou si rovny.

**5.20. Další příklady limit.** (1) Limita komplexní funkce $f:A\to\mathbb{C}$ existuje tehdy a jen tehdy, jestliže existují limity její reálné a imaginární části. V takovém případě je pak

$$\lim_{x\to x_0}f(x)=\lim_{x\to x_0}(\operatorname{re} f(x))+i\lim_{x\to x_0}(\operatorname{im} f(x)).$$

[3] Budeme v dalším i v případě nevlastní limity $a=\pm\infty$ říkat, že $a_n$ konverguje k $a$. V literatuře se ale často takovým posloupnostem říká *divergentní* a říká se o nich, že divergují k $\pm\infty$. Sami budeme tuto termilogii používat u součtů řad.

pro $n \in \mathbb{N}$ dávají

$$\lim_{n\to\infty} \frac{n}{\sqrt{n^2+n}} \le \lim_{n\to\infty} \left( \frac{1}{\sqrt{n^2+1}} + \cdots + \frac{1}{\sqrt{n^2+n}} \right) \le$$
$$\le \lim_{n\to\infty} \frac{n}{\sqrt{n^2+1}}.$$

Protože

$$\lim_{n\to\infty} \frac{n}{\sqrt{n^2+n}} = \lim_{n\to\infty} \frac{n}{\sqrt{n^2}} = 1,$$
$$\lim_{n\to\infty} \frac{n}{\sqrt{n^2+1}} = \lim_{n\to\infty} \frac{n}{\sqrt{n^2}} = 1,$$

je rovněž

$$\lim_{n\to\infty} \left( \tfrac{1}{\sqrt{n^2+1}} + \tfrac{1}{\sqrt{n^2+2}} + \cdots + \tfrac{1}{\sqrt{n^2+n}} \right) = 1 \,. \qquad \square$$

**5.53.** Spočtěte

(a)
$$\lim_{x\to 0} \frac{\sqrt{1+x} - \sqrt{1-x}}{x};$$

(b)
$$\lim_{x\to \pi/4} \frac{\cos x - \sin x}{\cos(2x)};$$

(c)
$$\lim_{x\to+\infty} \sqrt[3]{x^4} \left( \sqrt[3]{x^2+2x+3} - \sqrt[3]{x^2+2x+2} \right).$$

**Řešení.** Všechny uvedené limity vypočítáme pomocí vhodného rozšíření zadaného výrazu. V případě první limity vynásobíme čitatele i jmenovatele výrazem

$$\sqrt{1+x} + \sqrt{1-x}$$

a využijeme známého vztahu $(a-b)(a+b) = a^2 - b^2$. Takto obdržíme

$$\lim_{x\to 0} \frac{\sqrt{1+x} - \sqrt{1-x}}{x} = \lim_{x\to 0} \frac{(1+x)-(1-x)}{x\left(\sqrt{1+x}+\sqrt{1-x}\right)} =$$
$$= \lim_{x\to 0} \frac{2}{\sqrt{1+x}+\sqrt{1-x}} = \frac{2}{\sqrt{1}+\sqrt{1}} = 1.$$

Podobně vypočítáme

$$\lim_{x\to \pi/4} \frac{\cos x - \sin x}{\cos(2x)} = \lim_{x\to \pi/4} \frac{(\cos x + \sin x)(\cos x - \sin x)}{(\cos x + \sin x)\cos(2x)} =$$
$$= \lim_{x\to \pi/4} \frac{\cos^2 x - \sin^2 x}{(\cos x + \sin x)\cos(2x)} =$$
$$= \lim_{x\to \pi/4} \frac{1}{\cos x + \sin x} = \frac{1}{\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}} = \frac{\sqrt{2}}{2}.$$

U provedeného krácení připomeňme identitu

$$\cos(2x) = \cos^2 x - \sin^2 x, \quad x \in \mathbb{R}.$$

Abychom mohli při určování poslední limity použít

$$(a-b)\left(a^2+ab+b^2\right) = a^3 - b^3,$$

Důkaz je přímočarý a vychází přímo z definice vzdáleností a okolí bodů v komplexní rovině. Skutečně, příslušnost do $\delta$–okolí komplexní hodnoty $z$ je zajištěna pomocí reálných $(1/\sqrt{2})\delta$–okolí reálné a imaginární složky $z$. Odtud již tvrzení bezprostředně vyplývá.

(2) Nechť $f$ je reálný nebo komplexní polynom. Pak pro každý bod $x \in \mathbb{R}$ je

$$\lim_{x\to x_0} f(x) = f(x_0).$$

Skutečně, je-li $f(x) = a_n x^n + \cdots + a_0$, pak roznásobením $(x_0+\delta)^k = x_0^k + k\,\delta x_0^{k-1} + \cdots + \delta^k$ a dosazením pro $k = 0, \ldots, n$ vidíme, že volbou dostatečně malého $\delta$ se hodnotou libovolně blízko přiblížíme $f(x_0)$.

(3) Uvažme nyní docela ošklivou funkci definovanou na celé reálné přímce

$$f(x) = \begin{cases} 1 & \text{je-li } x \in \mathbb{Q}, \\ 0 & \text{jestliže } x \notin \mathbb{Q}. \end{cases}$$

Přímo z definice je zjevné, že tato funkce nemá limitu v žádném bodě (dokonce ani zleva nebo zprava).

(4) Následující funkce je ještě záludnější, než jsme viděli v předchozím případě. Funkce $f : \mathbb{R} \to \mathbb{R}$ je definována takto:[4]

$$f(x) = \begin{cases} \frac{1}{q} & \text{jestliže } x = \frac{p}{q} \in \mathbb{Q},\ p \text{ a } q \text{ nesoudělná}, \\ 0 & \text{jestliže } x \notin \mathbb{Q}. \end{cases}$$



Zvolíme-li libovolný bod $x$, ať už racionální či iracionální, a veliké přirozené $m$, bude $x$ v právě jednom z intervalů $\left[\frac{n}{m}, \frac{n+1}{m}\right)$ pro nějaké $n$ (je-li $x = \frac{p}{q}$, uvažujeme jen nesoudělná $m > q$). Za $\delta_k$ si zvolíme minimum ze vzdáleností bodu $x$ od hranic těchto intervalů pro uvažovaná $m$ menší než $k$. Samozřejmě vždy platí $\delta_k < \frac{1}{k}$.

Uvažme nyní nějaké $\varepsilon > 0$ a $k$ taková, že $\frac{1}{k} < \varepsilon$. Pak pro všechna $y$ v ryzím $\delta$–okolí bodu $x$ je buď $f(y) = 0$, jde-li o iracionální hodnotu, nebo $f(y) < \frac{1}{r}$ pro $r > k$, jde-li o hodnotu racionální. V každém případě je tedy $|f(y)| < \varepsilon$.

Tato funkce má proto limitu ve všech reálných bodech $x$ nulovou. Jen v iracionálních bodech je ale tato limita rovna funkční hodnotě.

**5.21. Věta** (O třech limitách)**.** *Buďte $f$, $g$, $h$ reálné funkce se shodným definičním oborem $A$ a takové, že existuje ryzí okolí hromadného bodu $x_0 \in \mathbb{R}$ definičního oboru, kde platí*

$$f(x) \le g(x) \le h(x).$$

*Pokud existují limity*

$$\lim_{x\to x_0} f(x) = f_0, \quad \lim_{x\to x_0} h(x) = h_0$$

*a navíc $f_0 = h_0$, pak také existuje limita*

$$\lim_{x\to x_0} g(x) = g_0$$

*a platí $g_0 = f_0 = h_0$.*

[4] Této funkci se říkává Thomaeova (ale též Riemannova) funkce podle německého matematika J. Thomae z druhé poloviny 19. století.

k rozšíření potřebujeme výraz

$$\sqrt[3]{\left(x^2+2x+3\right)^2}+\sqrt[3]{x^2+2x+3}\cdot\sqrt[3]{x^2+2x+2}+\sqrt[3]{\left(x^2+2x+2\right)^2},$$

který odpovídá $a^2+ab+b^2$, resp. volíme

$$a=\sqrt[3]{x^2+2x+3}, \qquad b=\sqrt[3]{x^2+2x+2}.$$

Tímto rozšířením převedeme limitu ze zadání na

$$\lim_{x\to+\infty}\frac{\sqrt[3]{x^4}\left(\left(x^2+2x+3\right)-\left(x^2+2x+2\right)\right)}{\sqrt[3]{\left(x^2+2x+3\right)^2}+\sqrt[3]{x^2+2x+3}\cdot\sqrt[3]{x^2+2x+2}+\sqrt[3]{\left(x^2+2x+2\right)^2}},$$

tj.

$$\lim_{x\to+\infty}\frac{\sqrt[3]{x^4}}{\sqrt[3]{\left(x^2+2x+3\right)^2}+\sqrt[3]{x^2+2x+3}\cdot\sqrt[3]{x^2+2x+2}+\sqrt[3]{\left(x^2+2x+2\right)^2}}.$$

Poslední limitu umíme snadno vyčíslit. Víme totiž, že je určena pouze jedním členem v čitateli a jedním ve jmenovateli, a to $ax^p$ pro největší $p$ (v tomto případě je uvažovaný člen ve jmenovateli rozdělen na několik sčítanců). Platí tudíž

$$\lim_{x\to+\infty}\frac{\sqrt[3]{x^4}}{\sqrt[3]{\left(x^2+2x+3\right)^2}+\sqrt[3]{x^2+2x+3}\cdot\sqrt[3]{x^2+2x+2}+\sqrt[3]{\left(x^2+2x+2\right)^2}}=$$

$$=\lim_{x\to+\infty}\frac{\sqrt[3]{x^4}}{\sqrt[3]{\left(x^2\right)^2}+\sqrt[3]{x^2}\cdot\sqrt[3]{x^2}+\sqrt[3]{\left(x^2\right)^2}}=\lim_{x\to+\infty}\frac{\sqrt[3]{x^4}}{3\sqrt[3]{x^4}}=\frac{1}{3}.$$

Celkem tak je

$$\lim_{x\to+\infty}\left(\sqrt[3]{x^4}\left(\sqrt[3]{x^2+2x+3}-\sqrt[3]{x^2+2x+2}\right)\right)=\frac{1}{3}. \qquad \square$$

**5.54.** Pro libovolné $n\in\mathbb{N}$ určete limitu

$$\lim_{x\to0}\frac{(1+2nx)^n-(1+nx)^{2n}}{x^2}.$$

**Řešení.** Podle binomické věty je

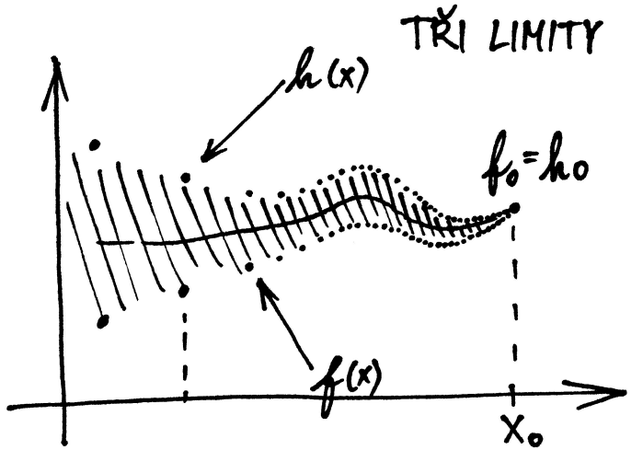
$$(1+2nx)^n=1+\binom{n}{1}2nx+\binom{n}{2}(2nx)^2+P(x)\,x^3, \quad x\in\mathbb{R},$$

$$(1+nx)^{2n}=1+\binom{2n}{1}nx+\binom{2n}{2}(nx)^2+Q(x)\,x^3, \quad x\in\mathbb{R}$$

pro jisté polynomy $P$, $Q$. Raději vyzdvihněme, že předchozí vyjádření skutečně platí pro všechna $n\in\mathbb{N}$. Pro $n=1$ si stačí uvědomit, že klademe $\binom{1}{2}=0$ a že polynomy $P$, $Q$ mohou být identicky rovny nule. Dostáváme tedy

$$(1+2nx)^n=1+2n^2x+2n^3(n-1)\,x^2+P(x)\,x^3, \quad x\in\mathbb{R},$$

$$(1+nx)^{2n}=1+2n^2x+n^3(2n-1)\,x^2+Q(x)\,x^3, \quad x\in\mathbb{R}.$$




Důkaz. Za předpokladů věty existuje pro libovolné $\varepsilon>0$ okolí $\mathcal{O}(x_0)$ bodu $x_0\in A\subset\mathbb{R}$, ve kterém jsou pro všechna $x\neq x_0$ hodnoty $f(x)$ i $h(x)$ obsaženy v intervalu $(f_0-\varepsilon,\,f_0+\varepsilon)$. Z podmínky $f(x)\le g(x)\le h(x)$ vyplývá, že i $g(x)\in(f_0-\varepsilon,\,f_0+\varepsilon)$, tedy $\lim_{x\to x_0}g(x)=f_0$.

Drobnou modifikací předchozího postupu si čtenář doplní i argumentaci pro nevlastní hodnoty limit nebo limity v nevlastním bodu $x_0$. Určitě bude dobré si tyto případy podrobně promyslet! $\square$

Všimněme si, že věta dává možnost výpočtu limit pro všechny typy diskutované výše, tj. limity posloupností, limity funkcí ve vnitřních bodech, jednostranné limity atd.

**5.22. Věta.** *Nechť $A\subseteq\mathbb{R}$ je definiční obor reálných nebo komplexních funkcí $f$ a $g$, $x_0$ nechť je hromadný bod $A$ a existují limity*

$$\lim_{x\to x_0}f(x)=a\in\mathbb{K}, \qquad \lim_{x\to x_0}g(x)=b\in\mathbb{K}.$$

*Potom:*

*(1) limita $a$ je určena jednoznačně,*

*(2) limita součtu $f+g$ existuje a platí*

$$\lim_{x\to x_0}(f(x)+g(x))=a+b,$$

*(3) limita součinu $f\cdot g$ existuje a platí*

$$\lim_{x\to x_0}(f(x)\cdot g(x))=a\cdot b,$$

*(4) pokud navíc $b\neq0$, pak limita podílu $f/g$ existuje a platí*

$$\lim_{x\to x_0}\frac{f(x)}{g(x)}=\frac{a}{b}.$$



Důkaz. (1) Předpokládejme, že $a$ a $a'$ jsou dvě hodnoty limity $\lim_{x\to x_0}f(x)$. Pokud je $a\neq a'$, pak existují disjunktní okolí $\mathcal{O}(a)$ a $\mathcal{O}(a')$. Pro dostatečně malá okolí $x_0$ ale mají hodnoty $f$ ležet v obou naráz, což je spor. Proto je $a=a'$.

(2) Zvolme si nějaké okolí $a+b$, třeba $\mathcal{O}_{2\varepsilon}(a+b)$. Pro dostatečně malé okolí $x_0$ a $x\neq x_0$ bude jak $f(x)$, tak $g(x)$ v $\varepsilon$– okolích bodů $a$ a $b$. Proto jejich součet bude v $2\varepsilon$–okolí kýžené hodnoty $a+b$. Tím je důkaz ukončen.

(3) Podobně postupujeme u součinu s $\mathcal{O}_{\varepsilon^2}(ab)$. Pro malá okolí $x_0$ se nám hodnoty $f$ i $g$ trefí do $\varepsilon$–okolí hodnot $a$ a $b$. Proto jejich součin bude v požadovaném $\varepsilon^2$–okolí.

(4) Podobný postup ponechán jako cvičení. $\square$

Pouhé dosazení a jednoduché úpravy již dávají

$$\lim_{x\to 0}\frac{(1+2nx)^n-(1+nx)^{2n}}{x^2}=$$
$$=\lim_{x\to 0}\frac{\left(2n^3(n-1)-n^3(2n-1)\right)x^2+(P(x)-Q(x))\,x^3}{x^2}=$$
$$=\lim_{x\to 0}\left(-n^3+(P(x)-Q(x))\,x\right)=-n^3+0=-n^3.$$

□

**5.55.** Spočítejte

$$\lim_{x\to\pi/4}(\operatorname{tg}x)^{\operatorname{tg}(2x)}.$$

**Řešení.** Limity typu $1^{\pm\infty}$ (jako je v zadání) lze počítat podle vzorce

$$\lim_{x\to x_0}f(x)^{g(x)}=\mathrm{e}^{\lim\limits_{x\to x_0}((f(x)-1)g(x))},$$

jestliže limita na pravé straně existuje a $f(x)\neq 1$ pro $x$ z jistého ryzího okolí bodu $x_0\in\mathbb{R}$. Určeme proto

$$\lim_{x\to\pi/4}(\operatorname{tg}x-1)\operatorname{tg}(2x)=\lim_{x\to\pi/4}\left(\frac{\sin x}{\cos x}-1\right)\frac{\sin(2x)}{\cos(2x)}=$$
$$=\lim_{x\to\pi/4}\frac{\sin x-\cos x}{\cos x}\cdot\frac{2\sin x\cos x}{\cos^2 x-\sin^2 x}=$$
$$=\lim_{x\to\pi/4}\frac{-2\sin x}{\cos x+\sin x}=\frac{-2\frac{\sqrt{2}}{2}}{\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}}=-1.$$

Odtud máme

$$\lim_{x\to\pi/4}(\operatorname{tg}x)^{\operatorname{tg}(2x)}=\frac{1}{\mathrm{e}}.$$

Doplňme, že použitý vzorec platí obecněji pro „typ $1^{\text{cokoli}}$“, tj. bez kladení jakýchkoli podmínek týkajících se limity $\lim_{x\to x_0}g(x)$, která tak ani nemusí existovat. □

**5.56.** Ukažte, že je

$$\lim_{x\to 0}\frac{\sin x}{x}=1.$$

**Řešení.** Uvažujme jednotkovou čtvrtkružnici v prvním kvadrantu a její bod $[\cos x,\sin x]$, $x\in(0,\pi/2)$. Délka kruhového oblouku mezi body $[\cos x,\sin x]$ a $[1,0]$ je rovna $x$. Zřejmě tedy je

$$\sin x<x,\quad x\in\left(0,\frac{\pi}{2}\right).$$

Hodnotu $\operatorname{tg}x$ potom vyjadřuje délka úsečky s krajními body $[1,\sin x/\cos x]$ a $[1,0]$. Vidíme, že je (příp. si nakreslete obrázek)

$$x<\operatorname{tg}x,\quad x\in\left(0,\frac{\pi}{2}\right).$$

Tato nerovnost rovněž vyplývá z toho, že trojúhelník s vrcholy $[0,0]$, $[1,0]$, $[1,\operatorname{tg}x]$ má očividně větší obsah než uvažovaná kruhová výseč. Dohromady jsme získali

$$\sin x<x<\frac{\sin x}{\cos x},\quad x\in\left(0,\frac{\pi}{2}\right),$$

**Poznámka.** Podrobnějším sledováním důkazů jednotlivých bodů věty můžeme její tvrzení rozšířit i na některé nekonečné hodnoty limit reálných funkcí: V prvém případě je zapotřebí, aby buď alespoň jedna z limit byla konečná nebo aby obě měly stejné znaménko. Pak opět platí, že limita součtu je součet limit s konvencemi z 5.18. Případ „$\infty-\infty$“ ale není zahrnut.

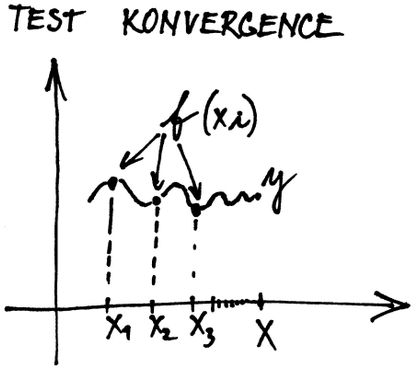
V druhém případě může být jedna z limit nekonečná a druhá nenulová. Pak opět platí, že limita součinu je součin limit. Případ „$0\cdot(\pm\infty)$“ není ale zahrnut.

V případě podílu může být $a\in\mathbb{R}$ a $b=\pm\infty$, kdy výsledek limity bude nula, nebo $a=\pm\infty$ a $b\in\mathbb{R}$, kde výsledek bude $\pm\infty$ podle znamének čitatele a jmenovatele. Případ „$\frac{\infty}{\infty}$“ není zahrnut.

Zdůrazněme, že naše věta jako speciální případ pokrývá také odpovídající tvrzení o konvergenci posloupností i o limitách zprava a zleva funkcí definovaných na intervalu.

Pro úvahy o limitách bývá technicky užitečný i následující jednoduchý důsledek definic, který uvádí do souvislosti limity posloupností a funkcí obecně.

**5.23. Důsledek.** *Uvažme reálnou nebo komplexní funkci $f$ definovanou na množině $A\subseteq\mathbb{R}$ a hromadný bod $x_0$ množiny $A$. Funkce $f$ má v bodě $x_0$ limitu $y$, právě když pro každou posloupnost bodů $x_n\in A$ konvergující k $x_0$ a různých od $x_0$ má i posloupnost hodnot $f(x_n)$ limitu $y$.*




Důkaz. Předpokládejme nejprve, že limita $f$ v bodě $x_0$ je skutečně $y$. Pak pro libovolné okolí $V$ bodu $y$ musí existovat okolí $V$ bodu $x_0$ takové, že pro všechna $x\in V\cap A$, $x\neq x_0$, je $f(x)\in U$. Pro každou posloupnost $x_n\to x_0$ bodů různých od $x_0$ ale budou pro všechna $n$ větší než vhodné $N$ i všechny body $x_n\in V$. Budou tedy posloupnosti hodnot $f(x_n)$ konvergovat k hodnotě $y$.

Předpokládejme naopak, že funkce $f$ nekonverguje k $y$ při $x\to x_0$. Pak pro nějaké okolí $U$ hodnoty $y$ existuje posloupnost bodů $x_m\neq x_0$ v $A$, které jsou bližší k $x_0$ než $1/m$ a přitom hodnota $f(x_m)$ nepatří do $U$. Tím jsme zkonstruovali posloupnost bodů z $A$ různých od $x_0$, pro které hodnoty $f(x_n)$ nekonvergují k $y$ a důkaz je ukončen. □

Nyní máme nachystány nástroje na korektní formulaci vlastnosti spojitosti, se kterou jsme dříve intuitivně nakládali u polynomů.

## Spojitost funkcí

**Definice.** Nechť $f$ je reálná nebo komplexní funkce definovaná na intervalu $A\subseteq\mathbb{R}$. Říkáme, že $f$ je *spojitá v bodě* $x_0\in A$, jestliže je



tj.

$$1 < \frac{x}{\sin x} < \frac{1}{\cos x}, \quad x \in \left(0, \frac{\pi}{2}\right),$$
$$1 > \frac{\sin x}{x} > \cos x, \quad x \in \left(0, \frac{\pi}{2}\right).$$

Z Věty o třech limitách nyní plynou nerovnosti

$$1 = \lim_{x\to 0+} 1 \geq \lim_{x\to 0+} \frac{\sin x}{x} \geq \lim_{x\to 0+} \cos x = \cos 0 = 1.$$

Dokázali jsme tak, že

$$\lim_{x\to 0+} \frac{\sin x}{x} = 1.$$

Funkce $y = (\sin x)/x$ definovaná pro $x \neq 0$ je ovšem sudá, a tudíž je

$$\lim_{x\to 0-} \frac{\sin x}{x} = \lim_{x\to 0+} \frac{\sin x}{x} = 1.$$

Protože obě jednostranné limity existují a jsou si rovny, existuje oboustranná limita a platí pro ni

$$\lim_{x\to 0} \frac{\sin x}{x} = \lim_{x\to 0\pm} \frac{\sin x}{x} = 1.$$

Poznamenejme ještě, že uvedenou limitu by sice šlo velmi snadno vyčíslit za pomoci l'Hospitalova pravidla, nicméně k odvození l'Hospitalova pravidla je používána právě tato limita, tudíž se při jejím výpočtu na zmíněné pravidlo odvolávat nemůžeme. □

**5.57.** Stanovte limity

$$\lim_{n\to\infty} \left(\frac{n}{n+1}\right)^n, \quad \lim_{n\to\infty} \left(1+\frac{1}{n^2}\right)^n, \quad \lim_{n\to\infty} \left(1-\frac{1}{n}\right)^{n^2};$$

$$\lim_{x\to 0} \frac{\sin^2 x}{x}, \quad \lim_{x\to 0} \frac{x}{\sin^2 x}, \quad \lim_{x\to 0} \frac{\arcsin x}{x};$$

$$\lim_{x\to 0} \frac{3\,\mathrm{tg}^2 x}{5\,x^2}, \quad \lim_{x\to 0} \frac{\sin(3x)}{\sin(5x)}, \quad \lim_{x\to 0} \frac{\mathrm{tg}\,(3x)}{\sin(5x)};$$

$$\lim_{x\to 0} \frac{\mathrm{e}^{5x} - \mathrm{e}^{2x}}{x}, \quad \lim_{x\to 0} \frac{\mathrm{e}^{5x} - \mathrm{e}^{-x}}{\sin(2x)}.$$

**Řešení.** Při určování těchto limit využijeme znalosti limit ($a \in \mathbb{R}$)

$$\lim_{n\to\infty} \left(1+\frac{a}{n}\right)^n = \mathrm{e}^a; \qquad \lim_{x\to 0} \frac{\sin x}{x} = 1; \qquad \lim_{x\to 0} \frac{\mathrm{e}^x - 1}{x} = 1.$$

Víme tedy, že je

$$\mathrm{e}^{-1} = \lim_{n\to\infty} \left(1-\frac{1}{n}\right)^n = \lim_{n\to\infty} \left(\frac{n-1}{n}\right)^n.$$

Substituce $m = n - 1$ dává

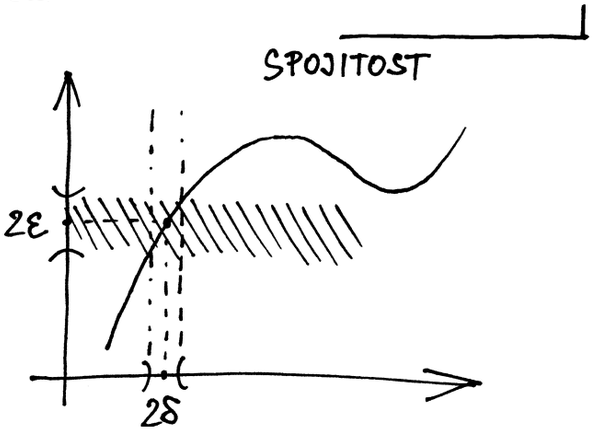
$$\lim_{n\to\infty} \left(\frac{n-1}{n}\right)^n = \lim_{m\to\infty} \left(\frac{m}{m+1}\right)^{m+1} =$$
$$= \lim_{m\to\infty} \left(\frac{m}{m+1}\right)^m \cdot \lim_{m\to\infty} \frac{m}{m+1}.$$

Celkem máme

$$\mathrm{e}^{-1} = \lim_{m\to\infty} \left(\frac{m}{m+1}\right)^m \cdot \lim_{m\to\infty} \frac{m}{m+1}.$$

$$\lim_{x\to x_0} f(x) = f(x_0).$$

Funkce $f$ je spojitá na množině $A$, jestliže je spojitá ve všech bodech $x_0 \in A$.




Všimněme si, že pro hraniční body intervalu $A$ říká naše definice, že $f$ v nich má hodnotu rovnou limitě zleva, resp. zprava. Říkáme, že je v takovém bodě *spojitá zprava, resp. zleva*. Již jsme také viděli, že každý polynom je spojitou funkcí na celém $\mathbb{R}$, viz 5.20(2). Potkali jsme také funkci, která je spojitá jen v iracionálních reálných číslech, přestože má limity i ve všech číslech racionálních, viz 5.20(4).

Z předchozí Věty 5.22 o vlastnostech limit okamžitě vyplývá většina následujících tvrzení

**5.24. Věta.** *Nechť $f$ a $g$ jsou (reálné nebo komplexní) funkce definované na intervalu $A$ a spojité v bodě $x_0 \in A$. Pak*

*(1) součet $f + g$ je funkce spojitá v $x_0$,*
*(2) součin $f \cdot g$ je funkce spojitá v $x_0$,*
*(3) pokud navíc $g(x_0) \neq 0$, pak podíl $f/g$ je dobře definován v nějakém okolí $x_0$ a je spojitý v $x_0$,*
*(4) pokud je spojitá funkce $h$ definována na okolí hodnoty $f(x_0)$ reálné funkce $f$, pak složená funkce $h \circ f$ je definována na okolí bodu $x_0$ a je v bodě $x_0$ spojitá.*

Důkaz. Tvrzení (1) a (2) jsou zřejmá, doplnit důkaz potřebujeme u tvrzení (3). Jestliže je $g(x_0) \neq 0$, pak také celé $\varepsilon$–okolí čísla $g(x_0)$ neobsahuje nulu pro dostatečně malé $\varepsilon > 0$. Ze spojitosti $g$ pak vyplývá, že na dostatečně malém $\delta$–okolí bodu $x_0$ bude $g$ nenulové a podíl $f/g$ tam bude tedy dobře definován. Pak bude ovšem i spojitý v $x_0$ podle předchozí věty.



(4) Zvolme nějaké okolí $\mathcal{O}$ hodnoty $h(f(x_0))$. Ze spojitosti $h$ k němu existuje okolí $\mathcal{O}'$ bodu $f(x_0)$, které je celé zobrazeno funkcí $h$ do $\mathcal{O}$. Do tohoto okolí $\mathcal{O}'$ spojité zobrazení $f$ zobrazí dostatečně malé okolí bodu $x_0$. To je ale právě definiční vlastnost spojitosti a důkaz je ukončen. □

Nyní si vcelku snadno můžeme odvodit zásadní souvislosti spojitých zobrazení a topologie reálných čísel:

**5.25. Věta.** *Nechť $f : \mathbb{R} \to \mathbb{R}$ je spojitá funkce. Pak*

*(1) vzor $f^{-1}(U)$ každé otevřené množiny $U$ je otevřená množina,*
*(2) vzor $f^{-1}(W)$ každé uzavřené množiny $W$ je uzavřená množina,*

Druhá z limit je zjevně rovna 1. Když změníme označení (nahradíme $n$ za $m$), můžeme napsat výsledek

$$\mathrm{e}^{-1} = \lim_{n\to\infty} \left(\frac{n}{n+1}\right)^n.$$

Dále platí

$$\lim_{n\to\infty} \left(1+\frac{1}{n^2}\right)^n = \lim_{n\to\infty} \left(1+\frac{1}{n^2}\right)^{\frac{n^2}{n}} = \\ = \lim_{n\to\infty} \left(\left(1+\frac{1}{n^2}\right)^{n^2}\right)^{\frac{1}{n}} = \mathrm{e}^0 = 1$$

a

$$\lim_{n\to\infty} \left(1-\frac{1}{n}\right)^{n^2} = \lim_{n\to\infty} \left(\left(1-\frac{1}{n}\right)^{n}\right)^{n} = 0.$$

Upozorněme, že první z předešlých vyčíslení vyplývá z limit

$$\lim_{n\to\infty} \left(1+\frac{1}{n^2}\right)^{n^2} = \lim_{m\to\infty} \left(1+\frac{1}{m}\right)^{m} = \mathrm{e}, \qquad \lim_{n\to\infty} \frac{1}{n} = 0$$

a druhé potom z

$$\lim_{n\to\infty} \left(1-\frac{1}{n}\right)^{n} = \mathrm{e}^{-1}, \qquad \lim_{n\to\infty} n = +\infty,$$

přičemž klademe $\mathrm{e}^{-\infty} = 0$ (zápis označuje $\lim_{x\to-\infty} \mathrm{e}^x = 0$ – jedná se o určitý výraz).

Snadno lze získat

$$\lim_{x\to0} \frac{\sin^2 x}{x} = \lim_{x\to0} \sin x \cdot \lim_{x\to0} \frac{\sin x}{x} = 0 \cdot 1 = 0.$$

Zřejmě je

$$\lim_{x\to0} \frac{x}{\sin x} = 1^{-1} = 1$$

a limita

$$\lim_{x\to0} \frac{1}{\sin x}$$

neexistuje (zapisujeme $1/\pm0$). Kdybychom tedy k výpočtu limity

$$\lim_{x\to0} \frac{x}{\sin^2 x}$$

užili pravidla o limitě součinu, obdrželi bychom $1 \cdot 1/\pm0 = 1/\pm0$. To znamená, že tato limita neexistuje (opět jde o určitý výraz). Ke stanovení

$$\lim_{x\to0} \frac{\arcsin x}{x}$$

použijeme identitu $x = \sin(\arcsin x)$ platnou pro $x \in (-1, 1)$, tj. v jistém okolí bodu 0. Pomocí substituce $y = \arcsin x$ dostáváme

$$\lim_{x\to0} \frac{\arcsin x}{x} = \lim_{x\to0} \frac{\arcsin x}{\sin(\arcsin x)} = \lim_{y\to0} \frac{y}{\sin y} = 1.$$

Poznamenejme, že $y \to 0$ plyne z dosazení $x = 0$ do $y = \arcsin x$ a ze spojitosti této funkce v počátku (to také zaručuje, že jsme tuto substituci mohli „bez obav“ zavést).

*(3) obraz $f(K)$ každé kompaktní množiny $K$ je kompaktní množina,*

*(4) na libovolné kompaktní množině $K$ dosahuje spojitá funkce svého maxima a minima.*

Důkaz. (1) Uvažme nějaký bod $x_0 \in f^{-1}(U)$. Nějaké okolí $\mathcal{O}$ hodnoty $f(x_0)$ je celé v $U$, protože je $U$ otevřená. Pak ovšem existuje okolí $\mathcal{O}'$ bodu $x_0$, které se celé zobrazí do $\mathcal{O}$, patří tedy do vzoru. Každý bod vzoru je tedy vnitřní a tím je důkaz ukončený.



(2) Uvažme nějaký hromadný bod $x_0$ vzoru $f^{-1}(W)$ a nějakou posloupnost $x_i$, $f(x_i) \in W$, která k němu konverguje. Ze spojitosti $f$ nyní zjevně vyplývá, že $f(x_i)$ konverguje k $f(x_0)$, a protože je $W$ uzavřená, musí i $f(x_0) \in W$. Zřejmě jsou tedy všechny hromadné body vzoru množiny $W$ ve $W$ také obsaženy.

(3) Zvolme libovolné otevřené pokrytí $f(K)$. Vzory jednotlivých intervalů budou sjednoceními otevřených intervalů a tedy také vytvoří pokrytí množiny $K$. Z něho lze vybrat konečné pokrytí a proto nám stačí konečně mnoho odpovídajících obrazů k pokrytí původní množiny $f(K)$.

(4) Protože je obrazem kompaktní množiny opět kompaktní množina, musí být obraz ohraničený a zároveň musí obsahovat svoje supremum i infimum. Odtud ale vyplývá, že tyto musí být zároveň maximem a minimem hodnot. □

**5.26. Důsledek.** *Nechť $f : \mathbb{R} \to \mathbb{R}$ je spojitá. Potom*

*(1) obraz každého intervalu je opět interval,*

*(2) $f$ na uzavřeném intervalu $[a, b]$ nabývá všech hodnot mezi svou maximální a minimální hodnotou.*[5]

Důkaz. (1) Uvažme nejprve nějaký otevřený interval $A$ a předpokládejme, že existuje bod $y \in \mathbb{R}$ takový, že $f(A)$ obsahuje body menší i větší než $y$, ale $y \notin f(A)$. Znamená to tedy, že pro otevřené množiny $B_1 = (-\infty, y)$ a $B_2 = (y, \infty)$ jejich vzory $A_1 = f^{-1}(B_1) \cap A$ a $A_2 = f^{-1}(B_2) \cap A$ pokrývají $A$. Tyto množiny jsou přitom opět otevřené, jsou disjunktní a obě mají neprázdný průnik s $A$. Stejnou úvahou jako v důkazu prvního bodu v 5.17 dospějeme k závěru, že musí existovat bod $x \in A$, který neleží v $A_1$, je ale jejím hromadným bodem. Musí pak tedy ležet v $A_2$ a to u disjunktních otevřených množin není možné.

Dokázali jsme tedy, že pokud nějaký bod $y$ nepatří do obrazu intervalu, musí být všechny hodnoty buď zároveň větší nebo zároveň menší. Odtud vyplývá, že obrazem bude opět interval. Všimněme si, že krajní body tohoto intervalu mohou a nemusí do obrazu patřit.

Pokud obsahuje definiční interval $A$ i některý ze svých hraničních bodů, musí jej spojitá funkce zobrazit opět buď na hraniční nebo vnitřní bod obrazu vnitřku $A$. Tím je tvrzení ověřeno.

(2) Toto tvrzení je přímým důsledkem předchozího, protože obrazem ohraničeného uzavřeného intervalu (tj. kompaktní množiny) musí být opět uzavřený interval. □

Na závěr naší úvodní diskuse spojitosti funkcí uvedeme ještě tvrzení, která jsou užitečným nástrojem při počítání limit.

**5.27. Věta** (O limitě složené funkce)**.** *Nechť $f, g : \mathbb{R} \to \mathbb{R}$ jsou funkce,* $\lim_{x\to a} f(x) = b$.

[5] Tomuto tvrzení se (zejména v české literatuře) říká Bolzanova věta. Bernard Bolzano pracoval na začátku 19. století v Praze.

Ihned vidíme, že je

$$\lim_{x\to0}\frac{3\operatorname{tg}^2 x}{5x^2}=\lim_{x\to0}\left(\frac{3}{5}\cdot\frac{\sin x}{x}\cdot\frac{\sin x}{x}\cdot\frac{1}{\cos^2 x}\right)=$$
$$=\frac{3}{5}\cdot\lim_{x\to0}\frac{\sin x}{x}\cdot\lim_{x\to0}\frac{\sin x}{x}\cdot\lim_{x\to0}\frac{1}{\cos^2 x}=$$
$$=\frac{3}{5}\cdot1\cdot1\cdot1=\frac{3}{5}.$$

Vhodné rozšíření a substituce dávají

$$\lim_{x\to0}\frac{\sin(3x)}{\sin(5x)}=\lim_{x\to0}\left(\frac{\sin(3x)}{3x}\cdot\frac{5x}{\sin(5x)}\cdot\frac{3}{5}\right)=$$
$$=\lim_{x\to0}\frac{\sin(3x)}{3x}\cdot\lim_{x\to0}\frac{5x}{\sin(5x)}\cdot\frac{3}{5}=$$
$$=\lim_{y\to0}\frac{\sin y}{y}\cdot\lim_{z\to0}\frac{z}{\sin z}\cdot\frac{3}{5}=1\cdot1\cdot\frac{3}{5}=\frac{3}{5}.$$

Pomocí předešlého výsledku pak lehce spočítáme

$$\lim_{x\to0}\frac{\operatorname{tg}(3x)}{\sin(5x)}=\lim_{x\to0}\left(\frac{\sin(3x)}{\sin(5x)}\cdot\frac{1}{\cos(3x)}\right)=$$
$$=\lim_{x\to0}\frac{\sin(3x)}{\sin(5x)}\cdot\lim_{x\to0}\frac{1}{\cos(3x)}=\frac{3}{5}\cdot1=\frac{3}{5}.$$

Podobně můžeme stanovit

$$\lim_{x\to0}\frac{\mathrm{e}^{5x}-\mathrm{e}^{2x}}{x}=\lim_{x\to0}\left(\mathrm{e}^{2x}\,\frac{\mathrm{e}^{(5-2)x}-1}{(5-2)x}\,(5-2)\right)=$$
$$=\lim_{x\to0}\mathrm{e}^{2x}\cdot\lim_{x\to0}\frac{\mathrm{e}^{3x}-1}{3x}\cdot3=$$
$$=\mathrm{e}^0\cdot\lim_{y\to0}\frac{\mathrm{e}^{y}-1}{y}\cdot3=1\cdot1\cdot3=3$$

a rovněž

$$\lim_{x\to0}\frac{\mathrm{e}^{5x}-\mathrm{e}^{-x}}{\sin(2x)}=\lim_{x\to0}\left(\frac{\mathrm{e}^{5x}-1}{\sin(2x)}-\frac{\mathrm{e}^{-x}-1}{\sin(2x)}\right)=$$
$$=\lim_{x\to0}\left(\frac{\mathrm{e}^{5x}-1}{5x}\cdot\frac{2x}{\sin(2x)}\cdot\frac{5}{2}-\frac{\mathrm{e}^{-x}-1}{-x}\cdot\frac{2x}{\sin(2x)}\cdot\left(-\frac{1}{2}\right)\right)=$$
$$=\lim_{x\to0}\frac{\mathrm{e}^{5x}-1}{5x}\cdot\lim_{x\to0}\frac{2x}{\sin(2x)}\cdot\frac{5}{2}-$$
$$-\lim_{x\to0}\frac{\mathrm{e}^{-x}-1}{-x}\cdot\lim_{x\to0}\frac{2x}{\sin(2x)}\cdot\left(-\frac{1}{2}\right)=$$
$$=\lim_{u\to0}\frac{\mathrm{e}^{u}-1}{u}\cdot\lim_{z\to0}\frac{z}{\sin z}\cdot\frac{5}{2}-\lim_{v\to0}\frac{\mathrm{e}^{v}-1}{v}\cdot\lim_{z\to0}\frac{z}{\sin z}\cdot\left(-\frac{1}{2}\right)=$$
$$=\frac{5}{2}+\frac{1}{2}=3.$$

□

**5.58.** Vypočtěte limity

$$\lim_{x\to0}\frac{1-\cos(2x)}{x\sin x};\qquad\lim_{x\to0}\frac{1-\cos x}{x^2}.$$

**Řešení.** Využijeme faktu, že

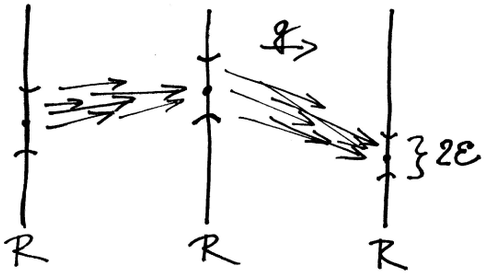
$$\lim_{x\to0}\frac{\sin x}{x}=1.$$

*(1) Pokud je funkce $g$ spojitá v bodě $b$, potom*

$$\lim_{x\to a}g\,(f(x))=g\left(\lim_{x\to a}f(x)\right)=g(b).$$

*(2) Jestliže existuje limita $\lim_{y\to b}g(y)$ a zároveň pro všechna $x$ z nějakého ryzího okolí bodu $a$ platí $f(x)\neq b$, potom*

$$\lim_{x\to a}g\,(f(x))=\lim_{y\to b}g(y).$$




Důkaz. První tvrzení se dokazuje podobně jako tvrzení 5.24(4). Ze spojitosti $g$ v bodě $b$ vyplývá, že pro jakékoliv okolí $V$ hodnoty $g(b)$ umíme najít dostatečně malé okolí $U$ bodu $b$, na kterém jsou už všechny hodnoty $g$ ve $V$. Pokud ale $f$ má bod $b$ jako limitu v bodě $a$, pak se do $U$ trefíme všemi hodnotami $f$ pro dostatečně malé ryzí okolí bodu $a$, což již ověřuje první tvrzení.

Pokud nemáme k dispozici spojitost funkce $g$ v bodě $b$, bude předchozí argumentace obecně platit také, když zajistíme, aby dostatečně malá ryzí okolí bodu $a$ byla funkcí $f$ zobrazena do ryzího okolí bodu $b$. □

**5.28. Kdo už je v ZOO.** Začali jsme budovat náš zvířetník funkcí s polynomy a s funkcemi, které se z nich dají vyrobit „po částech“. Zároveň jsme dovodili spoustu vlastností pro patrně obrovskou třídu spojitých funkcí, nemáme ale zatím moc prakticky zvladatelných příkladů, kromě polynomů. Jako další příklad si prohlédneme podíly polynomů.



Nechť $f$ a $g$ jsou dva polynomy, které mohou mít i komplexní hodnoty (tj. připouštíme výrazy $a_nx^n+\cdots+a_0$ s komplexními $a_i\in\mathbb{C}$, ale dosazujeme jen reálné hodnoty za proměnnou $x$).

Funkce $h:\mathbb{R}\setminus\{x\in\mathbb{R},\,g(x)=0\}\to\mathbb{C}$,

$$h(x)=\frac{f(x)}{g(x)}$$

je dobře definována ve všech reálných bodech $x$ kromě kořenů polynomu $g$. Takové funkce nazýváme *racionální funkce*. Z Věty 5.24 vyplývá, že racionální funkce jsou spojité ve všech bodech svého definičního oboru. V bodech, kde definovány nejsou, mohou mít

- konečnou limitu, když jde o společný kořen obou polynomů $f$ a $g$, přičemž jeho násobnost je v $f$ alespoň taková jako v $g$ (v tomto případě rozšířením jejich definice o limitní hodnotu v tomto bodě dostaneme funkci i v tomto bodě spojitou),
- nevlastní limitu, když nevlastní limity zprava a zleva v tomto bodě jsou stejné,
- různé nevlastní limity zprava a zleva.

Názorně je možné tuto situaci vidět na obrázku, který ukazuje hodnoty funkce

$$h(x)=\frac{(x-0{,}05a)(x-2-0{,}2a)(x-5)}{x(x-2)(x-4)}$$

Snadno získáváme

$$\lim_{x\to 0}\frac{1-\cos(2x)}{x\sin x}=\lim_{x\to 0}\frac{1-\left(\cos^2 x-\sin^2 x\right)}{x\sin x}=$$
$$=\lim_{x\to 0}\frac{\left(1-\cos^2 x\right)+\sin^2 x}{x\sin x}=$$
$$=\lim_{x\to 0}\frac{2\sin^2 x}{x\sin x}=\lim_{x\to 0}2\frac{\sin x}{x}=2;$$

resp.

$$\lim_{x\to 0}\frac{1-\cos x}{x^2}=\lim_{x\to 0}\left(\frac{1-\cos x}{x^2}\cdot\frac{1+\cos x}{1+\cos x}\right)=$$
$$=\lim_{x\to 0}\frac{1-\cos^2 x}{x^2\,(1+\cos x)}=\lim_{x\to 0}\frac{\sin^2 x}{x^2\,(1+\cos x)}=$$
$$=\left(\lim_{x\to 0}\frac{\sin x}{x}\right)^2\cdot\lim_{x\to 0}\frac{1}{1+\cos x}=\frac{1}{2}.$$

Dodejme, že jsme také mohli hned použít vyjádření

$$1-\cos(2x)=2\sin^2 x,\qquad x\in\mathbb{R}\,.$$ □

### D. Spojitost funkcí

**5.59.** Zkoumejte existenci limit a spojitost funkce $(x-1)^{-\operatorname{sgn} x}$ v bodech 0 a 1.

**Řešení.** Spočítejme nejprve jednostranné limity v bodě nula:

$$\lim_{x\to 0^-}(x-1)^{-\operatorname{sgn} x}=\lim_{x\to 0^-}(x-1)=-1,$$
$$\lim_{x\to 0^+}(x-1)^{-\operatorname{sgn} x}=\lim_{x\to 0^+}\frac{1}{x-1}=-1,$$

odtud $\lim_{x\to 0}(x-1)^{-\operatorname{sgn} x}=-1$, nicméně funkční hodnota této funkce je v bodě 0 rovna 1, tudíž zkoumaná funkce není v bodě 0 spojitá. Dále je

$$\lim_{x\to 1^-}(x-1)^{-\operatorname{sgn} x}=\lim_{x\to 1^-}\frac{1}{x-1}=-\infty,$$
$$\lim_{x\to 1^+}(x-1)^{-\operatorname{sgn} x}=\lim_{x\to 1^+}\frac{1}{x-1}=\infty.$$

V bodě 1 tedy existuje levostranná i pravostranná limita dané funkce, jejich hodnoty se ovšem liší, funkce tudíž nemá v bodě 1 limitu (a tak není v tomto bodě ani spojitá). □

**5.60.** Bez použití Věty o třech limitách dokažte, že funkce

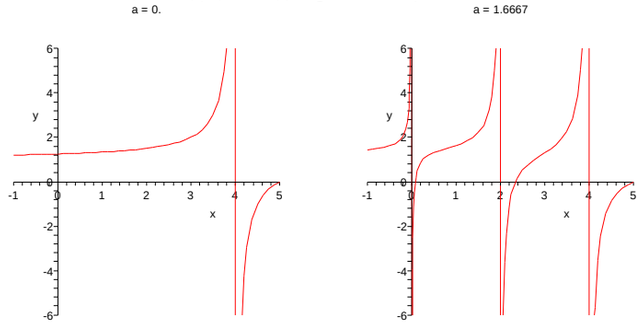
$$R(x)=\begin{cases}x, & x\in\left\{\frac{1}{n};\ n\in\mathbb{N}\right\};\\ 0, & x\in\mathbb{R}\setminus\left\{\frac{1}{n};\ n\in\mathbb{N}\right\}\end{cases}$$

je spojitá v bodě 0.

**Řešení.** Funkce $R$ je spojitá v bodě 0, právě když je

$$\lim_{x\to 0}R(x)=R(0)=0.$$

Z definice limity ukážeme, že tato limita se skutečně rovná 0. Při „obvyklém“ značení je $a=0$, $x_0=0$. Nechť $\delta>0$ je nadále libovolné. pro hodnoty $a=0$ (obrázek vlevo tedy vlastně zobrazuje racionální funkci $(x-5)/(x-4)$) a pro $a=5/3$.




**5.29. Funkce mocninné a exponenciální.** Polynomy jsou pomocí sčítání a násobení skaláry seskládány z jednoduchých mocninných funkcí $x\mapsto x^n$ s přirozeným exponentem $n=0,1,2,\ldots$. Samozřejmý smysl má také funkce $x\mapsto x^{-1}$ pro všechna $x\neq 0$. Tuto definici teď rozšíříme na obecnou *mocninnou funkci* $x^a$ s libovolným $a\in\mathbb{R}$.



Budeme vycházet z vlastností mocnin a odmocnin, které patrně považujeme za samozřejmé. Pro záporné celé číslo $-a$ proto definujeme

$$x^{-a}=(x^a)^{-1}=(x^{-1})^a.$$

Dále jistě chceme, aby ze vztahu $b^n=x$ pro $n\in\mathbb{N}$ vyplývalo, že $b$ je $n$–tou odmocninou z $x$, tj. $b=x^{\frac{1}{n}}$. Je třeba ale ověřit, že taková $b$ pro kladná reálná $x$ skutečně existují.

Z binomického rozkladu mocniny dvojčlenu je vidět, že funkce $y\mapsto y^n$ je pro $y>0$ stále rostoucí. Předpokládejme $x>0$ a uvažujme množinu $B=\{y\in\mathbb{R},\,y>0,\ y^n\leq x\}$. To je zřejmě shora ohraničená množina a zvolíme $b=\sup B$. O mocninné funkci s přirozeným $n$ již víme, že je to funkce spojitá, snadno tedy ověříme. že skutečně platí $b^n=x$. Skutečně, určitě je $b^n\leq x$ a kdyby platila ostrá nerovnost, našli bychom jistě i $y$ s hodnotou $b^n<y^n<x$, což nutně znamená i $b<y$ a tedy jde o spor s definicí suprema.

Máme tedy již korektně definovánu mocninnou funkci pro všechna racionální $a=\frac{p}{q}$, $x^a=(x^p)^{\frac{1}{q}}=(x^{\frac{1}{q}})^p$.

Konečně, pro hodnoty $a\in\mathbb{R}$ a $x>1$ si povšimněme, že jde pro racionální $a$ o striktně rostoucí výraz (pro větší $a$ je vždy větší výsledek). Proto klademe

$$x^a=\sup\{x^y,\,y\in\mathbb{Q},\ y\leq a\}.$$

Pro $0<x<1$ buď definujeme analogicky (je třeba si jen pohrát s nerovnítky) nebo klademe přímo $x^a=(\frac{1}{x})^{-a}$. Pro $x=1$ je pak $1^a=1$ pro libovolné $a$.

Obecnou mocninnou funkci $x\mapsto x^a$ máme tedy dobře definovanou pro všechny $x\in[0,\infty)$ a $a\in\mathbb{R}$. Naši konstrukci ale můžeme také číst následujícím způsobem: Pro každé pevné reálné $c>0$ existuje dobře definovaná funkce na celém $\mathbb{R}$, $y\mapsto c^y$. Této funkci říkáme *exponenciální funkce* o základu $c$.

Vlastnosti, které jsme použili při definici mocninné a exponenciální funkce $f(y)=c^y$, tj. $c=f(1)$, lze shrnout do jediné rovnosti pro libovolné reálné kladné $x$ a $y$:

$$f(x+y)=f(x)\cdot f(y)$$

Pro jakékoli $x \in (-\delta, \delta)$ je $R(x) = 0$, nebo $R(x) = x$, a tudíž (v obou případech) dostáváme $R(x) \in (-\delta, \delta)$. Jinými slovy, vezmeme-li libovolné $\delta$-okolí $(-\delta, \delta)$ hodnoty $a$ a přiřadíme-li mu $(-\delta, \delta)$ (jako okolí bodu $x_0$), pak pro každé $x \in (-\delta, \delta)$ (z uvažovaného okolí $x_0$) platí, že $R(x) \in (-\delta, \delta)$ (zde na interval $(-\delta, \delta)$ nahlížíme jako na okolí $a$). To odpovídá znění definice limity (nemuseli jsme ani požadovat, aby bylo $x \neq x_0$).

Uvažovaná funkce $R$ se nazývá Riemannova funkce (proto označení $R$). V literatuře se ovšem uvádí v různých modifikacích. Např. o funkci

$$f(x) = \begin{cases} 1, & x \in \mathbb{Z}; \\ \frac{1}{q}, & x = \frac{p}{q} \in \mathbb{Q} \text{ pro nesoudělná } p, q \in \mathbb{Z} \text{ a } q > 1; \\ 0, & x \notin \mathbb{Q} \end{cases}$$

se „často“ hovoří jako o Riemannově. □

**5.61.** Dodefinujte funkci

$$f(x) = \left(x^2 - 1\right) \sin \frac{2x-1}{x^2-1}, \quad x \neq \pm 1 \, (x \in \mathbb{R})$$

v bodech $-1$, 1 tak, aby byla spojitá na $\mathbb{R}$.

**Řešení.** Daná funkce je spojitá ve všech bodech svého definičního oboru. V bodech $-1$, 1 bude spojitá, právě když položíme

$$f(-1) := \lim_{x \to -1} \left( \left(x^2 - 1\right) \sin \frac{2x-1}{x^2-1} \right),$$

$$f(1) := \lim_{x \to 1} \left( \left(x^2 - 1\right) \sin \frac{2x-1}{x^2-1} \right).$$

Pokud by jedna z těchto limit neexistovala, příp. byla nevlastní, funkci by nešlo spojitě dodefinovat. Očividně je

$$\left| \sin \frac{2x-1}{x^2-1} \right| \leq 1, \quad x \neq \pm 1 \, (x \in \mathbb{R}),$$

odkud plyne

$$-\left|x^2 - 1\right| \leq f(x) \leq \left|x^2 - 1\right|, \quad x \neq \pm 1 \, (x \in \mathbb{R}).$$

Protože

$$\lim_{x \to \pm 1} \left|x^2 - 1\right| = 0,$$

z Věty o třech limitách již dostáváme výsledek $f(\pm 1) := 0$. □

**5.62.** Zjistěte, jestli má rovnice $\mathrm{e}^{2x} - x^4 + 3x^3 - 6x^2 = 5$ alespoň jedno kladné řešení.

**Řešení.** Uvažujme funkci

$$f(x) := \mathrm{e}^{2x} - x^4 + 3x^3 - 6x^2 - 5, \quad x \geq 0,$$

pro niž je

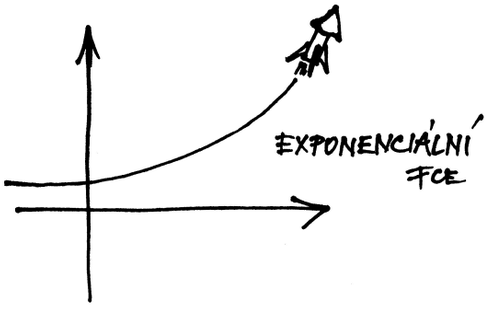
$$f(0) = -4, \quad \lim_{x \to +\infty} f(x) = \lim_{x \to +\infty} \mathrm{e}^{2x} = +\infty.$$

společně s požadavkem spojitosti.

Skutečně, pro $y = 0$ dostáváme z této rovnosti $f(0) = 1$, odtud pak $1 = f(0) = f(x - x) = f(x) \cdot (f(x))^{-1}$ a konečně pro přirozené $n$ je zjevně $f(nx) = (f(x))^n$. Takto jsme již jednoznačně určili hodnoty $x^a$ pro všechny $x > 0$ a $a \in \mathbb{Q}$ a požadavkem spojitosti byla již funkce určena všude.

Zejména tedy pro exponenciální funkci platí známé vztahy

$$a^x \cdot a^y = a^{x+y}, \quad (a^x)^y = a^{x \cdot y}. \tag{5.5}$$




**5.30. Logaritmické funkce.** Viděli jsme právě, že exponenciální funkce $f(x) = a^x$ je pro $a > 1$ stále rostoucí a pro $0 < a < 1$ je stále klesající. V obou případech tedy existuje k $f(x)$ funkce inverzní $f^{-1}(x)$ kterou nazýváme *logaritmickou funkcí se základem* $a$. Píšeme $\log_a(x)$ a definiční vztah tedy je $\log_a(a^x) = x$.

Rovnosti (5.5) jsou proto ekvivalentní vztahům

$$\log_a(x \cdot y) = \log_a(x) + \log_a(y), \quad \log_a(x^y) = y \cdot \log_a(x).$$

Logaritmické funkce jsou definovány jen pro kladné hodnoty argumentu a jsou pro základ $a > 1$ rostoucí, pro základ $0 < a < 1$ klesající na celém definičním oboru. Pro každé $a$ je $\log_a(1) = 0$.

Brzy uvidíme, že obzvlášť důležitou hodnotou pro $a$ je tzv. Eulerovo číslo e, viz odstavec 5.42. Funkci $\log_{\mathrm{e}}(x)$ nazýváme *přirozeným logaritmem*. Tuto funkci pak značíme $\ln(x)$.

### 3. Derivace



U polynomů jsme již v odstavci 5.6 diskutovali, jak popisovat jednoduše velikost růstu hodnot polynomu kolem daného bodu jeho definičního oboru. Tehdy jsme pozorovali podíl (5.2), který vyjadřoval směrnici sečny mezi body $[x, f(x)] \in \mathbb{R}^2$ a $[x+\Delta x, f(x+\Delta x)] \in \mathbb{R}^2$ pro (malý) přírůstek $\Delta x$ nezávisle proměnné. Tehdejší úvaha funguje zrovna stejně pro libovolnou reálnou nebo komplexní funkci $f$, jen musíme místo intuitivního „zmenšování“ přírůstku $\Delta x$ pracovat s pojmem limity.

Uvádíme definici pro vlastní i nevlastní derivace, tj. připouštíme i nekonečné hodnoty. Všimněte si, že na rozdíl od limity funkce, u derivace v daném bodě $x_0$ je nutné, aby byla sama funkce v tomto bodě definovaná.

DERIVACE FUNKCE JEDNÉ REÁLNÉ PROMĚNNÉ

**5.31.** Nechť $f$ je reálná nebo komplexní funkce definovaná na intervalu $A \subseteq \mathbb{R}$ a $x_0 \in A$. Jestliže existuje limita

$$\lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0} = a,$$

pak říkáme, že $f$ má v bodě $x_0$ *derivaci* $a$. Hodnotu derivace zapisujeme jako $f'(x_0)$ nebo $\frac{df}{dx}(x_0)$, případně $a = \frac{d}{dx} f(x_0)$.

Ze spojitosti funkce $f$ na celém jejím definičním oboru tudíž vyplývá, že nabývá všech hodnot $y \in [-4, +\infty)$. Zvláště její graf nutně protíná kladnou poloosu $x$, tj. rovnice $f(x) = 0$ má řešení. □

*5.63.* V jakých bodech $x \in \mathbb{R}$ je funkce

$$y = \cos\left(\operatorname{arctg}\left(\left|\,12x^{21} + 11\,\right| \cdot \frac{e^{\cos(x+2)-x^3}}{-11 - x^{12}}\right)\right) + \sin(\sin(\sin x))$$

s maximálním definičním oborem spojitá? ○

*5.64.* Rozhodněte, zda je funkce

$$f(x) = \begin{cases} x, & x < 0; \\ 0, & 0 \le x < 1; \\ x, & x = 1; \\ 0, & 1 < x < 2; \\ x, & 2 \le x \le 3; \\ \frac{1}{x-3}, & x > 3 \end{cases}$$

spojitá; spojitá zleva; spojitá zprava v bodech $-\pi, 0, 1, 2, 3, \pi$. ○

*5.65.* Dodefinujte funkci

$$f(x) = \operatorname{arctg}\left(1 + \frac{5}{x^2}\right) \cdot \sin^2 x^5, \qquad x \in \mathbb{R} \setminus \{0\}$$

pro $x = 0$ tak, aby byla v tomto bodě spojitá. ○

*5.66.* Uveďte $p \in \mathbb{R}$, pro které je funkce

$$f(x) = \frac{\sin(6x)}{3x}, \quad x \in \mathbb{R} \setminus \{0\}; \qquad f(0) = p$$

spojitá v počátku. ○

*5.67.* Zvolte reálnou hodnotu $a$ tak, aby funkce

$$h(x) = \frac{x^4 - 1}{x - 1}, \quad x > 1; \qquad h(x) = a, \quad x \le 1$$

byla spojitá v $\mathbb{R}$. ○

*5.68.* Vypočtěte

$$\lim_{x \to 0+} \frac{\sin^8 x}{x^3}; \qquad \lim_{x \to -\infty} \frac{\sin^8 x}{x^3}.$$

○

**5.69.** Určete všechny hodnoty parametru $a \in \mathbb{R}$ tak, aby byla nerovnice

$$(a-2)x^2 - (a-2)x + 1 > 0$$

splněna pro všechna reálná $x$.

**Řešení.** Všimněme si, že pro $a = 2$ je nerovnost triviálně splněna (levá strana je konstanta 1). Pro $a \neq 2$ je levá strana kvadratickou funkcí $f(x)$ proměnné $x$, přičemž je $f(0) = 1$. Vzhledem ke spojitosti funkce $f(x)$ tak bude nerovnost $f(x) > 0$ platit pro všechna reálná $x$, právě když rovnice $f(x) = 0$ nebude mít řešení v $\mathbb{R}$ (graf funkce $f$ pak bude celý „nad“ osou $x$) a to nastane, právě když diskriminant

Derivace reálné funkce je *vlastní*, resp. *nevlastní*, když je takovou příslušná limita.

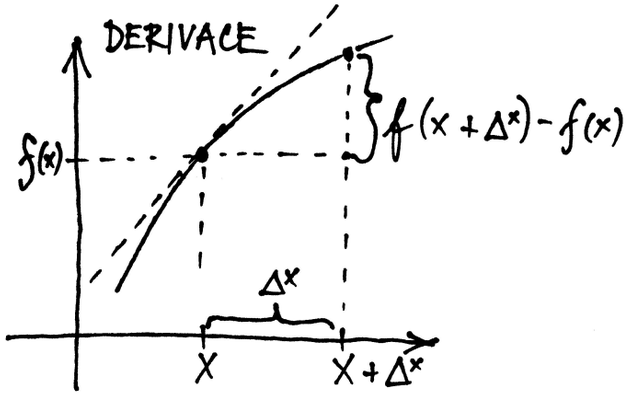
*Jednostranné derivace* (tj. derivaci zprava a zleva) definujeme zcela stejně pomocí limity zprava a zleva.

O funkci mající v bodě $x_0$ derivaci říkáme, že je v tomto bodě *diferencovatelná*. O funkci diferencovatelné v každém bodě intervalu říkáme, že je diferencovatelná na tomto intervalu.

S derivacemi se vcelku snadno počítá, dá nám ale dost práce korektně odvodit derivace i některých z funkcí, které už v našem zvěřinci máme. Proto s předstihem vsunujeme do textu souhrnnou tabulku, jak derivace pro několik z nich vychází. V posledním sloupci je odkaz na odstavec, kde se dá údaj skutečně i s úplným výkladem najít. Všimněme si také, že inverzní funkce k řadě z našich funkcí sice neumíme přímo vyjádřit elementárním způsobem, přesto ale budeme umět počítat jejich derivace, viz 5.35

NĚKTERÉ DERIVACE FUNKCÍ

| **funkce** | **definiční obor** | **derivace** | |
|---|---|---|---|
| polynomy $f(x)$ | celé $\mathbb{R}$ | $f'(x)$ je opět polynom | 5.6 |
| kubické splajny $h(x)$ | celé $\mathbb{R}$ | $h'(x)$ má spojitou pouze první derivaci | 5.9 |
| racionální funkce $f(x)/g(x)$ | celé $\mathbb{R}$ kromě kořenů $g$ | racionální funkce: $\frac{f'(x)g(x) - f(x)g'(x)}{g(x)^2}$ | 5.34 |
| mocninné funkce $f(x) = x^a$ | interval $(0, \infty)$ | $f'(x) = ax^{a-1}$ | 5.36, 5.44 |
| exponenciála $f(x) = a^x$, $a > 0, a \neq 1$ | celé $\mathbb{R}$ | $f'(x) = \ln(a) \cdot a^x$ | 5.36, 5.44 |
| logaritmus $f(x) = \ln_a(x)$, $a > 0, a \neq 1$ | interval $(0, \infty)$ | $f'(x) = (\ln(a))^{-1} \cdot \frac{1}{x}$ | 5.36, 5.44 |




Z formulace definice lze očekávat, že $f'(x_0)$ bude umožňovat dobře aproximovat danou funkci pomocí přímky

$$y = f(x_0) + f'(x_0)(x - x_0).$$

kvadratické rovnice $(a-2)x^2-(a-2)x+1=0$ bude záporný. Dostáváme tak nutnou a postačující podmínku

$$D=(a-2)^2-4(a-2)=(a-2)(a-6)<0.$$

Ta je splněna pro $a\in(2,6)$. Celkem je nerovnice splněna pro všechna reálná $x$ pro $a\in[2,6)$. □

**5.70.** V $\mathbb{R}$ řešte rovnici

$$2^x+3^x+4^x+5^x+6^x=5\,.$$

**Řešení.** Funkce na levé straně rovnice je součtem pěti rostoucích funkcí na $\mathbb{R}$, je tedy sama rostoucí funkcí na celém $\mathbb{R}$. Hodnota levé strany je pro $x=0$ rovna 5, což je tedy jediným řešením dané rovnice. □

*5.71.* V $\mathbb{R}$ řešte rovnici

$$2^x+3^x+6^x=1\,.$$ ○

*5.72.* Rozhodněte, zda polynom

$$x^{37}+5x^{21}-4x^9+5x^4-2x-3$$

má v intervalu $(-1,1)$ alespoň jeden reálný kořen. ○

### E. Derivace

Ukažme si nejprve, že derivace funkcí uvedené v tabulce v odstavci 5.31 jsou skutečně správně. Určíme je přímo z definice derivace.

**5.73.** Z definice (viz 5.31) určete hodnoty derivací funkcí $x^n$ ($x$ je proměnná, $n$ kladná celá konstanta), $\sqrt{x}$, $\sin x$.

**Řešení.** Nejprve podotkněme, že označíme-li v definici derivace výraz $x-x_0$ jako $h$, pak dostáváme

$$\lim_{x\to x_0}\frac{f(x)-f(x_0)}{x-x_0}=\lim_{h\to 0}\frac{f(x_0+h)-f(x_0)}{h}.$$

V následujících výpočtech budeme pracovat s druhým vyjádřením téže limity.



Takto lze rozumět následujícímu lemmatu, které říká, že nahrazením konstantního koeficientu $f'(x_0)$ ve vyjádření přímky spojitou funkcí $\psi(x)$ dostaneme přímo hodnoty $f$. Odchylka hodnot $\psi(x)$ na okolí bodu $x_0$ od hodnoty $\psi(x_0)$ pak přímo říká, jak se liší směrnice sečen a tečny v bodě $x_0$.

**Lemma.** *(Carathéodoryho) Reálná nebo komplexní funkce $f(x)$ má v bodě $x_0$ vlastní derivaci, právě když existuje na nějakém okolí $\mathcal{O}(x_0)$ funkce $\psi$ spojitá v $x_0$ a taková, že pro všechny $x\in\mathcal{O}(x_0)$ platí*

$$f(x)=f(x_0)+\psi(x)(x-x_0).$$

*Navíc pak vždy $\psi(x_0)=f'(x_0)$ a sama funkce $f$ je v bodě $x_0$ spojitá.*

Důkaz. Nejprve předpokládejme, že $f'(x_0)$ je vlastní derivace. Pokud má $\psi$ existovat, má jistě pro všechny $x\in\mathcal{O}\setminus\{x_0\}$ tvar

$$\psi(x)=(f(x)-f(x_0))/(x-x_0).$$

V bodě $x_0$ naopak definujme hodnotu derivací $f'(x_0)$. Pak jistě

$$\lim_{x\to x_0}\psi(x)=f'(x_0)=\psi(x_0)$$

jak je požadováno.

Naopak, jestliže taková funkce $\psi$ existuje, tentýž postup vypočte její limitu v $x_0$. Proto existuje i $f'(x_0)$ a je $\psi(x_0)$ rovna.

Z vyjádření $f$ pomocí spojitých funkcí je zřejmé, že je sama spojitá v bodě $x_0$. □

**5.32. Geometrický význam derivace.** Předchozí lemma lze názorně vysvětlit geometricky a tím popsat smysl derivace. Říká totiž, že na grafu funkce $y=f(x)$, tj. na příslušné křivce v rovině se souřadnicemi $x$ a $y$, poznáme, zda existuje derivace podle toho, jestli se spojitě mění hodnota směrnice sečny procházející body $[x_0,f(x_0)]$ a $[x,f(x)]$. Pokud ano, pak limitní hodnota této směrnice je hodnotou derivace.



Rostoucí a klesající funkce v bodě

**Důsledek.** *Má-li reálná funkce $f$ v bodě $x_0\in\mathbb{R}$ derivaci $f'(x_0)>0$, pak pro nějaké okolí $\mathcal{O}(x_0)$ platí $f(x)>f(x_0)$ pro všechny body $x\in\mathcal{O}(x_0)$, $x>x_0$ a $f(x)<f(x_0)$ pro všechny body $x\in\mathcal{O}(x_0)$, $x<x_0$.*

*Je-li derivace $f'(x_0)<0$, pak naopak pro nějaké okolí $\mathcal{O}(x_0)$ platí $f(x)<f(x_0)$ pro všechny body $x\in\mathcal{O}(x_0)$, $x>x_0$, a $f(x)>f(x_0)$ pro všechny body $x\in\mathcal{O}(x_0)$, $x<x_0$.*

Důkaz. Uvažme prvý případ. Pak podle předchozího lemmatu platí $f(x)=f(x_0)+\psi(x)(x-x_0)$ a $\psi(x_0)>0$. Protože je ale $\psi$ v $x_0$ spojitá, musí existovat okolí $\mathcal{O}(x_0)$, na kterém bude $\psi(x)>0$. Pak ale s rostoucím $x>x_0$ nutně poroste i hodnota $f(x)>f(x_0)$ a naopak pro $x<x_0$.

Stejná argumentace ověří i tvrzení se zápornou derivací. □

Funkce, které mají na nějakém okolí bodu $x_0$ vlastnost $f(x)>f(x_0)$, kdykoliv $x>x_0$, a $f(x)<f(x_0)$, když $x<x_0$, se nazývají *rostoucí v bodě* $x_0$. Funkce rostoucí ve všech bodech nějakého intervalu se nazývá *rostoucí na intervalu*. Samozřejmě pro funkce rostoucí na intervalu platí $f(b)>f(a)$ pro všechny $a<b$ z tohoto intervalu.

$$
\begin{aligned}
(x^n)' &= \lim_{h\to 0}\frac{(x+h)^n - x^n}{h} = \lim_{h\to 0}\frac{\binom{n}{1}x^{n-1}h + \binom{n}{2}x^{n-2}h^2 + \cdots + h^n}{h} = \\
&= nx^{n-1} + \lim_{h\to 0}\left(\binom{n}{2}x^{n-2}h + \binom{n}{3}x^{n-3}h^2 + \cdots + h^{n-1}\right) = \\
&= nx^{n-1}, \\
(\sqrt{x})' &= \lim_{h\to 0}\frac{\sqrt{x+h}-\sqrt{x}}{h} = \lim_{h\to 0}\frac{(\sqrt{x+h}-\sqrt{x})(\sqrt{x+h}+\sqrt{x})}{h(\sqrt{x+h}+\sqrt{x})} = \\
&= \lim_{h\to 0}\frac{h}{h(\sqrt{x+h}+\sqrt{x})} = \lim_{h\to 0}\frac{1}{\sqrt{x+h}+\sqrt{x}} = \frac{1}{2\sqrt{x}}, \\
(\sin x)' &= \lim_{h\to 0}\frac{\sin(x+h)-\sin x}{h} = \\
&= \lim_{h\to 0}\frac{\sin x\cos h + \cos x\sin h - \sin x}{h} = \\
&= \lim_{h\to 0}\frac{\cos x\sin h}{h} + \lim_{h\to 0}\frac{\sin x(\cos h - 1)}{h} = \\
&= \cos x\cdot\lim_{h\to 0}\frac{\sin h}{h} - \lim_{h\to 0}\frac{2(\sin\frac{h}{2})^2}{h} = \\
&= \cos x\cdot 1 + \lim_{t\to 0}\sin t\frac{\sin t}{t} = \cos x.
\end{aligned}
$$

□

**5.74.** Zderivujte a výsledek upravte:



i) $x\sin x$,
ii) $\frac{\sin x}{x}$,
iii) $\ln(x+\sqrt{x^2-a^2})$, $a\neq 0$, $|x|\geq|a|$,
iv) $\arctan\left(\frac{x}{\sqrt{1-x^2}}\right)$, $|x|\leq 1$,
v) $x^x$.

**Řešení.** (i) Podle pravidla o derivování součinu funkcí, tedy Leibnizova pravidla, viz 5.33 dostáváme

$$(x\sin x)' = x'\cdot\sin x + x\cdot(\sin x)' = \sin x + x\cos x.$$

(ii) Podle pravidla o derivování podílu funkcí (5.34) je

$$\left(\frac{\sin x}{x}\right)' = \frac{(\sin x)'\cdot x - \sin x\cdot x'}{x^2} = \frac{x\cos x - \sin x}{x^2}.$$

(iii) Použijeme pravidla pro derivování složené funkce (5.33). Označíme-li $h(x)=\ln(x)$, $f(x)=x+\sqrt{x^2-a^2}$, máme

$$
\begin{aligned}
\ln(x+\sqrt{x^2-a^2})' &= h(f(x))' = h'(f(x))\cdot f'(x) = \\
&= \frac{(x+\sqrt{x^2-a^2})'}{x+\sqrt{x^2-a^2}} = \frac{1+\frac{x}{x^2-a^2}}{x+\sqrt{x^2-a^2}},
\end{aligned}
$$

kde jsme pro derivování výrazu $\sqrt{x^2-a^2}$ použili opět pravidlo o derivování složené funkce.

Podobně je funkce *klesající v bodu* $x_0$, jestliže má na nějakém okolí bodu $x_0$ vlastnost $f(x) < f(x_0)$, kdykoliv $x > x_0$, a $f(x) > f(x_0)$, když $x < x_0$. Funkce je *klesající na intervalu*, jestliže je klesající ve všech bodech tohoto intervalu.

Náš důsledek tedy říká, že funkce, která má v bodě nenulovou konečnou derivaci, je v tomto bodě buď rostoucí nebo klesající podle znaménka této derivace.

Pokud má funkce $f$ v okolí bodu $x_0$ spojitou derivaci $f'(x_0)\neq 0$, pak je tato funkce na nějakém okolí bodu $x_0$ rostoucí nebo klesající, podle znaménka derivace. Skutečně, jako spojitá nenulová funkce má $f'(x_0)$ v nějakém okolí $x_0$ stále stejné znaménko.

Jako ilustraci jednoduchého použití vztahu derivace k růstu hodnot funkce se podívejme na existenci inverzí polynomů. Protože polynomy jen zřídka jsou výhradně rostoucí nebo klesající funkce, nemůžeme očekávat, že by k nim existovaly globálně definované inverzní funkce. Naopak ovšem inverzní funkce k polynomu $f$ existují na každém intervalu mezi kořeny derivace $f'$, tj. tam kde derivace polynomu je nenulová a nemění znaménko. Tyto inverzní funkce nebudou nikdy polynomy, až na případ polynomů stupně jedna, kdy z rovnice

$$y = ax + b$$

spočteme přímo

$$x = \frac{1}{a}(y-b).$$

U polynomu druhého stupně obdobně

$$y = ax^2 + bx + c$$

vede ke vztahu

$$x = \frac{-b \pm \sqrt{b^2 - 4a(c-y)}}{2a}$$

a inverze tedy existuje (a je dána touto formulí) jen pro $x$ na intervalech $\left(-\infty, -\frac{b}{2a}\right)$, $\left(-\frac{b}{2a}, \infty\right)$.

Pro práci s inverzními funkcemi k polynomům nevystačíme s dosavadními funkcemi a dostáváme v našem zvířetníku nové přírůstky.

**5.33. Pravidla pro počítání derivací.** Uveďme si nyní několik základních tvrzení o výpočtech derivací. Říkají nám, jak dobře se snáší operace derivování s algebraickými operacemi sčítání a násobení na reálných nebo komplexních funkcích. Poslední z pravidel pak umožňuje efektivní výpočet derivace složených funkcí a říkává se mu „řetězové pravidlo“.



Intuitivně jim můžeme všem velice snadno rozumět, když si derivaci funkce $y = f(x)$ představíme jako podíl přírůstků závislé proměnné $y$ a nezávislé proměnné $x$:

$$f' = \frac{\Delta y}{\Delta x}.$$

Samozřejmě pak při $y = h(x) = f(x) + g(x)$ je přírůstek $y$ dán součtem přírůstků $f$ a $g$ a přírůstek závislé proměnné zůstává stejný. Je tedy derivace součtu součtem derivací.

U součinu musíme být malinko pozornější. Pro $y = f(x)g(x)$ je přírůstek

$$
\begin{aligned}
\Delta y &= f(x+\Delta x)g(x+\Delta x) - f(x)g(x) = \\
&= f(x+\Delta x)(g(x+\Delta x)-g(x)) + (f(x+\Delta x)-f(x))g(x).
\end{aligned}
$$

(iv) Opět derivujeme složenou funkci:

$$\left[\arctan\left(\frac{x}{\sqrt{1-x^2}}\right)\right]' = \frac{1}{1+\frac{x^2}{1-x^2}} \cdot \left(\frac{x}{\sqrt{1-x^2}}\right)' =$$
$$= \frac{1}{1+\frac{x^2}{1-x^2}} \cdot \frac{\sqrt{1-x^2}+\frac{x^2}{\sqrt{1-x^2}}}{1-x^2} =$$
$$= \sqrt{1-x^2} + \frac{x^2}{\sqrt{1-x^2}} = \frac{1}{\sqrt{1-x^2}}.$$

(v) Funkci je nejprve převedeme na funkci o konstantním základu (nejlépe o základu $e$), kterou už umíme derivovat.

$$(x^x)' = \left((e^{\ln x})^x\right)' = (e^{x\ln x})' =$$
$$= (x\ln x)' \cdot e^{x\ln x} = (1+\ln x)\cdot x^x\ . \qquad \square$$

**5.75.** Určete derivaci funkce $y = x^{\sin x}$, $x > 0$.

**Řešení.** Platí

$$\left(x^{\sin x}\right)' = \left(\mathrm{e}^{\sin x\ \ln x}\right)' = \mathrm{e}^{\sin x\ \ln x}\left(\cos x\ \ln x + \frac{\sin x}{x}\right) =$$
$$= x^{\sin x}\left(\cos x\ \ln x + \frac{\sin x}{x}\right).$$

$\square$

*5.76.* Pro kladná $x$ uveďte derivaci funkce

$$f(x) = x^{\ln x}\ . \qquad \bigcirc$$

*5.77.* Pro $x \in (0, \pi/2)$ spočtěte derivaci funkce

$$y = (\sin x)^{\cos x}\ . \qquad \bigcirc$$

Doporučujeme čtenáři si vymyslet funkce, které potom sám zderivuje. Výsledek si může ověřit v celé řadě matematických výpočetních programů. V následujícím příkladu si uvědomíme geometrický význam derivace bodě, totiž, že určuje směrnici tečny ke grafu v daném bodě (viz 5.32)

**5.78.** Za pomoci diferenciálu přibližně určete arccotg 1,02.

**Řešení.** Diferenciál funkce $f$ se spojitou první derivací v bodě $x_0$ je roven

$$f'(x_0)\ dx = f'(x_0)\ (x - x_0)\ .$$

Rovnice tečny ke grafu funkce $f$ v bodě $[x_0, f(x_0)]$ je pak

$$y - f(x_0) = f'(x_0)\ (x - x_0)\ .$$

Odtud je vidět, že diferenciál funkce je přírůstek funkce na tečně. Hodnoty na tečně ovšem aproximují hodnoty $f(x)$, je-li rozdíl $x - x_0$ „malý“. Získáváme tak vzorec pro přibližné určení funkční hodnoty pomocí diferenciálu ve tvaru

$$f(x) \approx f(x_0) + f'(x_0)\ (x - x_0)\ .$$

Položíme-li tedy

$$f(x) := \operatorname{arccotg} x, \quad x_0 := 1,$$

Nyní ale když budeme zmenšovat přírůstek $\Delta x$, jde vlastně o výpočet limity součtu součinů a o tom už víme, že jej lze počítat jako součet součinů limit. Proto z naší formulky lze očekávat pro derivaci součinu $fg$ výraz $fg' + f'g$, kterému se říká *Leibnizovo pravidlo.*

Ještě zajímavěji se chová derivace složené funkce

$$g = h \circ f,$$

kde definiční obor funkce $z = h(y)$ obsahuje obor hodnot funkce $y = f(x)$. Opět vypsáním přírůstků dostáváme

$$g' = \frac{\Delta z}{\Delta x} = \frac{\Delta z}{\Delta y}\frac{\Delta y}{\Delta x}.$$

Můžeme tedy očekávat, že pravidlo pro výpočet bude

$$(h \circ f)'(x) = h'(f(x))\, f'(x).$$

Podáme nyní korektní formulace a důkaz:

### Pravidla pro derivování

**Věta.** *Nechť $f$ a $g$ jsou reálné nebo komplexní funkce definované na okolí bodu $x_0 \in \mathbb{R}$ a mající v tomto bodě vlastní derivaci. Potom*

*(1) pro každé reálné nebo komplexní číslo $c$ má funkce $x \mapsto c \cdot f(x)$ derivaci v $x_0$ a platí*

$$(cf)'(x_0) = c(f'(x_0)),$$

*(2) funkce $f + g$ má v $x_0$ derivaci a platí*

$$(f+g)'(x_0) = f'(x_0) + g'(x_0),$$

*(3) funkce $f \cdot g$ má v $x_0$ derivaci a platí*

$$(f\cdot g)'(x_0) = f'(x_0)g(x_0) + f(x_0)g'(x_0).$$

*(4) Je-li dále $h$ funkce definovaná na okolí obrazu $y_0 = f(x_0)$, která má derivaci v bodě $y_0$, má také složená funkce $h \circ f$ derivaci v bodě $x_0$ a platí*

$$(h\circ f)'(x_0) = h'(f(x_0)) \cdot f'(x_0).$$

Důkaz. (1) a (2) Přímé použití věty o součtech a součinech limit funkcí dává výsledek.

(3) Přepíšeme vztah pro podíl přírůstků, který jsme zmínili před formulací věty, takto

$$\frac{(fg)(x) - (fg)(x_0)}{x - x_0} =$$
$$= f(x)\frac{g(x) - g(x_0)}{x - x_0} + \frac{f(x) - f(x_0)}{x - x_0}g(x_0).$$

Limita tohoto výrazu pro $x \to x_0$ dá právě požadovaný výsledek, protože je funkce $f$ spojitá v $x_0$.

(4) Podle lemmatu 5.31 existují funkce $\psi$ a $\varphi$ spojité v bodech $x_0$ a $y_0 = f(x_0)$ takové, že

$$h(y) = h(y_0) + \varphi(y)(y - y_0),\ \ f(x) = f(x_0) + \psi(x)(x - x_0)$$

na nějakých okolích $x_0$ a $y_0$. Navíc pro ně platí $\psi(x_0) = f'(x_0)$ a $\varphi(y_0) = h'(y_0)$. Pak ovšem také platí

$$h(f(x)) - h(f(x_0)) = \varphi(f(x))(f(x) - f(x_0)) =$$
$$= \varphi(f(x))\psi(x)(x - x_0)$$

pro $x$ z okolí bodu $x_0$. Součin $\varphi(f(x))\psi(x)$ je ovšem spojitá funkce v $x_0$ a její hodnota v bodě $x_0$ je právě požadovaná derivace složené funkce, opět podle lemmatu 5.31. $\square$

obdržíme

$$\operatorname{arccotg} 1{,}02 \approx \operatorname{arccotg} 1 + \frac{-1}{1+1^2}\,(1{,}02-1) = \frac{\pi}{4} - 0{,}01.$$

Ještě podotkněme, že bod $x_0$ sice volíme tak, aby výraz $x - x_0$ byl blízký nule, ale současně musíme být schopni v tomto bodě vyčíslit funkce $f$ a $f'$. □

*5.79.* Za pomoci diferenciálu přibližně určete $\arcsin 0{,}497$. ○

*5.80.* Za pomoci diferenciálu vyčíslete

$$a := \operatorname{arctg} 1{,}02; \quad b := \sqrt[3]{70}\,.$$ ○

*5.81.* Pomocí diferenciálu přibližně vyjádřete

(a) $\sin\left(\frac{29}{180}\pi\right)$;

(b) $\sin\left(\frac{46}{180}\pi\right)$. ○

**5.82.** Určete parametr $c \in \mathbb{R}$ tak, aby tečna ke grafu funkce $\frac{\ln(c\cdot x)}{\sqrt{x}}$ v bodě $[1, 0]$ procházela bodem $[2, 2]$.

**Řešení.** Podle zadání má mít tečna směrnici $\frac{2-0}{2-1} = 2$. Směrnice je určena derivací funkce v daném bodě, dostáváme tedy podmínku

$$\left.\frac{2-\ln(cx)}{2\sqrt{x}}\right|_{x=1} = 2, \text{ neboli } \quad 2 - \ln(c) = 4,$$

tedy $c = \frac{1}{e^2}$. Pro $c = \frac{1}{e^2}$ je však hodnota funkce $\frac{ln(c\cdot x)}{\sqrt{x}}$ v bodě 1 rovna $-2$. Tedy žádné takové $c$ neexistuje. □

*5.83.* Rozhodněte, zda má polynom $x\,(x-4)^5$ alespoň v jednom bodě intervalu $(0, 4)$ tečnu rovnoběžnou s osou $x$. ○

*5.84.* Nechť $p \in (0, +\infty)$. Napište rovnici tečny k parabole $2py = x^2$ v obecném bodě $[x_0, ?]$. ○

*5.85.* Nalezněte rovnici normály ke grafu funkce $y = 1 - \mathrm{e}^{\frac{x}{2}}$, $x \in \mathbb{R}$ v bodě, který je průsečíkem tohoto grafu s osou $x$. ○

*5.86.* Najděte rovnice tečny a normály ke křivce

$$y = (x+1)\sqrt[3]{3-x}, \quad x \in \mathbb{R}$$

v bodě $[-1, 0]$. ○

*5.87.* Nechť je dána funkce

$$y = \frac{\ln\left(2x^3 + 4x^2 - x\right)}{1+x}, \quad x \in \left(\frac{1}{2}, +\infty\right).$$

Stanovte rovnice tečny a normály ke grafu této funkce v bodě $[1, ?]$. ○

*5.88.* V jakých bodech je tečna paraboly

$$y = 2 + x - x^2, \quad x \in \mathbb{R}$$

rovnoběžná s osou $x$? ○

*5.89.* Uveďte rovnice tečny $t$ a normály $n$ ke grafu funkce

$$y = \sqrt{x^2 - 3x + 11}, \quad x \in \mathbb{R}$$

DERIVACE PODÍLU

**5.34. Důsledek.** *Nechť $f$ a $g$ jsou reálné funkce, která mají v bodě $x_0$ vlastní derivace a $g(x_0) \neq 0$. Pak pro funkci $h(x) = f(x)(g(x))^{-1}$ platí*

$$h'(x_0) = \left(\frac{f}{g}\right)'(x_0) = \frac{f'(x_0)g(x_0) - f(x_0)g'(x_0)}{(g(x_0))^2}.$$

DŮKAZ. Dokážeme si nejprve speciální případ vzorce pro $h(x) = x^{-1}$. Přímo z definice derivace dostáváme

$$h'(x) = \lim_{\Delta x\to 0} \frac{\frac{1}{x+\Delta x} - \frac{1}{x}}{\Delta x} = \lim_{\Delta x\to 0} \frac{x - x - \Delta x}{\Delta x(x^2 + x\Delta x)} =$$

$$= \lim_{\Delta x\to 0} \frac{-1}{x^2 + x\Delta x}$$

a z pravidel pro počítání limit okamžitě plyne

$$h'(x) = -x^{-2}.$$

Nyní pravidlo pro derivaci složené funkce říká, že

$$(g^{-1})' = -g^{-2}\cdot g',$$

a konečně pravidlo pro derivaci součinu nám dává právě

$$(f/g)' = \left(f\cdot g^{-1}\right)' = f'g^{-1} - fg^{-2}g' = \frac{f'g - gf'}{g^2}$$

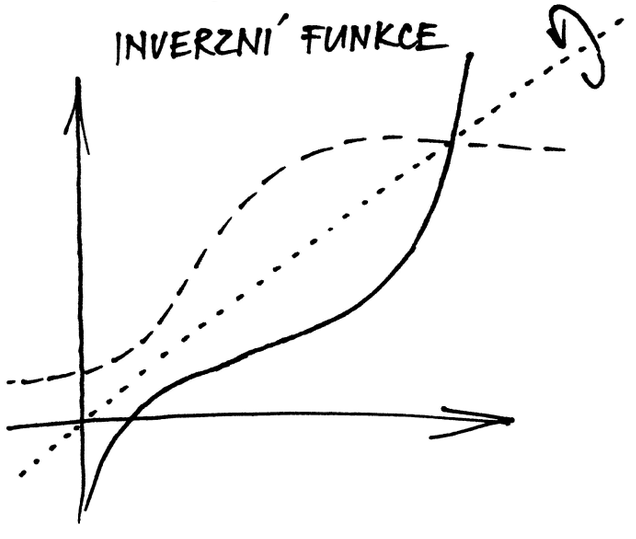
. □

**5.35. Derivace inverzních funkcí.** V odstavci 1.36 jsme při obecné diskusi relací a zobrazení formulovali pojem *inverzní funkce*. Pokud k dané funkci $f : \mathbb{R} \to \mathbb{R}$ inverzní funkce $f^{-1}$ existuje (nezaměňujme značení s funkcí $x \mapsto (f(x))^{-1}$), pak je dána jednoznačně kterýmkoliv ze vztahů



$$f^{-1}\circ f = \mathrm{id}_{\mathbb{R}}, \quad f\circ f^{-1} = \mathrm{id}_{\mathbb{R}},$$

a druhý již pak platí také. Pokud je $f$ definováno na podmnožině $A \subseteq \mathbb{R}$ a $f(A) = B$, je existence $f^{-1}$ podmíněna stejnými vztahy s identickými zobrazeními $\mathrm{id}_A$ resp. $\mathrm{id}_B$ na pravých stranách. Jak je vidět z obrázku, graf inverzní funkce prostě dostaneme záměnnou os závislé a nezávislé proměnné.



v bodě [2, ?]. Uveďte také všechny body, ve kterých je tečna rovnoběžná s osou $x$. ○

*5.90.* Pod jakým úhlem protíná graf funkce $y = \ln x$ osu $x$? (Úhlem protnutí rozumíme úhel tečny s kladnou poloosou $x$ v kladném smyslu otáčení.) ○

*5.91.* Určete rovnice tečny a normály ke křivce dané rovnicí

$$x^3 + y^3 - 2xy = 0$$

v bodě [1, 1]. ○

*5.92.* Dokažte, že platí

$$\tfrac{x}{1+x} < \ln(1+x) < x \quad \text{pro všechna } x > 0\,. \qquad ○$$

### F. Extremální úlohy

Jednoduché pozorování 5.32 o geometrickém významu derivace nám také říká, že extrémy diferencovatelné reálné funkce jedné reálné proměnné mohou nastat pouze v bodech, kde je derivace dané funkce nulová. Tohoto prostého faktu lze využít při řešení množství zajímavých praktických úloh.

**5.93.** Určete $x$-ovou souřadnici $x_A$ bodu paraboly $y = x^2$, který je nejblíže bodu $A = [1, 2]$.

**Řešení.** Není obtížné uvědomit si, že příklad má právě jedno řešení a že úkolem je vlastně najít absolutní minimum funkce

$$f(x) = \sqrt{(x-1)^2 + (x^2-2)^2}, \quad x \in \mathbb{R}.$$

Funkce $f$ má zjevně nejmenší hodnotu ve stejném bodě jako funkce

$$g(x) = (x-1)^2 + (x^2-2)^2, \quad x \in \mathbb{R}.$$

Neboť

$$g'(x) = 4x^3 - 6x - 2, \quad x \in \mathbb{R},$$

řešením rovnice $0 = 2x^3 - 3x - 1$ dostáváme nejprve stacionární bod $x = -1$ a po vydělení polynomu $2x^3 - 3x - 1$ polynomem $x + 1$ také zbývající dva stacionární body

$$\frac{1-\sqrt{3}}{2} \quad \text{a} \quad \frac{1+\sqrt{3}}{2}.$$

Protože funkce $g$ je polynomem (má derivaci na celé reálné ose), z geometrického významu úlohy již získáváme

$$x_A = \frac{1+\sqrt{3}}{2}\,. \qquad \square$$

**5.94.** Je dána elipsa $3x^2 + y^2 = 2$. Napište rovnici tečny, která vytíná v prvním kvadrantu trojúhelník o nejmenším obsahu a určete jeho velikost.

**Řešení.** Přímka zadaná rovnicí $ax + by + c = 0$ má s osami průsečíky $[-\frac{c}{a}, 0]$, $[0, -\frac{c}{b}]$ a obsah trojúhelníka s vrcholy v těchto bodech a

Pokud bychom věděli, že pro diferencovatelnou funkci $x = f(y)$ je i $y = f^{-1}(x)$ diferencovatelná, pravidlo pro derivaci složené funkce nám okamžitě říká

$$1 = (\mathrm{id})'(x) = \left(f \circ f^{-1}\right)'(x) = f'(y) \cdot \left(f^{-1}\right)'(x)$$

a tedy pak přímo dostáváme vzorec (zjevně $f'(y)$ v takovém případě nemůže být nulové).

DERIVACE INVERZNÍ FUNKCE

$$\left(f^{-1}\right)'(x) = \frac{1}{f'(y)} \tag{5.6}$$

To dobře odpovídá intuitivní představě, že pro $y = f(x)$ je přibližně $f' = \frac{\Delta y}{\Delta x}$ zatímco pro $x = f^{-1}(y)$ je to přibližně $\left(f^{-1}\right)'(y) = \frac{\Delta x}{\Delta y}$. Takto skutečně můžeme derivace inverzních funkcí počítat:

**Věta.** *Je-li $f$ reálná funkce diferencovatelná v bodě $y_0$ a v tomto bodě platí $f'(y_0) \neq 0$, pak existuje na nějakém okolí bodu $x_0 = f(y_0)$ funkce $f^{-1}$ inverzní k $f$, funkce $f^{-1}$ je diferencovatelná v bodě $x_0$ a platí vztah (5.6) v bodě $x_0$.*



DŮKAZ. Nejprve si povšimněme, že nenulovost derivace v $x_0$ znamená, že na nějakém okolí bodu $x_0$ je naše funkce $f$ buď rostoucí nebo klesající, viz důsledek 5.32. Proto na nějakém okolí nutně existuje inverzní funkce. Protože je obrazem ohraničeného uzavřeného intervalu ve spojité funkci opět uzavřený interval, nutně je také pro každou otevřenou množinu $U$ v definičním oboru $f$ i obraz $f(U)$ otevřený. Potom ale přímo z definice spojitosti pomocí okolí je tato inverzní funkce také spojitá.

Pro odvození našeho tvrzení nyní postačí pozorně znovu pročíst důkaz čtvrtého tvrzení věty 5.33. Jen volíme $f$ místo funkce $h$ a $f^{-1}$ místo $f$ a místo předpokladu existence derivací pro obě funkce víme, že funkce složená je diferencovatelná (a víme, že je to identická funkce): Skutečně, podle lemmatu 5.31 existuje funkce $\psi$ spojitá v bodě $y_0$ taková, že

$$f(y) - f(y_0) = \varphi(y)(y - y_0)$$

na nějakém okolí $y_0$. Navíc pro ni platí $\varphi(y_0) = f'(y_0)$. Pak ovšem po dosazení $y = f^{-1}(x)$ také platí

$$x - x_0 = \varphi\left(f^{-1}(x)\right)\left(f^{-1}(x) - f^{-1}(x_0)\right)$$

pro $x$ z nějakého okolí $\mathcal{O}(x_0)$ bodu $x_0$. Dále platí $f^{-1}(x_0) = y_0$, a protože je $f$ buď ostře rostoucí nebo klesající, je $\varphi(f^{-1}(x)) \neq 0$ pro všechny $x \in \mathcal{O}(x_0) \setminus \{x_0\}$. Můžeme tedy psát

$$\frac{f^{-1}(x) - f^{-1}(x_0)}{x - x_0} = \frac{1}{\varphi\left(f^{-1}(x)\right)} \neq 0$$

pro všechny $x \in \mathcal{O}(x_0)\setminus\{x_0\}$. Pravá strana tohoto výrazu je spojitá v bodě $x_0$ a limita je rovna

$$\frac{1}{\varphi\left(f^{-1}(x_0)\right)} = \frac{1}{f'(y_0)},$$

proto i limita levé strany existuje a je rovna témuž výrazu, tj. existuje

$$\left(f^{-1}\right)'(x_0) = \frac{1}{f'(y_0)}.$$

$\square$

v počátku je $S = \frac{c^2}{2ab}$. Rovnice tečny v bodě $[x_T, y_T]$ je $3xx_T + yy_T - 2 = 0$. Obsah trojúhelníka určený touto tečnou je tedy $S = \frac{2}{3x_T y_T}$. V prvním kvadrantu přitom máme $x_T, y_T > 0$. Minimalizovat tento obsah znamená maximalizovat součin $x_T y_T = x_T\sqrt{2 - 3x_T^2}$, což je v prvním kvadrantu to samé, jako maximalizovat $(x_T y_T)^2 = x_T^2(2 - 3x_T^2) = -3(x_T^2 - \frac{1}{3})^2 + \frac{1}{3}$. Hledané minimum obsahu je tedy v $x_T = \frac{1}{\sqrt{3}}$. Tečná má rovnici $\sqrt{3}x + y = 2$ a velikost tohoto obsahu je $S_{min} = \frac{2\sqrt{3}}{9}$. □

**5.95.** V čase $t = 0$ se začaly pohybovat tři body $P$, $Q$, $R$ v rovině a to bod $P$ z bodu $[-2, 1]$ směrem $(3, 1)$ rovnoměrnou rychlostí $\sqrt{10}$ m/s, bod $Q$ z bodu $[0, 0]$ směrem $(-1, 1)$ rovnoměrně zrychleným pohybem se zrychlením $2\sqrt{2}$ m/s$^2$ a bod $R$ z bodu $[0, 1]$ směrem $(1, 0)$ rovnoměrnou rychlostí 2 m/s. V jakém čase bude obsah trojúhelníku $PQR$ minimální?

**Řešení.** Rovnice bodů $P$, $Q$, $R$ v čase jsou

$$\begin{aligned} P &: [-2, 1] + (3, 1)t, \\ Q &: [0, 0] + (-1, 1)t^2, \\ R &: [0, 1] + (2, 0)t. \end{aligned}$$

Obsah trojúhelníka $PQR$ je určený např. polovinou absolutní hodnoty determinantu, jehož řádky jsou souřadnice vektorů $RP$ a $RQ$ (viz 1.34). Minimalizujeme tedy determinant:

$$\begin{vmatrix} -2 + t & t \\ -t^2 - 2t & -1 + t^2 \end{vmatrix} = 2t^3 - t + 2.$$

Derivace je $6t^2 - 1$, extrémy tedy nastávají pro $t = \pm\frac{1}{\sqrt{6}}$. Vzhledem k tomu, že uvažujeme pouze nezáporný čas, vyšetřujeme pouze $t = \frac{1}{\sqrt{6}}$. Druhá derivace uvažované funkce je v tomto bodě kladná, funkce obsahu zde tedy nabývá svého lokální minima. Navíc je její hodnota v tomto bodě kladná a menší, než hodnota v bodě 0 (krajní bod intervalu, na kterém hledáme extrém), jedná se tudíž o globální minimum obsahu v čase. □

**5.96.** V devět hodin ráno vylezl starý vlk z nory $N$ a v rámci ranní rozcvičky začal běhat proti směru hodinových ručiček po kružnici o poloměru 1km, kolem svého oblíbeného pařezu $P$ a to rovnoměrnou rychlostí 4 km/h. Ve stejnou dobu vyrazila Karkulka z domu $D$ k babičce sídlící v chaloupce $C$ rychlostí 4 km/h (po přímce). Kdy si budou nejblíž a jaká tato vzdálenost bude? Souřadnice (v kilometrech): $N = [2, 3]$, $P = [2, 2]$, $D = [0, 0]$, $C = [5, 5]$.

Vztah pro derivaci inverzní funkce platí i v případě, kdy je $f'(y_0) = 0$. Pak je derivace $(f^{-1})'(x_0)$ nevlastní, tj. $\pm\infty$, podle toho zda je $f$ rostoucí nebo klesající v bodě $y_0$.

**5.36. Derivace dalších funkcí.** Podívejme se konečně, jak je to s derivováním exponenciály $f(x) = a^x$. Pokud existuje derivace $a^x$ ve všech bodech $x$, bude jistě platit

$$f'(x) = \lim_{\Delta x \to 0} \frac{a^{x+\Delta x} - a^x}{\Delta x} = a^x \lim_{\Delta x \to 0} \frac{a^{\Delta x} - 1}{\Delta x} = f'(0)\, a^x.$$

Naopak, pokud existuje derivace v nule, pak tento výpočet ověřuje existenci derivace v kterémkoliv bodě a dává její hodnotu. Zároveň jsme ověřili platnost téhož vztahu pro derivace zprava a zleva.

Zanedlouho ověříme (viz 5.44, případně také 6.43), že derivace exponenciálních funkcí skutečně existují. Vyjděme teď ze (zatím nedokázaného) vztahu

$$\left(\mathrm{e}^x\right)' = \mathrm{e}^x$$

pro základ e, tzv. Eulerovo číslo.

Když tomuto vztahu uvěříme, okamžitě vidíme, že exponenciální funkce mají derivace úměrné hodnotám s konstantním koeficientem úměrnosti:

$$\left(a^x\right)' = \left(\mathrm{e}^{\ln(a)x}\right)' = \ln(a)\left(\mathrm{e}^{\ln(a)x}\right) = \ln(a) \cdot a^x.$$

Z definičního vztahu pro přirozený logaritmus

$$\mathrm{e}^{\ln x} = x$$

pak snadno spočteme:

$$(\ln)'(y) = (\ln)'\left(\mathrm{e}^x\right) = \frac{1}{(\mathrm{e}^x)'} = \frac{1}{\mathrm{e}^x} = \frac{1}{y}. \tag{5.7}$$

Pravidlo pro derivování obecné mocninné funkce

$$\left(x^a\right)' = ax^{a-1} \tag{5.8}$$

můžeme nyní snadno odvodit s pomocí vztahu pro derivaci exponenciální funkce a logaritmické funkce:

$$\left(x^a\right)' = \left(\mathrm{e}^{a \ln x}\right)' = \mathrm{e}^{a \ln x}(a \ln x)' = ax^{a-1}.$$

**5.37. Věty o střední hodnotě.** Než se pustíme do dalšího tématu na naší pouti za různorodými definicemi funkcí, odvodíme ještě několik jednoduchých výsledků o derivacích. Všechny jsou velice snadno intuitivně jasné z přiložených obrázků a důkazy vlastně jen rozepisují vizuální představu.

**Věta.** *Nechť funkce $f : \mathbb{R} \to \mathbb{R}$ je spojitá na konečném uzavřeném intervalu $[a, b]$ a diferencovatelná uvnitř tohoto intervalu. Jestliže platí $f(a) = f(b)$, pak existuje $c \in (a, b)$ takové, že $f'(c) = 0$.*

**Řešení.** Vlk se pohybuje po jednotkové kružnici, jeho úhlová rychlost je tedy stejná jako jeho absolutní rychlost a jeho dráhu můžeme v závislosti na čase popsat následujícími parametrickými rovnicemi:

$$x(t) = 2 - \cos(4t),\ \ y(t) = 2 - \sin(4t),$$

Karkulka se pak pohybuje po dráze

$$x(t) = 2\sqrt{2}t,\ \ y(t) = 2\sqrt{2}t.$$

Nalezněme extrémy (čtverce) vzdálenosti $\rho$ jejich drah v čase:

$$\begin{aligned}\rho(t) &= [2 - \cos(4t) - 2\sqrt{2}t]^2 + [2 - \sin(4t) - 2\sqrt{2}t]^2,\\ \rho'(t) &= 16(\cos(4t) - \sin(4t))(\sqrt{2}t - 1) + 32t + \\ &\quad + 4\sqrt{2}(\cos(4t) + \sin(4t)) - 16\sqrt{2}.\end{aligned}$$

Řešit algebraicky rovnici $\rho'(t) = 0$ se nám nepodaří (ani to nelze), zbývá pouze najít řešení numericky (pomocí výpočetního softwaru). Je jasné, že extrémů bude nekonečně mnoho: při každém kolečku je směr pohybu vlka v jistý časový okamžik rovnoběžný se směrem Karkulky, jejich vzdálenost se tedy po jistou dobu snižuje; Karkulka se však neustále vzdaluje konstantní rychlostí od středu kruhu, kolem kterého obíhá vlk. Zjistíme, že první lokální minimum nastává pro $t \doteq 0{,}31$ a poté pro $t \doteq 0{,}97$, kdy bude vzdálenost vlka a Karkulky asi 5 metrů. Je zřejmé, že půjde i o globální minimum.

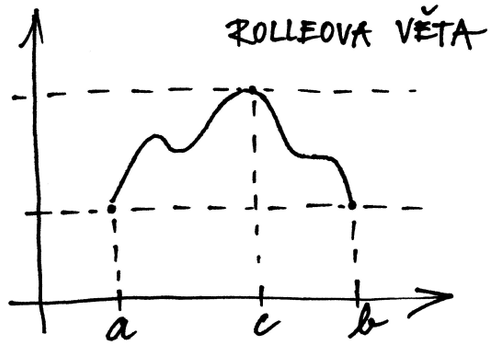
Situace, kdy neumíme explicitně vyřešit daný problém, je v praxi velmi častá a použití numerických metod výpočtu má velký význam. □

Další rozličné úlohy na hledání extrémů funkcí jedné proměnné viz strana 292.

**5.97.** Dokažte, že polynom $P(x) = x^5 - x^4 + 2x^3 - x^2 + x + 1$ má právě jeden reálný kořen.

**Řešení.** Libovolný polynom lichého stupně má alespoň jeden reálný kořen, neboť pro $x$ jdoucí k $-\infty$ jsou hodnoty polynomu velké (v absolutní hodnotě) záporné, pro velká kladná $x$ jsou hodoty polynomu velké kladné. Ze spojitosti polynomu tak tento musí mít reálný kořen. Také je možné argumentovat základní větou algeby (viz 11.20), neboť v oboru komplexních čísel má podle zmíněné věty daný polynom pět kořenů a protože komplexní kořeny polynomů s reálnými kořeny se vyskytují v komplexně sdružených dvojicích, musí být alespoň jeden kořen reálný.

Kdyby měl polynom alespoň dva reálné kořeny, řekněme $a, b$, pak by podle věty o střední hodnotě musela mít jeho derivace v nějakém bodě $c \in (a, b)$ hodnotu $P'(x) = 0$, avšak $P'(x) = 5x^4 - 4x^3 + 6x^2 - 2x + 1 = 2x^2(x-1)^2 + 3x^4 + 3x^2 + (x-1)^2 > 0$. Polynom má tedy právě jeden reálý kořen. □

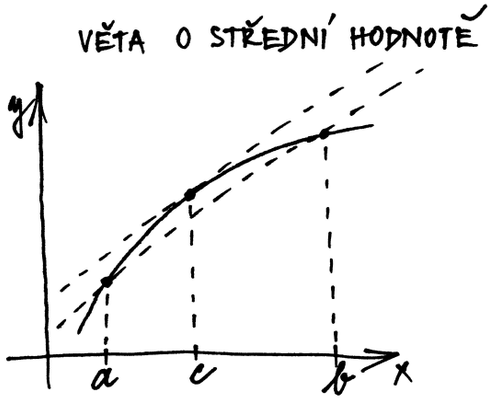



Důkaz. Protože je funkce $f$ spojitá na uzavřeném intervalu (tj. kompaktní množině), má na něm maximum a minimum. Pokud by maximum i minimum mělo stejnou hodnotu $f(a) = f(b)$, pak by funkce $f$ byla konstantní a tedy i její derivace by byla nulová ve všech bodech intervalu $(a, b)$. Předpokládejme tedy, že buď maximum nebo minimum je jiné. Pak ovšem nastává jedno z nich ve vnitřním bodě $c$. Kdyby platilo $f'(c) \neq 0$, pak by v tomto bodě byla byla funkce $f$ buď rostoucí nebo klesající (viz 5.32) a jistě by tedy v okolí bodu $c$ nabývala větších i menších hodnot, než je $f(c)$. Je tedy nutně $f'(c) = 0$. □

Právě dokázanému tvrzení se říká *Rolleova věta*. Z ní snadno vyplývá následující důsledek, známý jako *Lagrangeova věta o střední hodnotě.*

**5.38. Věta.** *Nechť funkce $f : \mathbb{R} \to \mathbb{R}$ je spojitá na intervalu $[a, b]$ a diferencovatelná uvnitř tohoto intervalu. Pak existuje $c \in (a, b)$ takové, že*

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$




Důkaz. Důkaz je prostým zápisem geometrického významu tvrzení: k sečně mezi body $[a, f(a)]$ a $[b, f(b)]$ existuje tečna, která je s ní rovnoběžná (podívejte se na obrázek). Rovnice naší sečny je



$$y = g(x) = f(a) + \frac{f(b) - f(a)}{b - a}(x - a).$$

Rozdíl $h(x) = f(x) - g(x)$ udává vzdálenost grafu od sečny (v hodnotách $y$). Jistě platí $h(a) = h(b)$ a

$$h'(x) = f'(x) - \frac{f(b) - f(a)}{b - a}.$$

Podle předchozí věty existuje bod $c$, ve kterém je $h'(c) = 0$. □

## G. L'Hospitalovo pravidlo

**5.98.** Ověřte, že je limita

(a)
$$\lim_{x\to 0}\frac{\sin(2x)-2\sin x}{2\mathrm{e}^x-x^2-2x-2}\quad \text{typu } \frac{0}{0};$$

(b)
$$\lim_{x\to 0+}\frac{\ln x}{\operatorname{cotg} x}\quad \text{typu } \frac{\infty}{\infty};$$

(c)
$$\lim_{x\to 1+}\left(\frac{x}{x-1}-\frac{1}{\ln x}\right)\quad \text{typu } \infty-\infty;$$

(d)
$$\lim_{x\to 1+}(\ln(x-1)\cdot\ln x)\quad \text{typu } 0\cdot\infty;$$

(e)
$$\lim_{x\to 0+}(\operatorname{cotg} x)^{\frac{1}{\ln x}}\quad \text{typu } \infty^0;$$

(f)
$$\lim_{x\to 0}\left(\frac{\sin x}{x}\right)^{\frac{1}{x^2}}\quad \text{typu } 1^\infty;$$

(g)
$$\lim_{x\to 1-}\left(\cos\frac{\pi x}{2}\right)^{\ln x}\quad \text{typu } 0^0.$$

Poté ji spočtěte užitím l'Hospitalova pravidla.

**Řešení.** Bezprostředně můžeme potvrdit, že je

(a)
$$\lim_{x\to 0}(\sin(2x)-2\sin x)=0-0=0,$$
$$\lim_{x\to 0}\left(2\mathrm{e}^x-x^2-2x-2\right)=2-0-0-2=0;$$

(b)
$$\lim_{x\to 0+}\ln x=-\infty,\qquad \lim_{x\to 0+}\operatorname{cotg} x=+\infty;$$

(c)
$$\lim_{x\to 1+}\frac{x}{x-1}=+\infty,\qquad \lim_{x\to 1+}\frac{1}{\ln x}=+\infty;$$

(d)
$$\lim_{x\to 1+}\ln x=0,\qquad \lim_{x\to 1+}\ln(x-1)=-\infty;$$

(e)
$$\lim_{x\to 0+}\operatorname{cotg} x=+\infty,\qquad \lim_{x\to 0+}\frac{1}{\ln x}=0;$$

(f)
$$\lim_{x\to 0}\frac{\sin x}{x}=1,\qquad \lim_{x\to 0}\frac{1}{x^2}=+\infty;$$

(g)
$$\lim_{x\to 1-}\cos\frac{\pi x}{2}=0,\qquad \lim_{x\to 1-}\ln x=0.$$

Větu o střední hodnotě můžeme také přepsat do tvaru:

$$f(b)=f(a)+f'(c)(b-a). \tag{5.9}$$

V případě parametricky zadané křivky v rovině, tj. dvojice funkcí $y=f(t)$, $x=g(t)$, je stejný výsledek o existenci rovnoběžné tečny k sečně krajními body popsán ve tvaru tzv. *Cauchyovy věty o střední hodnotě*:

**Důsledek.** *Nechť funkce $y=f(t)$ a $x=g(t)$ jsou spojité na intervalu $[a,b]$ a diferencovatelné uvnitř tohoto intervalu a $g'(t)\neq 0$ pro všechny $t\in(a,b)$. Pak existuje bod $c\in(a,b)$ takový, že platí*

$$\frac{f(b)-f(a)}{g(b)-g(a)}=\frac{f'(c)}{g'(c)}.$$

Důkaz. Opět spoléháme na použití Rolleovy věty. Položíme proto

$$h(t)=(f(b)-f(a))g(t)-(g(b)-g(a))f(t).$$

Nyní $h(a)=f(b)g(a)-f(a)g(b)$, $h(b)=f(b)g(a)-f(a)g(b)$, takže existuje $c\in(a,b)$ takový, že $h'(c)=0$. Protože je $g'(c)\neq 0$, dostáváme právě požadovaný vztah. □

Podobná úvaha jako v posledním tvrzení vede k mimořádně užitečnému nástroji pro počítání limit podílu funkcí. Tvrzení je znám jako *L'Hospitalovo pravidlo*:

**5.39. Věta.** *Předpokládejme, že $f$ a $g$ jsou funkce diferencovatelné v okolí bodu $x_0\in\mathbb{R}$, ne však nutně v bodě $x_0$ samotném, a nechť existují limity*

$$\lim_{x\to x_0}f(x)=0,\qquad \lim_{x\to x_0}g(x)=0.$$

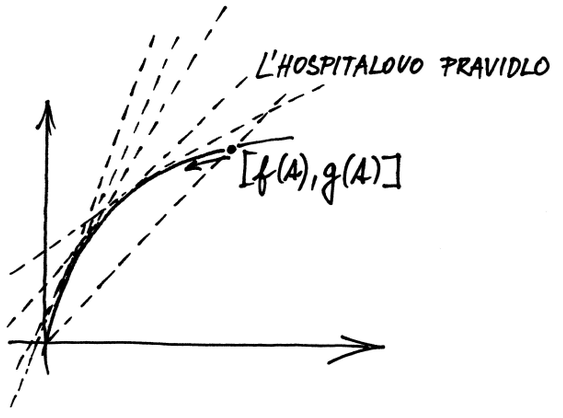
*Jestliže existuje limita*

$$\lim_{x\to x_0}\frac{f'(x)}{g'(x)},$$

*pak existuje i limita*

$$\lim_{x\to x_0}\frac{f(x)}{g(x)}$$

*a jsou si rovny.*




Důkaz. Bez újmy na obecnosti můžeme předpokládat, že v $x_0$ mají funkce $f$ a $g$ nulovou hodnotu.

Výsledek je opět jednoduše představitelný pomocí obrázku.



Uvažujme body $[g(x),f(x)]\in\mathbb{R}^2$ parametrizované proměnnou $x$. Podíl hodnot pak odpovídá směrnici sečny mezi body $[0,0]$ a $[f(x),g(x)]$. Zároveň víme, že podíl derivací odpovídá směrnici tečny v příslušném bodě.

Případ (a). Aplikování l'Hospitalova pravidla převádí limitu

$$\lim_{x\to 0}\frac{\sin(2x)-2\sin x}{2\mathrm{e}^x-x^2-2x-2}$$

na limitu

$$\lim_{x\to 0}\frac{2\cos(2x)-2\cos x}{2\mathrm{e}^x-2x-2},$$

která je ovšem typu 0/0. Dalšími dvěma aplikacemi l'Hospitalova pravidla dostáváme

$$\lim_{x\to 0}\frac{-4\sin(2x)+2\sin x}{2\mathrm{e}^x-2}$$

a (výše uvedená limita je opět typu 0/0)

$$\lim_{x\to 0}\frac{-8\cos(2x)+2\cos x}{2\mathrm{e}^x}=\frac{-8+2}{2}=-3.$$

Celkem tak máme (vrátíme se k původní limitě)

$$\lim_{x\to 0}\frac{\sin(2x)-2\sin x}{2\mathrm{e}^x-x^2-2x-2}=-3.$$

Dodejme, že opakované užití l'Hospitalova pravidla v jednom příkladu je běžné.

Nadále budeme klást, že se limity podílů derivací získané l'Hospitalovým pravidlem přímo rovnají původním limitám podílů. Takto si můžeme počínat, pokud obdržené limity na pravých stranách budou existovat, tj. o platnosti zápisů se vlastně budeme přesvědčovat dodatečně.

Případ (b). Tentokráte derivování čitatele a jmenovatele dává

$$\lim_{x\to 0+}\frac{\ln x}{\operatorname{cotg} x}=\lim_{x\to 0+}\frac{\frac{1}{x}}{\frac{-1}{\sin^2 x}}=\lim_{x\to 0+}\frac{-\sin^2 x}{x}.$$

Poslední limitu umíme snadno určit (dokonce ji známe). Z

$$\lim_{x\to 0+}-\sin x=0,\qquad \lim_{x\to 0+}\frac{\sin x}{x}=1$$

plyne výsledek $0=0\cdot 1$. Také jsme mohli znovu použít l'Hospitalovo pravidlo (nyní pro výraz 0/0) s výsledkem

$$\lim_{x\to 0+}\frac{-\sin^2 x}{x}=\lim_{x\to 0+}\frac{-2\cdot\sin x\cdot\cos x}{1}=\frac{-2\cdot 0\cdot 1}{1}=0.$$

Případ (c). Pouze převodem na společného jmenovatele

$$\lim_{x\to 1+}\left(\frac{x}{x-1}-\frac{1}{\ln x}\right)=\lim_{x\to 1+}\frac{x\ln x-(x-1)}{(x-1)\ln x}$$

jsme obdrželi typ 0/0. Je

$$\lim_{x\to 1+}\frac{x\ln x-(x-1)}{(x-1)\ln x}=\lim_{x\to 1+}\frac{\ln x+\frac{x}{x}-1}{\frac{x-1}{x}+\ln x}=\lim_{x\to 1+}\frac{\ln x}{1-\frac{1}{x}+\ln x}.$$

Máme podíl 0/0, pro který (opět dle l'Hospitalova pravidla) platí

$$\lim_{x\to 1+}\frac{\ln x}{1-\frac{1}{x}+\ln x}=\lim_{x\to 1+}\frac{\frac{1}{x}}{\frac{1}{x^2}+\frac{1}{x}}=\frac{1}{1+1}=\frac{1}{2}.$$

Návratem k původní limitě zapíšeme výsledek

$$\lim_{x\to 1+}\left(\frac{x}{x-1}-\frac{1}{\ln x}\right)=\frac{1}{2}.$$

Z existence limity směrnic tečen tedy chceme dovodit existenci limity směrnic sečen.

Technicky lze využít věty o střední hodnotě v parametrickém tvaru. Předně si uvědomme, že v tvrzení věty implicitně předpokládáme existenci výrazu $f'(x)/g'(x)$ na nějakém okolí $x_0$ (kromě bodu $x_0$ samotného), zejména tedy pro dostatečně blízké body $c$ k $x_0$ bude $g'(c)\neq 0$.[6] Díky větě o střední hodnotě nyní

$$\lim_{x\to x_0}\frac{f(x)}{g(x)}=\lim_{x\to x_0}\frac{f(x)-f(x_0)}{g(x)-g(x_0)}=\lim_{x\to x_0}\frac{f'(c_x)}{g'(c_x)},$$

kde $c_x$ je číslo mezi $x_0$ a $x$, závislé na $x$. Z existence limity

$$\lim_{x\to x_0}\frac{f'(x)}{g'(x)}$$

vyplývá, že stejnou hodnotu bude mít i limita libovolné posloupnosti vzniklé dosazením hodnot $x=x_n$ jdoucích k $x_0$ do $f'(x)/g'(x)$. Zejména tedy můžeme dosadit jakoukoliv posloupnost $c_{x_n}$ pro $x_n\to x_0$ a proto bude existovat i limita

$$\lim_{x\to x_0}\frac{f'(c_x)}{g'(c_x)}$$

a poslední dvě limity zjevně budou mít stejnou hodnotu. Dokázali jsme tedy, že naše hledaná limita existuje a má také stejnou hodnotu. □

Z důkazu věty je samozřejmé, že její tvrzení platí i pro jednostranné limity.

**5.40. Důsledky.** l'Hospitalovo pravidlo můžeme jednoduše rozšířit i pro limity v nevlastních bodech $\pm\infty$ a pro případ nevlastních hodnot limit. Je-li, např.

$$\lim_{x\to\infty}f(x)=0,\qquad \lim_{x\to\infty}g(x)=0,$$

potom je $\lim_{x\to 0_+}f(1/x)=0$ a $\lim_{x\to 0_+}g(1/x)=0$.

Zároveň z existence limity podílu derivací v nekonečnu dostaneme

$$\lim_{x\to 0_+}\frac{(f(1/x))'}{(g(1/x))'}=\lim_{x\to 0_+}\frac{f'(1/x)(-1/x^2)}{g'(1/x)\left(-1/x^2\right)}=$$
$$=\lim_{x\to 0_+}\frac{f'(1/x)}{g'(1/x)}=\lim_{x\to\infty}\frac{f'(x)}{g'(x)}.$$

Použitím předchozí věty tedy dostáváme, že v tomto případě bude existovat i limita podílu

$$\lim_{x\to\infty}\frac{f(x)}{g(x)}=\lim_{x\to 0_+}\frac{f(1/x)}{g(1/x)}=\lim_{x\to\infty}\frac{f'(x)}{g'(x)}.$$

Ještě jednodušší je postup při výpočtu limity v případě, kdy

$$\lim_{x\to x_0}f(x)=\pm\infty,\qquad \lim_{x\to x_0}g(x)=\pm\infty.$$

Stačí totiž psát

$$\lim_{x\to x_0}\frac{f(x)}{g(x)}=\lim_{x\to x_0}\frac{1/g(x)}{1/f(x)},$$

což je již případ pro použití l'Hospitalova pravidla z předchozí věty. Lze ale i dokázat, že l'Hospitalovo pravidlo platí ve stejné formě pro nevlastní limity:

[6] Pro samu existenci limity v obecném smyslu to vždy nutné není, nicméně pro tvrzení L'Hospitalovy věty je to potřebné. Podrobnou diskusi je možné najít (vygooglovat) v populárním článku 'R. P. Boas, Counterexamples to L'Hôpital's Rule, The American Mathematical Monthly, October 1986, Volume 93, Number 8, pp. 644–645.'

Případ (d). Uvedený výraz převedeme na typ $\infty/\infty$ (přesněji řečeno, na typ $-\infty/\infty$) vytvořením zlomku

$$\lim_{x\to 1+} \ln(x-1)\cdot\ln x = \lim_{x\to 1+} \frac{\ln(x-1)}{\frac{1}{\ln x}}.$$

Podle l'Hospitalova pravidla je

$$\lim_{x\to 1+} \frac{\ln(x-1)}{\frac{1}{\ln x}} = \lim_{x\to 1+} \frac{\frac{1}{x-1}}{-\frac{1}{\ln^2 x}\cdot\frac{1}{x}} = \lim_{x\to 1+} \frac{-x\ln^2 x}{x-1}.$$

Pro tento neurčitý výraz (typu 0/0) lze pokračovat l'Hospitalovým pravidlem a stanovit

$$\lim_{x\to 1+} \frac{-x\ln^2 x}{x-1} = \lim_{x\to 1+} \frac{-\ln^2 x - 2x\ln x\cdot\frac{1}{x}}{1} = -\frac{0+0}{1} = 0.$$

Případy (e), (f), (g). Protože

$$\lim_{x\to 0+} (\operatorname{cotg} x)^{\frac{1}{\ln x}} = \mathrm{e}^{\lim\limits_{x\to 0+} \frac{\ln(\operatorname{cotg} x)}{\ln x}};$$

$$\lim_{x\to 0} \left(\frac{\sin x}{x}\right)^{\frac{1}{x^2}} = \mathrm{e}^{\lim\limits_{x\to 0} \frac{\ln\frac{\sin x}{x}}{x^2}};$$

$$\lim_{x\to 1-} \left(\cos\frac{\pi x}{2}\right)^{\ln x} = \mathrm{e}^{\lim\limits_{x\to 1-} \left(\ln x\cdot\ln\left(\cos\frac{\pi x}{2}\right)\right)},$$

postačuje vypočítat limity uvedené v argumentu exponenciální funkce. Pomocí l'Hospitalova pravidla a jednoduchých úprav získáváme

$$\begin{aligned}
\lim_{x\to 0+} \frac{\ln(\operatorname{cotg} x)}{\ln x}\left[\text{typ } \frac{+\infty}{-\infty}\right] &= \lim_{x\to 0+} \frac{\frac{1}{\operatorname{cotg} x}\cdot\frac{-1}{\sin^2 x}}{\frac{1}{x}} = \\
&= \lim_{x\to 0+} \frac{-x}{\cos x\cdot\sin x}\left[\text{typ } \frac{0}{0}\right] = \\
&= \lim_{x\to 0+} \frac{-1}{\cos^2 x - \sin^2 x} = \\
&= \frac{-1}{1-0} = -1;
\end{aligned}$$

$$\begin{aligned}
\lim_{x\to 0} \frac{\ln\frac{\sin x}{x}}{x^2}\left[\text{typ } \frac{0}{0}\right] &= \lim_{x\to 0} \frac{\frac{x}{\sin x}\cdot\frac{x\cos x-\sin x}{x^2}}{2x} = \\
&= \lim_{x\to 0} \frac{x\cos x - \sin x}{2x^2\sin x}\left[\text{typ } \frac{0}{0}\right] = \\
&= \lim_{x\to 0} \frac{\cos x - x\sin x - \cos x}{4x\sin x + 2x^2\cos x} = \\
&= \lim_{x\to 0} \frac{-\sin x}{4\sin x + 2x\cos x}\left[\text{typ } \frac{0}{0}\right] = \\
&= \lim_{x\to 0} \frac{-\cos x}{4\cos x + 2\cos x - 2x\sin x} = \\
&= \frac{-1}{4+2-0} = -\frac{1}{6},
\end{aligned}$$

a tudíž

$$\lim_{x\to 0+} (\operatorname{cotg} x)^{\frac{1}{\ln x}} = \mathrm{e}^{-1} = \frac{1}{\mathrm{e}};$$

$$\lim_{x\to 0} \left(\frac{\sin x}{x}\right)^{\frac{1}{x^2}} = \mathrm{e}^{-\frac{1}{6}} = \frac{1}{\sqrt[6]{\mathrm{e}}}.$$

**Věta.** *Nechť $f$ a $g$ jsou funkce diferencovatelné v okolí bodu $x_0 \in \mathbb{R}$, ne však nutně v bodě $x_0$ samotném, a nechť existují limity $\lim_{x\to x_0} f(x) = \pm\infty$ a $\lim_{x\to x_0} g(x) = \pm\infty$. Jestliže existuje limita*

$$\lim_{x\to x_0} \frac{f'(x)}{g'(x)},$$

*pak existuje i limita*

$$\lim_{x\to x_0} \frac{f(x)}{g(x)}$$

*a jsou si rovny.*

Důkaz. Opět lze vyjít z věty o střední hodnotě. Základem je vyjádření podílu tak, abychom dostali do hry derivaci:

$$\frac{f(x)}{g(x)} = \frac{f(x)}{f(x)-f(y)}\cdot\frac{f(x)-f(y)}{g(x)-g(y)}\cdot\frac{g(x)-g(y)}{g(x)},$$

kde za $y$ volíme nějaký pevný bod ze zvoleného okolí $x_0$ a $x$ necháme blížit k $x_0$. Protože jsou limity $f$ i $g$ v $x_0$ nekonečné, můžeme jistě předpokládat, že rozdíly hodnot v $x$ a $y$ jsou u obou funkcí při pevném $y$ nenulové.

Pomocí věty o střední hodnotě můžeme nyní nahradit prostřední zlomek podílem derivací ve vhodném bodě $c$ mezi $x$ a $y$ a výraz ve zkoumané limitě dostává tvar

$$\frac{f(x)}{g(x)} = \frac{1-\frac{g(y)}{g(x)}}{1-\frac{f(y)}{f(x)}}\cdot\frac{f'(c)}{g'(c)},$$

kde $c$ závisí na $x$ i $y$. Při pevném $y$ a $x$ jdoucím k $x_0$ jde první zlomek zjevně k jedničce. Když zároveň budeme $y$ přibližovat k $x_0$, bude se nám druhý zlomek libovolně přesně blížit k limitní hodnotě podílu derivací. □

**5.41. Příklad použití.** Vhodnými úpravami sledovaných výrazů lze využít L'Hospitalova pravidla také na výrazy typu $\infty-\infty$, $1^\infty$, $0\cdot\infty$ apod. Zpravidla jde o prosté přepsání výrazů nebo o využití nějaké hladké funkce, např. exponenciální.

Ukážeme si pro ilustraci takového postupu souvislost aritmetického a geometrického průměru z $n$ nezáporných hodnot $x_i$. *Aritmetický průměr*

$$M^1(x_1,\ldots,x_n) = \frac{x_1+\cdots+x_n}{n}$$

je speciálním případem tzv. *mocninného průměru stupně r*:

$$M^r(x_1,\ldots,x_n) = \left(\frac{x_1^r+\cdots+x_n^r}{n}\right)^{\frac{1}{r}}.$$

Speciální hodnota $M^{-1}$ se nazývá *harmonický průměr*. Spočtěme si nyní limitní hodnotu $M^r$ pro $r$ jdoucí k nule. Za tímto účelem spočteme limitu pomocí L'Hospitalova pravidla (jde o výraz 0/0 a derivujeme podle $r$, zatímco $x_i$ jsou při výpočtu konstantní parametry).

Následující výpočet, ve kterém užíváme pravidla pro derivování složených funkcí a znalosti hodnot derivace mocninné funkce, musíme číst odzadu. Z existence poslední limity plyne existence

Obdobně lze postupovat při určování poslední limity. Platí

$$\lim_{x\to 1-}(\ln x)\cdot\ln\left(\cos\frac{\pi x}{2}\right)=\lim_{x\to 1-}\frac{\ln\left(\cos\frac{\pi x}{2}\right)}{\frac{1}{\ln x}}\left[\text{typ }\frac{-\infty}{-\infty}=\frac{\infty}{\infty}\right]=$$
$$=\lim_{x\to 1-}\frac{\frac{1}{\cos\frac{\pi x}{2}}\left(-\sin\frac{\pi x}{2}\right)\frac{\pi}{2}}{-\frac{1}{\ln^2 x}\cdot\frac{1}{x}}=$$
$$=\frac{\pi}{2}\lim_{x\to 1-}\frac{x\sin\frac{\pi x}{2}\cdot\ln^2 x}{\cos\frac{\pi x}{2}}.$$

Neboť je tento výraz typu 0/0, mohli bychom pokračovat k součinu limit

$$\lim_{x\to 1-}\left(x\sin\frac{\pi x}{2}\right)\cdot\lim_{x\to 1-}\frac{\ln^2 x}{\cos\frac{\pi x}{2}}=1\cdot\lim_{x\to 1-}\frac{\ln^2 x}{\cos\frac{\pi x}{2}}.$$

Teprve nyní aplikujeme l'Hospitalovo pravidlo pro

$$\lim_{x\to 1-}\frac{\ln^2 x}{\cos\frac{\pi x}{2}}\left[\text{typ }\frac{0}{0}\right]=\lim_{x\to 1-}\frac{2\ln x\cdot\frac{1}{x}}{\left(-\frac{\pi}{2}\right)\sin\frac{\pi x}{2}}=\frac{0}{-\frac{\pi}{2}}=0.$$

Celkem máme

$$\lim_{x\to 1-}\left(\ln x\cdot\ln\left(\cos\frac{\pi x}{2}\right)\right)=\frac{\pi}{2}\cdot 1\cdot 0=0,$$

tj.

$$\lim_{x\to 1-}\left(\cos\frac{\pi x}{2}\right)^{\ln x}=\mathrm{e}^0=1\,.$$ □

**5.99.** Jak jsme již implicitně zmínili, použití l'Hospitalova pravidla může vést k limitě, která neexistuje, ačkoliv původní limita existuje: určete limitu

$$\lim_{x\to\infty}\frac{x+\sin x}{x}.$$

**Řešení.** Limita je typu $\frac{\infty}{\infty}$, použitím l'Hospitalova pravidla dostáváme

$$\lim_{x\to\infty}\frac{x+\sin x}{x}=\lim_{x\to\infty}\frac{1+\cos x}{1},$$

a protože neexistuje limita $\lim_{x\to\infty}\cos x$, neexistuje ani limita $\lim_{x\to\infty}1+\cos x$. Původní limita ovšem existuje, je totiž

$$\frac{x-1}{x}\le\frac{x+\sin x}{x}\le\frac{x+1}{x},$$

a podle věty o třech limitách je

$1=\lim_{x\to\infty}\frac{x-1}{x}\le\lim_{x\to\infty}\frac{x+\sin x}{x}\le\lim_{x\to\infty}\frac{x+1}{x}=1\,.$ □

**5.100.** Určete

$$\lim_{x\to+\infty}\frac{\ln x}{x},\qquad\lim_{x\to 0+}x\ln\frac{1}{x},\qquad\lim_{x\to 0+}x\,\mathrm{e}^{\frac{1}{x}};$$

$$\lim_{x\to 0-}x\,\mathrm{e}^{-\frac{1}{x}},\qquad\lim_{x\to 0}\frac{\mathrm{e}^{-\frac{1}{x^2}}}{x^{100}},\qquad\lim_{x\to+\infty}(\ln x-x)\,;$$

$$\lim_{x\to+\infty}\frac{x}{x+\ln x\cdot\cos x},\qquad\lim_{x\to+\infty}\frac{\sqrt[3]{x+1}}{\sqrt[5]{x+3}},\qquad\lim_{x\to+\infty}\frac{x}{\sqrt{x^2+1}}.$$

předposlední a její hodnota atd.

$$\lim_{r\to 0}\ln\left(M^r(x_1,\dots,x_n)\right)=\lim_{r\to 0}\frac{\ln\left(\frac{1}{n}\left(x_1^r+\cdots+x_n^r\right)\right)}{r}=$$
$$=\lim_{r\to 0}\frac{\frac{x_1^r\ln x_1+\cdots+x_n^r\ln x_n}{n}}{\frac{x_1^r+\cdots+x_n^r}{n}}=$$
$$=\frac{\ln x_1+\cdots+\ln x_n}{n}=$$
$$=\ln\sqrt[n]{x_1\cdot\dots\cdot x_n}.$$

Odtud tedy je přímo vidět, že

$$\lim_{r\to 0}M^r(x_1,\dots,x_n)=\sqrt[n]{x_1\dots x_n},$$

což je hodnota známá pod názvem *geometrický průměr.*

### 4. Mocninné řady

**5.42. Jak se počítá $\mathrm{e}^x$.** Kromě sčítání a násobení už umíme také počítat s limitami posloupností. Podbízí se proto přibližovat nepolynomiální funkce pomocí posloupností spočítatelných hodnot.



Když se takto podíváme na funkci $\mathrm{e}^x$, hledáme vlastně funkci, jejíž okamžitý přírůstek je v každém bodě roven hodnotě této funkce. To si můžeme dobře představit jako úžasné úročení vkladu se sazbou rovnou okamžité hodnotě. Když budeme roční sazbu úroku realizovat jednou za měsíc, za den, za hodinu atd., budeme pro výnos vkladu $x$ po jednom roce dostávat výsledné hodnoty

$$\left(1+\frac{x}{12}\right)^{12},\quad\left(1+\frac{x}{365}\right)^{365},\quad\left(1+\frac{x}{8760}\right)^{8760},\quad\dots$$

Dalo by se tedy tušit, že bude platit:

$$\mathrm{e}^x=\lim_{n\to\infty}\left(1+\frac{x}{n}\right)^n.$$

Zároveň tušíme, že čím jemněji budeme postupovat při úročení, tím vyšší bude výnos, takže by posloupnost čísel na pravé straně měla být rostoucí.

Podívejme se tedy podrobně na číselnou posloupnost

$$a_n=\left(1+\frac{1}{n}\right)^n,$$

jejíž limita má být Eulerovo číslo e.

Bude se nám přitom hodit velice užitečná *Bernoulliova nerovnost*:

**Lemma.** *Pro každé reálné číslo $b\ge-1$, $b\ne 0$, a přirozené $n\ge 2$ platí $(1+b)^n>1+nb$.*

Důkaz. Pro $n=2$ dostáváme

$$(1+b)^2=1+2b+b^2>1+2b.$$

Dále postupujeme indukcí za předpokladu $b>-1$. Předpokládejme, že tvrzení platí pro nějaké $k\ge 2$ a počítejme

$$(1+b)^{k+1}=(1+b)^k(1+b)>(1+kb)(1+b)=$$
$$=1+(k+1)b+kb^2>1+(k+1)b.$$

Tvrzení zřejmě platí také pro $b=-1$. □

**Řešení.** Snadno lze zjistit (např. $n$-násobným užitím l'Hospitalova pravidla), že pro libovolné $n \in \mathbb{N}$ je

$$\lim_{x\to+\infty} \frac{x^n}{\mathrm{e}^x} = 0, \quad \text{tj.} \quad \lim_{x\to+\infty} \frac{\mathrm{e}^x}{x^n} = +\infty.$$

Z Věty o třech limitách potom pro reálná čísla $a > 0$ ihned plyne zobecnění

$$\lim_{x\to+\infty} \frac{x^a}{\mathrm{e}^x} = 0, \quad \text{tj.} \quad \lim_{x\to+\infty} \frac{\mathrm{e}^x}{x^a} = +\infty.$$

Uvážíme-li, že grafy funkcí $y = \mathrm{e}^x$ a $y = \ln x$ (inverzní funkce k $y = \mathrm{e}^x$) jsou symetrické vzhledem k přímce $y = x$, víme dále

$$\lim_{x\to+\infty} \frac{\ln x}{x} = 0, \quad \text{tj.} \quad \lim_{x\to+\infty} \frac{x}{\ln x} = +\infty.$$

Získali jsme tak první výsledek. Ten přitom dává rovněž l'Hospitalovo pravidlo, podle kterého je

$$\lim_{x\to+\infty} \frac{\ln x}{x} = \lim_{x\to+\infty} \frac{\frac{1}{x}}{1} = \lim_{x\to+\infty} \frac{1}{x} = 0.$$

Upozorněme, že l'Hospitalovo pravidlo lze použít k vyčíslení každé z dalších pěti uvedených limit. Je ovšem možné určit tyto limity jednoduššími způsoby. Např. substituce $y = 1/x$ vede na

$$\lim_{x\to0+} x \ln\frac{1}{x} = \lim_{y\to+\infty} \frac{\ln y}{y} = 0;$$
$$\lim_{x\to0+} x\,\mathrm{e}^{\frac{1}{x}} = \lim_{y\to+\infty} \frac{\mathrm{e}^y}{y} = +\infty.$$

Samozřejmě $x \to 0+$ dává $y = 1/x \to +\infty$ (píšeme $1/+0 = +\infty$).

Pomocí substitucí $u = -1/x$, $v = 1/x^2$ po řadě dostáváme

$$\lim_{x\to0-} x\,\mathrm{e}^{-\frac{1}{x}} = \lim_{u\to+\infty} -\frac{\mathrm{e}^u}{u} = -\infty;$$
$$\lim_{x\to0} \frac{\mathrm{e}^{-\frac{1}{x^2}}}{x^{100}} = \lim_{v\to+\infty} \frac{v^{50}}{\mathrm{e}^v} = 0,$$

přičemž $x \to 0-$ odpovídá $u = -1/x \to +\infty$ (píšeme $-1/-0 = +\infty$) a $x \to 0$ potom $v = 1/x^2 \to +\infty$ (znovu $1/+0 = +\infty$). Již dříve jsme také objasnili, že platí

$$\lim_{x\to+\infty} (\ln x - x) = \lim_{x\to+\infty} -x = -\infty.$$

Případné pochyby snad rozptýlí limita

$$\lim_{x\to+\infty} \frac{\ln x - x}{\ln x} = \lim_{x\to+\infty} \left(1 - \frac{x}{\ln x}\right) = -\infty,$$

která dokazuje, že při zmenšení absolutní hodnoty uvažovaného výrazu (aniž by došlo ke změně znaménka) stále výraz v absolutní hodnotě roste nade všechny meze.

Pro dva po sobě jdoucí členy $a_n$ naší posloupnosti můžeme nyní s využitím Bernoulliovy nerovnosti odhadnout jejich podíl

$$\frac{a_n}{a_{n-1}} = \frac{\left(1+\frac{1}{n}\right)^n}{\left(1+\frac{1}{n-1}\right)^{n-1}} = \frac{\left(\frac{n+1}{n}\right)^n}{\left(\frac{n}{n-1}\right)^{n-1}} = \frac{\left(n^2-1\right)^n n}{n^{2n}(n-1)} =$$
$$= \left(1-\frac{1}{n^2}\right)^n \frac{n}{n-1} > \left(1-\frac{1}{n}\right)\frac{n}{n-1} = 1.$$

Je tedy naše posloupnost skutečně rostoucí.

Následující obdobný výpočet (opět s využitím Bernoulliovy nerovnosti) ověřuje, že posloupnost čísel

$$b_n = \left(1+\frac{1}{n}\right)^{n+1} = \left(1+\frac{1}{n}\right)\left(1+\frac{1}{n}\right)^n$$

je klesající a jistě je $b_n > a_n$.

$$\frac{b_n}{b_{n+1}} = \frac{n}{n+1}\left(\frac{\frac{n+1}{n}}{\frac{n+2}{n+1}}\right)^{n+2} = \frac{n}{n+1}\left(\frac{n^2+2n+1}{n^2+2n}\right)^{n+2} =$$
$$= \frac{n}{n+1}\left(1+\frac{1}{n(n+2)}\right)^{n+2} >$$
$$> \frac{n}{n+1}\left(1+\frac{n+2}{n(n+2)}\right) = 1.$$

Posloupnost $a_n$ je tedy shora ohraničená a rostoucí, a proto je její limita dána jejím supremem. Zároveň vidíme, že je tato limita rovna také limitě klesající posloupnosti $b_n$, protože

$$\lim_{n\to\infty} b_n = \lim_{n\to\infty} \left(1+\frac{1}{n}\right) a_n = \lim_{n\to\infty} a_n.$$

Tato limita proto zadává jedno z nejdůležitějších čísel v matematice (vedle nuly, jedničky a Ludolfova čísla $\pi$), *Eulerovo číslo* e. Je tedy

$$\mathrm{e} = \lim_{n\to\infty} \left(1+\frac{1}{n}\right)^n.$$

**5.43. Mocninná řada pro $\mathrm{e}^x$.** Exponenciální funkci jsme definovali jako jedinou spojitou funkci splňující $f(1) = \mathrm{e}$ a $f(x+y) = f(x)\cdot f(y)$. Základ e máme vyjádřen jako limitu posloupnosti čísel $a_n$, nutně tedy je, pro každé pevné reálné číslo $x$,



$$\mathrm{e}^x = \lim_{n\to\infty} (a_n)^x.$$

Počítejme nyní pro jednoduchost s pevně zvoleným kladným $x$. Jestliže v hodnotách $a_n$ z minulého odstavce zaměníme $n$ za $n/x$, opět dostaneme stejnou limitu (rozmyslete si podrobně), a proto také

$$\mathrm{e} = \lim_{n\to\infty} \left(1+\frac{x}{n}\right)^{\frac{n}{x}}, \quad \mathrm{e}^x = \lim_{n\to\infty} \left(1+\frac{x}{n}\right)^n.$$

Stejně snadno umíme určit

$$\lim_{x\to+\infty}\frac{x}{x+\ln x\cdot\cos x}=\lim_{x\to+\infty}\frac{x}{x}=1;$$
$$\lim_{x\to+\infty}\frac{\sqrt[3]{x+1}}{\sqrt[5]{x+3}}=\lim_{x\to+\infty}\frac{\sqrt[3]{x}}{\sqrt[5]{x}}=+\infty;$$
$$\lim_{x\to+\infty}\frac{x}{\sqrt{x^2+1}}=\lim_{x\to+\infty}\frac{x}{\sqrt{x^2}}=1.$$

Viděli jsme, že l'Hospitalovo pravidlo nemusí být nejlepší metodou výpočtu limity jednoho z typů $0/0, \infty/\infty$. Na předchozích třech příkladech lze ilustrovat, že jej ani nelze vždy (pro neurčité výrazy) aplikovat. Kdybychom jej použili k řešení prvního z nich, obdrželi bychom pro $x>0$ podíl

$$\frac{1}{1+\frac{\cos x}{x}-\ln x\cdot\sin x}=\frac{x}{x+\cos x-x\ln x\cdot\sin x},$$

který je složitější než původní. Dokonce pro $x\to+\infty$ limitu nemá. Není tedy splněn jeden z předpokladů l'Hospitalova pravidla. Ve druhém případě pak (libovolný počet opakovaných) použití l'Hospitalova pravidla vede na neurčité výrazy. Pro poslední limitu nás l'Hospitalovo pravidlo vrátí do zadání: dává nejdříve zlomek

$$\frac{1}{\frac{2x}{2\sqrt{x^2+1}}}=\frac{\sqrt{x^2+1}}{x}$$

a následně

$$\frac{\frac{2x}{2\sqrt{x^2+1}}}{1}=\frac{x}{\sqrt{x^2+1}}.$$

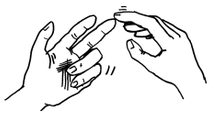
Odsud můžeme odvodit, že limita je rovna 1 (hledáme nezápornou hodnotu $a\in\mathbb{R}$ takovou, aby platilo $a=a^{-1}$), pouze když dříve dokážeme, že vůbec existuje. □

Další příklady na výpočet limit užitím L'Hospitalova pravidla naleznete na straně 310.

### H. Nekonečné řady

Nekonečné řady se přirozeně vyskytují v celé řadě (problémů).

**5.101. Sierpińského koberec.** Jednotkový čtverec se rozdělí na devět shodných čtverců a odstraní se prostřední čtverec. Každý ze zbývajících čtverců se znovu rozdělí na devět shodných čtverců a v každém z nich se odstraní prostřední čtverec. Určete obsah zbylého obrazce po prodloužení tohoto postupu do nekonečna.



**Řešení.** V prvním kroku se odstraní 1 čtverec o obsahu 1/9. Ve druhém kroku se odstraní 8 čtverců o obsahu $9^{-2}$, tj. o celkovém obsahu $8\cdot9^{-2}$. V každé další iteraci se odstraní osminásobek počtu čtverců

Označme $n$-tý člen této posloupnosti $u_n(x)=(1+x/n)^n$ a vyjádřeme jej pomocí binomické věty:

$$\begin{aligned}u_n(x)&=1+n\frac{x}{n}+\frac{n(n-1)x^2}{2!n^2}+\cdots+\frac{n!x^n}{n!n^n}=\\&=1+x+\frac{x^2}{2!}\left(1-\frac{1}{n}\right)+\\&\quad+\frac{x^3}{3!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)+\cdots+\\&\quad+\frac{x^n}{n!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\cdots\left(1-\frac{n-1}{n}\right).\end{aligned}\tag{5.10}$$

Protože jsou všechny závorky v součinech menší než jedna, dostáváme také

$$u_n(x)<v_n(x)=\sum_{j=0}^{n}\frac{1}{j!}x^j.$$

Pokud se přitom budeme dívat na $u_n$ pro hodně veliká $n$, budou první sčítance těchto výrazů hodně blízké hodnotám $\frac{1}{k!}x^k$. Skutečně pro všechna $x$ platí následující věta.

MOCNINNÁ ŘADA PRO $\mathrm{e}^x$

**5.44. Věta.** *Exponenciální funkce* $\mathrm{e}^x$ *je pro každé* $x\in\mathbb{R}$ *vyjádřena jako limita částečných součtů* $\lim_{k\to\infty}v_k$ *ve výrazu*

$$\mathrm{e}^x=1+x+\frac{1}{2!}x^2+\cdots+\frac{1}{n!}x^n+\cdots=\sum_{n=0}^{\infty}\frac{1}{n!}x^n.$$

*Funkce* $\mathrm{e}^x$ *je diferencovatelná a platí* $(\mathrm{e}^x)'=\mathrm{e}^x$.

DŮKAZ. Technický důkaz věty je pouze rozpracováním výše uvedené úvahy. Nejprve ukážeme, že formální nekonečný součet má, jakožto limita částečných součtů $v_n$, skutečně smysl, a pak dalším jemným odhadem ukážeme, že skutečně dává požadovanou hodnotu hodnotu $\lim_{n\to\infty}u_n$.

Uvažme tedy formální nekonečný součet

$$\sum_{j=0}^{\infty}c_j=\sum_{j=0}^{\infty}\frac{1}{j!}x^j,\tag{5.11}$$

ve kterém je $v_n(x)$ právě součet prvních $n$ členů.

Podíl dvou po sobě jdoucích členů v řadě je $c_{j+1}/c_j=x/(n+1)$. Pro každé pevné $x$ tedy existuje $N\in\mathbb{N}$ takové, že $c_{j+1}/c_j<1/2$ pro všechny $j\geq N$. Pro takto velká $j$ je ovšem $c_{j+1}<\frac{1}{2}c_j<2^{-(j-N+1)}c_N$. To ale znamená, že částečné součty prvních $n$ členů v našem formálním součtu jsou shora ohraničeny součty

$$v_n<\sum_{j=0}^{N-1}\frac{1}{j!}x^j+\frac{1}{N!}x^N\sum_{j=0}^{n-N}\frac{1}{2^j}.$$

Protože pro každé $q$ platí $(1-q)\left(1+q+\cdots+q^k\right)=1-q^{k+1}$, můžeme hodnoty $v_n$ také odhadnout

$$v_n<\sum_{j=0}^{N-1}\frac{1}{j!}x^j+\frac{2}{N!}x^N\left(1-2^{-n+N-1}\right).$$

Limita výrazů na pravé straně pro $n$ jdoucí do nekonečna proto jistě existuje a tedy existuje i limita rostoucí posloupnosti $v_n$.

z předešlého kroku, přičemž obsah každého z nich je devítinou obsahu jednoho čtverce z předchozího kroku. Součet obsahů všech odstraněných čtverců je

$$\frac{1}{9}+\frac{8}{9^2}+\frac{8^2}{9^3}+\cdots=\sum_{n=0}^{\infty}\frac{8^n}{9^{n+1}}.$$

Obsah zbylého obrazce (tzv. Sierpińského koberce) tak činí

$$1-\sum_{n=0}^{\infty}\frac{8^n}{9^{n+1}}=1-\frac{1}{9}\sum_{n=0}^{\infty}\left(\frac{8}{9}\right)^n=1-\frac{1}{9}\cdot\frac{1}{1-\frac{8}{9}}=0\,. \qquad \square$$

**5.102. Kochova vločka, 1904.** Vytvořte „sněhovou vločku“ následujícím postupem. Na začátku uvažujte rovnostranný trojúhelník s jednotkovou délkou strany. Každou z jeho stran rozdělte na třetiny a nad prostředními třetinami sestrojte rovnostranné trojúhelníky, kdy základny (prostřední třetiny stran původního trojúhelníku) odstraníte. Takto z původního trojúhelníku dostanete šesticípou hvězdu. Celý postup opakujte tak, že každou úsečku obdrženou v předchozím kroku rozdělíte na třetiny a prostřední třetinu nahradíte za rovnostranný trojúhelník bez základny. Sněhovou vločku pak získáte nekonečným opakováním tohoto postupu. Dokažte, že vzniklý útvar (vločka) má nekonečný obvod. Poté určete jeho obsah.

**Řešení.** Obvod původního trojúhelníku je roven 3. V každém kroku konstrukce se prodlouží obvod útvaru o třetinu, neboť ze tří částí každé úsečky vzniknou čtyři stejné délky. Odsud vyplývá, že obvod vločky lze vyjádřit jako limitu

$$d_n=3\left(\tfrac{4}{3}\right)^n \quad \text{a} \quad \lim_{n\to\infty} d_n=+\infty.$$

Útvar se zřejmě během konstrukce zvětšuje. Ke stanovení jeho obsahu nám tudíž stačí zachytit, o kolik se jeho obsah zvětší v jednotlivých krocích. Počet jeho stran se v libovolném kroku stává čtyřnásobným (úsečky se rozdělí na třetiny, kdy místo prostřední třetiny máme dvě úsečky), přičemž délka nových stran je třetinová. V následujícím kroku se obsah útvaru zvětší právě o obsahy stejných rovnostranných trojúhelníků, jejichž počet je stejný jako počet úseček v předchozím kroku a jejichž strany mají délku třetin těchto úseček. Když takto přecházíme od rovnostranného trojúhelníku k šesticípé hvězdě při první realizaci uvedeného postupu, obsah se zvětší o 3 rovnostranné trojúhelníky (jejich počet odpovídá počtu stran původního útvaru) s délkou stran 1/3 (ta je třetinová). Označme obsah původního trojúhelníku jako $S_0$. Pokud si uvědomíme, že zmenšením strany rovnostranného trojúhelníku na třetinu se jeho obsah zmenší devětkrát, dostaneme obsah šesticípé hvězdy ve tvaru

$$S_0+3\cdot\frac{S_0}{9}.$$



Nyní si prohlédněme pozorněji posloupnost čísel $u_n$, jejíž limitou je $e^x$. Budeme chtít uvažovat $n > N$ pro nějaké pevné $N$ (hodně velké) a $k < N$ pevné (docela malé) a označíme si $u_{n,k}$ prvních $k$ členů ve výrazu (5.10) pro $u_n$.

Pro dané $x$ a $\varepsilon > 0$, umíme zvolit $k$ tak, aby $u_{n,k}+\varepsilon > u_n$, pro všechna $n > k$ (skutečně, zbylé členy jsou všechny kladné a ještě menší, než ty ve $v_n$, které jsme odhadli výše). Přitom zároveň pro naše pevné $k$ můžeme volbou dostatečně velikého $N$ zařídit, aby pro všechna $n > N$ bylo také $u_{n,k} < v_k < u_{n,k}+\varepsilon$ (protože pro pevné $k$ máme ve výrazech pro $u_{n,k}$ jen konečně mnoho závorek a volbou velikého $n$ budou všechny libovolně blízko k jedničce).

Celkem tedy pro libovolné $\varepsilon$ vedou naše volby indexů $k$ a $n$ k odhadu $|v_k-u_n|<\varepsilon$. Když budeme volit posloupnost $\varepsilon_i=1/i$, dostaneme takové podposloupnosti $v_{k_i}$ a $u_{n_i}$ s hodnotami vzdálenými nejvýše o $1/i$, a proto také

$$\lim_{k\to\infty} v_k=\lim_{n\to\infty} u_n,$$

což jsme měli dokázat.

Podívejme se ještě na derivaci funkce $e^x$ v bodě $x=0$. Přímo z definice musíme spočíst limitu

$$\lim_{x\to0}\frac{(1+x+\frac{1}{2}x^2+\cdots)-1}{x}=\lim_{x\to0}\frac{x+\frac{1}{2}x^2+\frac{1}{6}x^3+\cdots}{x}.$$

Diskutujeme tedy limitní výraz

$$\lim_{x\to0}\left(\lim_{n\to\infty}\sum_{k=1}^{n}\frac{1}{k!}x^{k-1}\right)=1+\lim_{x\to0}\left(\lim_{n\to\infty}\sum_{k=2}^{n}\frac{1}{k!}x^{k-1}\right).$$

Nyní pro každé $\varepsilon > 0$ můžeme najít $N$ tak, aby $\lim_{n\to\infty}\sum_{k=N}^{n}\frac{1}{k!}x^{k-1}<\varepsilon$ pro všechna $-1\le x\le 1$. Pak jistě pro dostatečně malá $x$ můžeme zmenšit i součet prvních $N-2$ sčítanců na nejvýše $\varepsilon$. Půjdeme-li přitom s číslem $\varepsilon$ k nule, zjistíme, že limita limitního výrazu napravo je nulová, a proto zkoumaná limita skutečně existuje a je rovna jedné. $\square$

Čtenáři, kteří předchozí řádky přeskočili (ať už schválně nebo v nouzi) mohou v klidu počkat, až odvodíme předchozí výsledek z obecných teoretických úvah jednodušeji. Časem totiž ukážeme, že jsou funkce zadané jako nekonečné polynomy vždy diferencovatelné a že je lze derivovat člen po členu. Ještě později ukážeme, že podmínky $f'(x)=f(x)$ a $f(0)=1$ určují funkci $f$ jednoznačně.

**5.45. Číselné řady.** Při odvození předchozí důležité věty o funkci $e^x$ jsme mimoděk pracovali s několika mimořádně užitečnými pojmy a nástroji. Zformulujeme si je nyní obecněji:



### Číselné nekonečné řady

**Definice.** *Nekonečná řada čísel* je výraz

$$\sum_{n=0}^{\infty}a_n=a_0+a_1+a_2+\cdots+a_k+\ldots,$$

kde $a_n$ jsou reálná nebo komplexní čísla. Posloupnost *částečných součtů* je dána svými členy $s_k=\sum_{n=0}^{k}a_n$ a říkáme, že řada konverguje a je rovna $s$, jestliže existuje konečná limita částečných součtů

$$s=\lim_{k\to\infty} s_k.$$

Podobně v dalším kroku obdržíme obsah útvaru jako

$$S_0 + 3 \cdot \frac{S_0}{9} + 4 \cdot 3 \cdot \frac{S_0}{9^2}.$$

Počet přidávaných trojúhelníků je čtyřnásobný a délky jejich stran třetinové.

Nyní již není obtížné odvodit, že obsah vločky je roven limitě

$$\begin{aligned}
&\lim_{n\to\infty}\left(S_0 + 3\cdot\frac{S_0}{9} + 4\cdot 3\cdot\frac{S_0}{9^2} + \cdots + 4^n\cdot 3\cdot\frac{S_0}{9^{n+1}}\right) = \\
&= S_0 \lim_{n\to\infty}\left(1 + \frac{1}{3} + \frac{1}{3}\cdot\frac{4}{9} + \cdots + \frac{1}{3}\cdot\left(\frac{4}{9}\right)^n\right) = \\
&= S_0\left[1 + \frac{1}{3}\lim_{n\to\infty}\left(1 + \frac{4}{9} + \cdots + \left(\frac{4}{9}\right)^n\right)\right] = \\
&= S_0\left[1 + \frac{1}{3}\lim_{n\to\infty}\sum_{k=0}^{n}\left(\frac{4}{9}\right)^k\right] = S_0\left[1 + \frac{1}{3}\sum_{k=0}^{\infty}\left(\frac{4}{9}\right)^k\right] = \\
&= S_0\left[1 + \frac{1}{3}\cdot\frac{1}{1-\frac{4}{9}}\right] = \frac{8}{5}\,S_0.
\end{aligned}$$

Obsah vločky je tedy 8/5 obsahu původního trojúhelníka, tj.

$$\frac{8}{5}\,S_0 = \frac{8}{5}\cdot\frac{\sqrt{3}}{4} = \frac{2\sqrt{3}}{5}.$$

Zopakujme, že tato vločka je příkladem toho, jak nekonečně dlouhá křivka může ohraničovat konečnou plochu. □

**5.103.** Sečtěte řadu

(a) $\sum_{n=1}^{\infty}\left(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{n+1}}\right)$;

(b) $\sum_{n=0}^{\infty}\frac{5}{3^n}$;

(c) $\sum_{n=1}^{\infty}\left(\frac{3}{4^{2n-1}} + \frac{2}{4^{2n}}\right)$;

(d) $\sum_{n=1}^{\infty}\frac{n}{3^n}$;

(e) $\sum_{n=0}^{\infty}\frac{1}{(3n+1)(3n+4)}$.

**Řešení.** Případ (a). Podle definice je součet řady

$$\begin{aligned}
&\sum_{n=1}^{\infty}\left(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{n+1}}\right) = \\
&= \lim_{n\to\infty}\left(\left(\frac{1}{\sqrt{1}} - \frac{1}{\sqrt{2}}\right) + \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}}\right) + \cdots + \left(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{n+1}}\right)\right) = \\
&= \lim_{n\to\infty}\left(1 + \left(-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\right) + \cdots + \left(-\frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n}}\right) - \frac{1}{\sqrt{n+1}}\right) = 1.
\end{aligned}$$

Případ (b). Zjevně se jedná o pětinásobek konvergentní geometrické řady s kvocientem $q = 1/3$, a tudíž je

$$\sum_{n=0}^{\infty}\frac{5}{3^n} = 5\sum_{n=0}^{\infty}\left(\frac{1}{3}\right)^n = 5\cdot\frac{1}{1-\frac{1}{3}} = \frac{15}{2}.$$

Jestliže posloupnost reálných částečných součtů řady má nevlastní limitu, říkáme že řada *diverguje* k $\infty$ nebo $-\infty$, pokud limita částečných součtů neexistuje, říkáme, že je řada *osciluje*.

Z obecných vět o limitách posloupností okamžitě vyplývá, že součet konvergentních řad $\sum a_n$ a $\sum b_n$ je konvergentní řada $\sum(a_n + b_n)$ a obdobně pro násobek řady konstantou. Z věty o třech limitách také okamžitě dostáváme tzv. srovnávací kritérium, které říká, že při $0 \le a_n \le b_n$ vyplývá z konvergence řady $\sum b_n$ i konvergence řady $\sum a_n$, zatímco z divergence řady $\sum a_n$ vyplývá divergence řady $\sum b_n$.

K tomu, aby posloupnost částečných součtů $s_n$ konvergovala, je nutné a stačí, aby byla cauchyovská. Tzn. že

$$|s_m - s_n| = |a_{n+1} + \cdots + a_m|$$

musí být libovolně malé pro dostatečně velká $m > n$. Protože je

$$|a_{n+1}| + \cdots + |a_m| > |a_{n+1} + \cdots + a_m|,$$

vyplývá z konvergence řady $\sum_{k=0}^{\infty}|a_n|$ i konvergence řady $\sum_{k=0}^{\infty}a_n$.

### Absolutně konvergentní řady

Říkáme, že řada $\sum_{k=0}^{\infty}a_n$ *konverguje absolutně*, jestliže konverguje řada $\sum_{n=0}^{\infty}|a_n|$.



Absolutní konvergenci jsme zavedli, protože se často daleko snadněji ověřuje. Navíc, pokud konverguje řada $\sum_{i=1}^{\infty}|a_i|$, tak konverguje i řada $\sum_{i=1}^{\infty}a_i$. Důkaz okamžitě vyplývá z předchozí úvahy o cauchyovskosti posloupností částečných součtů.

Zároveň následující věta ukazuje, že se v případě absolutně konvergentních řad i jednoduché algebraické operace chovají všechny velice dobře:

**5.46. Věta.** *Nechť $S = \sum_{n=0}^{\infty}a_n$ a $T = \sum_{n=0}^{\infty}b_n$ jsou dvě absolutně konvergentní řady. Pak*

*(1) jejich součet absolutně konverguje k součtu*

$$S + T = \sum_{n=0}^{\infty}a_n + \sum_{n=0}^{\infty}b_n = \sum_{n=0}^{\infty}(a_n + b_n),$$

*(2) jejich rozdíl absolutně konverguje k rozdílu*

$$S - T = \sum_{n=0}^{\infty}a_n - \sum_{n=0}^{\infty}b_n = \sum_{n=0}^{\infty}(a_n - b_n),$$

*(3) jejich součin absolutně konverguje k součinu*

$$S \cdot T = \left(\sum_{n=0}^{\infty}a_n\right)\cdot\left(\sum_{n=0}^{\infty}b_n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}a_{n-k}b_k\right).$$

Důkaz. První i druhé tvrzení jsou bezprostředním důsledkem obdobných vlastností limit. Třetí tvrzení vyžaduje větší pozornost. Označme si

$$c_n = \sum_{k=0}^{n}a_{n-k}b_k.$$

Z předpokladů a podle pravidel pro limitu součinu posloupností dostáváme

$$\left(\sum_{n=0}^{k}a_n\right)\cdot\left(\sum_{n=0}^{k}b_n\right) \to \left(\sum_{n=0}^{\infty}a_n\right)\cdot\left(\sum_{n=0}^{\infty}b_n\right).$$

Případ (c). Platí (při substituci $m = n-1$)

$$\sum_{n=1}^{\infty}\left(\frac{3}{4^{2n-1}}+\frac{2}{4^{2n}}\right)=\frac{3}{4}\sum_{n=1}^{\infty}\left(\frac{1}{4^{2n-2}}\right)+\frac{2}{16}\sum_{n=1}^{\infty}\left(\frac{1}{4^{2n-2}}\right)=$$
$$=\left(\frac{3}{4}+\frac{2}{16}\right)\sum_{m=0}^{\infty}\frac{1}{4^{2m}}=\frac{14}{16}\sum_{m=0}^{\infty}\left(\frac{1}{16}\right)^{m}=$$
$$=\frac{14}{16}\cdot\frac{1}{1-\frac{1}{16}}=\frac{14}{15}.$$

Řadu lineárních kombinací jsme zde vyjádřili jako lineární kombinaci řad (přesněji řečeno, jako součet řad s vytknutím konstant), což je platná úprava, pokud obdržené řady jsou absolutně konvergentní.

Případ (d). Z částečného součtu

$$s_n=\frac{1}{3}+\frac{2}{3^2}+\frac{3}{3^3}+\cdots+\frac{n}{3^n},\quad n\in\mathbb{N}$$

bezprostředně získáváme

$$\frac{s_n}{3}=\frac{1}{3^2}+\frac{2}{3^3}+\cdots+\frac{n-1}{3^n}+\frac{n}{3^{n+1}},\quad n\in\mathbb{N}.$$

Je tedy

$$s_n-\frac{s_n}{3}=\frac{1}{3}+\frac{1}{3^2}+\frac{1}{3^3}+\cdots+\frac{1}{3^n}-\frac{n}{3^{n+1}},\quad n\in\mathbb{N}.$$

Protože $\lim_{n\to\infty}\frac{n}{3^{n+1}}=0$, dostáváme

$$\sum_{n=1}^{\infty}\frac{n}{3^n}=\lim_{n\to\infty}\frac{3}{2}\left(s_n-\frac{s_n}{3}\right)=\frac{3}{2}\lim_{n\to\infty}\sum_{k=1}^{n}\frac{1}{3^k}=$$
$$=\frac{3}{2}\sum_{k=1}^{\infty}\left(\frac{1}{3}\right)^{k}=\frac{3}{2}\left(\frac{1}{1-\frac{1}{3}}-1\right)=\frac{3}{4}.$$

Případ (e). Stačí použít vyjádření (jde o tzv. rozklad na parciální zlomky)

$$\frac{1}{(3n+1)(3n+4)}=\frac{1}{3}\cdot\frac{1}{3n+1}-\frac{1}{3}\cdot\frac{1}{3n+4},\quad n\in\mathbb{N}\cup\{0\},$$

které dává

$$\sum_{n=0}^{\infty}\frac{1}{(3n+1)(3n+4)}=\lim_{n\to\infty}\frac{1}{3}\left(1-\frac{1}{4}+\frac{1}{4}-\frac{1}{7}+\frac{1}{7}-\frac{1}{10}+\cdots\right.$$
$$\left.\cdots+\frac{1}{3n+1}-\frac{1}{3n+4}\right)=$$
$$=\lim_{n\to\infty}\frac{1}{3}\left(1-\frac{1}{3n+4}\right)=\frac{1}{3}.$$

□

**5.104.** Ověřte, že platí

$$\sum_{n=1}^{\infty}\frac{1}{n^2}<\sum_{n=0}^{\infty}\frac{1}{2^n}.$$

**Řešení.** Ihned je vidět, že

$$1\le 1,\quad \frac{1}{2^2}+\frac{1}{3^2}<2\cdot\frac{1}{2^2}=\frac{1}{2},\quad \frac{1}{4^2}+\frac{1}{5^2}+\frac{1}{6^2}+\frac{1}{7^2}<4\cdot\frac{1}{4^2}=\frac{1}{4},$$

Máme tedy dokázat, že

$$0=\lim_{k\to\infty}\left(\left(\sum_{n=0}^{k}a_n\right)\cdot\left(\sum_{n=0}^{k}b_n\right)-\sum_{n=0}^{k}c_k\right).$$

Porovnejme si nyní výrazy

$$\left(\sum_{n=0}^{k}a_n\right)\cdot\left(\sum_{n=0}^{k}b_n\right)=\sum_{0\le i,j\le k}a_ib_j,$$

$$c_n=\sum_{\substack{i+j=n\\0\le i,j\le k}}a_ib_j,\quad \sum_{n=0}^{k}c_n=\sum_{\substack{i+j\le k\\0\le i,j\le k}}a_ib_j.$$

Dostáváme tedy odhad

$$\left|\left(\sum_{n=0}^{k}a_n\right)\cdot\left(\sum_{n=0}^{k}b_n\right)-\sum_{n=0}^{k}c_n\right|=\left|\sum_{\substack{i+j>k\\0\le i,j\le k}}a_ib_j\right|\le\sum_{\substack{i+j>k\\0\le i,j\le k}}|a_ib_j|.$$

K odhadu posledního výrazu nám poslouží jednoduchý trik: aby mohl být součet indexů větší než $k$, musí být alespoň jeden z nich větší než $k/2$. Jistě tedy výraz nezmenšíme, když do něj přidáme více členů, tj. vezmeme všechny jako v součinu a odebereme pouze ty, u kterých jsou oba nejvýše $k/2$.

$$\sum_{\substack{i+j>k\\0\le i,j\le k}}|a_ib_j|\le\sum_{0\le i,j\le k}|a_ib_j|-\sum_{0\le i,j\le k/2}|a_ib_j|.$$

Oba výrazy v rozdílu jsou ale částečné součty pro součin $S\cdot T$, mají tedy také stejnou limitu, a proto jejich rozdíl jde k nule. □

Všimněme si, že pro řady, které nekonvergují absolutně, neumíme jejich součin zavést, protože hodnota limity roznásobených výrazů bude záviset na závorkování a pořadí sčítanců.

Další věta uvádí podmínky, pomocí kterých umíme ověřit konvergenci řad.

**5.47. Věta.** *Nechť $S=\sum_{n=0}^{\infty}a_n$ je nekonečná řada reálných nebo komplexních čísel.*

*(1) Jestliže řada $S$ konverguje, pak $\lim_{n\to\infty}a_n=0$.*

*(2) Předpokládejme, že existuje limita podílů po sobě jdoucích členů řady a platí*

$$\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right|=q.$$

*Pak řada $S$ konverguje absolutně při $|q|<1$ a nekonverguje při $|q|>1$. Při $|q|=1$ může řada konvergovat ale nemusí.*

*(3) Jestliže existuje limita*

$$\lim_{n\to\infty}\sqrt[n]{|a_n|}=q,$$

*pak při $q<1$ řada konverguje absolutně, zatímco při $q>1$ nekonverguje. Je-li $q=1$, může konvergovat i divergovat.*



Důkaz. (1) Víme, že existence a případná hodnota limity posloupnosti komplexních čísel je dána pomocí limit posloupností reálných a imaginárních složek. První tvrzení tedy stačí dokázat pro posloupnosti reálných čísel. Jestliže $\lim_{n\to\infty}a_n$ neexistuje nebo je nenulová, existuje pro dostatečně malé číslo $\varepsilon>0$ nekonečně mnoho členů $a_k$ s $|a_k|>\varepsilon$. Zároveň tedy musí mezi nimi existovat nekončeně mnoho kladných nebo nekonečně mnoho záporných. Pak ovšem při přidání kteréhokoliv z nich do částečného součtu dostáváme rozdíl dvou po sobě

resp. obecný odhad

$$\frac{1}{(2^n)^2}+\cdots+\frac{1}{(2^{n+1}-1)^2}<2^n\cdot\frac{1}{(2^n)^2}=\frac{1}{2^n},\quad n\in\mathbb{N}.$$

Odsud (porovnáním členů obou řad) dostáváme zadanou nerovnost, z níž mj. plyne absolutní konvergence řady $\sum_{n=1}^{\infty}\frac{1}{n^2}$. Ještě upřesněme, že je

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}<2=\sum_{n=0}^{\infty}\frac{1}{2^n}\,.$$ □

**5.105.** Vyšetřete konvergenci řady

$$\sum_{n=1}^{\infty}\ln\frac{n+1}{n}.$$

**Řešení.** Pokusme se uvedenou řadu sečíst. Platí

$$\sum_{n=1}^{\infty}\ln\frac{n+1}{n}=\lim_{n\to\infty}\left(\ln\frac{2}{1}+\ln\frac{3}{2}+\ln\frac{4}{3}+\cdots+\ln\frac{n+1}{n}\right)=$$

$$=\lim_{n\to\infty}\ln\frac{2\cdot3\cdot4\cdots(n+1)}{1\cdot2\cdot3\cdots n}=\lim_{n\to\infty}\ln(n+1)=+\infty.$$

Řada tudíž diverguje k $+\infty$. □

**5.106.** Prokažte, že řady

$$\sum_{n=0}^{\infty}\operatorname{arctg}\frac{n^2+2n+3\sqrt{n}+4}{n+1};\quad\sum_{n=1}^{\infty}\frac{3^n+1}{n^3+n^2-n}$$

nekonvergují.

**Řešení.** Protože

$$\lim_{n\to\infty}\operatorname{arctg}\frac{n^2+2n+3\sqrt{n}+4}{n+1}=\lim_{n\to\infty}\operatorname{arctg}\frac{n^2}{n}=\frac{\pi}{2}$$

a

$$\lim_{n\to\infty}\frac{3^n+1}{n^3+n^2-n}=\lim_{n\to\infty}\frac{3^n}{n^3}=+\infty,$$

není splněna nutná podmínka konvergence $\lim_{n\to\infty}a_n=0$ řady $\sum_{n=n_0}^{\infty}a_n$. □

**5.107.** Zjistěte, zda řada

(a) $\sum_{n=0}^{\infty}\frac{1}{(n+1)\cdot3^n}$;

(b) $\sum_{n=1}^{\infty}\frac{n^2+1}{n^3}$;

(c) $\sum_{n=1}^{\infty}\frac{1}{n-\ln n}$

konverguje.

**Řešení.** Všechny tři uvedené řady mají nezáporné členy, a tak mohou v jednotlivých variantách nastat jen dvě možnosti – součet je konečný, součet je roven $+\infty$. Platí

(a) $\sum_{n=0}^{\infty}\frac{1}{(n+1)\cdot3^n}\le\sum_{n=0}^{\infty}\left(\frac{1}{3}\right)^n=\frac{1}{1-\frac{1}{3}}<+\infty$;

(b) $\sum_{n=1}^{\infty}\frac{n^2+1}{n^3}\ge\sum_{n=1}^{\infty}\frac{n^2}{n^3}=\sum_{n=1}^{\infty}\frac{1}{n}=+\infty$;

jdoucích $s_n$ a $s_{n+1}$ o velikosti alespoň $\varepsilon$. Posloupnost částečných součtů proto nemůže být cauchyovská a tedy ani konvergentní.

(2) Protože chceme dokazovat absolutní konvergenci, můžeme rovnou předpokládat, že členy řady jsou reálná čísla $a_i>0$. Důkaz jsme pro speciální hodnotu $q=1/2$ provedli při odvození hodnoty $e^x$ pomocí řady. Uvažme nyní $q<r<1$ pro nějaké reálné $r$. Z existence limity podílů dovodíme pro všechna $j$ větší než dostatečně veliké $N$

$$a_{j+1}<r\cdot a_j\le r^{(j-N+1)}\,a_N.$$

To ale znamená, že částečné součty $s_n$ jsou pro velká $n>N$ shora ohraničeny součty

$$s_n<\sum_{j=0}^{N}a_j+a_N\sum_{j=0}^{n-N}r^j=\sum_{j=0}^{N}a_j+\frac{1-r^{n-N+1}}{1-r}.$$

Protože $0<r<1$, je množina všech částečných součtů shora ohraničená rostoucí posloupnost, a proto je její limitou její supremum.

Při hodnotě $q>r>1$ použijeme obdobný postup, ale z existence limity podílu $q$ hned na začátku odvodíme

$$a_{j+1}>r\cdot a_j\ge r^{(j-N+1)}\,a_N>0.$$

To ale znamená, že absolutní hodnoty velikostí jednotlivých členů řady nejdou k nule, a proto tato řada nemůže konvergovat podle již dokázané části věty.

(3) Důkaz je zde velmi podobný předchozímu případu. Z existence limity $q<1$ vyplývá, že pro každé $q<r<1$ existuje $N$ takové, že pro všechny $n>N$ platí $\sqrt[n]{|a_n|}<r$. Umocněním pak dostáváme $|a_n|<r^n$, takže jsme opět v situaci, kdy srovnáváme s geometrickou řadou. Důkaz se proto dokončí stejně jako v případě podílového testu. □

V důkazu druhého i třetího tvrzení jsme využívali slabšího tvrzení, než je existence limity. Potřebovali jsme pro studované posloupnosti nezáporných výrazů pouze tvrzení, že od určitého indexu už budou větší nebo menší než dané číslo.

K takovému odhadu nám ale postačí pro danou posloupnost $b_n$ uvažovat s každým indexem $n$ supremum hodnot členů s indexy vyššími. Tato suprema vždy existují a budou tvořit nerostoucí posloupnost. Její infimum pak označujeme jako *limes superior* dané posloupnosti a značíme

$$\limsup_{n\to\infty}b_n.$$

Výhodou je, že limes superior vždy existuje, můžeme proto předchozí výsledek (aniž bychom měnili důkaz) přeformulovat v silnější podobě:

**Důsledek.** *Nechť $S=\sum_{n=0}^{\infty}a_n$ je nekonečná řada reálných nebo komplexních čísel.*

*(1) Je-li*

$$q=\limsup_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right|,$$

*pak řada $S$ konverguje absolutně při $q<1$ a nekonverguje při $q>1$. Při $q=1$ může řada konvergovat ale nemusí.*

*(2) Je-li*

$$q=\limsup_{n\to\infty}\sqrt[n]{|a_n|},$$

*pak při $q<1$ řada konverguje absolutně, zatímco při $q>1$ diverguje. Je-li $q=1$, může konvergovat i divergovat.*

(c) $\sum_{n=1}^{\infty} \frac{1}{n-\ln n} \geq \sum_{n=1}^{\infty} \frac{1}{n} = +\infty$.

Odtud plyne, že řada (a) konverguje; (b) diverguje k $+\infty$; (c) diverguje k $+\infty$. □

**5.108.** Ukažte, že tzv. *harmonická řada*

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

diverguje.

**Řešení.** Pro libovolné přirozené k je součet prvních $2^k$ členů řady větší než $k/2$:

$$\underbrace{1+\frac{1}{2}}_{>\frac{1}{2}} + \underbrace{\frac{1}{3}+\frac{1}{4}}_{>\frac{1}{4}+\frac{1}{4}=\frac{1}{2}} + \underbrace{\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}}_{>\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}=\frac{1}{2}} + \ldots,$$

součet členů od $2^l + 1$ do $2^{l+1}$ je totiž vždy větší než $2^l$-krát (jejich počet) číslo $1/2^l$ (nejmenší z nich), což je dohromady $1/2$.

Divergenci této řady můžeme také ověřit integrálním kriteriem konvergence řad, viz 6.36 □

Další zajímavé příklady k číselným řadám naleznete na straně 311.

## I. Mocninné řady

V předchozí podkapitole jsme zkoumali, jestli lze přiřadit smysl součtu nekonečně mnoha čísel. Nyní se budeme zajímat o to, jaký může mít význam součet nekonečně mnoha funkcí.

**5.109.** Určete poloměr konvergence následujících mocninných řad:

i) $\sum_{n=1}^{\infty} \frac{2^n}{n} x^n$,

ii) $\sum_{n=1}^{\infty} \frac{1}{(1+i)^n} x^n$.

**Řešení.** (i) Podle 5.50 je

$$r = \frac{1}{\limsup_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right|} = \frac{1}{2}.$$

Daná mocninná řada tedy konverguje pro reálná $x \in (-\frac{1}{2}, \frac{1}{2})$, případně pro komplexní $|x| < \frac{1}{2}$. Všimněme si, že řada je divergentní pro $x = \frac{1}{2}$ (jde o harmonickou řadu) a naopak konverguje pro $x = -\frac{1}{2}$ (alternující harmonická řada). Rozhodnout o konvergenci pro libovolné $x$ ležící v komplexní rovině na kružnici o poloměru $\frac{1}{2}$ je těžší otázka a přesahuje rámec našeho kurzu.

(ii) $r = \limsup_{n\to\infty} \left|\sqrt[n]{\frac{1}{(1+i)^n}}\right| = \limsup_{n\to\infty} \left|\frac{1}{1+i}\right| = \frac{\sqrt{2}}{2}$. □

**5.48. Alternující řady.** Podmínka $a_n \to 0$ je nutnou, ale nikoliv dostatečnou podmínkou konverce řady $\sum_{n=1}^{\infty} a_n$. Platí ale naásledující tzv. *Leibnizovo kritérium* konvergence:

Řadu $\sum_{n=1}^{\infty}(-1)^n a_n$, kde $a_n$ je neklesající posloupnost kladných reálných čásel, nazýváme *alternující řadou*.

**Věta.** *Alternující řada je konvergentní, právě když platí* $\lim_{n\to\infty} a_n = 0$. *Její součet a se liší od částečného součtu* $s_{2k}$ *o nejvýše* $a_{2k+1}$.

Důkaz. Přímo z definičních vlastností dostáváme pro částečné součty $s_k$ alternující řady

$$s_{2(k+1)+1} = s_{2k+1} - a_{2k+2} + a_{2k+3} \leq s_{2k+1}$$
$$s_{2(k+1)} = s_{2k} + a_{2k+1} - a_{2k+2} \geq s_{2k}$$
$$s_{2k+1} - s_{2k} = a_{2k+1} \to 0$$
$$s_2 \leq s_{2k} \leq s_{2k+1} \leq s_1.$$

Z posledního řádku vyplývá, že posloupnost lichých částečných součtů konverguje ke svému infimu, zatímco posloupnost sudých částečných součtů ke svému supremu. Předchozí řádek ale zaručuje, že tyto limity musí být stejné.

Zároveň vidíme, že součet $a$ naší řady je vždy menší než $s_{2k+1}$ a větší než $s_{2k}$. Tyto částečné součty se proto nemohou lišit od limity o více než $a_{2k+1}$. □

**5.49. Mocninné řady.** Jestliže máme místo posloupnosti čísel $a_n$ k dispozici posloupnost funkcí $f_n(x)$ se stejným definičním oborem $A$, můžeme bod po bodu použít definici součtu číselné řady a dostáváme pojem součtu *řady funkcí*



$$S(x) = \sum_{n=0}^{\infty} f_n(x).$$

Konvergence mocninné řady

*Mocninná řada* je dána výrazem

$$S(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Řekneme, že $S(x)$ má *poloměr konvergence* $\rho \geq 0$, jestliže $S(x)$ konverguje pro každé $x$ splňující $|x| < \rho$ a nekonverguje při $|x| > \rho$.

**5.50. Vlastnosti mocninných řad.** Ačkoliv na podstatnou část důkazu následující věty si budeme muset počkat až na konec příští kapitoly, zformulujeme si základní vlastnosti mocninných řad hned:

Absolutní konvergence a derivování

**Věta.** *Nechť* $S(x) = \sum_{n=0}^{\infty} a_n x^n$ *je mocninná řada a existuje limita*

$$r = \lim_{n\to\infty} \sqrt[n]{|a_n|}.$$

*Pak je poloměr konvergence řady S roven* $\rho = r^{-1}$. *když* $r > 0$, $\rho = \infty$ *pro* $r = 0$, *a* $\rho = 0$, *když* $r = \infty$.

*Mocninná řada* $S(x)$ *konverguje na na celém svém intervalu konvergence absolutně a je na něm spojitá (včetně krajních bodů,*

**5.110.** Určete poloměr konvergence $r$ mocninné řady

(a) $\sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n\cdot 8^n}\, x^n$;

(b) $\sum_{n=1}^{\infty} (-4n)^n\, x^n$;

(c) $\sum_{n=1}^{\infty} \left(1+\frac{1}{n}\right)^{n^2} x^n$;

(d) $\sum_{n=1}^{\infty} \frac{n^5}{(2+(-1)^n)^n}\, x^n$.

**Řešení.** Platí

(a) $\lim_{n\to\infty} \sqrt[n]{|\,a_n\,|} = \lim_{n\to\infty} \frac{1}{\sqrt[n]{n}\cdot 8} = \frac{1}{8}$;

(b) $\lim_{n\to\infty} \sqrt[n]{|\,a_n\,|} = \lim_{n\to\infty} 4n = +\infty$;

(c) $\lim_{n\to\infty} \sqrt[n]{|\,a_n\,|} = \lim_{n\to\infty} \left(1+\frac{1}{n}\right)^n = \mathrm{e}$;

(d) $\limsup_{n\to\infty} \sqrt[n]{|\,a_n\,|} = \limsup_{n\to\infty} \frac{\sqrt[n]{n^5}}{2+(-1)^n} = \limsup_{n\to\infty} \frac{(\sqrt[n]{n})^5}{2+(-1)^n} = 1.$

Proto je poloměr konvergence (a) $r = 8$, (b) $r = 0$, (c) $r = 1/\mathrm{e}$, (d) $r = 1$. □

**5.111.** Stanovte poloměr konvergence $r$ mocninné řady

$$\sum_{n=1}^{\infty} \mathrm{e}^{in}\, \frac{\sqrt[3]{n^3+n}\cdot 3^n}{\sqrt[3]{n^4+2n^3+1}\cdot \pi^n}\, (x-2)^n.$$

**Řešení.** Poloměr konvergence libovolné mocninné řady se nezmění, pokud posuneme její střed nebo nahradíme koeficienty členů tak, že se nezmění jejich absolutní hodnota. Určeme tedy poloměr konvergence řady

$$\sum_{n=1}^{\infty} \frac{\sqrt[3]{n^3+n}\cdot 3^n}{\sqrt[3]{n^4+2n^3+1}\cdot \pi^n}\, x^n.$$

Protože

$$\lim_{n\to\infty} \sqrt[n]{n^a} = \left(\lim_{n\to\infty} \sqrt[n]{n}\right)^a = 1 \quad \text{pro } a > 0,$$

můžeme dále přejít k řadě

$$\sum_{n=1}^{\infty} \frac{3^n}{\pi^n}\, x^n$$

se stejným poloměrem konvergence $r = \pi/3$. □

**5.112.** Napište mocninnou řadu se středem v počátku, jejíž součet je na intervalu $(-3, 3)$ funkce

$$\frac{1}{x^2-x-12}.$$

**Řešení.** Neboť

$$\frac{1}{x^2-x-12} = \frac{1}{(x-4)(x+3)} = \frac{1}{7}\left(\frac{1}{x-4} - \frac{1}{x+3}\right)$$

*pokud v nich konverguje také) a na tomto intervalu existuje její derivace*

$$S'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}.$$

Důkaz. Pro ověření absolutní konvergence řady můžeme pro každou pevnou hodnotu $x$ použít odmocninový test z věty 5.47(3). Počítáme přitom

$$\lim_{n\to\infty} \sqrt[n]{|a_n x^n|} = rx$$

a řada konverguje absolutně, resp. nekonverguje, jestliže je tato limita různá od 1. Odtud plyne, že skutečně konverguje pro $|x| < \rho$ a diverguje pro $|x| > \rho$.

Tvrzení o spojitosti a derivaci dokážeme později v obecnějším kontextu, viz 6.43–6.45. □

Všimněme si také, že můžeme při důkazu konvergence použít silnější variantu odmocninového testu a tedy lze poloměr konvergence $r$ pro každou mocninnou řadu přímo zadat vztahem

$$r^{-1} = \limsup_{n\to\infty} \sqrt[n]{|a_n|}.$$

**5.51. Poznámky.** Pokud koeficienty řady velmi rychle rostou, např. $a_n = n^n$, pak je $r = \infty$, tj. poloměr konvergence je nula. Skutečně taková řada pak konverguje pouze v jediném bodě $x = 0$.



Podíváme se na příklady konvergence mocninných řad

$$S(x) = \sum_{n=0}^{\infty} x^n, \quad T(x) = \sum_{n=1}^{\infty} \frac{1}{n} x^n$$

včetně krajních bodů příslušného intervalu.

První příklad je *geometrická řada*, kterou jsme se zabývali již dříve, a její součet je pro všechna $x$, $|x| < 1$,

$$S(x) = \frac{1}{1-x},$$

zatímco $|x| > 1$ zaručuje divergenci. Pro $x = 1$ dostáváme také zjevně divergentní řadu $1+1+1+\ldots$ s nekonečným součtem, při $x = -1$ jde o řadu $1-1+1-\ldots$, jejíž částečné součty nemají limitu vůbec, tj. řada osciluje.

Věta 5.47(2) ukazuje, že poloměr konvergence druhého příkladu je také jedna, protože existuje

$$\lim_{n\to\infty} \left| \frac{\frac{1}{n+1} x^{n+1}}{\frac{1}{n} x^n} \right| = x \lim_{n\to\infty} \left| \frac{n}{n+1} \right| = x.$$

Pro $x = 1$ tu dostaneme divergentní řadu $1 + \frac{1}{2} + \frac{1}{3} + \ldots$, protože umíme odhadnout částečné součty tak, že vždy postupně pro $k = 1, 2, 3, \ldots$, sečteme $2^{k-1}$ po sobě jdoucích členů $1/2^{k-1}, \ldots, 1/\left(2^k - 1\right)$ a nahradíme všechny $2^{-k}$. Do spodního odhadu tedy každá taková část přispěje $1/2$ a odhad tedy roste nad všechny meze.

Naopak, řada $T(-1) = -1 + \frac{1}{2} - \frac{1}{3} + \ldots$ konverguje i když samozřejmě nemůže konvergovat absolutně. Vyplývá to z obecnějšího platného tvrzení, které ukážeme až v příští kapitole.

a

$$\frac{1}{x-4} = -\frac{\frac{1}{4}}{1-\frac{x}{4}} = -\frac{1}{4}\left(1+\frac{x}{4}+\frac{x^2}{4^2}+\cdots+\frac{x^n}{4^n}+\cdots\right),$$
$$\frac{1}{x+3} = \frac{\frac{1}{3}}{1-\left(-\frac{x}{3}\right)} = \frac{1}{3}\left(1-\frac{x}{3}+\frac{x^2}{3^2}+\cdots+\frac{(-x)^n}{3^n}+\cdots\right),$$

dostáváme

$$\frac{1}{x^2-x-12} = -\frac{1}{28}\sum_{n=0}^{\infty}\frac{x^n}{4^n} - \frac{1}{21}\sum_{n=0}^{\infty}\frac{(-x)^n}{3^n} = \sum_{n=0}^{\infty}\left(\frac{(-1)^{n+1}}{21\cdot 3^n} - \frac{1}{28\cdot 4^n}\right)x^n. \qquad \square$$

**5.113.** Nalezněte přibližnou hodnotu čísla $\sin 1°$ s chybou ostře menší než $10^{-10}$.

**Řešení.** Víme, že je

$$\sin x = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 - \frac{1}{7!}x^7 + \cdots = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}x^{2n+1},\ x\in\mathbb{R}.$$

Dosadíme-li $x = \pi/180$, pak částečné součty řady vpravo budou aproximacemi $\sin 1°$. Zbývá určit počet členů, které je třeba sečíst, aby chyba byla prokazatelně menší než $10^{-10}$. Číselná řada

$$\frac{\pi}{180} - \frac{1}{3!}\left(\frac{\pi}{180}\right)^3 + \frac{1}{5!}\left(\frac{\pi}{180}\right)^5 - \frac{1}{7!}\left(\frac{\pi}{180}\right)^7 + \cdots = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}\left(\frac{\pi}{180}\right)^{2n+1}$$

je alternující s vlastností, že posloupnost absolutních hodnot jejích členů je klesající. Pokud libovolnou takovou konvergentní řadu nahradíme jejím částečným součtem, chyba, jíž se tím dopustíme, bude menší než absolutní hodnota prvního členu uvažované řady nezahrnutého do částečného součtu. (Důkaz tohoto tvrzení uvádět nebudeme.) Chyba aproximace

$$\sin 1° \approx \frac{\pi}{180} - \frac{\pi^3}{180^3\cdot 3!}$$

je tak menší než

$$\frac{\pi^5}{180^5\cdot 5!} < 10^{-10}.$$

$\square$

*5.114.* Určete poloměr konvergence $r$ mocninné řady

$$\sum_{n=0}^{\infty}\frac{2^{2n}\cdot n!}{(2n)!}x^n\ . \qquad \bigcirc$$

*5.115.* Stanovte poloměr konvergence pro $\sum_{n=1}^{\infty}2^{\sqrt{n}}x^n$. $\bigcirc$

*5.116.* Bez počítání uveďte poloměr konvergence mocninné řady

$$\sum_{n=1}^{\infty}\frac{5}{n\cdot 3^{n-1}}x^{n-1}\ . \qquad \bigcirc$$

**5.52. Goniometrické funkce.** S mocninnými řadami nám do našeho společenství funkcí přibyla spousta nových příkladů hladkých funkcí, tj. funkcí libovolně krát diferencovatelných na celém svém definičním oboru. Podobně jako polynomy mají všechny tyto přírůstky do zvěřince navíc vlastnost, že jsou ve skutečnosti zadány vztahem, který definuje funkci $\mathbb{C}\to\mathbb{C}$.

Skutečně, naše úvahy o absolutní konvergenci jsou bezezbytku platné i pro komplexní číselné řady. Proto mocninné řady budou, po dosazeni komplexních čísel za $x$, na celém kruhu v komplexní rovině se středem v počátku a poloměrem $r$ představovat konvergentní číselné řady komplexních čísel.

Pohrajme si chvíli s nejvýznamnějším příkladem, exponenciálou

$$e^x = 1 + x + \frac{1}{2}x^2 + \cdots + \frac{1}{n!}x^n + \ldots.$$

Tato mocninná řada má poloměr konvergence nekonečný a dobře proto definuje hladkou funkci pro všechna komplexní čísla $x$. Její hodnoty jsou limitami hodnot (komplexních) polynomů s reálnými koeficienty a každý polynom je zcela určený konečně mnoha svými hodnotami. Zejména tedy jsou hodnoty mocninných řad i v komplexním oboru zcela určeny jejich hodnotami na reálných argumentech $x$. Proto i pro komplexní exponenciálu musí platit i obvyklé vztahy, které jsme pro reálné hodnoty proměnné $x$ již odvodili. Zejména tedy platí

$$e^{x+y} = e^x\cdot e^y,$$

viz vztah (5.5) a věta 5.46(3). Dosaďme si hodnoty $x = i\cdot t$, kde $i\in\mathbb{C}$ je imaginární jednotka, $t\in\mathbb{R}$ libovolné.

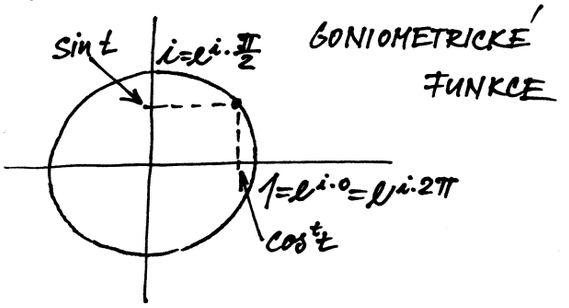
$$e^{it} = 1 + it - \frac{1}{2}t^2 - i\frac{1}{3!}t^3 + \frac{1}{4!}t^4 + i\frac{1}{5!}t^5 - \ldots$$

a zjevně tedy je komplexně konjugované číslo k $z = e^{it}$ číslo $\bar{z} = e^{-it}$. Proto

$$|z|^2 = z\cdot\bar{z} = e^{it}\cdot e^{-it} = e^0 = 1$$

a všechny hodnoty $z = e^{it}$ leží na jednotkové kružnici v komplexní rovině.

Reálné a imaginární složky bodů na jednotkové kružnici jsme popisovali pomocí *goniometrických funkcí* $\cos\theta$ a $\sin\theta$, kde $\theta$ je patřičný úhel.




Derivací parametrického popisu bodů kružnice, $t\mapsto e^{it}$ dostáváme vektory „rychlostí“, které budou dány výrazem (pokud zatím nevěříme derivování mocninných řad člen po členu, lze také zderivovat zvlášť reálnou a imaginární složku) $t\mapsto (e^{it})' = i\cdot e^{it}$ a jejich velikost proto také bude pořád jednotková. Odtud lze tušit, že celou kružnici oběhneme po dosažení hodnoty parametru rovného délce oblouku, tj. $2\pi$ (k pořádné definici délky křivky budeme potřebovat integrální počet, pak toto tvrzení ověříme). Tímto

*5.117.* Nalezněte obor konvergence mocninné řady

$$\sum_{n=1}^{\infty} \frac{\sqrt{n+1}}{3\sqrt{n}}\, x^n \ .$$

○

*5.118.* Určete, pro jaká $x \in \mathbb{R}$ řada

$$\sum_{n=1}^{\infty} \frac{(-3)^n}{\sqrt{n^4+2n^3+111}}\,(x-2)^n$$

konverguje. ○

*5.119.* Je pro libovolnou posloupnost reálných čísel $\{a_n\}_{n=0}^{\infty}$ poloměr konvergence mocninných řad

$$\sum_{n=0}^{\infty} a_n\, x^n\,, \qquad \sum_{n=1}^{\infty} \frac{a_{n-1}}{n}\, x^n$$

stejný? ○

*5.120.* Rozhodněte o platnosti implikací:

(a) Pokud existuje vlastní limita $\lim\limits_{n\to\infty} \sqrt[3n]{a_n^2}$, pak mocninná řada

$$\sum_{n=1}^{\infty} a_n (x-x_0)^n$$

konverguje absolutně alespoň ve dvou různých bodech $x$.

(b) Z neabsolutní konvergence řad $\sum_{n=1}^{\infty} a_n$, $\sum_{n=1}^{\infty} b_n$ plyne, že rovněž řada $\sum_{n=1}^{\infty}(6a_n - 5b_n)$ konverguje.

(c) Jestliže pro číselnou řadu $\sum_{n=0}^{\infty} a_n$ je

$$\lim_{n\to\infty} a_n^2 = 0,$$

pak tato řada konverguje.

(d) Pokud řada $\sum_{n=1}^{\infty} a_n^2$ konverguje, potom řada

$$\sum_{n=1}^{\infty} \frac{a_n}{n}$$

konverguje absolutně.

○

*5.121.* Určete $\cos\frac{\pi}{10}$ s chybou menší než $10^{-5}$. ○

*5.122.* Pro konvergentní řadu

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{\sqrt{n}+100}$$

odhadněte chybu aproximace jejího součtu částečným součtem $s_{9\,999}$.

○

*5.123.* Funkci $y = \mathrm{e}^x$ definovanou na celé reálné přímce vyjádřete jako nekonečný polynom se členy tvaru $a_n(x-1)^n$ a funkci $y = 2^x$ definovanou na $\mathbb{R}$ vyjádřete jako nekonečný polynom se členy $a_n x^n$.

○

*5.124.* Nalezněte funkci $f$, k níž pro $x \in \mathbb{R}$ konverguje posloupnost funkcí

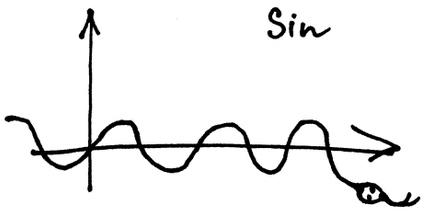
$$f_n(x) = \frac{n^2x^3}{n^2x^2+1}, \quad n \in \mathbb{N}.$$

postupem můžeme definovat tzv. *Ludolfovo číslo*[7] $\pi$ — je to délka poloviny jednotkové kružnice v euklidovském $\mathbb{R}^2$.

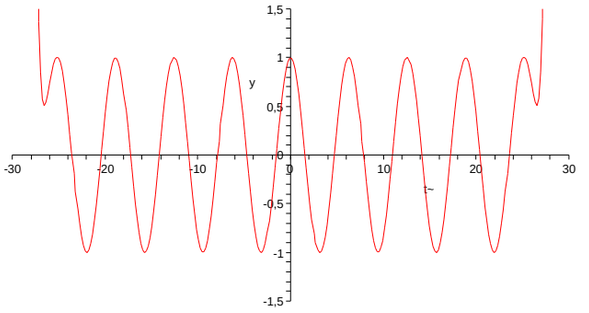
Můžeme se ale nyní aspoň částečně ujistit pohledem na nejmenší kladné kořeny reálné části částečných součtů naší řady, tj. příslušných polynomů. Již při řádu deset nám vyjde číslo $\pi$ přesně na 5 desetinných míst.

Dostáváme tedy přímou definici goniometrických funkcí pomocí mocninných řad:

$$\cos t = \mathrm{re}\,\mathrm{e}^{it} = 1 - \frac{1}{2}t^2 + \frac{1}{4!}t^4 - \frac{1}{6!}t^6 + \dots$$
$$\cdots + (-1)^k \frac{1}{(2k)!}t^{2k} + \dots,$$
$$\sin t = \mathrm{im}\,\mathrm{e}^{it} = t - \frac{1}{3!}t^3 + \frac{1}{5!}t^5 - \frac{1}{7!}t^7 + \dots$$
$$\cdots + (-1)^k \frac{1}{(2k+1)!}t^{2k+1} + \dots.$$




Ilustraci konvergence řady pro funkci cos je vidět na dalším obrázku. Jde o graf příslušného polynomu stupně 68. Při postupném vykreslení částečných součtů je vidět, že aproximace v okolí nuly je velice dobrá a prakticky beze změn. S rostoucím řádem se pak zlepšuje i dále od počátku.




Přímo z definice vyplývá známý vztah

$$\mathrm{e}^{it}\,\mathrm{e}^{-it} = \sin^2 t + \cos^2 t = 1$$

a také z derivace $(\mathrm{e}^{it})' = i\,\mathrm{e}^{it}$ vidíme, že

$$(\sin t)' = \cos t, \qquad (\cos t)' = -\sin t.$$

Tento výsledek lze samozřejmě ověřit přímo derivací našich řad člen po členu.

Označme $t_0$ nejmenší kladné číslo, pro které je $\mathrm{e}^{-it_0} = -\,\mathrm{e}^{it_0}$, tj. první kladný nulový bod funkce $\cos t$. Podle naší definice Ludolfova čísla je $t_0 = \frac{1}{2}\pi$.

[7] Číslo udávající poměr mezi průměrem a obvodem používali už Babyloňané a Řekové ve starověku. Označení Ludolfovo číslo je odvozeno od jména německého matematika Ludolfa van Ceulena, který Archimedovým postupem aproximace pomocí pravidelných mnohoúhelníků spočetl $\pi$ na 35 platných desetinných míst již v 16. století.

Je tato konvergence stejnoměrná na $\mathbb{R}$? ○

*5.125.* Konverguje řada

$$\sum_{n=1}^{\infty} \frac{n\,x}{n^4+x^2}, \quad \text{kde} \quad x \in \mathbb{R},$$

stejnoměrně na celé reálné ose? ○

*5.126.* Odhadněte

(a) kosinus deseti stupňů s přesností alespoň $10^{-5}$;

(b) určitý integrál $\int_0^{1/2} \frac{dx}{x^4+1}$ s přesností alespoň $10^{-3}$.

○

*5.127.* Určete mocninný rozvoj se středem v bodě $x_0 = 0$ funkce

$$f(x) = \int_0^x \mathrm{e}^{t^2}\,dt, \quad x \in \mathbb{R}\,. \qquad ○$$

*5.128.* Užitím integrálního kritéria nalezněte hodnoty $a > 0$, pro které řada

$$\sum_{n=1}^{\infty} \frac{1}{n^a}$$

konverguje. ○

*5.129.* Určete, pro která $x \in \mathbb{R}$ konverguje řada

$$\sum_{i=1}^{\infty} \frac{1}{2^n \cdot n \cdot \ln(n)} x^{3n}\,. \qquad ○$$

*5.130.* Určete všechna $x \in \mathbb{R}$, pro která konverguje mocninná řada $\sum_{i=1}^{\infty} \frac{x^{2n}}{n^2}$. ○

*5.131.* Pro jaká $x \in \mathbb{R}$ řada

$$\sum_{n=1}^{\infty} \frac{\ln(n!)}{n^x}$$

konverguje? ○

*5.132.* Rozhodněte, zda řada

$$\sum_{n=1}^{\infty} (-1)^{n-1} \operatorname{tg} \frac{1}{n\sqrt{n}}$$

konverguje absolutně, příp. relativně, nebo zda diverguje k $+\infty$, resp. k $-\infty$, či nic z toho (říkáme, že osciluje). ○

*5.133.* Stanovte součet číselné řady

$$\sum_{n=1}^{\infty} \frac{1}{n \cdot 3^n}$$

pomocí součtu vhodné mocninné řady. ○

*5.134.* Pro $x \in (-1, 1)$ sečtěte

$$x - 4x^2 + 9x^3 - 16x^4 + \cdots. \qquad ○$$

*5.135.* Je-li $|\,x\,| < 1$, určete součet řady

(a) $\sum_{n=1}^{\infty} \frac{1}{2n-1} x^{2n-1}$;

(b) $\sum_{n=1}^{\infty} n^2 x^{n-1}$.

Pak čtverec této hodnoty je $\mathrm{e}^{i2t_0} = \mathrm{e}^{-i2t_0} = (\mathrm{e}^{-it_0})^2$ a jde tedy o nulový bod funkce $\sin t$. Samozřejmě přitom platí pro libovolné $t$

$$\mathrm{e}^{i(4kt_0+t)} = (\mathrm{e}^{it_0})^{4k} \cdot \mathrm{e}^{it} = 1 \cdot \mathrm{e}^{it}\,.$$

Jsou tedy obě goniometrické funkce sin a cos *periodické* s periodou $2\pi$. Z našich definic je přitom vidět, že je to nejmenší jejich perioda. Současně je vidět, že v komplexním oboru je exponenciální funkce periodická s periodou $2\pi i$, neboť $\mathrm{e}^{z+2\pi i} = \mathrm{e}^z \cdot \mathrm{e}^{2\pi i} = \mathrm{e}^z$.

Nyní můžeme snadno odvodit všechny obvyklé vztahy mezi goniometrickými funkcemi. Uvedeme na ukázku několik z nich. Nejprve si všimněme, že definice vlastně říká

$$\cos t = \frac{1}{2}(\mathrm{e}^{it} + \mathrm{e}^{-it}), \tag{5.12}$$

$$\sin t = \frac{1}{2i}(\mathrm{e}^{it} - \mathrm{e}^{-it}). \tag{5.13}$$

Součin těchto funkcí jde tedy vyjádřit jako

$$\sin t \cos t = \frac{1}{4i}\left(\mathrm{e}^{it} - \mathrm{e}^{-it}\right)\left(\mathrm{e}^{it} + \mathrm{e}^{-it}\right) = \\ = \frac{1}{4i}\left(\mathrm{e}^{i2t} - \mathrm{e}^{-i2t}\right) = \frac{1}{2}\sin 2t.$$

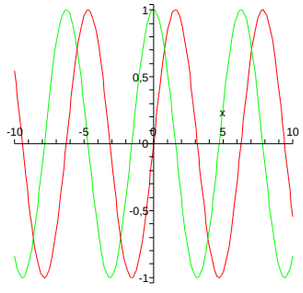
Dále můžeme využít naši znalost derivací:

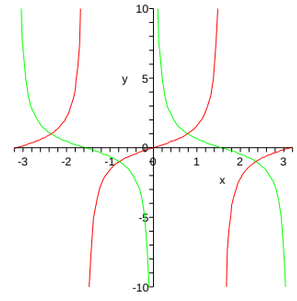
$$\cos 2t = \left(\frac{1}{2}\sin 2t\right)' = (\sin t \cos t)' = \cos^2 t - \sin^2 t.$$

Vlastnosti dalších goniometrických funkcí

$$\operatorname{tg} t = \frac{\sin t}{\cos t}, \qquad \operatorname{cotg} t = (\operatorname{tg} t)^{-1}$$

se snadno odvodí z jejich definice a pravidel pro derivování. Grafy funkcí sinus, cosinus, tangens a cotangens jsou na obrázcích:




*Cyklometrické funkce* jsou inverzní ke goniometrickým. Protože jsou goniometrické funkce všechny periodické s periodou $2\pi$, jsou jejich inverze definované vždy jen v rámci jedné periody a to ještě jen na části, kdy je daná funkce buď rostoucí nebo klesající. Jsou to funkce

$$\arcsin = \sin^{-1}$$

s definičním oborem $[-1, 1]$ a oborem hodnot $[-\pi/2, \pi/2]$. Dále

$$\arccos = \cos^{-1}$$

s definičním oborem $[-1, 1]$ a oborem hodnot $[0, \pi]$, viz obrázek vlevo.

*5.136.* Spočtěte

$$\sum_{n=1}^{\infty} \frac{2n-1}{(-2)^{n-1}}$$

pomocí součtu mocninné řady

$$\sum_{n=0}^{\infty} (-1)^n \, (2n+1) \, x^{2n}$$

pro jisté $x \in (-1, 1)$. ○

*5.137.* Pro $x \in \mathbb{R}$ sečtěte řadu

$$\sum_{n=0}^{\infty} \frac{1}{2^n \cdot n!} \, x^{3n+1} \ . \qquad ○$$

## J. Přírůstky do ZOO

*5.138.* Stanovte maximální podmnožinu $\mathbb{R}$, kde může být funkce

$$y = \operatorname{arctg}\left(x^{21} + \sin x\right) \cdot \frac{\mathrm{e}^{\cos(\sqrt[5]{x}-21+\cos x)+x-256x^3} - 11}{2 + x^{252}}$$

definována. ○

*5.139.* Napište maximální definiční obor funkce

$$y = \frac{\arccos\left(\ln x\right)}{\sqrt{x^2-1}} \ . \qquad ○$$

*5.140.* Uveďte definiční obor, obor hodnot a inverzní funkci funkce

$$y = \frac{x-1}{2-3x} \ . \qquad ○$$

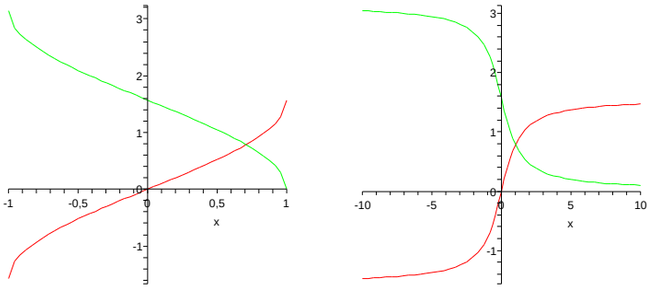
*5.141.* Je funkce

(a) $y = \frac{\cos x}{x^3}$;
(b) $y = \frac{\cos x}{x^3} + 1$;
(c) $y = \frac{\cos x}{x^4}$;
(d) $y = \frac{\cos x}{x^4} + 1$;
(e) $y = \sin x + \operatorname{tg} \frac{x}{2}$;
(f) $y = \ln \frac{1+x}{1-x}$;
(g) $y = \sinh x = \frac{\mathrm{e}^x - \mathrm{e}^{-x}}{2}$;
(h) $y = \cosh x = \frac{\mathrm{e}^x + \mathrm{e}^{-x}}{2}$

s maximálním definičním oborem lichá? ○

*5.142.* Je funkce

(a) $y = \frac{\cos x}{x^3}$;
(b) $y = \frac{\cos x}{x^3} + 1$;
(c) $y = \frac{\cos x}{x^4}$;
(d) $y = \frac{\cos x}{x^4} + 1$;
(e) $y = \sin x + \operatorname{tg} \frac{x}{2}$;
(f) $y = \ln \frac{1+x}{1-x}$;
(g) $y = \sinh x = \frac{\mathrm{e}^x - \mathrm{e}^{-x}}{2}$;
(h) $y = \cosh x = \frac{\mathrm{e}^x + \mathrm{e}^{-x}}{2}$




Zbývají ještě funkce (zobrazené na obrázku vpravo)

$$\operatorname{arctg} = \operatorname{tg}^{-1}$$

s definičním oborem $\mathbb{R}$ a oborem hodnot $(-\pi/2, \pi/2)$ a konečně

$$\operatorname{arccotg} = \operatorname{cotg}^{-1}$$

s definičním oborem $\mathbb{R}$ a oborem hodnot $(0, \pi)$.

Velice často se také využívají tzv. *hyperbolické funkce*

$$\sinh x = \frac{1}{2}\left(\mathrm{e}^x - \mathrm{e}^{-x}\right), \qquad \cosh x = \frac{1}{2}\left(\mathrm{e}^x + \mathrm{e}^{-x}\right).$$

Název naznačuje, že by funkce mohly mít něco společného s hyperbolou. Přímý výpočet dává (druhé mocniny se v roznásobených dvojčlenech všechny odečtou a zůstanou smíšené členy)

$$(\cosh x)^2 - (\sinh x)^2 = 2\frac{1}{2}\left(\mathrm{e}^x \, \mathrm{e}^{-x}\right) = 1.$$

Body $[\cosh t, \sinh t] \in \mathbb{R}^2$ tedy skutečně parametricky popisují hyperbolu v rovině (viz 4.31). Pro hyperbolické funkce lze snadno odvodit podobné identity jako pro funkce goniometrické. Mimo jiné je přímo z definice snadno vidět (dosazením do vztahů (5.12) a (5.13))

$$\cosh x = \cos(ix), \qquad i \sinh x = \sin(ix)$$
$$(\cosh)'(x) = \sinh(x), \qquad (\sinh)'(x) = \cosh(x).$$

**5.53. Poznámky.** **(1)** Jestliže mocninnou řadu $S(x)$ vyjádříme s posunutou hodnotou proměnné $x$ o konstantní posuv $x_0$, dostaneme funkci $T(x) = S(x - x_0)$. Jestliže je $\rho$ poloměr konvergence $S$, bude $T$ dobře definovaná na intervalu $(x_0 - \rho, x_0 + \rho)$. Říkáme, že $T$ je *mocninná řada se středem v* $x_0$.



Mocninné řady proto můžeme přímo definovat takto:

$$S(x) = \sum_{n=0}^{\infty} a_n (x - x_0)^n,$$

kde $x_0$ je libovolné pevně zvolené reálné číslo. Všechny naše předchozí úvahy jsou pořád platné, jen je třeba mít na paměti, že se vztahují k bodu $x_0$. Zejména tedy taková řada konverguje na intervalu $(x_0 - \rho, x_0 + \rho)$, kde $\rho$ je její poloměr konvergence.

Dále platí, že má-li mocninná řada $y = T(x)$ hodnoty v intervalu, kde je dobře definována řada $S(y)$, potom i hodnoty funkce $S \circ T$ jsou vyjádřeny mocninnou řadou, kterou dostaneme formálním dosazením $y = T(x)$ za $y$ do $S(y)$.

**(2)** Jakmile máme k dispozici mocninné řady s obecným středem, lze docela přímočaře počítat koeficienty mocninných řad

s maximálním definičním oborem sudá? ◯

*5.143.* Rozhodněte, zda je funkce

(a) $y = \sin x \cdot \ln|x|$;
(b) $y = \operatorname{arccotg} x$;
(c) $y = x^8 - \sqrt[5]{3}x^6 + 3x^2 - 6$;
(d) $y = \cos(\pi - x)$;
(e) $y = \frac{\operatorname{tg} x + x}{3 + 7\cos x}$

s maximálním definičním oborem lichá, sudá. ◯

*5.144.* Je funkce

(a) $y = \ln(\cos x)$ ;
(b) $y = \operatorname{tg}(3x) + 2\sin(6x)$

s maximálním definičním oborem periodická? ◯

*5.145.* Nakreslete grafy funkcí

$f(x) = \mathrm{e}^{|x|}, \quad x \in \mathbb{R}; \qquad g(x) = \ln|x|, \quad x \in \mathbb{R} \setminus \{0\}$ . ◯

*5.146.* Načrtněte graf funkce

$$y = 2^{-|x|}, \quad x \in \mathbb{R}\,. \qquad ◯$$

*5.147.* Hyperbolickými funkcemi rozumíme

$$\sinh x = \frac{\mathrm{e}^x - \mathrm{e}^{-x}}{2},\ x \in \mathbb{R}; \qquad \cosh x = \frac{\mathrm{e}^x + \mathrm{e}^{-x}}{2},\ x \in \mathbb{R};$$
$$\operatorname{tgh} x = \frac{\sinh x}{\cosh x},\ x \in \mathbb{R}; \qquad \operatorname{cotgh} x = \frac{\cosh x}{\sinh x},\ x \in \mathbb{R} \setminus \{0\}.$$

Stanovte derivace těchto funkcí na jejich definičních oborech. ◯

*5.148.* V libovolném bodě $x \in \mathbb{R}$ vypočítejte derivaci argumentu hyperbolického sinu, tj. derivaci inverzní funkce (značené jako argsinh) k funkci $y = \sinh x$ na $\mathbb{R}$. ◯

**Poznámka.** Inverzní funkce k hyperbolickým funkcím $y = \cosh x$, $x \in [0, +\infty)$, $y = \operatorname{tgh} x$, $x \in \mathbb{R}$ a $y = \operatorname{cotgh} x$, $x \in (-\infty, 0) \cup (0, +\infty)$ se nazývají hyperbolometrické (řadíme k nim rovněž $y = \operatorname{argsinh} x$). Označují se po řadě argcosh, argtgh, argcotgh (čteme argument hyperbolického kosinu, argument hyperbolického tangens, argument hyperbolického kotangens) a jsou definovány pro $x \in [1, +\infty)$, $x \in (-1, 1)$, resp. $x \in (-\infty, -1) \cup (1, +\infty)$. Dodejme, že platí

$$(\operatorname{argcosh} x)' = \tfrac{1}{\sqrt{x^2-1}}, \quad x > 1,$$
$$(\operatorname{argtgh} x)' = \tfrac{1}{1-x^2}, \quad |x| < 1,$$
$$(\operatorname{argcotgh} x)' = \tfrac{1}{1-x^2}, \quad |x| > 1.$$

zadávajících inverzní funkce. Nebudeme zde uvádět seznam formulí, snadno se k nim dostaneme například v Maplu procedurou „series“. Pro ilustraci se podívejme alespoň na dva příklady:

Viděli jsme, že

$$\mathrm{e}^x = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \frac{1}{24}x^4 + \dots.$$

Protože je $\mathrm{e}^0 = 1$, budeme hledat pro inverzní funkci $\ln x$ mocninnou řadu se středem v $x = 1$, tj.

$$\ln x = a_0 + a_1(x-1) + a_2(x-1)^2 + a_3(x-1)^3 + a_4(x-1)^4 + \dots.$$

Využijeme tedy rovnosti $x = \mathrm{e}^{\ln x} = \ln(\mathrm{e}^x)$ a přeskupením koeficientů podle mocnin $x$ po dosazení příslušných řad dostaneme:

$$\begin{aligned} x &= a_0 + a_1\left(x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \frac{1}{24}x^4 + \dots\right) + \\ &\quad + a_2\left(x + \frac{1}{2}x^2 + \dots\right)^2 + a_3\left(x + \frac{1}{2}x^2 + \dots\right)^3 + \dots = \\ &= a_0 + a_1 x + \left(\frac{1}{2}a_1 + a_2\right)x^2 + \left(\frac{1}{6}a_1 + a_2 + a_3\right)x^3 + \\ &\quad + \left(\frac{1}{24}a_1 + \left(\frac{1}{4} + \frac{2}{6}\right)a_2 + \frac{3}{2}a_3 + a_4\right)x^4 + \dots. \end{aligned}$$

Porovnáním koeficientů u stejných mocnin nalevo a napravo

$$a_0 = 0,\ a_1 = 1,\ a_2 = -\frac{1}{2},\ a_3 = \frac{1}{3},\ a_4 = -\frac{1}{4}, \dots,$$

což skutečně odpovídá platnému výrazu (ověříme později):

$$\ln x = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(x-1)^n.$$

Podobně si můžeme pohrát s řadou

$$\sin t = t - \frac{1}{3!}t^3 + \frac{1}{5!}t^5 - \frac{1}{7!}t^7 + \dots$$

a zatím neznámou řadou pro její inverzi (všimněme si, že počítáme opět se středem v nule, protože je $\sin 0 = 0$)

$$\arcsin t = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + a_4 t^4 + \dots.$$

Opět dosazením dostáváme

$$\begin{aligned} t &= a_0 + a_1\left(t - \frac{1}{3!}t^3 + \frac{1}{5!}t^5 + \dots\right) + \\ &\quad + a_2\left(t - \frac{1}{3!}t^3 + \frac{1}{5!}t^5 + \dots\right)^2 + \dots = \\ &= a_0 + a_1 t + a_2 t^2 + \left(-\frac{1}{6}a_1 + a_3\right)t^3 + \\ &\quad + \left(-\frac{2}{6}a_2 + a_4\right)t^4 + \left(\frac{1}{120}a_1 - \frac{3}{6}a_3 + a_5\right)t^5 + \dots, \end{aligned}$$

a proto

$$\arcsin t = t + \frac{1}{6}t^3 + \frac{3}{40}t^5 + \dots.$$

**(3)** Všimněme si také, že kdybychom předpokládali, že funkci $\mathrm{e}^x$ skutečně můžeme napsat jako mocninnou řadu se středem v nule a že se mocninné řady derivují člen po členu, pak bychom snadno obdrželi diferenční rovnici pro koeficienty $a_n$. Víme totiž $(x^{n+1})' = (n+1)x^n$, a proto z našeho požadavku, že exponenciála má mít v každém bodě derivaci rovnou své hodnotě, vyplývá $a_{n+1} = \frac{1}{n+1}a_n$ a $a_0 = 1$, odkud již dostáváme $a_n = \frac{1}{n!}$.

**5.149.** Sečtěte:

$$2+1+\frac{2}{2!}+\frac{1}{3!}+\frac{2}{4!}+\frac{1}{5!}+\frac{2}{6!}+\cdots .$$

**Řešení.** Porovnáme-li tvar součtu s rozvojem funkcí sinh a cosh do mocninných řad, dostáváme výsledek

$$\sinh(1)+2\cosh(1) .$$ □

### K. Doplňující příklady k celé kapitole

*5.150.* Určete polynom $P(x)$ co nejmenšího stupně splňující podmínky $P(1) = 1$, $P(2) = 28$, $P(0) = 2$, $P'(0) = 1$, $P'(1) = 9$. ○

*5.151.* Určete polynom $P(x)$ co nejmenšího stupně splňující podmínky $P(0) = 0$, $P(1) = 4$, $P(-1) = -2$, $P'(0) = 1$, $P'(1) = 7$. ○

*5.152.* Určete polynom $P(x)$ co nejmenšího stupně splňující podmínky $P(0) = -1$, $P(1) = -1$, $P'(-1) = 10$, $P'(0) = -1$, $P'(1) = 6$. ○

*5.153.* Z definice limity dokažte, že je

$$\lim_{x\to 0}\left(x^3 - 2\right) = -2.$$

○

*5.154.* Z definice limity určete

$$\lim_{x\to -1}\frac{(1+x)^2 - 3}{2},$$

tj. napište $\delta(\varepsilon)$-předpis jako v minulém příkladu. ○

*5.155.* Ukažte z definice limity, že

$$\lim_{x\to -\infty}\frac{3\,(x-2)^4}{2} = +\infty.$$

○

*5.156.* Určete obě jednostranné limity

$$\lim_{x\to 0+}\operatorname{arctg}\frac{1}{x}, \qquad \lim_{x\to 0-}\operatorname{arctg}\frac{1}{x}.$$

Na základě výsledku rozhodněte o existenci limity

$$\lim_{x\to 0}\operatorname{arctg}\frac{1}{x}.$$

○

*5.157.* Existuje některá z limit

$$\lim_{x\to 0}\frac{\sin x}{x^3}, \qquad \lim_{x\to 0}\frac{5x^4+1}{x}\ ?$$

○

*5.158.* Vypočtěte limitu

$$\lim_{x\to 0}\frac{\operatorname{tg} x - \sin x}{\sin^3 x}.$$

○

*5.159.* Určete

$$\lim_{x\to \pi/6}\frac{2\sin^3 x + 7\sin^2 x + 2\sin x - 3}{2\sin^3 x + 3\sin^2 x - 8\sin x + 3}.$$

○

*5.160.* Pro libovolné $m, n \in \mathbb{N}$ určete

$$\lim_{x\to 1}\frac{x^m - 1}{x^n - 1}.$$

○

*5.161.* Určete

$$\lim_{x\to+\infty}\left(\sqrt{x^2+x}-x\right).$$

○

*5.162.* Stanovte

$$\lim_{x\to+\infty}\left(x\sqrt{1+x^2}-x^2\right).$$

○

*5.163.* Vypočítejte

$$\lim_{x\to 0}\frac{\sqrt{2}-\sqrt{1+\cos x}}{\sin^2 x}.$$

○

*5.164.* Určete

$$\lim_{x\to 0}\frac{\sin(4x)}{\sqrt{x+1}-1}.$$

○

*5.165.* Spočtěte

$$\lim_{x\to 0-}\frac{\sqrt{1+\operatorname{tg} x}-\sqrt{1-\operatorname{tg} x}}{\sin x}.$$

○

*5.166.* Stanovte

$$\lim_{x\to-\infty}\frac{2^x+\sqrt{1+x^2-x^9}-7x^5+44x^2}{3^x+\sqrt[5]{6x^6+x^2}-18x^5-592x^4}.$$

○

*5.167.* Nechť $\lim_{x\to-\infty} f(x) = 0$. Je pravda, že $\lim_{x\to-\infty}(f(x)\cdot g(x)) = 0$ pro každou rostoucí funkci $g:\mathbb{R}\to\mathbb{R}$? ○

*5.168.* Určete limitu

$$\lim_{n\to\infty}\left(\frac{n}{n+5}\right)^{2n-1}.$$

○

*5.169.* Spočítejte

$$\lim_{x\to 0-}\frac{\sin x - x}{x^3}.$$

○

*5.170.* Pro $x >$ e určete znaménko derivace funkce

$$f(x) = \operatorname{arctg}\frac{\ln x}{-1+\ln x}.$$

○

*5.171.* Stanovte všechna lokální maxima a minima funkce

$$y = x\ln^2 x$$

definované na intervalu $(0,+\infty)$. ○

*5.172.* Existuje $a\in\mathbb{R}$, pro které má funkce $y = ax+\sin x$ v bodě $x_0 = 5\pi/4$ absolutní minimum na intervalu $[0,2\pi]$? ○

*5.173.* Nalezněte absolutní minimální hodnotu, jež v nějakém bodě svého definičního oboru nabývá funkce

$$y = \mathrm{e}\,x - \ln x, \quad x > 0.$$

○

*5.174.* Určete maximální hodnotu funkce

$$y = \sqrt[3]{3x}\,\mathrm{e}^{-x}, \quad x \in \mathbb{R}.$$

○

*5.175.* Stanovte absolutní extrémy polynomu $p(x) = x^3 - 3x + 2$ na intervalu $[-3, 2]$. ○

*5.176.* Nechť je uražená vzdálenost (v metrech) hmotného tělesa popsána funkcí

$$s(t) = -(t-3)^2 + 16, \quad t \in [0, 7],$$

kde $t$ je čas v sekundách. Stanovte

(a) počáteční (tj. v čase $t = 0\,\mathrm{s}$) rychlost tělesa;
(b) čas a polohu, ve kterých má těleso nulovou rychlost;
(c) rychlost a zrychlení tělesa v čase $t = 4\,\mathrm{s}$.

Doplňme, že rychlost je derivace dráhy a zrychlení je derivace rychlosti. ○

*5.177.* Z definice derivace $f'$ funkce $f$ v bodě $x_0$ spočtěte $f'$ pro $f(x) = \sqrt{x}$ v libovolném bodě $x_0 > 0$. ○

*5.178.* Rozhodněte o existenci derivace funkce

$$f(x) = x \operatorname{arctg} \frac{1}{x}, \quad x \in \mathbb{R} \setminus \{0\}, \qquad f(0) = 0$$

v bodě $x_0 = 0$. ○

*5.179.* Má funkce

$$y = \sin\left(\operatorname{arctg}\left(\left|\,12x^{21} + 11\,\right| \cdot \frac{\mathrm{e}^{\cos(x+2)-x^3}}{-11 - x^{12}}\right)\right) + \sin(\sin(\sin(\sin x))), \ x \in \mathbb{R}$$

derivaci v bodě $x_0 = \pi^3 + 3^\pi$? ○

*5.180.* Zjistěte, jestli má funkce

$$f(x) = \left(x^2 - 1\right) \sin \tfrac{1}{x+1}, \quad x \neq -1\,(x \in \mathbb{R}), \qquad f(-1) = 0$$

derivaci v bodě $x_0 = -1$. ○

*5.181.* Udejte příklad funkce $f : \mathbb{R} \to \mathbb{R}$, která je spojitá na celé reálné ose, ale v bodech $x_1 = 5$, $x_2 = 9$ nemá derivaci. ○

*5.182.* Uveďte funkce $f$ a $g$, které nemají derivaci v žádném reálném bodě, ale jejich kompozice $f \circ g$ má derivaci na celé reálné přímce. ○

*5.183.* Pomocí základních vzorců spočtěte derivaci funkce

(a) $y = \left(2 - x^2\right)\cos x + 2x \sin x, \quad x \in \mathbb{R}$;
(b) $y = \sin\left(\sin x\right), \quad x \in \mathbb{R}$;
(c) $y = \sin\left(\ln\left(x^3 + 2x\right)\right), \quad x \in (0, +\infty)$;
(d) $y = \frac{1+x-x^2}{1-x+x^2}, \quad x \in \mathbb{R}$.

○

*5.184.* Libovolným způsobem určete derivaci funkce

(a) $y = \sqrt{x\sqrt{x\sqrt{x}}}, \quad x \in (0, +\infty);$

(b) $y = \ln\left|\operatorname{tg}\frac{x}{2}\right|, \quad x \in \mathbb{R} \setminus \{n\pi;\ n \in \mathbb{Z}\}.$

○

*5.185.* Napište derivaci funkce

$$y = \sin(\sin(\sin x)), \quad x \in \mathbb{R}.$$

○

*5.186.* Pro funkci

$$f(x) = \arccos\tfrac{1-x}{\sqrt{2}} + \sqrt[3]{x^3}$$

s největším možným definičním oborem vypočítejte $f'$ na maximální podmnožině reálných čísel, kde tato derivace existuje. ○

*5.187.* V libovolném bodě $x \notin \{n\pi;\ n \in \mathbb{Z}\}$ určete první derivaci funkce $y = \sqrt[3]{\sin x}$. ○

*5.188.* Pro $x \in \mathbb{R}$ derivujte výraz

$$x\sqrt{1+x^2} + \mathrm{e}^x\left(x^2 - 2x + 2\right).$$

○

*5.189.* Vyčíslete $f'(1)$, je-li

$$f(x) = (x-1)(x-2)^2(x-3)^3, \quad x \in \mathbb{R}.$$

○

*5.190.* Stanovte derivaci funkce

$$y = \sqrt[3]{\tfrac{1+x^3}{1-x^3}}, \quad |x| \neq 1\ (x \in \mathbb{R}).$$

○

*5.191.* Derivujte (v reálné proměnné $x$)

$$x\,\ln^2\left(x + \sqrt{1+x^2}\right) - 2\sqrt{1+x^2}\,\ln\left(x + \sqrt{1+x^2}\right) + 2x$$

všude, kde derivace existuje. Obdržený výraz zjednodušte. ○

*5.192.* Určete $f'$ na maximální množině, jestliže $f(x) = \log_x \mathrm{e}$. ○

*5.193.* Vyjádřete derivaci součinu čtyř funkcí

$$\left[f(x)g(x)h(x)k(x)\right]'$$

ve tvaru součtu součinů daných funkcí či jejich derivací za předpokladu, že všechny tyto funkce mají derivaci. ○

*5.194.* Uveďte derivaci funkce

$$y = \frac{x^3\,(x+1)^2\sqrt[3]{x+2}}{(x+3)^2}$$

pro $x > 0$. ○

**5.195.** Vrtulník dálniční hlídky letí 3 km nad rovnou silnicí rychlostí 120 km/h. Pilot zaměří radarem auto jedoucí proti směru letu vrtulníku a naměří, že auto se při vzdušné vzdálenosti 5 km od vrtulníku k němu přibližuje rychlostí 160 km/h. Spočítejte rychlost auta (vůči předmětu pohozenému na vozovce).

**Řešení.** Pro jednoduchost budeme v celém příkladu vynechávat fyzikální jednotky, a to kilometry pro dráhu a hodiny pro čas (rychlost tedy bude v km/h). Pozici vrtulníku v čase $t$ vyjádřeme bodem $[y(t), 3]$ a auta potom bodem $[x(t), 0]$; tj. 1 jednotka na osách odpovídá 1 km a současně osy volíme tak, aby „auto jelo po ose $x$“. Jako $s(t)$ označme vzdušnou vzdálenost vrtulníku od auta a jako $t_0$ ten časový okamžik, ze kterého jsou údaje v zadání. Spočtěme rychlost auta vzhledem k předmětu umístěnému do počátku soustavy souřadnic. Můžeme předpokládat, že $x(t) > y(t) > 0$. Za tohoto předpokladu je $x'(t) \le 0$, $y'(t) \ge 0$ pro uvažovaná $t$. Auto se totiž blíží k bodu $[0, 0]$ zprava – hodnota $x(t)$ se zmenšuje pro zvětšující se $t$, a tudíž $x'(t) \le 0$. Podobně dostáváme $y'(t) \ge 0$ a také $s'(t) \le 0$. Ještě dodejme, že např. $y'(t)$ udává, jak rychle se mění funkce $y$ v čase $t$, tedy rychlost vrtulníku.

Víme, že je

$$s(t_0) = 5, \quad s'(t_0) = -160, \quad y'(t_0) = 120$$

a že platí ($s(t)$ je přepona pravoúhlého trojúhelníku)

$$(x(t) - y(t))^2 + 3^2 = s^2(t). \tag{5.1}$$

Odtud plyne ($x(t) > y(t) > 0$)

$$(x(t_0) - y(t_0))^2 + 3^2 = 5^2, \quad \text{tj.} \quad x(t_0) - y(t_0) = 4.$$

Derivováním identity (‖5.1‖) získáváme

$$2\,(x(t) - y(t))\,\big(x'(t) - y'(t)\big) = 2s(t)s'(t)$$

a následně pro $t = t_0$

$$2 \cdot 4\,\big(x'(t_0) - 120\big) = 2 \cdot 5 \cdot (-160), \quad \text{tj.} \quad x'(t_0) = -80.$$

Vypočítali jsme, že auto se blíží k předmětu na vozovce rychlostí 80 km/h. Stačí si uvědomit, s jakými jednotkami jsme pracovali. To, že jsme jako výsledek obdrželi zápornou hodnotu, je pak zapříčiněno naší volbou souřadnicového umístění. □

**5.196.** Do rovnoramenného trojúhelníku o základně $z$ a výšce $v$ (nad základnou) vepište obdélník (jedna jeho strana bude částí základny trojúhelníku) s největším obsahem. Stanovte obsah $S$ tohoto obdélníku.

**Řešení.** Pro vyřešení příkladu postačuje uvažovat úlohu, kdy se snažíme vepsat do pravoúhlého trojúhelníku s odvěsnami délek $z/2$ a $v$ obdélník s maximálním možným obsahem, přičemž dvě jeho strany musí být částmi odvěsen tohoto trojúhelníku. Úlohu takto převedeme na otázku maximalizace funkce proměnné $x$ (délka strany hledaného obdélníka):

$$f(x) = x\left(v - \tfrac{2vx}{z}\right)$$

na intervalu $I = [0, z/2]$. Neboť je

$$f'(x) = v - \tfrac{4vx}{z} \quad \text{pro všechna } x \in I$$

a dále

$$f(0) = f\left(\tfrac{z}{2}\right) = 0, \qquad f(x) \geq 0, \quad x \in I,$$

v jediném svém stacionárním bodě $x_0 = z/4$ nutně nabývá funkce $f$ maxima na $I$. Proto jsou strany hledaného obdélníku dlouhé $z/2$ (dvojnásobek $x_0$: uvažujeme původní úlohu) a $v/2$ (to lze získat dosazením $z/4$ za $x$ do výrazu $v - 2vx/z$). Odsud dostáváme, že $S = vz/4$. □

**5.197.** Mezi obdélníky, jejichž dva vrcholy leží na ose $x$ a další dva s kladnými druhými souřadnicemi na parabole $y = 8 - 2x^2$, najděte obdélník s maximálním obsahem.

**Řešení.** Základna obdélníku s maximálním obsahem měří $4/\sqrt{3}$, jeho výška pak $16/3$. Tento výsledek lze obdržet nalezením absolutního maxima funkce

$$S(x) = 2x\left(8 - 2x^2\right)$$

na intervalu $I = [0, 2]$. Neboť tato funkce je na $I$ nezáporná, v krajních bodech $I$ nulová a má derivaci na celém $I$, přičemž její derivace je nulová pouze v jednom bodě intervalu $I$, a to v bodě $x = 2/\sqrt{3}$, nabývá zde maximální hodnoty. □

**5.198.** Pro jaká $a \in \mathbb{R}$ je kubický polynom $P$ vyhovující vztahům $P(0) = 1$, $P'(0) = 1$, $P(1) = 2a + 2$, $P'(1) = 5a + 1$, monotónní funkcí na celém $\mathbb{R}$?

**Řešení.** Z podmínek $P(0) = 1$ a $P'(0) = 1$ plyne, že $P(x) = bx^3 + cx^2 + x + 1$, kde $b, c \in \mathbb{R}$, zbylé dvě podmínky určují dvě rovnice pro neznámé $b$ a $c$: $b+c+2 = 2a+2, 3b+2c+1 = 5a+1$ s jediným řešením $b = c = a$, polynomy vyhovující zadaným vztahům jsou tedy tvaru $P(x) = ax^3 + ax^2 + x + 1$, $a \in \mathbb{R}$. Podmínka na to, aby byl monotónní funkcí na celém $\mathbb{R}$, je ekvivalentní tomu, že polynom nemá lokální extrém. Extrémy mohou nastat v kritických bodech, tedy v bodech, kde jeho derivace mění znaménko. Pokud tedy derivace nebude na celém $\mathbb{R}$ měnit znaménko, funkce bude monotónní. Derivace je

$$P'(x) = 3ax^2 + 2ax + 1$$

a nebude měnit znaménko, bude-li její diskriminant nekladný. Dostáváme tedy podmínku

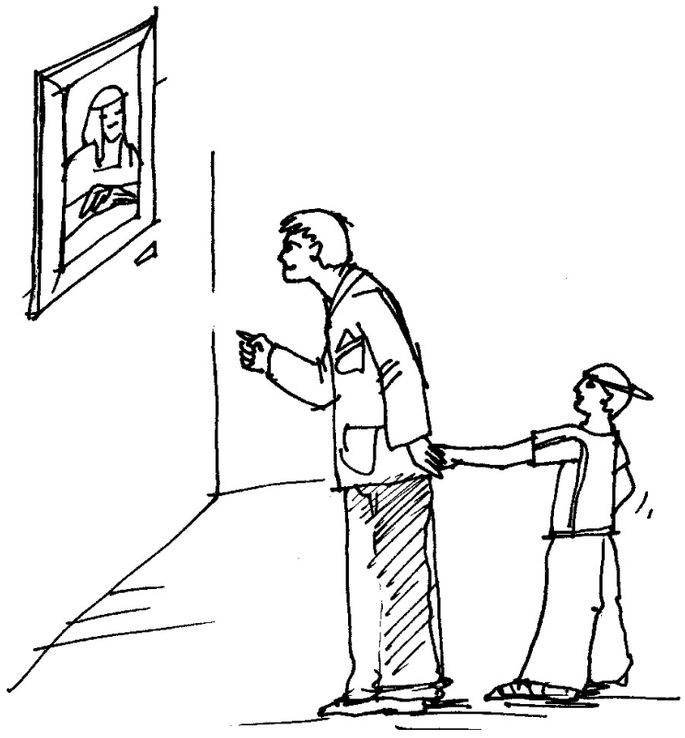
$$\begin{aligned} 4a^2 - 12a &\leq 0, \\ 4a(a-3) &\leq 0, \end{aligned}$$

což odpovídá $a \in [0, 3]$. Pro $a = 0$ však $P$ sice je monotónní funkcí, nikoliv však kubickým polynomem. Dané podmínky splňují právě $a \in (0, 3]$. □

**5.199. Regiomontanův problém, 1471.** V muzeu na stěně visí obraz. Jeho dolní okraj je $a$ metrů

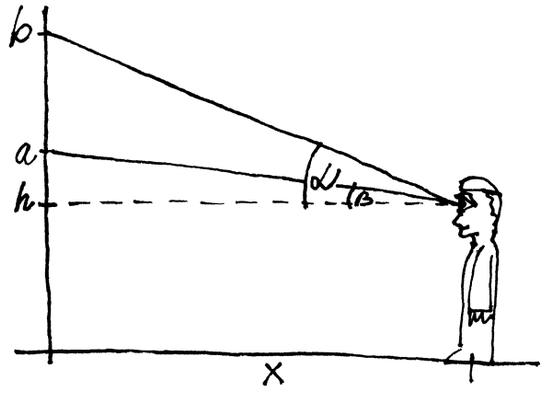


nad zemí a horní okraj pak $b$ metrů nad zemí (tj. výška obrazu je $b - a$). Na obraz se dívá turista, jehož oči jsou ve výšce $h < a$ metrů nad zemí. (Důvodem nerovnosti $h < a$ může např. být, že se tak dá umožnit výhled stejně vysokým návštěvníkům muzea stojícím v několika řadách.) Jak daleko od stěny má turista stát, aby maximalizoval velikost svého úhlu pohledu na obraz?



**Řešení.** Jako $x$ označme vzdálenost (v metrech) turisty od stěny a jako $\varphi$ jeho úhel pohledu na obraz. Dále zaveďme úhly $\alpha, \beta \in (0, \pi/2)$ vztahy

$$\operatorname{tg}\alpha = \tfrac{b-h}{x}, \qquad \operatorname{tg}\beta = \tfrac{a-h}{x}.$$




Naším úkolem je maximalizovat $\varphi = \alpha - \beta$. Doplňme, že pro $h > b$ lze postupovat analogicky a že pro $h \in [a, b]$ se zřejmě úhel $\varphi$ stále zvětšuje při zmenšujícím se $x$ ($\varphi = \pi$ pro $x = 0$ a $h \in (a, b)$).

Z podmínky $h < a$ plyne, že úhel $\varphi$ je ostrý, tj. $\varphi \in (0, \pi/2)$. Protože je funkce $y = \operatorname{tg} x$ rostoucí na intervalu $(0, \pi/2)$, můžeme přejít k maximalizování hodnoty $\operatorname{tg}\varphi$. Platí

$$\operatorname{tg}\varphi = \operatorname{tg}\,(\alpha - \beta) = \tfrac{\operatorname{tg}\alpha - \operatorname{tg}\beta}{1+\operatorname{tg}\alpha\operatorname{tg}\beta} = \tfrac{\frac{b-h}{x} - \frac{a-h}{x}}{1+\frac{b-h}{x}\cdot\frac{a-h}{x}} = \tfrac{x(b-a)}{x^2+(b-h)(a-h)}.$$

Stačí nám tedy najít globální maximum funkce

$$f(x) = \tfrac{x(b-a)}{x^2+(b-h)(a-h)}, \qquad x \in [0, +\infty).$$

Z vyjádření

$$f'(x) = \frac{(b-a)\left[x^2+(b-h)(a-h)\right]-2x^2(b-a)}{\left[x^2+(b-h)(a-h)\right]^2} = \frac{(b-a)\left[(b-h)(a-h)-x^2\right]}{\left[x^2+(b-h)(a-h)\right]^2}, \quad x \in (0,+\infty),$$

vidíme, že

$$f'(x) > 0 \quad \text{pro} \quad x \in \left(0, \sqrt{(b-h)(a-h)}\right),$$
$$f'(x) < 0 \quad \text{pro} \quad x \in \left(\sqrt{(b-h)(a-h)}, +\infty\right).$$

Funkce $f$ má proto globální maximum v bodě $x_0 = \sqrt{(b-h)(a-h)}$ (připomeňme nerovnosti $h < a < b$).

Určit bod $x_0$ lze samozřejmě i jinými způsoby. Můžeme např. místo hledání maxima kladné funkce $f$ na intervalu $(0,+\infty)$ pomocí diferenciálního počtu hledat globální minimum funkce

$$g(x) = \frac{1}{f(x)} = \frac{x^2+(b-h)(a-h)}{x(b-a)} = \frac{x}{b-a} + \frac{(b-h)(a-h)}{x(b-a)}, \qquad x \in (0,+\infty)$$

využitím tzv. A-G nerovnosti (mezi aritmetickým a geometrickým průměrem)

$$\frac{y_1+y_2}{2} \geq \sqrt{y_1\, y_2}, \qquad y_1, y_2 \geq 0,$$

ve které rovnost nastává právě pro $y_1 = y_2$. Volba

$$y_1(x) = \frac{x}{b-a}, \qquad y_2(x) = \frac{(b-h)(a-h)}{x(b-a)}$$

totiž dává

$$g(x) = y_1(x) + y_2(x) \geq 2\sqrt{y_1(x)\, y_2(x)} = \frac{2}{b-a}\sqrt{(b-h)\,(a-h)}.$$

Pokud tak existuje $x > 0$, pro které je $y_1(x) = y_2(x)$, má funkce $g$ v bodě $x$ globální minimum. Rovnice

$$y_1(x) = y_2(x), \quad \text{tj.} \quad \frac{x}{b-a} = \frac{(b-h)(a-h)}{x(b-a)},$$

má jediné kladné řešení $x_0 = \sqrt{(b-h)(a-h)}$.

Dvěma odlišnými způsoby jsme stanovili ideální vzdálenost turisty od stěny. Hodnotě $x_0$ odpovídá

$$\varphi_0 = \operatorname{arctg} \frac{x_0(b-a)}{x_0^2+(b-h)(a-h)} = \operatorname{arctg} \frac{b-a}{2\sqrt{(b-h)(a-h)}}.$$

Při pohledu z úrovně podlahy (kdyby se díval brouk) je $h = 0$, a tudíž je

$$x_0 = \sqrt{ab}, \qquad \varphi_0 = \operatorname{arctg} \frac{b-a}{2\sqrt{ab}}.$$

Je-li obraz vysoký 1 m a jeho dolní okraj je 2 m nad zemí ($a = 2$, $b = 3$), bude brouk vidět obraz pod největším úhlem $\varphi_0 \doteq 0{,}201\,4$ rad $\approx 11{,}5\,^\circ$ ve vzdálenosti $x_0 \doteq 2{,}45$ m od stěny. Pokud si bude stejný obraz prohlížet muž, který má oči ve výšce 1,8 m, se svým synem, který má oči ve výšce 1 m, měl by otec stát ve vzdálenosti $x_0 \doteq 0{,}49$ m a syn ve vzdálenosti $x_0 \doteq 1{,}41$ m. Všimněme si, že pro otce je $\varphi_0 \doteq 0{,}795\,6$ rad $\approx 45{,}6\,^\circ$, zatímco pro jeho syna je $\varphi_0 \doteq 0{,}339\,8$ rad $\approx 19{,}5\,^\circ$. Poměr

$$\frac{0795\,6}{0339\,8} \approx \frac{456}{195} \doteq 2{,}3$$

dokládá, jak výrazně má otec lepší výhled. □

**5.200. Halleyova úloha, 1686.** Hráč stojí před basketbalovým košem ve vzdálenosti $l$ od obroučky, která je ve výšce $h$ nad bodem odhodu. Určete minimální počáteční rychlost $v_0$, kterou musí udělit míči, aby skóroval, a příslušný elevační úhel $\varphi$ pro toto $v_0$.



**Řešení.** Opět vynecháváme fyzikální jednotky: můžeme předpokládat, že údaje o vzdálenostech jsou uváděny v metrech a časové údaje v sekundách (rychlosti pak v metrech za sekundu). Nechť hráč hodí míč v čase $t = 0$ a nechť míč projde obroučkou v čase $t_0 > 0$. Pozici míče (během jeho letu) vyjádříme body $[x(t), y(t)]$ pro $t \in [0, t_0]$, přičemž požadujeme, aby $x(0) = 0$, $y(0) = 0$, $x(t_0) = l$, $y(t_0) = h$.

Zřejmě je

$$x'(t) = v_0 \cos\varphi, \qquad y'(t) = v_0 \sin\varphi - gt$$

pro $t \in (0, t_0)$, kde $g$ je normální tíhové zrychlení (konstanta gravitačního zrychlení). Hodnoty $x'(t)$ a $y'(t)$ totiž po řadě udávají horizontální a vertikální rychlost míče. Integrováním těchto rovnic získáme

$$x(t) = v_0 t \cos\varphi + c_1, \qquad y(t) = v_0 t \sin\varphi - \tfrac{1}{2} gt^2 + c_2$$

pro $t \in (0, t_0)$ a $c_1, c_2 \in \mathbb{R}$. Z počátečních podmínek

$$\lim_{t\to 0+} x(t) = x(0) = 0, \qquad \lim_{t\to 0+} y(t) = y(0) = 0$$

plyne, že $c_1 = c_2 = 0$. Dosazení zbývajících podmínek

$$\lim_{t\to t_0-} x(t) = x(t_0) = l, \qquad \lim_{t\to t_0-} y(t) = y(t_0) = h$$

tak již dává

$$l = v_0 t_0 \cos\varphi, \qquad h = v_0 t_0 \sin\varphi - \tfrac{1}{2} g t_0^2.$$

Podle první rovnice je

$$t_0 = \frac{l}{v_0 \cos\varphi}, \tag{5.2}$$

a tudíž dostáváme jedinou rovnici

$$h = l \operatorname{tg}\varphi - \frac{g l^2}{2 v_0^2 \cos^2\varphi}, \tag{5.3}$$

přičemž $v_0 \in (0, +\infty)$, $\varphi \in (0, \pi/2)$.

Zopakujme, že naším úkolem je stanovit minimální $v_0$ a odpovídající $\varphi$, které této rovnici vyhovuje. Řečeno srozumitelněji, chceme určit minimální hodnotu $v_0$, pro kterou bude existovat $\varphi$ splňující (‖5.3‖). Neboť

$$\frac{1}{\cos^2\varphi} = \frac{\cos^2\varphi + \sin^2\varphi}{\cos^2\varphi} = 1 + \operatorname{tg}^2\varphi, \qquad \varphi \in \left(0, \frac{\pi}{2}\right),$$

rovnici (‖5.3‖) můžeme převést do tvaru

$$h - l \operatorname{tg}\varphi + \frac{g l^2}{2 v_0^2}\left(1 + \operatorname{tg}^2\varphi\right) = 0,$$

tj.

$$\operatorname{tg}^2\varphi - \frac{2 v_0^2}{gl} \operatorname{tg}\varphi + \frac{2 h v_0^2}{g l^2} + 1 = 0.$$

Z poslední rovnice (kvadratické rovnice pro neznámou $p = \operatorname{tg}\varphi$) vyplývá, že

$$\operatorname{tg}\varphi = \frac{\frac{2v_0^2}{gl} \pm \sqrt{\frac{4v_0^4}{g^2 l^2} - 4\left(\frac{2hv_0^2}{gl^2} + 1\right)}}{2},$$

tj.

$$\operatorname{tg}\varphi = \frac{v_0^2}{gl} \pm \frac{\sqrt{v_0^4 - 2hv_0^2 g - g^2 l^2}}{gl}. \tag{5.4}$$

Úhel $\varphi$ splňující (‖5.3‖) tedy existuje, právě když je

$$v_0^4 - 2gh\, v_0^2 - g^2 l^2 \geq 0.$$

Také nyní nám substituce (tentokráte $q = v_0^2$) umožní přejít ke kvadratickému výrazu (na levé straně nerovnice) a následně získat

$$\left(v_0^2 - g\left[h + \sqrt{h^2 + l^2}\right]\right)\left(v_0^2 - g\left[h - \sqrt{h^2 + l^2}\right]\right) \geq 0.$$

Protože $h < \sqrt{h^2 + l^2}$, musí být

$$v_0^2 \geq g\left[h + \sqrt{h^2 + l^2}\right], \quad \text{tj.} \quad v_0 \geq \sqrt{g\left[h + \sqrt{h^2 + l^2}\right]}.$$

Nejmenší přípustné hodnotě

$$v_0 = \sqrt{g\left[h + \sqrt{h^2 + l^2}\right]} \tag{5.5}$$

potom odpovídá (viz (‖5.4‖))

$$\operatorname{tg}\varphi = \frac{v_0^2}{gl} = \frac{h + \sqrt{h^2 + l^2}}{l}, \quad \text{tj.} \quad \varphi = \operatorname{arctg}\frac{h + \sqrt{h^2 + l^2}}{l}. \tag{5.6}$$

Předchozí výpočet byl ovšem založen na podmínkách $x(t_0) = l$, $y(t_0) = h$, které pouze udávají požadovanou polohu v čase $t_0$. Míč však mohl projít obroučkou zespodu. Doplňme proto podmínku $y'(t_0) < 0$, která říká, že míč v čase $t_0$ už klesal, a dokažme, že je pro $v_0$ z (‖5.5‖) a $\varphi$ z (‖5.6‖) splněna.

Připomeňme, že je (viz (‖5.2‖), (‖5.3‖))

$$t_0 = \frac{l}{v_0 \cos\varphi}, \qquad v_0^2 = \frac{gl^2}{2\,(l \operatorname{tg}\varphi - h)\cos^2\varphi}.$$

Využitím toho z

$$y'(t_0) = \lim_{t \to t_0 -} y'(t) = v_0 \sin\varphi - gt_0 < 0$$

dostáváme

$$\frac{gl^2}{2\,(l \operatorname{tg}\varphi - h)\cos^2\varphi} = v_0^2 < v_0 \cdot \frac{gt_0}{\sin\varphi} = \frac{gl}{\sin\varphi\,\cos\varphi},$$

tj. nerovnici

$$l\,\sin\varphi\,\cos\varphi < 2(l \operatorname{tg}\varphi - h)\cos^2\varphi,$$

z níž snadno vyjádříme

$$\frac{2h}{l} < \operatorname{tg}\varphi.$$

Porovnáním s (‖5.6‖) vidíme, že poslední nerovnost je splněna, neboť

$$\operatorname{tg}\varphi = \frac{h + \sqrt{h^2 + l^2}}{l} > \frac{h + \sqrt{h^2}}{l} = \frac{2h}{l}.$$

Tím jsme ukázali, že při počáteční rychlosti uvedené v (‖5.5‖) může hráč koš dát.

Při trestném hodu, kdy hráč odhazuje míč ve výšce 2 m, je

$$h = 1{,}05\ \text{m}, \quad l = 4{,}225\ \text{m}, \quad g = 9{,}806\,65\ \text{m}\cdot\text{s}^{-2},$$

a tudíž minimální počáteční rychlost míče činí

$$v_0 = \sqrt{9{,}806\,65\left[1{,}05 + \sqrt{(1{,}05)^2 + (4{,}225)^2}\right]}\ \text{m}\cdot\text{s}^{-1} \doteq$$
$$\doteq 7{,}28\ \text{m}\cdot\text{s}^{-1}.$$

Této rychlosti odpovídá úhel

$$\varphi = \operatorname{arctg}\frac{v_0^2}{9{,}806\,65 \cdot 4{,}225} \doteq 0{,}907\ \text{rad} \approx 52\,^\circ.$$

Zamysleme se ještě nad získanou hodnotou úhlu $\varphi$ pro minimální rychlost $v_0$. Podle obrázku je

$$2\beta + (\pi - \alpha) = \pi \qquad \text{a} \qquad \alpha + \gamma = \tfrac{\pi}{2},$$

odkud vyplývá

$$\beta = \frac{\alpha}{2} = \frac{\pi}{4} - \frac{\gamma}{2}.$$

Platí tedy

$$\varphi = \frac{\pi}{2} - \beta = \frac{\pi}{4} + \frac{\gamma}{2} = \frac{1}{2}\left(\frac{\pi}{2} + \gamma\right) = \frac{1}{2}\left(\frac{\pi}{2} + \operatorname{arctg}\frac{h}{l}\right).$$

Obdrželi jsme, že elevační úhel při hodu s minimální energií je aritmetickým průměrem pravého úhlu a úhlu pohledu na obroučku (z pozice míče).



Problém stanovení minimální nutné rychlosti odhazovaného míče vlastně vyřešil Edmond Halley už v roce 1686, když určil minimální potřebné množství střelného prachu k tomu, aby vystřelená dělová koule mohla zasáhnout cíl na výše položeném místě (např. za hradbami). Halley dokázal (tzv. Halleyovo kalibrační pravidlo), že pro zasažení cíle v bodě $[l, h]$ při střelbě z pozice $[0, 0]$ je potřeba stejné minimální množství prachu jako pro zasažení horizontálního cíle ve vzdálenosti $h + \sqrt{h^2 + l^2}$ (při úhlu $\varphi = 45\,^\circ$). Halley také prokázal, že hodnota $\varphi$ je stabilní vzhledem k malým odchylkám množství použitého střelného prachu a nevýrazným chybám v odhadu vzdálenosti cíle. □

**5.201.** Projektil je vystřelen pod úhlem $\varphi$ z bodu ve výšce $h$ nad zemí s počáteční rychlostí $v_0$. Dopadne na zem ve vzdálenosti $R$ od místa výstřelu. Stanovte úhel $\varphi$, při kterém bude hodnota $R$ maximální.



**Řešení.** Pozici projektilu v čase vyjádříme body $[x(t), y(t)]$. Předpokládáme, že projektil byl vystřelen v čase $t = 0$ z bodu $[0, 0]$ a dopadne na zem v bodě $[R, -h]$ v jistém čase $t = t_0$, tj. $x(0) = 0$, $y(0) = 0$, $x(t_0) = R$, $y(t_0) = -h$. Podobně jako v Halleyově úloze uvažujme rovnice

$$x'(t) = v_0 \cos\varphi, \qquad y'(t) = v_0 \sin\varphi - gt, \qquad t \in (0, t_0)$$

pro horizontální a vertikální rychlost projektilu, kde $g$ je normální tíhové zrychlení.

I nadále můžeme pokračovat jako při řešení Halleyovy úlohy, kdy integrováním těchto rovnic se zohledněním $x(0) = y(0) = 0$ získáme

$$x(t) = v_0 t \cos\varphi, \qquad y(t) = v_0 t \sin\varphi - \tfrac{1}{2} g t^2, \qquad t \in (0, t_0)$$

a z podmínek

$$\lim_{t \to t_0-} x(t) = x(t_0) = R, \lim_{t \to t_0-} y(t) = y(t_0) = -h$$

poté

$$R = v_0 t_0 \cos\varphi, \qquad -h = v_0 t_0 \sin\varphi - \tfrac{1}{2} g t_0^2.$$

Z první rovnice plyne

$$t_0 = \frac{R}{v_0 \cos\varphi},$$

a tak můžeme předchozí dvě rovnice vyjádřit jedinou rovnicí

$$-h = R\,\mathrm{tg}\,\varphi - \frac{gR^2}{2v_0^2\cos^2\varphi}, \tag{5.7}$$

přičemž $\varphi \in (0, \pi/2)$.

Na rozdíl od Halleyovy úlohy je však hodnota $v_0$ dána a měnné je $R$ v závislosti na $\varphi$. Je tak vlastně $R = R(\varphi)$ funkcí v proměnné $\varphi$, která musí splňovat (‖5.7‖) (je určena rovnicí (‖5.7‖)). Jedná se tedy o funkci zadanou implicitně. Rovnici (‖5.7‖) zapíšeme jako ($R$ nahradíme $R(\varphi)$)

$$R(\varphi)\,\mathrm{tg}\,\varphi \cdot 2v_0^2\cos^2\varphi - gR^2(\varphi) + h \cdot 2v_0^2\cos^2\varphi = 0.$$

Využitím vztahu

$$2\,\mathrm{tg}\,\varphi\cos^2\varphi = \sin 2\varphi$$

pak (‖5.7‖) převedeme do tvaru

$$R(\varphi)v_0^2\sin 2\varphi - gR^2(\varphi) + 2hv_0^2\cos^2\varphi = 0. \tag{5.8}$$

Derivování podle $\varphi$ nyní dává

$$R'(\varphi)v_0^2\sin 2\varphi + 2R(\varphi)v_0^2\cos 2\varphi - 2gR(\varphi)R'(\varphi) - \\ - 2hv_0^2\,(2\cos\varphi\sin\varphi) = 0,$$

tj.

$$R'(\varphi)\left[v_0^2\sin 2\varphi - 2gR(\varphi)\right] = -2R(\varphi)v_0^2\cos 2\varphi + 2hv_0^2\sin 2\varphi.$$

Vypočítali jsme tak, že

$$R'(\varphi) = \frac{2v_0^2\,[h\sin 2\varphi - R(\varphi)\cos 2\varphi]}{v_0^2\sin 2\varphi - 2gR(\varphi)}, \qquad \varphi \in \left(0, \frac{\pi}{2}\right).$$

Stačí ověřit, že $v_0^2\sin 2\varphi - 2gR(\varphi) \neq 0$ pro každé $\varphi \in (0, \pi/2)$. Předpokládejme opak a dosaďme

$$R = \frac{v_0^2\sin 2\varphi}{2g} = \frac{v_0^2\sin\varphi\cos\varphi}{g}$$

do (‖5.7‖) se ziskem

$$-h = \frac{v_0^2\sin\varphi\cos\varphi}{g}\,\mathrm{tg}\,\varphi - \frac{gv_0^4\sin^2\varphi\cos^2\varphi}{2g^2v_0^2\cos^2\varphi}.$$

Jednoduchými úpravami odtud obdržíme

$$-h = \frac{v_0^2\sin^2\varphi}{2g},$$

což nemůže nastat (výraz na levé straně je záporný, na pravé kladný).

Podařilo se nám tedy určit $R'(\varphi)$ pro všechna $\varphi \in (0, \pi/2)$. Navíc je ihned vidět, že tato derivace je nulová, právě když

$$h\sin 2\varphi = R(\varphi)\cos 2\varphi, \qquad \text{tj.} \qquad R(\varphi) = h\,\mathrm{tg}\,2\varphi.$$

Neboť funkce $R$ zřejmě nabývá na intervalu $(0, \pi/2)$ maximální hodnoty (podle fyzikálního významu úlohy se pro $\varphi \to 0+$ nebo $\varphi \to \pi/2-$ hodnota $R$ zmenšuje) a má derivaci v každém bodě tohoto intervalu, maxima musí nabývat tam, kde je derivace nulová. To znamená, že $R(\varphi)$ může být maximální pouze tehdy, když je

$$R\,(\varphi) = h\,\mathrm{tg}\,2\varphi. \tag{5.9}$$

Dosaďme proto (‖5.9‖) do (‖5.8‖). Získáváme

$$h \operatorname{tg} 2\varphi \, v_0^2 \sin 2\varphi - gh^2 \operatorname{tg}^2 2\varphi + 2hv_0^2 \cos^2 \varphi = 0.$$

Tuto rovnici postupně upravíme

$$\begin{aligned}
\operatorname{tg} 2\varphi \, v_0^2 \sin 2\varphi + 2v_0^2 \cos^2 \varphi &= gh \operatorname{tg}^2 2\varphi, \\
v_0^2 \frac{\sin^2 2\varphi}{\cos 2\varphi} + v_0^2 (\cos 2\varphi + 1) &= gh \frac{\sin^2 2\varphi}{\cos^2 2\varphi}, \\
v_0^2 \sin^2 2\varphi + v_0^2 \cos^2 2\varphi + v_0^2 \cos 2\varphi &= gh \frac{\sin^2 2\varphi}{\cos 2\varphi}, \\
v_0^2 + v_0^2 \cos 2\varphi &= gh \frac{1 - \cos^2 2\varphi}{\cos 2\varphi}, \\
v_0^2 (1 + \cos 2\varphi) &= gh \frac{(1 - \cos 2\varphi)\ (1 + \cos 2\varphi)}{\cos 2\varphi}, \\
v_0^2 \cos 2\varphi &= gh \, (1 - \cos 2\varphi)\ , \\
\left(v_0^2 + gh\right) \cos 2\varphi &= gh, \\
\cos 2\varphi &= \frac{gh}{v_0^2 + gh}.
\end{aligned}$$

Tím jsme však už jednoznačně určili bod

$$\varphi_0 = \tfrac{1}{2} \arccos \tfrac{gh}{v_0^2 + gh},$$

ve kterém je $R$ největší. Protože

$$\sin 2\varphi_0 = \sqrt{1 - \cos^2 2\varphi_0} = \sqrt{1 - \frac{g^2 h^2}{\left(v_0^2 + gh\right)^2}} = \frac{\sqrt{v_0^4 + 2ghv_0^2}}{v_0^2 + gh},$$

je funkční hodnota

$$R(\varphi_0) = h \operatorname{tg} 2\varphi_0 = h \frac{\frac{\sqrt{v_0^4 + 2ghv_0^2}}{v_0^2 + gh}}{\frac{gh}{v_0^2 + gh}} = \frac{\sqrt{v_0^4 + 2ghv_0^2}}{g} = \frac{v_0}{g} \sqrt{v_0^2 + 2gh}.$$

Nechť např. oštěpařka Barbora Špotáková udělí oštěpu ve výši $h = 1{,}8$ m rychlost $v_0 = 27{,}778$ m/s $\doteq$ 100 km/h (při $g = 9{,}806\,65$ m $\cdot$ s$^{-2}$). Potom oštěp může doletět do vzdálenosti

$$R(\varphi_0) = \frac{27{,}778}{9{,}806\,65} \sqrt{27{,}778^2 + 2 \cdot 9{,}806\,65 \cdot 1{,}8}\ \text{m} \doteq 80{,}46\ \text{m}.$$

Této vzdálenosti by bylo dosaženo pro

$$\varphi_0 = \frac{1}{2} \arccos \frac{9{,}806\,65 \cdot 1{,}8}{27{,}778^2 + 9{,}806\,65 \cdot 1{,}8} \doteq 0{,}774\,2\ \text{rad} \approx 44{,}36\,^\circ.$$

Světový rekord Barbory Špotákové se ovšem hranici 80 m ani neblíží, přestože další vlivy (kupř. odpor vzduchu) lze zanedbat. Nesmíme však zapomenout, že IAAF (Mezinárodní asociace atletických federací) rozhodla o posunutí těžiště oštěpu směrem ke špičce k 1. dubnu 1999 (v ženském oštěpu), čímž se zkrátila vzdálenost hodů zhruba o 10 %. Původní rekord (se „správně vyváženým“ typem oštěpu) byl právě 80,00 m.



Provedené úvahy a získaný výsledek lze uplatnit také v jiných atletických disciplínách a sportech. Při golfu je třeba $h$ blízké 0, a tudíž právě při úhlu

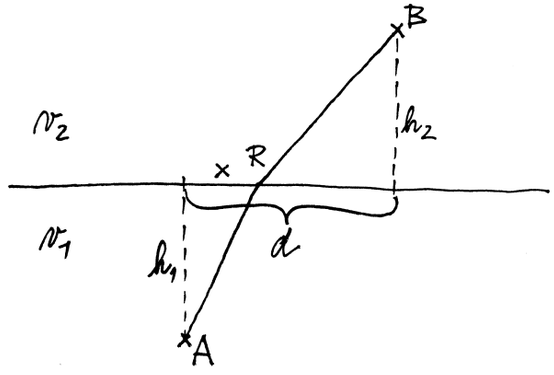
$$\varphi_0 = \lim_{h\to 0+} \frac{1}{2} \arccos \frac{gh}{v_0^2 + gh} = \frac{1}{2} \arccos 0 = \frac{\pi}{4} \text{ rad} = 45\,^\circ$$

míček dopadne do největší vzdálenosti

$$R(\varphi_0) = \lim_{h\to 0+} \frac{v_0}{g} \sqrt{v_0^2 + 2gh} = \frac{v_0^2}{g}.$$

Uvědomme si, že pro $h = 0$ nelze náš výpočet použít ($\varphi_0 = \pi/4$), neboť bychom pro vzdálenost $R$ dostali nedefinovaný výraz $\operatorname{tg}(\pi/2)$. My jsme však úlohu vyřešili pro libovolné $h > 0$, a proto jsme si mohli pomoci příslušnou jednostrannou limitou. □

**5.202. Snellův zákon.** Určete lomený světelný paprsek mezi bodem $A$ v homogenním prostředí s rychlostí šíření světla $v_1$ a bodem $B$ v homogenním prostředí s rychlostí šíření světla $v_2$.




**Řešení.** V celém příkladu nebudeme uvádět fyzikální jednotky: můžeme kupř. předpokládat, že údaje o vzdálenostech budou v metrech a rychlosti $v_1$, $v_2$ jsou v metrech za sekundu (čas bude vyjádřen v sekundách). Paprsek je určen principem minimálního času, kdy k přenosu energie elektromagnetickým vlněním mezi body $A$ a $B$ dochází takovým způsobem, aby se odehrál v co nejkratším čase. V homogenních prostředích bude paprsek úsečkou. Stačí tedy stanovit bod $R$ (určený hodnotou $x$), kde dojde k lomu. Vzdálenost mezi body $A$ a $R$ činí $\sqrt{h_1^2 + x^2}$ a mezi body $R$ a $B$ pak $\sqrt{h_2^2 + (d-x)^2}$. Celková doba přenosu energie mezi body $A$ a $B$ je tak dána funkcí

$$T(x) = \frac{\sqrt{h_1^2+x^2}}{v_1} + \frac{\sqrt{h_2^2+(d-x)^2}}{v_2}$$

v proměnné $x \in [0, d]$. Zdůrazněme, že chceme nalézt bod $x \in [0, d]$, ve kterém je hodnota $T(x)$ minimální.

Derivace

$$T'(x) = \frac{x}{v_1\sqrt{h_1^2+x^2}} - \frac{d-x}{v_2\sqrt{h_2^2+(d-x)^2}}$$

je spojitou funkcí na intervalu $[0, d]$, a proto o znaménku derivace můžeme snadno rozhodnout pomocí jejích nulových bodů. Z rovnice

$$T'(x) = 0, \quad \text{tj.} \quad \frac{x}{v_1\sqrt{h_1^2+x^2}} = \frac{d-x}{v_2\sqrt{h_2^2+(d-x)^2}},$$

jednoduchou úpravou dostáváme

$$\frac{\frac{x}{\sqrt{h_1^2+x^2}}}{\frac{d-x}{\sqrt{h_2^2+(d-x)^2}}} = \frac{v_1}{v_2}.$$

Tento tvar je pro nás užitečný, neboť (viz obrázek)

$$\sin\varphi_1 = \frac{x}{\sqrt{h_1^2+x^2}}, \qquad \sin\varphi_2 = \frac{d-x}{\sqrt{h_2^2+(d-x)^2}}.$$

Existuje tudíž nejvýše jeden stacionární bod; a ten je určen vztahem

$$\frac{\sin\varphi_1}{\sin\varphi_2} = \frac{v_1}{v_2}. \tag{5.10}$$

Uvědomme si, že při zvětšujícím se $\varphi_1 \in [0, \pi/2]$ (když $x$ roste) se úhel $\varphi_2 \in [0, \pi/2]$ zmenšuje. Funkce sinus je nezáporná a rostoucí na intervalu $[0, \pi/2]$, a tak je podíl $(\sin\varphi_1)/(\sin\varphi_2)$ rostoucí funkcí v závislosti na $x$. Protože $T'(0) < 0$ a $T'(d) > 0$, existuje právě jeden stacionární bod $x_0$. Z nerovností $T'(x) < 0$ pro $x \in [0, x_0)$ a $T'(x) > 0$ pro $x \in (x_0, d]$ již plyne, že ve stacionárním bodě $x_0$ je globální minimum.

Shrňme předchozí. Paprsek je zadán bodem lomu $R$ (hodnotou $x_0$) a bod $R$ je potom určen identitou (‖5.10‖), která se ve fyzice označuje jako Snellův zákon.

Podíl rychlostí $v_1$ a $v_2$ je pro uvedená homogenní prostředí konstantní a vyjadřuje důležitou veličinu, jež popisuje rozhraní optických prostředí. Nazývá se index lomu a značí se $n$. Obvykle se požaduje, aby první z prostředí bylo vakuum, tj. klade se $v_1 = c$ a $v_2 = v$, se ziskem (absolutního) indexu lomu $n = c/v$. Pro vakuum je $n = 1$. Také pro vzduch se používá $n = 1$, neboť při standardních podmínkách (tj. při tlaku 101 325 Pa, teplotě 293 K a absolutní vlhkosti 0,9 g m$^{-3}$) je pro vzduch $n \doteq 1{,}000272$. U ostatních prostředí se uvádí $n > 1$ (např. se klade $n = 1{,}31$ pro led, $n = 1{,}33$ pro vodu, $n = 1{,}5$ pro běžné sklo).

Index lomu ovšem rovněž závisí na vlnové délce uvažovaného elektromagnetického vlnění (kupř. pro vodu a světlo se jedná o rozsah od $n \doteq 1{,}331$ až po $n \doteq 1{,}344$), kdy index lomu zpravidla klesá s rostoucí vlnovou délkou. Rychlost světla v optickém prostředí s indexem lomu $n > 1$ totiž závisí na frekvenci světla. Hovoří se o tzv. disperzi světla. Právě disperze světla způsobuje, že se paprsky světla různých barev lámou pod různými úhly. (Nejvíce se láme paprsek fialového světla a nejméně paprsek světla červeného.) To je mj. příčina vzniku duhy. Můžeme dále vzpomenout slavný Newtonův pokus se skleněným jehlanem (optickým hranolem) z roku 1666.

Na závěr ještě doplňme, že naše úloha měla vždy řešení, protože jsme mohli volit bod $R$ libovolně. Pokud by byl s rychlostmi $v_1$ a $v_2$ zadán také úhel $\varphi_1$ (naším úkolem by třeba bylo vypočítat, kde paprsek vycházející z bodu $A$ protne přímku $y = c$ pro jisté $c < 0$, když rozhraní optických prostředí je součástí osy $x$), pak by úhel $\varphi_2 \in (0, \pi/2)$ splňující (‖5.10‖) nemusel existovat. Takové situaci odpovídá úplný odraz světla (k lomu světla vůbec nedojde). □

**5.203. Duha.** Proč má duha kruhový tvar?



**Řešení.** V příkladu ‖5.202‖ jsme si objasnili, co je příčinou vzniku duhy. (Duha vzniká rozkladem slunečního světla na vodních kapkách.) Nyní na tento příklad navážeme. Přesněji, detailně se podíváme, co se děje se světlem při jeho průchodu dešťovou kapkou. Viz obrázek. Paprsek dopadající na povrch kapky v bodě $A$ se „rozdvojí“. Část světla se odrazí (pod úhlem $\varphi_i$ od normály) a část se zlomí dovnitř kapky pod vyznačeným úhlem $\varphi_r$. Paprsek uvnitř kapky se odrazí od povrchu kapky v bodě $B$. Protože je $|\,OA\,| = |\,OB\,|$, úhel odrazu je roven $\varphi_r$. Samozřejmě během tohoto odrazu se opět část světla lomí ven z kapky. Paprsek odražený uvnitř kapky však dopadá na povrch kapky v bodě $C$ a láme se směrem k pozorovateli pod úhlem $\varphi_i$ od normály. Doplňme, že zanedbáváme možnost vzniku tzv. sekundární (vedlejší) duhy, kdy se paprsek v kapce odrazí dvakrát (a pochopitelně i vícečetné odrazy).

Vyjádříme si úhel $\alpha := \measuredangle AIC$. Neboť $\measuredangle OAI = \varphi_i$ a $\measuredangle OAB = \varphi_r$, je $\measuredangle BAI = \varphi_i - \varphi_r$. Platí tak

$$\measuredangle BIA = \pi - (\measuredangle ABI) - (\measuredangle BAI) = \pi - (\pi - \varphi_r) - (\varphi_i - \varphi_r) = 2\varphi_r - \varphi_i$$

a dále

$$\alpha = 2 \cdot \measuredangle BIA = 4\varphi_r - 2\varphi_i.$$

Podle Snellova zákonu lomu je

$$\tfrac{\sin\varphi_i}{\sin\varphi_r} = n,$$

kde $n$ označuje index lomu pro vodu (klademe totiž index lomu pro vzduch roven 1). Máme tedy vztah

$$\varphi_r = \arcsin \tfrac{\sin\varphi_i}{n},$$

z něhož již plyne

$$\alpha = 4\arcsin\left(\frac{\sin\varphi_i}{n}\right) - 2\varphi_i. \tag{5.11}$$

Pro paprsky vycházející z kapky je hodnota $\alpha$ odlišná. Konkrétní přípustné hodnoty $\alpha$ však nejsou rozloženy rovnoměrně. Je-li $R$ poloměr kapky a $y$ udává vzdálenost bodu $A$ od horizontální roviny procházející středem kapky, platí

$$\sin\varphi_i = \frac{y}{R} \quad \text{pro} \quad y \in [0, R]. \tag{5.12}$$

Samozřejmě můžeme předpokládat (vzhledem k výrazné vzdálenosti Slunce), že množství sluneční energie pro $y \in [a-\delta, a+\delta]$ nezávisí na $a \in [\delta, R-\delta]$, ale závisí pouze na velikosti uvažovaného rozsahu hodnot $y$ pro dostatečně malá $\delta > 0$. Má tak smysl analyzovat funkci (viz (‖5.11‖) a (‖5.12‖))

$$\alpha(y) = 4\arcsin \tfrac{y}{nR} - 2\arcsin \tfrac{y}{R}, \qquad y \in [0, R].$$

Volbou vhodné jednotky délky (pro kterou je $R = 1$) přejdeme k funkci

$$\alpha(x) = 4\arcsin \tfrac{x}{n} - 2\arcsin x, \qquad x \in [0, 1].$$

Po výpočtu derivace

$$\alpha'(x) = \frac{4}{n\sqrt{1-\frac{x^2}{n^2}}} - \frac{2}{\sqrt{1-x^2}}, \qquad x \in (0, 1),$$

snadno určíme, že rovnice $\alpha'(x) = 0$ má jediné řešení

$$x_0 = \sqrt{\tfrac{4-n^2}{3}} \in (0, 1), \quad \text{pokud} \quad n^2 \in (1, 4).$$

Položme $n = 4/3$ (což je přibližně index lomu pro vodu). Dále je

$$\alpha'(x) > 0, \quad x \in (0, x_0), \qquad \alpha'(x) < 0, \quad x \in (x_0, 1).$$

Zjistili jsme, že v bodě

$$x_0 = \sqrt{\frac{4-\left(\frac{4}{3}\right)^2}{3}} = \frac{2}{3}\sqrt{\frac{5}{3}} \doteq 0,86$$

má funkce $\alpha$ globální maximum

$$\alpha(x_0) = 4 \arcsin \frac{\sqrt{5}}{2\sqrt{3}} - 2 \arcsin \frac{2\sqrt{5}}{3\sqrt{3}} \doteq 0{,}734 \text{ rad} \approx 42°.$$

Přestože je zajímavé, že vrchol duhy nemůže být nad úrovní přibližně 42° vůči tomu, kdo ji pozoruje, ještě zajímavější jsou vyčíslení

$$\alpha(0{,}74) \doteq 39{,}4°, \quad \alpha(0{,}94) \doteq 39{,}2°, \quad \alpha(0{,}8) \doteq 41{,}2°, \quad \alpha(0{,}9) \doteq 41{,}5°.$$

Ta totiž implikují (funkce $\alpha$ roste na intervalu $[0, x_0]$ a klesá na intervalu $[x_0, 1]$), že více než 20 % hodnot $\alpha$ leží v úzkém pásu zhruba od 39° do 42° a 10 % v pásu o šířce menší než 1°. Pokud navíc uvážíme např.

$$\alpha(0{,}84) \doteq 41{,}9°, \qquad \alpha(0{,}88) \doteq 41{,}9°,$$

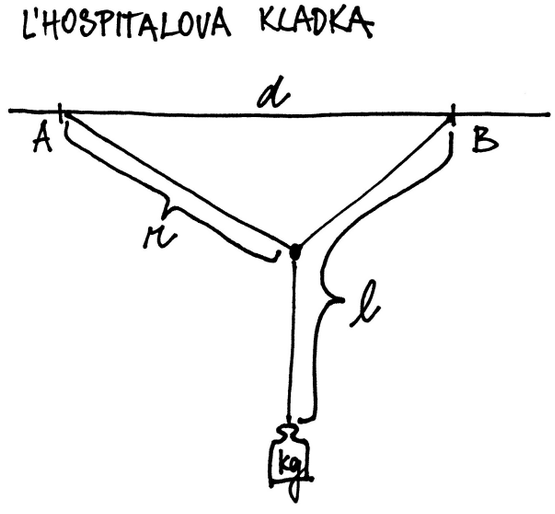
vidíme, že paprsky, pro které je $\alpha$ blízké hodnotě 42°, mají největší intenzitu. Vyzdvihněme, že se jedná o případ tzv. principu minimální odchylky, kdy platí, že k největší koncentraci rozptýleného světla dochází právě u paprsků s minimální odchylkou. Celková úhlová odchylka paprsku se totiž rovná úhlu $\delta = \pi - \alpha$.

Kapky, ze kterých směřují paprsky k pozorovateli vidícímu duhu, tak leží na povrchu kuželu s centrálním úhlem $2\alpha(x_0)$. Nadzemní část tohoto kuželu se pak jeví pozorovateli právě jako kruhový oblouk duhy. Při západu Slunce by tedy měla duha tvar půlkružnice. Uvažte také, že duha se realizuje vzhledem k pozorovateli – není nikde v prostoru. Na závěr poznamenejme, že onen kruhový tvar duhy podrobně zdokumentoval již René Descartes, který duhu vědecky zkoumal v letech 1635–1637. □

**5.204. L'Hospitalova kladka.**



Ke stropu je v bodě $A$ uvázáno lano délky $r$. Na jeho druhém konci je připevněna kladka. Ve vzdálenosti $d$ (v bodě $B$) od bodu $A$ je ke stropu přivázáno druhé lano délky $l > \sqrt{d^2 + r^2}$, které prochází kladkou. Na tomto druhém laně je zavěšeno závaží. V jaké pozici se závaží ustálí (systém přejde do stacionární polohy)? Při řešení úlohy zanedbejte hmotnost i velikost lan a kladky.



**Řešení.** Systém bude ve stacionární poloze, pokud bude minimalizována jeho potenciální energie, tj. vzdálenost závaží od stropu $f(x)$ bude maximální. To však znamená, že pro $r \geq d$ se kladka pouze přesune pod bod $B$. Nadále proto budeme předpokládat, že $r < d$. Podle Pythagorovy věty je vzdálenost kladky od stropu $\sqrt{r^2 - x^2}$ a vzdálenost kladky a závaží je $l - \sqrt{(d-x)^2 + r^2 - x^2}$, což dává

$$f(x) = \sqrt{r^2 - x^2} + l - \sqrt{(d-x)^2 + r^2 - x^2}\,.$$

Poloha systému je zcela popsána hodnotou $x \in [0, r]$ (viz obrázek), a tudíž stačí najít globální maximum funkce $f$ na intervalu $[0, r]$.

Nejprve spočítáme derivaci

$$f'(x) = \frac{-x}{\sqrt{r^2-x^2}} - \frac{-(d-x)-x}{\sqrt{(d-x)^2+r^2-x^2}} = \frac{-x}{\sqrt{r^2-x^2}} + \frac{d}{\sqrt{(d-x)^2+r^2-x^2}}, \quad x \in (0, r).$$

Umocnění rovnice $f'(x) = 0$ pro $x \in (0, r)$ vede na

$$\frac{x^2}{r^2-x^2} = \frac{d^2}{(d-x)^2+r^2-x^2}.$$

Vynásobením obou stran výrazem $\left(r^2 - x^2\right)\left((d-x)^2 + r^2 - x^2\right)$ pak (po úpravě) dostaneme

$$2dx^3 - \left(2d^2 + r^2\right)x^2 + d^2r^2 = 0, \qquad x \in (0, r).$$

Všimneme-li si, že jedním z kořenů polynomu na levé straně je zřejmě $x = d$, snadno převedeme poslední rovnici do tvaru

$$(x-d)\left(2dx^2 - r^2x - dr^2\right) = 0, \qquad x \in (0, r),$$

resp. (pro kvadratickou rovnici máme vzorec)

$$2d\,(x-d)\left(x - \frac{r^2 + r\sqrt{r^2+8d^2}}{4d}\right)\left(x - \frac{r^2 - r\sqrt{r^2+8d^2}}{4d}\right) = 0, \qquad x \in (0, r).$$

Odsud vidíme, že rovnice $f'(x) = 0$ má v intervalu $(0, r)$ nejvýše jedno řešení. (Neboť je $r < d$ a $\sqrt{r^2 + 8d^2} > r$, dva kořeny uvažovaného polynomu v proměnné $x$ určitě v intervalu $(0, r)$ neleží.) Zbývá rozhodnout, zda

$$x_0 = \frac{r^2 + r\sqrt{r^2+8d^2}}{4d} = \frac{1}{4}\,r\left[\frac{r}{d} + \sqrt{\left(\frac{r}{d}\right)^2 + 8}\right] \in (0, r).$$

Když však uvážíme, že $r, d > 0$ a $r < d$, snadno získáme

$$0 < x_0 < \frac{1}{4}\,r\left[1 + \sqrt{1^2 + 8}\right] = r.$$

Vzhledem ke spojistosti funkce $f'$ na intervalu $(0, r)$ může dojít ke změně jejího znaménka pouze v bodě $x_0$. Z limit

$$\lim_{x \to 0+} f'(x) = \frac{d}{\sqrt{d^2+r^2}}, \qquad \lim_{x \to r-} f'(x) = -\infty$$

tak již vyplývá, že

$$f'(x) > 0, \quad x \in (0, x_0), \qquad f'(x) < 0, \quad x \in (x_0, r).$$

Funkce $f$ má proto globální maximum na intervalu $[0, r]$ v bodě $x_0$. □

**5.205.** 

Nejmenovaná poštovní společnost má ve svých podmínkách uvedeno, že délka jí přepravovaného balíku nesmí být větší než 108 palců a že součet jeho délky a maximálního obvodu nesmí přesáhnout hodnotu 165 palců. Nalezněte balík největšího objemu, který podle svých podmínek společnost může doručit.

**Řešení.** Nechť $M$ označuje hodnotu 165 in (tj. palců) a $x$ délku balíku (v palcích). Hledaný balík bude mít zřejmě takový tvar, že jeho průřez pro libovolné $t \in (0, x)$ bude mít stejný (ten maximální) obvod, který (rovněž vyjádřen v palcích) budeme značit jako $o$. Chceme, aby balík měl maximální objem, a tudíž aby průřez daného obvodu měl maximální obsah. Není obtížné si uvědomit, že rovinný útvar, který má při daném obvodu maximální obsah, je kruh. Tím jsme dospěli k závěru, že hledaný balík největšího objemu má tvar válce o výšce $x$ a poloměru podstavy $r = o/2\pi$.

Jeho objem je

$$V = \pi r^2 x = \tfrac{o^2 x}{4\pi},$$

přičemž musí být $o + x \leq M$ a také $x \leq 108$ in. Uvažujme proto balík, pro který je právě $o + x = M$. Ten má objem

$$V(x) = \tfrac{(M-x)^2 x}{4\pi} = \tfrac{x^3 - 2Mx^2 + M^2 x}{4\pi}, \quad \text{kde} \quad x \in (0, 108].$$

Spočítáme-li derivaci

$$V'(x) = \tfrac{3x^2 - 4Mx + M^2}{4\pi} = \tfrac{3(x-M)\left(x - \frac{M}{3}\right)}{4\pi}, \qquad x \in (0, 108),$$

snadno zjistíme, že funkce $V$ roste na intervalu $(0, 55] = (0, M/3]$ a klesá na intervalu $[55, 108] = [M/3, \min\{108, M\}]$. Největší objem tak dostáváme pro $x = M/3$, přičemž

$$V\left(\tfrac{M}{3}\right) = \tfrac{M^3}{27\pi} \doteq 0{,}011\,789\, M^3 \approx 0{,}867\,8 \text{ m}^3.$$

Pokud by společnost v přepravních podmínkách požadovala, aby měl balík tvar kvádru, příp. jistého hranolu, můžeme předchozí úvahy zopakovat pro daný průřez o obsahu $S$, aniž bychom specifikovali, jak tento průřez vypadá. Stačí si uvědomit, že nutně $S = ko^2$ pro jisté $k > 0$, které je právě určeno tvarem průřezu. (Když se pouze změní velikost mnohoúhelníku, jenž je průřezem, tak se změní ve stejném poměru také jeho obvod. Obsah se však např. zdevítinásobí při trojnásobné velikosti – trojnásobném obvodu.) Objem balíku je tedy funkcí

$$V(x) = Sx = ko^2 x = k\,(M - x)^2\, x, \qquad x \in (0, 108].$$

Konstanta $k$ neovlivňuje bod, kde je globální maximum funkce $V$, a proto toto maximum nastává opět pro $x = M/3$. Např. pro nejobjemnější kvádr s podstavou čtverce je $o = M - x = 2M/3$, tj. délka strany jeho podstavy je $a = M/6$ a objem potom

$$V = a^2 x = \tfrac{M^3}{6^2 \cdot 3} \doteq 0{,}009\,259\, M^3 \approx 0{,}681\,6 \text{ m}^3.$$

Pro balík ve tvaru koule, kdy je $x$ průměrem, podmínku $o + x \leq M$ můžeme ihned přepsat do tvaru $\pi x + x \leq M$, tj. $x \leq M/(\pi + 1) < 108$ in. Pro $x = M/(\pi + 1)$ tak získáváme maximální objem

$$V = \tfrac{4}{3}\pi \left(\tfrac{x}{2}\right)^3 = \tfrac{\pi M^3}{6(\pi+1)^3} \doteq 0{,}007\,370\, M^3 \approx 0{,}542\,6 \text{ m}^3.$$

Podobně pro balík ve tvaru krychle, kdy $x$ udává délku hrany, podmínka $o + x \leq M$ znamená, že $x \leq M/5 < 108$ in. Takže pro $x = M/5$ dostáváme maximální objem

$$V = x^3 = \left(\tfrac{M}{5}\right)^3 = 0{,}008\, M^3 \approx 0{,}588\,9 \text{ m}^3.$$

Ještě doplňme, že krychle, která má stejný objem jako nalezený válec, má délku hrany

$$a = \tfrac{M}{3\sqrt[3]{\pi}} \doteq 0{,}227\,595\, M \approx 0{,}953\,849 \text{ m}.$$

Uvědomme si, že pro ni je součet její délky a obvodu roven $5a \doteq 1{,}138\, M$, tj. o bezmála 14 % překračuje hodnotu stanovenou společností. □

**5.206.** Rozlehlý vojenský prostor (nadále zkráceno na VP) s půdorysem čtverce o rozloze 100 km$^2$ je kolem dokola ohraničený úzkou cestou. Z výchozího místa v jednom rohu VP se lze dostat do cílového místa uvnitř VP tak, že se jde 5 km po cestě a poté 2 km kolmo k ní. Ovšem můžete jít libovolnou dobu po cestě rychlostí 5 km za hodinu a potom šikmo přes VP rychlostí 3 km za hodinu. Kolik (kilo)metrů musíte jít po cestě, abyste došli na místo určení co nejdříve?

**Řešení.** K tomu, abychom po cestě ušli $x$ km, přičemž $x \in [0, 5]$, potřebujeme $x/5$ hodin. Naše cesta přes VP pak bude měřit

$$\sqrt{2^2 + (5-x)^2} = \sqrt{x^2 - 10x + 29}$$

kilometrů a ujdeme ji za $\sqrt{x^2 - 10x + 29}/3$ hodin. Celkem bude naše cesta trvat

$$f(x) = \tfrac{1}{5}x + \tfrac{1}{3}\sqrt{x^2 - 10x + 29}$$

hodin (připomeňme, že $x \in [0, 5]$). Jediný nulový bod funkce

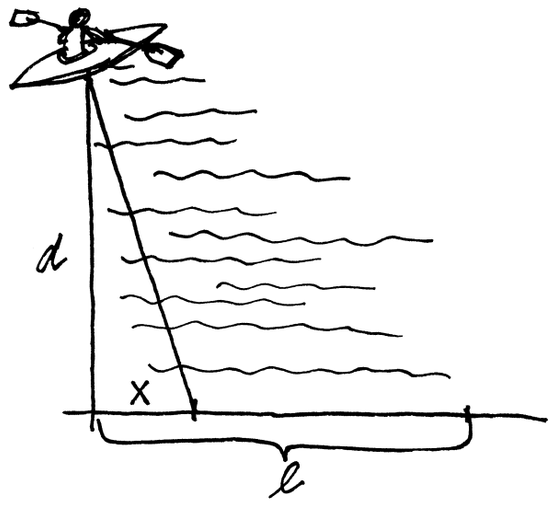
$$f'(x) = \tfrac{1}{5} + \tfrac{1}{3}\,\frac{x-5}{\sqrt{x^2-10x+29}}$$

je $x = 7/2$. Protože derivace $f'$ existuje v každém bodě intervalu $[0, 5]$ a protože

$$f\left(\tfrac{7}{2}\right) = \tfrac{23}{15} < f(5) = \tfrac{5}{3} < f(0) = \tfrac{\sqrt{29}}{3},$$

funkce $f$ má v bodě $x = 7/2$ absolutní minimum. Po cestě bychom tudíž měli jít 3,5 km. □

**5.207.** Jste ve člunu na jezeře ve vzdálenosti $d$ km od pobřeží. Chcete se dostat co nejrychleji do určeného místa na pobřeží ve vzdušné vzdálenosti $\sqrt{d^2 + l^2}$ km od Vás (viz obrázek). Jak si budete počínat, pokud dokážete veslovat rychlostí $v_1$ km/h a po břehu běžet rychlostí $v_2$ km/h? Jak dlouho Vám bude cesta trvat?




**Řešení.** Optimální strategie je zřejmě dána tím, že dorazíte ke břehu v jistém bodě $[0, x]$ pro $x \in [0, l]$ a poté budete běžet podél břehu do cílového místa $[0, l]$ (viz obrázek), kdy je tedy trajektorie složena ze dvou úseček (příp. z jedné pro $x = l$). Doplout ke břehu v bodě $[0, x]$ Vám bude trvat

$$\tfrac{\sqrt{d^2+x^2}}{v_1} \text{ hodin}$$

a běh po pobřeží pak

$$\tfrac{l-x}{v_2} \text{ hodin.}$$

Jde o to, aby celkový čas byl minimální, tj. je potřeba minimalizovat funkci

$$t(x) = \tfrac{\sqrt{d^2+x^2}}{v_1} + \tfrac{l-x}{v_2}$$

na intervalu $[0, l]$. Navíc lze předpokládat, že $v_1 < v_2$. (Pro $v_1 \geq v_2$ je nepochybně nejrychlejší veslovat přímo k cílovému místu, čemuž odpovídá $x = l$.)

Nejprve vypočítáme první derivaci

$$t'(x) = \frac{x}{v_1\sqrt{d^2+x^2}} - \frac{1}{v_2}, \qquad x \in (0, l),$$

a poté druhou

$$t''(x) = \frac{d^2}{v_1\sqrt{(d^2+x^2)^3}}, \qquad x \in (0, l).$$

Dále vyřešíme rovnici

$$t'(x) = 0, \qquad \text{tj.} \qquad \frac{x}{\sqrt{d^2+x^2}} = \frac{v_1}{v_2}.$$

Jejím umocněním obdržíme

$$x^2 = \left(\frac{v_1}{v_2}\right)^2 \left(d^2 + x^2\right).$$

Jednoduchá úprava tak již dává

$$x^2 = \frac{\left(\frac{v_1}{v_2}\right)^2 d^2}{1-\left(\frac{v_1}{v_2}\right)^2}, \qquad \text{tj.} \qquad x = \frac{\frac{v_1}{v_2}\, d}{\sqrt{1-\left(\frac{v_1}{v_2}\right)^2}}.$$

Uvědomme si, že uvažujeme pouze $x \in (0, l)$. Zajímá nás proto, zda je

$$\frac{\frac{v_1}{v_2}\, d}{\sqrt{1-\left(\frac{v_1}{v_2}\right)^2}} < l, \qquad \text{po úpravě } \frac{v_1}{v_2} < \frac{l}{\sqrt{l^2+d^2}}.$$

Pokud je tato nerovnost splněna, je rovněž $v_1 < v_2$ a funkce $t'$ mění znaménko pouze v bodě

$$x_0 = \frac{\frac{v_1}{v_2}\, d}{\sqrt{1-\left(\frac{v_1}{v_2}\right)^2}} \in (0, l),$$

a to ze záporného na kladné (uvažte $\lim_{x\to 0+} t'(x) < 0$ a $t''(x) > 0$, $x \in (0, l)$). To znamená, že v tomto případě je v bodě $x_0$ globální minimum funkce $t$ na intervalu $[0, l]$. Jestliže nerovnost (‖5.207‖) splněna není, pak je $t'(x) < 0$ pro všechna $x \in (0, l)$, odkud plyne, že globální minimum funkce $t$ na $[0, l]$ je v pravém krajním bodě (funkce $t$ je na svém definičním oboru klesající). Nejrychlejší cesta tedy bude trvat (v hodinách)

$$t(x_0) = \frac{\sqrt{d^2+x_0^2}}{v_1} + \frac{l-x_0}{v_2} = \frac{1}{v_1}\left(d^2 + \frac{\left(\frac{v_1}{v_2}\right)^2 d^2}{1-\left(\frac{v_1}{v_2}\right)^2}\right)^{\frac{1}{2}} + \frac{1}{v_2}\left(l - \frac{\frac{v_1}{v_2}\, d}{\sqrt{1-\left(\frac{v_1}{v_2}\right)^2}}\right) =$$

$$= \frac{d}{v_1\sqrt{1-\left(\frac{v_1}{v_2}\right)^2}} + \frac{l\sqrt{1-\left(\frac{v_1}{v_2}\right)^2} - \frac{v_1}{v_2}\, d}{v_2\sqrt{1-\left(\frac{v_1}{v_2}\right)^2}} = \frac{dv_2 + lv_1\sqrt{1-\left(\frac{v_1}{v_2}\right)^2} - \frac{v_1^2}{v_2}\, d}{v_1 v_2\sqrt{1-\left(\frac{v_1}{v_2}\right)^2}} =$$

$$= \frac{dv_2\left(1-\left(\frac{v_1}{v_2}\right)^2\right) + lv_1\sqrt{1-\left(\frac{v_1}{v_2}\right)^2}}{v_1 v_2\sqrt{1-\left(\frac{v_1}{v_2}\right)^2}} = \frac{dv_2\sqrt{1-\left(\frac{v_1}{v_2}\right)^2} + lv_1}{v_1 v_2} = \frac{d\sqrt{v_2^2-v_1^2}}{v_1 v_2} + \frac{l}{v_2},$$

platí-li (‖5.207‖), a

$$t(l) = \frac{\sqrt{d^2+l^2}}{v_1} \text{ hodin},$$

když (‖5.207‖) neplatí. □

**5.208.** Firma hledá obdélníkovou parcelu o rozměrech $5a \times b$ se záměrem ji po obvodu celou oplotit a pak ještě ploty kolmými na první stranu rozdělit na 5 stejně velkých parcel o rozměrech $a \times b$. Pro jaké hodnoty $a, b$ bude rozloha parcely $S = 5ab$ maximální, má-li být celková délka plotů 2 400 m?

**Řešení.** Přeformulujme zadání: Chceme maximalizovat součin $5ab$ při splnění podmínky

$$6b + 10a = 2\,400, \quad a, b > 0. \tag{5.13}$$

Lehce lze ukázat, že funkce

$$a \mapsto 5a\,\tfrac{2\,400-10a}{6}$$

definovaná pro $a \in [0, 240]$ nabývá maximální hodnoty v bodě $a = 120$. Proto je výsledek

$$a = 120\ \text{m}, \quad b = 200\ \text{m}.$$

Doplňme, že uvedená hodnota $b$ bezprostředně plyne z (‖5.13‖). □

*5.209.* Do rovnostranného trojúhelníka o straně $a$ je vepsán pravoúhelník (jedna jeho strana leží na straně trojúhelníka, zbylé dva vrcholy leží na zbylých stranách trojúhelníka). Jaký může mít maximálně obsah? ○

*5.210.* Zvolte rozměry otevřeného bazénu se čtvercovým dnem o objemu 32 $\text{m}^3$ tak, aby na natření jeho stěn a dna bylo potřeba nejmenší množství barvy. ○

*5.211.* Číslo 28 rozložte na 2 nezáporné sčítance tak, aby součet druhé mocniny prvního sčítance a třetí mocniny druhého sčítance byl minimální. ○

*5.212.* Pomocí první derivace nalezněte reálné číslo $a > 0$, pro které je součet $a + 1/a$ minimální. Poté tuto úlohu řešte bez použití diferenciálního počtu. ○

*5.213.* Vepište do půlkruhu o poloměru $r$ obdélník s největším možným obvodem. Uveďte jeho obvod. ○

*5.214.* Existuje-li mezi obdélníky o obvodu $4c$ obdélník s maximálním obsahem, stanovte délky jeho stran. ○

*5.215.* Zjistěte výšku $v$ a poloměr podstavy $r$ nejobjemnějšího kužele, který se vejde do koule o poloměru $R$. ○

*5.216.* Ze všech trojúhelníků s konstantním obvodem $o > 0$ vyberte ten, jenž má největší obsah. ○

*5.217.* Na parabole $2x^2 - 2y = 9$ najděte body s minimální vzdáleností od počátku soustavy souřadnic. ○

*5.218.* Vaším úkolem je vyrobit jednolitrovou plechovou konzervu „obvyklého“ tvaru rotačního válce tak, aby na její výrobu bylo potřeba co nejméně plechu. Určete správný poměr mezi její výškou $v$ a poloměrem podstavy $r$. ○

*5.219.* Určete vzdálenost bodu $[3, -1] \in \mathbb{R}^2$ od paraboly $y = x^2 - x + 1$. ○

*5.220.* Určete vzdálenost bodu $[-4, -2] \in \mathbb{R}^2$ od paraboly $y = x^2 + x + 1$. ○

*5.221.* V čase $t = 0$ vyjelo auto z bodu $A = [5, 0]$ rychlostí 4 jednotky za sekundu směrem $(-1, 0)$. Ve stejném čase vyjelo druhé auto z bodu $B = [-2, -1]$ rychlostí 2 jednotky za sekundu směrem $(0, 1)$. Kdy si budou auta nejblíže a jaká bude tato vzdálenost? ○

*5.222.* V čase $t = 0$ vyjelo auto z bodu $A = [0, 0]$ rychlostí 2 jednotky za sekundu směrem $(1, 0)$. Ve stejném čase vyjelo druhé auto z bodu $B = [1, -1]$ rychlostí 3 jednotky za sekundu směrem $(0, 1)$. Kdy si budou auta nejblíže a jaká bude tato vzdálenost? ◯

*5.223.* Určete maximální možný objem kužele o povrchu $3\pi$ cm$^2$ (do povrchu kužele počítáme i obsah podstavy). Povrch kužele spočítáme jako $P = \pi r(r + v)$, objem jako $V = \frac{1}{3}\pi r^2 v$, kde $r$ je poloměr podstavy a $v$ výška kužele. ◯

*5.224.* O dům je opřený žebřík dlouhý 13 stop. Náhle základna žebříku podklouzne a žebřík začne sjíždět k zemi (stále zůstává opřený o dům). Když je základna žebříku 12 stop od domu, klouže od něj rychlostí 5 stop/s. Jak rychle v tomto okamžiku

(a) klesá vršek žebříku po zdi;

(b) se mění obsah trojúhelníku vymezeného žebříkem, domem a zemí;

(c) se mění úhel, který svírá žebřík se zemí?

◯

*5.225.* Předpokládejte, že vlastníte dostatek finančních prostředků bez možnosti investovat mimo svou továrnu s působností na cenově regulovaném trhu s takřka neomezenou poptávkou a omezeným přístupem k některým klíčovým surovinám, což Vám umožňuje produkovat nejvýše 10 000 výrobků denně. Víte, že pro hrubé výnosy $v$ a náklady $n$ jako funkce proměnné $x$, udávající v tisících průměrný počet výrobků vyrobených za den, platí

$$v(x) = 9x, \quad n(x) = x^3 - 6x^2 + 15x, \quad x \in [0, 10].$$

Při jakém objemu výroby budete mít z Vaší továrny největší zisky? ◯

**5.226.** Určete

$$\lim_{x\to 0}\left(\operatorname{cotg} x - \frac{1}{x}\right).$$

**Řešení.** Uvědomíme-li si, že je

$$\lim_{x\to 0+} \operatorname{cotg} x = +\infty, \qquad \lim_{x\to 0+} \frac{1}{x} = +\infty,$$

$$\lim_{x\to 0-} \operatorname{cotg} x = -\infty, \qquad \lim_{x\to 0-} \frac{1}{x} = -\infty,$$

vidíme, že v případě obou jednostranných limit dostáváme typ $\infty - \infty$. Můžeme tedy uvažovat najednou oboustrannou limitu. Funkci kotangens zapíšeme jako podíl kosinu a sinu a zlomky převedeme na společného jmenovatele, tj.

$$\lim_{x\to 0}\left(\operatorname{cotg} x - \frac{1}{x}\right) = \lim_{x\to 0} \frac{x\cos x - \sin x}{x \sin x}.$$

Obdrželi jsme výraz $0/0$, pro který platí (podle l'Hospitalova pravidla)

$$\lim_{x\to 0} \frac{x\cos x - \sin x}{x \sin x} = \lim_{x\to 0} \frac{\cos x - x\sin x - \cos x}{\sin x + x\cos x} = \lim_{x\to 0} \frac{-x\sin x}{\sin x + x\cos x}.$$

Druhým použitím l'Hospitalova pravidla pro typ $0/0$ pak již dostaneme

$$\lim_{x\to 0} \frac{-x\sin x}{\sin x + x\cos x} = \lim_{x\to 0} \frac{-\sin x - x\cos x}{\cos x + \cos x - x\sin x} = \frac{0-0}{1+1-0} = 0.$$

□

*5.227.* Určete limitu

$$\lim_{x\to 1-} (1-x)\,\operatorname{tg}\tfrac{\pi x}{2}\,.$$

○

*5.228.* Stanovte

$$\lim_{x\to \frac{\pi}{2}-} \left(\frac{\pi}{2} - x\operatorname{tg} x\right).$$

○

*5.229.* Pomocí l'Hospitalova pravidla určete

$$\lim_{x\to+\infty} \left(\left(3^{\frac{1}{x}} - 2^{\frac{1}{x}}\right) x\right).$$

○

*5.230.* Vypočtěte

$$\lim_{x\to 1} \left(\frac{1}{2\ln x} - \frac{1}{x^2-1}\right).$$

○

*5.231.* Užitím l'Hospitalova pravidla spočtěte limitu

$$\lim_{x\to+\infty} \left(\cos\frac{2}{x}\right)^{x^2}.$$

○

*5.232.* Vypočtěte

$$\lim_{x\to 0} (1-\cos x)^{\sin x} = \ldots$$

○

*5.233.* Určete následující dvě limity

$$\lim_{x\to 0+} x^{\frac{\alpha}{\ln x}}, \qquad \lim_{x\to+\infty} x^{\frac{\alpha}{\ln x}},$$

přičemž $\alpha \in \mathbb{R}$ je libovolné. ○

*5.234.* Libovolným způsobem ověřte, že je

$$\lim_{x\to 0} \frac{\mathrm{e}^x - 1}{x} = 1.$$

○

**5.235.** Aplikací podílového (tzv. d'Alembertova) kritéria (viz 5.47) určete, jestli nekonečná řada

(a) $\sum_{n=1}^{\infty} \frac{2^n\cdot(n+1)^3}{3^n}$;

(b) $\sum_{n=1}^{\infty} \frac{6^n}{n!}$;

(c) $\sum_{n=1}^{\infty} \frac{n^n}{n^2\cdot n!}$

konverguje.

**Řešení.** Protože ($a_n \geq 0$ pro všechna $n$)

(a) $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \lim_{n\to\infty} \frac{2^{n+1}\cdot(n+2)^3\cdot 3^n}{3^{n+1}\cdot 2^n\cdot(n+1)^3} = \lim_{n\to\infty} \frac{2(n+2)^3}{3(n+1)^3} = \lim_{n\to\infty} \frac{2n^3}{3n^3} = \frac{2}{3} < 1$;

(b) $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \lim_{n\to\infty} \left(\frac{6^{n+1}}{(n+1)!}\cdot\frac{n!}{6^n}\right) = \lim_{n\to\infty} \frac{6}{n+1} = 0 < 1$;

(c) $\lim\limits_{n\to\infty}\frac{a_{n+1}}{a_n} = \lim\limits_{n\to\infty}\left(\frac{(n+1)^{n+1}}{(n+1)^2\cdot(n+1)!}\cdot\frac{n^2\cdot n!}{n^n}\right) = \lim\limits_{n\to\infty}\frac{n^2}{(n+1)^2}\cdot\lim\limits_{n\to\infty}\frac{(n+1)^n}{n^n} = \lim\limits_{n\to\infty}\frac{n^2}{n^2}\cdot\lim\limits_{n\to\infty}\left(1+\frac{1}{n}\right)^n = 1\cdot\mathrm{e} > 1,$

řada (a) konverguje; (b) konverguje; (c) nekonverguje (diverguje k $+\infty$). □

**5.236.** Aplikací odmocninového (tzv. Cauchyova) kritéria určete, jestli nekonečná řada

(a) $\sum\limits_{n=1}^{\infty}\frac{1}{\ln^n(n+1)}$;

(b) $\sum\limits_{n=1}^{\infty}\frac{\left(\frac{n+1}{n}\right)^{n^2}}{n^3\cdot 3^n}$;

(c) $\sum\limits_{n=1}^{\infty}\arcsin^n\frac{2n}{2^n}$

konverguje.

**Řešení.** Opět máme řady s nezápornými členy, přičemž je

(a) $\lim\limits_{n\to\infty}\sqrt[n]{a_n} = \lim\limits_{n\to\infty}\frac{1}{\ln(n+1)} = 0 < 1;$

(b) $\lim\limits_{n\to\infty}\sqrt[n]{a_n} = \lim\limits_{n\to\infty}\frac{\left(\frac{n+1}{n}\right)^n}{\sqrt[n]{n^3\cdot 3}} = \frac{\lim\limits_{n\to\infty}\left(1+\frac{1}{n}\right)^n}{3\left(\lim\limits_{n\to\infty}\sqrt[n]{n}\right)^3} = \frac{\mathrm{e}}{3} < 1;$

(c) $\lim\limits_{n\to\infty}\sqrt[n]{a_n} = \lim\limits_{n\to\infty}\arcsin\frac{2n}{2^n} = \arcsin 0 = 0 < 1.$

To znamená, že všechny zadané řady konvergují. □

**5.237.** Rozhodněte, zda řada

(a) $\sum\limits_{n=1}^{\infty}(-1)^n\,\ln\left(1+\frac{1}{2^n}\right)$;

(b) $\sum\limits_{n=1}^{\infty}\frac{(-2)^{n^2}}{n!}$;

(c) $\sum\limits_{n=1}^{\infty}\frac{(-3)^n}{(6+(-1)^n)^n}$

konverguje.

**Řešení.** Případ (a). Podle l'Hospitalova pravidla je

$$\lim_{x\to+\infty}\frac{\ln\left(1+\frac{1}{2^x}\right)}{\frac{1}{2^x}} = \lim_{x\to+\infty}\frac{\frac{1}{1+\frac{1}{2^x}}\left(1+\frac{1}{2^x}\right)'}{\left(\frac{1}{2^x}\right)'} = \lim_{x\to+\infty}\frac{1}{1+\frac{1}{2^x}} = 1,$$

a proto platí

$$0 < \ln\left(1+\frac{1}{2^n}\right) \le \frac{2}{2^n}$$

pro všechna dostatečně velká $n\in\mathbb{N}$. Ovšem o řadě $\sum_{n=1}^{\infty}\frac{2}{2^n}$ víme, že je konvergentní. Musí tak být

$$\sum_{n=1}^{\infty}\ln\left(1+\frac{1}{2^n}\right) < +\infty,$$

tj. řada v zadání konverguje (absolutně).

Případ (b). Podílové kritérium dává

$$\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right| = \lim_{n\to\infty}\frac{2^{(n+1)^2}\cdot n!}{(n+1)!\cdot 2^{n^2}} = \lim_{n\to\infty}\frac{2^{2n+1}}{n+1} = \lim_{n\to\infty}\frac{2\cdot 4^n}{n+1} = +\infty.$$

Řada tedy nekonverguje.

Případ (c). Nyní použijeme obecnou verzi odmocninového kritéria

$$\limsup_{n\to\infty}\sqrt[n]{|\,a_n\,|} = \limsup_{n\to\infty}\frac{3}{6+(-1)^n} = \frac{3}{5} < 1,$$

z níž plyne (absolutní) konvergence řady. □

**5.238.** Libovolným způsobem dojděte k rozhodnutí o konvergenci alternující řady

(a) $\sum_{n=1}^{\infty}(-1)^n \frac{n^2+3n-1}{(3n-2)^2}$;

(b) $\sum_{n=1}^{\infty}(-1)^{n-1} \frac{3n^4-3n^3+9n-1}{(5n^3-2)\cdot 4^n}$.

**Řešení.** Případ (a). Z toho, že je

$$\lim_{n\to\infty} \frac{n^2+3n-1}{(3n-2)^2} = \lim_{n\to\infty} \frac{n^2}{9n^2} = \frac{1}{9} \neq 0,$$

ihned vyplývá neexistence limity

$$\lim_{n\to\infty} (-1)^n \frac{n^2+3n-1}{(3n-2)^2}.$$

Řada tudíž nekonverguje (není splněna nutná podmínka konvergence).

Případ (b). Viděli jsme, že při použití podílového (nebo odmocninového) kritéria polynomy v čitateli ani jmenovateli členů řady neovlivňují hodnotu počítané limity. Uvažujme tedy řadu

$$\sum_{n=1}^{\infty}(-1)^{n-1} \frac{1}{4^n},$$

pro kterou je

$$\lim_{n\to\infty} \left| \frac{a_{n+1}}{a_n} \right| = \frac{1}{4} < 1.$$

To ovšem znamená, že rovněž původní řada je (absolutně) konvergentní. □

**5.239.** Konverguje řada

$$\sum_{n=1}^{\infty}(-1)^{n+1} \operatorname{arctg} \frac{2}{\sqrt{3n}}?$$

**Řešení.** Posloupnost $\left\{2/\sqrt{3n}\right\}_{n\in\mathbb{N}}$ je zřejmě klesající a funkce $y = \operatorname{arctg} x$ rostoucí (na celé reálné ose), a tudíž posloupnost $\left\{\operatorname{arctg}\left(2/\sqrt{3n}\right)\right\}_{n\in\mathbb{N}}$ je klesající. Je tedy zadána alternující řada splňující, že posloupnost absolutních hodnot jejích členů je klesající. Taková alternující řada konverguje, právě když posloupnost jejích členů konverguje k 0 (tzv. Leibnizovo kritérium), což je ovšem splněno:

$$\lim_{n\to\infty} \operatorname{arctg} \frac{2}{\sqrt{3n}} = \operatorname{arctg} 0 = 0, \text{ tj. } \lim_{n\to\infty} \left((-1)^{n+1} \operatorname{arctg} \frac{2}{\sqrt{3n}}\right) = 0.$$

□

**5.240.** Zjistěte, jestli řada

(a) $\sum_{n=1}^{\infty} \frac{\sin n}{n^2}$;

(b) $\sum_{n=1}^{\infty} \frac{\cos(\pi n)}{\sqrt[3]{n^2}}$

konverguje absolutně, příp. neabsolutně (relativně), nebo nekonverguje.

**Řešení.** Případ (a). Ukázat, že tato řada konverguje absolutně, je snadné. Např. je

$$\sum_{n=1}^{\infty} \left| \frac{\sin n}{n^2} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^2} < \sum_{n=0}^{\infty} \frac{1}{2^n} = 2,$$

přičemž druhou nerovnost jsme dokázali dříve.

Případ (b). Je vidět, že $\cos(\pi n) = (-1)^n$, $n \in \mathbb{N}$. Máme tedy alternující řadu, jejíž posloupnost členů v absolutní hodnotě je klesající. Proto z limity

$$\lim_{n\to\infty} \frac{1}{\sqrt[3]{n^2}} = 0$$

již plyne, že řada konverguje. Zároveň však je

$$\sum_{n=1}^{\infty} \left| \frac{\cos(\pi n)}{\sqrt[3]{n^2}} \right| = \sum_{n=1}^{\infty} \frac{1}{\sqrt[3]{n^2}} \geq \sum_{n=1}^{\infty} \frac{1}{n} = +\infty.$$

Řada tak konverguje neabsolutně. □

**5.241.** Jaký je součet řady $\sum_{n=2}^{\infty} \frac{1}{\sqrt[n]{\ln n}}$?

**Řešení.** Z nerovností (uvažte graf přirozeného logaritmu)

$$1 \leq \ln n \leq n, \quad n \geq 3, \ n \in \mathbb{N}$$

plyne

$$\sqrt[n]{1} \leq \sqrt[n]{\ln n} \leq \sqrt[n]{n}, \quad n \geq 3, \ n \in \mathbb{N}.$$

Podle Věty o třech limitách je

$$\lim_{n\to\infty} \sqrt[n]{\ln n} = 1, \quad \text{tj.} \quad \lim_{n\to\infty} \frac{1}{\sqrt[n]{\ln n}} = 1.$$

Řada tedy není konvergentní. Neboť má nezáporné členy, musí divergovat k $+\infty$. □

**5.242.** Rozhodněte o následujících řadách, jestli konvergují či divergují:

i) $\sum_{n=1}^{\infty} \frac{2^n}{n}$

ii) $\sum_{n=1}^{\infty} \frac{1}{\sqrt{n}}$

iii) $\sum_{n=1}^{\infty} \frac{1}{n \cdot 2^{100000}}$

iv) $\sum_{n=1}^{\infty} \frac{1}{(1+i)^n}$

**Řešení.**

i) Budeme zkoumat konvergenci podílovým kritériem:

$$\lim_{n\to\infty} \left| \frac{a_{n+1}}{a_n} \right| = \lim_{n\to\infty} \left| \frac{\frac{2^{n+1}}{n+1}}{\frac{2^n}{n}} \right| = \lim_{n\to\infty} \frac{2(n+1)}{n} = 2 > 1,$$

řada tedy diverguje.

ii) Odhadneme řadu ze spodu: víme, že pro libovolné přirozené $n$ platí $\frac{1}{n} \leq \frac{1}{\sqrt{n}}$. Pro posloupnost částečných součtů $s_n$ zkoumané řady a posloupnost částečných součtů harmonické řady $s'_n$ tedy platí:

$$s_n = \sum_{i=1}^{n} \frac{1}{\sqrt{n}} \geq \sum_{i=1}^{n} \frac{1}{n} = s'_n.$$

A protože harmonická řada diverguje (viz předchozí příklad), diverguje i její posloupnost částečných součtů $\{s'_n\}_{n=1}^{\infty}$, tedy diverguje i posloupnost částečných součtů $\{s_n\}_{n=1}^{\infty}$, tedy diverguje i zadaná posloupnost.

iii) Diverguje, jedná se o násobek harmonické řady.

iv) Jedná se o geometrickou řadu s koeficientem $\frac{1}{1+i}$, ta bude konvergovat, bude-li absolutní hodnota koeficientu menší než 1. Víme, že

$$\left|\frac{1}{1+i}\right| = \left|\frac{1-i}{2}\right| = \left|\frac{1}{2} - \frac{1}{2}i\right| = \sqrt{\frac{1}{4} + \frac{1}{4}} = \frac{\sqrt{2}}{2} < 1,$$

řada tedy konverguje a umíme ji dokonce sečíst:

$$\sum_{n=1}^{\infty} \frac{1}{(1+i)^n} = \frac{1}{1 - \frac{1}{1+i}} = \frac{1+i}{i} = 1 - i.$$

□

*5.243.* Do čtverce o délce strany $a > 0$ je vepsán čtverec, jehož strany jsou spojnicemi středů stran zadaného čtverce. Do vepsaného čtverce je stejným způsobem vepsán další čtverec atd. Stanovte součet obsahů a součet obvodů všech těchto (nekonečně mnoha) čtverců. ○

*5.244.* Nechť je dána posloupnost řádků půlkruhů, přičemž v $n$-tém řádku je $2^n$ půlkruhů o poloměru $2^{-n}$ pro každé $n \in \mathbb{N}$. Jaký bude obsah libovolného obrazce složeného ze všech těchto půlkruhů, když nebudou umístěny přes sebe? ○

*5.245.* Vyřešte rovnici

$$1 - \operatorname{tg} x + \operatorname{tg}^2 x - \operatorname{tg}^3 x + \operatorname{tg}^4 x - \operatorname{tg}^5 x + \cdots = \tfrac{\operatorname{tg} 2x}{\operatorname{tg} 2x+1}\,.$$ ○

*5.246.* Určete

$$\sum_{n=1}^{\infty} \left(\tfrac{1}{2^{n-1}} + \tfrac{2}{3^{n-1}}\right).$$

○

*5.247.* Sečtěte

$$\sum_{n=1}^{\infty} \sqrt[5n]{n^2 + 2n + 1}.$$

○

*5.248.* Dokažte konvergenci a nalezněte součet řady

$$\sum_{n=1}^{\infty} \tfrac{3^n+2^n}{6^n}.$$

○

*5.249.* Stanovte součet řady

(a) $\sum_{n=1}^{\infty} \tfrac{2n-1}{2^n}$;

(b) $\sum_{n=0}^{\infty} \tfrac{n+1}{3^n}$.

○

*5.250.* Sečtěte

$$\tfrac{1}{1\cdot 3} + \tfrac{1}{3\cdot 5} + \tfrac{1}{5\cdot 7} + \cdots = \sum_{n=1}^{\infty} \tfrac{1}{(2n-1)(2n+1)}.$$

○

*5.251.* Pomocí rozkladu na parciální zlomky vyčíslete

(a) $\sum_{n=2}^{\infty} \tfrac{1}{n^2-1}$;

(b) $\sum_{n=1}^{\infty} \tfrac{1}{n^3+3n^2+2n}$.

○

*5.252.* Sečtěte konvergentní řadu

$$\sum_{n=0}^{\infty} \tfrac{1}{4n^2-1}.$$

○

*5.253.* Určete součet řady

$$\sum_{n=1}^{\infty} \tfrac{1}{n^2+3n}.$$

○

*5.254.* V závislosti na

$$s := \sum_{n=1}^{\infty} \tfrac{(-1)^{n-1}}{n} = 1 - \tfrac{1}{2} + \tfrac{1}{3} - \tfrac{1}{4} + \tfrac{1}{5} - \tfrac{1}{6} + \tfrac{1}{7} - \tfrac{1}{8} + \cdots$$

vyjádřete součty řad

$$\left(1 - \tfrac{1}{2} - \tfrac{1}{4}\right) + \left(\tfrac{1}{3} - \tfrac{1}{6} - \tfrac{1}{8}\right) + \cdots;$$
$$\left(1 + \tfrac{1}{3} - \tfrac{1}{2}\right) + \left(\tfrac{1}{5} + \tfrac{1}{7} - \tfrac{1}{4}\right) + \cdots,$$

které z výše uvedené řady vznikly přerovnáním (tj. změnou pořadí členů). ○

*5.255.* Zjistěte, zda řada

$$\sum_{n=0}^{\infty} \tfrac{2^n+(-2)^n}{5^n}$$

konverguje. ○

*5.256.* Dokažte následující tvrzení:

Jestliže řada $\sum_{n=0}^{\infty} a_n$ konverguje, pak je $\lim_{n\to\infty} \sin(3a_n + \pi) = 0$. ○

*5.257.* Pro jaké $\alpha \in \mathbb{R}$; $\beta \in \mathbb{Z}$; $\gamma \in \mathbb{R} \setminus \{0\}$ konvergují řady

$$\sum_{n=120}^{\infty} \tfrac{\mathrm{e}^{-\alpha n}}{n}; \qquad \sum_{n=240}^{\infty} \tfrac{\beta^n \cdot n!}{n^n}; \qquad \sum_{n=360}^{\infty} \tfrac{n}{\gamma^n}?$$ ○

*5.258.* Rozhodněte, zda řada

$$\sum_{n=21}^{\infty} (-1)^n \tfrac{n^8-5n^6+2n}{2^n}$$

konverguje absolutně, konverguje neabsolutně (relativně), nebo nekonverguje. ○

*5.259.* Zjistěte, jestli je limita

$$\lim_{n\to\infty} \left(\tfrac{1}{n^2} + \tfrac{2}{n^2} + \cdots + \tfrac{n-1}{n^2}\right)$$

vlastní. Upozorněme, že k tomu nelze využít součtů

$$\sum_{n=1}^{\infty} \tfrac{1}{n^2} = \tfrac{\pi^2}{6}, \qquad \sum_{n=2}^{\infty} \tfrac{n-1}{n^2} = +\infty.$$

○

*5.260.* Najděte všechna reálná čísla $A \geq 0$, pro která řada

$$\sum_{n=1}^{\infty} (-1)^n \ln\left(1 + A^{2n}\right)$$

konverguje. ○

*5.261.* Zopakujme, že harmonická řada diverguje; tj. platí

$$\sum_{n=1}^{\infty} \tfrac{1}{n} = +\infty.$$

Rozhodněte, zda také řada

$$\tfrac{1}{1} + \cdots + \tfrac{1}{9} + \tfrac{1}{11} + \cdots + \tfrac{1}{19} + \tfrac{1}{21} + \cdots + \tfrac{1}{29} + \cdots$$
$$\cdots + \tfrac{1}{91} + \cdots + \tfrac{1}{99} + \tfrac{1}{111} + \cdots + \tfrac{1}{119} + \tfrac{1}{121} + \cdots$$

diverguje. ○

*5.262.* Udejte příklad divergentních číselných řad $\sum_{n=1}^{\infty} a_n$, $\sum_{n=1}^{\infty} b_n$ s kladnými členy, pro které řada $\sum_{n=1}^{\infty} (3a_n - 2b_n)$ absolutně konverguje. ○

*5.263.* Zjistěte, zda jednotlivé řady

$$\sum_{n=1}^{\infty} (-1)^n \tfrac{(n!)^2}{(2n)!}; \qquad \sum_{n=1}^{\infty} (-1)^n \tfrac{n^7 - n^4 + n}{n^8 + 2n^6 + n}$$

konvergují absolutně, konvergují neabsolutně, či nekonvergují. ○

*5.264.* Konverguje řada

$$\sum_{n=1}^{\infty} (-1)^{n+1} \tfrac{\sqrt[3]{n} + \sqrt[5]{n} + 1}{n + \sqrt[7]{n}} ?$$

○

*5.265.* Nalezněte hodnoty parametru $p \in \mathbb{R}$, pro které řada

$$\sum_{n=1}^{\infty} (-1)^n \sin^n \tfrac{p}{n}$$

konverguje. ○

### Řešení cvičení

*5.2.* $P(x) = (-\frac{3}{5} - \frac{4}{5}i)x^2 + (2+3i)x - \frac{3}{5} - \frac{14}{5}i$.

*5.11.* $3x^2 - 2x - 4$.

*5.12.* $\left(2x^2 - 5\right)/3$; např. $\left(\frac{2}{3}x^2 - \frac{5}{3}\right)^3$.

*5.13.* $a = 1, b = -2, c = 0, d = 1$.

*5.14.* $x^3 + x^2 - x + 2$.

*5.15.* Nekonečně mnoho.

*5.16.* $P(x) = x^3 - 2x^2 + 5x - 3$; $Q(x) = x^3 - 2x^2 + 3x - 3$.

*5.17.* $x^5 - 2x^4 - 5x + 2$.

*5.18.* $x^2$.

*5.19.* $x^3 - 2x + 5$; $x^3 - x + 6$.

*5.20.* Nekonečně mnoho.

*5.21.* Např. $x^2 - 3x + 6$.

*5.22.* $S_1(x) = \frac{1}{2}(x+1)^3 - \frac{3}{2}(x+1) + 1, x \in [-1, 0]$; $S_2(x) = -\frac{1}{2}x^3 + \frac{3}{2}x^2, x \in [0, 1]$.

*5.23.* $S_1(x) = \frac{1}{2}(x+1)^3 - \frac{3}{2}(x+1) + 1, x \in [-1, 0]$; $S_2(x) = -\frac{1}{2}x^3 + \frac{3}{2}x^2, x \in [0, 1]$.

*5.24.* $S_1(x) \equiv x$; $S_2(x) \equiv x$.

*5.25.* $S_1(x) \equiv 1$; $S_2(x) \equiv 1$.

*5.26.* $S_i(x) = x + 3, x \in [-3 + i - 1, -3 + i]; i \in \{1, 2\}$.

*5.27.* $S_1(x) = 1 - \frac{11}{20}x + \frac{1}{20}x^3$; $S_2(x) = \frac{1}{2} - \frac{2}{5}(x-1) + \frac{3}{20}(x-1)^2 - \frac{1}{40}(x-1)^3$.

*5.29.*

$$\begin{aligned} &\sup A = 6, && \inf A = -3; \\ &\sup B = \frac{1}{4}, && \inf B = -1; \\ &\sup C = 9, && \inf C = -9. \end{aligned}$$

*5.30.* Lehce lze ukázat, že

$$\sup A = \frac{3}{2}, \qquad \inf A = 0.$$

*5.31.* Zřejmě je

$$\inf \mathbb{N} = 1, \quad \sup \mathcal{M} = 0, \quad \inf \mathcal{J} = 0, \quad \sup \mathcal{J} = 5.$$

*5.32.* Lze položit kupř.

$$M := \mathbb{Z} \setminus \mathbb{N}; \qquad N := \mathbb{N}.$$

*5.33.* Uvažte jakoukoli jednoprvkovou množinu $X \subset \mathbb{R}$.

*5.34.* Množina $C$ musí být jednoprvková. Nechť je tedy např. $C = \{0\}$. Nyní můžeme zvolit $A = (-1, 0)$, $B = (0, 1)$.

*5.40.* Platí

$$\lim_{n\to\infty}\left(\frac{1}{n^2} + \frac{2}{n^2} + \cdots + \frac{n-2}{n^2} + \frac{n-1}{n^2}\right) = \lim_{n\to\infty}\left(\frac{n}{n^2}\cdot\frac{n-1}{2}\right) = \frac{1}{2}.$$

*5.41.* Snadno lze ukázat, že

$$\lim_{n\to\infty}\frac{\sqrt{n^3 - 11n^2 + 2} + \sqrt[5]{n^7 - 2n^5 - n^3} - n + \sin^2 n}{2 - \sqrt[3]{5n^4 + 2n^3 + 5}} = -\infty.$$

*5.42*. Limita je rovna 1.

*5.43*. Kupř. lze položit

$$x_n := n, \quad y_n := -n + 1, \qquad n \in \mathbb{N}.$$

*5.44*. Správná odpověď je $\pm 1$.

*5.45*. Výsledek je

$$\limsup_{n\to\infty} a_n = 1, \qquad \liminf_{n\to\infty} a_n = 0.$$

*5.46*. Platí

$$\liminf_{n\to\infty} \left( (-1)^n \left(1 + \frac{1}{n}\right)^n + \sin\frac{n\pi}{4} \right) = -\mathrm{e} - \frac{\sqrt{2}}{2}.$$

*5.63*. Uvedená funkce je spojitá na celém $\mathbb{R}$.

*5.64*. V bodech $-\pi$, 0, $\pi$ je spojitá; v bodě 2 je spojitá pouze zprava a v bodě 3 pouze zleva; v bodě 1 není spojitá ani z jedné strany.

*5.65*. Je nutné položit $f(0) := 0$.

*5.66*. Funkce je spojitá právě pro $p = 2$.

*5.67*. Správná odpověď je $a = 4$.

*5.68*. Je

$$\lim_{x\to 0+} \frac{\sin^8 x}{x^3} = \lim_{x\to -\infty} \frac{\sin^8 x}{x^3} = 0.$$

*5.71*. Jediné řešení $x = -1$.

*5.72*. Ano.

*5.76*. $f'(x) = 2x^{\ln x - 1} \cdot \ln x$.

*5.77*. $(\sin x)^{1+\cos x} \left(\operatorname{cotg}^2 x - \ln(\sin x)\right)$.

*5.79*. $\frac{\pi}{6} - \frac{2}{\sqrt{3}}\,0{,}003$.

*5.80*. $a \approx \frac{\pi}{4} + 0{,}01$; $b \approx 4{,}125$.

*5.81*. (a) $\frac{1}{2} - \frac{\sqrt{3}}{360}\pi$; (b) $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{360}\pi$.

*5.83*. Ano, má.

*5.84*. $y = \frac{x_0}{p}\,x - \frac{x_0^2}{2p}$.

*5.85*. $y = \sqrt[3]{4}\,(x+1)$; $y = -\frac{\sqrt[3]{2}}{2}\,(x+1)$.

*5.86*. $y = 2x$.

*5.87*. $y - \frac{\ln 5}{2} = \left(\frac{13}{10} - \frac{\ln 5}{4}\right)(x-1)$; $y - \frac{\ln 5}{2} = \frac{20}{5\ln 5 - 26}(x-1)$.

*5.88*. $\left[\frac{1}{2}, 2\frac{1}{4}\right]$.

*5.89*. $t : y = \frac{x}{6} + \frac{8}{3}$; $n : y = -6x + 15$; $\left[\frac{3}{2}, \sqrt{\left(\frac{3}{2}\right)^2 - 3\,\frac{3}{2} + 11}\right]$.

*5.90*. $\pi/4$.

*5.91*. $y = 2 - x$; $y = x$.

*5.92*. Nerovnosti plynou např. z Věty o střední hodnotě (tzv. Lagrangeovy věty) aplikované na funkci $y = \ln(1+t)$, $t \in [0, x]$.

*5.114*. $r = +\infty$.

*5.115.* 1.
*5.116.* 3.
*5.117.* $[-1, 1]$.
*5.118.* $x \in \left[2 - \frac{1}{3}, 2 + \frac{1}{3}\right]$.
*5.119.* Ano.
*5.120.*

(a) Platí.
(b) Neplatí.
(c) Neplatí.
(d) Platí.

*5.121.* $1 - \frac{\pi^2}{10^2 \cdot 2} + \frac{\pi^4}{10^4 \cdot 4!}$.
*5.122.* Chyba náleží do intervalu $(0, 1/200)$.
*5.123.* $\sum_{n=0}^{\infty} \frac{\mathrm{e}}{n!} (x-1)^n$; $\sum_{n=0}^{\infty} \frac{\ln^n 2}{n!} x^n$.
*5.124.* $f(x) = x, x \in \mathbb{R}$; ano.
*5.125.* Nikoli.
*5.126.* (a) $1 - \frac{\pi^2}{18^2 \cdot 2!} + \frac{\pi^4}{18^4 \cdot 4!}$; (b) $\frac{1}{2} - \frac{1}{5 \cdot 2^5}$.
*5.127.* $\sum_{n=0}^{\infty} \frac{1}{(2n+1)\, n!} x^{2n+1}$.
*5.128.* $a > 1$.
*5.129.* $[-\sqrt[3]{2}, \sqrt[3]{2})$.
*5.130.* Pro $x \in [-1, 1]$.
*5.131.* $x > 2$.
*5.132.* Konverguje absolutně.
*5.133.* $\ln(3/2)$.
*5.134.* $\frac{x(1-x)}{(1+x)^3}$.
*5.135.* (a) $\frac{1}{2} \ln \frac{1+x}{1-x}$; (b) $\frac{1+x}{(1-x)^3}$.
*5.136.* $2/9$.
*5.137.* $x\, \mathrm{e}^{\frac{x^3}{2}}$.
*5.138.* $\mathbb{R}$.
*5.139.* $(1, \mathrm{e}]$.
*5.140.* $\left(-\infty, \frac{2}{3}\right) \cup \left(\frac{2}{3}, +\infty\right)$; $\left(-\infty, -\frac{1}{3}\right) \cup \left(-\frac{1}{3}, +\infty\right)$; $y = \frac{2x+1}{3x+1}$, $x \neq -\frac{1}{3}$.
*5.141.* (a) ano; (b) ne; (c) ne; (d) ne; (e) ano; (f) ano; (g) ano; (h) ne.
*5.142.* (a) ne; (b) ne; (c) ano; (d) ano; (e) ne; (f) ne; (g) ne; (h) ano.
*5.143.* Lichá funkce je uvedena ve variantách (a), (e); sudá v (c), (d).
*5.144.* Je periodická s primitivní periodou (a) $2\pi$; (b) $\pi/3$.
*5.145.* Funkce $f$ a $g$ jsou sudé – k vykreslení jejich grafů tak postačují grafy funkcí $y = \mathrm{e}^x$, $x \in [0, +\infty)$ a $y = \ln x$, $x \in (0, +\infty)$.
*5.146.* Zadaná funkce je sudá, a proto k načrtnutí jejího grafu stačí znát graf funkce $y = 2^x$, $x \in (-\infty, 0]$.
*5.147.* $(\sinh x)' = \cosh x$; $(\cosh x)' = \sinh x$; $(\operatorname{tgh} x)' = \frac{1}{\cosh^2 x}$; $(\operatorname{cotgh} x)' = -\frac{1}{\sinh^2 x}$.
*5.148.* $\frac{1}{\sqrt{1+x^2}}$.
*5.150.* $x^4 + 2x^3 - x^2 + x - 2$.
*5.151.* $x^4 + 2x^3 - 2x^2 + x + 2$.
*5.152.* $x^4 + 3x^3 - 3x^2 - x - 1$.

*5.153.* Pro každé $\varepsilon > 0$ stačí $\varepsilon$-okolí bodu $-2$ přiřadit $\delta$-okolí bodu 0 předpisem

$$\varepsilon \mapsto \delta, \qquad \delta = \varepsilon,$$

přičemž bez újmy na obecnosti lze požadovat, aby $\varepsilon \leq 1$. Pokud by totiž bylo $\varepsilon > 1$, lze položit $\delta = 1$.

*5.154.* Existence limity a rovnost

$$\lim_{x \to -1} \frac{(1+x)^2 - 3}{2} = -\frac{3}{2}$$

např. opět plyne z volby $\delta := \varepsilon$ pro $\varepsilon \in (0, 1)$.

*5.155.* Neboť $-(x-2)^4 < x$ pro $x < 0$, dostáváme $3\,(x-2)^4/2 > -x$ pro $x < 0$.

*5.156.* Neboť

$$\lim_{x \to 0+} \operatorname{arctg} \frac{1}{x} = \frac{\pi}{2}, \qquad \lim_{x \to 0-} \operatorname{arctg} \frac{1}{x} = -\frac{\pi}{2},$$

uvažovaná oboustranná limita neexistuje.

*5.157.* První z limit je rovna $+\infty$, druhá neexistuje.

*5.158.* Limitu lze spočítat více způsoby. Nabízí se např.

$$\begin{aligned}\lim_{x \to 0} \frac{\operatorname{tg} x - \sin x}{\sin^3 x} &= \lim_{x \to 0} \left( \frac{\operatorname{tg} x - \sin x}{\sin^3 x} \cdot \frac{\operatorname{cotg} x}{\operatorname{cotg} x} \right) = \\ &= \lim_{x \to 0} \frac{1 - \cos x}{\cos x \cdot \sin^2 x} = \lim_{x \to 0} \frac{1 - \cos x}{\cos x \left(1 - \cos^2 x\right)} = \\ &= \lim_{x \to 0} \frac{1}{\cos x \,(1 + \cos x)} = \frac{1}{2}.\end{aligned}$$

*5.159.* Platí

$$\lim_{x \to \pi/6} \frac{2\sin^3 x + 7\sin^2 x + 2\sin x - 3}{2\sin^3 x + 3\sin^2 x - 8\sin x + 3} = \lim_{x \to \pi/6} \frac{\sin x + 1}{\sin x - 1} = -3.$$

*5.160.* Je

$$\lim_{x \to 1} \frac{x^m - 1}{x^n - 1} = \frac{m}{n}.$$

*5.161.* Po rozšíření výrazem

$$\frac{\sqrt{x^2 + x} + x}{\sqrt{x^2 + x} + x}$$

lze lehce dostat

$$\lim_{x \to +\infty} \left( \sqrt{x^2 + x} - x \right) = \frac{1}{2}.$$

*5.162.* Platí

$$\lim_{x \to +\infty} \left( x\sqrt{1 + x^2} - x^2 \right) = \frac{1}{2}.$$

*5.163.* Je

$$\lim_{x \to 0} \frac{\sqrt{2} - \sqrt{1 + \cos x}}{\sin^2 x} = \frac{\sqrt{2}}{8}.$$

*5.164.* Rozšířením zlomku ze zadání je možné obdržet

$$\lim_{x \to 0} \frac{\sin(4x)}{\sqrt{x+1} - 1} = 8.$$

*5.165.* Platí

$$\lim_{x \to 0-} \frac{\sqrt{1 + \operatorname{tg} x} - \sqrt{1 - \operatorname{tg} x}}{\sin x} = 1.$$

*5.166.* Zřejmě je

$$\lim_{x\to-\infty}\frac{2^x+\sqrt{1+x^2-x^9}-7x^5+44x^2}{3^x+\sqrt[5]{6x^6+x^2}-18x^5-592x^4}=\frac{7}{18}.$$

*5.167.* Výrok není pravdivý. Uvažte kupř.

$$f(x):=\frac{1}{x},\quad x\in(-\infty,0);\qquad g(x):=x,\quad x\in\mathbb{R}.$$

*5.168.*

$$\lim_{n\to\infty}\left(\frac{n}{n+5}\right)^{2n-1}=\mathrm{e}^{-10}.$$

*5.169.*

$$\lim_{x\to0-}\frac{\sin x-x}{x^3}=-\frac{1}{6}.$$

*5.170.* $f'(x)<0, x>\mathrm{e}$.

*5.171.* V bodě $x_1=\mathrm{e}^{-2}$ nabývá zadaná funkce lokálního maxima a v bodě $x_2=1$ potom lokálního minima.

*5.172.* Neexistuje: pro $a=\sqrt{2}/2$ nastává v daném bodě pouze lokální extrém.

*5.173.* $2=\mathrm{e}^{\frac{1}{\mathrm{e}}}-\ln\frac{1}{\mathrm{e}}$.

*5.174.* $\frac{1}{\sqrt[3]{\mathrm{e}}}$.

*5.175.* $4=p(-1)=p(2), -16=p(-3)$.

*5.176.* (a) $v(0)=6\,\mathrm{m/s}$; (b) $t=3\,\mathrm{s}, s(3)=16\,\mathrm{m}$; (c) $v(4)=-2\,\mathrm{m/s}, a(4)=-2\,\mathrm{m/s^2}$.

*5.177.* $f'(x_0)=\frac{1}{2\sqrt{x_0}}$.

*5.178.* Derivace neexistuje: jednostranné derivace, a to $\pi/2$ (jednostranná derivace zprava) a $-\pi/2$ (jednostranná derivace zleva), se nerovnají.

*5.179.* Ano.

*5.180.* Nikoli.

*5.181.* $f(x):=|x-5|+|x-9|$.

*5.182.* Např. $f=g$ pro funkci $f$ definovanou tak, že v racionálních bodech nabývá hodnoty 1, zatímco v iracionálních hodnoty $-1$.

*5.183.* (a) $x^2\ \sin x$; (b) $\cos(\sin x)\cdot\cos x$; (c) $\frac{3x^2+2}{x^3+2x}\ \cos\left(\ln\left(x^3+2x\right)\right)$; (d) $\frac{2(1-2x)}{(1-x+x^2)^2}$.

*5.184.* (a) $\frac{7}{8}\,x^{-\frac{1}{8}}$; (b) $\operatorname{cosec} x=\frac{1}{\sin x}$.

*5.185.* $\cos x\cdot\cos(\sin x)\cdot\cos(\sin(\sin x))$.

*5.186.* $f'(x)=\frac{1}{\sqrt{1+2x-x^2}}+1, x\in\left(1-\sqrt{2},1+\sqrt{2}\right)$.

*5.187.* $\frac{\cos x}{3\sqrt[3]{\sin^2 x}}$.

*5.188.* $\frac{1+2x^2}{\sqrt{1+x^2}}+x^2\,\mathrm{e}^x$.

*5.189.* $-8$.

*5.190.* $\frac{2x^2}{1-x^6}\sqrt[3]{\frac{1+x^3}{1-x^3}}$.

*5.191.* $\ln^2\left(x+\sqrt{1+x^2}\right), x\in\mathbb{R}$.

*5.192.* $f'(x)=-\frac{1}{x}\left(\log_x\mathrm{e}\right)^2, x>0, x\neq1$.

*5.193.* $\left[f(x)g(x)h(x)k(x)\right]'=f'(x)g(x)h(x)k(x)+f(x)g'(x)h(x)k(x)+f(x)g(x)h'(x)k(x)+$
$+f(x)g(x)h(x)k'(x)$.

*5.194.* $\frac{x^3\,(x+1)^2\,\sqrt[3]{x+2}}{(x+3)^2}\left(\frac{3}{x}+\frac{2}{x+1}+\frac{1}{3(x+2)}-\frac{2}{x+3}\right)$.

*5.209.* Vepsaný pravoúhelník má strany $x$, $\sqrt{3}/2(a-x)$, tedy obsah $\sqrt{3}/2(a-x)x$. Maximum pro $x=a/2$, tedy maximální obsah je $(\sqrt{3}/8)a^2$.

*5.210.* $4\,\mathrm{m}\times 4\,\mathrm{m}\times 2\,\mathrm{m}$.

*5.211.* $28=24+4$.

*5.212.* $a=1$.

*5.213.* $2\sqrt{5}\,r$.

*5.214.* Jedná se o čtverec (s délkou strany $c$).

*5.215.* $v=\frac{4}{3}R$, $r=\frac{2\sqrt{2}}{3}R$.

*5.216.* Největší obsah $\sqrt{3}\,o^2/36$ má rovnostranný trojúhelník.

*5.217.* $\left[2,-1/2\right]$, $\left[-2,-1/2\right]$.

*5.218.* $v=2r$.

*5.219.* Nejbližší bod $[1,1]$, vzdálenost $2\sqrt{2}$.

*5.220.* Nejbližší bod $[-1,1]$, vzdálenost $3\sqrt{2}$.

*5.221.* $t=1,5s$, vzdálenost $\sqrt{5}$ jednotek.

*5.222.* V čase $t=\frac{5}{13}\,s$ si budou auta nejblíže a to $\frac{\sqrt{13}}{13}$ jednotky.

*5.223.* $P=\pi rv+\pi r^2 \Longrightarrow v=\frac{P-\pi r^2}{\pi r} \Longrightarrow V=\frac{1}{3}r(P-\pi r^2)$. Extrém $r=\sqrt{\frac{P}{3\pi}}$, dosazením do objemu $V=\frac{2\pi}{3}\ \mathrm{cm}^3$.

*5.224.* (a) $12\,\mathrm{ft/s}$; (b) $-59,5\,\mathrm{ft}^2/\mathrm{s}$; (c) $-1\,\mathrm{rad/s}$.

*5.225.* Při produkci zhruba 3 414 výrobků denně.

*5.226.* Trojnásobné použití l'Hospitalova pravidla dává

$$\lim_{x\to 0-}\frac{\sin x-x}{x^3}=-\frac{1}{6}.$$

*5.227.* $2/\pi$.

*5.228.*

$$\lim_{x\to\frac{\pi}{2}-}\left(\frac{\pi}{2}-x\right)\operatorname{tg}x=1.$$

*5.229.*

$$\lim_{x\to+\infty}\left(\left(3^{\frac{1}{x}}-2^{\frac{1}{x}}\right)x\right)=\ln\frac{3}{2}.$$

*5.230.* $1/2$.

*5.231.* Platí

$$\lim_{x\to+\infty}\left(\cos\frac{2}{x}\right)^{x^2}=\mathrm{e}^{-2}.$$

*5.232.* Dvojnásobnou aplikací l'Hospitalova pravidla lze obdržet

$$\lim_{x\to 0}(1-\cos x)^{\sin x}=\mathrm{e}^0=1.$$

*5.233.* V obou případech je výsledek $\mathrm{e}^{\alpha}$.

*5.234.* Limitu lze snadno určit např. pomocí l'Hospitalova pravidla.

*5.243.* $2a^2$; $4a\left(2+\sqrt{2}\right)$.

*5.244.* $\pi/2$.

*5.245.* $x=\frac{\pi}{6}+k\pi$, $x=\frac{5\pi}{6}+k\pi$, $k\in\mathbb{Z}$.

*5.246.* 5.
*5.247.* $+\infty$.
*5.248.* $3/2$.
*5.249.* (a) 3; (b) $9/4$.
*5.250.* $1/2$.
*5.251.* (a) $3/4$; (b) $1/4$.
*5.252.* $-1/2$.
*5.253.* $11/18$.
*5.254.* $s/2$; $3s/2$ ($s = \ln 2$).
*5.255.* Konverguje.
*5.256.* Postačuje uvážit nutnou podmínku konvergence $\lim_{n\to\infty} a_n = 0$.
*5.257.* $\alpha > 0$; $\beta \in \{-2, -1, 0, 1, 2\}$; $\gamma \in (-\infty, -1) \cup (1, +\infty)$.
*5.258.* Konverguje absolutně.
*5.259.* Limita je rovna 1/2.
*5.260.* $A \in [0, 1)$.
*5.261.* Součet uvedené řady je konečný – řada konverguje.
*5.262.* Např. $a_n = n/3$, $b_n = n/2$, $n \in \mathbb{N}$.
*5.263.* První řada konverguje absolutně; druhá neabsolutně.
*5.264.* Ano.
*5.265.* $p \in \mathbb{R}$.

KAPITOLA 6

# Diferenciální a integrální počet

*zvěřinec teď máme, ale co s ním?*
*– naučíme se s ním zacházet...*



## A. Derivace vyšších řádů

Nejprve zaveďme konvenci, jak značit derivace vyšších řádů: druhou derivaci funkce $f$ jedné proměnné budeme značit $f''$ nebo $f^{(2)}$, derivace od třetího řádu výše pak pouze $f^{(3)}$, $f^{(4)}$, …, $f^{(n)}$. Na připomenutí ale zahájíme trochu rafinovaným příkladem „pouze“ na první derivace.

**6.1.** Derivujte výraz

$$\frac{\sqrt[4]{x-1}\cdot(x+2)^3}{\mathrm{e}^x(x+132)^2}$$

proměnné $x > 1$.

**Řešení.** Úlohu vyřešíme pomocí tzv. logaritmické derivace. Nechť je $f$ libovolná kladná funkce. Víme, že je

$$\big[\ln f(x)\big]' = \frac{f'(x)}{f(x)}, \quad \text{tj.} \quad f'(x) = f(x)\cdot\big[\ln f(x)\big]',$$

pokud derivace $f'(x)$ existuje. Užitečnost tohoto vzorce je dána tím, že pro jisté funkce je jednodušší derivovat jejich logaritmus než je samé.

V minulé kapitole jsme si postupně hráli buď s mimořádně velikými třídami funkcí — všechny spojité, všechny diferencovatelné apod. — nebo jen s konkrétními funkcemi — např. exponenciální, goniometrické, polynomy atd. Měli jsme ale přitom minimum nástrojů a vše jsme počítali tak říkajíc na koleně. Z kvalitativního pohledu jsme jen naznačili, jak využívat znalost lineárního přiblížení funkce její derivací k diskusi lokálního chování takové funkce kolem daného bodu. Teď dáme dohromady několik výsledků, které umožní snáze pracovat s funkcemi při modelování reálných problémů.

Pomocí derivování jsme se naučili zaznamenávat velkosti okamžitých změn. V této kapitole se vyrovnáme i s úlohou, jak sčítat nekonečně mnoho takových „nekonečně malých“ změn, tj. jak „integrovat“. Nejdříve si ale uděláme více jasno o derivacích.

V poslední části kapitoly se vrátíme k řadám funkcí a doplníme přitom i několik chybějících kroužků v naší dosavadní argumentaci.

## 1. Derivování

**6.1. Derivace vyšších řádů.** Jestliže má první derivace $f'(x)$ reálné nebo komplexní funkce $f$ v bodě $x_0$ derivaci $(f')'(x_0)$, říkáme že existuje *druhá derivace* funkce $f$, resp. derivace druhého řádu.



Píšeme pak $f''(x_0) = (f')'(x_0)$ nebo také $f^{(2)}(x_0)$.

Funkce $f$ je *dvakrát diferencovatelná* na nějakém intervalu, jestliže má druhou derivaci v každém jeho bodě. Derivace vyšších řádů definujeme induktivně:

*k*–KRÁT DIFERENCOVATELNÉ FUNKCE

Reálná nebo komplexní funkce $f$ je $(k+1)$*–krát diferencovatelná* v bodě $x_0$ , pro nějaké přirozené číslo $k$, jestliže je $k$–krát diferencovatelná na nějakém okolí bodu $x_0$ a její $k$–tá derivace má v bodě $x_0$ derivaci. Pro $k$-tou derivaci funkce $f(x)$ píšeme $f^{(k)}(x)$. Pro $k = 0$ rozumíme 0–krát diferencovatelnými funkcemi funkce spojité.

Jestliže existují derivace všech řádů na intervalu, říkáme, že je tam funkce $f$ *hladká*.

Pro funkce se spojitou $k$–tou derivací používáme označení *třída funkcí* $C^k(A)$ na intervalu $A$, kde $k$ může nabývat hodnot $1, 2, \ldots, \infty$. Často píšeme pouze $C^k$, je-li definiční obor znám z kontextu.

Píšeme také $C^0(A)$ nebo $C(A)$ pro funkce spojité na množině $A$. Jde-li o interval, píšeme bez závorek, např. $C[a,b]$.

Takový je právě výraz v zadání. Dostáváme totiž

$$\left(\frac{\sqrt[4]{x-1}\cdot(x+2)^3}{\mathrm{e}^x(x+132)^2}\right)' = \frac{\sqrt[4]{x-1}\cdot(x+2)^3}{\mathrm{e}^x(x+132)^2}\cdot\left[\ln\frac{\sqrt[4]{x-1}\cdot(x+2)^3}{\mathrm{e}^x(x+132)^2}\right]' =$$
$$= \frac{\sqrt[4]{x-1}\cdot(x+2)^3}{\mathrm{e}^x(x+132)^2}\cdot\left[3\ln(x+2)+\frac{1}{4}\ln(x-1)-x\,\ln\mathrm{e}-2\ln(x+132)\right]' =$$
$$= \frac{\sqrt[4]{x-1}\cdot(x+2)^3}{\mathrm{e}^x(x+132)^2}\left[\frac{3}{x+2}+\frac{1}{4(x-1)}-1-\frac{2}{x+132}\right].$$

□

**6.2.** Určete následující derivace:

i) $(x^2\cdot\sin x)''$,
ii) $(x^x)''$,
iii) $\left(\frac{x}{\ln x}\right)^{(3)}$,
iv) $(x^n)^{(n)}$,
v) $(\sin x)^{(n)}$.

**Řešení.**

(a) $(x^2\cdot\sin x)'' = (2x\sin x + x^2\cos x)' = 2\sin x + 4x\cos x - x^2\sin x$.

(b) $(x^x)'' = [(1+\ln x)x^x]' = x^{x-1} + x^x(1+\ln x)^2$.

(c) $\left(\frac{x}{\ln x}\right)^{(3)} = \frac{1}{x^2(\ln x)^2} - \frac{6}{x^2(\ln x)^4}$.

(d) $(x^n)^{(n)} = \left[(x^n)'\right]^{(n-1)} = (nx^{n-1})^{(n-1)} = \cdots = n!$.

(e) $(\sin x)^{(n)} = \mathrm{re}(i^n\sin x) + \mathrm{im}(i^n\cos x)$. □

**6.3.** Nechť $n\in\mathbb{N}$ je libovolné. Najděte $n$-tou derivaci funkce

$$y = \ln\tfrac{1+x}{1-x},\quad x\in(-1,1).$$

**Řešení.** Vzhledem k vyjádření

$$\ln\tfrac{1+x}{1-x} = \ln(1+x) - \ln(1-x)\,,\quad x\in(-1,1)$$

zavedeme pomocnou funkci

$$f(x) := \ln(ax+1)\,,\quad x\in(-1,1),\ a=\pm1.$$

Pro $x\in(-1,1)$ lze snadno (postupně) vypočíst

$$f'(x) = \tfrac{a}{ax+1}\,,$$
$$f''(x) = \tfrac{-a^2}{(ax+1)^2}\,,$$
$$f^{(3)}(x) = \tfrac{2a^3}{(ax+1)^3}\,,$$
$$f^{(4)}(x) = \tfrac{-6a^4}{(ax+1)^4}\,.$$

Na základě těchto výsledků můžeme usoudit, že

$$f^{(n)}(x) = \frac{(-1)^{n-1}(n-1)!\,a^n}{(ax+1)^n},\quad x\in(-1,1),\ n\in\mathbb{N}. \tag{6.1}$$

Správnost tohoto vzorce ověříme matematickou indukcí. Protože pro $n=1,2,3,4$ platí, zbývá ukázat, že z jeho platnosti pro $k\in\mathbb{N}$ plyne jeho platnost pro $k+1$. Neboť přímý výpočet dává

$$f^{(k+1)}(x) = \left(\frac{(-1)^{k-1}(k-1)!\,a^k}{(ax+1)^k}\right)' = \frac{(-1)^{k-1}(k-1)!\,a^k\,(-k)\,a}{(ax+1)^{k+1}} = \frac{(-1)^k k!\,a^{k+1}}{(ax+1)^{k+1}},$$

vzorec (‖6.1‖) platí pro všechna $n\in\mathbb{N}$. Podle něj je

$$\ln^{(n)}(1+x) = \tfrac{(-1)^{n-1}(n-1)!}{(x+1)^n},\quad \ln^{(n)}(1-x) = -\tfrac{(n-1)!}{(-x+1)^n},\quad x\in(-1,1).$$

Pojem derivace vyššího řádu můžeme rychle ilustrovat na polynomech. Protože výsledkem derivování polynomu je opět polynom, ale derivací se vždy o jedničku snižuje jeho stupeň, dostaneme po konečném počtu derivací nulový polynom. Přesněji řečeno, právě po $k+1$ derivacích, kde $k$ je stupeň polynomu, dostaneme nulu. Samozřejmě pak existují derivace všech řádů, tj. $f\in C^\infty(\mathbb{R})$.

Při konstrukci splajnů, viz 5.9, jsme pohlídali, aby výsledné funkce byly třídy $C^2(\mathbb{R})$. Jejich třetí derivace budou po částech konstantní funkce. Proto nebudou splajny patřit do $C^3(\mathbb{R})$, přestože jejich všechny derivace vyšších řádů budou nulové ve všech vnitřních bodech jednotlivých intervalů v interpolaci. Promyslete si podrobně tento příklad!

Následující tvrzení je jednoduchým kombinatorickým důsledkem Leibnizova pravidla pro derivaci součinu funkcí:

**Lemma.** *Jsou-li $f$ a $g$ dvě funkce mající derivaci řádu $k$ v bodě $x_0$, pak má derivaci řádu $k$ i jejich součin a platí:*

$$(f\cdot g)^{(k)}(x_0) = \sum_{i=0}^{k}\binom{k}{i}f^{(i)}(x_0)g^{(k-i)}(x_0).$$

Důkaz. Pro $k=0$ je tvrzení triviální, pro $k=1$ je to Leibnizovo pravidlo pro derivaci součinu. Jestliže pravidlo platí pro nějaké $k$, derivací pravé strany a použitím Leibnizova pravidla dostaneme obdobný výraz

$$\sum_{i=0}^{k}\binom{k}{i}\Big(f^{(i+1)}(x_0)g^{(k-i)}(x_0) + f^{(i)}(x_0)g^{(k-i+1)}(x_0)\Big).$$

V této nové sumě je součet řádů derivací u součinů v jednotlivých sčítancích $k+1$ a koeficienty u $f^{(j)}(x_0)g^{(k+1-j)}(x_0)$ jsou součty binomických koeficientů $\binom{k}{j-1}+\binom{k}{j}=\binom{k+1}{j}$. □

**6.2. Násobné kořeny a inverze polynomů.** Derivace polynomů jsme spočítali již v odstavci 5.6 a je vidět, že jde o hladké funkce. Derivace je v tomto případě vlastně prosté algebraické zobrazení a podívejme se, jak se nám derivace bude hodit pro diskusi násobných kořenů polynomů.



Nejprve zformulujme *základní větu algebry*, jejíž důkaz odložíme do odstavce 11.20 na straně 663.

**Věta.** *Každý nenulový komplexní polynom $f:\mathbb{C}\to\mathbb{C}$ stupně alespoň jedna má kořen.*

Nutně tedy polynom stupně $k>0$ má právě $k$ komplexních kořenů včetně násobností a můžeme jej vždy psát jednoznačně ve tvaru

$$f(x) = b(x-a_1)^{c_1}\cdot(x-a_q)^{c_q},$$

kde $b\in\mathbb{C}$, $b\neq0$, $a_1,\dots,a_q$ jsou všechny kořeny polynomu $f$ a $1\le c_1,\dots,c_q\le k$ jsou jejich násobnosti (tj. přirozená čísla).

Derivací $f(x)$ jakožto funkce reálné proměnné $x$ dostaneme

$$f'(x) = bc_1(x-a_1)^{c_1-1}\dots(x-a_q)^{c_q} + \cdots +$$
$$+ bc_q(x-a_1)^{c_1}\dots(x-a_q)^{c_q-1}.$$

Jestliže je $c_1=1$ a kořen $a_1$ je reálný, bude hodnota derivace $f'$ v bodě $a_1$ nenulová, protože první člen výrazu je nenulový, zatímco všechny zbývající po dosazení hodnoty $x=a_1$ zmizí. Obdobně to bude i s ostatními kořeny. Ověřili jsme tedy užitečnou vlastnost, že reálný kořen $a$ polynomu $f$ je vícenásobný tehdy a jen tehdy,

Odtud již dostáváme výsledek

$$\left(\ln\tfrac{1+x}{1-x}\right)^{(n)} = (n-1)!\left(\tfrac{1}{(1-x)^n} - \tfrac{(-1)^n}{(1+x)^n}\right)$$

pro $x \in (-1, 1)$ a $n \in \mathbb{N}$. □

*6.4.* Určete druhou derivaci funkce $y = \operatorname{tg} x$ na celém jejím definičním oboru, tj. pro $\cos x \neq 0$. ○

*6.5.* Stanovte pátou a šestou derivaci polynomu

$p(x) = \left(3x^2 + 2x + 1\right) \cdot (2x - 6) \cdot \left(2x^2 - 5x + 9\right), \quad x \in \mathbb{R}$. ○

*6.6.* Bez počítání uveďte 12. derivaci funkce

$y = \mathrm{e}^{2x} + \cos x + x^{10} - 5x^7 + 6x^3 - 11x + 3, \quad x \in \mathbb{R}$. ○

*6.7.* Napište 26. derivaci funkce

$f(x) = \sin x + x^{23} - x^{18} + 15x^{11} - 13x^8 - 5x^4 - 11x^3 + 16 + \mathrm{e}^{2x}$

pro $x \in \mathbb{R}$. ○

Ukažme si ještě některé zajímavé příklady na užití diferenciálního počtu. Nejprve však zmiňme Jensenovu nerovnost, která hovoří o konvexních, resp. konkávních funkcích a kterou dále využijeme.

**6.8. Jensenova nerovnost.** Pro ostře konvexní funkci $f$ na intervalu $I$ a pro libovolné body $x_1, \ldots, x_n \in I$ a reálná čísla $c_1, \ldots, c_n > 0$ taková, že $c_1 + \cdots + c_n = 1$, platí

$$f\left(\sum_{i=1}^{n} c_i\, x_i\right) \leq \sum_{i=1}^{n} c_i\, f\,(x_i)\,,$$

přičemž rovnost nastane, právě když je $x_1 = \cdots = x_n$.

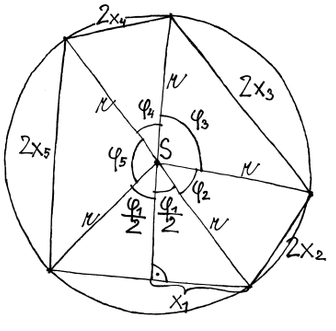
**Řešení.** Důkaz lze nalézt v literatuře. □



**Poznámka.** Jensenovu nerovnost lze zformulovat i více intuitivně: těžiště hmotných bodů umístěných na grafu ostře konvexní funkce leží nad tímto grafem.

**6.9.** Dokažte, že mezi všemi (konvexními) $n$-úhelníky vepsanými do kružnice má největší obsah právě pravidelný $n$-úhelník (pro libovolné $n \geq 3$).

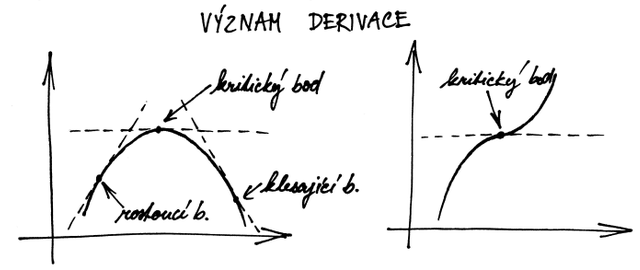
**Řešení.** Stačí uvažovat $n$-úhelníky, uvnitř kterých leží střed kružnice. Každý takový $n$-úhelník vepsaný do dané kružnice o poloměru $r$ rozdělíme podle obrázku na $n$ trojúhelníků s obsahy $S_i$, $i \in \{1, \ldots, n\}$. Vzhledem k tomu, že




$$\sin\tfrac{\varphi_i}{2} = \tfrac{x_i}{r}, \quad \cos\tfrac{\varphi_i}{2} = \tfrac{h_i}{r}, \qquad i \in \{1, \ldots, n\},$$

když je zároveň kořenem jeho derivace $f'$. (Toto tvrzení si časem rozšíříme i na všechny komplexní kořeny.)

**6.3. Význam druhé derivace.** Již jsme viděli, že první derivace funkce je jejím lineárním přiblížením v okolí daného bodu a že ze znaménka nenulové derivace vyplývá, že funkce je v bodě $x_0$ rostoucí nebo klesající. Body, ve kterých je první derivace nulová se nazývají *kritické body* nebo také *stacionární body* dané funkce.




Je-li $x_0$ stacionární bod funkce $f$, může být chování funkce $f$ v okolí bodu $x_0$ jakékoliv. Vidíme to již z chování funkce $f(x) = x^n$ v okolí nuly pro libovolné $n$. Pro lichá $n > 0$ bude $f(x)$ rostoucí, pro sudá $n$ naopak bude nalevo klesající a napravo rostoucí, dosáhne tedy v bodě $x_0$ své minimální hodnoty mezi body z (dostatečně malého) okolí bodu $x_0 = 0$.

Tentýž pohled můžeme aplikovat na funkci $f'$. Jestliže totiž je druhá derivace nenulová, určuje její znaménko chování derivace první. Proto v kritickém bodě $x_0$ bude derivace $f'(x)$ rostoucí při kladné druhé derivaci a klesající při záporné. Jestliže je ale rostoucí, znamená to, že nutně bude záporná nalevo od kritického bodu a kladná napravo od něj. Funkce $f$ v takovém případě je klesající nalevo od kritického bodu a rostoucí napravo od něj. To znamená, že má funkce $f$ v bodě $x_0$ minimum ze všech hodnot z nějakého malého okolí bodu $x_0$.

Naopak, je-li druhá derivace záporná v $x_0$, je první derivace klesající, tedy záporná vlevo od $x_0$ a kladná vpravo. Funkce $f$ bude tedy mít v bodě $x_0$ maximální hodnotu ze všech hodnot na nějakém okolí.

Funkce diferencovatelná na $(a, b)$ a spojitá na $[a, b]$ má jistě na tomto intervalu absolutní maximum a minimum. Může ho dosáhnout pouze buď na hranici nebo v bodě s nulovou derivací, tj. v kritickém bodě. Pro diskusi extrémů nám tedy mohou stačit kritické body a druhé derivace pomůžou určit typy extrémů, pokud jsou nenulové. Pro přesnější diskusi ale potřebujeme lepší než lineární aproximace zkoumaných funkcí. Proto se nejprve budeme věnovat úvahám v tomto směru a teprve poté se vrátíme k diskusi průběhu funkcí.

**6.4. Taylorův rozvoj.** Jako překvapivě jednoduché využití Rolleovy věty teď odvodíme mimořádně důležitý výsledek. Říkává se mu *Taylorův rozvoj se zbytkem*. Intuitivně se k němu můžeme dostat obrácením našich úvah kolem mocninných řad. Máme-li totiž mocninnou řadu se středem v bodě $a$,

$$S(x) = \sum_{n=0}^{\infty} a_n (x-a)^n,$$

a derivujeme-li ji opakovaně, dostáváme mocninné řady (víme, že je možné takový výraz derivovat člen po členu, i když jsme to ještě

platí

$$S_i = x_i\, h_i = r^2 \sin\tfrac{\varphi_i}{2} \cos\tfrac{\varphi_i}{2} = \tfrac{1}{2} r^2 \sin\varphi_i, \quad i \in \{1, \dots, n\}.$$

Odsud plyne, že obsah celého $n$-úhelníku je

$$S = \sum_{i=1}^{n} S_i = \tfrac{1}{2} r^2 \sum_{i=1}^{n} \sin\varphi_i.$$

Chceme tedy maximalizovat součet $\sum_{i=1}^{n} \sin\varphi_i$, přičemž pro hodnoty $\varphi_i \in (0, \pi)$ musí zjevně být

$$\varphi_1 + \cdots + \varphi_n = \sum_{i=1}^{n} \varphi_i = 2\pi. \tag{6.2}$$

Funkce $y = \sin x$ je ostře konkávní na intervalu $(0, \pi)$, což znamená, že funkce $y = -\sin x$ je na tomto intervalu ostře konvexní. Podle Jensenovy nerovnosti pro $c_i = 1/n$ a $x_i = \varphi_i$ je proto

$$-\sin\left(\sum_{i=1}^{n} \tfrac{1}{n}\, \varphi_i\right) \le -\sum_{i=1}^{n} \tfrac{1}{n}\, \sin\varphi_i,$$

$$\text{tj.} \quad \sin\left(\sum_{i=1}^{n} \tfrac{1}{n}\, \varphi_i\right) \ge \sum_{i=1}^{n} \tfrac{1}{n}\, \sin\varphi_i.$$

Navíc víme, že rovnost nastává právě pro $\varphi_1 = \cdots = \varphi_n$. Když tak vyjádříme (s pomocí (‖6.2‖))

$$S = \tfrac{r^2 n}{2} \sum_{i=1}^{n} \tfrac{1}{n}\, \sin\varphi_i \le \tfrac{r^2 n}{2} \sin\left(\sum_{i=1}^{n} \tfrac{1}{n}\, \varphi_i\right) = \tfrac{r^2 n}{2} \sin\tfrac{2\pi}{n},$$

vidíme, že $S$ může nabývat nejvýše hodnoty na pravé straně. Ovšem to nastane tehdy a jenom tehdy, když je $\varphi_1 = \cdots = \varphi_n$ (volili jsme $x_i = \varphi_i$). Maximální obsah má tudíž pravidelný $n$-úhelník, neboť právě pro něj je $\varphi_1 = \cdots = \varphi_n = 2\pi/n$. □

**6.10. Izoperimetrický podíl.** Pro uzavřenou rovinnou křivku ohraničující jistý obrazec se definuje její izoperimetrický podíl jako číslo

$$I\,Q := \frac{S}{\pi\left(\frac{o}{2\pi}\right)^2} = \frac{4\pi S}{o^2},$$

kde $S$ udává obsah uvažovaného obrazce a $o$ jeho obvod (tj. délku křivky). Izoperimetrický podíl tedy udává podíl obsahu obrazce a obsahu kruhu, který má stejný obvod jako daný obrazec. Označení $I\,Q$ je tak nejen anglickou zkratkou izoperimetrického podílu, ale lze jej označit i za „inteligenci útvaru“ s jakou využívá svůj obvod pro vytvoření co největší plochy. Izoperimetrická věta pak říká, že pro každou uzavřenou křivku je její $I\,Q \le 1$, přičemž rovnost nastává jedině pro kružnici, neboli že („kružnice je nejchytřejší“).

Určete $I\,Q$ pro pravidelný mnohoúhelník a kružnici a najděte kruhovou výseč, pro niž je IQ její hranice největší.

**Řešení.** Nejdříve si uvědomme, že hodnota $I\,Q$ se nemění při změně měřítka na osách (na obou shodné).

Podle obrázku je

$$h = \cos\varphi = \cos\tfrac{\pi}{n}, \qquad \tfrac{x}{2} = \sin\varphi = \sin\tfrac{\pi}{n},$$

nedokázali)

$$S^{(k)}(x) = \sum_{n=k}^{\infty} n(n-1)\dots(n-k+1) a_n (x-a)^{n-k}.$$

V bodě $x = a$ je tedy $S^{(k)}(a) = k! a_k$. Můžeme tedy naopak číst poslední tvrzení jako rovnici pro $a_k$ a původní řadu přepsat jako

$$S(x) = \sum_{n=0}^{\infty} \frac{1}{k!} S^{(k)}(a)(x-a)^n.$$

Jestliže místo mocninné řady máme nějakou dostatečně hladkou funkci $f(x)$, je tedy na místě se ptát, zda ji můžeme vyjádřit jako mocninnou řadu a jak rychle budou konvergovat částečné součty (tj. přiblížení funkce $f$ polynomy). Naše úvaha právě naznačila, že můžeme očekávat v okolí bodu $a$ dobrou aproximaci polynomy.

TAYLOROVY POLYNOMY FUNKCE $f$

Pro $k$–krát diferencovatelnou funkci $f$ definujeme její *Taylorův polynom k–tého stupně* vztahem

$$T_{k,a} f(x) = f(a) + f'(a)(x-a) + \frac{1}{2} f''(a)(x-a)^2 + \\ + \frac{1}{6} f^{(3)}(a)(x-a)^3 + \cdots + \frac{1}{k!} f^{(k)}(a)(x-a)^k.$$

Přesná odpověď vypadá podobně jako věta o střední hodnotě, jen pracujeme s vyššími stupni polynomů:

**Věta** (Taylorův rozvoj se zbytkem)**.** *Nechť je $f(x)$ funkce k–krát diferencovatelná na intervalu $(a, b)$ a spojitá na $[a, b]$. Pak pro každé $x \in (a, b)$ existuje číslo $c \in (a, x)$ takové, že*

$$f(x) = f(a) + f'(a)(x-a) + \cdots + \\ + \frac{1}{(k-1)!} f^{(k-1)}(a)(x-a)^{k-1} + \frac{1}{k!} f^{(k)}(c)(x-a)^k = \\ = T_{k-1,a} f(x) + \frac{1}{k!} f^{(k)}(c)(x-a)^k.$$

DŮKAZ. Definujme zbytek $R$ (tj. chybu při aproximaci pro pevně zvolené $x$) takto



$$f(x) = T_{k-1,a} f(x) + R$$

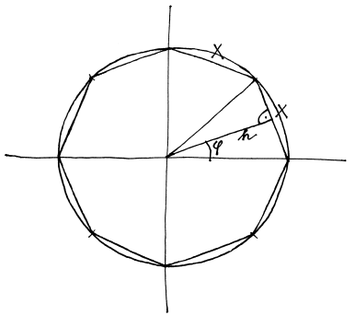
tj. $R = \frac{1}{k!} r (x-a)^k$ pro vhodné číslo $r$ (závislé na $x$). Nyní uvažujme funkci $F(\xi)$ definovanou

$$F(\xi) = \sum_{j=0}^{k-1} \frac{1}{j!} f^{(j)}(\xi)(x-\xi)^j + \frac{1}{k!} r (x-\xi)^k.$$

Její derivace (přičemž $x$ je pro nás konstantní parametr) je

$$F'(\xi) = f'(\xi) + \\ + \sum_{j=1}^{k-1} \left( \frac{1}{j!} f^{(j+1)}(\xi)(x-\xi)^j - \frac{1}{(j-1)!} f^{(j)}(\xi)(x-\xi)^{j-1} \right) - \\ - \frac{1}{(k-1)!} r (x-\xi)^{k-1} = \\ = \frac{1}{(k-1)!} f^{(k)}(\xi)(x-\xi)^{k-1} - \frac{1}{(k-1)!} r (x-\xi)^{k-1} = \\ = \frac{1}{(k-1)!} (x-\xi)^{k-1} (f^{(k)}(\xi) - r),$$

Když se totiž rozměry obrazce $a$-krát zvětší (pro libovolné $a > 0$), obvod se také zvětší $a$-krát a obsah $a^2$-krát (jde o plošnou míru). Takže $IQ$ nezávisí na velikosti obrazce, nýbrž pouze na jeho tvaru. Uvažujme proto pravidelný $n$-úhelník vepsaný do jednotkové kružnice.




což dává vyjádření pro jeho obvod

$$o_n = n \cdot x = 2n \sin \tfrac{\pi}{n}$$

i obsah

$$S_n = n \cdot \tfrac{1}{2}\, hx = n \cos \tfrac{\pi}{n} \sin \tfrac{\pi}{n}.$$

Pro pravidelný $n$-úhelník tak je

$$IQ = \frac{4\pi n \cos \frac{\pi}{n} \sin \frac{\pi}{n}}{4n^2 \sin^2 \frac{\pi}{n}} = \frac{\pi}{n} \operatorname{cotg} \frac{\pi}{n},$$

což můžeme ověřit kupř. pro čtverec ($n = 4$) s délkou strany $a$, kdy máme

$$IQ = \frac{4\pi a^2}{(4a)^2} = \frac{\pi}{4} = \frac{\pi}{4} \operatorname{cotg} \frac{\pi}{4}.$$

Provedeme-li limitní přechod pro $n \to \infty$ s použitím limity

$$\lim_{x \to 0} \frac{\sin x}{x} = 1,$$

dostaneme izoperimetrický podíl pro kružnici

$$IQ = \lim_{n \to \infty} \frac{\pi}{n} \operatorname{cotg} \frac{\pi}{n} = \lim_{n \to \infty} \frac{\cos \frac{\pi}{n}}{\frac{\sin \frac{\pi}{n}}{\frac{\pi}{n}}} = \frac{\cos 0}{1} = 1.1$$

Pochopitelně jsme také mohli pro kružnici o poloměru $r$ přímo vypočítat

$$IQ = \frac{4\pi S}{o^2} = \frac{4\pi(\pi r^2)}{(2\pi r)^2} = 1.$$

Pro hranici kruhové výseče o poloměru $r$ a středovém úhlu $\varphi \in (0, 2\pi)$ je

$$IQ = \frac{4\pi S}{o^2} = \frac{4\pi\, \frac{\varphi r^2}{2}}{(2r + r\varphi)^2} = \frac{2\pi\varphi}{(2+\varphi)^2}.$$

Hledáme tedy maximum funkce

$$f(\varphi) := \frac{2\pi\varphi}{(2+\varphi)^2}, \qquad \varphi \in (0, 2\pi).$$

Výpočtem

$$f'(\varphi) = 2\pi\, \frac{(2+\varphi)^2 - 2\varphi(2+\varphi)}{(2+\varphi)^4} = 2\pi\, \frac{2-\varphi}{(2+\varphi)^3}, \quad \varphi \in (0, 2\pi)$$

však snadno získáváme, že

$$f'(\varphi) > 0, \quad \varphi \in (0, 2), \qquad f'(\varphi) < 0, \quad \varphi \in (2, 2\pi).$$

Funkce $f$ tedy nabývá maximální hodnoty pro $\varphi_0 = 2$ a při středovém úhlu $\varphi_0 = 2$ (radiány) dostáváme největší

$$IQ = \frac{2\pi\varphi_0}{(2+\varphi_0)^2} = \frac{\pi}{4}.$$

protože výrazy v sumě se postupně vzájemně ruší. Nyní si stačí všimnout, že $F(a) = F(x) = f(x)$ (připomeňme, že $x$ je libovolně zvolená ale pevná hodnota v intervalu $(a, b)$). Proto podle Rolleovy věty existuje číslo $c$, $a < c < x$, takové, že $F'(c) = 0$. To ale je právě požadovaný vztah. □

**6.5. Odhady pro rozvoje se zbytkem.** Obzvlášť jednoduchý je Taylorův rozvoj libovolného polynomu

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0.$$

Protože je $(n+1)$–ní derivace $f$ identicky nulová, má Taylorův polynom stupně $n$ nulový zbytek a tedy je pro každé $x_0 \in \mathbb{R}$

$$f(x) = f(x_0) + f'(x_0)(x - x_0) + \cdots + \frac{1}{n!} f^{(n)}(x_0)(x - x_0)^n$$

a všechny derivace snadno vyčíslíme (např. poslední výraz je vždy tvaru $a_n(x - x_0)^n$).

Tento výsledek je velmi speciálním odhadem chyby v Taylorově rozvoji se zbytkem. Víme totiž předem, že zbytek je odhadnutelný pomocí velikosti derivace a ta je u polynomu od určitého řádu identicky nulová.

I obecněji vede odhad velikost $k$–té derivace na nějakém intervalu k odhadu chyby na témže intervalu. Speciálním případem je také věta o střední hodnotě coby aproximace Taylorovým rozvojem řádu nula, viz (5.9).

Dobrým příkladem pro rozvoj libovolného stupně jsou goniometrické funkce sin a cos. Iterováním derivace funkce $\sin x$ dostaneme vždy buď sinus nebo cosinus s nějakým znaménkem, ale v absolutní hodnotě budou hodnoty vždy nejvýše jedna. Dostáváme tedy přímý odhad rychlosti konvergence mocninné řady

$$|\sin x - (T_{k,0} \sin)(x)| \leq \frac{|x|^{k+1}}{(k+1)!}.$$

Odhad ukazuje, že pro $x$ výrazně menší než $k$ bude chyba malá, pro $x$ srovnatelné s $k$ nebo větší ale bude obrovská. Srovnej s obrázkem aproximace funkce $\cos x$ Taylorovým polynomem stupně 68 v odstavci 5.52.

Jak jsme zmínili v úvodu diskuse Taylorova rozvoje funkcí, pokud začneme s mocninnou řadou $f(x)$ se středem v bodě $a$, pak její částečné součty splývají s Taylorovými polynomy $T_{k,a} f(x)$. Následující tvrzení je jednou z jednoduchých formulací opačné implikace, tj. kdy je daná funkce $f(x)$ ve skutečnosti mocninnou řadou.

**Důsledek** (Taylorova věta)**.** *Předpokládejme, že funkce $f(x)$ je na intervalu $(a - \rho, a + \rho)$ hladká a že všechny její derivace jsou zde omezeny stejnoměrně konstantou $M > 0$, tj.*

$$|f^{(k)}(x)| \leq M, \quad k = 0, 1, \ldots, \; x \in (a - \rho, a + \rho).$$

*Pak mocninná řada $S(x) = \sum_{n=0}^{\infty} \frac{1}{k!} f^{(k)}(a)(x - a)^n$ konverguje na intervalu $(a - \rho, a + \rho)$ k funkci $f(x)$.*

Důkaz. Důkaz je shodný s úvahou v konkrétním případě funkce $\cos x$ výše. Promyslete si podrobnosti! □

**6.6. Analytické a hladké funkce.** Je-li $f$ v bodě $a$ hladká, pak můžeme napsat formálně mocninnou řadu

$$S(x) = \sum_{n=0}^{\infty} \frac{1}{k!} f^{(k)}(a)(x - a)^n.$$

Pokud má tato mocninná řadanenulový poloměr konvergence a zároveň platí $S(x) = f(x)$ na příslušném intervalu, pak říkáme, že

Doplňme ještě, že pro těleso v trojrozměrném prostoru (přesněji řečeno, pro uzavřenou plochu, která je jeho hranicí) se klade

$$IQ := \frac{V}{\frac{4\pi}{3}\left(\frac{S}{4\pi}\right)^{\frac{3}{2}}},$$

kde $V$ je objem a $S$ povrch tělesa. Porovnáváme tedy objem tělesa daného povrchu s objemem koule téhož povrchu.○ □

**6.11.** Je dán provázek délky $l$. Máte jej rozstříhat na $n$ částí tak, aby



ze vzniklých $n$ menších provázků bylo možné vytvořit hranice předem daných geometrických obrazců (kupř. čtverce, trojúhelníku, kruhu, půlkruhu) s nejmenším součtem ploch.

**Řešení.** K vyřešení příkladu použijeme izoperimetrický podíl křivek a Jensenovu nerovnost (uvedené v předchozích příkladech). Pro předem určené geometrické obrazce označujme hodnoty jejich izoperimetrických podílů jako

$$\frac{1}{\lambda_i} := \frac{4\pi S_i}{o_i^2}, \qquad i \in \{1, \ldots, n\},$$

přičemž $S_i$ je obsah a $o_i$ obvod $i$-tého obrazce. Ještě budeme používat označení

$$\Lambda := \sum_{i=1}^{n} \lambda_i.$$

Připomeňme, že izoperimetrický podíl je dán pouze tvarem obrazce a nezávisí na jeho velikosti. Zvláště hodnota $\Lambda$ je konstantní (je určena tvarem zadaných obrazců).

Naším úkolem je minimalizovat součet $\sum_{i=1}^{n} S_i$ při dodržení podmínky $\sum_{i=1}^{n} o_i = l$. Protože je však

$$S_i = \frac{o_i^2}{4\pi\lambda_i}, \qquad i \in \{1, \ldots, n\},$$

jde nám o minimalizaci výrazu

$$S := \frac{1}{4\pi} \sum_{i=1}^{n} \frac{o_i^2}{\lambda_i}.$$

Použijeme-li Jensenovu nerovnost pro ostře konvexní funkci $y = x^2$ (na celé reálné ose), obdržíme

$$\left(\sum_{i=1}^{n} c_i\, x_i\right)^2 \le \sum_{i=1}^{n} c_i\, x_i^2$$

pro $x_i \in \mathbb{R}$ a $c_i > 0$ s vlastností $c_1 + \cdots + c_n = 1$. Dále víme, že v této nerovnosti nastane rovnost právě tehdy, když je $x_1 = \cdots = x_n$. Volbou

$$c_i = \frac{\lambda_i}{\Lambda}, \quad x_i = \frac{o_i}{\lambda_i}, \qquad i \in \{1, \ldots, n\}$$

pak dostaneme

$$\left(\sum_{i=1}^{n} \frac{\lambda_i}{\Lambda}\,\frac{o_i}{\lambda_i}\right)^2 \le \sum_{i=1}^{n} \frac{\lambda_i}{\Lambda}\left(\frac{o_i}{\lambda_i}\right)^2.$$

Jednoduchými úpravami přejdeme k nerovnici

$$\frac{1}{\Lambda^2}\left(\sum_{i=1}^{n} o_i\right)^2 \le \frac{1}{\Lambda}\sum_{i=1}^{n} \frac{o_i^2}{\lambda_i}$$

$f$ je *analytická funkce* v bodě $a$. Funkce je analytická na intervalu, je-li analytická v každém jeho bodě.

Ne všechny hladké funkce jsou ale analytické. Ve skutečnosti lze dokázat, že pro každou posloupnost čísel $a_n$ umíme najít hladkou funkci, jejíž derivace řádů $k$ budou tato čísla $a_k$.[1]



Abychom si alespoň představili podstatu problému, ukážeme si (jak se později uvidí velice užitečnou) funkci, která má v nule všechny derivace nulové, je však všude kromě tohoto bodu nenulová.

Uvažme funkci definovanou vztahem

$$f(x) = \mathrm{e}^{-1/x^2}.$$

Evidentně jde o dobře definovanou hladkou funkcí ve všech bodech $x \neq 0$. Ověříme, že bodě $x = 0$ existuje limita $\lim_{x\to 0} f(x) = 0$. Můžeme proto dodefinovat $f(0) = 0$ a získáváme spojitou funkci.

Přímým výpočtem s použitím L'Hospitalova pravidla vyjádříme derivaci a stačí přitom počítat derivaci zprava, protože jde o sudou funkci.

$$f'(0) = \lim_{x\to 0^+} \frac{\mathrm{e}^{-1/x^2} - 0}{x} = \lim_{x\to 0^+} \frac{x^{-1}}{\mathrm{e}^{1/x^2}} = \frac{1}{2}\lim_{x\to 0^+} \frac{x}{\mathrm{e}^{1/x^2}} = 0.$$

Derivací funkce $f(x)$ v obecném bodě $x \neq 0$ dostaneme $f'(x) = \mathrm{e}^{-1/x^2}\cdot 2x^{-3}$ a opakovaným derivováním výsledků dostaneme vždy součet konečně mnoha členů tvaru

$$C \cdot \mathrm{e}^{-1/x^2} \cdot x^{-j},$$

kde $C$ je nějaké celé číslo a $j$ je přirozené číslo.

Budeme tedy předpokládat, že jsme už dokázali, že derivace řádu $k$ naší funkce $f(x)$ existuje a je v nule nulová. Při výpočtu následující derivace budeme opět počítat stejně jako v případě $k = 0$ výše. Budeme počítat limitu výrazu $f^{(k)}(x)/x$ pro $x \to 0^+$, tj. konečný součet limit výrazů $x^{-j}\,\mathrm{e}^{-1/x^2} = x^{-j}/\mathrm{e}^{1/x^2}$. To jsou samé výrazy typu $\infty/\infty$, na které můžeme opakovaně použít L'Hospitalovo pravidlo. Zjevně po několika derivacích čitatele i jmenovatele (a obdobné úpravě jako v případu výše) bude ve jmenovateli stále stejný výraz, zatímco v čitateli již bude mocnina nezáporná. Celý výraz tedy nutně má v nule limitu nulovou, stejně jako jsme spočítali v případě první derivace výše. Totéž tedy bude platit pro konečný součet takových výrazů a zjistili jsme, že bude v nule existovat i každá derivace $f^{(k)}(x)$ a její hodnota bude nula.

Ukázali jsme, že naše funkce $f(x)$ je hladká na celém $\mathbb{R}$, je samozřejmě nenulovou funkcí všude mimo $x = 0$, všechny její derivace v tomto bodě jsou ale nulové. Samozřejmě to tedy není analytická funkce v bodě $x_0 = 0$.

Uvidíme v dalším (hlavně v kapitole deváté), že ještě důležitější je chování této funkce v nekonečnu, tj. bude nás zajímat funkce $x \mapsto \mathrm{e}^{-x^2}$ v okolí bodu $x_0 = 0$. Této funkci se říká *gaussián*.

[1] Jde o speciální případ tzv. Whitneyho věty, která říká, že k tomu, aby existovala hladká reálná funkce s předepsanými parciálními derivacemi všech řádů na uzavřené množině $M \subset \mathbb{R}^n$, je nutné a stačí, aby tento předpis derivací splňoval na libovolné komppaktní podmnožině $K \subset M$ odhady Taylorova rozvoje se zbytkem (pro funkce více proměnných budeme Taylorův rozvoj diskutovat v osmé kapitole). Zadáním v jediném bodě (nebo v diskrétní množině bodů) je tedy podmínka ve Whitneyho větě prázdná.

a poté (uvažte, že $\sum_{i=1}^{n} o_i = l$)

$$\frac{l^2}{\Lambda} \le \sum_{i=1}^{n} \frac{o_i^2}{\lambda_i},$$

přičemž opět rovnost nastává právě pro

$$x_1 = \cdots = x_n, \qquad \text{tj.} \qquad \frac{o_1}{\lambda_1} = \cdots = \frac{o_n}{\lambda_n}. \tag{6.3}$$

Odsud vyplývá, že $S$ je nejmenší, právě když platí (‖6.3‖). Tato nejmenší hodnota $S$ je $l^2/(4\pi\Lambda)$. Zbývá stanovit délky nastříhaných částí $o_i$. Pokud je (‖6.3‖) splněno, musí zjevně být $o_i = k\,\lambda_i$ pro každé $i \in \{1, \ldots, n\}$ a jistou konstantu $k > 0$. Z

$$\sum_{i=1}^{n} o_i = l \quad \text{a současně} \quad \sum_{i=1}^{n} o_i = k \sum_{i=1}^{n} \lambda_i = k\,\Lambda$$

ihned plyne, že $k = l/\Lambda$, tj.

$$o_i = \tfrac{\lambda_i}{\Lambda}\, l, \qquad i \in \{1, \ldots, n\}.$$

Podívejme se na konkrétní situaci, kdy máme provázek o délce 1 m rozříznout na dva menší a z nich potom vytvořit čtverec a kruh tak, aby součet jejich obsahů byl co nejmenší. Pro čtverec a kruh je po řadě (viz příklad nazvaný Izoperimetrický podíl)

$$\lambda_1 = \tfrac{4}{\pi}, \quad \lambda_2 = 1, \qquad \text{tj.} \qquad \Lambda = \lambda_1 + \lambda_2 = \tfrac{4+\pi}{\pi}.$$

Délky příslušných částí tak jsou (v metrech)

$$o_1 = \frac{\frac{4}{\pi}}{\frac{4+\pi}{\pi}} \cdot 1 = \frac{4}{4+\pi} \doteq 0,56, \quad o_2 = \frac{1}{\frac{4+\pi}{\pi}} \cdot 1 = \frac{\pi}{4+\pi} \doteq 0,44.$$

Obsah čtverce o obvodu 0,56 m (s délkou strany $a = 0,14$ m) je $0,0196\ \mathrm{m}^2$ a obsah kruhu s obvodem 0,44 m (a poloměrem $r \doteq 0,07$ m) pak činí přibližně $0,0154\ \mathrm{m}^2$. Můžeme ověřit, že (v $\mathrm{m}^2$)

$$\frac{l^2}{4\pi\Lambda} = \frac{1}{4(4+\pi)} \doteq 0,035 = 0,0196 + 0,0154\,. \qquad \square$$

**Taylorovy rozvoje.** Derivace vyšších řádů nutně potřebujeme k tomu, abychom určili Taylorův rozvoj dané funkce.

**6.12.** Určete Taylorovy rozvoje $T_x^k$ ($k$-tého řádu v bodě $x$) z následujících funkcí:

i) $T_0^3$ z funkce $\sin x$,
ii) $T_1^3$ z funkce $\frac{e^x}{x}$.

**Řešení.** (i) Spočítáme hodnoty první až třetí derivace funkce $f = \sin$ v bodě 0: $f'(0) = \cos(0) = 1$, $f^{(2)}(0) = -\sin(0) = 0$, $f^{(3)}(0) = -\cos(0) = -1$, dále $f(0) = 0$. Taylorův rozvoj 3-tího řádu funkce $\sin(x)$ v bodě 0 je tedy

$$T_0^3(\sin(x)) = x - \frac{1}{6}x^3.$$



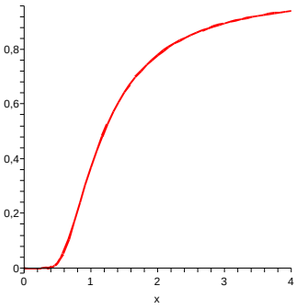
**6.7. Příklady neanalytických hladkých funkcí.** Snadno můžeme naši funkci $f(x)$ z předchozího odstavce modifikovat takto:

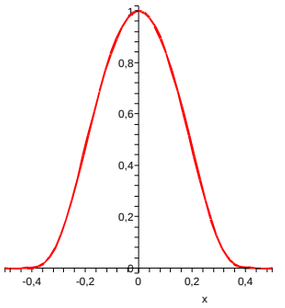
$$g(x) = \begin{cases} 0 & \text{je-li } x \le 0 \\ \mathrm{e}^{-1/x^2} & \text{je-li } x > 0 \end{cases}.$$

Opět jde o hladkou funkci na celém $\mathbb{R}$. Další úpravou můžeme získat funkci nenulovou ve všech vnitřních bodech intervalu $[-a, a]$, $a > 0$ a nulovou jinde:

$$h(x) = \begin{cases} 0 & \text{je-li } |x| \ge a \\ \mathrm{e}^{\frac{1}{x^2-a^2}+\frac{1}{a^2}} & \text{je-li } |x| < a\,. \end{cases}$$

Tato funkce je opět hladká na celém $\mathbb{R}$. Poslední dvě funkce jsou na obrázcích, vpravo je použit parametr $a = 1$.

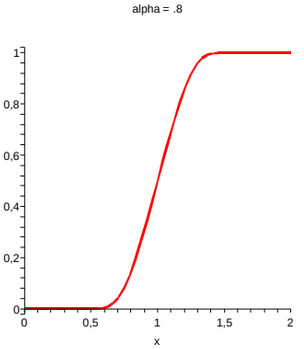


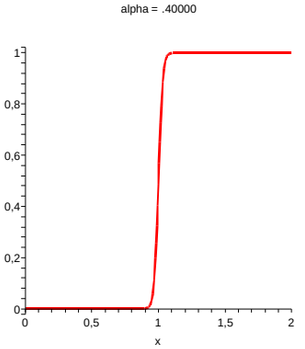




Nakonec ještě ukážeme, jak lze dostat hladké analogie Heavisideových funkcí. Pro dvě pevně zvolená reálná čísla $a < b$ definujeme funkci $f(x)$ s použitím výše definované funkce $g$ takto:

$$f(x) = \frac{g(x-a)}{g(x-a) + g(b-x)}.$$

Zjevně je pro každé $x \in \mathbb{R}$ jmenovatel zlomku kladný (pro každý z intervalů určených čísly $a$ a $b$ je totiž alespoň jeden ze sčítanců jmenovatele nenulový a tedy je celý jmenovatel kladný). Dostáváme z našeho definičního vztahu proto hladkou funkci $f(x)$ na celém $\mathbb{R}$. Při $x \le a$ je přitom jmenovatel zlomku přímo dle definice funkce $g$ nulový, při $x \ge b$ je čitatel i jmenovatel stejný. Na dalších dvou obrázcích jsou právě funkce $f(x)$ a to s parametry $a = 1 - \alpha$, $b = 1 + \alpha$, kde nalevo je $\alpha = 0.8$ a napravo $\alpha = 0.4$.




Snadno nyní také vytvoříme hladkou obdobu charakteristické funkce intervalu $[c, d]$.

Označme si jako $f_\varepsilon(x)$ výše uvedenou funkci $f(x)$ s parametry $a = -\varepsilon$, $b = +\varepsilon$. Nyní pro interval $(c, d)$, s délkou $d - c > 2\varepsilon$ definujeme funkci $h_\varepsilon(x) = f_\varepsilon(x - c) \cdot f_\varepsilon(d - x)$. Tato funkce je identicky nulová na intervalech $(-\infty, c - \varepsilon)$ a $(d + \varepsilon, \infty)$ a je

(ii) Opět $f(1) = e$,

$$\begin{aligned} f'(1) &= \frac{e^x}{x} - \frac{e^x}{x^2}\Big|_{x=1} = 0, \\ f^{(2)}(1) &= \frac{e^x}{x} - 2\frac{e^x}{x} + \frac{2e^x}{x^3}\Big|_{x=1} = e, \\ f^{(3)}(1) &= \frac{e^x}{x} - 3\frac{e^x}{x} + \frac{6e^x}{x^3} - \frac{6e^x}{x^4}\Big|_{x=1} = -2e. \end{aligned}$$

Dostáváme tedy Taylorův rozvoj třetího řádu funkce $\frac{e^x}{x}$ v bodě 1:

$$T_1^3(\frac{e^x}{x}) = e + \frac{e}{2}(x-1)^2 - \frac{e}{3}(x-1)^3 = e(-\frac{x^3}{3} + \frac{3x^2}{2} - 2x + \frac{5}{6}).$$

□

**6.13.** Určete Taylorův polynom $T_0^6$ funkce sin a pomocí věty (6.4) odhadněte chybu polynomu v bodě $\pi/4$.

**Řešení.** Podobně jako v předchozím příkladu určíme

$$T_0^6(\sin(x)) = x - \frac{1}{6}x^3 + \frac{1}{120}x^5.$$

Dle věty 6.4 pak odhadneme velikost zbytku (chyby) $R$. Podle věty existuje $c \in (0, \frac{\pi}{4})$ takové, že

$$R(\pi/4) = \left|\frac{-\cos(c)\pi^7}{7!4^7}\right| < \frac{1}{7!} \doteq 0,0002\,. \qquad \square$$

**6.14.** Rozviňte funkci $\ln(1+x)$ do mocninné řady v bodech 0 a 1 a určete **všechna** $x \in \mathbb{R}$, pro která tyto řady konvergují.

**Řešení.** Nejprve určeme rozvoj v bodě 0. Rozvinout funkci do mocninné řady v daném bodě je to stejné, jako určit její Taylorův rozvoj v daném bodě. Snadno nahlédneme, že

$$[\ln(x+1)]^{(n)} = (-1)^{n+1}\frac{(n-1)!}{(x+1)^n},$$

takže vyčíslením derivací v nule máme $\ln(x+1) = \ln 1 + \sum_{n=1}^{\infty} a_n x^n$, kde

$$a_n = \frac{(-1)^{n+1}(n-1)!}{n!} = \frac{(-1)^{n+1}}{n}.$$

Můžeme tedy psát

$$\begin{aligned} \ln(x+1) &= x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \frac{1}{4}x^4 + \cdots = \\ &= \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}x^n. \end{aligned}$$

identicky rovna jedné na intervalu $(c+\varepsilon, d-\varepsilon)$, přičemž je všude hladká a lokálně je buď konstantní nebo monotonní. Čím menší je $\varepsilon > 0$, tím rychleji naše funkce přeskočí z nuly na jedničku kolem začátku intervalu nebo zpět na konci intervalu.

Vidíme tedy, že hladké funkce jsou velice „plastické" — z lokálního chování kolem jednoho bodu nemůžeme říci vůbec nic o globálním chování takové funkce. Naopak, analytické funkce jsou zcela určené dokonce jen derivacemi v jediném bodě. Zejména jsou tedy bezezbytku určené svým chováním na libovolně malém okolí jediného bodu ze svého definičního oboru. Jsou tedy v tomto smyslu velice „rigidní".

**6.8. Lokální chování funkcí.** Viděli jsme, že znaménko první derivace určuje u každé diferencovatelné funkce, zda roste nebo klesá na nějakém okolí daného bodu. Pokud je ale derivace nulová, sama o sobě mnoho o chování funkce neříká.



Už jsme se ale setkali s významem druhé derivace při popisu kritických bodů. Teď zobecníme diskusi kritických bodů pro všechny řády. Začneme diskusí lokálních extrémů funkcí, tj. hodnot, které jsou ostře větší nebo ostře menší než všechny ostatní hodnoty z nějakého okolí daného bodu.

Budeme v dalším uvažovat funkce s dostatečným počtem spojitých derivací, aniž bychom tento předpoklad přímo uváděli.

Řekneme, že bod $a$ v definičním oboru funkce $f$ je *kritický bod řádu k*, jestliže platí

$$f'(a) = \cdots = f^{(k)}(a) = 0, \quad f^{(k+1)}(a) \neq 0.$$

Předpokládejme, že $f^{(k+1)}(a) > 0$. Pak je tato spojitá derivace kladná i na jistém okolí $\mathcal{O}(a)$ bodu $a$. Taylorův rozvoj se zbytkem nám v takovém případě dává pro všechna $x$ z $\mathcal{O}(a)$

$$f(x) = f(a) + \frac{1}{(k+1)!}f^{(k+1)}(c)(x-a)^{k+1}.$$

Je proto změna hodnot $f(x)$ v okolí bodu $a$ dána chováním funkce $(x-a)^{k+1}$. Je-li přitom $k+1$ sudé číslo, jsou nutně hodnoty $f(x)$ v takovém okolí větší než hodnota $f(a)$ a zjevně je proto bod $a$ bodem lokálního minima. Pokud je ale $k$ sudé číslo, pak jsou hodnoty vlevo menší a vpravo větší než než $f(a)$, extrém tedy ani lokálně nenastává. Zato si můžeme všimnout, že graf funkce $f(x)$ protíná svoji tečnu $y = f(a)$ bodem $[a, f(a)]$.

Naopak, je-li $f^{(k+1)}(a) < 0$, pak ze stejného důvodu jde o lokální maximum při lichém $k$ a extrém opět nenastává pro $k$ sudé.

**6.9. Konvexní a konkávní funkce.** Říkáme, že diferencovatelná funkce $f$ je v bodě $a$ *konkávní*, jestliže se její graf nachází v jistém okolí celý pod tečnou v bodě $[a, f(a)]$, tj. požadujeme



$$f(x) \leq f(a) + f'(a)(x-a).$$

Říkáme, že funkce $f$ je *konvexní* v bodě $a$, jestliže naopak je její graf nad tečnou v bodě $a$, tj.

$$f(x) \geq f(a) + f'(a)(x-a).$$

Funkce je konvexní nebo konkávní na intervalu, jestliže má tuto vlastnost v každém jeho bodě.

Pro poloměr konvergence potom použijeme limitu podílu následujících koeficientů členů mocninné řady

$$r = \frac{1}{\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right|} = \frac{1}{\lim_{n\to\infty}\frac{\frac{1}{n+1}}{\frac{1}{n}}} = 1.$$

Řada tedy konverguje pro libovolné $x \in (-1, 1)$. Pro $x = -1$ dostáváme harmonickou řadu (se znaménkem minus), pro $x = 1$ dostáváme alternující harmonickou řadu, která podle Leibnizova kriteria konverguje. Daná řada proto konverguje právě pro $x \in (-1, 1]$.

Pro rozvoj v bodě 1 dostáváme podobně vyčíslením výše uvedených derivací z ‖6.14‖

$$\ln(x+1) = \ln(2) + \frac{1}{2}(x-1) - \frac{1}{8}(x-1)^2 + \\ + \frac{1}{3\cdot 2^3}(x-1)^3 - \cdots = \ln(2) + \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n\cdot 2^n}(x-1)^n,$$

pro poloměr konvergence této řady pak dostáváme

$$r = \frac{1}{\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right|} = \frac{1}{\lim_{n\to\infty}\frac{\frac{1}{2^{n+1}(n+1)}}{\frac{1}{2^n n}}} = 2.$$

První řada konverguje pro $-1 < x \le 1$, druhá pro $-1 < x \le 3$. □

*6.15.* Nalezněte odhad chyby přibližného vyjádření

$$\ln(1+x) \approx x - \tfrac{x^2}{2}$$

pro $x \in (-1, 0)$. ○

*6.16.* Najděte Taylorův polynom 3. stupně funkce

$$y = \operatorname{arctg} x, \quad x \in \mathbb{R}$$

v bodě $x_0 = 1$. ○

*6.17.* Určete Taylorův rozvoj 3. řádu v bodě $x_0 = 0$ funkce

(a) $y = \frac{1}{\cos x}$;
(b) $y = \mathrm{e}^{-\frac{x^2}{2}}$;
(c) $y = \sin(\sin x)$ ;
(d) $y = \operatorname{tg} x$;
(e) $y = \mathrm{e}^x \sin x$

definované v jistém okolí bodu $x_0$. ○

*6.18.* Stanovte Taylorův rozvoj 4. řádu funkce $y = \ln x^2$, $x \in (0, 2)$ v bodě $x_0 = 1$. ○

*6.19.* Napište Taylorův polynom 4. stupně funkce $y = \sin x$, $x \in \mathbb{R}$ se středem v počátku. Pomocí tohoto polynomu přibližně vyčíslete $\sin 1°$ a stanovte limitu

$$\lim_{x\to 0+}\frac{x\sin x - x^2}{x^4}.$$ ○

Předpokládejme navíc, že má funkce $f$ spojité druhé derivace v okolí bodu $a$. Z Taylorova rozvoje druhého řádu se zbytkem dostáváme

$$f(x) = f(a) + f'(a)(x-a) + \frac{1}{2}f''(c)(x-a)^2.$$

Proto je zjevně funkce konvexní, kdykoliv je $f''(a) > 0$, a je konkávní, kdykoliv $f''(a) < 0$.

Pokud je druhá derivace nulová, můžeme použít derivace vyšších řádů. Stejný závěr ovšem umíme učinit pouze, pokud první další nenulová derivace po první derivaci bude sudého řádu. Pokud bude naopak první nenulová řádu lichého, budou zjevně body grafu funkce na různých stranách nějakého malého okolí zkoumaného bodu na opačných stranách tečny v tomto bodě.

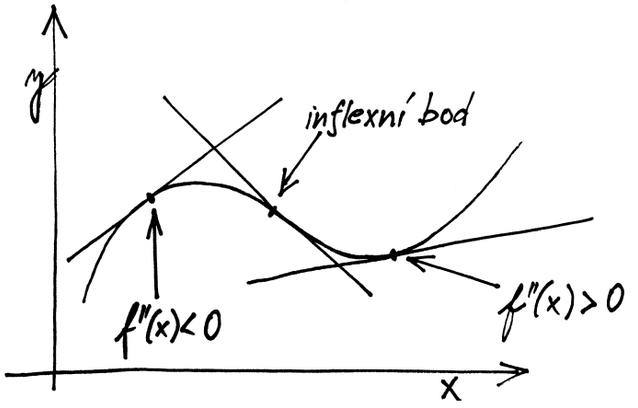
**6.10. Inflexní body.** Bod $a$ nazýváme *inflexní bod* diferencovatelné funkce $f$, jestliže graf funkce $f$ přechází z jedné strany tečny na druhou.

Předpokládejme, že $f$ má spojité třetí derivace a napišme si Taylorův rozvoj třetího řádu se zbytkem:

$$f(x) = f(a) + f'(a)(x-a) + \frac{1}{2}f''(a)(x-a)^2 + \frac{1}{6}f'''(c)(x-a)^3.$$

Je-li $a$ nulový bod druhé derivace takový, že $f'''(a) \neq 0$, pak je třetí derivace nenulová i na nějakém okolí a jde proto zjevně o inflexní bod. Znaménko třetí derivace nám v takovém případě určuje, zda graf funkce přechází tečnu zdola nahoru nebo naopak.

Pokud je bod $a$ navíc izolovaným nulovým bodem druhé derivace a zároveň inflexním bodem, pak zjevně je na nějakém malém okolí bodu $a$ funkce na jedné straně konkávní a na druhé konvexní. Inflexní body tedy můžeme také vnímat jako body přechodu mezi konkávním a konvexním chováním grafu funkce.




**6.11. Asymptoty grafu funkce.** Uvedeme ještě jednu dobrou pomůckou pro náčrtek grafu funkce. Zkusíme zjistit tzv. *asymptoty*, tj. přímky, ke kterým se blíží hodnoty funkce $f$. Asymptotou v nevlastním bodě $\infty$ je taková přímka $y = ax + b$, pro kterou je



$$\lim_{x\to\infty}(f(x) - ax - b) = 0.$$

Říkáme jí také *asymptota se směrnicí*. Pokud taková asymptota existuje, platí

$$\lim_{x\to\infty}(f(x) - ax) = b$$

*6.20.* Uveďte Taylorův polynom se středem v počátku stupně alespoň 8 funkce $y = \mathrm{e}^{2x}$, $x \in \mathbb{R}$. ◯

*6.21.* Polynom $x^3 - 2x + 5$ vyjádřete jako polynom v proměnné $u = x - 1$. ◯

**6.22.** Rozviňte funkci

(a) $y = \ln \frac{1+x}{1-x}$, $\quad x \in (-1, 1)$;

(b) $y = \mathrm{e}^{x^2} + x^2 \mathrm{e}^{-2x}$, $\quad x \in \mathbb{R}$

do Taylorovy řady se středem v počátku.

**Řešení.** Pokud lze funkci vyjádřit jako součet mocninné řady (s kladným poloměrem konvergence) na jejím oboru konvergence, pak je tato řada nutně Taylorovou řadou uvažované funkce (svého součtu). To nám umožní snadno najít příslušné Taylorovy řady.

Případ (a). Víme, že je

$$\ln(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n, \quad x \in (-1, 1),$$

tj.

$$\ln(1-x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} (-x)^n = -\sum_{n=1}^{\infty} \frac{1}{n} x^n, \quad x \in (-1, 1).$$

Celkem máme

$$\ln \tfrac{1+x}{1-x} = \ln(1+x) - \ln(1-x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}+1}{n} x^n = \sum_{n=1}^{\infty} \frac{2}{2n-1} x^{2n-1}$$

pro $x \in (-1, 1)$.

Případ (b). Podobně ze známé identity

$$\mathrm{e}^x = \sum_{n=0}^{\infty} \frac{1}{n!} x^n, \quad x \in \mathbb{R},$$

plyne

$$\mathrm{e}^{x^2} = \sum_{n=0}^{\infty} \frac{1}{n!} \left(x^2\right)^n = \sum_{n=0}^{\infty} \frac{1}{n!} x^{2n}, \quad x \in \mathbb{R},$$

a

$$x^2 \mathrm{e}^{-2x} = x^2 \sum_{n=0}^{\infty} \frac{1}{n!} (-2x)^n = \sum_{n=0}^{\infty} \frac{(-2)^n}{n!} x^{n+2}, \quad x \in \mathbb{R}.$$

Platí tudíž

$$\mathrm{e}^{x^2} + x^2 \mathrm{e}^{-2x} = \sum_{n=0}^{\infty} \frac{x^{2n} + (-2)^n x^{n+2}}{n!}, \quad x \in \mathbb{R}.$$

□ R

**6.23.** Určete Taylorovu řadu se středem v počátku funkce

(a) $y = \frac{1}{(1+x)^2}$, $\quad x \in (-1, 1)$;

(b) $y = \operatorname{arctg} x$, $\quad x \in (-1, 1)$.

**Řešení.** Případ (a). Využijeme vzorec

$$\frac{1}{1+x} = \sum_{n=0}^{\infty} (-x)^n = \sum_{n=0}^{\infty} (-1)^n x^n, \quad x \in (-1, 1)$$

o součtu geometrické řady. Jeho derivováním dostáváme

$$-\frac{1}{(1+x)^2} = \left( \sum_{n=0}^{\infty} (-1)^n x^n \right)' = \sum_{n=1}^{\infty} (-1)^n n\, x^{n-1}, \quad x \in (-1, 1),$$

a tedy existuje i limita

$$\lim_{x \to \infty} \frac{f(x)}{x} = a.$$

Pokud ovšem existují poslední dvě limity, existuje i limita z definice asymptoty, jde proto i o podmínky dostatečné. Obdobně se definuje a počítá asymptota i v nevlastním bodě $-\infty$.

Tímto způsobem dohledáme všechny potenciální přímky splňující vlastnosti asymptot se směrnicí. Zbývají nám případné přímky kolmé na osu $x$: Asymptoty v bodech $a \in \mathbb{R}$ jsou přímky $x = a$ takové, že funkce $f$ má v bodě $a$ alespoň jednu jednostrannou limitu nekonečnou. Hovoříme také o *asymptotách bez směrnice*.

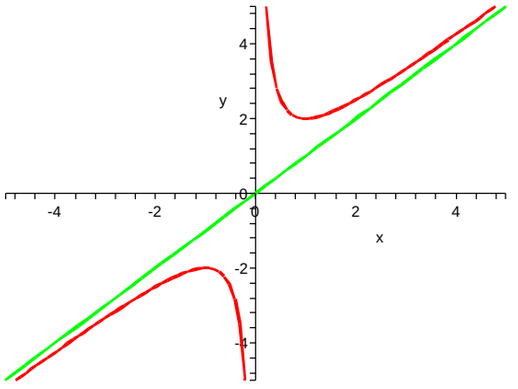
Např. racionální funkce lomené mají v nulových bodech jmenovatele, které nejsou nulovými body čitatele, asymptotu.

Spočtěme aspoň jeden jednoduchý příklad: Funkce $f(x) = x + \frac{1}{x}$ má za asymptoty přímky $y = x$ a $x = 0$. Skutečně, jednostranné limity zprava a zleva v nule jsou zjevně $\pm\infty$, zatímco limita $f(x)/x = 1 + 1/x^2$ je samozřejmě v nevlastních bodech právě $\pm 1$, zatímco limita $f(x) - x = 1/x$ je v nevlastních bodech nulová.

Derivací obdržíme

$$f'(x) = 1 - x^{-2}, \quad f''(x) = 2x^{-3}.$$

Funkce $f'(x)$ má dva nulové body $\pm 1$. V bodě $x = 1$ má funkce lokální minimum, v bodě $x = -1$ lokální maximum. Druhá derivace nemá nulové body v celém definičním oboru $(-\infty, 0) \cup (0, \infty)$, proto nemá naše funkce žádný inflexní bod.




**6.12. Diferenciál funkce.** Při praktickém používání diferenciálního počtu často pracujeme se závislostmi mezi různými veličinami, řekněme $y$ a $x$, a není dána pevně volba závislé a nezávislé proměnné. Explicitní vztah $y = f(x)$ s nějakou funkcí $f$ je tedy jen jednou z možností. Derivování pak vyjadřuje, že okamžitá změna $y = f(x)$ je úměrná okamžité změně $x$ a to s úměrou $f'(x) = \frac{df}{dx}(x)$. Tento vztah se často píše jako

$$df(x) = \frac{df}{dx}(x)dx,$$

kde $df(x)$ interpretujeme jako lineární zobrazení přírůstků dané $df(x)(\Delta x) = f'(x) \cdot \Delta x$, zatímco $dx(x)(\Delta x) = \Delta x$.

přičemž $\left(x^0\right)' = 0$, a tak je dolní index $n = 1$. Vidíme, že

$$\tfrac{1}{(1+x)^2} = \sum_{n=1}^{\infty} (-1)^{n+1}\, n\, x^{n-1}, \quad x \in (-1, 1)\,.$$

Případ (b). Derivaci funkce $y = \operatorname{arctg} t$ umíme vyjádřit jako

$$(\operatorname{arctg} t)' = \tfrac{1}{1+t^2} = \sum_{n=0}^{\infty} \left(-t^2\right)^n = \sum_{n=0}^{\infty} (-1)^n t^{2n}, \quad t \in (-1, 1)\,.$$

Protože pro $x \in (-1, 1)$ je

$$\int_0^x (\operatorname{arctg} t)'\, dt = \operatorname{arctg} x - \operatorname{arctg} 0 = \operatorname{arctg} x$$

a

$$\int_0^x \left(\sum_{n=0}^{\infty} (-1)^n t^{2n}\right) dt = \sum_{n=0}^{\infty} \left((-1)^n \int_0^x t^{2n}\, dt\right) = \sum_{n=0}^{\infty} \tfrac{(-1)^n}{2n+1}\, x^{2n+1},$$

máme již výsledek

$$\operatorname{arctg} x = \sum_{n=0}^{\infty} \tfrac{(-1)^n}{2n+1}\, x^{2n+1}, \quad x \in (-1, 1)\,. \qquad \square$$

**6.24.** Najděte Taylorovu řadu se středem $x_0 = 0$ funkce

$$f(x) = \int_0^x u\, \cos u^2\, du, \quad x \in \mathbb{R}.$$

**Řešení.** Z vyjádření

$$\cos t = \sum_{n=0}^{\infty} \tfrac{(-1)^n}{(2n)!}\, t^{2n}, \quad t \in \mathbb{R}$$

plyne

$$u\, \cos u^2 = u \sum_{n=0}^{\infty} \tfrac{(-1)^n}{(2n)!} \left(u^2\right)^{2n} = \sum_{n=0}^{\infty} \tfrac{(-1)^n}{(2n)!}\, u^{4n+1}, \quad u \in \mathbb{R}$$

a následně (pro $x \in \mathbb{R}$)

$$f(x) = \int_0^x u\, \cos u^2\, du = \int_0^x \left(\sum_{n=0}^{\infty} \tfrac{(-1)^n}{(2n)!}\, u^{4n+1}\right) du =$$
$$= \sum_{n=0}^{\infty} \left(\tfrac{(-1)^n}{(2n)!} \int_0^x u^{4n+1}\, du\right) = \sum_{n=0}^{\infty} \tfrac{(-1)^n}{(2n)!\,(4n+2)}\, x^{4n+2}\,. \qquad \square$$

**6.25.** Na intervalu konvergence $(-1, 1)$ stanovte součet řady

$$\sum_{n=1}^{\infty} n\,(n+1)\, x^n\,.$$

**Řešení.** Platí

$$\sum_{n=1}^{\infty} n\,(n+1)\, x^n = \sum_{n=1}^{\infty} n \left(x^{n+1}\right)' =$$
$$= \left(\sum_{n=1}^{\infty} n\, x^{n+1}\right)' = \left(\sum_{n=1}^{\infty} n\, x^{n-1}\, x^2\right)' = \left[x^2 \sum_{n=1}^{\infty} (x^n)'\right]' =$$
$$= \left[x^2 \left(\sum_{n=1}^{\infty} x^n\right)'\right]' = \left[x^2 \left(-1 + \sum_{n=0}^{\infty} x^n\right)'\right]' =$$
$$= \left[x^2 \left(-1 + \tfrac{1}{1-x}\right)'\right]' = \left[x^2 \cdot \frac{1}{(1-x)^2}\right]' = \frac{2x}{(1-x)^3}$$

pro všechna $x \in (-1, 1)$. $\square$

**6.26.** Rozviňte do mocninné řady funkci $\cos^2(x)$ (tj. určete Taylorův rozvoj funkce) v bodě 0 a určete pro která reálná čísla tato řada konverguje.

Hovoříme o *diferenciálu funkce* $f$ pokud platí aproximační vlastnost

$$\lim_{\Delta x \to 0} \frac{f(x + \Delta x) - f(x) - df(x)(\Delta x)}{\Delta x} = 0$$

Z Taylorovy věty tedy vyplývá, že funkce s ohraničenou derivací $f'$ má diferenciál $df$. To zejména v bodě $x$ nastane, když v něm první derivace $f'(x)$ existuje a je spojitá.

Pokud je veličina $x$ vyjádřena pomocí další veličiny $t$, tj. $x = g(t)$, a to opět funkcí se spojitou první derivací, pak pravidlo o derivaci složené funkce říká, že i složená funkce $f \circ g$ má opět diferenciál

$$df(t) = \frac{df}{dx}(x)\frac{dx}{dt}(t)dt.$$

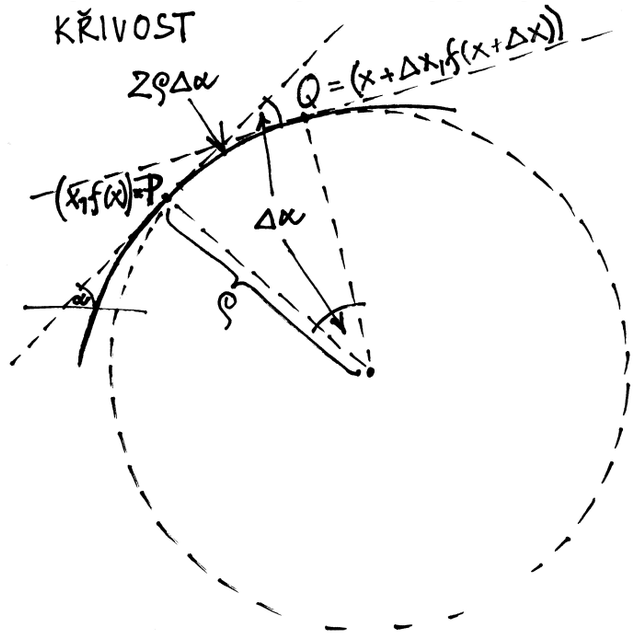
Můžeme proto vnímat $df$ jako lineární přiblížení dané veličiny v závislosti na přírůstcích závislé proměnné, ať už je tato závislost dána jakkoliv.

**6.13. Křivost grafu funkce.** Budeme ted graf hladké funkce



$f(x)$ chvíli diskutovat jako zvláštní případ parametrizované křivky v rovině. Můžeme si ji představit jako pohyb v rovině parametrizovaný pomocí nezávislé proměnné $x$. Pro libovolný bod $x$ z definičního oboru naší funkce můžeme okamžitě výpočtem první derivace vidět vektor $(1, f'(x)) \in \mathbb{R}^2$, který představuje okamžitou rychlost takového pohybu. Tečna bodem $[x, f(x)]$ parametrizovaná pomocí tohoto směrového vektoru pak představuje lineární přiblížení křivky.

Viděli jsme už také, že v případě, že $f''(x) = 0$ a zároveň $f'''(x) \neq 0$, přechází graf naší funkce přes svoji tečnu, tzn. že tečna je i nejlepším přiblížením křivky v bodě $x$ i do druhého řádu. To zpravidla popisujeme tvrzením, že má graf funkce $f$ v bodě $x$ *nulovou křivost*. Tak jak u první derivace nenulové hodnoty vyjadřovaly rychlost růstu (ať už s jakýmkoliv znaménkem), stejně asi intuitivně očekáváme, že druhá derivace bude popisovat míru zakřivení grafu. Zatím jsme jen viděli, že je graf funkce nad svojí tečnou pro kladnou hodnotu a pod tečnou v případě opačném.



**6.27.** Rozviňte do mocninné řady funkci $\sin^2(x)$ v bodě 0 a určete pro která reálná čísla tato řada konverguje.

*6.28.* Rozviňte do mocninné řady funkci $\ln(x^3+3x^2+3x+1)$ v bodě 0 a určete, pro která $x \in \mathbb{R}$ konverguje. ○

*6.29.* Rozviňte do mocninné řady funkci $\ln\sqrt{x}$ v bodě 1 a určete, pro která $x \in \mathbb{R}$ konverguje. ○

Další příklady na Taylorovy polynomy a řady naleznete na straně 388.

Nyní uvedeme několik „klasických“ příkladů, ve kterých budeme vyšetřovat průběh různých funkcí.

**6.30.** Stanovte obor hodnot funkce

$$f(x) = \tfrac{e^x-1}{e^x+1}, \quad x \in \mathbb{R}.$$

**Řešení.** Přímka $y = 1$ je zjevně asymptotou funkce $f$ v $+\infty$ a přímka $y = -1$ asymptotou v $-\infty$, neboť

$$\lim_{x\to\infty} \tfrac{e^x-1}{e^x+1} = \lim_{x\to\infty} \tfrac{e^x}{e^x} = 1, \qquad \lim_{x\to-\infty} \tfrac{e^x-1}{e^x+1} = \tfrac{0-1}{0+1} = -1.$$

Z nerovnosti

$$f'(x) = \tfrac{2e^x}{(e^x+1)^2} > 0, \quad x \in \mathbb{R}$$

dále plyne, že $f$ je spojitá a rostoucí na $\mathbb{R}$. Oborem hodnot je tedy interval $(-1, 1)$. □

*6.31.* Uveďte všechny intervaly, kde je funkce $y = e^{-x^2}$, $x \in \mathbb{R}$ konkávní. ○

*6.32.* Uvažujte funkci

$$y = \operatorname{arctg} \tfrac{x-1}{x}, \quad x \neq 0\,(x \in \mathbb{R}).$$

Určete intervaly, kde je tato funkce konvexní a kde konkávní; a také všechny její asymptoty. ○

*6.33.* Najděte všechny asymptoty funkce

(a) $y = x\,e^x$;
(b) $y = \frac{(x+3)^3}{(x-2)^3}$

s maximálním definičním oborem. ○

*6.34.* Stanovte asymptoty funkce

$$y = 2\operatorname{arctg}\left|\tfrac{x}{x^2-1}\right|, \quad x \neq \pm 1\,(x \in \mathbb{R})\,. \qquad ○$$

*6.35.* Uvažujte funkci

$$y = \ln \tfrac{3e^{2x}+e^x+10}{e^x+1}$$

definovanou pro všechna reálná $x$. Nalezněte její asymptoty. ○

Tečnu grafu v pevném bodě $P = [x, f(x)]$ jsme dostali pomocí limity sečen, tj. přímek procházejícími body $P$ a $Q = [x + \Delta x, f(x + \Delta x)]$. Chceme-li přiblížit druhou derivaci, budeme body $P$ a $Q \neq P$ prokládat kružnicí $C_Q$, jejíž střed je na průsečíku kolmic na tečny, vztyčených v bodech $P$ a $Q$.

Z obrázku je patrné, že jestliže tečna v pevném bodě $P$ svírá s osou $x$ úhel $\alpha$ a tečna v $Q$ úhel $\alpha + \Delta\alpha$, pak i úhel zmíněných kolmic v jejich průsečíku bude $\Delta\alpha$. Označíme-li poloměr naší kružnice $\rho$, pak délka oblouku kružnice mezi body $P$ a $Q$ bude $\rho\Delta\alpha$. Jestliže budeme limitně přibližovat bod $Q$ k pevnému bodu $P$, bude se zároveň délka oblouku kružnice blížit délce $s$ studované křivky, tj. grafu funkce $f(x)$, a kružnice limitně přejde do kružnice $C_P$. Dostáváme tedy pro limitní poloměr $\rho$ kružnice $C_P$ základní vztah

$$\rho = \lim_{\Delta\alpha\to 0} \frac{\Delta s}{\Delta\alpha} = \frac{ds}{d\alpha}.$$

*Křivost* grafu funkce $f$ v bodě $P$ definujeme jako číslo $1/\rho$. Nulová křivost tedy odpovídá nekonečnému poloměru $\rho$.

Pro výpočet poloměru $\rho$ potřebujeme umět vyjádřit délku oblouku $s$ pomocí změny úhlu $\alpha$ a derivaci této funkce pak vyjádřit pomocí derivací funkce $f$.

Všimněme si již teď, že při rostoucím úhlu $\alpha$ může délka oblouku buď také růst nebo klesat, podle toho, jestli má kružnice $C_Q$ střed nad nebo pod grafem funkce $f$. Znaménko $\rho$ nám tedy odráží, zda je funkce konkávní nebo konvexní. Je třeba také pomyslet na zvláštní případ, kdy střed limitně „uteče“ do nekonečna, tj. místo kružnice limitně dostaneme přímku a to opět tečnu.

Evidentně nemáme přímý nástroj na vyčíslení derivace $\frac{ds}{d\alpha}$. Víme však, že $\operatorname{tg}\alpha = df/dx$ a derivováním této rovnosti podle $x$ dostaneme (s využitím pravidla pro derivaci složených funkcí)

$$\frac{1}{(\cos\alpha)^2}\frac{d\alpha}{dx} = f''.$$

Na levé straně můžeme dosadit $\frac{1}{(\cos\alpha)^2} = 1 + (\operatorname{tg}\alpha)^2 = 1 + (f')^2$ a proto platí také (viz pravidlo pro derivování inverzní funkce)

$$\frac{dx}{d\alpha} = \frac{1+(\operatorname{tg}\alpha)^2}{f''} = \frac{1+(f')^2}{f''}.$$

To už jsme ale skoro hotoví, protože přírůstek délky oblouku $s$ v závislosti na proměnné $x$ je dán vztahem

$$\frac{ds}{dx} = (1+(f')^2)^{1/2}$$

a tedy můžeme již snadno spočíst podle pravidla pro derivování složené funkce

$$\rho = \frac{ds}{d\alpha} = \frac{ds}{dx}\frac{dx}{d\alpha} = \frac{(1+(f')^2)^{3/2}}{f''}.$$

Nyní již můžeme vyčíst vztah křivosti a druhé derivace: čitatel našeho zlomku je, nezávisle na hodnotě první derivace, vždy kladný. Je roven třetí mocnině velikosti tečného vektoru ke studované křivce. Znaménko křivosti tedy je dáno jen znaménkem druhé derivace, což jen znovu potvrzuje naši úvahu o konkávních a konvexních bodech funkcí. V případě, že je druhá derivace nulová, dostaneme i křivost nulovou.

Kružnici, pomocí které jsme křivost definovali nazýváme *oskulační kružnicí*.

Zkuste si spočíst křivost jednoduchých funkcí sami a využijte oskulační kružnice při náčrtech jejich grafů. Nejjednodušší je

**6.36.** Vyšetřete průběh funkce

$$f(x) = \sqrt[3]{|x|^3 + 1}.$$

**Řešení.** Definičním oborem i oborem spojitosti je celá reálná osa ($f$ tedy nemá body nespojitosti). Postačuje např. uvážit, že funkce $y = \sqrt[3]{x}$ je spojitá v každém bodě $x \in \mathbb{R}$ (na rozdíl od odmocnin o sudém základě definovaných pouze na nezáporné poloose). Ihned je také vidět, že $f(x) \geq 1$ a $f(-x) = f(x)$ pro všechna $x \in \mathbb{R}$, tj. funkce $f$ je kladná a sudá. Bod $[0, 1]$ jako jediný průsečík grafu $f$ s osami proto dostaneme dosazením $x = 0$. Limitní chování funkce má smysl uvažovat pouze v $\pm\infty$ (neexistují body nespojitosti), kde lehce určíme

$$\lim_{x\to\pm\infty} \sqrt[3]{|x|^3 + 1} = \lim_{x\to\pm\infty} \sqrt[3]{|x|^3} = \lim_{x\to\pm\infty} |x| = +\infty. \tag{6.4}$$

Nyní přistoupíme ke zkoumání průběhu funkce pomocí jejích derivací. Pro $x > 0$ je

$$f(x) = \sqrt[3]{x^3 + 1} = \left(x^3 + 1\right)^{\frac{1}{3}},$$

a tedy

$$f'(x) = \frac{1}{3}\left(x^3 + 1\right)^{-\frac{2}{3}} 3x^2 = \frac{x^2}{\sqrt[3]{\left(x^3 + 1\right)^2}} > 0, \qquad x > 0. \tag{6.5}$$

Odtud vyplývá, že funkce $f$ je rostoucí na intervalu $(0, +\infty)$. Vzhledem ke své spojitosti v počátku je však nutně $f$ rostoucí na $[0, +\infty)$. Neboť se jedná o sudou funkci, víme dále, že na intervalu $(-\infty, 0]$ klesá. Má tak jediné lokální minimum v bodě $x_0 = 0$, které je současně (ostrým) minimem globálním. Protože nekonstantní spojitá funkce zobrazuje interval na interval, je oborem hodnot $f$ právě $[1, +\infty)$ (uvažte $f(x_0) = 1$ a (‖6.4‖)). Všimněme si, že díky sudosti funkce jsme nemuseli počítat derivaci $f'$ na záporné poloose, kterou lze však snadno určit náhradou $|x|^3 = (-x)^3 = -x^3$ se ziskem

$$f'(x) = \tfrac{1}{3}\left(-x^3 + 1\right)^{-\frac{2}{3}}\left(-3x^2\right) = -\frac{x^2}{\sqrt[3]{\left(-x^3+1\right)^2}} < 0, \qquad x < 0.$$

Při výpočtu $f'(0)$ můžeme vyjít přímo z definice nebo pomocí limit

$$\lim_{x\to 0+} \frac{x^2}{\sqrt[3]{\left(x^3 + 1\right)^2}} = 0 = \lim_{x\to 0-} -\frac{x^2}{\sqrt[3]{\left(-x^3 + 1\right)^2}}$$

stanovit jednostranné derivace a následně $f'(0) = 0$. Ve skutečnosti jsme nemuseli počítat první derivaci ani na kladné poloose. K tomu, abychom obdrželi, že $f$ roste na $(0, +\infty)$, si stačilo uvědomit, že funkce $y = \sqrt[3]{x}$ a $y = x^3 + 1$ jsou rostoucí na $\mathbb{R}$ a že kompozice rostoucích funkcí je funkce rostoucí.

Snadno pro $x > 0$ však z (‖6.5‖) vypočítáme druhou derivaci

$$f''(x) = \frac{2x\sqrt[3]{\left(x^3 + 1\right)^2} - \frac{2}{3}x^2\sqrt[3]{\left(x^3 + 1\right)^{-1}}\left(3x^2\right)}{\sqrt[3]{\left(x^3 + 1\right)^4}},$$

výpočet v kritických bodech funkce $f$, protože v těch dostáváme poloměr oskulační kružnice jako reciprokou hodnotu druhé derivace opatřenou znaménkem.

**6.14. Vektorový diferenciální počet.** Jak jsme zmínili hned



v úvodu k páté kapitole, pro naše úvahy o derivování bylo vesměs podstatné, že jsme zkoumali funkce definované na reálných číslech a že jejich hodnoty lze mezi sebou sčítat a lze je násobit reálnými čísly. Potřebujeme proto, aby naše funkce $f : \mathbb{R} \to V$ měly hodnoty ve vektorovém prostoru $V$. Budeme jim pro odlišení říkat *vektorové funkce jedné reálné proměnné* nebo stručněji *vektorové funkce*.

Nyní se budeme podrobněji věnovat reálným funkcím s hodnotami v rovině nebo prostoru, tj. $f : \mathbb{R} \to \mathbb{R}^2$ a $f : \mathbb{R} \to \mathbb{R}^3$. Hovoříme o (parametrizovaných) křivkách v rovině a v prostoru. Obdobně bychom mohli pracovat s hodnotami v $\mathbb{R}^n$ pro jakoukoliv konečnou dimenzi $n$.

Pro zjednodušení budeme pracovat v pevných standardních bázích $e_i$ v $\mathbb{R}^2$ a $\mathbb{R}^3$, takže naše křivky budou dány dvojicemi, resp. trojicemi obyčejných reálných funkcí jedné reálné proměnné. Vektorová funkce $r$ v rovině, resp. v prostoru, je tedy dána

$$r(t) = x(t)e_1 + y(t)e_2, \quad r(t) = x(t)e_1 + y(t)e_2 + z(t)e_3.$$

Derivace takové vektorové funkce je opět vektor, který přibližuje zobrazení $r$ pomocí lineárního zobrazení přímky do roviny či prostoru. V rovině je to tedy

$$\frac{dr(t)}{dt}(t) = r'(t) = x'(t)e_1 + y'(t)e_2$$

a podobně v prostoru. V tomto kontextu je také třeba vnímat diferenciál vektorové funkce:

$$dr = \left(\frac{dx}{dt}e_1 + \frac{dy}{dt}e_2 + \frac{dz}{dt}e_3\right)dt$$

kde výraz na pravé straně chápeme tak, že se přírůstek skalární nezávislé proměnné $t$ lineárně zobrazí pomocí vynásobení vektoru derivace a tím dostaneme příslušný přírůstek vektorové veličiny $r$.

Jestliže vektor $r(t)$ představuje parametrizaci křivky, pak jeho derivace je vektorem rychlosti takto zadané dráhy. Speciální případ vektoru $r(t) = te_1 + f(t)e_2$ zadávajícího graf funkce $f$ jsme zkoumali v minulém odstavci. Druhá derivace pak představuje zrychlení takto zadaného pohybu. Všimněme si, že samozřejmě zrychlení nemusí být kolineární s rychlostí. V případě grafu funkce je dokonce zrychlení kolineární s rychlostí pouze v bodech, kde je $f''$ nulová, což odpovídá představě, že kolineární může zrychlení být pouze tehdy, když je křivost grafu nulová.

**6.15. Derivování složených zobrazení.** V lineární algebře a geo-



metrii jsou velice užitečná zobrazení, kterým říkáme formy. Jako argumenty mají jeden nebo více vektorů a v každém ze svých argumentů jsou lineární. Zadáváme tak velikost vektorů (skalární součin je symetrická bilineární forma) nebo objem rovnoběžnostěnů (to je $n$-lineární antisymetrická forma, kde $n$ je dimenze prostoru), viz např. odstavce 2.44 a 4.22.

Do těchto operací samozřejmě můžeme dosazovat vektory $r(t)$ závisející na parametru. Přímočarou aplikací Leibnizova pravidla pro derivaci součinu funkcí ověříme následující

tj. po úpravě máme

$$f''(x) = \frac{2x}{\sqrt[3]{(x^3+1)^5}} > 0, \qquad x > 0. \tag{6.6}$$

Podobně můžeme spočítat

$$f''(x) = -\frac{2x\sqrt[3]{(-x^3+1)^2} - \frac{2}{3}x^2\sqrt[3]{(-x^3+1)^{-1}}(-3x^2)}{\sqrt[3]{(-x^3+1)^4}} =$$

$$= -\frac{2x}{\sqrt[3]{(-x^3+1)^5}} > 0,$$

pro $x > 0$ a poté $f''(0) = 0$. Dále pak limitním přechodem:

$$\lim_{x\to 0+} \frac{2x}{\sqrt[3]{(x^3+1)^5}} = 0 = \lim_{x\to 0-} -\frac{2x}{\sqrt[3]{(-x^3+1)^5}}.$$

Podle nerovnosti (‖6.6‖) je $f$ ryze konvexní na intervalu $(0, +\infty)$. Také dostáváme ryzí konvexnost funkce $f$ na $(-\infty, 0)$. K tomuto závěru ovšem opět nebylo potřeba druhou derivaci pro $x < 0$ počítat: stačilo využít sudosti zadané funkce. Celkem jsme pak obdrželi, že $f$ je konvexní na celém svém definičním oboru (nemá inflexní body).

K vykreslení grafu funkce ještě potřebujeme nalézt asymptoty (vyčíslení funkce v jistých bodech přenecháváme čtenáři). Neboť je funkce $f$ spojitá na $\mathbb{R}$, asymptoty bez směrnice mít nemůže. Přímka $y = ax + b$ je pak asymptotou se směrnicí pro $x \to \infty$ tehdy a jenom tehdy, když existují (jako vlastní) obě limity

$$\lim_{x\to\infty} \tfrac{f(x)}{x} = a, \qquad \lim_{x\to\infty} (f(x) - ax) = b.$$

Analogické tvrzení platí pro $x \to -\infty$. Z limit

$$\lim_{x\to\infty} \frac{f(x)}{x} = \lim_{x\to\infty} \frac{\sqrt[3]{x^3+1}}{x} = \lim_{x\to\infty} \frac{\sqrt[3]{x^3}}{x} = 1,$$

$$\lim_{x\to\infty} (f(x) - 1\cdot x) = \lim_{x\to\infty} \left(\sqrt[3]{x^3+1} - x\right) =$$

$$= \lim_{x\to\infty} \left( \left[\sqrt[3]{x^3+1} - x\right] \frac{\sqrt[3]{(x^3+1)^2} + x\sqrt[3]{x^3+1} + x^2}{\sqrt[3]{(x^3+1)^2} + x\sqrt[3]{x^3+1} + x^2} \right) =$$

$$= \lim_{x\to\infty} \frac{x^3 + 1 - x^3}{\sqrt[3]{(x^3+1)^2} + x\sqrt[3]{x^3+1} + x^2} = \lim_{x\to\infty} \frac{1}{3x^2} = 0$$ tak již

plyne, že přímka $y = x$ je asymptotou v $+\infty$. Když znovu uvážíme, že funkce $f$ je sudá, bezprostředně obdržíme přímku $y = -x$ jako asymptotu v $-\infty$. □

Další příklady na vyšetřování funkcí můžete najít na straně 373.

Nyní přejděme od vyšetřování funkcí k dalším tématům spojených s derivacemi funkcí. Nejprve demonstrujme pojem křivosti a oskulační kružnice na elipse.

**6.37.** Určete křivost elipsy $x^2 + 2y^2 = 2$ v jejích vrcholech (‖4.47‖). Udejte též rovnice oskulačních kružnic v těchto vrcholech.

**Věta.** *(1) Je-li $r(t) : \mathbb{R} \to \mathbb{R}^n$ diferencovatelný vektor a $\Psi : \mathbb{R}^n \to \mathbb{R}^m$ lineární zobrazení, pak pro derivaci zobrazení $\Psi \circ r$ platí*

$$\frac{d(\Psi \circ r)}{dt} = \Psi \circ \frac{dr}{dt}.$$

*(2) Uvažujme diferencovatelné vektory $r_1, \ldots, r_k : \mathbb{R} \to \mathbb{R}^n$ a $k$–lineární formu $\Phi : \mathbb{R}^n \times \ldots \times \mathbb{R}^n$ na prostoru $\mathbb{R}^n$. Pak pro derivaci složeného zobrazení*

$$\varphi(t) = \Phi(r_1(t), \ldots, r_k(t))$$

*platí (zobecněné Leibnizovo) pravidlo*

$$\frac{d\varphi}{dt} = \Phi\big(\frac{dr_1}{dt}, r_2, \ldots, r_k\big) + \cdots + \Phi\big(r_1, \ldots, r_{k-1}, \frac{dr_k}{dt}\big).$$

*(3) Předchozí tvrzení zůstává bezezbytku v platnosti i pokud $\Phi$ má také hodnoty ve vektorovém prostoru (a je lineární ve všech $k$ argumentech).*

Důkaz. (1) V lineární algebře se ukazuje, že lineární zobrazení jsou dána konstantní maticí skalárů $A = (a_{ij})$ tak, že

$$\Psi \circ r(t) = \Big(\sum_{i=1}^n a_{1i} r_i(t), \ldots, \sum_{i=1}^n a_{mi} r_i(t)\Big).$$

Derivaci nyní provádíme po jednotlivých souřadnicích výsledku. Víme ale, že derivace se chová lineárně vůči skalárním lineárním kombinacím, viz Věta 5.33. Proto skutečně dostaneme derivaci $\Psi \circ r(t)$ prostým vyčíslením původního lineárního zobrazení $\Psi$ na derivaci $r'(t)$.

(2) Zcela obdobně dostaneme i druhé tvrzení. V souřadnicích rozepíšeme vyčíslení $k$–lineární formy na vektorech $r_1, \ldots, r_k$ takto

$$\Phi(r_1(t), \ldots, r_k(t)) = \sum_{i_1,\ldots,i_k=1}^n B_{i_1\ldots i_k} \cdot (r_1)_{i_1}(t) \ldots (r_k)_{i_k}(t),$$

kde skaláry $B_{i_1\ldots i_k}$ jsou pro každou volbu indexů dány jako hodnota dané formy $\Phi(e_{i_1}, \ldots, e_{i_k})$ na zvolené $k$–tici bázových vektorů. Pravidlo pro derivaci součinu skalárních funkcí nám dá právě dokazované tvrzení.

(3) Pokud má $\Phi$ vektorové hodnoty, je zadáno konečně mnoha komponentami a můžeme použít předchozí úvahu na každou z nich. □

Na euklidovském prostoru $\mathbb{R}^3$ máme kromě skalárního součinu, který dvěma vektorům přiřadí skalár, také vektorový součin, který dvěma vektorům $u$ a $v$ přiřadí vektor $u \times v \in \mathbb{R}^3$, viz 4.24. Tento vektor $u \times v$ je kolmý na oba vektory $u$ a $v$, má velikost rovnou obsahu rovnoběžníku určeného vektory $u$ a $v$ (v tomto pořadí) a orientaci takovou, aby trojice $u, v, u \times v$ byla kladně orientovanou bází.

Z předchozí věty okamžitě vyplývají užitečná tvrzení:

**Důsledek.** *V prostoru $\mathbb{R}^3$ uvažme vektory $u(t)$ a $v(t)$. Pro derivace jejich skalárního součinu $\langle u(t), v(t)\rangle$ a vektorového součinu $u(t) \times v(t)$ platí*

$$\frac{d}{dt}\langle u(t), v(t)\rangle = \langle u'(t), v(t)\rangle + \langle u(t), v'(t)\rangle \tag{6.1}$$

$$\frac{d}{dt}(u(t) \times v(t)) = u'(t) \times v(t) + u(t) \times v'(t) \tag{6.2}$$

**Řešení.** Protože elipsa je v daných souřadnicích již v základním tvaru (nejsou přítomny ani smíšené ani lineární členy), je zadaná báze již bází polární. Jejími osami jsou souřadnicové osy $x$ a $y$, vrcholy pak body $[\sqrt{2},0]$, $[-\sqrt{2},0]$, $[0,1]$ a $[0,-1]$. Spočítejme nejprve křivost ve vrcholu $[0,1]$. Uvážíme-li souřadnici $y$ jakožto funkci souřadnice $x$ (v okolí bodu $[0,1]$ je jednoznačně určena), pak derivací rovnice elipsy podle proměnné $x$ dostáváme $2x+4yy'=0$, tedy $y'=-\frac{x}{2y}$ ($y'$ značí derivaci funkce $y(x)$ podle proměnné $x$; nejedná se vlastně o nic jiného, než o vyjádření derivace funkce dané implicitně, viz 8.18. Derivací této rovnice podle $x$ pak obdržíme $y''=-\frac{1}{2}(\frac{1}{y}-\frac{xy'}{y^2})$. V bodě $[1,0]$ pak dostáváme $y'=0$ a $y''=-\frac{1}{2}$ (ke stejným výsledkům bychom došli, kdybychom explicitně vyjádřili z rovnice elipsy $y=\frac{1}{2}\sqrt{2-x^2}$ a derivovali; výpočet by byl jen o něco složitější, jak si jistě čtenář sám ověří). Poloměr oskulační kružnice bude tedy dle vztahu v 6.13

$$\frac{(1+(y')^2)^{\frac{3}{2}}}{(y'')^2}=-2,$$

respektive 2 a znaménko nám říká, že kružnice bude „pod“ grafem funkce. Z úvah v 6.13 a 6.16 vyplývá, že její střed bude ve směru opačném k normále této křivky, tedy na ose $y$ (funkce $y$ jakožto funkce proměnné $x$ má derivaci v bodě $[0,1]$, tečna k jejímu grafu v tomto bodě bude tudíž rovnoběžná z osou $x$, normála je pak kolmá na tečnu, což je v tomto bodě osa $y$. Poloměr je 2, střed tak bude v bodě $[0,\,1-2]=[0,\,-1]$. Celkem bude rovnice oskulační kružnice elipsy $x^2+2y^2=2$ v bodě $[0,1]$ znít $x^2+(y+1)^2=4$. Analogicky určíme rovnici oskulační kružnice v bodě $[0,-1]$: $x^2+(y-1)^2=4$. Křivosti elipsy (jakožto křivky) v těchto bodech jsou pak rovny $\frac{1}{2}$ (absolutní hodnota křivosti grafu funkce).

Pro určení oskulační kružnice v bodě $[\sqrt{2},0]$ budeme uvažovat rovnici elipsy, jakožto předpis pro proměnnou $x$ pomocí proměnné $y$, tedy $x$ jako funkci $y$. (v okolí bodu $[\sqrt{2},0]$ není totiž určena proměnná $y$ jako funkce $x$ jednoznačně, nemůžeme tedy použít předchozí postup – technicky by to dopadlo tak, že bychom dělili nulou). Postupně dostáváme: $2xx'+4y=0$, tedy $x'=-2\frac{y}{x}$, a $x''=-2(\frac{1}{x}-\frac{yx'}{x^2})$. V bodě $[\sqrt{2},0]$ je tudíž $x'=0$ a $x''=-\sqrt{2}$ a poloměr oskulační kružnice je podle 6.13 $\rho=-\frac{1}{\sqrt{2}}=\frac{\sqrt{2}}{2}$. Normála směřuje v bodě $[\sqrt{2},0]$ po ose $x$ do $-\infty$, střed oskulační kružnice tedy bude na ose $x$ na druhou stranu ve vzdálenosti $\frac{\sqrt{2}}{2}$, tudíž v bodě $[\sqrt{2}-\frac{\sqrt{2}}{2},0]=$ $=[\frac{\sqrt{2}}{2},0]$. Celkem rovnice oskulační kružnice ve vrcholu $[\sqrt{2},0]$ bude $(x-\frac{\sqrt{2}}{2})^2+y^2=\frac{1}{2}$. Křivost je v obou těchto vrcholech rovna $\sqrt{2}$.

**6.16. Křivost křivek.** Nyní máme daleko mocnější nástroje pro studium křivek systematičtějším způsobem, než když jsme diskutovali křivost grafů funkcí.



Podívejme se obecně na křivky $r(t)$ v prostoru a předpokládejme, že jsou parametrizovány tak, aby jejich tečný vektor měl stále velikost jedna, tj. $\langle r'(t),r'(t)\rangle=1$ pro všechna $t$. Říkáme, že je křivka $r(t)$ *parametrizována délkou*. Další derivací tohoto jednotkového vektoru $r'(t)$ dostaneme vektor $r''(t)$, pro který spočteme (využíváme symetrie skalárního součinu)

$$0=\frac{d}{dt}\langle r'(t),r'(t)\rangle=2\langle r''(t),r'(t)\rangle$$

a je tedy vektor zrychlení $r''(t)$ vždy kolmý na vektor rychlosti. To odpovídá představě, že při volbě parametrizace s konstantní velikostí rychlosti nemůže být zrychlení ve směru pohybu znatelné, musí tedy celé zrychlení být v rovině kolmé k vektoru rychlosti.

Pokud je druhá derivace nenulová, nazýváme normovaný vektor

$$n(t)=\frac{1}{\|r''(t)\|}r''(t)$$

*hlavní normálou* křivky $r(t)$. Skalární funkce $\kappa(t)$ splňující (v bodech, kde je $r''(t)\neq 0$)

$$r''(t)=\kappa(t)n(t)$$

se nazývá *křivost křivky* $r(t)$. V nulových bodech druhé derivace definujeme $\kappa(t)$ také nulovou hodnotou.

V nenulových bodech křivosti je dobře definován jednotkový vektor $b(t)=r'(t)\times n(t)$, který nazýváme *binormála křivky* $r(t)$. Přímým výpočtem dostáváme

$$\begin{aligned}0=\frac{d}{dt}\langle b(t),r'(t)\rangle&=\langle b'(t),r'(t)\rangle+\langle b(t),r''(t)\rangle=\\&=\langle b'(t),r'(t)\rangle+\kappa(t)\langle b(t),n(t)\rangle=\langle b'(t),r'(t)\rangle,\end{aligned}$$

což ukazuje, že je tečný vektor k binormále kolmý jak na $b(t)$, tak na $r'(t)$. Musí tedy být násobkem vektoru hlavní normály. Píšeme

$$b'(t)=-\tau(t)n(t)$$

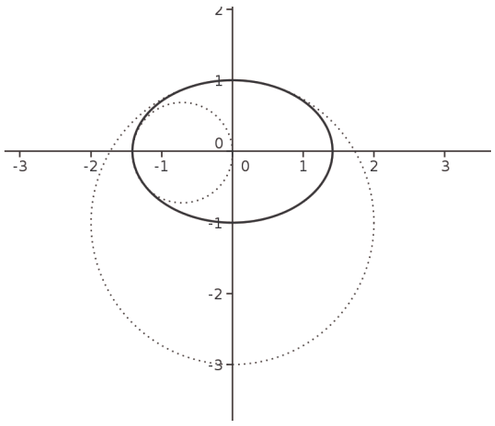
a skalární funkci $\tau(t)$ nazýváme *torze křivky* $r(t)$.

Ještě jsme nespočetli rychlost změny hlavní normály, kterou můžeme také psát jako $n(t)=b(t)\times r'(t)$.

$$\begin{aligned}n'(t)&=b'(t)\times r'(t)+\kappa(t)b(t)\times n(t)=\\&=-\tau(t)n(t)\times r'(t)+\kappa(t)(-r'(t))=\\&=\tau(t)b(t)-\kappa(t)r'(t).\end{aligned}$$

Postupně jsme pro všechny body s nenulovou druhou derivací křivky $r(t)$ parametrizované délkou oblouku odvodili význačnou bázi $(r'(t),n(t),b(t))$, které se v klasické literatuře říká *Frenetův repér* a zároveň jsme v této bázi vyjádřili derivace jejích komponent formou tzv. *Frenetových–Serretových vzorců*

$$\frac{dr'}{dt}(t)=\kappa(t)n(t),\qquad\frac{dn}{dt}(t)=\tau(t)b(t)-\kappa(t)r'(t),$$
$$\frac{db}{dt}(t)=-\tau(t)n(t).$$




□

**6.38. Poznámka.** Vrcholy elipsy (obecně uzavřené hladké křivky v rovině) lze definovat jako body, ve kterých má funkce křivosti nějaký extrém. To, že elipsa měla čtyři vrcholy není náhoda. Platí tzv. „Věta o čtyřech vrcholech“, sice že uzavřená křivka třídy $C^3$ má alespoň čtyři vrcholy. (Křivka třídy $C^3$ je lokálně dána parametricky body $[f(t), g(t)] \in \mathbb{R}^2, t \in (a, b) \subset \mathbb{R}$, kde $f$ i $g$ jsou funkce třídy $C^3(\mathbb{R})$.) Křivost elipsy v jakémkoli jejím bodě se tedy nalézá mezi křivostmi v jejích vrcholech, tj. mezi $\frac{1}{2}$ a $\sqrt{2}$.

### B. Integrování

Nejprve několik jednoduchých příkladů, které by měl zvládnout každý.

**6.39.** Užitím základních vzorců vypočtěte

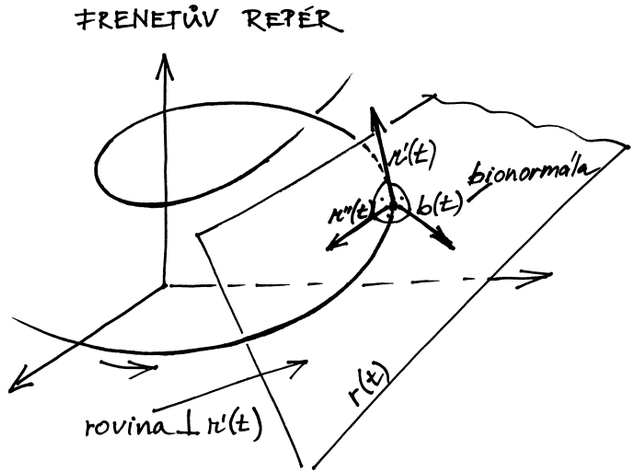
(a) $\int \frac{1}{\sqrt[3]{x}}\, dx,\ x \neq 0$;
(b) $\int \operatorname{tg}^2 x\, dx,\ x \neq \frac{\pi}{2} + k\pi,\ k \in \mathbb{Z}$;
(c) $\int \frac{\cos x}{1+\sin x}\, dx,\ x \neq -\frac{\pi}{2} + 2k\pi,\ k \in \mathbb{Z}$;
(d) $\int 6\sin 5x + \cos\frac{x}{2} + 2\,\mathrm{e}^{\frac{2x}{3}}\, dx,\ x \in \mathbb{R}$.

**Řešení.** Případ (a). Ihned určíme

$$\int \frac{1}{\sqrt[3]{x}}\, dx = \int x^{-1/3}\, dx = \frac{x^{\frac{2}{3}}}{\frac{2}{3}} + C = \frac{3}{2}\sqrt[3]{x^2} + C,$$

přičemž zápisu, ve kterém přičítáme $C \in \mathbb{R}$, je třeba rozumět tak, že všechny primitivní funkce získáme právě pomocí konstantního posunutí libovolné primitivní funkce. To ovšem platí pouze na intervalu. Jinak řečeno, hodnota $C$ je obecně různá pro $x < 0$ a pro $x > 0$. Měli bychom tedy uvažovat hodnoty $C_1$ a $C_2$. Pro jednoduchost budeme ale používat zápis bez indexů a uvádění příslušných intervalů. Navíc si budeme pomáhat položeními $aC = C$ pro $a \in \mathbb{R} \setminus \{0\}$ a $C + b = C$ pro $b \in \mathbb{R}$, která jsou založena na skutečnosti, že

$$\{C;\ C \in \mathbb{R}\} = \{aC;\ C \in \mathbb{R}\} = \{C + b;\ C \in \mathbb{R}\} = \mathbb{R}.$$




Všimněme si, že pokud křivka $r(t)$ leží stále v jedné rovině, pak je její torze identicky nulovou funkcí. Ve skutečnosti platí i obrácené tvrzení, které tu nebudeme dokazovat, vyplývá ale z následujícího klasického výsledku geometrické teorie křivek:

Dvě křivky v prostoru parametrizované délkou oblouku lze jednu na druhou zobrazit pomocí euklidovské transformace, právě když jejich funkce křivosti a torze splývají, až na konstantní posuv parametru. Navíc, pro každou volbu hladkých funkcí $\kappa$ a $\tau$ existuje hladká křivka s těmito parametry. Tento výsledek tu nebudeme dokazovat.

Přímým výpočtem můžeme zkontrolovat, že křivost grafu funkce $y = f(x)$ v rovině a křivost $\kappa$ této křivky zavedené v tomto odstavci splývají. Skutečně, výpočtem derivace složené funkce s pomocí diferenciálu délky oblouku pro graf funkce ve tvaru

$$dt = (1 + (f_x)^2)^{1/2} dx, \qquad dx = (1 + (f_x)^2)^{-1/2} dt$$

(píšeme zde $f_x = \frac{df}{dx}$) dostaneme pro náš jednotkový tečný vektor grafu křivky vztah

$$r'(t) = (x'(t), y'(t)) = \left((1 + (f_x)^2)^{-1/2},\ f_x(1 + (f_x)^2)^{-1/2}\right)$$

a poměrně nepřehledným, ale obdobným výpočtem druhé derivace a její velikosti skutečně obdržíme

$$\kappa^2 = \|r''\|^2 = (\tfrac{d^2 f}{dx^2})^2 (1 + (f_x)^2)^{-3}.$$

**6.17. Aproximace derivací a asymptotické odhady.** Hned na



začátku této učebnice jsme v odstavcích 1.3, 1.9 a dále diskutovali, jak zadávat hodnotu funkce pomocí změn, tj. diferencí. V další části textu budeme obdobně rekonstruovat funkci $f$ z jejích derivací, tj. okamžitých změn. Předtím se ale pozastavme u souvislosti derivací a diferencí. Klíčem nám k tomu bude Taylorův rozvoj se zbytkem.

Předpokládejme, že z (dostatečně) diferencovatelné funkce $f(x)$, definované na intervalu $[a, b]$, známe hodnoty $f_i = f(x_i)$ v bodech $x_0 = a, x_1, x_2, \ldots, x_n = b$, přičemž pro všechny indexy $i = 1, \ldots, n$ platí $x_i - x_{i-1} = h > 0$ pro nějakou konstantu $h$. Taylorův rozvoj pro funkci $f$ v bodě $x_i$ pišme ve tvaru

$$f(x_i \pm h) = f_i \pm h f'(x_i) + \frac{h^2}{2} f''(x_i) \pm \frac{h^3}{3!} f^{(3)}(x_i) + \ldots$$

Zcela korektní vyjádření bychom pak obdrželi např. substitucemi $\hat{C} = aC$, $\tilde{C} = C + b$. Tato zjednodušení prokáží svou užitečnost při počítání náročnějších příkladů. Činí totiž postupy a úpravy přehlednějšími.

Případ (b). Postupné úpravy integrované funkce vedou na

$$\int \operatorname{tg}^2 x\,dx = \int \tfrac{\sin^2 x}{\cos^2 x}\,dx = \int \tfrac{1-\cos^2 x}{\cos^2 x}\,dx = \\ = \int \tfrac{1}{\cos^2 x}\,dx - \int 1\,dx = \operatorname{tg} x - x + C,$$

kde jsme si pomohli znalostí derivace

$$(\operatorname{tg} x)' = \tfrac{1}{\cos^2 x}, \qquad x \neq \tfrac{\pi}{2} + k\pi,\ k \in \mathbb{Z}.$$

Případ (c). Stačí si uvědomit, že se jedná o speciální případ vzorce

$$\int \tfrac{f'(x)}{f(x)}\,dx = \ln|f(x)| + C,$$

jenž můžeme přímo ověřit derivováním

$$(\ln|f(x)| + C)' = \big(\ln\big[\pm f(x)\big]\big)' + (C)' = \tfrac{[\pm f(x)]'}{\pm f(x)} = \tfrac{\pm f'(x)}{\pm f(x)} = \tfrac{f'(x)}{f(x)}.$$

Platí tudíž

$$\int \tfrac{\cos x}{1+\sin x}\,dx = \ln\,(1+\sin x) + C.$$

Případ (d). Protože integrál součtu je součtem integrálů (pokud mají jednotlivé integrály smysl) a nenulovou konstantu lze z integrálu vytknout kdykoli, je

$$\int 6\sin 5x + \cos\frac{x}{2} + 2\,\mathrm{e}^{\frac{2x}{3}}\,dx = -\frac{6}{5}\cos 5x + 2\sin\frac{x}{2} + 3\,\mathrm{e}^{\frac{2x}{3}} + C.$$

□

**6.40.** Integrováním „po paměti“ vyjádřete

(a) $\int \mathrm{e}^{-x}\,dx,\ x \in \mathbb{R}$;
(b) $\int \frac{1}{\sqrt{4-x^2}}\,dx,\ x \in (-2,2)$;
(c) $\int \frac{1}{x^2+3}\,dx,\ x \in \mathbb{R}$;
(d) $\int \frac{3x^2+1}{x^3+x+2}\,dx,\ x \neq -1$.

**Řešení.** Snadno získáváme

(a) $\int \mathrm{e}^{-x}\,dx = -\int -\mathrm{e}^{-x}\,dx = -\mathrm{e}^{-x} + C$;
(b) $\int \frac{1}{\sqrt{4-x^2}}\,dx = \int \frac{\frac{1}{2}}{\sqrt{1-\left(\frac{x}{2}\right)^2}}\,dx = \arcsin\frac{x}{2} + C$;
(c) $\int \frac{1}{x^2+3}\,dx = \frac{1}{3}\int \frac{1}{\frac{x^2}{3}+1}\,dx = \frac{1}{\sqrt{3}}\int \frac{\frac{1}{\sqrt{3}}}{1+\left(\frac{x}{\sqrt{3}}\right)^2}\,dx = \\ = \frac{1}{\sqrt{3}}\operatorname{arctg}\frac{x}{\sqrt{3}} + C$;
(d) $\int \frac{3x^2+3}{x^3+3x+2}\,dx = \ln\left|x^3+3x+2\right| + C$,
kde jsme využili vzorec $\int \frac{f'(x)}{f(x)}\,dx = \ln|f(x)| + C$. □

**6.41.** Spočtěte neurčitý integrál

$$\int \left(7^x + 4\,\mathrm{e}^{\frac{2x}{3}} - \tfrac{1}{2^x} + 9\sin 5x + 2\cos\tfrac{x}{2} - \tfrac{3}{\cos^2 x} + \tfrac{1}{3-x}\right)dx$$

pro $x \neq 3$, $x \neq \frac{\pi}{2} + k\,\pi$, $k \in \mathbb{Z}$.

**Řešení.** Pouze spojením dříve odvozených vzorců dostáváme $\int \left(7^x + 4\,\mathrm{e}^{\frac{2x}{3}} - \frac{1}{2^x} + 9\sin 5x + 2\cos\frac{x}{2} - \frac{3}{\cos^2 x} + \frac{1}{3-x}\right)dx =$

Víme, že když v rozvoji skončíme členem řádu $k$ v $h$, tj. výrazem obsahujícím $h^k$, pak se dopustíme chyby, která je omezená odhadem výrazu

$$\frac{h^{k+1}}{(k+1)!}f^{(k+1)}(x)$$

na intervalu $[x_i - h, x_i + h]$. Pokud je $(k+1)$–ní derivace $f$ spojitá, můžeme ji odhadnout konstantou. Vidíme pak, že se pro malá $h$ chová chyba aproximace pomocí Taylorova polynomu stupně $k$ stejně jako $h^{k+1}$, až na konstantní násobek. Takovému odhadu se říká *asymptotický odhad*.

**Definice.** Řekneme, že výraz $G(h)$ je pro $h \to 0$ asymptoticky stejný s výrazem $F(h)$ a píšeme $G(h) = \mathrm{O}(F(h))$, jestliže existuje konečná limita

$$\lim_{h\to 0}\frac{G(h)}{F(h)} = a \in \mathbb{R}.$$

Označme si hledané odhady hodnot derivací $f(x)$ v bodech $x_i$ jako $f_i^{(j)}$ a pišme Taylorův rozvoj stručně takto:

$$f_{i\pm1} = f_i \pm f_i' h + \frac{f_i''}{2}h^2 \pm \frac{f_i'''}{6}h^3 + \dots$$

Pro odhady první derivace můžeme okamžitě použít tři různé diference spočtené z Taylorova rozvoje:

$$f_i^{(1)} = \frac{f_{i+1} - f_{i-1}}{2h} - \frac{h^2}{3!}f^{(3)}(x_i) - \dots$$
$$f_i^{(1)} = \frac{f_{i+1} - f_i}{h} - \frac{h}{2!}f''(x_i) + \dots$$
$$f_i^{(1)} = \frac{f_i - f_{i-1}}{h} + \frac{h}{2!}f''(x_i) + \dots$$

kde jsme prostě jen odečetli příslušné polynomy. Získáváme tak numerická vyjádření pro první derivaci. První z nich má asymptotický odhad chyby

$$f^{(1)} = \frac{f_{i+1} - f_{i-1}}{2h} + \mathrm{O}(h^2),$$

další dvě mají chybu $\mathrm{O}(h)$. Říkáme jim *středová diference*, *dopředná diference* a *zpětná diference*. Kupodivu je středová diference o řád lepší než zbylé dvě.

Stejně můžeme postupovat při odhadu druhé derivace. Abychom uměli spočíst $f''(x_i)$ z vhodné kombinace Tayulorových polynomů, potřebujeme vyrušit první derivace i hodnotu v $x_i$. Nejjednodušší kombinace vyruší i všechny liché derivace:

$$f_i^{(2)} = \frac{f_{i+1} - 2f_i + f_{i+1}}{h^2} + \frac{h^2}{12}f^{(4)}(x_i) + \dots.$$

Hovoříme o *diferenci druhého řádu* a stejně jako u středové první diference je asymptotický odhad chyby o jeden řád lepší, než bychom na první pohled čekali:

$$f_i^{(2)} = \frac{f_{i+1} - 2f_i + f_{i+1}}{h^2} + \mathrm{O}(h^2).$$

### 2. Integrování

**6.18. Newtonův integrál.** Nyní se budeme zajímat o opačný postup než tomu bylo u derivování. Budeme chtít ze znalosti okamžitých změn nějaké funkce rekonstruovat její skutečné hodnoty. Jestliže danou funkci $f(x)$ považujeme za derivaci neznámé funkce $F(x)$, pak na úrovni diferenciálů můžeme psát

$= \frac{7^x}{\ln 7} + 6\,\mathrm{e}^{\frac{2x}{3}} + \frac{1}{2^x \ln 2} - \frac{9}{5}\cos 5x + 4\sin\frac{x}{2} - 3\,\mathrm{tg}\,x - \ln|3-x| + C$
.

□

Pro vyjádření následujících integrálů použijeme metody per partes (viz 6.20).

**6.42.** Vypočtěte $\int x\cos x\,\mathrm{d}x$, $x \in \mathbb{R}$ a $\int \ln x\,dx$, $x > 0$;

**Řešení.**

$$\int \ln x\,\mathrm{d}x = \left|\begin{matrix} u = \ln x & u' = \frac{1}{x} \\ v' = 1 & v = x \end{matrix}\right| =$$

$$= x\ln x - \int 1\,\mathrm{d}x = x\ln x - x + C,$$

$$\int x\cos x\,\mathrm{d}x = \left|\begin{matrix} u = x & u' = 1 \\ v' = \cos x & v = \sin x \end{matrix}\right| = x\sin x -$$

$$- \int \sin x\,\mathrm{d}x = x\sin x + \cos x + C.$$

□

**6.43.** Metodou per partes vypočítejte

(a) $\int \left(x^2+1\right)\mathrm{e}^{-x}\,dx$, $x \in \mathbb{R}$,
(b) $\int (2x-1)\ln x\,dx$, $x > 0$,
(c) $\int \mathrm{arctg}\,x\,dx$, $x \in \mathbb{R}$,
(d) $\int \mathrm{e}^x \sin x\,dx$, $x \in \mathbb{R}$,

**Řešení.** Nejdříve vyzdvihněme, že metodou per partes lze vypočítat každý integrál ve tvaru

$$\int P(x)\,a^{bx}\,dx, \quad \int P(x)\sin(bx)\,dx, \quad \int P(x)\cos(bx)\,dx,$$

$$\int P(x)\log_a^n x\,dx, \qquad \int x^b \log_a^n (kx)\,dx,$$

$$\int P(x)\arcsin(bx)\,dx, \qquad \int P(x)\arccos(bx)\,dx,$$

$$\int P(x)\,\mathrm{arctg}\,(bx)\,dx, \qquad \int P(x)\,\mathrm{arccotg}\,(bx)\,dx,$$

$$\int a^{bx}\sin(cx)\,dx, \qquad \int a^{bx}\cos(cx)\,dx,$$

kde $P$ je libovolný polynom a

$$a \in (0,1)\cup(1,+\infty), \quad b, c \in \mathbb{R}\setminus\{0\}, \quad n \in \mathbb{N}, \quad k > 0.$$

$$dF = f(x)dx.$$

Funkci $F$ nazýváme *primitivní funkce* nebo *neurčitý integrál* funkce $f$ a tradičně píšeme

$$F(x) = \int f(x)dx.$$

**Lemma.** *Primitivní funkce $F(x)$ k funkci $f(x)$ je na každém intervalu $[a,b]$ určena jednoznačně až na aditivní konstantu.*

Důkaz. Tvrzení je okamžitým důsledkem Lagrangeovy věty o střední hodnotě, viz 5.38. Skutečně, pokud je $F'(x) = G'(x) = f(x)$ na celém intervalu $[a,b]$, funkce $(F-G)(x)$ má ve všech bodech $c$ intervalu $[a,b]$ nulovou derivaci. Pak ale podle věty o střední hodnotě pro všechny body $x$ v tomto intervalu

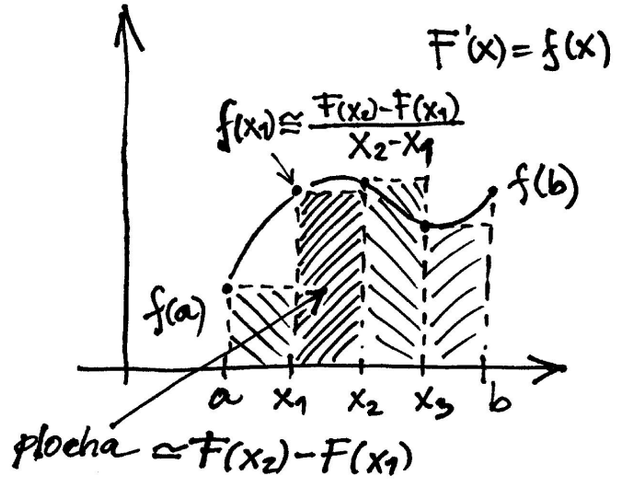
$$F(x) - G(x) = F(a) - G(a) + 0\cdot(x-a).$$

Musí tedy být rozdíl hodnot funkcí $F$ a $G$ stejný na celém intervalu $[a,b]$. □

Předchozí lemma nás vede k tomu, že neurčitý integrál obvykle zapisujeme ve tvaru

$$F(x) = \int f(x)dx + C$$

s neznámou konstantou $C$.




Hodnotu reálné funkce $f(x)$ můžeme také považovat za okamžitý přírůstek plochy vymezené grafem funkce $f$ a osou $x$ a snažit se najít velikost této plochy mezi krajními hodnotami $a$ a $b$ nějakého intervalu. Zkusme tuto představu dát do souvislosti s neurčitým integrálem. Předpokládejme tedy, že na intervalu $[a,b]$ známe reálnou funkci a její neurčitý integrál $F(x)$, tj. $F'(x) = f(x)$.

Jestliže rozdělíme interval $[a,b]$ na $n$ částí volbou bodů

$$a = x_0 < x_1 < \cdots < x_n = b$$

a přiblížíme hodnoty derivací v bodech $x_i$ výrazy

$$f(x_i) = F'(x_i) \simeq \frac{F(x_{i+1}) - F(x_i)}{x_{i+1} - x_i},$$

Proto víme, že

$$\begin{aligned}
\text{(a)}\ \int \left(x^2+1\right)\mathrm{e}^{-x}\,dx &= \left|\begin{array}{l|l} F(x)=x^2+1 & F'(x)=2x \\ G'(x)=\mathrm{e}^{-x} & G(x)=-\mathrm{e}^{-x}\end{array}\right| = \\
&= -\left(x^2+1\right)\mathrm{e}^{-x}+\int 2x\,\mathrm{e}^{-x}\,dx = \\
&= \left|\begin{array}{l|l} F(x)=2x & F'(x)=2 \\ G'(x)=\mathrm{e}^{-x} & G(x)=-\mathrm{e}^{-x}\end{array}\right| = \\
&= -\left(x^2+1\right)\mathrm{e}^{-x}-2x\,\mathrm{e}^{-x}+\int 2\,\mathrm{e}^{-x}\,dx = \\
&= -\left(x^2+1\right)\mathrm{e}^{-x}-2x\,\mathrm{e}^{-x}-2\,\mathrm{e}^{-x}+C = \\
&= -\mathrm{e}^{-x}\left(x^2+2x+3\right)+C; \\
\text{(b)}\ \int (2x-1)\ln x\ dx &= \left|\begin{array}{l|l} F(x)=\ln x & F'(x)=1/x \\ G'(x)=2x-1 & G(x)=x^2-x\end{array}\right| = \\
&= \left(x^2-x\right)\ln x-\int \frac{x^2-x}{x}\,dx = \\
&= \left(x^2-x\right)\ln x+\int 1-x\,dx = \\
&= \left(x^2-x\right)\ln x+x-\frac{x^2}{2}+C; \\
\text{(c)}\ \int \operatorname{arctg} x\,dx &= \left|\begin{array}{l|l} F(x)=\operatorname{arctg} x & F'(x)=\frac{1}{1+x^2} \\ G'(x)=1 & G(x)=x\end{array}\right| = \\
&= x\operatorname{arctg} x-\int \frac{x}{1+x^2}\,dx = \\
&= x\operatorname{arctg} x-\frac{1}{2}\int \frac{2x}{1+x^2}\,dx = \\
&= x\operatorname{arctg} x-\frac{1}{2}\ln\left(1+x^2\right)+C; \\
\text{(d)}\ \int \mathrm{e}^x\sin x\,dx &= \left|\begin{array}{l|l} F(x)=\mathrm{e}^x & F'(x)=\mathrm{e}^x \\ G'(x)=\sin x & G(x)=-\cos x\end{array}\right| = \\
&= -\mathrm{e}^x\cos x+\int \mathrm{e}^x\cos x\,dx = \\
&= \left|\begin{array}{l|l} F(x)=\mathrm{e}^x & F'(x)=\mathrm{e}^x \\ G'(x)=\cos x & G(x)=\sin x\end{array}\right| = \\
&= -\mathrm{e}^x\cos x+\mathrm{e}^x\sin x-\int \mathrm{e}^x\sin x\,dx,
\end{aligned}$$

odkud plyne

$$\int \mathrm{e}^x\sin x\,dx=\tfrac{1}{2}\,\mathrm{e}^x\,(\sin x-\cos x)+C\,. \qquad \square$$

Pro vyjádření následujících integrálů je výhodné použít substituční metodu (viz 6.21).

**6.44.** Integrujte

(a) $\int \cos^5 x\cdot\sin x\ dx,\ x\in\mathbb{R}$;
(b) $\int \cos^5 x\cdot\sin^2 x\ dx,\ x\in\mathbb{R}$;
(c) $\int \frac{\sin^4 x}{\cos^4 x}\,dx,\ x\in\left(-\frac{\pi}{2},\frac{\pi}{2}\right)$;
(d) $\frac{1-\sqrt[3]{x}+\sqrt{x}}{\sqrt[6]{x^5}+x}\,dx,\ x>0$.

dostáváme součtem přes všechny intervaly našeho dělení odhad hledané velikosti plochy:

$$\sum_{i=0}^{n-1} f(x_i)\cdot(x_{i+1}-x_i)\simeq\sum_{i=0}^{n-1}\frac{F(x_{i+1})-F(x_i)}{x_{i+1}-x_i}\cdot(x_{i+1}-x_i)= F(b)-F(a).$$

Dá se tedy očekávat, že pro „dostatečně pěkné“ funkce $f(x)$ velikost plochy vymezené grafem funkce a osou $x$ skutečně spočteme jako rozdíl hodnot primitivní funkce v krajních bodech intervalu. Tomuto postupu se říká *Newtonův integrál*. Píšeme

$$\int_a^b f(x)dx=[F(x)]_a^b=F(b)-F(a)$$

a hovoříme také o (Newtonově) *určitém integrálu* v mezích $a$, $b$.

V případě komplexní funkce $f$ je reálná a imaginární část jejího neurčitého integrálu jednoznačně dána reálnou a imaginární částí $f$, budeme proto dále bez dalších komentářů pracovat s reálnými funkcemi a ke komplexním se vrátíme v aplikacích, jak je to bude třeba.

**6.19. Integrace „po paměti“.** Ještě než si uděláme jasno, jak



Newtonův integrál skutečně souvisí s velikostí plochy a jak jej případně lze používat pro modelování praktických problémů, ukážeme několik postupů, jak Newtonův integrál spočítat. Budeme přitom využívat jen naše znalosti o derivacích.

Nejsnadnější je případ, kdy v integrované funkci umíme derivaci přímo uvidět. K tomu v jednoduchých případech stačí číst tabulky pro derivace funkcí v našem zvěřinci naopak. Dostáváme tak např. následující tvrzení pro všechna $a\in\mathbb{R}$ a $n\in\mathbb{Z}$, $n\neq-1$:

$$\int a\,dx=ax+C$$
$$\int ax^n\,dx=\tfrac{a}{n+1}x^{n+1}+C$$
$$\int \mathrm{e}^{ax}\,dx=\tfrac{1}{a}\,\mathrm{e}^{ax}+C$$
$$\int \frac{a}{x}\,dx=a\ln x+C$$
$$\int a\cos(bx)\,dx=\tfrac{a}{b}\sin(bx)+C$$
$$\int a\sin(bx)\,dx=-\tfrac{a}{b}\cos(bx)+C$$
$$\int a\cos(bx)\sin^n(bx)\,dx=\tfrac{a}{b(n+1)}\sin^{n+1}(bx)+C$$
$$\int a\sin(bx)\cos^n(bx)\,dx=-\tfrac{a}{b(n+1)}\cos^{n+1}(bx)+C$$
$$\int a\operatorname{tg}(bx)\,dx=-\frac{a}{b}\ln(\cos(bx))+C$$
$$\int \frac{a}{a^2+x^2}\,dx=\operatorname{arctg}\left(\tfrac{x}{a}\right)+C$$
$$\int \frac{-1}{\sqrt{a^2-x^2}}\,dx=\arccos\left(\tfrac{x}{a}\right)+C$$
$$\int \frac{1}{\sqrt{a^2-x^2}}\,dx=\arcsin\left(t\frac{x}{a}\right)+C.$$

Ve všech případech je zapotřebí dobře promyslet definiční obor, na kterém je neurčitý integrál dobře definován.

**Řešení.** Případ (a). Jde o jednoduchý příklad na tzv. první substituční metodu, jejíž podstatou je zapsat integrál ve tvaru

$$\int f(\varphi(x))\,\varphi'(x)\,dx \tag{6.7}$$

pro jisté funkce $f$ a $\varphi$. Takový integrál lze totiž pomocí substituce $y = \varphi(x)$ (nahrazujeme rovněž $dy = \varphi'(x)\,dx$, což dostáváme diferencováním $y = \varphi(x)$) převést na integrál $\int f(y)\,dy$. Substitucí $y = \cos x$, kdy je $dy = -\sin x\,dx$, tak obdržíme

$$\int \cos^5 x \cdot \sin x\,dx = -\int \cos^5 x\,(-\sin x)\;dx = -\int y^5\,dy =$$
$$= -\tfrac{y^6}{6} + C = -\tfrac{\cos^6 x}{6} + C.$$

Případ (b). Při vyjádření

$$\int \cos^5 x \cdot \sin^2 x\,dx = \int \left(\cos^2 x\right)^2 \sin^2 x \cdot \cos x\,dx =$$
$$= \int \left(1 - \sin^2 x\right)^2 \sin^2 x \cdot \cos x\,dx$$

se nabízí substituce $t = \sin x$, která dává

$$\int \cos^5 x \cdot \sin^2 x\,dx = \left| \begin{array}{c} t = \sin x \\ dt = \cos x\,dx \end{array} \right| = \int \left(1 - t^2\right)^2 t^2\,dt =$$
$$\int t^6 - 2t^4 + t^2\,dt = \tfrac{t^7}{7} - 2\tfrac{t^5}{5} + \tfrac{t^3}{3} + C = \tfrac{\sin^7 x}{7} - \tfrac{2\sin^5 x}{5} + \tfrac{\sin^3 x}{3} + C.$$

Případ (c). Neboť je sinus i kosinus v sudé mocnině, nelze postupovat jako v předchozím případě. Zkusme proto použít tzv. druhou substituční metodu znamenající přechod od $\int f(y)\,dy$ ke tvaru (‖6.7‖) pro $y = \varphi(x)$. Situace, kdy nahrazujeme jednodušší výraz za komplikovanější, může působit překvapivě. Nesmíme však zapomínat, že onen komplikovanější integrál může mít takovou podobu, že jej budeme schopni spočítat. Chceme určit primitivní funkce funkce $f(x) = \operatorname{tg}^4 x$. Má tedy smysl uvažovat substituci $u = \operatorname{tg} x$. Získáváme

$$\int \tfrac{\sin^4 x}{\cos^4 x}\,dx = \left| \begin{array}{c} x = \operatorname{arctg} u \\ dx = \frac{du}{1+u^2} \end{array} \right| = \int \tfrac{u^4}{1+u^2}\,du = \int u^2 - 1 + \tfrac{1}{u^2+1}\,du =$$
$$= \tfrac{u^3}{3} - u + \operatorname{arctg} u + C = \tfrac{\operatorname{tg}^3 x}{3} - \operatorname{tg} x + \operatorname{arctg}(\operatorname{tg} x) + C =$$
$$= \tfrac{\operatorname{tg}^3 x}{3} - \operatorname{tg} x + x + C.$$

Případ (d). Platí

$$\int \tfrac{1-\sqrt[3]{x}+\sqrt{x}}{\sqrt[6]{x^5}+x}\,dx = \left| \begin{array}{c} z^6 = x \\ 6z^5\,dz = dx \end{array} \right| = \int \tfrac{1-z^2+z^3}{z^5+z^6}\,6z^5\,dz =$$
$$= 6\int \tfrac{1-z^2+z^3}{1+z}\,dz =$$
$$= 6\int z^2 - 2z + 2 - \tfrac{1}{z+1}\,dz =$$
$$= 6\left(\tfrac{z^3}{3} - z^2 + 2z - \ln|z+1|\right) + C =$$
$$= 2\sqrt{x} - 6\sqrt[3]{x} + 12\sqrt[6]{x} - 6\ln\left(\sqrt[6]{x} + 1\right) + C,$$

kde jsme opět substitucí lehce určili (pro $z \neq -1$)

$$\int \tfrac{dz}{z+1} = \left| \begin{array}{c} v = z + 1 \\ dv = dz \end{array} \right| = \int \tfrac{dv}{v} = \ln|v| + C = \ln|z+1| + C\,. \quad \square$$

**6.45.** Vhodnou substitucí stanovte

(a) $\int \sqrt{2x-5}\,dx$, $x > \frac{5}{2}$;
(b) $\int \frac{(7+\ln x)^7}{x}\,dx$, $x > 0$;
(c) $\int \frac{\cos x}{(1+\sin x)^2}\,dx$, $x \neq \frac{(3+4k)\pi}{2}$, $k \in \mathbb{Z}$;
(d) $\int \frac{\cos x}{\sqrt{1+\sin^2 x}}\,dx$, $x \in \mathbb{R}$.

K takovýmto tabulkovým pravidlům pro integraci lze relativně snadno dodávat další pravidla jednoduchými pozorováními vhodné struktury integrovaných funkcí. Např.

$$\int \frac{f'(x)}{f(x)}\,dx = \ln|f(x)| + C$$

pro všechny spojitě diferencovatelné funkce $f$ na intervalech, kde jsou nenulové. Samozřejmě také z pravidel pro derivaci součtu diferencovatelných funkcí a konstantních násobků diferencovatelných funkcí je zřejmé že obdobná pravidla platí neurčitý integrál také.

**6.20. Integrace per partes.** Výpočet integrálu pomocí primitivní funkce (neurčitého integrálu), spolu s pravidlem

$$(F \cdot G)'(t) = F'(t) \cdot G(t) + F(t) \cdot G'(t)$$

pro derivaci součinu funkcí, dává následující formuli pro neurčitý integrál

$$F(x) \cdot G(x) + C = \int F'(x)G(x)\,dx + \int F(x)G'(x)\,dx.$$

Tato formule se většinou používá tak, že jeden z integrálů napravo je ten, který máme spočíst, zatímco druhý umíme spočítat snáze.

Nejlépe je princip vidět na příkladu. Spočteme

$$I = \int x \sin x\,dx.$$

V tomto případě pomůže volba $F(x) = x$, $G'(x) = \sin x$. Odtud $G(x) = -\cos x$ a proto také

$$I = -x\cos x - \int -\cos x\,dx = -x\cos x + \sin x + C.$$

Obvyklým trikem je také použít tento postup s $F'(x) = 1$:

$$\int \ln x\,dx = \int 1 \cdot \ln x\,dx = x\ln x - \int \frac{1}{x}x\,dx = x\ln x - x + C.$$

**6.21. Integrace pomocí substituce.** Další užitečný postup je odvozen z derivování složených funkcí. Jestliže

$$F'(y) = f(y), \qquad y = \varphi(x),$$

pro diferencovatelnou funkci $\varphi$ s nenulovou derivací, potom

$$\frac{dF(\varphi(x))}{dx} = F'(y) \cdot \varphi'(x)$$

a tedy $F(y) + C = \int f(y)\,dy$ lze spočíst jako

$$F(\varphi(x)) + C = \int f(\varphi(x))\varphi'(x)\,dx.$$

Dosazením $x = \varphi^{-1}(y)$ pak dostaneme původně požadovanou primitivní funkci. Častěji zapisujeme tuto skutečnost takto:

$$\int f(y)\,dy = \int f(\varphi(x))\varphi'(x)\,dx$$

a hovoříme o substituci za proměnnou $y$. Přímo na úrovni diferenciálů je možné substituci porozumět snadno tak, že (linearizované) přírůstky v proměnné $y$ a v $x$ jsou vzájemně ve vztahu popsaném formálně

$$dy = \varphi'(x)\,dx,$$

což odpovídá vztahu mezi integrovanými veličinami

$$f(y)dy = f(\varphi(x))\varphi'(x)dx.$$

**Řešení.** Platí

(a) $\int \sqrt{2x-5}\,dx = \left| \begin{array}{l} t = 2x-5 \\ dt = 2\,dx \end{array} \right| = \frac{1}{2}\int \sqrt{t}\,dt = \frac{1}{3}t^{\frac{3}{2}} + C =$
$= \frac{1}{3}\sqrt{(2x-5)^3} + C;$

(b) $\int \frac{(7+\ln x)^7}{x}\,dx = \left| \begin{array}{l} t = 7+\ln x \\ dt = \frac{1}{x}\,dx \end{array} \right| = \int t^7\,dt = \frac{t^8}{8} + C =$
$= \frac{(7+\ln x)^8}{8} + C;$

(c) $\int \frac{\cos x}{(1+\sin x)^2}\,dx = \left| \begin{array}{l} t = 1+\sin x \\ dt = \cos x\,dx \end{array} \right| = \int \frac{dt}{t^2} = -\frac{1}{t} + C =$
$= -\frac{1}{1+\sin x} + C;$

(d) $\int \frac{\cos x}{\sqrt{1+\sin^2 x}}\,dx = \left| \begin{array}{l} t = \sin x \\ dt = \cos x\,dx \end{array} \right| = \int \frac{1}{\sqrt{1+t^2}}\,dt =$
$= \left| \begin{array}{l} u = t + \sqrt{1+t^2} > 0 \\ du = \left(1 + \frac{t}{\sqrt{1+t^2}}\right)dt \\ \frac{du}{t+\sqrt{1+t^2}} = \frac{1}{\sqrt{1+t^2}}\,dt \end{array} \right| = \int \frac{1}{u}\,du = \ln u + C =$
$= \ln\left(t + \sqrt{1+t^2}\right) + C = \ln\left(\sin x + \sqrt{1+\sin^2 x}\right) + C.$

□

**6.46.** Určete

(a) $\int \frac{x}{\cos^2 x}\,dx,\ x \neq \frac{\pi}{2} + k\,\pi,\ k \in \mathbb{Z}$;
(b) $\int x^2\,\mathrm{e}^{-3x}\,dx,\ x \in \mathbb{R}$;
(c) $\int \cos^2 x\,dx,\ x \in \mathbb{R}$.

**Řešení.** Případ (a). Metodou per partes dostáváme
$\int \frac{x}{\cos^2 x}\,dx = \left| \begin{array}{ll} F(x) = x & F'(x) = 1 \\ G'(x) = \frac{1}{\cos^2 x} & G(x) = \operatorname{tg} x \end{array} \right| = x\operatorname{tg} x - \int \operatorname{tg} x\,dx =$
$= x\operatorname{tg} x + \int \frac{-\sin x}{\cos x}\,dx = x\operatorname{tg} x + \ln|\cos x| + C.$

Případ (b). Tentokráte očividně integrujeme součin dvou funkcí. Aplikováním metody per partes integrál převádíme na jiný integrál tak, že jednu funkci derivujeme a druhou integrujeme. Integrovat umíme obě (derivovat umíme všechny elementární funkce). Musíme se proto rozhodnout, kterou ze dvou variant metody použijeme (zda budeme integrovat funkci $y = x^2$, nebo $y = \mathrm{e}^{-3x}$). Uvědomme si, že per partes můžeme použít opakovaně a že $n$-tá derivace polynomu stupně $n \in \mathbb{N}$ je konstantní polynom. To nám dává způsob, jak lze spočítat

$$\int x^2\,\mathrm{e}^{-3x}\,dx = \left| \begin{array}{ll} F(x) = x^2 & F'(x) = 2x \\ G'(x) = \mathrm{e}^{-3x} & G(x) = -\frac{1}{3}\,\mathrm{e}^{-3x} \end{array} \right| =$$
$$= -\frac{1}{3}x^2\,\mathrm{e}^{-3x} + \frac{2}{3}\int x\,\mathrm{e}^{-3x}\,dx$$

a dále

$$\int x\,\mathrm{e}^{-3x}\,dx = \left| \begin{array}{ll} F(x) = x & F'(x) = 1 \\ G'(x) = \mathrm{e}^{-3x} & G(x) = -\frac{1}{3}\,\mathrm{e}^{-3x} \end{array} \right| =$$
$$= -\frac{1}{3}x\,\mathrm{e}^{-3x} + \frac{1}{3}\int \mathrm{e}^{-3x}\,dx = -\frac{1}{3}x\,\mathrm{e}^{-3x} - \frac{1}{9}\,\mathrm{e}^{-3x} + C.$$

Jako příklad ověříme touto metodou předposlední integrál v seznamu v 6.19. Pro integrál

$$I = \int \frac{1}{\sqrt{1-x^2}}\,dx$$

zvolíme substituci $x = \sin t$. Odtud $dx = \cos t\,dt$ a dostáváme

$$I = \int \frac{1}{\sqrt{1-\sin^2 t}}\cos t\,dt = \int \frac{1}{\sqrt{\cos^2 t}}\cos t\,dt =$$
$$= \int dt = t + C.$$

Zpětným dosazením $t = \operatorname{arcsin} x$ dopočítáme již známý vztah $I = \operatorname{arcsin} x + C$.

Při substitucích je třeba dát pozor na skutečnou existenci inverzní funkce k $y = \varphi(x)$, při výpočtu určitého Newtonova integrálu je třeba také správně přepočítávat meze integrování. Problémům s definičními obory inverzních funkcí se lze někdy vyhnout rozdělením integrace na několik intervalů.

**6.22. Integrace převedením na rekurence.** Často vede použití substitucí a metody per partes k rekurentním vztahům, ze kterých teprve lze dopočíst hledané integrály. Budeme ilustrovat na příkladu. Metodou per partes počítáme



$$I_m = \int \cos^m x\,dx = \int \cos^{m-1} x\cos x\,dx =$$
$$= \cos^{m-1} x\sin x - (m-1)\int \cos^{m-2} x(-\sin x)\sin x\,dx =$$
$$= \cos^{m-1} x\sin x + (m-1)\int \cos^{m-2} x\sin^2 x\,dx.$$

Odtud díky vztahu $\sin^2 x = 1 - \cos^2 x$ dostáváme

$$m I_m = \cos^{m-1} x\sin x + (m-1)I_{m-2}$$

a počáteční hodnoty jsou

$$I_0 = x, \quad I_1 = \sin x.$$

K těmto typům integrálů se substitucí $x = \operatorname{tg} t$ často převádí integrály, kde integrovaná funkce závisí na výrazech tvaru $(x^2+1)$. Skutečně, např. pro

$$J_k = \int \frac{dx}{(x^2+1)^k}$$

dostáváme zmíněnou substitucí (povšimněme si, že $dx = \cos^{-2} t\,dt$)

$$J_k = \int \frac{dt}{\cos^2 t\left(\frac{\sin^2 t}{\cos^2 t} + 1\right)^k} = \int \cos^{2k-2} t\,dt.$$

Pro $k = 2$ je výsledkem

$$J_2 = \frac{1}{2}(\cos t\sin t + t) = \frac{1}{2}\left(\frac{\operatorname{tg} t}{1+\operatorname{tg}^2 t} + t\right)$$

a proto také po zpětné substituci $t = \operatorname{arctg} x$

$$J_2 = \frac{1}{2}\left(\frac{x}{1+x^2} + \operatorname{arctg} x\right) + C.$$

Dohromady tak máme

$$\int x^2\,\mathrm{e}^{-3x}\,dx = -\tfrac{1}{3}x^2\,\mathrm{e}^{-3x} - \tfrac{2}{9}x\,\mathrm{e}^{-3x} - \tfrac{2}{27}\mathrm{e}^{-3x} + C = \\ = -\tfrac{1}{3}\mathrm{e}^{-3x}\left(x^2 + \tfrac{2}{3}x + \tfrac{2}{9}\right) + C\,.$$

Poznamenejme, že opakované použití per partes v rámci výpočtu jednoho integrálu je běžné (podobně jako při počítání limit l'Hospitalovým pravidlem).

Případ (c). Opět aplikujeme metodu per partes při vyjádření

$$\int \cos^2 x\,dx = \int \cos x\cdot\cos x\,dx = \\ = \left|\begin{array}{l|l} F(x)=\cos x & F'(x)=-\sin x \\ G'(x)=\cos x & G(x)=\sin x \end{array}\right| = \\ = \cos x\cdot\sin x + \int \sin^2 x\,dx = \cos x\cdot\sin x + \int 1-\cos^2 x\,dx = \\ = \cos x\cdot\sin x + \int 1\,dx - \int \cos^2 x\,dx = \cos x\cdot\sin x + x - \int \cos^2 x\,dx\,.$$

Přestože návrat k zadanému integrálu může vyvolat u čtenáře pochyby, ze vztahu

$$\int \cos^2 x\,dx = \cos x\cdot\sin x + x - \int \cos^2 x\,dx$$

je možné vyvodit

$$2\int \cos^2 x\,dx = \cos x\cdot\sin x + x + C,$$

tj.

$$\int \cos^2 x\,dx = \frac{1}{2}\,(x + \sin x\cdot\cos x) + C. \tag{6.8}$$

Stačí si vzpomenout, že klademe $C/2 = C$ a že neurčitý integrál (jako nekonečnou množinou) lze reprezentovat jednou konkrétní funkcí a jejími posunutími.

Vyzdvihněme, že většinou vhodné úpravy či substituce vedou k výsledku rychleji než metoda per partes. Např. pomocí identity

$$\cos^2 x = \tfrac{1}{2}\,(1+\cos 2x)\,, \qquad x\in\mathbb{R}$$

jednodušeji dostaneme

$$\int \cos^2 x\,dx = \int \tfrac{1}{2}\,dx + \int \tfrac{1}{2}\cos 2x\,dx = \tfrac{x}{2} + \tfrac{\sin 2x}{4} + C = \\ = \tfrac{x}{2} + \tfrac{2\sin x\cos x}{4} + C = \tfrac{1}{2}\,(x+\sin x\cdot\cos x) + C\,. \qquad \square$$

**6.47.** Kombinací metody per partes a substituční metody určete

(a) $\int x^3\,\mathrm{e}^{-x^2}\,dx,\ x\in\mathbb{R}$;

(b) $\int x\arcsin x^2\,dx,\ x\in(-1,1)$.

**Řešení.** Případ (a). Substituční metoda vede na integrál

$$\int x^3\,\mathrm{e}^{-x^2}\,dx = \left|\begin{array}{l} t=-x^2 \\ dt=-2x\,dx \end{array}\right| = \tfrac{1}{2}\int t\,\mathrm{e}^t\,dt,$$

který lze snadno vypočítat metodou per partes se ziskem

$$\tfrac{1}{2}\int t\,\mathrm{e}^t\,dt = \left|\begin{array}{l|l} F(t)=t & F'(t)=1 \\ G'(t)=\mathrm{e}^t & G(t)=\mathrm{e}^t \end{array}\right| = \tfrac{1}{2}t\,\mathrm{e}^t - \tfrac{1}{2}\int \mathrm{e}^t\,dt = \\ = \tfrac{1}{2}t\,\mathrm{e}^t - \tfrac{1}{2}\,\mathrm{e}^t + C = -\tfrac{1}{2}\,\mathrm{e}^{-x^2}\left(x^2+1\right) + C.$$

Při počítání určitých integrálů je možné celou rekurenci rovnou počítat po vyčíslení v zadaných mezích. Tak například je okamžitě vidět, že při integraci přes interval $[0,2\pi]$ mají naše integrály hodnoty:

$$I_0 = \int_0^{2\pi} dx = [x]_0^{2\pi} = 2\pi$$

$$I_1 = \int_0^{2\pi} \cos x\,dx = [\sin x]_0^{2\pi} = 0$$

$$I_m = \int_0^{2\pi} \cos^m x\,dx = \begin{cases} 0 & \text{pro sudá } m \\ \frac{m-1}{m} I_{m-2} & \text{pro lichá } m \end{cases}.$$

Pro sudé $m = 2n$ tedy dostáváme přímo výsledek

$$\int_0^{2\pi} \cos^{2n} x\,dx = \frac{(2n-1)(2n-3)\ldots 3\cdot 1}{2n(2n-2)\ldots 2}2\pi,$$

zatímco u lichých $m$ je to vždy nula (jak bylo možné přímo uhádnout z grafu funkce $\cos x$).

**6.23. Integrace racionálních funkcí lomených.** U racionálních



funkcí lomených si můžeme při integraci pomoci několika zjednodušeními. Zejména v případě, že je stupeň polynomu $f$ v čitateli větší nebo roven stupni polynomu $g$ ve jmenovateli, je rozumné hned z kraje dělením se zbytkem, viz odstavec 5.2, převést integraci na součet dvou integrálů. První pak bude integrací polynomu a druhý integrací výrazu $f/g$ se stupněm $g$ ostře větším, než je stupeň $f$ (takovým funkcím říkáme *ryze racionální lomené*).

Toho skutečně dosáhneme prostým vydělením polynomu:

$$f = q\cdot g + h, \qquad \frac{f}{g} = q + \frac{h}{g}.$$

Můžeme tedy zrovna předpokládat, že stupeň $g$ je ostře větší než stupeň $f$. Další postup si ukažme na jednoduchém příkladě. Zkusme si rozebrat, jak se dostaneme k výsledku

$$\frac{f(x)}{g(x)} = \frac{4x+2}{x^2+3x+2} = \frac{-2}{x+1} + \frac{6}{x+2},$$

který již umíme integrovat přímo:

$$\int \frac{4x+2}{x^2+3x+2}\,dx = -2\ln|x+1| + 6\ln|x+2| + C.$$

Především převedením součtu zlomků na společného jmenovatele tuto rovnost snadno ověříme. Pokud naopak víme, že lze náš výraz rozepsat ve tvaru

$$\frac{4x+2}{x^2+3x+2} = \frac{A}{x+1} + \frac{B}{x+2},$$

jde nám pouze o výpočet koeficientů $A$ a $B$. Můžeme pro ně získat rovnice pomocí roznásobení obou stran polynomem $x^2+3x+2$ ze jmenovatele a porovnáním koeficientů u jednotlivých mocnin $x$ ve výsledných polynomech napravo i nalevo:

$$4x+2 = A(x+2) + B(x+1) \implies 2A + B = 2,\ A + B = 4.$$

Odtud již přímo vychází náš rozklad. Říká se mu *rozklad na parciální zlomky*.

Tento elementární postup lze snadno zobecnit. Jde o čistě algebraickou úvahu opírající se o vlastnosti polynomů, ke kterým se budeme vracet v kapitole jedenácté.

Předpokládejme, že jmenovatel $g(x)$ a čitatel $f(x)$ nesdílí žádné reálné ani komplexní kořeny a že $g(x)$ má právě $n$ různých

Případ (b). Podobně obdržíme

$$\int x \arcsin x^2\,dx = \left|\begin{array}{c} t = x^2 \\ dt = 2x\,dx \end{array}\right| = \tfrac{1}{2}\int \arcsin t\,dt =$$
$$= \left|\begin{array}{ll} F(t) = \arcsin t & F'(t) = \frac{1}{\sqrt{1-t^2}} \\ G'(t) = 1 & G(t) = t \end{array}\right| = \tfrac{1}{2}t\arcsin t - \tfrac{1}{2}\int \tfrac{t}{\sqrt{1-t^2}}\,dt =$$
$$= \left|\begin{array}{c} u = 1-t^2 \\ du = -2t\,dt \end{array}\right| = \tfrac{1}{2}t\arcsin t + \tfrac{1}{4}\int \tfrac{du}{\sqrt{u}} = \tfrac{1}{2}t\arcsin t + \tfrac{1}{2}\sqrt{u} + C =$$
$$= \tfrac{1}{2}t\arcsin t + \tfrac{1}{2}\sqrt{1-t^2} + C = \tfrac{1}{2}x^2\arcsin x^2 + \tfrac{1}{2}\sqrt{1-x^4} + C. \quad \square$$

**6.48.** Dvěma různými způsoby vypočítejte integrál

$$\int \sqrt{1-x^2}\,dx, \qquad x \in (-1,1).$$

**Řešení.** Metoda per partes dává

$$\int \sqrt{1-x^2}\,dx = \left|\begin{array}{ll} F(x) = \sqrt{1-x^2} & F'(x) = \frac{-x}{\sqrt{1-x^2}} \\ G'(x) = 1 & G(x) = x \end{array}\right| =$$
$$= x\sqrt{1-x^2} + \int \tfrac{x^2}{\sqrt{1-x^2}}\,dx = x\sqrt{1-x^2} - \int \tfrac{1-x^2-1}{\sqrt{1-x^2}}\,dx =$$
$$= x\sqrt{1-x^2} - \int \sqrt{1-x^2}\,dx + \int \tfrac{1}{\sqrt{1-x^2}}\,dx =$$
$$= x\sqrt{1-x^2} - \int \sqrt{1-x^2}\,dx + \arcsin x,$$

odkud plyne

$$2\int \sqrt{1-x^2}\,dx = x\sqrt{1-x^2} + \arcsin x + C,$$

tj.

$$\int \sqrt{1-x^2}\,dx = \tfrac{1}{2}\left(x\sqrt{1-x^2} + \arcsin x\right) + C.$$

Substituční metodou pak s pomocí (‖6.8‖) dostáváme

$$\int \sqrt{1-x^2}\,dx = \left|\begin{array}{c} x = \sin y \\ dx = \cos y\,dy \end{array}\right| = \int \sqrt{1-\sin^2 y}\cdot\cos y\,dy =$$
$$= \int \cos^2 y\,dy = \tfrac{1}{2}(y + \sin y\cdot\cos y) + C =$$
$$= \tfrac{1}{2}\left(\sin y\cdot\sqrt{1-\sin^2 y} + y\right) + C = \tfrac{1}{2}\left(x\sqrt{1-x^2} + \arcsin x\right) + C,$$

kde $y \in (-\pi/2, \pi/2)$ pro $x \in (-1,1)$, a mj. tak je

$$0 < \cos y = |\cos y| = \sqrt{\cos^2 y} = \sqrt{1-\sin^2 y}\,. \quad \square$$

**6.49.** Stanovte

$$\int \mathrm{e}^{\sqrt{x}}\,dx, \qquad x > 0.$$

**Řešení.** Touto úlohou lze ilustrovat možnosti kombinování substituční metody a metody per partes (v rámci jednoho příkladu). Nejprve použijeme substituci $y = \sqrt{x}$, abychom odstranili odmocninu z argumentu exponenciální funkce. Tím přejdeme k integrálu

$$\int \mathrm{e}^{\sqrt{x}}\,dx = \left|\begin{array}{c} y^2 = x \\ 2y\,dy = dx \end{array}\right| = 2\int y\,\mathrm{e}^y\,dy.$$

Nyní pomocí per partes určíme

$$\int y\,\mathrm{e}^y\,dy = \left|\begin{array}{ll} F(y) = y & F'(y) = 1 \\ G'(y) = \mathrm{e}^y & G(y) = \mathrm{e}^y \end{array}\right| = y\,\mathrm{e}^y - \int \mathrm{e}^y\,dy =$$
$$= y\,\mathrm{e}^y - \mathrm{e}^y + C.$$

Celkem tedy je

$$\int \mathrm{e}^{\sqrt{x}}\,dx = 2y\,\mathrm{e}^y - 2\,\mathrm{e}^y + C = 2\,\mathrm{e}^{\sqrt{x}}\left(\sqrt{x} - 1\right) + C\,. \quad \square$$

reálných kořenů $a_1, \ldots, a_n$. Pak jsou body $a_1, \ldots a_n$ právě všechny body nespojitosti funkce $f(x)/g(x)$.

Pro zjednodušení úvahy nejprve pišme $g(x)$ jako součin

$$g(x) = p(x)q(x)$$

dvou nesoudělných polynomů. Díky Bezoutově identitě (viz 11.21 na str. 664), která je důsledkem obyčejného dělení polynomů se zbytkem, existují polynomy $a(x)$ a $b(x)$ se stupni ostře menšími než je stupeň $g$ takové, že

$$a(x)p(x) + b(x)q(x) = 1.$$

Vynásobením této rovnosti podílem $f(x)/g(x)$ dostáváme

$$\frac{f(x)}{g(x)} = \frac{a(x)}{q(x)}f(x) + \frac{b(x)}{p(x)}f(x).$$

Předpokládejme nyní, že náš polynom $g(x)$ nemá jiné než reálné kořeny, má tedy jednoznačný rozklad na faktory $(x-a_i)^{n_i}$, kde $n_i$ jsou násobnosti kořenů $a_i$, $i = 1, \ldots, k$. Postupným použitím předchozího postupu s nesoudělnými polynomy $p(x)$ a $q(x)$ dostaneme vyjádření $f(x)/g(x)$ pomocí součtu zlomků ve tvaru

$$\frac{r_1(x)}{(x-a_1)^{n_1}} + \cdots + \frac{r_k(x)}{(x-a_k)^{m_j}},$$

kde stupně polynomů $r_i(x)$ jsou ostře menší než stupně v jmenovatelích. Každý z nich ale jde velmi snadno rozepsat jako součet

$$\frac{r(x)}{(x-a)^n} = \frac{A_1}{x-a} + \frac{A_2}{(x-a)^2} + \cdots + \frac{A_n}{(x-a)^n},$$

když začneme od nejvyšších mocnin v polynomu $r(x)$ a postupně počítáme $A_1$, $A_2, \ldots$ vhodným doplňováním a odebíráním sčítanců v čitateli. Např.

$$\frac{5x-16}{(x-2)^2} = 5\frac{x-2}{(x-2)^2} - 6\frac{1}{(x-2)^2} = \frac{5}{x-2} + \frac{6}{(x-2)^2}.$$

Zbývá ošetřit ještě případ, kdy reálných kořenů není dostatek. Vždycky ale existuje rozklad $g(x)$ na lineární faktory s případně komplexními kořeny. Opakování předchozí úvahy pro komplexní polynomy nám dá tentýž výsledek. Pokud ale předem víme, že koeficienty polynomů jsou reálné, budou komplexní kořeny v našich výrazech vystupovat vždy po dvojicích komplexně sdružených kořenů. Můžeme proto rovnou pracovat s kvadratickými faktory ve tvaru součtu čtverců $(x-a)^2 + b^2$ a jejich mocnin. Naše předchozí úvaha opět dobře funguje a zaručuje, že bude možné hledat příslušné sčítance ve tvaru

$$\frac{Bx + C}{((x-a)^2 + b^2)^n}.$$

Obdobně jako v případě reálných kořenů se tedy i v případě mocniny $((x-a)^2 + b^2)^n$ takového kvadratického (nerozložitelného) faktoru vždy podaří najít odpovídající rozklad na parciální zlomky tvaru

$$\frac{A_1x + B_1}{(x-a)^2 + b^2} + \cdots + \frac{A_nx + B_n}{((x-a)^2 + b^2)^n}.$$

Konkrétní výsledky lze také snadno ozkoušet v Maplu pomocí volání procedury „convert(h, parfrac, x)“, které rozloží výraz $h$ racionálně závislý na proměnné $x$ na parciální zlomky.

Všechny výše uvedené parciální zlomky už umíme integrovat. Připomeňme, že ty poslední zmíněné vedou mimo jiné na integrály diskutované v Příkladě 6.22.

**6.50.** Dokažte, že

$$\frac{1}{2}\sin^4 x = -\frac{1}{4}\cos(2x) + \frac{1}{16}\cos(4x) + \frac{3}{16}.$$

**Řešení.** Snadnější, než porovnávat dané výrazy přímo, je ukázat, že funkce na pravé a levé straně rovnosti mají shodné derivace. Je totiž

$$L' = 2\cos x \sin^3 x = \sin(2x)\sin^2 x,$$
$$P' = \tfrac{1}{2}\sin(2x) - \tfrac{1}{4}\sin(4x) = \sin 2x\,(\tfrac{1}{2} - \tfrac{1}{2}\cos(2x)) =$$
$$= \sin(2x)\sin^2 x.$$

Levá a pravá strana se tedy liší o konstantu. Tuto konstantu určíme porovnáním funkčních hodnot v jednom bodě, například bodě 0. Hodnota obou funkcí je v nule nulová, jsou si tedy rovny. □

### C. Integrace racionálních lomených funkcí

**6.51.** Spočítejte

$$\int \frac{x}{(x-1)^2(x^2+2x+2)}\,dx, \qquad x \neq 1.$$

**Řešení.** Protože je stupeň polynomu v čitateli nižší než ve jmenovateli, tyto polynomy nemají společný kořen a je zadáno vyjádření jmenovatele ve tvaru součinu kořenových činitelů, známe tvar rozkladu integrované funkce na parciální zlomky

$$\frac{x}{(x-1)^2(x^2+2x+2)} = \frac{A}{x-1} + \frac{B}{(x-1)^2} + \frac{Cx+D}{x^2+2x+2}$$

pro $A, B, C, D \in \mathbb{R}$. Pokud tuto rovnici vynásobíme jmenovatelem levé strany, dostaneme identitu

$$x =$$
$$= A\,(x-1)\left(x^2+2x+2\right) + B\left(x^2+2x+2\right) + (Cx+D)\,(x-1)^2,$$

která má platit pro všechna $x \in \mathbb{R} \setminus \{1\}$. Na obou jejích stranách jsou ale polynomy, a tak rovnost musí nastat rovněž pro $x = 1$. Dosazením této hodnoty ihned obdržíme, že $1 = B(1+2+2)$, tj. $B = 1/5$.

Mohli bychom volit další reálná (příp. komplexní) čísla a dosazovat je do uvedené rovnice. Nelze však již očekávat, že bychom tím přímo určili další z neznámých (pokud nedosadíme kořen jmenovatele). Raději proto budeme porovnávat koeficienty u stejných mocnin polynomů

$$x - \tfrac{1}{5}\left(x^2+2x+2\right) = -\tfrac{1}{5}x^2 + \tfrac{3}{5}x - \tfrac{2}{5},$$
$$A\,(x-1)\left(x^2+2x+2\right) + (Cx+D)\,(x-1)^2 =$$
$$= (A+C)\,x^3 + (A-2C+D)\,x^2 + (C-2D)\,x - 2A + D,$$

čímž získáme systém rovnic

$$\begin{aligned} 0 &= A + C, \\ -1/5 &= A - 2C + D, \\ 3/5 &= C - 2D, \\ -2/5 &= -2A + D. \end{aligned}$$

Celkově můžeme shrnout, že racionální funkce $f(x)/g(x)$ lze poměrně snadno integrovat, pokud se podaří najít příslušný rozklad polynomu ve jmenovateli $g(x)$. Při výpočtu Newtonových integrálů jsou ale problematické body nespojitosti racionálních funkcí lomených, v jejichž okolí jsou tyto funkce neohraničené. Tomuto problému se budeme obecně ještě věnovat později (viz odstavec 6.30 níže).

**6.24. Riemannův integrál.** Myšlenku počítat integrál jako vyjádření plochy vymezené grafem funkce a osou $x$ je třeba zpřesnit. To nyní učiníme a vzápětí dokážeme, že pro všechny spojité funkce tato definice dává stejné výsledky jako Newtonův integrál.

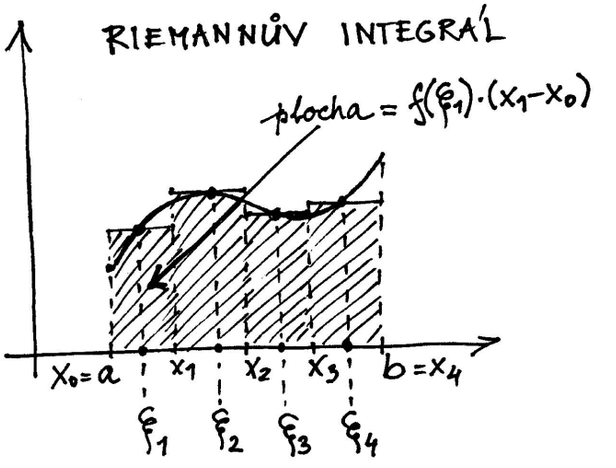


Uvažme reálnou funkci $f$ definovanou na intervalu $[a, b]$ a zvolme dělení tohoto intervalu spolu s výběrem reprezentantů $\xi_i$ jednotlivých částí, tj. $a = x_0 < x_1 < \cdots < x_n = b$ a zároveň $\xi_i \in [x_{i-1}, x_i]$, $i = 1, \ldots, n$. *Normou dělení* nazýváme číslo $\delta = \min_i\{x_i - x_{i-1}\}$. *Riemannův součet* odpovídající zvolenému dělení s reprezentanty

$$\Xi = (x_0, \ldots, x_n; \xi_1, \ldots, \xi_n)$$

definujeme jako

$$S_\Xi = \sum_{i=1}^{n} f(\xi_i)\cdot(x_i - x_{i-1}).$$




Řekneme, že *Riemannův integrál* funkce $f$ na intervalu $[a, b]$ existuje, jestliže pro každou posloupnost dělení s reprezentanty $(\Xi_k)_{k=0}^{\infty}$ s normami dělení $\delta_k$ jdoucími k nule existuje limita

$$\lim_{k\to\infty} S_{\Xi_k} = S\,,$$

jejíž hodnota navíc nezávisí na volbě posloupnosti dělení a jejich reprezentantů. Píšeme v takovém případě

$$S = \int_a^b f(x)dx.$$

Tato definice nevypadá příliš prakticky, nicméně nám dovolí snadno zformulovat a dokázat řadu jednoduchých vlastností Riemannova integrálu:

**Věta.** *(1) Je-li $f$ omezená reálná funkce definovaná na intervalu $[a, b]$ a $c \in [a, b]$ je nějaký vnitřní bod tohoto intervalu, potom*

Podotkněme, že tato soustava musí mít právě jedno řešení (které je jednoznačně určeno libovolnými třemi z uvedených rovnic). Hledané řešení potom je

$$A = \tfrac{1}{25}, \qquad C = -\tfrac{1}{25}, \qquad D = -\tfrac{8}{25}.$$

Platí tak

$$\begin{aligned}\int \tfrac{x}{(x-1)^2(x^2+2x+2)}\,dx &= \int \tfrac{dx}{25(x-1)} + \int \tfrac{dx}{5(x-1)^2} - \int \tfrac{x+8}{25(x^2+2x+2)}\,dx = \\ &= \tfrac{1}{25}\ln|x-1| - \tfrac{1}{5(x-1)} - \tfrac{1}{50}\ln\left(x^2+2x+2\right) - \\ &\quad - \tfrac{7}{25}\operatorname{arctg}(x+1) + C,\end{aligned}$$

kde jsme využili

$$\int \tfrac{x+8}{x^2+2x+2}\,dx = \int \tfrac{\frac{1}{2}(2x+2)}{x^2+2x+2} + \tfrac{7}{x^2+2x+2}\,dx = \tfrac{1}{2}\int \tfrac{2x+2}{x^2+2x+2}\,dx +$$
$$+ 7\int \tfrac{1}{(x+1)^2+1}\,dx = \tfrac{1}{2}\ln\left(x^2+2x+2\right) + 7\operatorname{arctg}(x+1) + C. \qquad \square$$

**6.52.** Integrujte

(a) $\int \frac{6}{x-2}\,dx$, $x \neq 2$;
(b) $\int \frac{6}{(x+4)^3}\,dx$, $x \neq -4$;
(c) $\int \frac{3x+7}{x^2-4x+15}\,dx$, $x \in \mathbb{R}$;
(d) $\int \frac{30x-77}{(x^2-6x+13)^2}\,dx$, $x \in \mathbb{R}$.

**Řešení.** Případy (a), (b). Platí

$$\int \tfrac{6}{x-2}\,dx = \left|\begin{matrix} y = x-2 \\ dy = dx \end{matrix}\right| = \int \tfrac{6}{y}\,dy = 6\ln|y| + C = 6\ln|x-2| + C$$

a podobně

$$\int \tfrac{6}{(x+4)^3}\,dx = \left|\begin{matrix} y = x+4 \\ dy = dx \end{matrix}\right| = \int \tfrac{6}{y^3}\,dy = \tfrac{6}{-2y^2} + C = -\tfrac{3}{(x+4)^2} + C.$$

Vidíme, že integrování typů parciálních zlomků, které odpovídají reálným kořenům jmenovatele racionální lomené funkce, je velmi snadné. Navíc zcela obecně lze obdržet

$$\begin{aligned}\int \tfrac{A}{x-x_0}\,dx &= \left|\begin{matrix} y = x-x_0 \\ dy = dx \end{matrix}\right| = \int \tfrac{A}{y}\,dy = \\ &= A\ln|y| + C = A\ln|x-x_0| + C\end{aligned}$$

a

$$\begin{aligned}\int \tfrac{A}{(x-x_0)^n}\,dx &= \left|\begin{matrix} y = x-x_0 \\ dy = dx \end{matrix}\right| = \int \tfrac{A}{y^n}\,dy = \tfrac{A\,y^{-n+1}}{-n+1} + C = \\ &= \tfrac{A}{(1-n)(x-x_0)^{n-1}} + C\end{aligned}$$

pro každé $A, x_0 \in \mathbb{R}$, $n \geq 2$, $n \in \mathbb{N}$.

Případ (c). Nyní máme integrovat parciální zlomek odpovídající dvojici komplexně sdružených kořenů. Ve jmenovateli je tedy polynom stupně 2 a v čitateli stupně nejvýše 1. Pokud je stupně 1, zapíšeme parciální zlomek tak, abychom v čitateli měli násobek derivace jmenovatele a k tomu přičítali zlomek, v jehož čitateli je již pouze konstanta. Takto dostaneme

$$\begin{aligned}\int \tfrac{3x+7}{x^2-4x+15}\,dx &= \tfrac{3}{2}\int \tfrac{2x-4}{x^2-4x+15}\,dx + 13\int \tfrac{dx}{x^2-4x+15} = \\ &= \tfrac{3}{2}\ln\left(x^2-4x+15\right) + 13\int \tfrac{dx}{(x-2)^2+11} =\end{aligned}$$

*integrál $\int_a^b f(x)dx$ existuje tehdy a jen tehdy, když existují oba integrály $\int_a^c f(x)dx$ a $\int_c^b f(x)dx$. V takovém případě pak také platí*

$$\int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx.$$

*(2) Jsou-li $f$ a $g$ dvě reálné funkce definované na intervalu $[a,b]$ a jestliže existují integrály $\int_a^b f(x)dx$ a $\int_a^b g(x)dx$, pak existuje také integrál jejich součtu a platí*

$$\int_a^b (f(x)+g(x))dx = \int_a^b f(x)dx + \int_a^b g(x)dx.$$

*(3) Je-li $f$ reálná funkce definovaná na intervalu $[a,b]$, $C \in \mathbb{R}$ je konstanta a jestliže existuje integrál $\int_a^b f(x)dx$, pak existuje také integrál $\int_a^b C\cdot f(x)dx$ a platí*

$$\int_a^b C\cdot f(x)dx = C\cdot\int_a^b f(x)dx.$$

Důkaz. (1) Předpokládejme nejprve, že existuje integrál přes celý interval. Jistě se lze při jeho výpočtu omezit na limity Riemannových součtů, jejichž dělení mají bod $c$ mezi svými dělícími body. Každý takový součet dostaneme jako součet dvou dílčích Riemannových součtů. Pokud by tyto dílčí součty v limitě závisely na zvolených rozděleních a reprezentantech, pak by celkové součty nemohly být v limitě na volbách nezávislé (stačí ponechat jednu posloupnost dělení podintervalu stejnou a druhou měnit tak, aby se limita změnila).

Naopak, jestliže existují Riemannovy integrály na obou podintervalech, jsou libovolně přesně aproximovatelné Riemannovými součty a to navíc nezávisle na jejich volbě. Pokud do libovolné posloupnosti Riemannových součtů přes celý interval $[a,b]$ přidáme v jejich děleních jeden dělící bod $c$ navíc, změníme hodnotu celého součtu i částečných součtů přes intervaly patřící do $[a,c]$ a $[c,b]$ nejvýše o násobek normy dělení a možných rozdílů omezené funkce $f$ na celém $[a,b]$. To je číslo jdoucí libovolně blízko k nule při zmenšující se normě dělení. Proto nutně i částečné Riemannovy součty naší funkce nutně konvergují k limitám, jejichž součtem je Riemannův integrál přes $[a,b]$.

(2) V každém Riemannově součtu se součet funkcí projeví jako součet hodnot ve vybraných reprezentantech. Protože je násobení reálných čísel distributivní, vyplývá odtud právě dokazované tvrzení.

(3) Stejná úvaha jako v předchozím případě. $\square$

Následující výsledek je zcela zásadní pro pochopení vztahu mezi integrálem a derivací:

**6.25. Věta** (Základní věta integrálního počtu)**.** *Pro každou spojitou funkci $f$ na konečném intervalu $[a,b]$ existuje její Riemannův integrál $\int_a^b f(x)dx$. Navíc je funkce $F(t)$ zadaná na intervalu $[a,b]$ pomocí Riemannova integrálu*

$$F(x) = \int_a^x f(t)dt$$

*primitivní funkcí k $f$ na tomto intervalu.*

Celý důkaz tohoto významného tvrzení bude poněkud delší. V prvním kroku pro důkaz existence integrálu použijeme alternativní definici, ve které nahrazujeme výběr reprezentantů a příslušné hodnoty $f(\xi_i)$ pomocí suprem $M_i$ hodnot $f(x)$ v příslušném intervalu $[x_{i-1}, x_i]$, resp. pomocí infim $m_i$ funkce $f(x)$ tamtéž.

$$= \tfrac{3}{2}\ln\left(x^2-4x+15\right) + \tfrac{13}{11}\int \frac{dx}{\left(\frac{x-2}{\sqrt{11}}\right)^2+1} = \left|\begin{array}{l} y = \frac{x-2}{\sqrt{11}} \\ dy = \frac{dx}{\sqrt{11}} \end{array}\right| =$$
$$= \tfrac{3}{2}\ln\left(x^2-4x+15\right) + \tfrac{13}{\sqrt{11}}\int \frac{dy}{y^2+1} =$$
$$= \tfrac{3}{2}\ln\left(x^2-4x+15\right) + \tfrac{13}{\sqrt{11}}\operatorname{arctg} y + C =$$
$$= \tfrac{3}{2}\ln\left(x^2-4x+15\right) + \tfrac{13}{\sqrt{11}}\operatorname{arctg}\tfrac{x-2}{\sqrt{11}} + C.$$

Opět můžeme obecně vyjádřit

$$\int \frac{Ax+B}{(x-x_0)^2+a^2}\,dx = \tfrac{A}{2}\int \frac{2(x-x_0)}{(x-x_0)^2+a^2}\,dx + (B+A\,x_0)\int \frac{1}{(x-x_0)^2+a^2}\,dx$$

a spočítat

$$\int \frac{2(x-x_0)}{(x-x_0)^2+a^2}\,dx = \left|\begin{array}{l} y = (x-x_0)^2+a^2 \\ dy = 2\,(x-x_0)\,dx \end{array}\right| = \int \frac{dy}{y} =$$
$$= \ln|\,y\,| + C = \ln[(x-x_0)^2+a^2] + C,$$
$$\int \frac{1}{(x-x_0)^2+a^2}\,dx = \tfrac{1}{a^2}\int \frac{dx}{\left(\frac{x-x_0}{a}\right)^2+1} = \left|\begin{array}{l} z = \frac{x-x_0}{a} \\ dz = \frac{dx}{a} \end{array}\right| = \tfrac{1}{a}\int \frac{dz}{z^2+1} =$$
$$= \tfrac{1}{a}\operatorname{arctg} z + C = \tfrac{1}{a}\operatorname{arctg}\tfrac{x-x_0}{a} + C,$$

tj.

$$\int \frac{Ax+B}{(x-x_0)^2+a^2}\,dx = \tfrac{A}{2}\ln\left((x-x_0)^2+a^2\right) + \tfrac{B+A\,x_0}{a}\operatorname{arctg}\tfrac{x-x_0}{a} + C,$$

kde hodnoty $A, B, x_0 \in \mathbb{R}$, $a > 0$ jsou libovolné.

Případ (d). Zbývají parciální zlomky pro vícenásobné komplexní kořeny ve tvaru

$$\frac{Ax+B}{\left[(x-x_0)^2+a^2\right]^n}, \qquad A, B, x_0 \in \mathbb{R},\ a > 0, n \in \mathbb{N} \setminus \{1\},$$

které analogicky upravíme na

$$\tfrac{A}{2}\cdot\frac{2(x-x_0)}{\left[(x-x_0)^2+a^2\right]^n} + (B+A\,x_0)\cdot\frac{1}{\left[(x-x_0)^2+a^2\right]^n}.$$

Poté určíme

$$\int \frac{2(x-x_0)}{\left[(x-x_0)^2+a^2\right]^n}\,dx = \left|\begin{array}{l} y = (x-x_0)^2+a^2 \\ dy = 2\,(x-x_0)\,dx \end{array}\right| = \int \frac{dy}{y^n} =$$
$$= \frac{1}{(1-n)y^{n-1}} + C = \frac{1}{(1-n)\left[(x-x_0)^2+a^2\right]^{n-1}} + C$$

a

$$K_n(x_0,a) := \int \frac{1}{\left[(x-x_0)^2+a^2\right]^n}\,dx =$$
$$= \left|\begin{array}{ll} F(x) = \frac{1}{\left[(x-x_0)^2+a^2\right]^n} & F'(x) = \frac{-2n(x-x_0)}{\left[(x-x_0)^2+a^2\right]^{n+1}} \\ G'(x) = 1 & G(x) = x-x_0 \end{array}\right| =$$
$$= \frac{x-x_0}{\left[(x-x_0)^2+a^2\right]^n} + 2n\int \frac{(x-x_0)^2+a^2}{\left[(x-x_0)^2+a^2\right]^{n+1}} - \frac{a^2}{\left[(x-x_0)^2+a^2\right]^{n+1}}\,dx =$$
$$= \frac{x-x_0}{\left[(x-x_0)^2+a^2\right]^n} + 2n\left(K_n(x_0,a) - a^2\,K_{n+1}(x_0,a)\right),$$

odkud plyne

$$K_{n+1}(x_0,a) = \tfrac{1}{a^2}\left(\tfrac{2n-1}{2n}\,K_n(x_0,a) + \tfrac{1}{2n}\frac{x-x_0}{\left[(x-x_0)^2+a^2\right]^n}\right),$$

což zřejmě platí také pro $n = 1$. Poslední rekurentní formuli ještě doplňme o v případě (c) odvozený integrál

$$K_1(x_0,a) = \tfrac{1}{a}\operatorname{arctg}\tfrac{x-x_0}{a} + C.$$

V zadaném příkladu je

$$\int \frac{30x-77}{\left(x^2-6x+13\right)^2}\,dx = 15\int \frac{2x-6}{\left(x^2-6x+13\right)^2}\,dx + 13\int \frac{1}{\left(x^2-6x+13\right)^2}\,dx$$

a dále

Hovoříme o horních Riemannových součtech, resp. dolních Riemannových součtech (někdy je v literatuře tento postup označován jako *Darbouxův integrál*).

**6.26. Horní a dolní Riemannův integrál.** Protože je naše



funkce spojitá, je jistě i omezená na uzavřeném intervalu a proto jsou všechna výše uvažovaná suprema i infima konečná. Je tedy *horní Riemannův součet* příslušný dělení $\Xi = (x_0, \ldots, x_n)$ zadán výrazem

$$S_{\Xi,\sup} = \sum_{i=1}^{n}\Big(\sup_{x_{i-1}\le\xi\le x_i} f(\xi)\Big)\cdot(x_i - x_{i-1}) = \sum_{i=1}^{n} M_i(x_i - x_{i-1})$$

zatímco *dolní Riemannův součet* je

$$S_{\Xi,\inf} = \sum_{i=1}^{n}\Big(\inf_{x_{i-1}\le\xi\le x_i} f(\xi)\Big)\cdot(x_i - x_{i-1}) = \sum_{i=1}^{n} m_i(x_i - x_{i-1}).$$

Protože pro každé dělení $\Xi = (x_0, \ldots, x_n; \xi_1, \ldots, \xi_n)$ s reprezentanty platí odhady

$$S_{\Xi,\inf} \le S_{\Xi,\xi} \le S_{\Xi,\sup} \tag{6.3}$$

a infima i suprema lze libovolně přesně aproximovat skutečnými hodnotami, lze tušit, že bude Riemannův integrál existovat právě, když bude existovat pro libovolné posloupnosti dělení s normou jdoucí k nule limita horních i dolních součtů a tyto si budou rovny. Dokážeme, že tomu tak skutečně musí být pro všechny omezené funkce:

**Věta.** *Nechť je funkce $f$ omezená na uzavřeném intervalu $[a,b]$. Pak*

$$S_{\sup} = \inf_{\Xi} S_{\Xi,\sup}, \qquad S_{\inf} = \sup_{\Xi} S_{\Xi,\inf}$$

*jsou limity všech posloupností horních, resp. dolních, součtů s normou jdoucí k nule.*

*Riemannův integrál omezené funkce $f$ přes interval $[a,b]$ existuje, právě když $S_{\sup} = S_{\inf}$.*

Důkaz. Pokud zjemníme nějaké rozdělení $\Xi_1$ na $\Xi_2$ přidáním dalších bodů, zřejmě bude

$$S_{\Xi_1,\sup} \ge S_{\Xi_2,\sup}, \qquad S_{\Xi_1,\inf} \le S_{\Xi_2,\inf}.$$

Každá dvě dělení mají společné zjemnění, jsou tedy hodnoty

$$S_{\sup} = \inf_{\Xi} S_{\Xi,\sup}, \qquad S_{\inf} = \sup_{\Xi} S_{\Xi,\inf}$$

dobrými kandidáty na limity horních a dolních součtů. Skutečně, pokud existuje společná limita horních součtů $S$ nezávislá na zvolené posloupnosti dělení, musí to být právě $S_{\sup}$, a podobně pro dolní součty.

Naopak, uvažme nějaké pevně zvolené dělení $\Xi$ s $n$ vnitřními dělícími body intervalu $[a,b]$, a jiné dělení $\Xi_1$, jehož norma je hodně malé číslo $\delta$. Ve společném zjemnění $\Xi_2$ bude jen $n$ intervalů, které budou do součtu $S_{\Xi_2,\sup}$ přispívat případně menším příspěvkem než je tomu v $\Xi_1$. Protože je $f$ omezená funkce na $[a,b]$, bude každý z těchto příspěvků ohraničený univerzální konstantou krát norma dělení (tj. maximální velikost příslušného intervalu v dělení). Při zvolení dostatečně malého $\delta$ tedy nebude vzdálenost $S_{\Xi_1,\sup}$ od $S_{\sup}$ více než dvakrát vzdálenost $S_{\Xi,\sup}$ od $S_{\sup}$.

Jestliže nyní zvolíme libovolnou posloupnost $\Xi_k$ s horními součty, jejichž limitou je $S_{\sup}$, pak pro pevně zvolené $\varepsilon > 0$ najdeme vždy $N$ takové,že pro $k > N$ bude $S_{\Xi_k,\sup}$ k $S_{\sup}$ blíže než

$$\int \frac{2x-6}{(x^2-6x+13)^2}\,dx = \left|\begin{array}{l} y = x^2-6x+13 \\ dy = (2x-6)\,dx \end{array}\right| = \int \frac{dy}{y^2} = -\frac{1}{y} + C = $$
$$= -\frac{1}{x^2-6x+13} + C,$$
$$\int \frac{1}{(x^2-6x+13)^2}\,dx = \int \frac{dx}{\left[(x-3)^2+2^2\right]^2} =$$
$$= \frac{1}{2^2}\left(\frac{2-1}{2}\,K_1(3,2) + \frac{1}{2}\,\frac{x-3}{(x-3)^2+2^2}\right) =$$
$$= \frac{1}{4}\left(\frac{1}{4}\operatorname{arctg}\frac{x-3}{2} + C + \frac{1}{2}\,\frac{x-3}{x^2-6x+13}\right) =$$
$$= \frac{1}{16}\operatorname{arctg}\frac{x-3}{2} + \frac{1}{8}\,\frac{x-3}{x^2-6x+13} + C.$$

Celkem tak máme

$$\int \frac{30x-77}{(x^2-6x+13)^2}\,dx = -\frac{15}{x^2-6x+13} + \frac{13}{16}\operatorname{arctg}\frac{x-3}{2} + \frac{13}{8}\,\frac{x-3}{x^2-6x+13} + C =$$
$$= \frac{13}{16}\operatorname{arctg}\frac{x-3}{2} + \frac{13x-159}{8(x^2-6x+13)} + C\,. \qquad \square$$

**6.53.** Integrujte racionální lomené funkce

(a) $\int \frac{x^3+1}{x(x-1)^3}\,dx$, $x \neq 0$, $x \neq 1$;
(b) $\int \frac{x-4}{5x^2+6x+3}\,dx$, $x \in \mathbb{R}$;
(c) $\int \frac{1}{(x-4)(x-2)(x^2+2x+2)}\,dx$, $x \neq 2$, $x \neq 4$;
(d) $\int \frac{x}{x^4-x^3-x+1}\,dx$, $x \neq 1$;
(e) $\int \frac{2x+1}{(x^2+4x+13)^2}\,dx$, $x \in \mathbb{R}$;
(f) $\int \frac{5x^2-12}{x^4-12x^3+62x^2-156x+169}\,dx$, $x \in \mathbb{R}$.

**Řešení.** Všechny zadané integrály budeme počítat takovým způsobem, jakým lze postupovat při integrování racionálních lomených funkcí vždy. Nepoužijeme tedy žádnou specifickou úpravu či substituci. Dokonce rekurentní vzorec ‖6.52‖ pro $K_{n+1}(x_0, a)$, který jsme odvodili v obecné podobě, použijeme pouze pro $x_0 = 0$, $a = 1$ (a to také tehdy, když bude $n = 0$). Dříve uvedenými postupy tak získáváme

(a)

$$\int \frac{x^3+1}{x(x-1)^3}\,dx = 2\int \frac{dx}{x-1} + \int \frac{dx}{(x-1)^2} + 2\int \frac{dx}{(x-1)^3} - \int \frac{dx}{x} =$$
$$= 2\ln|x-1| - \frac{1}{x-1} - \frac{1}{(x-1)^2} - \ln|x| + C;$$

(b)

$$\int \frac{x-4}{5x^2+6x+3}\,dx = \frac{1}{10}\int \frac{10x+6}{5x^2+6x+3}\,dx - \frac{23}{5}\int \frac{dx}{5x^2+6x+3} =$$
$$= \frac{1}{10}\ln\left(5x^2+6x+3\right) - \frac{23}{25}\int \frac{dx}{\left(x+\frac{3}{5}\right)^2+\frac{6}{25}} =$$
$$= \frac{1}{10}\ln\left(5x^2+6x+3\right) - \frac{23}{6}\int \frac{dx}{\left(\frac{5x+3}{\sqrt{6}}\right)^2+1} =$$
$$= \left|\begin{array}{l} t = \frac{5x+3}{\sqrt{6}} \\ dt = \frac{5}{\sqrt{6}}\,dx \end{array}\right| =$$
$$= \frac{1}{10}\ln\left(5x^2+6x+3\right) - \frac{23\sqrt{6}}{30}\int \frac{dt}{t^2+1} =$$
$$= \frac{1}{10}\ln\left(5x^2+6x+3\right) - \frac{23\sqrt{6}}{30}\operatorname{arctg} t + C =$$
$$= \frac{1}{10}\ln\left(5x^2+6x+3\right) - \frac{23\sqrt{6}}{30}\operatorname{arctg}\frac{5x+3}{\sqrt{6}} + C;$$

(c)

$$\int \frac{dx}{(x-4)(x-2)(x^2+2x+2)} =$$
$$= \frac{1}{52}\int \frac{dx}{x-4} - \frac{1}{20}\int \frac{dx}{x-2} + \frac{1}{130}\int \frac{4x+11}{x^2+2x+2}\,dx = \frac{1}{52}\ln|x-4| -$$
$$- \frac{1}{20}\ln|x-2| + \frac{1}{130}\left(2\int \frac{2x+2}{x^2+2x+2}\,dx + 7\int \frac{dx}{x^2+2x+2}\right) =$$

o $\varepsilon$. Zároveň ale umíme podle předchozí úvahy najít $\delta$ tak, že pro všechna dělení s normou menší než $\delta$ budeme se součtem blíže než o $2\varepsilon$. Právě jsme proto ukázali, že pro libovolné číslo $\varepsilon > 0$ umíme najít takové $\delta > 0$, že pro všechna dělení s normou nejvýše $\delta$ bude $|S_{\sup} - S_{\Xi}| < \varepsilon$. To je přesně tvrzení, že číslo $S_{\sup}$ je limitou všech posloupností horních součtů s normami dělení jdoucími k nule. Úplně stejně se dokáže i tvrzení pro součty dolní.

Pokud Riemannův integrál neexistuje, existují posloupnosti dělení a reprezentantů s různými limitami Riemannových součtů. Pak ovšem z již dokázaného tvrzení plyne, že budou různé i limity horních součtů a dolních součtů. Naopak, předpokládejme, že $S_{\sup} = S_{\inf}$, pak ovšem i všechny Riemannovy součty posloupností dělení musí mít tutéž limitu díky nerovnostem (6.3). $\square$

**6.27. Stejnoměrná spojitost.** Prozatím jsme ze spojitosti naší funkce $f$ využili pouze to, že každá taková funkce je na konečném uzavřeném intervalu omezená. Zbývá nám ale ukázat, že pro spojité funkce je $S_{\sup} = S_{\inf}$.



Z definice spojitosti víme, že pro každý pevně zvolený bod $x \in [a,b]$ a každé okolí $\mathcal{O}_\varepsilon(f(x))$ existuje okolí $\mathcal{O}_\delta(x)$ takové, že $f(\mathcal{O}_\delta(x)) \subset \mathcal{O}_\varepsilon(f(x))$. Toto tvrzení lze přepsat takto: jsou-li $y, z \in \mathcal{O}_\delta(x)$, tzn. mimo jiné platí

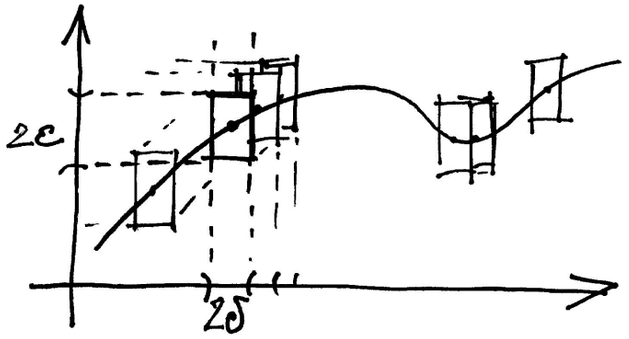
$$|y - z| < 2\delta,$$

je také $f(y), f(z) \in \mathcal{O}_\varepsilon(f(x))$, tzn. mimo jiné platí

$$|f(y) - f(z)| < 2\varepsilon.$$

Budeme potřebovat globální variantu takové vlastnosti, říkáme jí *stejnoměrná spojitost* funkce $f$:

STEJNOMĚRNÁ SPOJITOST




**Věta.** *Nechť je $f$ spojitá funkce na uzavřeném konečném intervalu $[a,b]$. Pak je na $[a,b]$ stejnoměrně spojitá, tj. pro každé číslo $\varepsilon > 0$ existuje takové číslo $\delta > 0$, že pro všechny $z, y \in [a,b]$ splňující $|y - z| < \delta$ platí $|f(y) - f(z)| < \varepsilon$.*

Důkaz. Protože je každý konečný uzavřený interval kompaktní, umíme jej celý pokrýt konečně mnoha okolími $\mathcal{O}_{\delta(x)}(x)$ zmiňovanými v souvislosti se spojitostí výše, přičemž jejich poloměr $\delta(x)$ závisí na středu $x$, zatímco čísla $\varepsilon$ budeme uvažovat pořád stejná. Zvolíme konečně za $\delta$ minimum ze všech (konečně mnoha) $\delta(x)$. Naše spojitá funkce $f$ tedy má požadovanou vlastnost (pouze zaměňujeme čísla $\varepsilon$ a $\delta$ za jejich dvojnásobky). $\square$

$$= \tfrac{1}{260}\ln\left|\tfrac{(x-4)^5}{(x-2)^{13}}\right| + \tfrac{2}{130}\ln\left(x^2+2x+2\right) + \tfrac{7}{130}\int \tfrac{dx}{(x+1)^2+1} =$$
$$= \left|\begin{array}{l} t = x+1 \\ dt = dx \end{array}\right| = \tfrac{1}{260}\ln\left|\tfrac{(x-4)^5\left(x^2+2x+2\right)^4}{(x-2)^{13}}\right| + \tfrac{7}{130}\int \tfrac{dt}{t^2+1} =$$
$$= \tfrac{1}{260}\ln\left|\tfrac{(x-4)^5\left(x^2+2x+2\right)^4}{(x-2)^{13}}\right| + \tfrac{7}{130}\operatorname{arctg} t + C =$$
$$= \tfrac{1}{260}\left[\ln\left|\tfrac{(x-4)^5\left(x^2+2x+2\right)^4}{(x-2)^{13}}\right| + 14\operatorname{arctg}(x+1)\right] + C;$$

(d)

$$\int \tfrac{x}{x^4-x^3-x+1}\,dx = \tfrac{1}{3}\int \tfrac{dx}{(x-1)^2} - \tfrac{1}{3}\int \tfrac{dx}{x^2+x+1} =$$
$$= -\tfrac{1}{3(x-1)} - \tfrac{1}{3}\int \tfrac{dx}{\left(x+\frac{1}{2}\right)^2+\frac{3}{4}} = -\tfrac{1}{3(x-1)} - \tfrac{4}{9}\int \tfrac{dx}{\left(\frac{2x+1}{\sqrt{3}}\right)^2+1} =$$
$$= \left|\begin{array}{l} t = \frac{2x+1}{\sqrt{3}} \\ dt = \frac{2}{\sqrt{3}}\,dx \end{array}\right| = -\tfrac{1}{3(x-1)} - \tfrac{2}{3\sqrt{3}}\int \tfrac{dt}{t^2+1} =$$
$$= -\tfrac{1}{3(x-1)} - \tfrac{2}{3\sqrt{3}}\operatorname{arctg} t + C = -\tfrac{1}{3(x-1)} - \tfrac{2}{3\sqrt{3}}\operatorname{arctg}\tfrac{2x+1}{\sqrt{3}} + C;$$

(e)

$$\int \tfrac{2x+1}{(x^2+4x+13)^2}\,dx = \int \tfrac{2x+4}{(x^2+4x+13)^2}\,dx - 3\int \tfrac{dx}{(x^2+4x+13)^2} =$$
$$= \left|\begin{array}{l} t = x^2+4x+13 \\ dt = (2x+4)\,dx \end{array}\right| = \int \tfrac{dt}{t^2} - 3\int \tfrac{dx}{\left[(x+2)^2+9\right]^2} =$$
$$= -\tfrac{1}{t} - \tfrac{1}{27}\int \tfrac{dx}{\left[\left(\frac{x+2}{3}\right)^2+1\right]^2} = \left|\begin{array}{l} u = \frac{x+2}{3} \\ du = \frac{1}{3}\,dx \end{array}\right| = -\tfrac{1}{x^2+4x+13} -$$
$$-\tfrac{1}{9}\int \tfrac{du}{(u^2+1)^2} = -\tfrac{1}{x^2+4x+13} - \tfrac{1}{9}\left(\tfrac{1}{2}\operatorname{arctg} u + \tfrac{1}{2}\tfrac{u}{u^2+1}\right) + C =$$
$$= -\tfrac{1}{x^2+4x+13} - \tfrac{1}{18}\operatorname{arctg}\tfrac{x+2}{3} - \tfrac{1}{18}\tfrac{\frac{x+2}{3}}{\left(\frac{x+2}{3}\right)^2+1} + C =$$
$$= -\tfrac{1}{18}\operatorname{arctg}\tfrac{x+2}{3} - \tfrac{1}{6}\tfrac{x+8}{x^2+4x+13} + C;$$

(f)

$$\int \tfrac{5x^2-12}{x^4-12x^3+62x^2-156x+169}\,dx = \int \tfrac{5x^2-12}{(x^2-6x+13)^2}\,dx =$$
$$= 5\int \tfrac{dx}{x^2-6x+13} + \int \tfrac{30x-77}{(x^2-6x+13)^2}\,dx =$$
$$= 5\int \tfrac{dx}{(x-3)^2+4} + 15\int \tfrac{2x-6}{(x^2-6x+13)^2}\,dx + 13\int \tfrac{dx}{(x^2-6x+13)^2} =$$
$$= \tfrac{5}{4}\int \tfrac{dx}{\left(\frac{x-3}{2}\right)^2+1} + 15\int \tfrac{2x-6}{(x^2-6x+13)^2}\,dx + 13\int \tfrac{dx}{\left[(x-3)^2+4\right]^2} =$$
$$= \left|\begin{array}{ll} t = \frac{x-3}{2} & u = x^2-6x+13 \\ dt = \frac{1}{2}dx & du = (2x-6)\,dx \end{array}\right| =$$
$$= \tfrac{5}{2}\int \tfrac{dt}{t^2+1} + 15\int \tfrac{du}{u^2} + \tfrac{13}{16}\int \tfrac{dx}{\left[\left(\frac{x-3}{2}\right)^2+1\right]^2} =$$
$$= \tfrac{5}{2}\operatorname{arctg} t - \tfrac{15}{u} + \tfrac{13}{8}\int \tfrac{dt}{\left[t^2+1\right]^2} =$$
$$= \tfrac{5}{2}\operatorname{arctg}\tfrac{x-3}{2} - \tfrac{15}{x^2-6x+13} + \tfrac{13}{8}\left(\tfrac{1}{2}\operatorname{arctg} t + \tfrac{1}{2}\tfrac{t}{t^2+1}\right) + C =$$
$$= \tfrac{5}{2}\operatorname{arctg}\tfrac{x-3}{2} - \tfrac{15}{x^2-6x+13} + \tfrac{13}{16}\operatorname{arctg}\tfrac{x-3}{2} + \tfrac{13}{16}\tfrac{\frac{x-3}{2}}{\left(\frac{x-3}{2}\right)^2+1} + C =$$
$$= \tfrac{5}{2}\operatorname{arctg}\tfrac{x-3}{2} + \tfrac{13}{16}\operatorname{arctg}\tfrac{x-3}{2} - \tfrac{15}{x^2-6x+13} + \tfrac{13}{8}\tfrac{x-3}{(x-3)^2+4} + C =$$
$$= \tfrac{53}{16}\operatorname{arctg}\tfrac{x-3}{2} + \tfrac{13x-159}{8(x^2-6x+13)} + C. \qquad \square$$

**6.54.** Určete

(a) $\int \tfrac{x^3+2x^2+x-1}{x^2-x+1}\,dx$, $x \in \mathbb{R}$;

(b) $\int \tfrac{x^8}{x^8-1}\,dx$, $x \neq \pm 1$.

**6.28. Dokončení důkazu Věty 6.25.** Nyní již snadno dokončíme



celý důkaz existence Riemannova integrálu. Zvolme si $\varepsilon$ a $\delta$ jako v předchozí větě o stejnoměrné spojitosti a uvažujme jakékoliv dělení $\Xi$ s $n$ intervaly a normou nejvýš $\delta$. Pak

$$\left|\sum_{i=1}^{n} \sup_{x_{i-1}\le\xi\le x_i} f(\xi)\cdot(x_i - x_{i-1}) - \sum_{i=1}^{n} \inf_{x_{i-1}\le\xi\le x_i} f(\xi)\cdot(x_i - x_{i-1})\right| \le$$
$$\le \sum_{i=1}^{n} \left|\sup_{x_{i-1}\le\xi\le x_i} f(\xi) - \inf_{x_{i-1}\le\xi\le x_i} f(\xi)\right|\cdot(x_i - x_{i-1}) \le$$
$$\le \varepsilon\cdot(b-a).$$

Vidíme tedy, že se zmenšující se normou dělení jsou k sobě horní a dolní součty libovolně blízké. Proto infima a suprema splývají. To jsme potřebovali ukázat.

Pro úplný důkaz základní věty integrálního počtu ještě zbývá ověřit tvrzení o existenci primitivní funkce. Víme již, že pro spojitou funkci $f$ na intervalu $[a,b]$ existuje pro každé $t \in [a,b]$ integrál $\int_a^t f(x)dx$. Zvolme, stejně jako v tvrzení o stejnoměrné spojitosti, k pevnému malému $\varepsilon > 0$ číslo $\delta > 0$ tak, aby

$$|f(x+\Delta x) - f(x)| < \varepsilon$$

pro všechna $0 \le \Delta x < \delta$ na celém intervalu $[a,b]$. Rozdíl derivace naší funkce $F(x)$ a integrované funkce $f(x)$ je vyjádřen pomocí limity výrazů

$$\frac{1}{\Delta x}\left(\int_a^{x+\Delta x} f(t)dt - \int_a^x f(t)dt\right) - f(x)$$

pro $\Delta x$ jdoucí k nule. Pokud však volíme $0 < \Delta x < \delta$, pak v absolutní hodnotě je tento výraz odhadnut

$$\left|\frac{1}{\Delta x}\left(\int_x^{x+\Delta x} f(t)dt\right) - f(x)\right| < \varepsilon,$$

protože ve výrazu nalevo můžeme libovolně přesně nahradit integrál jeho Riemannovým součtem a ve sčítancích $f(\xi_i)(x_i - x_{i-1})$ s $\xi_i \in [x, x+\Delta x]$ v jakémkoliv Riemannově součtu jsou $f(\xi)$ vzdáleny od $f(x)$ nejvýše o velikost $\varepsilon$. Proto nahrazením $f(x)$ za všechny $f(\xi_i)$ dostáváme nalevo nulový výraz a dopouštíme se chyby nejvýše $\varepsilon$.

To ovšem znamená, že existuje v bodě $x$ derivace funkce $F(x)$ zprava a je rovna $f(x)$. Stejně dokážeme výsledek pro derivaci zleva a celá věta 6.25 je dokázaná.

**6.29. Důležité poznámky.** (1) Věty 6.25 a 6.24 nám říkají, že integrál je lineární zobrazení

$$\int : C[a,b] \to \mathbb{R}$$

vektorového prostoru spojitých funkcí na intervalu $[a,b]$ do reálných čísel. Je to tedy lineární forma na prostoru $C[a,b]$.

(2) Dokázali jsme, že každá spojitá funkce je derivací nějaké funkce. Newtonův a Riemannův integrál tedy jako koncepty pro spojité funkce splývají. Riemannův integrál spojitých funkcí lze proto spočíst pomocí rozdílu hodnot $F(b) - F(a)$ primitivní funkce $F$.

(3) V prvním kroku důkazu věty 6.25 jsme dokázali důležité tvrzení, že pro omezenou funkci $f$ na intervalu $[a,b]$ vždy existují

**Řešení.** Případ (a). Nejdříve musíme provést dělení polynomů

$$\left(x^3+2x^2+x-1\right):\left(x^2-x+1\right)=x+3+\tfrac{3x-4}{x^2-x+1},$$

abychom uvažovali ryze lomenou racionální funkci (stupeň čitatele byl nižší než jmenovatele). Nyní už spočítáme

$$\int \tfrac{x^3+2x^2+x-1}{x^2-x+1}\,dx=\int x+3\,dx+\int \tfrac{3x-4}{x^2-x+1}\,dx=$$
$$=\tfrac{x^2}{2}+3x+\tfrac{3}{2}\int \tfrac{2x-1}{x^2-x+1}\,dx-\tfrac{5}{2}\int \frac{dx}{\left(x-\frac12\right)^2+\left(\frac{\sqrt3}{2}\right)^2}=$$
$$=\tfrac{x^2}{2}+3x+\tfrac{3}{2}\ln\left(x^2-x+1\right)-\tfrac{5}{\sqrt3}\operatorname{arctg}\tfrac{2x-1}{\sqrt3}+C.$$

Případ (b). Platí

$$\int \tfrac{x^8}{x^8-1}\,dx=\int 1\,dx+\tfrac18\int\tfrac{dx}{x-1}-\tfrac18\int\tfrac{dx}{x+1}-\tfrac14\int\tfrac{dx}{x^2+1}+$$
$$+\tfrac18\int\tfrac{\sqrt2x-2}{x^2-\sqrt2x+1}\,dx-\tfrac18\int\tfrac{\sqrt2x+2}{x^2+\sqrt2x+1}\,dx=$$
$$=x+\tfrac18\ln|x-1|-\tfrac18\ln|x+1|-\tfrac14\operatorname{arctg}x+\tfrac{\sqrt2}{16}\int\tfrac{2x-\sqrt2}{x^2-\sqrt2x+1}\,dx-$$
$$-\tfrac18\int\frac{dx}{\left(x-\frac{\sqrt2}{2}\right)^2+\left(\frac{\sqrt2}{2}\right)^2}-\tfrac{\sqrt2}{16}\int\tfrac{2x+\sqrt2}{x^2+\sqrt2x+1}\,dx-\tfrac18\int\frac{dx}{\left(x+\frac{\sqrt2}{2}\right)^2+\left(\frac{\sqrt2}{2}\right)^2}=$$
$$=x+\tfrac18\ln|x-1|-\tfrac18\ln|x+1|-\tfrac14\operatorname{arctg}x+$$
$$+\tfrac{\sqrt2}{16}\ln\left(x^2-\sqrt2x+1\right)-\tfrac{\sqrt2}{8}\operatorname{arctg}\left(\sqrt2x-1\right)-$$
$$-\tfrac{\sqrt2}{16}\ln\left(x^2+\sqrt2x+1\right)-\tfrac{\sqrt2}{8}\operatorname{arctg}\left(\sqrt2x+1\right)+C.\qquad\square$$

**6.55.** Integrujte

(a) $\int \frac{x}{1+x^4}\,dx$, $x\in\mathbb{R}$;

(b) $\int \frac{5\ln x}{x\ln^3 x+x\ln^2 x-2x}\,dx$, $x>0, x\neq \mathrm{e}$.

**Řešení.** Případ (a). Výhodou výše popsané metody integrování racionálních lomených funkcí je její univerzálnost (umíme díky ní najít primitivní funkce každé racionální lomené funkce). Někdy je však výhodnější použití substituční metody nebo per partes. Např. je

$$\int \tfrac{x}{1+x^4}\,dx=\left|\begin{array}{c} y=x^2\\ dy=2x\,dx\end{array}\right|=\int\tfrac{dy}{2(1+y^2)}=\tfrac12\int\tfrac{dy}{1+y^2}=$$
$$=\tfrac12\operatorname{arctg}y+C=\tfrac12\operatorname{arctg}x^2+C.$$

Případ (b). Pomocí substituce získáváme integrál racionální lomené funkce

$$\int\tfrac{5\ln x}{x\ln^3 x+x\ln^2 x-2x}=\int\tfrac{5\ln x}{\ln^3 x+\ln^2 x-2}\cdot\tfrac1x\,dx=\left|\begin{array}{c} y=\ln x\\ dy=\frac1x\,dx\end{array}\right|=$$
$$=\int\tfrac{5y}{y^3+y^2-2}\,dy=\int\tfrac{1}{y-1}+\tfrac{-y+2}{y^2+2y+2}\,dy=$$
$$=\int\tfrac{1}{y-1}\,dy-\tfrac12\int\tfrac{2y+2}{y^2+2y+2}\,dy+3\int\tfrac{1}{(y+1)^2+1^2}\,dy=$$
$$=\ln|y-1|-\tfrac12\ln\left(y^2+2y+2\right)+3\operatorname{arctg}(y+1)+C=$$
$$=\ln|\ln x-1|-\tfrac12\ln\left(\ln^2x+2\ln x+2\right)+3\operatorname{arctg}(\ln x+1)+C.\ \square$$

**6.56.** Určete

(a) $\int\frac{1}{\sqrt{x^3}+\sqrt[5]{x^7}}\,dx$, $x>0$;

(b) $\int\frac{x+1}{\sqrt[3]{3x+1}}\,dx$, $x\neq-\frac13$;

(c) $\int\frac1x\sqrt{\frac{x+1}{x-1}}\,dx$, $x\in\mathbb{R}\setminus[-1,1]$;

(d) $\int\frac{1}{(x+4)\sqrt{x^2+3x-4}}\,dx$, $x\in(-\infty,-4)\cup(1,+\infty)$;

(e) $\int\frac{1}{1+\sqrt{-x^2+x+2}}\,dx$, $x\in(-1,2)$;

limity horních součtů i dolních součtů. Říká se jim také *horní Riemannův integrál* a *dolní Riemannův integrál* a používá se pro ně často značení $\overline{\int_a^b} f(x)\,dx$ a $\underline{\int_a^b} f(x)\,dx$.

Takto lze pro omezené funkce ekvivalentně definovat i Riemannův integrál (jak jsme konečně v důkazu i činili).

(4) V dalším kroku v důkazu jsme odvodili důležitou vlastnost spojitých funkcí, které se říká *stejnoměrná spojitost* na uzavřeném intervalu $[a,b]$. Zjevně je každá stejnoměrně spojitá funkce také spojitá, naopak to ale na otevřených intervalech platit nemusí. Příkladem může sloužit třeba funkce $f(x)=\sin(1/x)$ na intervalu $(0,1)$.

(5) Uvažme funkci $f$ na intervalu $[a,b]$, která je pouze *po částech spojitá*. To znamená, že je spojitá ve všech bodech $c\in[a,b]$ kromě konečně mnoha *bodů nespojitosti* $c_i, a<c_i<b$, ve kterých ovšem má konečné jednostranné limity. Vzhledem k aditivnosti integrálu vůči intervalu přes který se integruje, viz 6.24(1), existuje podle poslední věty v takovém případě integrál

$$F(x)=\int_a^x f(t)dt$$

pro všechna $x\in[a,b]$ a derivace funkce $F(x)$ existuje ve všech bodech $x$, ve kterých je $f$ spojitá. Navíc se snadno ověří, že ve zbývajících bodech je funkce $F(x)$ spojitá, je to tedy spojitá funkce na celém intervalu $[a,b]$. Při výpočtu integrálu pomocí primitivních funkcí je zapotřebí volit její jednotlivé části tak, aby na sebe navazovaly. Pak bude i celý integrál vyčíslen jako rozdíl funkce $F(x)$ v krajních hodnotách.

(6) Lagrangeova věta o střední hodnotě diferencovatelné funkce má analogii, které se říká *integrální věta o střední hodnotě*. Uvažme funkci $f(x)$ spojitou na intervalu $[a,b]$ a její primitivní funkci $F(x)$. Věta o střední hodnotě říká, že existuje vnitřní bod $a<c<b$ takový, že

$$\int_a^b f(x)\,dx=F(b)-F(a)=F'(c)(b-a)=f(c)(b-a).$$

Toto tvrzení lze vcelku snadno odvodit přímo z definice Riemannova integrálu a pak jej je možné přímočaře využít v závěrečném kroku důkazu základní věty integrálního počtu.

**6.30. Nevlastní integrály.** Při diskusi integrace racionálních lomených funkcí jsme viděli, že bychom rádi pracovali také s určitými integrály přes intervaly, v nichž jsou i body, kde integrovaná funkce $f(x)$ má nevlastní (jednostranné) limity. V takovém případě není integrovaná funkce ani spojitá ani omezená a proto pro ni nemusí platit námi odvozené výsledky. Hovoříme o „nevlastním integrálu“.



Jednoduchým východiskem je diskutovat v takovém případě určité integrály na menších intervalech s hranicí blížící se problematickému bodu a zkoumat, zda existuje limitní hodnota takovýchto určitých integrálů. Pokud existuje, řekneme, že příslušný nevlastní integrál existuje a je roven této limitě. Uvedeme postup na jednoduchém příkladě:

$$I=\int_0^2\frac{dx}{\sqrt[4]{2-x}}$$

je nevlastní integrál, protože uvedená integrovaná funkce $f(x)=(2-x)^{-1/4}$ má v bodě $b=2$ limitu zleva rovnou $\infty$. V ostatních bodech je integrovaná funkce spojitá. Zajímáme se

(f) $\int \frac{1}{(x-1)\sqrt{x^2+x+1}}\,dx$, $x \neq 1$.

**Řešení.** V tomto příkladu budeme ilustrovat použití substituční metody při integrování výrazů s odmocninami.

Případ (a). Má-li počítaný integrál tvar

$$\int f\left(\sqrt[p(1)]{x},\ \sqrt[p(2)]{x},\ \ldots,\ \sqrt[p(j)]{x}\right)\,dx$$

pro jistá čísla $p(1), p(2), \ldots, p(j) \in \mathbb{N}$ a racionální lomenou funkci $f$ (více proměnných), doporučuje se substituce $t^n = x$, kde $n$ je (nejmenší) společný násobek čísel $p(1), \ldots, p(j)$. Touto substitucí lze totiž převést integrand (integrovanou funkci) na racionální lomenou funkci, kterou umíme integrovat vždy. Dostáváme

$$\int \frac{dx}{\sqrt{x^3}+\sqrt[5]{x^7}} = \int \frac{dx}{x\left(\sqrt{x}+\sqrt[5]{x^2}\right)} = \left|\begin{array}{c} t^{10} = x,\ \sqrt[10]{x} = t \\ 10t^9\,dt = dx \end{array}\right| = \int \frac{10t^9}{t^{10}\left(t^5+t^4\right)}\,dt =$$

$$= 10\int \frac{dt}{t^6+t^5} = 10\int \left(\tfrac{1}{t} - \tfrac{1}{t^2} + \tfrac{1}{t^3} - \tfrac{1}{t^4} + \tfrac{1}{t^5} - \tfrac{1}{t+1}\right)dt =$$
$$= 10\left[\ln t + \tfrac{1}{t} - \tfrac{1}{2t^2} + \tfrac{1}{3t^3} - \tfrac{1}{4t^4} - \ln(1+t)\right] + C =$$
$$= \ln\frac{x}{(1+\sqrt[10]{x})^{10}} + \frac{10}{\sqrt[10]{x}} - \frac{5}{\sqrt[5]{x}} + \frac{10}{3\sqrt[10]{x^3}} - \frac{5}{2\sqrt[5]{x^2}} + C.$$

Případ (b). Pro integrály

$$\int f\left(x,\ \sqrt[p(1)]{ax+b},\ \sqrt[p(2)]{ax+b},\ \ldots,\ \sqrt[p(j)]{ax+b}\right)\,dx,$$

kde opět $p(1), \ldots, p(j) \in \mathbb{N}$, $f$ je racionální lomený výraz a $a,\ b \in \mathbb{R}$, volíme substituci $t^n = ax + b$ při zachování významu $n$. Takto obdržíme

$$\int \frac{x+1}{\sqrt[3]{3x+1}}\,dx = \left|\begin{array}{c} t^3 = 3x+1 \\ dx = t^2\,dt \end{array}\right| = \int \frac{\frac{t^3-1}{3}+1}{t}\,t^2\,dt =$$
$$= \int \frac{t^3-1+3}{3}\,t\,dt = \frac{1}{3}\int t^4 + 2t\,dt =$$
$$= \frac{1}{3}\left(\frac{t^5}{5} + t^2\right) + C = \frac{t^2}{3}\left(\frac{t^3}{5} + 1\right) + C =$$
$$= \frac{\sqrt[3]{(3x+1)^2}}{3}\left(\frac{3x+1}{5} + 1\right) + C = \sqrt[3]{(3x+1)^2}\,\frac{x+2}{5} + C.$$

Případ (c). Dalším zobecněním jsou integrály typu

$$\int f\left(x,\ \sqrt[p(1)]{\frac{ax+b}{cx+d}},\ \sqrt[p(2)]{\frac{ax+b}{cx+d}},\ \ldots,\ \sqrt[p(j)]{\frac{ax+b}{cx+d}}\right)\,dx,$$

přičemž se navíc požaduje pouze to, aby hodnoty $a, b, c, d \in \mathbb{R}$ splňovaly nabízející se podmínku $ad - bc \neq 0$. Při zachování významu uvedených symbolů nyní klademe $t^n = \frac{ax+b}{cx+d}$. Konkrétně je

$$\int \frac{1}{x}\sqrt{\frac{x+1}{x-1}}\,dx = \left|\begin{array}{c} t^2 = \frac{x+1}{x-1} \\ x = \frac{t^2+1}{t^2-1} \\ dx = -\frac{4t}{(t^2-1)^2}\,dt \end{array}\right| = \int \frac{t^2-1}{t^2+1}\,\frac{-4t^2}{(t^2-1)^2}\,dt =$$
$$= \int \frac{-4t^2}{(t^2+1)(t^2-1)}\,dt = \int \left(\frac{1}{t+1} - \frac{1}{t-1} - \frac{2}{t^2+1}\right)dt =$$
$$= \ln|t+1| - \ln|t-1| - 2\operatorname{arctg} t + C =$$
$$= \ln\left|\sqrt{\tfrac{x+1}{x-1}} + 1\right| - \ln\left|\sqrt{\tfrac{x+1}{x-1}} - 1\right| - 2\operatorname{arctg}\sqrt{\tfrac{x+1}{x-1}} + C.$$

Úpravy

proto o integrály

$$I_\delta = \int_0^{2-\delta} \frac{dx}{\sqrt[4]{2-x}} = \int_\delta^2 y^{-1/4}\,dy =$$
$$= \left[-\frac{4}{3}y^{3/4}\right]_\delta^2 = \frac{4}{3}2^{3/4} - \frac{4}{3}\delta^{3/4}.$$

Všimněme si, že jsme ve výpočtu substitucí dostali integrál s přepočtenou horní mezí $\delta$ a dolní mezí 2. Otočením mezí do obvyklé polohy jsme do výrazu přidali jedno znaménko minus navíc.

Limita pro $\delta \to 0$ zprava zjevně existuje a spočítali jsme tedy nevlastní určitý integrál

$$I = \int_0^2 \frac{dx}{\sqrt[4]{2-x}} = \frac{4}{3}2^{3/4}.$$

Stejně budeme postupovat, pokud je zadáno integrování přes neohraničený interval. Často v tomto případě hovoříme o *nevlastních integrálech 1. druhu*, zatímco integrály z neohraničených funkcí na konečných intervalech jsou *nevlastní integrály 2. druhu*.

Obecně tedy např. pro $a \in \mathbb{R}$

$$I = \int_a^\infty f(x)\,dx = \lim_{b\to\infty}\int_a^b f(x)\,dx,$$

pokud limita vpravo existuje. Obdobně můžeme mít horní mez integrování konečnou a druhou nekonečnou. Pokud jsou nekonečné obě, počítáme integrál jako součet dvou integrálů s libovolně pevně zvolenou pevnou mezí uprostřed, tj.

$$\int_{-\infty}^\infty f(x)\,dx = \int_{-\infty}^a f(x)\,dx + \int_a^\infty f(x)\,dx.$$

Existence ani hodnota nezávisí na volbě takové meze, protože její změnou pouze o stejnou konečnou hodnotu měníme oba sčítance, ovšem s opačným znaménkem. Naopak limita při které by stejně rychle šla horní i dolní mez do $\pm\infty$ může vést k odlišným výsledkům! Např.

$$\int_{-a}^a x\,dx = \left[\frac{1}{2}x^2\right]_{-a}^a = 0,$$

přestože hodnoty integrálů $\int_a^\infty x\,dx$ s jednou pevnou mezí utečou rychle k nekončených hodnotám.

Při výpočtu určitého integrálu z racionální funkce lomené musíme pečlivě rozdělit zadaný interval podle bodů nespojitosti integrované funkce a spočítat jednotlivé nevlastní integrály každý zvlášť. Navíc je nutné rozdělit celý interval tak, abychom vždy integrovali funkci neohraničenou pouze v okolí jednoho z krajních bodů.

**6.31. Přírůstky do ZOO.** Z již spočítaných příkladů se může zdát, že je obvyklé najít neurčitý integrál pomocí výrazů složených ze známých elementárních funkcí. To je úplně mylný dojem.



$$\ln\left|\sqrt{\tfrac{x+1}{x-1}}+1\right|-\ln\left|\sqrt{\tfrac{x+1}{x-1}}-1\right|=\ln\left|\frac{\sqrt{\frac{x+1}{x-1}}+1}{\sqrt{\frac{x+1}{x-1}}-1}\right|=\ln\left|\frac{\sqrt{\frac{|x+1|}{|x-1|}}+1}{\sqrt{\frac{|x+1|}{|x-1|}}-1}\right|=$$
$$=\ln\left|\frac{\sqrt{|x+1|}+\sqrt{|x-1|}}{\sqrt{|x+1|}-\sqrt{|x-1|}}\right|=\ln\frac{\left(\sqrt{|x+1|}+\sqrt{|x-1|}\right)^2}{||x+1|-|x-1||}=$$
$$=2\ln\left(\sqrt{|x+1|}+\sqrt{|x-1|}\right)-\ln 2$$

pro $x\in(-\infty,-1)\cup(1,\infty)$ dále umožňují zapsat

$$\int\tfrac{1}{x}\sqrt{\tfrac{x+1}{x-1}}\,dx=2\ln\left(\sqrt{|x+1|}+\sqrt{|x-1|}\right)-2\operatorname{arctg}\sqrt{\tfrac{x+1}{x-1}}+C.$$

Případy (d), (e), (f). Nyní se zaměříme na integrály

$$\int f\left(x,\sqrt{ax^2+bx+c}\right)\,dx,$$

kde očekáváme $a\neq 0$ a $b^2-4ac\neq 0$ pro jinak libovolná čísla $a,b,c\in\mathbb{R}$. Připomeňme, že $f$ je racionální lomený výraz. Rozlišíme dva případy, kdy kvadratický polynom $ax^2+bx+c$ má reálné kořeny a kdy reálné kořeny nemá.

Pokud je $a>0$ a polynom $ax^2+bx+c$ má reálné kořeny $x_1,x_2$, vyjádříme

$$\sqrt{ax^2+bx+c}=\sqrt{a}\sqrt{(x-x_1)^2\tfrac{x-x_2}{x-x_1}}=\sqrt{a}\,|x-x_1|\sqrt{\tfrac{x-x_2}{x-x_1}}$$

a položíme $t^2=\frac{x-x_2}{x-x_1}$. Pokud je $a<0$ a polynom $ax^2+bx+c$ má reálné kořeny $x_1<x_2$, vyjádříme

$$\sqrt{ax^2+bx+c}=\sqrt{-a}\sqrt{(x-x_1)^2\tfrac{x_2-x}{x-x_1}}=\sqrt{-a}\,(x-x_1)\sqrt{\tfrac{x_2-x}{x-x_1}}$$

a zavedeme $t^2=\frac{x_2-x}{x-x_1}$. Pokud polynom $ax^2+bx+c$ nemá reálné kořeny (nutně musí být $a>0$), volíme substituci

$$\sqrt{ax^2+bx+c}=\pm\sqrt{a}\cdot x\pm t$$

při jakékoli volbě znamének. Poznamenejme, že znaménka samozřejmě volíme tak, abychom dostali co nejjednodušší výraz pro následné integrování. Ve všech uvedených případech potom tyto substituce vedou opět na racionální lomené funkce.

Platí tedy

(d)

$$\int\frac{dx}{(x+4)\sqrt{x^2+3x-4}}=\int\frac{dx}{(x+4)\sqrt{(x-1)(x+4)}}=\int\frac{dx}{(x+4)|x+4|\sqrt{\frac{x-1}{x+4}}}=$$
$$=\left|\begin{array}{c}t^2=\frac{x-1}{x+4}\\ x=\frac{5}{1-t^2}-4\\ dx=\frac{10t}{(1-t^2)^2}\,dt\end{array}\right|=\int\frac{\frac{10t}{(1-t^2)^2}}{\left(\frac{5}{1-t^2}\right)\left|\frac{5}{1-t^2}\right|t}\,dt=\int\frac{2}{5}\frac{|1-t^2|}{1-t^2}\,dt=$$
$$=\tfrac{2}{5}\operatorname{sgn}\left(1-t^2\right)\int 1\,dt=\tfrac{2}{5}\operatorname{sgn}\left(\tfrac{5}{x+4}\right)t+C=$$
$$=\tfrac{2}{5}\operatorname{sgn}(x)\sqrt{\tfrac{x-1}{x+4}}+C;$$

(e)

$$\int\frac{dx}{1+\sqrt{-x^2+x+2}}=\int\frac{dx}{1+\sqrt{-(x-2)(x+1)}}=\int\frac{dx}{1+(x+1)\sqrt{\frac{2-x}{x+1}}}=$$
$$=\left|\begin{array}{c}t^2=\frac{2-x}{x+1}\\ x=\frac{3}{t^2+1}-1\\ dx=\frac{-6t}{(t^2+1)^2}\,dt\end{array}\right|=\int\frac{\frac{-6t}{(t^2+1)^2}}{1+\frac{3}{t^2+1}t}\,dt=$$
$$=\int\frac{-6t}{(t^2+1)^2}\,\frac{t^2+1}{t^2+3t+1}\,dt=$$

Naopak, drtivá většina spojitých funkcí vede na integrály, které tak vyjádřit neumíme. A to i když integrujeme funkce docela jednoduché. Protože se integrací získané funkce velice často v praxi vyskytují, mnohé mají jména a před nástupem počítačů byly pro potřeby inženýrů vydávány obsáhlé tabulky hodnot takových funkcí. V dalším textu se ještě budeme vracet k metodám, jak numerické aproximace takových funkcí získávat.

Uvedeme si nyní aspoň nějaké příklady. V metodách pro zpracování signálu je velice důležitá funkce

$$\operatorname{sinc}(x)=\frac{\sin(x)}{x}.$$

Docela přímočaře, byť pracně, lze ověřit, že jde o hladkou funkci s limitními hodnotami

$$f(0)=1,\ f'(0)=0,\ f''(0)=-\frac{2}{3}.$$

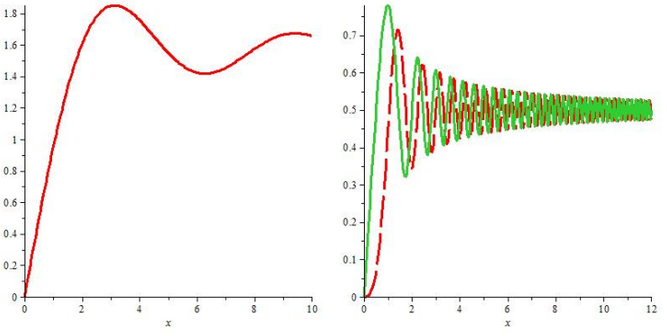
Je tedy okamžitě vidět, že tato sudá funkce bude mít v bodě $x=0$ absolutní maximum a s narůstající absolutní hodnotou $x$ se bude vlnit se stále se zmenšující amplitudou. Funkce *sinusintegrál* je definovaná vztahem

$$\operatorname{Si}(x)=\int_0^x\operatorname{sinc}(t)\,dt.$$

Důležité jsou také *Fresnelovy sinové a kosinové integrály*

$$\operatorname{FresnelS}(x)=\int_0^x\sin\left(\tfrac{1}{2}\pi t^2\right)dt$$
$$\operatorname{FresnelC}(x)=\int_0^x\cos\left(\tfrac{1}{2}\pi t^2\right)dt.$$

Na levém obrázku je průběh funkce $Si(x)$, na pravém vidíme obě Fresnelovy funkce.




Nové typy funkcí dostáváme také, když do integrovaného výrazu povolíme volný parametr, na kterém pak výsledek závisí. Příkladem může být jedna z nejdůležitějších funkcí v matematice vůbec — tzv. Gamma funkce. Je definovaná vztahem

$$\Gamma(z)=\int_0^\infty\mathrm{e}^{-t}\,t^{z-1}\,dt.$$

Lze ukázat, že tato funkce je analytická ve všech bodech $z\notin\mathbb{Z}$ a pro malá $z\in\mathbb{N}$ můžeme počítat:

$$\Gamma(1)=\int_0^\infty\mathrm{e}^{-t}\,t^0\,dt=[-\mathrm{e}^{-t}]_0^\infty=1$$
$$\Gamma(2)=\int_0^\infty\mathrm{e}^{-t}\,t^1\,dt=[-\mathrm{e}^{-t}\,t]_0^\infty+\int_0^\infty\mathrm{e}^{-t}\,dt=0+1=1$$
$$\Gamma(3)=\int_0^\infty\mathrm{e}^{-t}\,t^2\,dt=0+2\int_0^\infty\mathrm{e}^{-t}\,tdt=0+2=2$$

$$= \int \tfrac{-6t}{(t^2+1)(t^2+3t+1)}\,dt =$$
$$= \int \left(-\tfrac{4}{5}\tfrac{\sqrt{5}}{2t+3+\sqrt{5}} - \tfrac{2}{t^2+1} - \tfrac{4}{5}\tfrac{\sqrt{5}}{-2t-3+\sqrt{5}}\right) dt =$$
$$= -\tfrac{2\sqrt{5}}{5}\ln\left|2t+3+\sqrt{5}\right| - 2\operatorname{arctg} t +$$
$$+ \tfrac{2\sqrt{5}}{5}\ln\left|-2t-3+\sqrt{5}\right| + C =$$
$$= -\tfrac{2\sqrt{5}}{5}\ln\left|2\sqrt{\tfrac{2-x}{x+1}}+3+\sqrt{5}\right| - 2\operatorname{arctg}\sqrt{\tfrac{2-x}{x+1}} +$$
$$+ \tfrac{2\sqrt{5}}{5}\ln\left|-2\sqrt{\tfrac{2-x}{x+1}}-3+\sqrt{5}\right| + C =$$
$$= \tfrac{2\sqrt{5}}{5}\ln\frac{2\sqrt{\frac{2-x}{x+1}}+3-\sqrt{5}}{2\sqrt{\frac{2-x}{x+1}}+3+\sqrt{5}} - 2\operatorname{arctg}\sqrt{\tfrac{2-x}{x+1}} + C;$$

(f)

$$\int \tfrac{dx}{(x-1)\sqrt{x^2+x+1}} = \left|\begin{array}{c}\sqrt{x^2+x+1} = x+t\\ x^2+x+1 = x^2+2xt+t^2\\ x = -\frac{t^2+2t-2}{2t-1}+1\\ dx = \frac{-2(t^2-t+1)}{(2t-1)^2}\,dt\end{array}\right| =$$
$$= \int \frac{\frac{-2(t^2-t+1)}{(2t-1)^2}}{-\frac{t^2+2t-2}{2t-1}\,\frac{t^2-t+1}{2t-1}}\,dt = \int \tfrac{2}{t^2+2t-2}\,dt =$$
$$= \int \left(\tfrac{\sqrt{3}}{3}\tfrac{1}{t+1-\sqrt{3}} - \tfrac{\sqrt{3}}{3}\tfrac{1}{t+1+\sqrt{3}}\right) dt =$$
$$= \tfrac{\sqrt{3}}{3}\ln\left|t+1-\sqrt{3}\right| - \tfrac{\sqrt{3}}{3}\ln\left|t+1+\sqrt{3}\right| + C =$$
$$= \tfrac{\sqrt{3}}{3}\ln\left|\tfrac{t+1-\sqrt{3}}{t+1+\sqrt{3}}\right| + C = \tfrac{\sqrt{3}}{3}\ln\frac{\left|\sqrt{x^2+x+1}-x+1-\sqrt{3}\right|}{\sqrt{x^2+x+1}-x+1+\sqrt{3}} + C.$$

□

**6.57.** Pomocí vhodné substituce spočítejte

$$\int \tfrac{dx}{x+\sqrt{x^2+x-1}}\,dx, \quad x \in \left(-\infty, \tfrac{-\sqrt{5}-1}{2}\right) \cup \left(\tfrac{\sqrt{5}-1}{2}, +\infty\right).$$

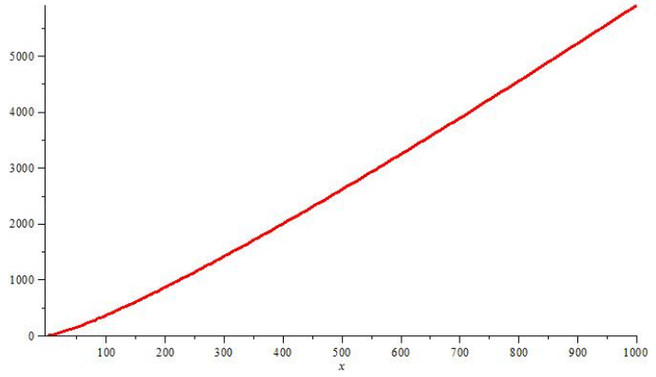
**Řešení.** Přestože kvadratický polynom pod odmocninou má reálné kořeny $x_1$, $x_2$, nebudeme příklad řešit pomocí substituce $t^2 = \frac{x-x_2}{x-x_1}$. Sice bychom tak postupovat mohli, ale raději použijeme metodu, kterou jsme zavedli pro případ komplexních kořenů. Tato metoda totiž dává velmi jednoduchý integrál racionální lomené funkce, jak vidíme z výpočtu

$$\int \tfrac{dx}{x+\sqrt{x^2+x-1}} = \left|\begin{array}{c}\sqrt{x^2+x-1} = x+t\\ x^2+x-1 = x^2+2xt+t^2\\ x = \frac{t^2+1}{1-2t}\\ dx = \frac{-2t^2+2t+2}{(1-2t)^2}\,dt\end{array}\right| = \int \tfrac{-2t^2+2t+2}{(t+2)(1-2t)}\,dt =$$
$$= \int \left(1 - \tfrac{2}{t+2} - \tfrac{1}{2}\tfrac{1}{t-\frac{1}{2}}\right) dt = t - 2\ln|t+2| - \tfrac{1}{2}\ln\left|t-\tfrac{1}{2}\right| + C =$$
$$= \sqrt{x^2+x-1} - x - 2\ln\left(\sqrt{x^2+x-1}-x+2\right) -$$
$$- \tfrac{1}{2}\ln\left|\sqrt{x^2+x-1}-x-\tfrac{1}{2}\right| + C.$$

Dodejme, že každou doporučenou substituci (viz dříve uvedené příklady) lze ve většině konkrétních úloh nahradit jinou substitucí, která umožní dospět k výsledku výrazně snazším způsobem. Nespornou výhodou doporučených substitucí však je univerzálnost: jejich a pomocí indukce snadno dovodíme, že pro všechna kladná celá čísla $n$ dává tato funkce hodnotu faktoriálu:

$$\Gamma(n) = (n-1)!$$

Následující obrázek ukazuje v logaritmickém měřítku závislé proměnné průběh funkce $f(x) = \ln(\Gamma(x))$. Vidíme z něj tedy, jak rychle skutečně roste faktoriál.




Než se pustíme do dalších témat matematické analýzy, uvedeme ještě několik přímých použití pro Riemannův integrál.

**6.32. Riemannovsky měřitelné množiny.** Sama definice Riemannova integrálu byla odvozena od představy velikosti plochy v rovině se souřadnicemi $x$ a $y$ ohraničené osou $x$, hodnotami funkce $y = f(x)$ a hraničními přímkami $x = a$, $x = b$. Přitom je plocha nad osou $x$ dána s kladným znaménkem zatímco hodnoty pod osou vedou ke znaménku zápornému. Ve skutečnosti víme zatím pouze, co je to plocha rovnoběžnostěnu určeného dvěma vektory, obecněji ve vektorovém prostoru $\mathbb{R}^n$ víme, co je to objem rovnoběžnostěnu. Plochy jiných podmnožin je teprve třeba definovat. Pro některé jednoduché objekty jako třeba mnohoúhelníky je definice dána přirozeně předpokládanými vlastnostmi.



Námi vybudovaný koncept Riemannova integrálu můžeme teď přímo použít k měření „objemu“ jednorozměrných podmnožin.

O podmnožině $A \subset \mathbb{R}$ řekneme, že je *(riemannovsky) měřitelná*, jestliže je funkce $\chi : \mathbb{R} \to \mathbb{R}$

$$\chi_A(x) = \begin{cases} 1 & \text{jestliže je } x \in A \\ 0 & \text{jestliže je } x \notin A. \end{cases}$$

riemannovsky integrovatelná, tj. existuje integrál (ať už s konečnou nebo nekonečnou hodnotou)

$$m(A) = \int_{-\infty}^{\infty} \chi_A(x)\,dx.$$

Funkci $\chi_A$ říkáme *charakteristická funkce množiny* $A$, hodnotě $m(A)$ říkáme *riemannovská míra množiny* $A$. Všimněme si, že pro interval $A = [a,b]$ jde vlastně o hodnotu

$$\int_{\infty}^{\infty} \chi_A(x)\,dx = \int_a^b dx = b-a,$$

přesně jak jsme očekávali.

Zároveň má takováto definice „velikosti“ očekávanou vlastnost, že míra sjednocení konečně mnoha riemannovsky měřitelných a po dvou disjunktních množin vyjde jako součet. Zejména každá konečná množina $A$ má riemannovskou míru nulovou.

zavedením lze vypočítat všechny integrály příslušných typů. □

Další metody integrování naleznete na straně 381

### D. Určité integrály

Pro libovolnou funkci $f$ spojitou a ohraničenou na ohraničeném intervalu $(a, b)$ platí tzv. Newtonův-Leibnizův vzorec

$$\int_a^b f(x)\,dx = [F(x)]_a^b := \lim_{x\to b-} F(x) - \lim_{x\to a+} F(x), \tag{6.9}$$

kde $F'(x) = f(x)$, $x \in (a, b)$. Zdůrazněme, že za uvedených podmínek vždy existuje primitivní funkce $F$ a jako vlastní obě limity v (‖6.9‖). K výpočtu určitého integrálu nám tedy stačí najít antiderivaci a určit příslušné jednostranné limity (příp. jen funkční hodnoty, je-li primitivní funkce spojitá v krajních bodech uvažovaného intervalu).

**6.58.** Vyčíslete určité integrály

$$\int_{\frac{\pi}{6}}^{\frac{\pi}{3}} \operatorname{tg}^2 x\ dx, \qquad \int_0^{\frac{\pi}{4}} \tfrac{x}{\cos^2 x}\ dx.$$

**Řešení.** Pro $x \neq \frac{\pi}{2} + k\,\pi$, kde $k \in \mathbb{Z}$, je

$$\int \operatorname{tg}^2 x\,dx = \operatorname{tg} x - x + C,$$

jak jsme vypočítali dříve. Odsud vyplývá, že

$$\int_{\pi/6}^{\pi/3} \operatorname{tg}^2 x\,dx = \left[\operatorname{tg} x - x\right]_{\pi/6}^{\pi/3} = \sqrt{3} - \tfrac{\pi}{3} - \left(\tfrac{1}{\sqrt{3}} - \tfrac{\pi}{6}\right) = \tfrac{2}{\sqrt{3}} - \tfrac{\pi}{6}.$$

Určité integrály lze pochopitelně počítat také přímo. Substituce $y = \operatorname{tg} x$ kupř. dává

$$\int_{\pi/6}^{\pi/3} \operatorname{tg}^2 x\,dx = \int_{\pi/6}^{\pi/3} \tfrac{\sin^2 x}{\cos^2 x}\,dx = \left|\begin{array}{l} y = \operatorname{tg} x;\ dy = \frac{dx}{\cos^2 x} \\ \sin^2 x = \frac{\operatorname{tg}^2 x}{1+\operatorname{tg}^2 x} = \frac{y^2}{1+y^2} \end{array}\right| =$$

$$= \int_{1/\sqrt{3}}^{\sqrt{3}} \tfrac{y^2}{1+y^2}\,dy = \int_{1/\sqrt{3}}^{\sqrt{3}} 1 - \tfrac{1}{1+y^2}\,dy = \left[y - \operatorname{arctg} y\right]_{1/\sqrt{3}}^{\sqrt{3}} = \tfrac{2}{\sqrt{3}} - \tfrac{\pi}{6}.$$

Pouze je třeba nezapomenout změnit při substituci meze integrálu na hodnoty získané dosazením $\sqrt{3} = \operatorname{tg}(\pi/3)$, $1/\sqrt{3} = \operatorname{tg}(\pi/6)$.

Druhý integrál vyčíslíme metodou per partes pro určitý integrál. (Poznamenejme, že primitivní funkce funkce $y = x\cos^{-2} x$ jsme také stanovili již dříve.) Platí

$$\int_0^{\pi/4} \tfrac{x}{\cos^2 x}\,dx = \left|\begin{array}{ll} F(x) = x & F'(x) = 1 \\ G'(x) = \frac{1}{\cos^2 x} & G(x) = \operatorname{tg} x \end{array}\right| =$$

$$= \left[x\operatorname{tg} x\right]_0^{\pi/4} - \int_0^{\pi/4} \operatorname{tg} x\,dx = \left[x\operatorname{tg} x\right]_0^{\pi/4} + \int_0^{\pi/4} \tfrac{-\sin x}{\cos x}\,dx =$$

$$= \left[x\operatorname{tg} x\right]_0^{\pi/4} + \left[\ln(\cos x)\right]_0^{\pi/4} = \tfrac{\pi}{4} + \ln\tfrac{\sqrt{2}}{2} = \tfrac{\pi - 2\ln 2}{4}.$$ □

Pokud ale vezmeme spočetné sjednocení, taková vlastnost již neplatí. Např. stačí vzít množinu $\mathbb{Q}$ všech racionálních čísel jakožto sjednocení jednoprvkových podmnožin. Zatímco každá množina o konečně mnoha bodech má podle naší definice míru nulovou, charakteristická funkce $\chi_{\mathbb{Q}}$ není riemannovsky integrovatelná.

Povšimněme si, že horní Riemannův integrál z charakteristické množiny $\chi_A$ odpovídá infimu součtů délek konečně mnoha disjunktních intervalu, kterými umíme pokrýt danou množinu $A$, zatímco dolní integrál je supremem součtu délek konečně mnoha disjunktních intervalů, které umíme vložit do množiny $A$. Takto lze postupovat i ve vyšších dimenzích při definici tzv. *Jordanovy míry*. Pro definici plochy (objemu) ve vícerozměrných prostorech budeme umět použít i přímo koncept Riemannova integrálu, až jej zobecníme do vícerozměrného případu. Nicméně je dobré si už teď povšimnout, že skutečně původní představa o ploše rovinného útvaru uzavřeného výše uvedeným způsobem grafem funkce bude bezezbytku naplněna.

**6.33. Střední hodnota funkce.** U konečné množiny hodnot jsme zvyklí uvažovat o jejich střední hodnotě a definujeme ji zpravidla jako aritmetický průměr.

Pro riemannovsky integrovatelnou funkci $f(x)$ na intervalu (konečném nebo nekonečném) $[a, b]$ je definována její *střední hodnota* výrazem

$$m(f) = \frac{1}{b-a}\int_a^b f(x)\,dx.$$

Z definice je $m(f)$ výška obdélníka (s orientací podle znaménka) nad intervalem $[a, b]$, který má stejnou plochu jako je plocha mezi osou $x$ a grafem funkce $f(x)$. Platí tedy obecně *integrální věta o střední hodnotě*

**Tvrzení.** *Je-li $f(x)$ riemannovsky integrovatelná reálná funkce na intervalu $[a, b]$, pak existuje číslo $m(f)$, pro které platí*

$$\int_a^b f(x)\,dx = m(f)(b-a).$$

Na konci odstavce 6.29 jsme odvodili, že spojitá funkce $f$ na intervalu $[a, b]$ nabývá své střední hodnoty $m(f)$ uvnitř tohoto intervalu.

**6.34. Délka prostorové křivky.** Námi vybudovaný integrál jde



také dobře použít pro výpočet *délky křivky* ve vícerozměrném vektorovém prostoru $\mathbb{R}^n$. Pro jednoduchost si to předvedeme na případu křivky v rovině $\mathbb{R}^2$ se souřadnicemi $x$, $y$. Mějme tedy parametrický popis křivky $F : \mathbb{R} \to \mathbb{R}^2$,

$$F(t) = [g(t), f(t)]$$

a představme si ji jako dráhu pohybu. Pro jednoduchost předpokládejme, že funkce $f(t)$ a $g(t)$ mají po částech spojitou derivaci.

Derivací zobrazení $F(t)$ dostaneme hodnoty, které budou odpovídat rychlosti pohybu po takovéto dráze. Proto celková délka křivky (tj. dráha uražená za dobu mezi hodnotami $t = a$, $t = b$) bude dána integrálem přes interval $[a, b]$, kde integrovanou funkcí $h(t)$ budou právě velikosti vektorů $F'(t)$. Chceme tedy spočíst délku $s$ rovnou

$$s = \int_a^b h(t)\,dt = \int_a^b \sqrt{(f'(t))^2 + (g'(t))^2}\,dt.$$

**6.59.** Vyčíslete určité integrály

(a) $\int_0^1 \frac{x}{\sqrt{1-x^2}}\,dx$;

(b) $\int_1^2 \frac{1}{\sqrt{x^2-1}}\,dx$;

(c) $\int_0^1 \left(\frac{e^x}{e^{2x}+3} + \frac{1}{\cos^2 x}\right) dx$;

**Řešení.** Platí

(a)

$$\int_0^1 \frac{x}{\sqrt{1-x^2}}\,dx = \left|\begin{array}{c} y = 1-x^2 \\ dy = -2x\,dx \end{array}\right| = -\int_1^0 \frac{y^{-1/2}}{2}\,dy =$$
$$= \int_0^1 \frac{y^{-1/2}}{2}\,dy = \left[\sqrt{y}\right]_0^1 = 1;$$

(b)

$$\int_1^2 \frac{dx}{\sqrt{x^2-1}} = \left|\begin{array}{c} z = x + \sqrt{x^2-1} \\ dz = \frac{\sqrt{x^2-1}+x}{\sqrt{x^2-1}}\,dx \end{array}\right| = \int_1^{2+\sqrt{3}} \frac{1}{z}\,dz =$$
$$= \left[\ln z\,\right]_1^{2+\sqrt{3}} = \ln\left(2+\sqrt{3}\right);$$

(c)

$$\int_0^1 \left(\frac{e^x}{e^{2x}+3} + \frac{1}{\cos^2 x}\right) dx = \int_0^1 \frac{e^x}{e^{2x}+3}\,dx + \int_0^1 \frac{1}{\cos^2 x}\,dx =$$
$$= \left|\begin{array}{c} p = e^x \\ dp = e^x\,dx \end{array}\right| = \int_1^e \frac{1}{p^2+3}\,dp + [\operatorname{tg} x]_0^1 =$$
$$= \frac{1}{3}\int_1^e \frac{1}{\left(\frac{p}{\sqrt{3}}\right)^2+1}\,dp + \operatorname{tg} 1 = \left|\begin{array}{c} s = \frac{p}{\sqrt{3}} \\ ds = \frac{1}{\sqrt{3}}\,dp \end{array}\right| =$$
$$= \frac{\sqrt{3}}{3}\int_{1/\sqrt{3}}^{e/\sqrt{3}} \frac{1}{s^2+1}\,ds + \operatorname{tg} 1 = \frac{\sqrt{3}}{3}[\operatorname{arctg} s]_{1/\sqrt{3}}^{e/\sqrt{3}} + \operatorname{tg} 1 =$$
$$= \frac{\sqrt{3}}{3}\left(\operatorname{arctg}\frac{e\sqrt{3}}{3} - \frac{\pi}{6}\right) + \operatorname{tg} 1;$$

□

**6.60.** Dokažte, že platí

$$\frac{\sqrt{2}}{20} \le \int_0^1 \frac{x^9}{\sqrt{1+x}}\,dx \le \frac{1}{10}.$$

**Řešení.** Neboť

$$0 \le \frac{x^9}{\sqrt{2}} \le \frac{x^9}{\sqrt{1+x}} \le x^9, \quad x \in [0,1],$$

z geometrického významu určitého integrálu plyne

$$\frac{\sqrt{2}}{20} = \int_0^1 \frac{x^9}{\sqrt{2}}\,dx \le \int_0^1 \frac{x^9}{\sqrt{1+x}}\,dx \le \int_0^1 x^9\,dx = \frac{1}{10}.$$ □

**6.61.** Bez symbolů derivace a integrace vyjádřete

$$\left(\int_x^0 t^5 \ln(t+1)\,dt\right)', \quad x \in (-1,1),$$

je-li derivováno podle $x$.

**Řešení.** O integrování se často hovoří jako o inverzní operaci k derivování. V tomto příkladu této „inverznosti“ využijeme. Funkce

Ve speciálním případě, kdy křivka je grafem funkce $y = f(x)$ mezi body $a < b$ obdržíme pro její délku

$$s = \int_a^b \sqrt{1 + (f'(x))^2}\,dx$$

Tentýž výsledek lze intuitivně vidět jako důsledek Pythagorovy věty: pro lineární přírůstek délky křivky $\Delta s$ odpovídající přírůstku $\Delta x$ proměnné $x$ spočteme totiž právě

$$\Delta s = \sqrt{(\Delta x)^2 + (\Delta y)^2}$$

a to při pohledu přímo na naši definici integrálu znamená

$$s = \int_a^b \sqrt{1 + \left(\frac{dy}{dx}\right)^2}\,dx.$$

Naopak základní věta diferenciálního počtu (viz 6.25) ukazuje, že na úrovni diferenciálů takto definovaná veličina délky grafu funkce $y = y(x)$ splňuje

$$ds = \sqrt{1 + (y'(x))^2}\,dx,$$

přesně dle očekávání.

Jako snadný příklad spočteme délku jednotkové kružnice jako dvojnásobek integrálu funkce $y = \sqrt{1-x^2}$ v mezích $[-1,1]$. Víme již, že musí vyjít číslo $2\pi$, protože jsme takto číslo $\pi$ definovali.

$$s = 2\int_{-1}^1 \sqrt{1+(y')^2}\,dx = 2\int_{-1}^1 \sqrt{1 + \frac{x^2}{1-x^2}}\,dx =$$
$$= 2\int_{-1}^1 \frac{1}{\sqrt{1-x^2}}\,dx = 2[\arcsin x]_{-1}^1 = 2\pi.$$

Jestliže v předchozím výpočtu budeme počítat s

$$y = \sqrt{r^2 - x^2} = r\sqrt{1 - (x/r)^2}$$

a meze budou $[-r, r]$, dostaneme substitucí $x = rt$ délku kružnice o poloměru $r$:

$$s(r) = 2\int_{-r}^r \sqrt{1 + \frac{(x/r)^2}{1-(x/r)^2}}\,dx = 2\int_{-1}^1 \frac{r}{\sqrt{1-t^2}}\,dt =$$
$$= 2r[\arcsin x]_{-1}^1 = 2\pi r.$$

Výsledek samozřejmě známe z elementární geometrie. Nicméně teď se nám z východisek integrálního počtu podařilo dovodit zásadní skutečnost, že je délka kružnice lineárně závislá na jejím průměru $2r$. Číslo $\pi$ je právě poměr, ve kterém se tato závislost realizuje.

**6.35. Plochy a objemy.** Riemannův integrál můžeme přímo použít na výpočet ploch či objemů útvarů definovaných pomocí grafu funkce.

Jako příklad spočtěme plochu kružnice s poloměrem $r$. Půlkruh vymezený funkcí $\sqrt{r^2-x^2}$ má plochu, jejíž dvojnásobek $a(r)$ spočteme substitucí $x = r\sin t$, $dx = r\cos t\,dt$ (s využitím výsledku pro $I_2$ v odstavci 6.22)

$$a(r) = 2\int_{-r}^r \sqrt{r^2-x^2}\,dx = 2r^2\int_{-\pi/2}^{\pi/2} \cos^2 t\,dt =$$
$$= \frac{2r^2}{2}[\cos t \sin t + t]_{-\pi/2}^{\pi/2} = \pi r^2.$$

$$F(x) := \int_0^x t^5 \ln(t+1)\, dt, \quad x \in (-1,1)$$

je očividně antiderivací funkce $f(x) := x^5 \ln(x+1)$ na intervalu $(-1,1)$, tj. jejím derivováním dostaneme právě $f$. Platí tedy

$$\left(\int_x^0 t^5 \ln(t+1)\, dt\right)' = -\left(\int_0^x t^5 \ln(t+1)\, dt\right)' = -x^5 \ln(x+1)\,.$$

□

### E. Nevlastní integrály

**6.62.** Rozhodněte, zda

$$\int_1^{+\infty} \frac{\operatorname{arctg} x}{x\sqrt{x}}\, dx \in \mathbb{R}.$$

**Řešení.** Nevlastní integrál udává obsah obrazce mezi grafem kladné funkce

$$y = \frac{\operatorname{arctg} x}{x\sqrt{x}}, \quad x \geq 1$$

a osou $x$ (zleva je obrazec ohraničen přímkou $x = 1$). Integrál je proto kladným reálným číslem, nebo je roven $+\infty$. Víme, že

$$\frac{\pi}{4} \leq \operatorname{arctg} x \leq \frac{\pi}{2}, \quad x \in [1, +\infty).$$

Odsud ovšem dostáváme

$$\frac{\pi}{2} = \frac{\pi}{4} \int_1^{+\infty} x^{-\frac{3}{2}}\, dx \leq \int_1^{+\infty} \frac{\operatorname{arctg} x}{x\sqrt{x}}\, dx \leq \frac{\pi}{2} \int_1^{+\infty} x^{-\frac{3}{2}}\, dx = \pi,$$

tj. zvláště

$$\int_1^{+\infty} \frac{\operatorname{arctg} x}{x\sqrt{x}}\, dx \in \mathbb{R}\,. \qquad \square$$

Vzorec (‖6.9‖) lze použít také tehdy, když je funkce $f$ neohraničená nebo interval $(a, b)$ je neohraničený. Mluvíme o tzv. nevlastních integrálech. Pro nevlastní integrály však limity na pravé straně mohou být nevlastní, příp. nemusejí vůbec existovat. Pokud jedna z limit neexistuje nebo obdržíme výraz $\infty - \infty$, znamená to, že integrál neexistuje ($\infty - \infty$ tedy v tomto případě nemá charakter neurčitého výrazu). Říkáme, že integrál osciluje. V každém jiném případě máme výsledek (připomeňme, že $\infty + \infty = +\infty$, $-\infty - \infty = -\infty$, $\pm\infty + a = \pm\infty$ pro $a \in \mathbb{R}$).

**6.63.** Určete

(a) $\int_1^{\infty} \sin x\, dx$;

(b) $\int_1^{\infty} \frac{dx}{x^4+x^2}$;

(c) $\int_0^4 \frac{dx}{\sqrt{x}}$;

(d) $\int_{-1}^1 \frac{dx}{x^2}$.

**Řešení.** Případ (a). Ihned stanovíme

Opět stojí za pozornost, že tento dobře známý vzoreček je odvozen z principů integrálního počtu a že kupodivu je plocha kruhu nejen úměrná kvadrátu poloměru, ale zároveň je tento poměr daný opět konstantou $\pi$.

Všimněme si ještě poměru obsahu a obvodu kruhu, tj.

$$\frac{\pi r^2}{2\pi r} = \frac{r}{2}.$$

Čtverec o stejném obsahu má stranu o velikosti $\sqrt{\pi}r$ a tedy obvod $4\sqrt{\pi}r$. Obvod čtverce o obsahu jednotkového kruhu je tedy $4\sqrt{\pi}$, což je o přibližně 0.8 více, než je obvod jednotkového kruhu. Lze dovodit, že ve skutečnosti je kružnice útvarem s nejmenším obvodem mezi všemi se stejným obsahem. K odvozování takových výsledků se dostaneme v našich poznámkách o tzv. variačním počtu v pozdějších kapitolách.

Další obdobou téhož principu je výpočet *povrchu nebo objemu rotačního tělesa*. Pokud vznikne těleso rotací grafu funkce $f$ kolem osy $x$ v intervalu $[a, b]$, vzniká při přírůstku $\Delta x$ nárůst plochy o násobek $\Delta s$ délky křivky zadané grafem funkce $y = f(x)$ a velikosti kružnice o poloměru $f(x)$. Plocha se proto spočte formulí

$$A(f) = 2\pi \int_a^b f(x)\, ds = 2\pi \int_a^b f(x)\sqrt{1 + (f'(x))^2}\, dx,$$

kde $ds$ je dán přírůstkem délky křivky $y = f(x)$, viz výše. Pokud bychom rotační těleso zadali jeho hranicí parametrizovanou dvojicí funkcí $[x(t), y(t)]$, bude příslušný diferenciál tvaru $ds = \sqrt{(x'(t))^2 + (y'(t))^2}\, dt$ a pro povrch dostaneme

$$A = 2\pi \int_a^b y(t)\sqrt{(y'(t))^2 + (x'(t))^2}\, dt.$$

Objem stejného tělesa naroste při změně $\Delta x$ o násobek tohoto přírůstku a plochy kružnice o poloměru $f(x)$. Proto je dán formulí

$$V(f) = \pi \int_a^b (f(x))^2\, dx.$$

Jako příklad užití vzorců pro obsah a objem odvodíme známé formule pro plochu sféry a objem koule o poloměru $r$.

$$A_r = 2\pi \int_{-r}^r r\sqrt{1 - (x/r)^2}\, \frac{1}{\sqrt{1 - (x/r)^2}}\, dt = 2\pi r \int_{-r}^r dt = 4\pi r^2,$$

$$V_r = \pi \int_{-r}^r (r^2 - x^2)\, dx = \pi \left[r^2 x - \frac{1}{3}x^3\right]_{-r}^r = \frac{4}{3}\pi r^3.$$

Stejně jako u kružnice i koule je objektem, který má mezi všemi s daným objemem ten nejmenší povrch. To je důvod, proč jsou mýdlové bubliny vždy prakticky tohoto tvaru.

**6.36. Integrální kriterium konvergence řad.** Pomocí nevlastního integrálu také umíme rozhodnout o konvergenci širší třídy nekonečných řad než doposud:

**Věta.** *Buď $\sum_{n=1}^{\infty} f(n)$ řada taková, že funkce $f : \mathbb{R} \to \mathbb{R}$ je kladná a nerostoucí na intervalu $\langle 1, \infty)$. Pak tato řada konverguje právě tehdy, když konverguje integrál*

$$\int_1^{\infty} f(x)\, \mathrm{d}x.$$

$$\int_1^\infty \sin x\,dx = [-\cos x]_1^\infty = \lim_{x\to\infty}(-\cos x) + \cos 1.$$

Protože limita na pravé straně neexistuje, uvažovaný integrál osciluje.

Případy (b), (c). Stejně lehce vypočítáme

$$\int_1^\infty \tfrac{dx}{x^4+x^2} = \int_1^\infty \tfrac{dx}{x^2(x^2+1)} = \int_1^\infty \tfrac{1}{x^2} - \tfrac{1}{1+x^2}\,dx = \left[-\tfrac{1}{x} - \operatorname{arctg} x\right]_1^\infty =$$
$$= \lim_{x\to\infty}\left(-\tfrac{1}{x} - \operatorname{arctg} x\right) + \tfrac{1}{1} + \operatorname{arctg} 1 = 0 - \tfrac{\pi}{2} + 1 + \tfrac{\pi}{4} = 1 - \tfrac{\pi}{4}$$

a ještě snazší pak je

$$\int_0^4 \tfrac{dx}{\sqrt{x}} = \left[2\sqrt{x}\,\right]_0^4 = 4 - 0 = 4,$$

kde je primitivní funkce v počátku spojitá zprava (uvažovaná limita je tak rovna funkční hodnotě).

Případ (d). Kdybychom bezmyšlenkovitě vypočítali

$$\int_{-1}^1 \tfrac{dx}{x^2} = \left[-\tfrac{1}{x}\right]_{-1}^1 = -1 - 1 = -2,$$

obdrželi bychom zjevně chybný výsledek (zápornou hodnotu při integrování kladné funkce). Důvodem, proč Newtonův-Leibnizův vzorec nejde takto aplikovat, je nespojitost uvažované funkce v počátku. Využijeme-li však tzv. pravidla návaznosti

$$\int_a^b f(x)\,dx = \int_a^c f(x)\,dx + \int_c^b f(x)\,dx,$$

které platí vždy, když mají integrály na pravé straně smysl, nalezneme správný výsledek

$$\int_{-1}^1 \tfrac{dx}{x^2} = \int_{-1}^0 \tfrac{dx}{x^2} + \int_0^1 \tfrac{dx}{x^2} = \left[-\tfrac{1}{x}\right]_{-1}^0 + \left[-\tfrac{1}{x}\right]_0^1 =$$
$$= \lim_{x\to 0-}\left(-\tfrac{1}{x}\right) - 1 - 1 - \lim_{x\to 0+}\left(-\tfrac{1}{x}\right) = \infty - 2 + \infty = +\infty.$$

Podotkněme, že ze sudosti funkce $y = x^{-2}$ také plyne

$$\int_{-1}^1 \tfrac{dx}{x^2} = 2\int_0^1 \tfrac{dx}{x^2} = 2\cdot\infty = +\infty\,. \qquad \square$$

**6.64.** Vyčíslete určité integrály

(a) $\int_0^\infty \frac{1}{(x+2)^5}\,dx$;
(b) $\int_{-2}^2 \ln|x|\,dx$;
(c) $\int_1^\infty \frac{e^{-\sqrt{x}}}{\sqrt{x}}\,dx$;
(d) $\int_{-1}^0 \frac{e^{1/x}}{x^3}\,dx$;
(e) $\int_1^2 \frac{1}{x\ln x}\,dx$.

**Řešení.** Platí

(a)

$$\int_0^\infty \tfrac{dx}{(x+2)^5} = -\tfrac{1}{4}\left[(x+2)^{-4}\right]_0^\infty =$$
$$= -\tfrac{1}{4}\left(\lim_{x\to\infty}(x+2)^{-4} - 2^{-4}\right) = -\tfrac{1}{4}\left(0 - \tfrac{1}{16}\right) = \tfrac{1}{64};$$

(b)



Důkaz. Pokud interpretujeme integrál, jako plochu pod křivkou, je kriterium zřejmé.

Daná řada konverguje nebo diverguje, právě když se stejným způsobem chová i řada $\sum_{n=2}^\infty f(n)$. Pro libovolné $k \in \mathbb{N}$ máme pro $k$-té částečné součty nerovnosti

$$\textstyle\sum_{n=2}^k f(n) \le \int_1^k f(x)\,dx \le \sum_{n=1}^k f(n)$$

neboť levá strana je dolním součtem Riemannova integrálu $\int_1^k f(x)\,dx$, zatímco pravá strana je součtem horním.

Odtud již bezprostředně plyne dokazované tvrzení. $\square$

### 3. Nekonečné řady

Již jsme se při budování našeho zvířetníku funkcí setkali s mocninnými řadami, které přirozeným způsobem rozšiřují skupinu všech polynomů, viz 5.45. Zároveň jsme si říkali, že takto získáme třídu analytických funkcí, ale nedokazovali jsme tehdy ani to, že jsou mocninné řady spojitými funkcemi. Snadno nyní ukážeme, že tomu tak je a že skutečně umíme mocninné řady i derivovat a integrovat po jednotlivých sčítancích. Právě proto ale také uvidíme, že není možné pomocí mocninných řad získat dostatečně širokou třídu funkcí. Např. nikdy tak nedostaneme jen po částech spojité periodické funkce, které jsou tak důležité pro modelování a zpracování audio a video signálů.

**6.37. Jak ochočené máme řady funkcí?** Vraťme se nyní



k diskusi limit posloupností funkcí a součtu řad funkcí z pohledu uplatnění postupů diferenciálního a integrálního počtu. Uvažujme tedy konvergentní řadu funkcí

$$S(x) = \sum_{n=1}^\infty f_n(x)$$

na intervalu $[a,b]$. Přirozené dotazy jsou:

- Jsou-li všechny funkce $f_n(x)$ spojité v nějakém bodě $x_0 \in [a,b]$, je spojitá i funkce $S(x)$ v bodě $x_0$?
- Jsou-li všechny funkce $f_n(x)$ diferencovatelné v nějakém bodě $a \in [a,b]$, je v něm diferencovatelná i funkce $S(x)$ a platí vztah $S'(x) = \sum_{n=1}^\infty f_n'(x)$?
- Jsou-li všechny funkce $f_n(x)$ riemannovsky integrovatelné na intervalu $[a,b]$, je integrovatelná i funkce $S(x)$ a platí vztah $\int_a^b S(x)dx = \sum_{n=1}^\infty \int_a^b f_n(x)dx$?

Ukážeme si nejprve na příkladech, že odpovědi na všechny tři takto kladené otázky jsou „NE!“. Poté ale najdeme jednoduché dodatečné podmínky na konvergenci řady, které naopak platnosti všech tří tvrzení zajistí. Řady funkcí tedy obecně moc zvladatelné nejsou, nicméně si umíme vybrat velikou třídu takových, se kterými se už pracuje velmi dobře. Mezi ně naštěstí budou patřit mocninné řady.

Poté se také zamyslíme nad alternativními koncepcemi integrování, které fungují více uspokojivě i pro větší třídy funkcí.

**6.38. Příklady ošklivých posloupností.** (1) Uvažme nejprve funkce

$$f_n(x) = (\sin x)^n$$

na intervalu $[0,\pi]$. Hodnoty těchto funkcí budou ve všech bodech $0 \le x \le \pi$ nezáporné a menší než jedna, kromě $x = \frac{\pi}{2}$, kde je

$$\int_{-2}^{2} \ln|x|\,dx = \int_{-2}^{0} \ln|x|\,dx + \int_{0}^{2} \ln|x|\,dx = 2\int_{0}^{2} \ln x\,dx =$$
$$= \left| \begin{array}{ll} F(x)=\ln x & F'(x)=\frac{1}{x} \\ G'(x)=1 & G(x)=x \end{array} \right| = 2\left( [x\ln x]_0^2 - \int_0^2 1\,dx \right) =$$
$$= 2\left( [x\ln x]_0^2 - [x]_0^2 \right) =$$
$$= 2\left( 2\ln 2 - \lim_{x\to 0+} (x\ln x) - 2 + 0 \right) =$$
$$= 4\ln 2 - 4;$$

(c)
$$\int_1^\infty \frac{\mathrm{e}^{-\sqrt{x}}}{\sqrt{x}}\,dx = \left| \begin{array}{l} t=\sqrt{x} \\ dt=\frac{1}{2\sqrt{x}}\,dx \end{array} \right| = 2\int_1^\infty \mathrm{e}^{-t}\,dt = 2\left[-\mathrm{e}^{-t}\right]_1^\infty =$$
$$= -2\left( \lim_{t\to\infty} \mathrm{e}^{-t} - \mathrm{e}^{-1} \right) = \frac{2}{\mathrm{e}};$$

(d)
$$\int_{-1}^{0} \frac{\mathrm{e}^{1/x}}{x^3}\,dx = \left| \begin{array}{l} u=1/x \\ du=-\frac{1}{x^2}\,dx \end{array} \right| = -\int_{-1}^{-\infty} u\,\mathrm{e}^u\,du =$$
$$= \int_{-\infty}^{-1} u\,\mathrm{e}^u\,du = \left| \begin{array}{ll} F(u)=u & F'(u)=1 \\ G'(u)=\mathrm{e}^u & G(u)=\mathrm{e}^u \end{array} \right| =$$
$$= [u\,\mathrm{e}^u]_{-\infty}^{-1} - \int_{-\infty}^{-1} \mathrm{e}^u\,du = [u\,\mathrm{e}^u]_{-\infty}^{-1} - [\mathrm{e}^u]_{-\infty}^{-1} =$$
$$= -\frac{1}{\mathrm{e}} - \lim_{u\to-\infty} u\,\mathrm{e}^u - \frac{1}{\mathrm{e}} + \lim_{u\to-\infty} \mathrm{e}^u = -\frac{2}{\mathrm{e}};$$

(e)
$$\int_1^2 \frac{dx}{x\ln x} = \left| \begin{array}{l} r=\ln x \\ dr=\frac{1}{x}\,dx \end{array} \right| = \int_0^{\ln 2} \frac{dr}{r} = [\ln r]_0^{\ln 2} =$$
$$= \ln(\ln 2) - \lim_{r\to 0+} \ln r = \ln(\ln 2) + \infty = +\infty. \qquad \square$$

**6.65.** Vypočítejte nevlastní integrály

$$\int_0^\infty x^2\,\mathrm{e}^{-x}\,dx; \qquad \int_{-\infty}^{\infty} \frac{dx}{\mathrm{e}^x+\mathrm{e}^{-x}}.$$

**Řešení.** Při výpočtu nevlastních integrálů můžeme používat metody, které jsme používali při výpočtu určitých integrálů. Metodou per partes získáváme

$$\int_0^\infty x^2\,\mathrm{e}^{-x}\,dx = \left| \begin{array}{ll} F(x)=x^2 & F'(x)=2x \\ G'(x)=\mathrm{e}^{-x} & G(x)=-\mathrm{e}^{-x} \end{array} \right| =$$
$$= \left[-x^2\,\mathrm{e}^{-x}\right]_0^\infty + 2\int_0^\infty x\,\mathrm{e}^{-x}\,dx = \left| \begin{array}{ll} F(x)=x & F'(x)=1 \\ G'(x)=\mathrm{e}^{-x} & G(x)=-\mathrm{e}^{-x} \end{array} \right| =$$
$$= -\lim_{x\to\infty} \frac{x^2}{\mathrm{e}^x} + 2\left[-x\,\mathrm{e}^{-x}\right]_0^\infty + 2\int_0^\infty \mathrm{e}^{-x}\,dx =$$
$$= 0 - 2\lim_{x\to\infty} \frac{x}{\mathrm{e}^x} + 2\left[-\mathrm{e}^{-x}\right]_0^\infty = 0 + 2\left( \lim_{x\to\infty} -\mathrm{e}^{-x} + 1 \right) = 2.$$

Substituční metoda potom dává

$$\int_{-\infty}^{\infty} \frac{dx}{\mathrm{e}^x+\mathrm{e}^{-x}} = \int_{-\infty}^{\infty} \frac{\mathrm{e}^x}{\mathrm{e}^{2x}+1}\,dx = \left| \begin{array}{l} y=\mathrm{e}^x \\ dy=\mathrm{e}^x\,dx \end{array} \right| = \int_0^\infty \frac{dy}{y^2+1} =$$
$$= \left[\operatorname{arctg} y\right]_0^\infty = \lim_{y\to\infty} \operatorname{arctg} y = \frac{\pi}{2},$$

kde nové meze integrálu plynou z limit

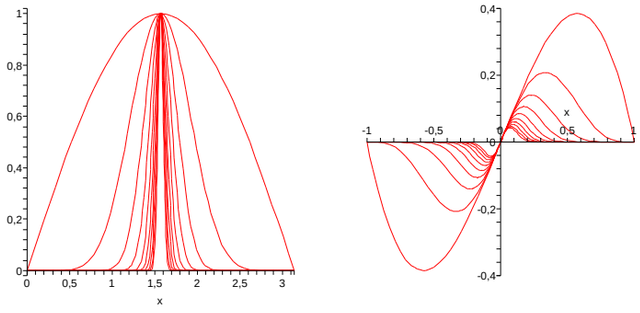
$$\lim_{x\to-\infty} \mathrm{e}^x = 0, \qquad \lim_{x\to\infty} \mathrm{e}^x = +\infty\,. \qquad \square$$

hodnota 1. Proto na celém intervalu $[0,\pi]$ budou bod po bodu tyto funkce konvergovat k funkci

$$f(x) = \lim_{n\to\infty} f_n(x) = \begin{cases} 0 & \text{pro všechna } x \neq \frac{\pi}{2} \\ 1 & \text{pro } x = \frac{\pi}{2}. \end{cases}$$

Zjevně tedy je limita posloupnosti funkcí $f_n$ nespojitou funkcí, ačkoliv jsou všechny funkce $f_n(x)$ spojité. Problematický je přitom dokonce vnitřní bod intervalu.

Tentýž jev umíme najít i pro řady funkcí, protože součet je limitou částečných součtů. Stačí tedy v předchozím příkladě vyjádřit $f_n$ jako $n$-tý částečný součet. Např. $f_1(x) = \sin x$, $f_2(x) = (\sin x)^2 - \sin x$, atd. Levý obrázek vykresluje funkce $f_m(x)$ pro $m = n^3$, $n = 1,\ldots,10$.




(2) Podívejme se nyní na druhou otázku, tj. na špatně se chovající derivace. Celkem přirozená je idea na podobném principu jako výše sestavit posloupnost funkcí, které budou mít v jednom bodě stále stejnou nenulovou derivaci, ale budou čím dál tím menší, takže bodově dokonvergují k funkci identicky nulové.

Předchozí obrázek napravo vykresluje funkce

$$f_n(x) = x(1-x^2)^n$$

na intervalu $[-1,1]$ pro hodnoty $n = m^2$, $m = 1,\ldots,10$. Na první pohled je zjevné, že

$$\lim_{n\to\infty} f_n(x) = 0$$

a všechny funkce $f_n(x)$ jsou hladké. V bodě $x = 0$ je jejich derivace

$$f_n'(0) = \left((1-x^2)^n - 2nx^2(1-x^2)^{n-1}\right)|_{x=0} = 1$$

nezávisle na $n$. Limitní funkce pro posloupnost $f_n$ přitom má samozřejmě všude derivaci nulovou!

(3) Protipříklad k třetímu tvrzení jsme už viděli v 6.32. Charakteristickou funkci $\chi_{\mathbb{Q}}$ racionálních čísel můžeme vyjádřit jako součet spočetně mnoha funkcí, které budou očíslovány právě racionálními čísly a budou vždy všude nulové, kromě jediného bodu, podle které jsou pojmenovány, kde jsou rovny 1. Riemannovy integrály všech takových funkcí budou nulové, jejich součet ale není riemannovsky integrovatelnou funkcí.

Právě tento příklad ukazuje na zásadní nedostatek Riemannova integrálu, ke kterému se ještě vrátíme.

Snadno ale najdeme i příklad, kdy limitní funkce $f$ je integrovatelná, všechny funkce $f_n$ jsou spojité a přesto hodnota integrálu není limitou hodnot integrálů $f_n$. Stačí lehce upravit posloupnost funkcí, které jsme použili výše:

$$f_n(x) = 2nx(1-x^2)^n.$$

**6.66.** Spočtěte

$$\int_0^\infty x^{2n+1}\,\mathrm{e}^{-x^2}\,dx, \qquad n \in \mathbb{N}.$$

**Řešení.** Příklad řešme nejprve substituční metodou a následně opakovaně aplikujme per partes se ziskem

$$\begin{aligned}
\int_0^\infty x^{2n+1}\,\mathrm{e}^{-x^2}\,dx &= \left|\begin{array}{l} y = x^2 \\ dy = 2x\,dx \end{array}\right| = \tfrac{1}{2}\int_0^\infty y^n\,\mathrm{e}^{-y}\,dy = \\
&= \left|\begin{array}{ll} F(y) = y^n & F'(y) = ny^{n-1} \\ G'(y) = \mathrm{e}^{-y} & G(y) = -\mathrm{e}^{-y} \end{array}\right| = \\
&= \tfrac{1}{2}\left(\left[-y^n\,\mathrm{e}^{-y}\right]_0^\infty + n\int_0^\infty y^{n-1}\,\mathrm{e}^{-y}\,dy\right) = \tfrac{n}{2}\int_0^\infty y^{n-1}\,\mathrm{e}^{-y}\,dy = \\
&= \left|\begin{array}{ll} F(y) = y^{n-1} & F'(y) = (n-1)y^{n-2} \\ G'(y) = \mathrm{e}^{-y} & G(y) = -\mathrm{e}^{-y} \end{array}\right| = \\
&= \tfrac{n}{2}\left(\left[-y^{n-1}\,\mathrm{e}^{-y}\right]_0^\infty + (n-1)\int_0^\infty y^{n-2}\,\mathrm{e}^{-y}\,dy\right) = \\
&= \tfrac{n(n-1)}{2}\int_0^\infty y^{n-2}\,\mathrm{e}^{-y}\,dy = \cdots = \tfrac{n(n-1)\cdots 2}{2}\int_0^\infty y\,\mathrm{e}^{-y}\,dy = \\
&= \left|\begin{array}{ll} F(y) = y & F'(y) = 1 \\ G'(y) = \mathrm{e}^{-y} & G(y) = -\mathrm{e}^{-y} \end{array}\right| = \\
&= \tfrac{n!}{2}\left(\left[-y\,\mathrm{e}^{-y}\right]_0^\infty + \int_0^\infty \mathrm{e}^{-y}\,dy\right) = \\
&= \tfrac{n!}{2}\left[-\mathrm{e}^{-y}\right]_0^\infty = \tfrac{n!}{2}.
\end{aligned}$$

□

*6.67.* V závislosti na $a \in \mathbb{R}^+$ určete integrál $\int_0^1 \frac{1}{x^a}\,\mathrm{d}x$. ○

### F. Délky, obsahy, povrchy, objemy

**6.68.** Určete délku křivky dané parametricky

$$x = \sin^2 t, \quad y = \cos^2 t,$$

pro $t \in [0, \frac{\pi}{2}]$.

**Řešení.** Podle 6.34 je délka křivky daná integrálem

$$\begin{aligned}
\int_0^{\frac{\pi}{2}} \sqrt{(x'(t))^2 + (y'(t))^2}\,\mathrm{d}t &= \int_0^{\frac{\pi}{2}} \sqrt{(\sin 2t)^2 + (-\sin 2t)^2}\,\mathrm{d}t = \\
&= \int_0^{\frac{\pi}{2}} \sqrt{2}\sin 2t\,\mathrm{d}t = \sqrt{2}.
\end{aligned}$$

Pokud si uvědomíme, že daná křivka je částí přímky $y = 1 - x$ (neboť $\sin^2 t + \cos^2 t = 1$) a sice úsečka s koncovými body $[0, 1]$ (pro hodnotu $t = 0$) a $[1, 0]$ (pro hodnotu $t = \frac{\pi}{2}$) tak okamžitě můžeme psát její délku, tedy $\sqrt{2}$. □

**6.69.** Určete délku křivky dané parametricky

$$x = t^2, \quad y = t^3$$

pro $t \in [0, \sqrt{5}]$.

Snadno ověříme, že i hodnoty těchto funkcí konvergují pro každé $x \in [0, 1]$ k nule (např. vidíme, že $\ln(f_n(x)) \to -\infty$). Přitom

$$\int_0^1 f_n(x)\,dx = \frac{n}{n+1} \to 1 \neq 0.$$

**6.39. Stejnoměrná konvergence.** Zjevným důvodem neúspěchu ve všech třech předchozích příkladech je skutečnost, že rychlost bodové konvergence hodnot $f_n(x) \to f(x)$ se bod od bodu velice liší. Přirozenou myšlenkou tedy je omezit se na takové případy, kdy bude naopak konvergence probíhat přibližně stejně rychle po celém intervalu.



#### Stejnoměrná konvergence

**Definice.** Říkáme, že posloupnost funkcí $f_n(x)$ *konverguje stejnoměrně* na intervalu $[a, b]$ k limitě $f(x)$, jestliže pro každé kladné číslo $\varepsilon$ existuje přirozené číslo $N \in \mathbb{N}$ takové, že pro všechna $n \geq N$ a všechna $x \in [a, b]$ platí

$$|f_n(x) - f(x)| < \varepsilon.$$

O řadě funkcí řekneme, že konverguje stejnoměrně na intervalu, jestliže stejnoměrně konverguje posloupnost jejích částečných součtů.

Tedy volba čísla $N$ sice závisí na zvoleném $\varepsilon$, je ale nezávislá na bodu $x \in [a, b]$. To je rozdíl od bodové konvergence, kde $N$ závisí na $\varepsilon$ i $x$. Graficky si definici můžeme představit tak, že do pásu vzniklého posunutím limitní funkce $f(x)$ na $f(x) \pm \varepsilon$ pro libovolně malé, ale pevně zvolené kladné $\varepsilon$, vždy padnou všechny funkce $f_n(x)$, až na konečně mnoho z nich. Tuto vlastnost zjevně neměl první a poslední z předchozích příkladů, u druhého ji postrádala posloupnost derivací $f_n'$.

Následující tři věty lze stručně shrnout tvrzením, že všechna tři obecně neplatná tvrzení v 6.37 platí pro stejnoměrnou konvergenci (pozor ale na jemnosti u derivování).



**6.40. Věta.** *Nechť $f_n(x)$ je posloupnost funkcí spojitých na intervalu $[a, b]$, která na tomto intervalu stejnoměrně konverguje k funkci $f(x)$. Pak je také $f(x)$ spojitá funkce na intervalu $[a, b]$.*

Důkaz. Chceme ukázat, že pro libovolný pevně zvolený bod $x_0 \in [a, b]$ a jakékoliv pevně zvolené malé $\varepsilon > 0$ bude

$$|f(x) - f(x_0)| < \varepsilon$$

pro všechna $x$ dostatečně blízká k $x_0$. Z definice stejnoměrné konvergence je pro nějaké $\varepsilon > 0$

$$|f_n(x) - f(x)| < \varepsilon$$

pro všechna $x \in [a, b]$ a všechna dostatečně velká $n$. Zvolme si tedy nějaké takové $n$ a uvažme $\delta > 0$ tak, aby také

$$|f_n(x) - f_n(x_0)| < \varepsilon$$

pro všechna $x$ z $\delta$-okolí $x_0$ (to je možné, protože všechny $f_n(x)$ jsou spojité). Pak

$$\begin{aligned}
|f(x) - f(x_0)| \leq |f(x) - f_n(x)| + |f_n(x) - f_n(x_0)| + \\
+ |f_n(x_0) - f(x_0)| < 3\varepsilon
\end{aligned}$$

pro všechna $x$ z námi zvoleného $\delta$-okolí bodu $x_0$. □

**Řešení.** Délku $l$ určíme opět využitím vztahu 6.34:

$$l = \int_0^{\sqrt{5}} \sqrt{4t^2 + 9t^4}\,\mathrm{d}t = \int_0^{\sqrt{5}} t\sqrt{9t^2 + 4}\,\mathrm{d}t =$$
$$= \frac{1}{2}\int_0^5 \sqrt{9u + 4}\,\mathrm{d}t = \frac{2}{27}[(9u+4)^{\frac{3}{2}}]_0^5 = \frac{335}{27}.$$

□

**6.70.** Určete plochu ležící napravo od přímky $x = 3$ a dále ohraničenou grafem funkce $y = \frac{1}{x^3-1}$ a osou $x$.

**Řešení.** Plocha je dána nevlastním integrálem $\int_3^\infty \frac{1}{x^3-1}\,\mathrm{d}x$. Vypočteme jej metodou rozkladu na parciální zlomky:

$$\begin{aligned}
\frac{1}{x^3-1} &= \frac{Ax+B}{x^2+x+1} + \frac{C}{x-1},\\
1 &= (Ax+B)(x-1) + C(x^2+x+1),\\
x = 1 &\implies C = \frac{1}{3},\\
x^0 : 1 = C - B &\implies B = -\frac{2}{3},\\
x^2 : 0 = A + C &\implies A = -\frac{1}{3}
\end{aligned}$$

a můžeme psát

$$\int_3^\infty \frac{1}{x^3-1}\,\mathrm{d}x = \frac{1}{3}\int_3^\infty \left(\frac{1}{x-1} - \frac{x+2}{x^2+x+1}\right)\mathrm{d}x.$$

Nyní určíme zvlášť neurčitý integrál $\int \frac{x+2}{x^2+x+1}\,\mathrm{d}x$:

$$\begin{aligned}
&\int \frac{x+2}{x^2+x+1}\,\mathrm{d}x =\\
&= \int \frac{x+\frac{1}{2}}{(x+\frac{1}{2})^2+\frac{3}{4}}\,\mathrm{d}x + \frac{3}{2}\int \frac{1}{(x+\frac{1}{2})^2+\frac{3}{4}}\,\mathrm{d}x =\\
&= \left|\begin{array}{l} t = x^2+x+1 \\ \mathrm{d}t = 2(x+\frac{1}{2})\,\mathrm{d}x \end{array}\right| =\\
&= \frac{1}{2}\int \frac{1}{t}\,\mathrm{d}t + \frac{3}{2}\int \frac{1}{(x+\frac{1}{2})^2+\frac{3}{4}} = \left|\begin{array}{l} s = x+\frac{1}{2} \\ \mathrm{d}s = \mathrm{d}x \end{array}\right| =\\
&= \frac{1}{2}\ln(x^2+x+1) + \frac{3}{2}\int \frac{1}{s^2+\frac{3}{4}}\,\mathrm{d}s =\\
&= \frac{1}{2}\ln((x^2+x+1) + \frac{3}{2}\frac{4}{3}\int \frac{1}{\left(\frac{2}{\sqrt{3}}s\right)^2+1}\,\mathrm{d}s =\\
&= \left|\begin{array}{l} u = \frac{2}{\sqrt{3}}s \\ \mathrm{d}u = \frac{2}{\sqrt{3}}\,\mathrm{d}s \end{array}\right| =\\
&= \frac{1}{2}\ln(x^2+x+1) + 2\frac{\sqrt{3}}{2}\int \frac{1}{u^2+1}\,\mathrm{d}u =\\
&= \frac{1}{2}\ln(x^2+x+1) + \sqrt{3}\arctan(u) =\\
&= \frac{1}{2}\ln(x^2+x+1) + \sqrt{3}\arctan\left(\frac{2x+1}{\sqrt{3}}\right).
\end{aligned}$$

Ve skutečnosti jsme v důkazu ověřili platnost o něco obecnějšího tvrzení.

**Tvrzení** (Věta o záměně limit)**.** *Jestliže posloupnost funkcí $f_n(x)$ konverguje na intervalu $[a,b]$ stejnoměrně k funkci $f(x)$ a jestliže existují limity*

$$\lim_{x\to x_0} f_n(x) = a_n, \qquad \lim_{n\to\infty} a_n = a,$$

*pak také existuje limita $\lim_{x\to x_0} f(x) = a$. Jinak řečeno, za uvedených podmínek platí*

$$\lim_{n\to\infty}\big(\lim_{x\to x_0} f_n(x)\big) = \lim_{x\to x_0}\big(\lim_{n\to\infty} f_n(x)\big).$$

**6.41. Věta.** *Nechť $f_n(x)$ je posloupnost riemannovsky integrovatelných funkcí na konečném intervalu $[a,b]$, které na tomto intervalu stejnoměrně konvergují k funkci $f(x)$. Pak také $f(x)$ je riemannovsky integrovatelná a platí*

$$\lim_{n\to\infty}\int_a^b f_n(x)\,dx = \int_a^b \left(\lim_{n\to\infty} f_n(x)\right)dx = \int_a^b f(x)\,dx.$$

Důkaz této věty se opírá o zobecnění vlastností cauchyovských posloupností čísel na stejnoměrnou konvergenci funkcí. Tímto způsobem umíme pracovat s existencí limity posloupnosti integrálů, aniž bychom ji potřebovali znát.

### Stejnoměrně cauchyovské posloupnosti

**Definice.** Řekneme, že posloupnost funkcí $f_n(x)$ na intervalu $[a,b]$ je *stejnoměrně Cauchyovská*, jestliže pro každé (malé) kladné číslo $\varepsilon$ existuje (velké) přirozené číslo $N$ takové, že pro všechna $x \in [a,b]$ a všechna $n \geq N$ platí

$$|f_n(x) - f_m(x)| < \varepsilon.$$

Zřejmě je každá stejnoměrně konvergentní posloupnost funkcí na intervalu $[a,b]$ také stejnoměrně Cauchyovská na témže intervalu, stačí si povšimnout obvyklého odhadu

$$|f_n(x) - f_m(x)| \leq |f_n(x) - f(x)| + |f(x) - f_m(x)|$$

založeného na trojúhelníkové nerovnosti.

Toto pozorování nám už stačí k důkazu naší věty, zastavíme se ale napřed u užitečného obráceného tvrzení:

**Tvrzení.** *Každá stejnoměrně Cauchyovská posloupnost funkcí $f_n(x)$ na intervalu $[a,b]$ stejnoměrně konverguje k nějaké funkci $f$ na tomto intervalu.*

Důkaz. Z podmínky cauchyovskosti posloupnosti funkcí vyplývá, že také pro každý bod $x \in [a,b]$ je posloupnost hodnot $f_n(x)$ Cauchyovskou posloupností reálných (případně komplexních) čísel. Bodově tedy nutně konverguje posloupnost funkcí $f_n(x)$ k nějaké funkci $f(x)$.

Ukážeme, že ve skutečnosti konverguje posloupnost $f_n(x)$ ke své limitě stejnoměrně. Zvolme $N$ tak velké, aby

$$|f_n(x) - f_m(x)| < \varepsilon$$

pro nějaké předem zvolené malé kladné $\varepsilon$ a všechna $n \geq N$, $x \in [a,b]$. Nyní zvolíme pevně jedno takové $n$ a odhadneme

$$|f_n(x) - f(x)| = \lim_{m\to\infty} |f_n(x) - f_m(x)| \leq \varepsilon$$

pro všechna $x \in [a,b]$. □

Celkem pak pro nevlastní integrál můžeme psát:

$$\begin{aligned}
&\int_3^\infty \frac{1}{x^3-1}\,\mathrm{d}x = \\
&= \frac{1}{3}\lim_{\delta\to\infty}\left[\ln|x-1| - \frac{1}{2}\ln(x^2+x+1) - \sqrt{3}\arctan\left(\frac{2x+1}{\sqrt{3}}\right)\right]_3^\delta = \\
&= \frac{1}{3}\lim_{\delta\to\infty}\left(\frac{1}{3}\ln|\delta-1| - \frac{1}{2}\ln(\delta^2+\delta+1) - \sqrt{3}\arctan\left(\frac{2\delta+1}{\sqrt{3}}\right)\right) - \\
&\quad -\frac{1}{3}\ln 2 + \frac{1}{6}\ln 13 + \frac{\sqrt{3}}{3}\arctan\frac{7}{\sqrt{3}} = \\
&= \frac{1}{6}\ln 13 - \frac{1}{3}\ln 2 + \frac{\sqrt{3}}{3}\arctan\frac{7}{\sqrt{3}} - \\
&\quad -\frac{1}{3}\lim_{\delta\to\infty}\ln\left|\frac{x-1}{\sqrt{x^2+x+1}}\right| - \frac{1}{3}\lim_{\delta\to\infty}\sqrt{3}\arctan\left(\frac{2\delta+1}{\sqrt{3}}\right) = \\
&= \frac{1}{6}\ln 13 + \frac{1}{\sqrt{3}}\arctan\frac{7}{\sqrt{3}} - \frac{1}{3}\ln 2 - \frac{\sqrt{3}}{6}\pi.
\end{aligned}$$

□

**6.71.** Určete povrch a objem rotačního paraboloidu, který vznikne rotací části paraboly $y = 2x^2$ pro $x \in [0, 1]$ kolem osy $y$.

**Řešení.** Vzorce pro výpočet objemu rotačního tělesa uvedené v odstavci 6.35 platí pro tělesa vzniklá rotací křivky kolem osy $x$. Je tedy nutno buď integrovat danou křivku podle neznámé $y$, nebo transformovat souřadnice.

$$\begin{aligned}
V &= \int_0^2 \frac{x}{2}\,\mathrm{d}x = \pi \\
S &= 2\pi\int_0^2 \sqrt{\frac{x}{2}}\sqrt{1+\frac{1}{8x}}\,\mathrm{d}x = 2\pi\int_0^2\sqrt{\frac{x}{2}+\frac{1}{16}}\,\mathrm{d}x = \\
&= \pi\frac{17\sqrt{17}-1}{24}.
\end{aligned}$$

□

**6.72.** Vypočtěte obsah $S$ obrazce složeného ze dvou částí roviny vymezených přímkami $x = 0$, $x = 1$, $x = 4$, osou $x$ a grafem funkce

$$y = \frac{1}{\sqrt[3]{x-1}}.$$

**Řešení.** Nejprve si uvědomme, že

$$\frac{1}{\sqrt[3]{x-1}} < 0, \quad x \in [0,1), \qquad \frac{1}{\sqrt[3]{x-1}} > 0, \quad x \in (1,4]$$

a že

$$\lim_{x\to 1-}\frac{1}{\sqrt[3]{x-1}} = -\infty, \quad \lim_{x\to 1+}\frac{1}{\sqrt[3]{x-1}} = +\infty.$$

První část obrazce (ležící pod osou $x$) je proto ohraničena křivkami

$$y = 0, \quad x = 0, \quad x = 1, \quad y = \frac{1}{\sqrt[3]{x-1}}$$

s obsahem daným nevlastním integrálem

$$S_1 = -\int_0^1 \frac{1}{\sqrt[3]{x-1}}\,dx;$$

zatímco druhá část (nad osou $x$) vymezená křivkami

Důkaz Věty. Připomeňme, že každá stejnoměrně konvergentní posloupnost funkcí je také stejnoměrně Cauchyovská a že Riemannovy součty pro jednotlivé členy naší posloupnosti konvergují k $\int_a^b f_n(x)\,dx$ nezávisle na výběru dělení a reprezentantů. Proto, jestliže platí

$$|f_n(x) - f_m(x)| < \varepsilon$$

pro všechna $x \in [a, b]$, pak také

$$\left|\int_a^b f_n(x)\,dx - \int_a^b f_m(x)\,dx\right| \le \varepsilon|b-a|.$$

Je tedy posloupnost čísel $\int_a^b f_n(x)\,dx$ Cauchyovská a proto konvergentní. Současně ale také díky stejnoměrné konvergenci posloupnosti $f_n(x)$ platí pro limitní funkci $f(x)$ ze stejného důvodu, že její Riemannovy součty jsou libovolně blízké Riemannovým součtům pro funkce $f_n$ s dostatečně velkým $n$ a limitní funkce $f(x)$ bude tedy opět integrovatelná. Zároveň

$$\left|\int_a^b f_n(x)\,dx - \int_a^b f(x)\,dx\right| \le \varepsilon|b-a|$$

a musí proto jít o správnou limitní hodnotu. □

Pro příslušný výsledek o derivacích je třeba zvýšené pozornosti ohledně předpokladů:

**6.42. Věta.**



*Nechť $f_n(x)$ je posloupnost funkcí diferencovatelných na intervalu $[a, b]$, a předpokládejme $f_n(x_0) \to f(x_0)$ v nějakém bodě $x_0 \in [a, b]$. Dále nechť jsou všechny derivace $g_n(x) = f_n'(x)$ spojité a nechť konvergují na témže intervalu stejnoměrně k funkci $g(x)$. Pak je také funkce $f(x) = \int_{x_0}^x g(t)\,dt$ diferencovatelná na intervalu $[a, b]$, funkce $f_n(x)$ konvergují k $f(x)$ a platí $f'(x) = g(x)$.*

Důkaz. Jestliže budeme místo $f_n(x)$ uvažovat funkce $\tilde{f}_n(x) = f_n(x) - f_n(x_0)$, budou předpoklady i závěry ve větě platné nebo neplatné pro obě posloupnosti zároveň. Bez újmy na obecnosti můžeme proto předpokládat, že všechny naše funkce splňují $f_n(x_0) = 0$. Pak ovšem můžeme psát pro všechny $x \in [a, b]$

$$f_n(x) = \int_{x_0}^x g_n(t)\,dt.$$

Protože ale funkce $g_n$ stejnoměrně konvergují k funkci $g$ na celém $[a, b]$, konvergují funkce $f_n(x)$ k funkci

$$f(x) = \int_{x_0}^x g(t)\,dt.$$

Protože je funkce $g$ coby stejnoměrná limita spojitých funkcí opět spojitou funkcí, dokázali jsme vše potřebné, viz Věta 6.24 o Riemannově integrálu a primitivní funkci. □

Pro nekonečné řady můžeme předchozí výsledky shrnout takto:

**6.43. Důsledek.** *Uvažme funkce $f_n(x)$ na intervalu $[a, b]$.*

*(1) Jsou-li všechny funkce $f_n(x)$ spojité na $[a, b]$ a řada*

$$S(x) = \sum_{n=1}^\infty f_n(x)$$

*konverguje stejnoměrně k funkci $S(x)$, je i funkce $S(x)$ spojitá na $[a, b]$.*

$$y = 0, \quad x = 1, \quad x = 4, \quad y = \frac{1}{\sqrt[3]{x-1}}$$

má obsah

$$S_2 = \int_1^4 \frac{1}{\sqrt[3]{x-1}}\, dx.$$

Neboť

$$\int \frac{1}{\sqrt[3]{x-1}}\, dx = \tfrac{3}{2}\sqrt[3]{(x-1)^2} + C,$$

jako součet $S_1 + S_2$ získáváme

$$S = -\lim_{x\to 1-}\left(\tfrac{3}{2}\sqrt[3]{(x-1)^2} - \tfrac{3}{2}\right) + \lim_{x\to 1+}\left(\tfrac{3}{2}\sqrt[3]{9} - \tfrac{3}{2}\sqrt[3]{(x-1)^2}\right) = \\ = \tfrac{3}{2}\left(1 + \sqrt[3]{9}\right).$$

Ukázali jsme mj. to, že uvedený obrazec má konečný obsah, přestože není (shora ani zdola) ohraničený. (Blížíme-li se k $x = 1$ zprava, příp. zleva, jeho výška roste nade všechny meze.) Připomeňme zde neurčitý výraz typu $0 \cdot \infty$. Obrazec je totiž ohraničený, když se omezíme na $x \in [0, 1-\delta] \cup [1+\delta, 4]$ při libovolně malém $\delta > 0$. □

**6.73.** Určete průměrnou rychlost $v_p$ tělesa v časovém intervalu $[1, 2]$, pokud je jeho rychlost

$$v(t) = \frac{t}{\sqrt{1+t^2}}, \quad t \in [1, 2].$$

Jednotky neuvažujte.

**Řešení.** K vyřešení příkladu si stačí uvědomit, že hledaná průměrná rychlost je střední hodnota funkce $v$ na intervalu $[1, 2]$. Platí tak

$$v_p = \frac{1}{2-1}\int_1^2 \frac{t}{\sqrt{1+t^2}}\, dt = \int_2^5 \frac{1}{2\sqrt{x}}\, dx = \sqrt{5} - \sqrt{2},$$

přičemž $1 + t^2 = x$, $t\, dt = dx/2$. □

**6.74.** Vypočítejte délku $s$ části křivky označované jako traktrix dané parametrickým popisem

$$f(t) = r\cos t + r\ln\left(\operatorname{tg}\tfrac{t}{2}\right), \quad g(t) = r\sin t, \quad t \in [\pi/2, a],$$

kde $r > 0$, $a \in (\pi/2, \pi)$.

**Řešení.** Protože

$$f'(t) = -r\sin t + \frac{r}{2\operatorname{tg}\frac{t}{2}\cdot\cos^2\frac{t}{2}} = -r\sin t + \frac{r}{\sin t} = \frac{r\cos^2 t}{\sin t},$$

$g'(t) = r\cos t$ na intervalu $[\pi/2, a]$,

pro délku $s$ dostáváme

$$s = \int_{\pi/2}^{a} \sqrt{\frac{r^2\cos^4 t}{\sin^2 t} + r^2\cos^2 t}\, dt = \int_{\pi/2}^{a} \sqrt{\frac{r^2\cos^2 t}{\sin^2 t}}\, dt = \\ = -r\int_{\pi/2}^{a} \frac{\cos t}{\sin t}\, dt = -r\left[\ln(\sin t)\right]_{\pi/2}^{a} = -r\ln(\sin a).$$ □

**6.75.** Spočtěte objem tělesa vzniklého otáčením omezené plochy, jejíž hranicí je křivka $x^4 - 9x^2 + y^4 = 0$, kolem osy $x$.

**Řešení.** Pokud je $[x, y]$ bodem křivky $x^4 - 9x^2 + y^4 = 0$, zřejmě tato křivka prochází rovněž body $[-x, y]$, $[x, -y]$, $[-x, -y]$. Je tedy

*(2) Jsou-li všechny funkce $f_n(x)$ spojitě diferencovatelné na intervalu $[a, b]$, řada $S(x) = \sum_{n=1}^{\infty} f_n(x)$ konverguje pro nějaké $x_0 \in [a, b]$ a řada $T(x) = \sum_{n=1}^{\infty} f_n'(x)$ konverguje stejnoměrně na $[a, b]$, pak také řada $S(x)$ konverguje a je spojitě diferencovatelná na $[a, b]$ a platí $S'(x) = T(x)$, tj.*

$$\left(\sum_{n=1}^{\infty} f_n(x)\right)' = \sum_{n=1}^{\infty} f_n'(x).$$

*(3) Jsou-li všechny funkce $f_n(x)$ riemannovsky integrovatelné na $[a, b]$ a řada*

$$S(x) = \sum_{n=1}^{\infty} f_n(x)$$

*konverguje stejnoměrně k funkci $S(x)$ na $[a, b]$, je tamtéž integrovatelná i funkce $S(x)$ a platí vztah*

$$\int_a^b \left(\sum_{n=1}^{\infty} f_n(x)\right) dx = \sum_{n=1}^{\infty} \int_a^b f_n(x)\, dx.$$

**6.44. Test stejnoměrné konvergence.** Nejjednodušším způsobem pro zjištění stejnoměrné konvergence posloupnosti funkcí je porovnání s absolutní konvergencí vhodné posloupnosti čísel. Říkává se tomu často *Weierstrassův test*.



Předpokládejme tedy, že máme řadu funkcí $f_n(x)$ na intervalu $I = [a, b]$ a že navíc známe odhad

$$|f_n(x)| \le a_n \in \mathbb{R}$$

pro vhodné reálné konstanty $a_n$ a všechna $x \in [a, b]$. Okamžitě můžeme odhadnout rozdíly částečných součtů

$$s_k(x) = \sum_{n=1}^{k} f_n(x)$$

pro různé indexy $k$. Pro $k > m$ dostáváme

$$|s_k(x) - s_m(x)| = \left|\sum_{n=m+1}^{k} f_n(x)\right| \le \sum_{n=m+1}^{k} |f_n(x)| \le \sum_{n=m+1}^{k} a_k.$$

Pokud je řada (nezáporných) konstant $\sum_{n=1}^{\infty} a_n$ konvergentní, pak bude samozřejmě posloupnost jejích částečných součtů cauchyovská. Právě jsme ale spočetli, že v takovém případě bude posloupnost částečných součtů $s_n(x)$ stejnoměrně cauchyovská.

Díky tvrzení dokázanému před chvílí v 6.41 jsme tedy právě dokázali následující

**Věta** (Weierstrassův test)**.** *Nechť $f_n(x)$ je posloupnost funkcí definovaných na intervalu $[a, b]$ a platí $|f_n(x)| \le a_n \in \mathbb{R}$.*

*Je-li řada čísel $\sum_{n=1}^{\infty} a_n$ konvergentní, pak řada $S(x) = \sum_{n=1}^{\infty} f_n(x)$ konverguje stejnoměrně.*

**6.45. Důsledky pro mocninné řady.** Weierstrassův test je velice užitečný pro diskusi mocninných řad

$$S(x) = \sum_{n=0}^{\infty} a_n(x - x_0)^n$$

se středem v bodě $x_0$.

souměrná vzhledem k oběma osám $x$, $y$. Pro $y = 0$ dostáváme $x^2\,(x-3)\,(x+3) = 0$, tj. osu $x$ protíná hraniční křivka v bodech $[-3,0]$, $[0,0]$, $[3,0]$. V prvním kvadrantu ji pak můžeme vyjádřit jako graf funkce

$$f(x) = \sqrt[4]{9x^2 - x^4}, \quad x \in [0,3].$$

Hledaný objem je proto dvojnásobkem (zde uvažujeme $x > 0$) integrálu

$$\int_0^3 \pi f^2(x)\,dx = \pi \int_0^3 \sqrt{9x^2 - x^4}\,dx.$$

Pomocí substituce $t = \sqrt{9 - x^2}$ ($x\,dx = -t\,dt$) pak snadno spočítáme

$$\int_0^3 \sqrt{9x^2 - x^4}\,dx = \int_0^3 x \cdot \sqrt{9 - x^2}\,dx = -\int_3^0 t^2\,dt = 9,$$

a tak obdržíme výsledek $18\pi$. □

**6.76. Torricelliho trychtýř, 1641.** Nechť část větve hyperboly $xy = 1$ pro $x \geq a$, kde $a > 0$, rotuje kolem osy $x$. Ukažte, že obdržené rotační těleso má konečný objem $V$ a současně nekonečný povrch $S$.

**Řešení.** Víme, že platí

$$V = \pi \int_a^{+\infty} \left(\tfrac{1}{x}\right)^2 dx = \pi \int_a^{+\infty} \tfrac{1}{x^2}\,dx = \pi \left( \lim_{x\to+\infty} -\tfrac{1}{x} - \left(-\tfrac{1}{a}\right)\right) = \tfrac{\pi}{a}$$

a

$$S = 2\pi \int_a^{+\infty} \tfrac{1}{x} \cdot \sqrt{1 + \left(-\tfrac{1}{x^2}\right)^2}\,dx = 2\pi \int_a^{+\infty} \tfrac{\sqrt{x^4+1}}{x^3}\,dx \geq 2\pi \int_a^{+\infty} \tfrac{1}{x}\,dx =$$

$$= 2\pi \left( \lim_{x\to+\infty} \ln x - \ln a \right) = +\infty.$$

Skutečnost, že uvažované těleso (tzv. Torricelliho trychtýř) nelze natřít za pomoci konečného množství barvy, ale lze jej naplnit konečným množstvím kapaliny, se nazývá Torricelliho paradox. Uvědomme si však, že reálný nátěr barvou má nenulovou tloušťku, což jsme při výpočtu nijak nezohlednili. Kdybychom jej kupř. natírali zevnitř, jediná kapka barvy by nepochybně trychtýř nekonečné délky „ucpala“. □

Další příklady na výpočet délek křivek, obsahů rovinných útvarů a objemů částí prostoru naleznete na straně 390.

**6.77. Aplikace integrálního kriteria konvergence.** Nyní se opět vraťme k (číselným) řadám. Díky integrálnímu kriteriu konvergence (viz 6.33) umíme rozhodnout o konvergenci širší třídy řad: Rozhodněte, zda následující sumy konvergují či divergují:

a) $\sum_{n=1}^{\infty} \frac{1}{n \ln n}$,

b) $\sum_{n=1}^{\infty} \frac{1}{n^2}$.



Při našem prvním setkání s mocninnými řadami jsme ukázali v 5.49, že každá taková řada konverguje na $(x_0 - \delta,\ x_0 + \delta)$, kde tzv. poloměr konvergence $\delta \geq 0$ může být také nula nebo $\infty$ (viz také 5.53). Zejména jsme v důkazu věty 5.49 pro ověření konvergence řady $S(x)$ používali srovnání s vhodnou geometrickou posloupností. Podle Weierstrassova testu je proto řada $S(x)$ stejnoměrně konvergentní na každém kompaktním (tj. konečném) intervalu [a,b] uvnitř intervalu $(x_0 - \delta,\ x_0 + \delta)$. Dokázali jsme tedy

**Věta.** *Každá mocninná řada $S(x)$ je ve všech bodech uvnitř svého intervalu konvergence spojitá a spojitě diferencovatelná. Funkce $S(x)$ je také integrovatelná a derivování i integrování lze provádět člen po členu.*

Ve skutečnosti platí také tzv. *Abelova věta*, která říká, že mocninné řady jsou spojité i v hraničních bodech svého definičního oboru (včetně případných nekonečných limit). Tu zde nedokazujeme.

Právě dokázané příjemné vlastnosti mocninných řad zároveň poukazují na hranice jejich použitelnosti při modelování závislostí nějakých praktických jevů nebo procesů. Zejména není možné pomocí mocninných řad dobře modelovat po částech spojité funkce. Jak uvidíme vzápětí, je možné pro konkrétněji vymezené potřeby nacházet lepší sady funkcí $f_n(x)$ než jsou hodnoty $f_n(x) = x^n$. Nejznámějšími příklady jsou Fourierovy řady a tzv. wawelety, které přiblížíme v další kapitole.

**6.46. Laurentovy řady.** V kontextu Taylorových rozvojů se ještě



podívejme na hladkou funkci $f(x) = \mathrm{e}^{-1/x^2}$ z odstavce 6.6. Viděli jsme, že není analytická v nule, protože tam má všechny derivace nulové. Takže zatímco ve všech ostatních bodech $x_0$ je tato funkce dána konvergentní Taylorovou řadou s poloměrem konvergence $r = |x_0|$, v počátku řada konverguje jen v jediném bodě.

Pokud ale do mocninné řady pro $\mathrm{e}^x$ dosadíme za $x$ výraz $-1/x^2$, dostaneme řadu funkcí

$$S(x) = \sum_{n=0}^{\infty} \frac{1}{n!}(-1)^n x^{-2n} = \sum_{n=-\infty}^{0} \frac{(-1)^{|n|}}{|n|!} x^{2n},$$

která bude konvergovat ve všech bodech $x \neq 0$ a dává nám dobrý popis pro chování kolem výjimečného bodu $x = 0$. Podbízí se proto uvažovat následující obecnější řady docela podobné mocninným:

LAURENTOVY ŘADY

Řadu funkcí tvaru

$$S(x) = \sum_{n=-\infty}^{\infty} a_n (x - x_0)^n$$

nazýváme *Laurentova řada se středem v $x_0$*. Řadu nazveme konvergentní, jestliže konvergují samostatně její části s kladnými a zápornými exponenty.

Smysl Laurentových řad je dobře viditelný u racionálních funkcí lomených. Uvažme takovou funkci $S(x) = f(x)/g(x)$ s nesoudělnými polynomy $f$ a $g$ a uvažme kořen $x_0$ polynomu $g(x)$. Je-li násobnost tohoto kořenu $s$, pak vynásobením dostaneme funkci

**Řešení.** Všimněme si nejprve, že ani u jedné z uvažovaných řad neumíme o její konvergenci rozhodnout na základě podílového či odmocninového kriteria (všechny limity $\lim_{n\to\infty} |\frac{a_{n+1}}{a_n}|$ i $\lim_{n\to\infty} \sqrt[n]{a_n}$ jsou rovny 1). Pomocí integrálního kriteria pro konvergenci řad pak dostáváme:

a)

$$\int_1^\infty \frac{1}{x\ln(x)}\,\mathrm{d}x = \int_0^\infty \frac{1}{t}\,\mathrm{d}t = \lim_{\delta\to\infty}[\ln(t)]_0^\delta = \infty,$$

daná řada tedy diverguje.

b)

$$\int_1^\infty \frac{1}{x^2}\,\mathrm{d}x = \lim_{\delta\to\infty}\left[-\frac{1}{x}\right]_1^\delta = 1,$$

a daná řada tedy konverguje. □

**6.78.** Pomocí integrálního kritéria rozhodněte o konvergenci řady

$$\sum_{n=1}^{\infty} \tfrac{1}{(n+1)\ln^2(n+1)}.$$

**Řešení.** Funkce

$$f(x) = \tfrac{1}{(x+1)\ln^2(x+1)}, \quad x \in [1,+\infty)$$

je zjevně na svém definičním oboru kladná a nerostoucí, a proto řada v zadání konverguje, právě když konverguje integrál $\int_1^{+\infty} f(x)\,dx$. Užitím substituce $y = \ln(x+1)$ (kdy je $dy = dx/(x+1)$) můžeme vyčíslit

$$\int_1^{+\infty} \tfrac{1}{(x+1)\ln^2(x+1)}\,dx = \int_{\ln 2}^{+\infty} \tfrac{1}{y^2}\,dy = \tfrac{1}{\ln 2}.$$

Řada tedy konverguje. □

## G. Stejnoměrná konvergence

**6.79.** Konverguje posloupnost funkcí

$$y_n = \mathrm{e}^{\frac{x^4}{4n^2}}, \quad x \in \mathbb{R}, \quad n \in \mathbb{N}$$

stejnoměrně na $\mathbb{R}$?

**Řešení.** Posloupnost $\{y_n\}_{n\in\mathbb{N}}$ bodově konverguje ke konstantní funkci $y = 1$ na $\mathbb{R}$, neboť

$$\lim_{n\to\infty} \mathrm{e}^{\frac{x^4}{4n^2}} = \mathrm{e}^0 = 1, \quad x \in \mathbb{R}.$$

Z vyčíslení

$$y_n\left(\sqrt{2n}\right) = \mathrm{e} > 2 \quad \text{pro každé } n \in \mathbb{N}$$

však vyplývá, že se nejedná o stejnoměrnou konvergenci. (V definici stejnoměrné konvergence postačuje uvážit $\varepsilon \in (0,1)$.) □

$\tilde{S}(x) = S(x)(x-x_0)^s$, která už bude na nějakém okolí bodu $x_0$ analytická a proto můžeme psát

$$S(x) = \frac{a_{-s}}{(x-x_0)^s} + \cdots + \frac{a_{-1}}{x-x_0} + a_0 + a_1(x-x_0) + \cdots = \sum_{n=-s}^{\infty} a_n(x-x_0)^n.$$

Uvažujme nyní odděleně části obecné Laurentovy řady

$$S(x) = S_- + S_+ = \sum_{n=-\infty}^{-1} a_n(x-x_0)^n + \sum_{n=0}^{\infty} a_n(x-x_0)^n.$$

Pro řadu $S_+$ víme z Věty 5.49, že její poloměr konvergence $R$ je dán rovností

$$R^{-1} = \limsup_{n\to\infty} \sqrt[n]{|a_n|}.$$

Když však aplikujeme tutéž úvahu na řadu $S_-$ s dosazenými hodnotami $1/x$ za $x$, zjistíme, že řada $S_-(x)$ konverguje pro $|x-x_0| > r$, kde

$$r^{-1} = \limsup_{n\to\infty} \sqrt[n]{|a_{-n}|}.$$

Tyto úvahy platí bezezbytku i pro komplexní hodnoty $x$ dosazované do našich výrazů.

**Věta.** *Laurentova řada $S(x)$ se středem $x_0$ konverguje pro všechna $x \in \mathbb{C}$ splňující $r < |x-x_0| < R$ a diverguje pro všechna $x$ splňující $|x-x_0| < r$ nebo $|x-x_0| > R$.*

Vidíme tedy, že Laurentova řada nemusí konvergovat ve vůbec žádném bodě, protože klidně můžeme dospět k hodnotám $R < r$. Podíváme-li se ale např. na výše uvedený případ racionálních funkcí lomených rozvíjených do Laurentovy řady v některém z kořenů jmenovatele, pak zjevně je $r = 0$ a tedy, dle očekávání, bude konvergovat skutečně na prstencovém okolí tohoto bodu $x_0$, zatímco $R$ bude v tomto případě dáno právě vzdáleností k dalšímu nejbližšímu kořenu jmenovatele. V případě našeho prvního příkladu, funkce $\mathrm{e}^{-1/x^2}$ je $r = 0$ a $R = \infty$.

**6.47. Numerická přiblížení integrace.** Podobně jako na konci předchozí části textu (viz odstavec 6.17), nyní využijeme Taylorova rozvoje k návrhu co nejlepších a zároveň jednoduchých aproximací integrace. Budeme pracovat s integrálem $I = \int_a^b f(x)dx$ analytické funkce $f(x)$ a rovnoměrným dělením intervalu $[a,b]$ pomocí bodů $a = x_0, x_1, \ldots, x_n = b$ se vzdálenostmi $x_i - x_{i-1} = h > 0$. Body uprostřed intervalů v děleních si označíme $x_{i+1/2}$, hodnoty naší funkce v bodech dělení budeme psát jako $f(x_i) = f_i$.



Příspěvek jednoho dílku dělení k integrálu spočteme pomocí Taylorova rozvoje a předchozí věty 6.45. Záměrně přitom integrujeme symetricky kolem středových hodnot, aby se nám při procesu integrace vzájemně vyrušily derivace lichých stupňů:

$$\int_{-h/2}^{h/2} f(x_{i+1/2}+t)dt = \int_{-h/2}^{h/2}\left(\sum_{n=0}^{\infty}\frac{1}{n!}f^{(n)}(x_{i+1/2})t^n\right)dt = \sum_{k=0}^{\infty}\left(\int_{-h/2}^{h/2}\frac{1}{k!}f^{(k)}(x_{i+1/2})t^k\,dt\right) = \sum_{k=0}^{\infty}\frac{h^{2k+1}}{2^{2k}(2k+1)!}f^{(2k)}(x_{i+1/2}).$$

**6.80.** Určete, zda řada

$$\sum_{n=1}^{\infty} \tfrac{\sqrt{x}\cdot n}{n^4+x^2}$$

stejnoměrně konverguje na intervalu $(0, +\infty)$.

**Řešení.** Při označení

$$f_n(x) = \tfrac{\sqrt{x}\cdot n}{n^4+x^2}, \quad x > 0, \quad n \in \mathbb{N},$$

je

$$f_n'(x) = \tfrac{n(n^4-3x^2)}{2\sqrt{x}(n^4+x^2)^2}, \quad x > 0, \quad n \in \mathbb{N}.$$

Nechť $n \in \mathbb{N}$ je nadále libovolné. Nerovnosti $f_n'(x) > 0$ pro $x \in \left(0, n^2/\sqrt{3}\right)$ a $f_n'(x) < 0$ pro $x \in \left(n^2/\sqrt{3}, +\infty\right)$ implikují, že maximum funkce $f_n$ nastává právě v bodě $x = n^2/\sqrt{3}$. Protože

$$f_n\left(\tfrac{n^2}{\sqrt{3}}\right) = \tfrac{\sqrt[4]{27}}{4n^2} \quad \text{a} \quad \sum_{n=1}^{\infty} \tfrac{\sqrt[4]{27}}{4n^2} = \tfrac{\sqrt[4]{27}}{4} \sum_{n=1}^{\infty} \tfrac{1}{n^2} < +\infty,$$

podle Weierstrassova kritéria řada $\sum_{n=1}^{\infty} f_n(x)$ konverguje stejnoměrně na intervalu $(0, +\infty)$. □

**6.81.** Pro $x \in [-1, 1]$ sečtěte

$$\sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}}{n(n+1)}\, x^{n+1}.$$

**Řešení.** Nejprve upozorněme, že symbolem pro neurčitý integrál budeme označovat jednu konkrétní primitivní funkci (při zachování proměnné), kterou je vhodné chápat jako tzv. funkci horní meze, přičemž dolní mez je nula. Užitím věty o integraci mocninné řady pro $x \in (-1, 1)$ obdržíme

$$\textstyle\sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n(n+1)}\, x^{n+1} = \sum_{n=1}^{\infty} \left( \frac{(-1)^{n+1}}{n} \int x^n\, dx \right) =$$

$$= \boxed{\int \sum_{n=1}^{\infty} \left( \frac{(-1)^{n+1}}{n}\, x^n \right) dx} = \int \textstyle\sum_{n=1}^{\infty} \left( (-1)^{n+1} \int x^{n-1}\, dx \right) dx =$$

$$= \int \left( \int \textstyle\sum_{n=1}^{\infty} (-x)^{n-1}\, dx \right) dx = \int \left( \int 1 - x + x^2 - x^3 + \cdots\, dx \right) dx =$$

$$= \int \left( \int \tfrac{1}{1+x}\, dx \right) dx = \boxed{\int \ln(1+x) + C_1\, dx}.$$

Jelikož

$$\int \sum_{n=1}^{\infty} \left( \frac{(-1)^{n+1}}{n}\, x^n \right) dx = \int \ln(1+x) + C_1\, dx,$$

ze spojitosti uvažovaných funkcí víme, že

$$\sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}}{n}\, x^n = \ln(1+x) + C_1, \qquad x \in (-1, 1).$$

Volba $x = 0$ potom dává $0 = \ln 1 + C_1$, tj. $C_1 = 0$. Dále je

$$\int \ln(1+x)\ dx = \left| \text{ per partes } \right| = \left| \begin{array}{ll} u = \ln(1+x) & u' = \frac{1}{1+x} \\ v' = 1 & v = x \end{array} \right| =$$

$$= x \ln(1+x) - \int \tfrac{x}{1+x}\ dx = x \ln(1+x) - \int 1 - \tfrac{1}{1+x}\ dx =$$

$$= x \ln(1+x) - x + \ln(1+x) + C_2 = (x+1) \ln(1+x) - x + C_2.$$

Velmi jednoduchým numerickým přiblížením integrace na jednom dílku dělení je tzv. *lichoběžníkové pravidlo*, které pro aproximaci využívá plochu lichoběžníka určeného body $[x_i, 0]$, $[x_i, f_i]$, $[0, x_{i+1}]$, $[x_{i+1}, f_{i+1}]$. Tato plocha je

$$P_i = \frac{1}{2}(f_i + f_{i+1})h$$

a celkem tedy integrál $I$ odhadujeme hodnotou

$$I_{\text{lich}} = \sum_{i=0}^{n-1} P_i = \frac{h}{2}(f_0 + 2f_1 + \cdots + 2f_{n-1} + f_n).$$

Srovnáme nyní $I_{\text{lich}}$ s přesnou hodnotou $I$ spočtenou pomocí příspěvků po jednotlivých dílcích dělení. Hodnoty $f_i$ můžeme vyjádřit pomocí prostředních hodnot a derivací $f_{i+1/2}^{(k)}$ takto:

$$f_{i+1/2\pm 1/2} = f_{i+1/2} \pm \frac{h}{2} f_{i+1/2}' + \frac{h^2}{2!2^2} f''(i+1/2) \pm$$
$$\pm \frac{h^3}{3!2^3} f^{(3)}(i+1/2) + \ldots,$$

takže pro příspěvek $P_i$ do odhadu dostáváme

$$P_i = \frac{1}{2}(f_i + f_{i+1})h = h\Big(f_{i+1/2} + \frac{h^2}{2!2^2} f''(i+1/2)\Big) + \mathrm{O}(h^5).$$

Odtud dostáváme odhad chyby $I - I_{\text{lich}}$ na jednom dílku dělení

$$\Delta_i = h\Big(f_{i+1/2} + \frac{h^2}{24} f''_{i+1/2} - f_{i+1/2} - \frac{h^2}{8} f''_{i+1/2} + \mathrm{O}(h^4)\Big) =$$
$$= \frac{h^3}{12} f''_{i+1/2} + \mathrm{O}(h^5).$$

Celková chyba tedy je odhadnuta jako

$$I - I_{\text{lich}} = \frac{1}{12} n h^3 f'' + n\,\mathrm{O}(h^5) = \frac{1}{12}(b-a)h^2 f'' + \mathrm{O}(h^4)$$

kde $f''$ vyjadřuje odhad pro druhou derivaci $f$.

Pokud nám lineární aproximace funkce po jednotlivých dílcích nestačí, dalším pokusem může být aproximace kvadratickým polynomem. K tomu ale budeme potřebovat vždy tři body, takže budeme pracovat s dílky dělení po dvou. Předpokládejme tedy že $n = 2m$ a uvažujme $x_i$ s lichými indexy. Budeme požadovat

$$f_{i+1} = f(x_i + h) = f_i + \alpha h + \beta h^2,$$
$$f_{i-1} = f(x_i - h) = f_i - \alpha h + \beta h^2,$$

což dává (viz podobnost s diferencí pro aproximaci druhé derivace)

$$\beta = \frac{1}{2h^2}(f_{i+1} + f_{i-1} - 2f_i).$$

Plocha přibližného vyjádření integrálu na dvou dílcích dělení mezi $x_{i-1}$ a $x_{i+1}$ je nyní odhadnuta výrazem

$$P_i = \int_{-h}^{h} f_i + \alpha t + \beta t^2\, dt = 2hf_i + \frac{2}{3}\beta h^3 =$$
$$= 2hf_i + \frac{2h}{6}(f_{i+1} + f_{i-1} - 2f_i) =$$
$$= \frac{h}{3}(4f_{i+1} + f_{i-1} - 2f_i).$$

Tomuto postupu se říká *Simpsonovo pravidlo*. Celý integrál je nyní přiblížen výrazem

$$I_{\text{Simp}} = \frac{1}{3} h\Big(f_0 + f_{2n} + 4 \sum_{\text{liché } k} f_k + 2 \sum_{\text{sudé } k} f_k\Big).$$

Protože zadaná řada konverguje v bodě $x = 0$ se součtem 0, analogicky jako pro $C_1$ z

$$0 = 1 \cdot \ln 1 - 0 + C_2$$

vyplývá, že $C_2 = 0$. Celkem tedy získáváme

$$\sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}}{n(n+1)}\, x^{n+1} = (x+1)\,\ln(x+1) - x, \qquad x \in (-1, 1).$$

Navíc podle Abelovy věty (viz 6.45)je součet uvažované řady roven (případné nevlastní) limitě funkce $(x+1)\,\ln(x+1) - x$ v bodech $-1$ a 1. V našem případě jsou obě limity vlastní (v bodě 1 je dokonce funkce spojitá a hodnota limity v bodě 1 je pak rovna funkční hodnotě $2\ln 2 - 1$. Pro výpočet hodnoty limity v bodě $-1$ použijeme L'Hospitalova pravidla:

$$\begin{aligned}\lim_{x\to -1^+} (x+1)\,\ln(x+1) - x &= \lim_{t\to 0^+} t\,\ln t + 1 = \\ &= \lim_{t\to 0^+} \frac{\ln t}{\frac{1}{t}} + 1 = \\ &= \lim_{t\to 0^+} \frac{\frac{1}{t}}{-\frac{1}{t^2}} + 1 = \lim_{t\to 0^+} -t + 1 = 1.\end{aligned}$$

Konvergenci řady v bodech $\pm 1$ lze samozřejmě ověřit přímo. Dokonce lze přímo i odvodit $\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1$ (rozepsáním $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$. □

**6.82. Součet řady.** Pomocí věty 6.41 „o záměně limity a integrálu posloupnosti stejnoměrně konvergentních funkcí" nyní sečteme číselnou řadu

$$\sum_{n=1}^{\infty} \frac{1}{n2^n}.$$

Využijeme toho, že $\int_2^{\infty} \frac{\mathrm{d}x}{x^{n+1}} = \frac{1}{n2^n}$.

**Řešení.** Na intervalu $(2, \infty)$ konverguje řada funkcí $\sum_{n=1}^{\infty} \frac{1}{x^{n+1}}$ stejnoměrně. To plyne například z Weierstrassova kriteria: každá z funkcí $\frac{1}{x^{n+1}}$ je klesající na intervalu $(2, \infty)$, její hodnota tedy nepřevyšuje $\frac{1}{2^{n+1}}$; řada $\sum_{n=1}^{\infty} \frac{1}{2^{n+1}}$ je ovšem konvergentní (jedná se o geometrickou řadu s kvocientem $\frac{1}{2}$. Podle Weierstrassova kriteria tedy řada funkcí $\sum_{n=1}^{\infty} \frac{1}{x^{n+1}}$ tedy konverguje stejnoměrně. Dokonce umíme výslednou funkci explicitně vyjádřit. Její hodnota v libovolném $x \in (2, \infty)$ je hodnotou geometrické řady s kvocientem $\frac{1}{x}$, označíme-li tedy limitu jako $f(x)$, je

$$f(x) = \sum_{n=1}^{\infty} \frac{1}{x^{n+1}} = \frac{1}{x^2}\,\frac{1}{1-\frac{1}{x}} = \frac{1}{x(x-1)}.$$

Obdobným postupem jako výše odvodíme, že celková chyba je odhadnuta výrazem

$$I - I_{\mathrm{Simp}} = \frac{1}{180}(b-a)h^4 f^{(4)} + \mathrm{O}(h^5),$$

kde $f^{(4)}$ představuje odhad pro čtvrtou derivaci funkce $f$.

Závěrem této kapitoly se zastavíme u dalších konceptů integrace. Jako první uvedeme modifikaci Riemannova integrálu, která bude později užitečná v úvahách o pravděpodobnosti a statistice. Ve výkladu vesměs už ale zůstaneme spíše v rovině poznámek a postřehů, zájemce o podrobný výklad bude muset vyhledat jiné zdroje.

**6.48. Riemannův–Stieltjesův integrál.** Při naší představě o integraci jakožto sčítání nekonečně mnoha linearizovaných (nekonečně) malých přírůstků do plochy zadané funkcí $f(x)$ jsme pominuli možnost, že bychom pro různé hodnoty $x$ brali přírůstky různě vážně. To by jistě mohlo být na infinitesimální úrovni zajištěno záměnou diferenciálu $dx$ za $\varphi(x)dx$ pro nějakou vhodnou funkci $\varphi$. Takové chování jsme viděli např. při výpočtu délky parametrizované křivky v prostoru.



Jistě si ale také umíme představit, že v některém bodě $x_0$ je přírůstek do integrované veličiny dán jako $\alpha f(x_0)$ nezávisle na na velikosti přírůstku $x$. Třeba můžeme sledovat pravděpodobnost, že množství promile alkoholu v krvi řidiče při kontrole bude nejvýše $x$. S docela velkou pravděpodobností získáme hodnotu 0, tedy pro jakýkoliv integrální součet musí dílek obsahující nulu přispět i konstantním nenulovým příspěvkem, nezávisle na normě dělení. Takové chování neumíme namodelovat vynásobením diferenciálu $dx$ nějakou reálnou funkcí. Místo toho můžeme zobecnit Riemannův integrál následovně:

Zvolme na konečném intervalu $[a, b]$ reálnou neklesající funkci $g$. Pro každé dělení $\Xi$ s reprezentanty $\xi_i$ a dělícími body

$$a = x_0, x_1, \ldots, x_n = b$$

definujeme *Riemannův–Stieltjesův integrální součet* pro funkci $f(x)$ takto:

$$S_\Xi = \sum_{i=1}^{n} f(\xi_i)\big(g(x_i) - g(x_{i-1})\big).$$

Řekneme pak, že Riemannův–Stieltjesův integrál

$$I = \int_a^b f(x)dg(x)$$

existuje a má hodnotu $I$, jestliže pro každé reálné $\varepsilon > 0$ existuje norma dělení $\delta > 0$ taková, že pro všechna dělení $\Xi$ s normou menší než $\delta$ platí

$$|S_\Xi - I| < \varepsilon.$$

Např., jestliže zvolíme na intervalu $[0, 1]$ za $g(x)$ po částech konstantní funkci s konečně mnoha body nespojitosti $c_1, \ldots, c_k$ a „skoky"

$$\alpha_i = \lim_{x\to c_{i+}} g(x) - \lim_{x\to c_{i-}} g(x)$$

pak Riemannův–Stieltjesův integrál existuje pro každou spojitou $f(x)$ a je roven

$$I = \int_0^1 f(x)dg(x) = \sum_{i=1}^{k} \alpha_i f(c_k).$$

Použitím (6.43) (3) dostáváme

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{1}{n2^n} &= \sum_{n=1}^{\infty}\int_2^{\infty}\frac{\mathrm{d}x}{x^{n+1}} = \\ &= \int_2^{\infty}\left(\sum_{n=1}^{\infty}\frac{1}{x^{n+1}}\right)\mathrm{d}x = \\ &= \int_2^{\infty}\frac{1}{x(x-1)}\,\mathrm{d}x = \\ &= \lim_{\delta\to\infty}\int_2^{\delta}\frac{1}{x-1}-\frac{1}{x}\,\mathrm{d}x = \\ &= \lim_{\delta\to\infty}\left[(\ln(\delta-1)-\ln(\delta)-\ln(1)+\ln 2\right] = \\ &= \lim_{\delta\to\infty}\left[\ln\left(\frac{\delta-1}{\delta}\right)\right]+\ln(2) = \\ &= \ln\left(\lim_{\delta\to\infty}\frac{\delta-1}{\delta}\right)+\ln 2 = \ln 2.\end{aligned}$$

□

**6.83.** Uvažme funkci $f(x)=\sum_{n=1}^{\infty} ne^{-nx}$. Určete

$$\int_{\ln 2}^{\ln 3} f(x)\,\mathrm{d}x.$$

**Řešení.** Obdobně jako v předchozím případě z Weierstrassova kriteria pro stejnoměrnou konvergenci vyplývá, že řada funkcí $\sum_{n=1}^{\infty} ne^{-nx}$ konverguje stejnoměrně na intervalu $(\ln 2, \ln 3)$, neboť každá z funkcí $ne^{-nx}$ je menší než $\frac{n}{2^n}$ na $(\ln 2, \ln 3)$ a řada $\sum_{n=1}^{\infty}\frac{n}{2^n}$ konverguje, což plyne třeba z podílového kriteria pro konvergenci řad:

$$\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right| = \lim_{n\to\infty}\frac{(n+1)2^{-(n+1}}{n2^n} = \lim_{n\to\infty}\frac{1}{2}\frac{n+1}{n} = \frac{1}{2}.$$

Celkem podle (6.43) (3) platí

$$\begin{aligned}\int_{\ln 2}^{\ln 3} f(x)\,\mathrm{d}x &= \int_{\ln 2}^{\ln 3}\sum_{n=1}^{\infty} ne^{-nx} = \\ &= \sum_{n=1}^{\infty}\int_{\ln 2}^{\ln 3} ne^{-nx}\,\mathrm{d}x = \\ &= \sum_{n=1}^{\infty}[-e^{-nx}]_{\ln 2}^{\ln 3} = \sum_{n=1}^{\infty}\left(\frac{1}{2^n}-\frac{1}{3^n}\right) = 1-\frac{1}{2} = \frac{1}{2}.\end{aligned}$$

□

**6.84.** Určete následující limitu (postup výpočtu zdůvodněte):

$$\lim_{n\to\infty}\int_0^{\infty}\frac{\cos\left(\frac{x}{n}\right)}{\left(1+\frac{x}{n}\right)^n}\,\mathrm{d}x.$$

Stejnou technikou, jako jsme používali u Riemannova integrálu, lze i nyní zavést horní a dolní součty a horní a dolní Riemannův–Stieltjesův integrál, které mají tu výhodu, že pro omezené funkce vždy existují a jejich hodnoty splývají, právě když existuje Riemannův–Stieltjesův integrál ve výše uvedeném smyslu.

Již u Riemannova integrálu jsme měli problém s integrovatelností funkcí, které byly „příliš rozeskákané". Technicky pro funkci $g(x)$ na konečném intervalu $[a,b]$ zavádíme její *variaci* vztahem

$$\mathrm{var}_a^b\, g = \sup_{\Xi}\sum_{i=1}^{n}|g(x_i)-g(x_{i-1})|,$$

kde supremum bereme přes všechna dělení $\Xi$ intervalu $[a,b]$. Pokud je supremum nekonečné, říkáme, že $g(x)$ má neomezenou variaci na $[a,b]$, v opačném případě říkáme, že je $g$ funkce s omezenou variací na intervalu $[a,b]$.

Podobně, jak jsme postupovali u Riemannova integrálu, můžeme docela snadno odvodit následující:

**Věta.** *Nechť $f(x)$ a $g(x)$ jsou reálné funkce na konečném intervalu $[a,b]$.*

*(1) Pokud je $g(x)$ neklesající a spojitě diferencovatelná, pak Riemannův integrál nalevo a Riemannův–Stieltjesův integrál napravo existují současně a jejich hodnoty jsou si rovny*

$$\int_a^b f(x)g'(x)dx = \int_a^b f(x)dg(x)$$

*(2) Pokud je $f(x)$ spojitá a $g(x)$ je neklesající funkce s konečnou variací, pak integrál $\int_a^b f(x)dg(x)$ existuje.*

**6.49. Kurzweilův integrál.** 
Posledním zastavením bude modifikace Riemannova integrálu, která napravuje nešťastné chování ve třetím bodu v odstavci 6.37, tj. limity neklesajících posloupností integrovatelných funkcí budou opět integrovatelné. Pak budeme moci i v těchto případech měnit pořadí limitního procesu a integrace, jak tomu bylo u stejnoměrné konvergence.

Všimněme si napřed v čem je jádro problému. Intuitivně bychom měli předpokládat, že hodně malé množiny musí mít velikost nulovou, a tudíž by změny hodnot funkcí na takovýchto množinách neměly ovlivnit integraci. Navíc, spočetné sjednocení takových „pro integraci zanedbatelných" množin by mělo mít opět velikost nulovou. Jistě bychom tedy čekali, že např. množina racionálních čísel uvnitř konečného intervalu bude mít takovouto vlastnost a tedy její charakteristická funkce by měla být integrovatelná a hodnota takového integrálu má být nulová.

Řekneme, že množina $A\subset\mathbb{R}$ má *nulovou míru*, když pro každé $\varepsilon>0$ můžeme najít pokrytí množiny $A$ spočetným systémem otevřených intervalů $J_i$, $i=1,2,\ldots$, takových, že

$$\sum_{i=1}^{\infty} m(J_i) < \varepsilon.$$

V dalším budeme vždy výrokem „funkce $f$ má na množině $B$ danou vlastnost skoro všude" myslet skutečnost, že má $f$ tuto vlastnost ve všech bodech, až na podmnožinu $A\subset B$ míry nula. Např. tedy charakteristická funkce racionálních čísel je skoro všude nulová, po částech spojitá funkce je skoro všude spojitá atd.

Chtěli bychom nyní modifikovat definici Riemannova integrálu tak, abychom uměli při volbě dělení a příslušných Riemannových součtů eliminovat neblahý vliv hodnot integrované funkce

**Řešení.** Určeme nejprve $\lim_{n\to\infty} \frac{\cos(\frac{x}{n})}{(1+\frac{x}{n})^n}$. Posloupnost těchto funkcí konverguje bodově a s využitím 5.43 máme

$$\lim_{n\to\infty} \frac{\cos(\frac{x}{n})}{\left(1+\frac{x}{n}\right)^n} = \frac{1}{\lim\limits_{n\to\infty}\left(1+\frac{x}{n}\right)^n} = \frac{1}{e^x}$$

Lze ukázat, že daná posloupnost konverguje stejnoměrně. Potom podle (6.41)

$$\begin{aligned}\lim_{n\to\infty}\int_0^\infty \frac{\cos\left(\frac{x}{n}\right)}{\left(1+\frac{x}{n}\right)^n}\,\mathrm{d}x &= \int_0^\infty \left[\lim_{n\to\infty}\frac{\cos\left(\frac{x}{n}\right)}{\left(1+\frac{x}{n}\right)^n}\right]\mathrm{d}x = \\ &= \int_0^\infty \frac{1}{e^x} = 1\end{aligned}$$

Ověření stejnoměrné konvergence dané posloupnosti necháváme na čtenáři (podotýkáme jenom, že diskuze je složitější než v předchozích příkladech). □

na předem známé množině míry nula. Nabízí se zkusit zajistit, aby dílky v uvažovaných děleních s reprezentanty měly tu vlastnost, že kolem bodů takovéto množiny budou kontrolovatelně malé.

Kladnou reálnou funkci $\delta$ na konečném intervalu $[a,b]$ nazýváme *kalibr*. Dělení $\Xi$ intervalu $[a,b]$ s reprezentanty $\xi_i$ nazýváme $\delta$–kalibrované, jestliže pro všechna $i$ platí

$$\xi_i - \delta(\xi_i) < x_{i-1} \le \xi_i \le x_i < \xi_i + \delta(\xi_i).$$

Pro další postup je podstatné ověřit, že ke každému kalibru $\delta$ lze najít nějaké $\delta$–kalibrované dělení s reprezentanty. Tomuto tvrzení se říká Cousinovo lemma a lze jej dokázat např. obvyklým postupem opřeným o vlastnosti suprem. Pro daný kalibr $\delta$ na $[a,b]$ si označíme $M$ množinu všech bodů $x \in [a,b]$ takových. že na $[a,x]$ lze $\delta$–kalibrované dělení s reprezentanty najít. Jistě je $M$ neprázdná a ohraničená a má tedy supremum $s$. Kdyby $s \neq b$, pak bychom uměli najít kalibrované dělení s reprezentantem v $s$ a to vede na spor.

Nyní již můžeme zavést zobecnění Riemannova integrálu takto:

**Definice.** Funkce $f$ definovaná na konečném intervalu $[a,b]$ má Kurzweilův integrál

$$I = \int_a^b f(x)\,dx,$$

jestliže pro každé $\varepsilon > 0$ existuje kalibr $\delta$ takový, že pro každé $\delta$–kalibrované dělení s reprezentanty $\Xi$ platí pro příslušný Riemannův součet $S_\Xi$ odhad $|S_\Xi - I| < \varepsilon$.

**6.50. Vlastnosti Kurzweilova integrálu.** Předně si povšimněme,



že jsme při definici Kurzweilova integrálu jen omezili množinu všech dělení, pro které Riemannovy součty bereme v úvahu. Pokud tedy bude naše funkce riemannovsky integrovatelná, musí mít nutně i Kurzweilův integrál a tyto dva integrály jsou si rovny.

Ze stejného důvodu můžeme zopakovat argumentaci ve Větě 6.24 o jednoduchých vlastnostech Riemannova integrálu a opět ověřit, že se stejně chová i integrál Kurzweilův. Zejména je lineární kombinace integrovatelných funkcí $cf(x) + dg(x)$ opět integrovatelná a její integrál je $c\int_a^b f(x)dx + d\int_a^b g(x)dx$ atd. Při důkazu je potřeba jen promyslet drobné modifikace při diskusi zjemněných dělení, která navíc mají být $\delta$–kalibrovaná.

Podobně lze rozšířit pro případ monotonních posloupností bodově konvergentních funkcí argumentaci ověřující, že limity stejnoměrně konvergující posloupnosti integrovatelných funkcí $f_n$ jsou opět integrovatelné a integrálem limity je limita hodnot integrálů $f_n$.

Konečně, Kurzweilův integrál se chová tak, jak bychom si přáli, i vůči množinám s nulovou mírou:

**Věta.** *Uvažme funkci $f$ na intervalu $[a,b]$, která je skoro všude nulová. Pak Kurzweilův integrál $\int_a^b f(x)d(x)$ existuje a je roven nule.*

Důkaz. Jde o pěknou ilustraci myšlenky, že se můžeme zbavit vlivu hodnot na malé množině pomocí chytré volby kalibru. Označme si $M$ příslušnou množinu míry nula, vně které je $f(x) = 0$ a pišme $M_k \subset [a,b]$, $k = 1,\dots,$ pro podmnožinu bodů, pro které je $k-1 < |f(x)| \le k$. Protože má každá z množin $M_k$ nulovou míru, můžeme ji pokrýt spočetným systémem v součtu libovolně malých a po dvou disjunktních otevřených

intervalů $J_{k,i}$. Definujme si nyní kalibr $\delta(x)$ pro $x \in J_{k,i}$ tak, aby celé intervaly $(x - \delta(x), x + \delta(x))$ byly stále obsaženy v $J_{k,i}$. Mimo množinu $M$ pak $\delta$ dodefinujeme libovolně.

Pro $\delta$–kalibrované dělení $\Xi$ intervalu $[a, b]$ pak můžeme odhadnout příslušný Riemannův součet

$$\left|\sum_{i=0}^{n-1} f(\xi_i)(x_{i+1} - x_i)\right| = \left|\sum_{\substack{i=0 \\ \xi_i \in M}}^{n-1} f(\xi_i)(x_{i+1} - x_i)\right| \leq$$

$$\leq \sum_{k=1}^{\infty} \sum_{\substack{i=0 \\ \xi_i \in M_k}}^{n-1} \left|f(\xi_i)\right|(x_{i+1} - x_i) \leq$$

$$\leq \sum_{k=1}^{\infty} k \left( \sum_{\substack{j=0 \\ \xi_i \in M_k}}^{n-1} m(J_{k,j}) \right).$$

Pokud tedy pro předem známé $\varepsilon$ chceme dosáhnout, aby tento odhad byl menší než $\varepsilon$, stačí volit pokrytí intervaly $J_{k,j}$ tak, aby

$$\sum_{j=1}^{\infty} m(J_{k,j}) \leq \frac{\varepsilon}{k2^k}.$$

Pak totiž v posledním výrazu v našem odhadu můžeme dosadit za vnitřní sumu, sečíst geometrickou řadu $\sum_{k=1}^{\infty} 2^{-k}$ a dostaneme právě požadované $\varepsilon$. □

**Důsledek.** *Integrovatelnost dané funkce $f(x)$ ve smyslu Kurzweila ani hodnotu jejího integrálu nezměníme, pozměníme-li hodnoty $f(x)$ na množině míry nula.*

V literatuře lze najít mnoho krásných a užitečných výsledků o integrálech, které připouští záměnu limitních procesů daleko šířeji než je tomu i Riemannova integrálu. Kurzweilův integrál je jednou z možných cest, častější je použití integrálu Lebesgueova a souvislostí s abstraktní teorií míry. Nemáme tu nyní prostor pro další úvahy v těchto směrech.

### H. Doplňující příklady k celé kapitole

*6.85.* Nechť je dána funkce $f$ a bod $z$, přičemž platí

$$f(z) = 0, \quad f'(z) = 0, \quad f''(z) = 0, \quad f^{(3)}(z) = 1.$$

Která z následujících tvrzení:

(a) tečnou ke grafu funkce $f$ v bodě $[z, f(z)]$ je osa $x$;
(b) funkce $f$ není polynomem druhého stupně;
(c) funkce $f$ v bodě $z$ roste;
(d) funkce $f$ nemá v bodě $z$ ostré lokální minimum;
(e) bod $z$ je inflexním bodem funkce $f$

jsou zcela jistě pravdivá? ○

**6.86.** Vyšetřete průběh funkce

$$f(x) = \tfrac{\cos x}{\cos 2x}.$$

**Řešení.** Do definičního oboru náleží všechna $x \in \mathbb{R}$, pro která je $\cos 2x \neq 0$. Rovnice $\cos 2x = 0$ je splněna právě pro

$$2x = \tfrac{\pi}{2} + k\pi,\ k \in \mathbb{Z}, \quad \text{tj.} \quad x = \tfrac{\pi}{4} + \tfrac{k\pi}{2},\ k \in \mathbb{Z}.$$

Jako definiční obor tak obdržíme množinu

$$\mathbb{R} \setminus \left\{ \tfrac{\pi}{4} + \tfrac{k\pi}{2};\ k \in \mathbb{Z} \right\}.$$

Zřejmě je

$$f(-x) = \tfrac{\cos(-x)}{\cos(-2x)} = \tfrac{\cos x}{\cos 2x} = f(x)$$

pro všechna $x$ z definičního oboru, a tudíž je $f$ s definičním oborem symetrickým kolem počátku sudou funkcí, což vyplynulo ze sudosti funkce $y = \cos x$. Když dále uvážíme, že kosinus je periodický s periodou $2\pi$ (tj. $y = \cos 2x$ má periodu $\pi$), dostaneme, že postačuje uvažovat funkci $f$ pro

$$x \in \mathcal{D} := [0, \pi] \setminus \left\{ \tfrac{\pi}{4} + \tfrac{k\pi}{2};\ k \in \mathbb{Z} \right\} = \left[0, \tfrac{\pi}{4}\right) \cup \left(\tfrac{\pi}{4}, \tfrac{3\pi}{4}\right) \cup \left(\tfrac{3\pi}{4}, \pi\right],$$

neboť průběh zadané funkce na celém jejím definičním oboru lze odvodit s použitím toho, že je sudá a periodická s periodou $2\pi$.

Zabývejme se proto pouze body nespojitosti $x_1 = \pi/4$ a $x_2 = 3\pi/4$ a stanovme pro ně příslušné jednostranné limity

$$\lim_{x \to \frac{\pi}{4}-} \tfrac{\cos x}{\cos 2x} = +\infty, \qquad \lim_{x \to \frac{\pi}{4}+} \tfrac{\cos x}{\cos 2x} = -\infty,$$
$$\lim_{x \to \frac{3\pi}{4}-} \tfrac{\cos x}{\cos 2x} = +\infty, \qquad \lim_{x \to \frac{3\pi}{4}+} \tfrac{\cos x}{\cos 2x} = -\infty.$$

Přihlédneme-li ke spojitosti $f$ na intervalu $(\pi/4, 3\pi/4)$, vidíme, že $f$ na tomto intervalu nabývá všech reálných hodnot. Oborem hodnot $f$ je tedy celé $\mathbb{R}$. Rovněž jsme zjistili, že body nespojitosti jsou tzv. druhého druhu, kdy aspoň jedna jednostranná limita je nevlastní (příp. neexistuje). Tím jsme současně dokázali, že přímky $x = \pi/4$ a $x = 3\pi/4$ jsou asymptotami bez směrnice. Kdybychom předchozí výsledky formulovali bez omezení se na interval $[0, \pi]$, tak můžeme např. říci, že ve všech bodech

$$\hat{x}_k = \tfrac{\pi}{4} + \tfrac{k\pi}{2}, \qquad k \in \mathbb{Z}$$

má $f$ nespojitost druhého druhu a že každá přímka

$$x = \tfrac{\pi}{4} + \tfrac{k\pi}{2}, \qquad k \in \mathbb{Z}$$

je asymptotou bez směrnice. Současně z periodičnosti funkce $f$ vyplývá, že jiné asymptoty neexistují. Zvláště nemůže mít žádné asymptoty se směrnicí, ani nemohou existovat (jako nevlastní) limity $\lim_{x\to+\infty} f(x)$, $\lim_{x\to-\infty} f(x)$. Ještě určíme průsečíky s osami. Průsečík $[0, 1]$ s osou $y$ nalezneme vyčíslením $f(0) = 1$. Při hledání průsečíků s osou $x$ uvažujeme rovnici $\cos x = 0, x \in \mathcal{D}$ s jediným řešením $x = \pi/2$. Snadno dále získáme intervaly $[0, \pi/4)$, $(\pi/2, 3\pi/4)$, kde je funkce $f$ kladná, a intervaly $(\pi/4, \pi/2)$, $(3\pi/4, \pi]$, kde je záporná.

Nyní přistoupíme k výpočtu derivace

$$\begin{aligned} f'(x) &= \frac{-\sin x \cos 2x - 2\cos x\,(-\sin 2x)}{\cos^2 2x} = \\ &= \frac{-\sin x\left(\cos^2 x - \sin^2 x\right) + 2\cos x\,(2\sin x \cos x)}{\cos^2 2x} = \\ &= \frac{\sin^3 x + 3\cos^2 x \sin x}{\cos^2 2x} = \frac{\left(\sin^2 x + \cos^2 x + 2\cos^2 x\right)\sin x}{\cos^2 2x} = \\ &= \frac{\left(2\cos^2 x + 1\right)\sin x}{\cos^2 2x},\ x \in \mathcal{D}. \end{aligned}$$

Body, ve kterých je $f'(x) = 0$, jsou řešením rovnice $\sin x = 0, x \in \mathcal{D}$, tj. derivace je nulová v bodech $x_3 = 0, x_4 = \pi$. Z nerovností

$$2\cos^2 x + 1 \geq \cos^2 2x > 0, \quad \sin x > 0, \qquad x \in \mathcal{D} \cap (0, \pi)$$

plyne, že v každém vnitřním bodě množiny $\mathcal{D}$ funkce $f$ roste, a tudíž $f$ roste na každém podintervalu $\mathcal{D}$. Sudost $f$ potom implikuje, že klesá v každém bodě $x \in (-\pi, 0), x \neq -3\pi/4, x \neq -\pi/4$. Funkce má proto ostré lokální extrémy právě v bodech

$$\tilde{x}_k = k\pi, \qquad k \in \mathbb{Z}.$$

Vzhledem k periodičnosti $f$ tyto extrémy jednoznačně popíšeme pozorováním, že pro $x_3 = \tilde{x}_0 = 0$ dostáváme lokální minimum (zopakujme funkční hodnotu $f(0) = 1$) a pro $x_4 = \tilde{x}_1 = \pi$ lokální maximum s funkční hodnotou $f(\pi) = -1$.

Spočítejme druhou derivaci

$$\begin{aligned} f''(x) &= \frac{\left[4\cos x(-\sin x)\sin x + \left(2\cos^2 x + 1\right)\cos x\right]\cos^2 2x - 4\cos 2x(-\sin 2x)\left(2\cos^2 x + 1\right)\sin x}{\cos^4 2x} \\ &= \frac{\left[-4\cos x \sin^2 x + 2\cos^3 x + \cos x\right]\left(\cos^2 x - \sin^2 x\right) - 4(-2\sin x \cos x)\left(2\cos^2 x + 1\right)\sin x}{\cos^3 2x} \\ &= \frac{-6\cos^3 x \sin^2 x + 2\cos^5 x + \cos^3 x + 4\cos x \sin^4 x - \cos x \sin^2 x + 16\sin^2 x \cos^3 x + 8\sin^2 x \cos x}{\cos^3 2x} \\ &= \frac{\left[10\sin^2 x \cos^2 x + 2\cos^4 x + \cos^2 x + 4\sin^4 x + 7\sin^2 x\right]\cos x}{\cos^3 2x}, \qquad x \in \mathcal{D}. \end{aligned}$$

Poznamenejme, že jednoduchými úpravami lze také vyjádřit

$$f''(x) = \frac{\left(3 + 4\cos^2 x \sin^2 x + 8\sin^2 x\right)\cos x}{\cos^3 2x}, \qquad x \in \mathcal{D}$$

nebo

$$f''(x) = \frac{\left(11 - 4\cos^4 x - 4\cos^2 x\right)\cos x}{\cos^3 2x}, \qquad x \in \mathcal{D}.$$

Protože

$$10\sin^2 x \cos^2 x + 2\cos^4 x + \cos^2 x + 4\sin^4 x + 7\sin^2 x > 0, \quad x \in \mathbb{R},$$

resp.

$$3 + 4\cos^2 x \sin^2 x + 8\sin^2 x = 11 - 4\cos^4 x - 4\cos^2 x \geq 3, \quad x \in \mathbb{R},$$

je $f''(x) = 0$ pro jisté $x \in \mathcal{D}$ tehdy a jen tehdy, když $\cos x = 0$. Tomu ale vyhovuje pouze $x_5 = \pi/2 \in \mathcal{D}$. Je vidět, že v tomto bodě mění $f''$ znaménko, tj. jedná se o inflexní bod. Jiný inflexní bod neexistuje (druhá derivace $f''$ je spojitá na $\mathcal{D}$). K dalším změnám znaménka $f''$ dochází v nulových bodech

jmenovatele, které jsme již dříve určili jako body nespojitosti $x_1 = \pi/4$ a $x_2 = 3\pi/4$. Znaménko se tedy mění právě v bodech $x_1, x_2, x_5$, a tak z nerovnosti

$$f''(x) > 0 \quad \text{pro} \quad x \to 0^+$$

vyplývá, že $f$ je konvexní na intervalu $[0, \pi/4)$, konkávní na $(\pi/4, \pi/2]$, konvexní na $[\pi/2, 3\pi/4)$ a konkávní na $(3\pi/4, \pi]$. Konvexnost a konkávnost funkce $f$ na jiných podintervalech je dána její periodičností a následujícím jednoduchým pozorováním. Je-li funkce sudá a konvexní na intervalu $(a, b)$, kde $0 \le a < b$, potom je konvexní rovněž na $(-b, -a)$.

Zbývá jen vyčíslit derivaci (k odhadu rychlosti růstu funkce) v inflexním bodě se ziskem $f'(\pi/2) = 1$. S pomocí všech předchozích výsledků lze již lehce sestrojit graf funkce $f$. □

*6.87.* Vyšetřete celkový průběh funkce

$$f(x) = -\tfrac{x^2}{x+1}, \quad x \in \mathbb{R} \setminus \{-1\}.$$

Tedy určete (má-li smysl):

(a) definiční obor (ten je zadán) a obor hodnot;
(b) případnou sudost, lichost, periodicitu;
(c) body nespojitosti a jejich druh (včetně příslušných jednostranných limit);
(d) průsečíky s osami $x$, $y$;
(e) intervaly, kde je funkce kladná a kde záporná;
(f) limity $\lim_{x\to-\infty} f(x)$, $\lim_{x\to+\infty} f(x)$;
(g) první a druhou derivaci;
(h) kritické a tzv. stacionární body, ve kterých je první derivace nulová (příp. body, ve kterých neexistuje první nebo druhá derivace);
(i) intervaly monotonie;
(j) ostré i neostré lokální a absolutní extrémy;
(k) intervaly, kde je funkce konvexní a kde konkávní;
(l) inflexní body;
(m) asymptoty bez směrnice a se směrnicí;
(n) hodnoty funkce $f$ a její derivace $f'$ ve „významných“ bodech;
(o) graf.

○

*6.88.* Vyšetřete průběh funkce

$$f(x) = \tfrac{1-x^3}{x^2}.$$

Vyšetřením průběhu funkce $f$ se (nejen v tomto příkladu) rozumí udat definiční obor, obor hodnot a případnou lichost, sudost, periodicitu; spočítat limity

$$\lim_{x\to-\infty} f(x) \quad \text{a} \quad \lim_{x\to+\infty} f(x),$$

jestliže existují; určit body nespojitosti a jejich druh včetně příslušných jednostranných limit (pokud existují), nulové body (pokud existují) a intervaly, kde je funkce kladná a kde záporná; stanovit první (a druhou, je-li potřeba) derivaci a *intervaly, na kterých funkce roste, klesá, či je konstantní*; nalézt stacionární (kritické) body a všechny *lokální extrémy* (pokud existují); určit *inflexní body* a *intervaly, kde je funkce konvexní a kde konkávní*; vypočítat hodnoty ve význačných bodech (tj. vyčíslit funkci

ve stacionárních a v inflexních bodech, pomůže-li to při kreslení grafu, a uvést průsečíky s osami, existují-li); načrtnout její *graf* s *asymptotami*“. ○

*6.89.* Vyšetřete průběh funkce

$$\frac{x}{\ln(x)},$$

a načrtněte její graf. ○

**Řešení.**

i) Nejprve určíme definiční obor funkce: $\mathbb{R}^+ \setminus \{1\}$.

ii) Nalezneme intervaly monotónnosti funkce: nejprve nalezneme nulové body derivace:

$$f'(x) = \frac{\ln(x) - 1}{\ln^2(x)} \quad = \quad 0$$

Tato rovnice má kořen $e$. Dále vidíme, že $f'(x)$ je na intervalu $(0, 1)$ i $(1, e)$ záporná, tedy je $f(x)$ na intervalu $(0, 1)$ i na $(1, e)$ klesající, dále je $f'(x)$ na intervalu $(e, \infty)$ kladná a tedy $f(x)$ rostoucí. Má tedy funkce $f$ jediný extrém v bodě $e$ a to minimum. (také bychom o tom mohli rozhodnout pomocí znaménka druhé derivace funkce $f$ v bodě $e$, je totiž $f^{(2)}(e) > 0$)

iii) Určíme inflexní body:

$$f^{(2)}(x) = \frac{2 - \ln(x)}{x \ln^3(x)} = 0$$

Tato rovnice má kořen $e^2$, který musí být inflexním bodem (extrém to již být nemůže vzhledem k předchozímu bodu).

iv) Asymptoty. Funkce má asymptotu přímku $x = 1$. Dále hledejme asymptoty s konečnou směrnicí $k$:

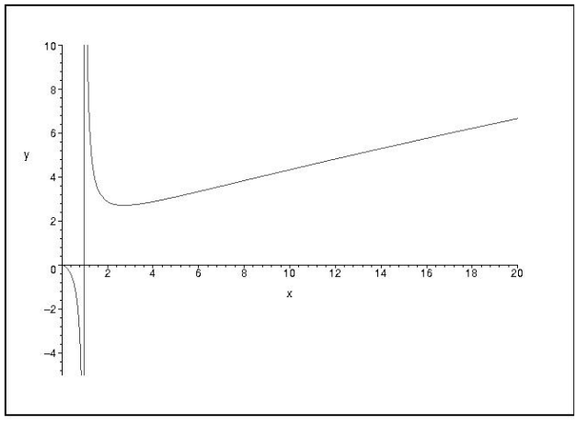
$$k = lim_{x\to\infty} \frac{\frac{x}{\ln(x)}}{x} = \lim_{x\to\infty} \frac{1}{\ln(x)} = 0.$$

Pokud asymptota existuje, má tedy směrnici 0. Pokračujme tedy ve výpočtu

$$\lim_{x\to\infty} \frac{x}{\ln(x)} - 0 \cdot x = \lim_{x\to\infty} x = \infty,$$

a protože limita není konečná, asymptota s konečnou směrnicí neexistuje.

Průběh funkce:



□

*6.90.* Vyšetřete průběh funkce

$$f(x) = \tfrac{x^3-3x^2+3x+1}{x-1}.$$

○

*6.91.* Vyšetřete průběh funkce

$$f(x) = \sqrt[3]{x}\,\mathrm{e}^{-x}.$$

○

*6.92.* Vyšetřete průběh funkce

$$f(x) = \operatorname{arctg} \tfrac{x}{2-x}.$$

○

*6.93.* Vyšetřete průběh funkce $\frac{\ln x}{x}$, mimo jiné nalezněte extrémy, inflexní body, asymptoty a načrtněte její graf. ○

*6.94.* Vyšetřete průběh funkce, mimo jiné nalezněte extrémy, inflexní body, asymptoty.

$$\ln(x^2 - 3x + 2) + x.$$

○

*6.95.* Vyšetřete průběh funkce, mimo jiné nalezněte extrémy, inflexní body a asymptoty.

$$(x^2 - 2)e^{x^2-1}.$$

○

*6.96.* Vyšetřete průběh funkce, mimo jiné nalezněte extrémy, inflexní body a asymptoty.

$$\ln(2x^2 - x - 1).$$

○

*6.97.* Vyšetřete průběh funkce, mimo jiné nalezněte extrémy, inflexní body a asymptoty.

$$\frac{x^2 - 2}{x - 1}.$$

○

*6.98.* Použitím základních vzorců určete libovolnou primitivní funkci k funkci

(a) $y = \sqrt{x\sqrt{x\sqrt{x}}}, \quad x \in (0, +\infty)$;
(b) $y = (2^x + 3^x)^2, \quad x \in \mathbb{R}$;
(c) $y = \frac{1}{\sqrt{4-4x^2}}, \quad x \in (-1, 1)$;
(d) $y = \frac{\cos x}{1+\sin x}, \quad x \in \left(-\frac{\pi}{2}, \frac{3\pi}{2}\right)$.

○

*6.99.* Využijte derivací funkcí $y = \operatorname{tg} x$ a $y = \operatorname{cotg} x$ k nalezení neurčitých integrálů funkcí

(a) $y = \operatorname{cotg}^2 x, \quad x \in (0, \pi)$;
(b) $y = \frac{1}{\sin^2 x \, \cos^2 x}, \quad x \in \left(0, \frac{\pi}{2}\right)$.

○

*6.100.* Uveďte primitivní funkci k funkci

$$y = \mathrm{e}^x + \frac{3}{\sqrt{4-x^2}}$$

na intervalu $(-2, 2)$. ○

*6.101.* Určete

$$\int \frac{x^3}{1+x^4}\, dx, \quad x \in \mathbb{R}.$$

○

*6.102.* Stanovte

$$\int \frac{4}{x^2-2x+3}\, dx, \quad x \in \mathbb{R}.$$

○

*6.103.* Pro $x \in (0, 1)$ vypočtěte

$$\int \left( \frac{x^2+1}{x(x^2-1)} + \frac{3}{\sqrt{4-4x^2}} + 4\sin x - 5\cos x \right) dx\,.$$

○

*6.104.* Vyjádřete neurčité integrály

(a) $\int \operatorname{arctg} x \, dx, \quad x \in \mathbb{R}$;
(b) $\int \frac{\ln x}{x}\, dx, \quad x > 0$

pomocí integrační metody per partes. ○

*6.105.* Opakovaným užitím pravidla per partes pro všechna $x \in \mathbb{R}$ vypočtěte

(a) $\int x^2 \sin x \, dx$;
(b) $\int x^2 \, \mathrm{e}^x \, dx$.

○

**6.106.** Určete integrály

a) $\int \frac{\mathrm{d}x}{\sin^2(x)-\cos^2(x)}$,
b) $\int x^2 \sqrt{2x+1}\, \mathrm{d}x$.

**Řešení.** Pro výpočet prvního z integrálů zvolíme substituci $t = \operatorname{tg} x$, kterou lze často s výhodou uplatnit.

$$\begin{aligned}
&\int \frac{\mathrm{d}x}{\sin^2(x) - \cos^2(x)} = \\
&= \left| \begin{array}{l} t = \operatorname{tg} x \\ dt = \frac{1}{\cos^2 x}\,\mathrm{d}x = (1 + \operatorname{tg}^2(x))\,\mathrm{d}x = (1 + t^2)\,\mathrm{d}x \\ \sin^2(x) = \frac{\operatorname{tg}^2(x)}{1+\operatorname{tg}^2(x)} = \frac{t^2}{1+t^2} \\ \cos^2(x) = \frac{1}{1+\operatorname{tg}^2(x)} = \frac{1}{1+t^2} \end{array} \right| = \\
&= \int \frac{1}{t^2 - 1}\,\mathrm{d}t = \frac{1}{2}\int \frac{1}{t-1} - \frac{1}{2}\int \frac{1}{t+1} = \\
&= \frac{1}{2}\ln\left(\frac{\operatorname{tg}(x) - 1}{\operatorname{tg}(x) + 1}\right) + C.
\end{aligned}$$

Nyní určeme druhý integrál:

$$\begin{aligned}
&\int x^2\sqrt{2x+1}\,\mathrm{d}x = \\
&= \left| \begin{array}{ll} u = x^2 & u' = 2x \\ v' = \sqrt{2x+1} & v = \frac{1}{3}(2x+1)^{\frac{3}{2}} \end{array} \right| = \\
&= \frac{1}{3}x^2(2x+1)^{\frac{3}{2}} - \frac{4}{3}\int x^2\sqrt{2x+1}\,\mathrm{d}x - \frac{2}{9}(2x+1)^{\frac{3}{2}} + C,
\end{aligned}$$

což můžeme chápat jako rovnici, kde neznámou je hledaný integrál. Převedením na jednu stranu pak

$$\begin{aligned}
&\int x^2\sqrt{2x+1}\,\mathrm{d}x = \\
&= \frac{1}{7}x^2(2x+1)^{\frac{3}{2}} - \frac{2}{7}\int x\sqrt{2x+1} = \\
&\quad = \left| \begin{array}{ll} u = x & u' = 1 \\ v' = \sqrt{2x+1} & v = \frac{1}{3}\sqrt{2x+1} \end{array} \right| = \\
&= \frac{1}{7}x^2(2x+1)^{\frac{3}{2}} - \frac{2}{7}\left(\frac{1}{3}x\sqrt{2x+1} - \frac{1}{3}\int (2x+1)^{\frac{3}{2}}\,\mathrm{d}x\right) = \\
&= \frac{1}{7}x^2(2x+1)^{\frac{3}{2}} - \frac{2}{21}x\sqrt{2x+1} + \frac{2}{105}(2x+1)^{\frac{5}{2}} = \\
&= \frac{1}{7}x^2(2x+1)^{\frac{3}{2}} - \frac{2}{35}x(2x+1)^{\frac{3}{2}} + \frac{2}{105}(2x+1)^{\frac{3}{2}} + C.
\end{aligned}$$

□

*6.107.* Například integrací per partes určete

$$\int x\ln^2 x\ dx$$

pro $x > 0$. ○

*6.108.* Pomocí metody per partes spočtěte

$$\int \left(2 - x^2\right)\mathrm{e}^x\,dx$$

na celé reálné ose. ○

*6.109.* Integrujte

(a) $\int (2x+5)^{10}\,dx, \quad x \in \mathbb{R}$;
(b) $\int \frac{1}{x\ln^2 x}\,dx, \quad x > 0$;
(c) $\int \mathrm{e}^{-x^3}x^2\,dx, \quad x \in \mathbb{R}$;

(d) $\int 15\,\frac{\arcsin^2 x}{\sqrt{1-x^2}}\,dx, \quad x \in (-1,1)$;
(e) $\int \frac{\ln x}{x}\,dx, \quad x > 0$;
(f) $\int \frac{\operatorname{arctg}\sqrt{x}}{\sqrt{x}(1+x)}\,dx, \quad x > 0$;
(g) $\int \frac{e^x}{e^{2x}+3}\,dx, \quad x \in \mathbb{R}$;
(h) $\int \sin\sqrt{x}\,dx, \quad x > 0$

aplikací substituční metody. ○

**6.110.** Vypočtěte

$$\int \frac{2x^4+2x^2-5x+1}{x\left(x^2-x+1\right)^2}\,dx, \qquad x \neq 0.$$

**Řešení.** Platí

$$\begin{aligned}
&\int \frac{2x^4+2x^2-5x+1}{x\left(x^2-x+1\right)^2}\,dx = \int \frac{dx}{x} + \int \frac{x+3}{x^2-x+1}\,dx + \int \frac{x-6}{\left(x^2-x+1\right)^2}\,dx = \\
&= \ln|x| + \tfrac{1}{2}\int \frac{2x-1}{x^2-x+1}\,dx + \tfrac{7}{2}\int \frac{dx}{x^2-x+1} + \tfrac{1}{2}\int \frac{2x-1}{(x^2-x+1)^2}\,dx - \\
&\quad - \tfrac{11}{2}\int \frac{dx}{(x^2-x+1)^2} = \left|\begin{array}{c} t = x^2-x+1 \\ dt = (2x-1)\,dx \end{array}\right| = \ln|x| + \\
&+ \tfrac{1}{2}\ln\left(x^2-x+1\right) + \tfrac{7}{2}\int \frac{dx}{\left(x-\frac{1}{2}\right)^2+\frac{3}{4}} + \tfrac{1}{2}\int \frac{dt}{t^2} - \tfrac{11}{2}\int \frac{dx}{\left[\left(x-\frac{1}{2}\right)^2+\frac{3}{4}\right]^2} = \\
&= \ln\left|x\sqrt{x^2-x+1}\right| + \tfrac{14}{3}\int \frac{dx}{\left(\frac{2x-1}{\sqrt{3}}\right)^2+1} - \frac{1}{2t} - \tfrac{88}{9}\int \frac{dx}{\left[\left(\frac{2x-1}{\sqrt{3}}\right)^2+1\right]^2} = \\
&= \left|\begin{array}{c} u = \frac{2x-1}{\sqrt{3}} \\ du = \frac{2}{\sqrt{3}}\,dx \end{array}\right| = \ln\left|x\sqrt{x^2-x+1}\right| + \tfrac{7\sqrt{3}}{3}\int \frac{du}{u^2+1} - \frac{1}{2(x^2-x+1)} - \\
&- \tfrac{44\sqrt{3}}{9}\int \frac{du}{\left[u^2+1\right]^2} = \ln\left|x\sqrt{x^2-x+1}\right| + \tfrac{7\sqrt{3}}{3}\operatorname{arctg} u - \frac{1}{2(x^2-x+1)} - \\
&\quad - \tfrac{44\sqrt{3}}{9}\left(\tfrac{1}{2}\operatorname{arctg} u + \tfrac{1}{2}\,\frac{u}{u^2+1}\right) + C = \ln\left|x\sqrt{x^2-x+1}\right| + \\
&+ \tfrac{7\sqrt{3}}{3}\operatorname{arctg}\tfrac{2x-1}{\sqrt{3}} - \tfrac{22\sqrt{3}}{9}\operatorname{arctg}\tfrac{2x-1}{\sqrt{3}} - \frac{1}{2(x^2-x+1)} - \tfrac{22\sqrt{3}}{9}\,\frac{\frac{2x-1}{\sqrt{3}}}{\left(\frac{2x-1}{\sqrt{3}}\right)^2+1} + \\
&\qquad + C = \ln\left|x\sqrt{x^2-x+1}\right| - \tfrac{\sqrt{3}}{9}\operatorname{arctg}\tfrac{2x-1}{\sqrt{3}} - \tfrac{1}{3}\,\frac{11x-4}{x^2-x+1} + C.
\end{aligned}$$

□

*6.111.* Pro $x \in (0,1)$ pomocí vhodných substitucí převeďte integrály

$$\int x^2\sqrt{\frac{x}{1-x}}\,dx\,; \quad \int \frac{dx}{(x-1)\sqrt{x^2+x+1}}$$

na integrály racionálních lomených funkcí. ○

*6.112.* Pro $x \in (-\pi/2, \pi/2)$ vypočtěte

$$\int \frac{dx}{1+\sin^2 x}$$

pomocí substituce $t = \operatorname{tg} x$. ○

*6.113.* Libovolným způsobem určete

$$\int \frac{\sqrt{x}}{\sqrt{x}+1}\,dx\,, \quad x > 0.$$

○

*6.114.* Spočtěte

(a) $\int x^n \ln x\,dx, \quad x > 0,\ n \neq -1$;
(b) $\int \frac{x}{1+x^4}\,dx, \quad x \in \mathbb{R}$.

○

**6.115.** Pro $x > 0$ stanovte

(a) $\int \frac{(2+5x)^3}{\sqrt[4]{x^3}}\,dx$;

(b) $\int \frac{\sqrt[3]{1+\sqrt[4]{x}}}{\sqrt{x}}\,dx$;

(c) $\int \frac{1}{\sqrt[4]{1+x^4}}\,dx$.

**Řešení.** Všechny tři zadané integrály jsou tzv. binomické, tj. lze je zapsat jako

$$\int x^m (a+bx^n)^p\,dx \quad \text{pro jistá čísla } a, b \in \mathbb{R},\ m, n, p \in \mathbb{Q}.$$

Binomické integrály se tradičně řeší aplikací substituční metody. Pokud $p \in \mathbb{Z}$ (nikoli nutně $p < 0$), volí se substituce $x = t^s$, kde $s$ je společný jmenovatel čísel $m$ a $n$; pokud $\frac{m+1}{n} \in \mathbb{Z}$ a $p \notin \mathbb{Z}$, klade se $a + bx^n = t^s$, kde $s$ je jmenovatel čísla $p$; a pokud $\frac{m+1}{n} + p \in \mathbb{Z}$ ($p \notin \mathbb{Z}$, $\frac{m+1}{n} \notin \mathbb{Z}$), zavádí se $a + bx^n = t^s x^n$, kde $s$ je jmenovatel $p$. V těchto třech případech je potom zaručen přechod k integrování racionální lomené funkce.

Snadno tak vypočítáme

(a)

$$\int \frac{(2+5x)^3}{\sqrt[4]{x^3}}\,dx = \int x^{-\frac{3}{4}}(2+5x)^3\,dx = \left|\begin{array}{c} p \in \mathbb{Z} \\ x = t^4 \\ dx = 4t^3\,dt \end{array}\right| = 4\int \left(2+5t^4\right)^3\,dt =$$
$$= 4\int \left(8 + 60t^4 + 150t^8 + 125t^{12}\right)dt = 4\left(8t + 12t^5 + \tfrac{50}{3}t^9 + \tfrac{125}{13}t^{13}\right) + C =$$
$$= 4\left(8\sqrt[4]{x} + 12\sqrt[4]{x^5} + \tfrac{50}{3}\sqrt[4]{x^9} + \tfrac{125}{13}\sqrt[4]{x^{13}}\right) + C;$$

(b)

$$\int \frac{\sqrt[3]{1+\sqrt[4]{x}}}{\sqrt{x}}dx = \int x^{-\frac{1}{2}}\left(1+x^{\frac{1}{4}}\right)^{\frac{1}{3}}dx = \left|\begin{array}{c} p \notin \mathbb{Z},\ \frac{m+1}{n} \in \mathbb{Z} \\ 1 + x^{\frac{1}{4}} = t^3 \\ x = (t^3-1)^4 \\ dx = 12t^2\left(t^3-1\right)^3\,dt \end{array}\right| = 12\int t^3\left(t^3-1\right)\,dt =$$
$$= 12\int t^6 - t^3\,dt = 12\left(\tfrac{t^7}{7} - \tfrac{t^4}{4}\right) + C = 12\sqrt[3]{(1+\sqrt[4]{x})^4}\left(\tfrac{1+\sqrt[4]{x}}{7} - \tfrac{1}{4}\right) + C;$$

(c)

$$\int \frac{1}{\sqrt[4]{1+x^4}}\,dx = \int \left(1+x^4\right)^{-\frac{1}{4}}dx = \left|\begin{array}{c} p \notin \mathbb{Z},\ \frac{m+1}{n} \notin \mathbb{Z},\ \frac{m+1}{n} + p \in \mathbb{Z} \\ 1 + x^4 = t^4x^4 \\ x = \left(t^4-1\right)^{-\frac{1}{4}} \\ dx = -t^3\left(t^4-1\right)^{-\frac{5}{4}}\,dt \end{array}\right| = -\int \tfrac{t^2}{t^4-1}dt =$$
$$= -\int \tfrac{t^2}{(t-1)(t+1)(t^2+1)}\,dt = -\tfrac{1}{4}\int\left(\tfrac{1}{t-1} - \tfrac{1}{t+1} + \tfrac{2}{t^2+1}\right)dt =$$
$$= -\tfrac{1}{4}\left(\ln|t-1| - \ln|t+1| + 2\operatorname{arctg} t\right) + C =$$
$$= -\tfrac{1}{4}\left[\ln\frac{\sqrt[4]{\frac{1}{x^4}+1}-1}{\sqrt[4]{\frac{1}{x^4}+1}+1} + 2\operatorname{arctg}\left(\sqrt[4]{\tfrac{1}{x^4}+1}\right)\right] + C\,.$$

□

**6.116.** Pro $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ integrujte

(a) $\int \frac{\sin^3 x}{1+4\cos^2 x+3\sin^2 x}\,dx$;

(b) $\int \frac{1}{1+\sin^2 x}\,dx$;

(c) $\int \frac{1}{2-\cos x}\,dx$.

**Řešení.** Integrály ve tvaru $\int f(\sin x, \cos x)\, dx$ pro jistou racionální lomenou funkci $f$ se obvykle řeší substituční metodou. Je-li $f(\sin x, -\cos x) = -f(\sin x, \cos x)$, volí se $t = \sin x$; je-li $f(-\sin x, \cos x) = -f(\sin x, \cos x)$, volí se $t = \cos x$; a je-li $f(-\sin x, -\cos x) = f(\sin x, \cos x)$, pak $t = \operatorname{tg} x$. Jestliže neplatí žádný z uvedených vztahů, používá se substituce $t = \operatorname{tg} \frac{x}{2}$. Ukážeme si to na zadaných integrálech.

Případ (a). Ve jmenovateli je

$$1 + 4\cos^2 x + 3\sin^2 x = 4 + \cos^2 x$$

a v čitateli pouze funkce sinus v liché mocnině, tj. substituce $t = \cos x$, kdy je $dt = -\sin x\, dx$, umožňuje nahradit všechny siny a kosiny, a tak obdržet

$$\int \frac{\sin^3 x}{1+4\cos^2 x+3\sin^2 x}\, dx = \int \frac{\sin x\left(1-\cos^2 x\right)}{4+\cos^2 x}\, dx = \int \frac{-\left(1-t^2\right)}{4+t^2}\, dt = \int \left(1 - \frac{5}{4+t^2}\right) dt =$$
$$= t - \frac{5}{2}\operatorname{arctg}\frac{t}{2} + C = \cos x - \frac{5}{2}\operatorname{arctg}\frac{\cos x}{2} + C.$$

Případ (b). Neboť je sinus (i kosinus) v sudé mocnině, v rámci substituce $t = \operatorname{tg} x$ provedeme nahrazení

$$\sin^2 x = \frac{t^2}{1+t^2}, \quad \cos^2 x = \frac{1}{1+t^2}, \quad dx = \frac{1}{1+t^2}\, dt,$$

čímž získáme

$$\int \frac{dx}{1+\sin^2 x} = \int \frac{\frac{1}{1+t^2}}{1+\frac{t^2}{1+t^2}}\, dt = \int \frac{1}{1+2t^2}\, dt = \frac{\sqrt{2}}{2}\operatorname{arctg}\left(\sqrt{2}t\right) + C = \frac{\sqrt{2}}{2}\operatorname{arctg}\left(\sqrt{2}\operatorname{tg} x\right) + C.$$

Případ (c). Nyní použijeme univerzální substituci $t = \operatorname{tg}\frac{x}{2}$, kdy je

$$\sin x = \frac{2t}{1+t^2}, \quad \cos x = \frac{1-t^2}{1+t^2}, \quad dx = \frac{2}{1+t^2}\, dt.$$

S její pomocí určíme

$$\int \frac{dx}{2-\cos x} = \int \frac{\frac{2}{1+t^2}}{2-\frac{1-t^2}{1+t^2}}\, dt = 2\int \frac{dt}{1+3t^2} = \frac{2\sqrt{3}}{3}\operatorname{arctg}\left(\sqrt{3}t\right) + C = \frac{2\sqrt{3}}{3}\operatorname{arctg}\left(\sqrt{3}\operatorname{tg}\frac{x}{2}\right) + C\,.$$

□

*6.117.* Proveďte naznačené dělení polynomů

$$\frac{2x^5-x^4+3x^2-x+1}{x^2-2x+4}$$

pro $x \in \mathbb{R}$. ○

*6.118.* Vyjádřete funkci

$$y = \frac{3x^4+2x^3-x^2+1}{3x+2}$$

jako součet polynomu a ryze lomené racionální funkce. ○

*6.119.* Rozložte racionální lomený výraz

(a) $\frac{4x^2+13x-2}{x^3+3x^2-4x-12}$;

(b) $\frac{2x^5+5x^3-x^2+2x-1}{x^6+2x^4+x^2}$

na součet parciálních zlomků. ○

*6.120.* Vyjádřete funkci

$$y = \frac{2x^3+6x^2+3x-6}{x^4-2x^3}$$

ve tvaru parciálních zlomků. ○

*6.121.* Rozložte výraz

$$\frac{7x^2-10x+37}{x^3-3x^2+9x+13}$$

na parciální zlomky. ○

*6.122.* Vyjádřete racionální lomenou funkci

$$y = \frac{-5x+2}{x^4-x^3+2x^2}$$

ve tvaru součtu parciálních zlomků. ○

*6.123.* Rozložte na parciální zlomky funkci

$$y = \frac{1}{x^3(x+1)}.$$

○

*6.124.* Uveďte tvar rozkladu na parciální zlomky racionální lomené funkce

$$y = \frac{2x^2-114}{(x-2)\,x^2\,(3x^2+x+4)^2}.$$

Neurčité koeficienty nepočítejte! ○

*6.125.* Upravte funkci

$$y = \frac{x^4+6x^2+x-2}{x^4-2x^3}$$

na součet polynomu a ryze lomené racionální funkce $Q$. Získanou funkci $Q$ poté vyjádřete ve tvaru součtu parciálních zlomků. ○

*6.126.* Napište primitivní funkci racionální lomené funkce

(a) $y = \frac{3}{x-2}, \quad x \neq 2;$
(b) $y = -\frac{2}{(x-2)^3}, \quad x \neq 2.$

○

*6.127.* Vyjádřete

$$\int \frac{3x+5}{x^2+4x+8}\,dx, \quad x \in \mathbb{R}.$$

○

*6.128.* Vypočtěte neurčitý integrál funkce

$$y = \frac{1}{(x^2+x+1)^2}, \quad x \in \mathbb{R}.$$

○

*6.129.* Určete

$$\int \frac{dx}{x^3+1}, \quad x \neq -1.$$

○

*6.130.* Integrujte

$$\int \frac{1}{x^3-1}\,dx\,, \quad x \neq 1.$$

○

*6.131.* Spočtěte integrál

$$\int \frac{x^3}{(x-1)(x-2)^2}\,dx\,, \quad x \in \mathbb{R} \setminus \{1, 2\}.$$

○

*6.132.* Pro $x \in \left(0, \frac{\pi}{2}\right)$ vypočítejte

(a) $\int \sin^3 x \, \cos^4 x \, dx$;
(b) $\int \frac{1+\cos^2 x}{1+\cos 2x}\,dx$;
(c) $\int 2\sin^2 \frac{x}{2}\,dx$;
(d) $\int \cos^2 x \, dx$;
(e) $\int \cos^5 x \, \sqrt{\sin x}\,dx$;
(f) $\int \frac{dx}{\sin^2 x \, \cos^4 x}$;
(g) $\int \frac{dx}{\sin^3 x}$;
(h) $\int \frac{dx}{\sin x}$ .

○

*6.133.* Nechť je dána funkce $y = |\,x\,|$ na intervalu $I = [-1, 1]$ a dělení

$$\Xi_n = \left(-1, -\tfrac{n-1}{n}, \ldots, -\tfrac{1}{n}, 0, \tfrac{1}{n}, \ldots, \tfrac{n-1}{n}, 1\right)$$

intervalu $I$ pro libovolné $n \in \mathbb{N}$. Určete $S_{\Xi_n,\,\sup}$ a $S_{\Xi_n,\,\inf}$ (tedy horní a dolní Riemannův součet odpovídající danému dělení).

Na základě tohoto výsledku rozhodněte, zda je funkce $y = |\,x\,|$ na $[-1, 1]$ integrovatelná (v Riemannově smyslu). ○

*6.134.* Vyčíslete

$$\lim_{n\to\infty} \frac{\sqrt{1+\frac{1}{n}}+\sqrt{1+\frac{2}{n}}+\cdots+\sqrt{1+1}}{n}.$$

○

*6.135.* Kolik existuje různých primitivních funkcí k funkci $y = \cos(\ln x)$ na intervalu $(0, 10)$? ○

*6.136.* Zavedťe funkci $f$ na intervalu $I = [0, 1]$ tak, aby k ní na $I$ neexistovala primitivní funkce. ○

*6.137.* Pomocí Newtonova integrálu vyčíslete

(a) $\int_0^{\pi} \sin x \; dx$;

(b) $\int_0^{1} \operatorname{arctg} x \; dx$;

(c) $\int_{-\pi/4}^{3\pi/4} \frac{\cos x}{1+\sin x} \; dx$;

(d) $\int_{1/\mathrm{e}}^{\mathrm{e}} |\ln x| \, dx$.

○

*6.138.* Spočtěte

$$\int_1^2 \frac{x}{\sqrt{1+x^2}} \; dx.$$

○

*6.139.* Pro libovolná reálná čísla $a < b$ určete

$$\int_a^b \operatorname{sgn} x \; dx.$$

Připomeňme, že $\operatorname{sgn} x = 1$, je-li $x > 0$; $\operatorname{sgn} x = -1$, je-li $x < 0$; a $\operatorname{sgn} 0 = 0$. ○

*6.140.* Vyčíslete určitý integrál

$$\int_0^1 \frac{x^3}{1+x^4} \; dx.$$

○

*6.141.* Např. opakovaným užitím pravidla per partes spočítejte

$$\int_0^{\pi/2} \mathrm{e}^{2x} \cos x \; dx.$$

○

*6.142.* Stanovte

$$\int_{-1}^{1} x^2 \, \mathrm{e}^{-x} \, dx.$$

○

*6.143.* Vyčíslete integrál

$$\int_{-1}^{1} \frac{x}{\sqrt{5-4x}}\,dx$$

za pomoci substituční metody. ○

*6.144.* Vypočtěte

(a) $\int_{1}^{e^8} \frac{dx}{x\sqrt{1+\ln x}}$;

(b) $\int_{0}^{\ln 2} \frac{x}{e^x}\,dx$.

○

*6.145.* Které z kladných čísel

$$p := \int_{0}^{\pi/2} \cos^7 x\,dx, \quad q := \int_{0}^{\pi} \cos^2 x\,dx$$

je větší? ○

*6.146.* Určete znaménka těchto tří čísel (hodnot integrálů)

$$a := \int_{-2}^{2} x^3\,2^x\,dx; \quad b := \int_{0}^{\pi} \cos x\,dx; \quad c := \int_{0}^{2\pi} \frac{\sin x}{x}\,dx.$$

○

*6.147.* Seřaďte čísla

$$A := \int_{0}^{\pi/2} \cos x\,\sin^2 x\,dx, \quad B := \int_{0}^{\pi/2} \sin^2 x\,dx, \quad C := \int_{-1}^{1} -x^5\,5^x\,dx,$$

$$D := \int_{2\pi}^{10} \frac{x^2+2}{x^6+4}\,dx + \int_{\pi}^{2\pi} \frac{x^2+2}{x^6+4}\,dx + \int_{10}^{\pi} \frac{x^2+2}{x^6+4}\,dx$$

podle velikosti. ○

*6.148.* Uvážením geometrického významu určitého integrálu stanovte

(a) $\int_{-2}^{2} |\,x-1\,|\,dx$;

(b) $\int_{-0,10}^{0,10} \operatorname{tg} x\,dx$;

(c) $\int_{0}^{2\pi} \sin x\,dx$.

○

*6.149.* Vypočtěte $\int_{-1}^{1} |\,x\,|\,dx$. ○

*6.150.* Určete

$$\int_{-1}^{1} x^5\,\sin^2 x\,dx.$$

○

*6.151.* S chybou menší než 1/10 přibližně vyčíslete

$$\int_{1}^{2} \left(x - \frac{\cos^{10} x}{10}\right) \ln x\,dx\,.$$

○

*6.152.* Vyjádřete bez symbolů derivace a integrace výraz

$$\left(\int_{x^2}^{a} 3t^2 \cos t \; dt\right)'$$

s proměnnou $x \in \mathbb{R}$ a reálnou konstantou $a$, je-li derivováno podle $x$. ○

*6.153.* Spočtěte neurčitý integrál

$$\int \frac{1}{x^4 + 3x^3 + 5x^2 + 4x + 2}\,\mathrm{d}x.$$

○

*6.154.* Vypočtěte integrál

$$\int_{\frac{\pi}{4}}^{\frac{\pi}{2}} \frac{\sin t}{1 - \cos^2 t}\,\mathrm{d}t.$$

○

*6.155.* Vypočtěte integrál

$$\int_0^{\ln 2} \frac{\mathrm{d}x}{e^{2x} - 3e^x}.$$

○

*6.156.* Vypočtěte:

(i) $\int_0^{\frac{\pi}{2}} \sin x \sin 2x \,\mathrm{d}x$,

(ii) $\int \sin^2 x \sin 2x \,\mathrm{d}x$.

○

*6.157.* Vyčíslete nevlastní integrál

(a) $\int_{-\infty}^{+\infty} \frac{dx}{1+x^2}$;

(b) $\int_0^{+\infty} \frac{dx}{x}$;

(c) $\int_0^4 \frac{2x^2+\sqrt{x}}{x}\,dx$;

(d) $\int_{-1}^{1} \ln|x|\,dx$.

○

*6.158.* Určete

$$\int_0^{3\pi/2} \frac{\cos x}{1+\sin x}\,dx.$$

○

*6.159.* Spočítejte nevlastní integrál

$$\int_{-\infty}^{+\infty} \frac{1}{x^2+x+1}\,dx\,.$$

○

*6.160.* Vyčíslete

$$\int_{-\infty}^{+\infty} \frac{e^x}{e^{2x}+e^x+1}\,dx\,.$$

○

*6.161.* Užitím substituční metody vypočtěte

$$\int_{-\infty}^{0} x\,e^{-x^2}\,dx\,; \quad \int_{0}^{\infty} \frac{e^{-\frac{1}{x}}}{x^2}\,dx\,.$$

○

*6.162.* Vyčíslete integrály

$$\int_0^1 \frac{e^{-\sqrt{x}}}{\sqrt{x}}\,dx; \quad \int_1^4 \frac{e^{-\sqrt{x}}}{\sqrt{x}}\,dx; \quad \int_4^{+\infty} \frac{e^{-\sqrt{x}}}{\sqrt{x}}\,dx.$$

○

*6.163.* Uveďte hodnoty $\alpha \in \mathbb{R}$, pro něž

(a) $\int_1^{+\infty} \frac{dx}{x^\alpha} \in \mathbb{R}$;

(b) $\int_0^1 \frac{dx}{x^\alpha} \in \mathbb{R}$;

(c) $\int_{-\infty}^{+\infty} \sin \alpha x\ dx \in \mathbb{R}$.

○

*6.164.* Pro jaká $p, q \in \mathbb{R}$ je integrál

$$\int_2^{+\infty} \frac{dx}{x^p \ln^q x}$$

konečný? ○

*6.165.* Rozhodněte, zda platí

(a) $\int_{-\infty}^{+\infty} \frac{dx}{x^2+3} \in \mathbb{R}$;

(b) $\int_{-\infty}^{+\infty} \frac{dx}{x^2-3} \in \mathbb{R}$;

(c) $\int_1^{+\infty} \frac{1+2\sin^3 x}{x^5+x^3+1}\,dx \in \mathbb{R}$.

○

*6.166.* Vyčíslete $\cos \frac{\pi}{10}$ s chybou menší než $10^{-5}$. ○

*6.167.* Pro konvergentní řadu

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{\sqrt{n}+100}$$

odhadněte chybu aproximace jejího součtu částečným součtem $s_{9999}$. ○

*6.168.* Bez počítání derivací uveďte Taylorův polynom 4. stupně se středem v bodě $x_0 = 0$ funkce

$$f(x) = \cos x - 2\sin x - \ln(1+x), \quad x \in (-1, 1).$$

Poté rozhodněte, zda je graf funkce $f$ v okolí bodu $[0, 1]$ nad tečnou, pod tečnou. ○

*6.169.* Z Taylorova rozvoje se středem v počátku funkce $y = \sin x$ získejte pomocí derivace Taylorův rozvoj funkce $y = \cos x$. ○

*6.170.* Najděte analytickou funkci, jejíž Taylorova řada je

$$x - \tfrac{1}{3}x^3 + \tfrac{1}{5}x^5 - \tfrac{1}{7}x^7 + \cdots,$$

přičemž $x \in [-1, 1]$. ○

*6.171.* Ze znalosti součtu geometrické řady odvoďte Taylorovu řadu funkce

$$y = \tfrac{1}{5+2x}$$

se středem v počátku. Poté určete její poloměr konvergence. ○

*6.172.* Rozviňte funkci

$$y = \tfrac{1}{3-2x}, \quad x \in \left(-\tfrac{3}{2}, \tfrac{3}{2}\right)$$

v Taylorovu řadu se středem v počátku. ○

*6.173.* Rozviňte do mocninné řady funkci $\cos^2(x)$ v bodě $\pi/4$ a určete pro která $x \in \mathbb{R}$ tato řada konverguje. ○

*6.174.* Funkci $y = \mathrm{e}^x$ definovanou na celé reálné přímce vyjádřete jako nekonečný polynom se členy tvaru $a_n(x-1)^n$ a funkci $y = 2^x$ definovanou na $\mathbb{R}$ vyjádřete jako nekonečný polynom se členy $a_n x^n$. ○

*6.175.* Nalezněte funkci $f$, k níž pro $x \in \mathbb{R}$ konverguje posloupnost funkcí

$$f_n(x) = \tfrac{n^2x^3}{n^2x^2+1}, \quad n \in \mathbb{N}.$$

Je tato konvergence stejnoměrná na $\mathbb{R}$? ○

*6.176.* Konverguje řada

$$\sum_{n=1}^{\infty} \tfrac{n\,x}{n^4+x^2}, \quad \text{kde} \quad x \in \mathbb{R},$$

stejnoměrně na celé reálné ose? ○

*6.177.* Z Taylorova rozvoje se středem v počátku funkce $y = \sin x$ získejte pomocí derivace Taylorův rozvoj funkce $y = \cos x$. ○

*6.178.* Odhadněte

(a) kosinus deseti stupňů s přesností alespoň $10^{-5}$;

(b) určitý integrál $\int_0^{1/2} \frac{dx}{x^4+1}$ s přesností alespoň $10^{-3}$.

○

*6.179.* Určete mocninný rozvoj se středem v bodě $x_0 = 0$ funkce

$$f(x) = \int_0^x \mathrm{e}^{t^2}\,dt, \quad x \in \mathbb{R}.$$

○

*6.180.* Najděte analytickou funkci, jejíž Taylorova řada je

$$x - \tfrac{1}{3}x^3 + \tfrac{1}{5}x^5 - \tfrac{1}{7}x^7 + \cdots,$$

přičemž $x \in [-1, 1]$. ○

*6.181.* Ze znalosti součtu geometrické řady odvoďte Taylorovu řadu funkce

$$y = \tfrac{1}{5+2x}$$

se středem v počátku. Poté určete její poloměr konvergence. ○

*6.182.* Nechť je pohyb tělesa (dráha hmotného bodu) popsán(a) funkcí

$$s(t) = -(t-3)^2 + 16, \quad t \in [0, 7]$$

v jednotkách m, s. Stanovte

(a) počáteční (tj. v čase $t = 0$ s) rychlost tělesa;

(b) čas a polohu, ve kterých má těleso nulovou rychlost;

(c) rychlost a zrychlení tělesa v čase $t = 4$ s.

Doplňme, že rychlost je derivace dráhy a zrychlení je derivace rychlosti. ○

## Řešení cvičení

*6.4.* $\frac{2\sin x}{\cos^3 x}$.

*6.5.* $p^{(5)}(x) = 12 \cdot 5!$; $p^{(6)}(x) = 0$.

*6.6.* $2^{12}\,\mathrm{e}^{2x} + \cos x$.

*6.7.* $f^{(26)}(x) = -\sin x + 2^{26}\,\mathrm{e}^{2x}$.

*6.15.* $\frac{-x^3}{3(1+x)^3}$.

*6.16.* $\frac{\pi}{4} + \frac{1}{2}(x-1) - \frac{1}{4}(x-1)^2 + \frac{1}{12}(x-1)^3$.

*6.17.* (a) $1 + \frac{x^2}{2}$; (b) $1 - \frac{x^2}{2}$; (c) $x - \frac{x^3}{3}$; (d) $x + \frac{x^3}{3}$; (e) $x + x^2 + \frac{x^3}{3}$.

*6.18.* $2(x-1) - (x-1)^2 + \frac{2}{3}(x-1)^3 - \frac{1}{2}(x-1)^4$.

*6.19.* $x - \frac{x^3}{6}$; $\sin 1^\circ \approx \frac{\pi}{180} - \frac{\pi^3}{6\cdot 180^3}$; $\lim_{x\to 0+} \frac{x\ \sin x - x^2}{x^4} = -\frac{1}{6}$.

*6.20.* $\sum_{k=0}^{n} \frac{2^k}{k!}\,x^k$, $n \geq 8$, $n \in \mathbb{N}$.

*6.21.* $(x-1)^3 + 3(x-1)^2 + (x-1) + 4$.

*6.26.*

$$\sum_{i=0}^{\infty} (-1)^n \frac{2^{2n-1}}{(2n)!} x^{2n},$$

konverguje pro libovolné reálné $x$.

*6.27.*

$$\sum_{n=1}^{\infty} (-1)^{n+1} \frac{2^{2n-1}}{(2n)!} x^{2n},$$

konverguje pro libovolné reálné $x$.

*6.28.*

$$f(x) = \sum_{n=1}^{\infty} \frac{3(-1)^{n+1}}{n} x^n,$$

konverguje pro $x \in (-1, 1]$.

*6.29.* Je dobré si uvědomit, že rozvíjíme $\frac{1}{2}\ln(x)$.

$$f(x) = \sum_{i=0}^{\infty} (-1)^{i+1} \frac{1}{2i} (x-1)^i,$$

Konverguje na intervalu $(0, 2]$.

*6.31.* $\left(-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$.

*6.32.* Konvexní je na intervalech $(-\infty, 0)$ a $(0, 1/2)$; konkávní na intervalu $(1/2, +\infty)$. Má pouze jednu asymptotu, a to přímku $y = \pi/4$ (v $\pm\infty$).

*6.33.* (a) $y = 0$ v $-\infty$; (b) $x = 2$ – bez směrnice, $y = 1$ v $\pm\infty$.

*6.34.* $y = 0$ pro $x \to \pm\infty$.

*6.35.* $y = \ln 10$, $y = x + \ln 3$.

*6.67.* $\frac{1}{1-a}$ pro $a \in (0, 1)$, $\infty$ jinak.

*6.85.* Všechna.

*6.87.* Oborem hodnot je $(-\infty, 0] \cup [4, +\infty)$. Funkce $f$ není lichá, sudá ani periodická. Má jediný bod nespojitosti, a to $x_0 = -1$, přičemž

$$\lim_{x\to -1+} f(x) = -\infty, \qquad \lim_{x\to -1-} f(x) = +\infty.$$

Funkce protíná osu $x$ pouze v počátku. Je kladná pro $x < -1$ a nekladná pro $x > -1$. Lehce lze ukázat, že

$$\lim_{x\to -\infty} f(x) = +\infty, \qquad \lim_{x\to +\infty} f(x) = -\infty;$$

$$f'(x) = -\frac{x^2+2x}{(x+1)^2}, \quad f''(x) = -\frac{2}{(x+1)^3}, \quad x \in \mathbb{R} \setminus \{-1\}.$$

Odtud plyne, že $f$ roste na intervalech $[-2,-1)$, $(-1,0]$ a klesá na intervalech $(-\infty,-2]$, $[0,+\infty)$. Ve stacionárním bodě $x_1=0$ nabývá ostrého lokálního maxima a ve stacionárním bodě $x_2=-2$ má ostré lokální minimum $y_2=4$. Je konvexní na intervalu $(-\infty,-1)$, konkávní na intervalu $(-1,+\infty)$. Nemá inflexní bod. Přímka $x=-1$ je asymptotou bez směrnice. Asymptotou se směrnicí v $\pm\infty$ je přímka $y=-x+1$. Dodejme např. $f(-3)=9/2$, $f'(-3)=-3/4$, $f(1)=-1/2$, $f'(1)=-3/4$.

*6.88.* Funkce je definována i spojitá na $\mathbb{R}\setminus\{0\}$. Není lichá, sudá ani periodická. Je záporná právě na intervalu $(1,+\infty)$. Jediným průsečíkem grafu s osami je bod $[1,0]$. V počátku má $f$ tzv. nespojitost druhého druhu a jejím oborem hodnot je $\mathbb{R}$, neboť

$$\lim_{x\to 0} f(x)=+\infty,\qquad \lim_{x\to+\infty} f(x)=-\infty,\qquad \lim_{x\to-\infty} f(x)=+\infty.$$

Platí

$$f'(x)=-\tfrac{x^3+2}{x^3},\quad x\in\mathbb{R}\setminus\{0\},$$
$$f''(x)=\tfrac{6}{x^4},\quad x\in\mathbb{R}\setminus\{0\}.$$

Jediným stacionárním bodem je $x_1=-\sqrt[3]{2}$. Funkce $f$ roste na intervalu $[x_1,0)$, klesá na intervalech $(-\infty,x_1]$, $(0,+\infty)$. V bodě $x_1$ má tudíž lokální minimum $y_1=3/\sqrt[3]{4}$. Inflexní body daná funkce nemá. Je konvexní na celém svém definičním oboru. Asymptotou bez směrnice je přímka $x=0$, přímka $y=-x$ je pak asymptotou se směrnicí v $\pm\infty$.

*6.90.* Funkce je definována i spojitá na $\mathbb{R}\setminus\{1\}$. Není lichá, sudá ani periodická. Průsečíky grafu $f$ s osami jsou body $\left[1-\sqrt[3]{2},0\right]$ a $[0,-1]$. V bodě $x_0=1$ má funkce $f$ nespojitost druhého druhu a jejím oborem hodnot je $\mathbb{R}$, což bezprostředně plyne z limit

$$\lim_{x\to 1-} f(x)=-\infty,\qquad \lim_{x\to 1+} f(x)=+\infty,\qquad \lim_{x\to\pm\infty} f(x)=+\infty.$$

Po úpravě

$$f(x)=(x-1)^2+\tfrac{2}{x-1},\quad x\in\mathbb{R}\setminus\{1\},$$

není obtížné spočítat

$$f'(x)=2\,\tfrac{(x-1)^3-1}{(x-1)^2},\quad x\in\mathbb{R}\setminus\{1\},$$
$$f''(x)=2\,\tfrac{(x-1)^3+2}{(x-1)^3},\quad x\in\mathbb{R}\setminus\{1\}.$$

Jediným stacionárním bodem je $x_1=2$. Funkce $f$ roste na intervalu $[2,+\infty)$, klesá na intervalech $(-\infty,1)$, $(1,2]$. V bodě $x_1$ tudíž nabývá hodnoty lokálního minima $y_1=3$. Je konvexní na intervalech $\left(-\infty,1-\sqrt[3]{2}\right)$, $(1,+\infty)$ a konkávní na intervalu $\left(1-\sqrt[3]{2},1\right)$. Bod $x_2=1-\sqrt[3]{2}$ je tak inflexním bodem. Přímka $x=1$ je asymptotou bez směrnice. Asymptoty se směrnicí daná funkce nemá.

*6.91.* Funkce je definována i spojitá na celém $\mathbb{R}$. Není lichá, sudá ani periodická. Nabývá kladných hodnot na kladné poloose, záporných na záporné. Průsečíkem grafu $f$ s osami je pouze bod $[0,0]$. Snadno se určí derivace

$$f'(x)=\tfrac{\mathrm{e}^{-x}}{3\sqrt[3]{x^2}}-\sqrt[3]{x}\,\mathrm{e}^{-x},\quad x\in\mathbb{R}\setminus\{0\},\qquad f'(0)=+\infty,$$
$$f''(x)=\sqrt[3]{x}\,\mathrm{e}^{-x}-\tfrac{2\mathrm{e}^{-x}}{3\sqrt[3]{x^2}}-\tfrac{2\mathrm{e}^{-x}}{9\sqrt[3]{x^5}},\quad x\in\mathbb{R}\setminus\{0\}.$$

Jediným nulovým bodem první derivace je bod $x_0=1/3$. Funkce $f$ roste na intervalu $(-\infty,1/3]$ a klesá na intervalu $[1/3,+\infty)$. V bodě $x_0$ má proto absolutní maximum $y_0=1/\sqrt[3]{3\mathrm{e}}$. Neboť $\lim_{x\to-\infty} f(x)=-\infty$, jejím oborem hodnot je $(-\infty,y_0]$. Inflexní body jsou

$$x_1=\tfrac{1-\sqrt{3}}{3},\quad x_2=0,\quad x_3=\tfrac{1+\sqrt{3}}{3},$$

přičemž funkce $f$ je konvexní na intervalech $(x_1,x_2)$, $(x_3,+\infty)$, konkávní na intervalech $(-\infty,x_1)$, $(x_2,x_3)$. Jedinou asymptotou je přímka $y=0$ v $+\infty$, tj. $\lim_{x\to+\infty} f(x)=0$.

*6.92.* Funkce je definována i spojitá na $\mathbb{R}\setminus\{2\}$. Není lichá, sudá ani periodická. Je kladná právě na intervalu $(0,2)$. Jediným průsečíkem grafu funkce $f$ s osami je bod $[0,0]$. V bodě $x_0=2$ nastává tzv. skok o velikosti $\pi$, jak vyplývá z limit

$$\lim_{x\to 2-} f(x) = \tfrac{\pi}{2}, \quad \lim_{x\to 2+} f(x) = -\tfrac{\pi}{2}.$$

Platí

$$f'(x) = \tfrac{1}{x^2-2x+2}, \quad x \in \mathbb{R} \setminus \{2\},$$
$$f''(x) = \tfrac{2\,(1-x)}{(x^2-2x+2)^2}, \quad x \in \mathbb{R} \setminus \{2\}.$$

První derivace nemá nulový bod. Funkce $f$ proto roste v každém bodě svého definičního oboru. Neboť

$$\lim_{x\to-\infty} f(x) = -\tfrac{\pi}{4}, \quad \lim_{x\to+\infty} f(x) = -\tfrac{\pi}{4},$$

oborem hodnot je množina $(-\pi/2, \pi/2) \setminus \{-\pi/4\}$. Funkce $f$ je konvexní na intervalu $(-\infty, 1)$, konkávní na intervalech $(1, 2)$, $(2, +\infty)$. Bod $x_1 = 1$ je tedy inflexním bodem, přičemž $f(1) = \pi/4$. Jedinou asymptotou je přímka $y = -\pi/4$ v $\pm\infty$.

*6.93.* Def. obor $\mathbb{R}^+$, globální maximum $x = e$, infl. bod $x = \sqrt{e^3}$, rostoucí na int $(0, e)$, klesající na $(e, \infty)$, konkávní $(0, \sqrt{e^3}$, konvexní $(\sqrt{e^3}, \infty)$, asymptoty $x = 0$ a $y = 0$, $\lim_{x\to 0} f(x) = -\infty$, $\lim_{x\to\infty} f(x) = 0$.

*6.94.* Def. obor $\mathbb{R} \setminus [1, 2]$. Lokální maximum $x = \frac{1-\sqrt{5}}{2}$, na celém definičním oboru konkávní, asymptoty $x = 1$, $x = 2$.

*6.95.* Def. obor $\mathbb{R}$. Lokální minima v $-1$, 1, maximum v 0. Funkce sudá. Inflexní body $\pm\frac{1}{\sqrt{2}}$, bez asymptot.

*6.96.* Def. obor $\mathbb{R} \setminus [-\frac{1}{2}, 1]$. Glob. extrémy nemá. Bez inflexních bodů, asymptoty $x = -\frac{1}{2}$, $x = 1$.

*6.97.* Def. obor $\mathbb{R} \setminus \{1\}$. Bez extrémů. Bez infl. bodů, na int. $(-\infty, 1)$ konvexní, $(1, \infty)$ konkávní, Asymptota bez směrnice $x = 1$. Asymptota se směrnicí $y = x + 1$.

*6.98.* (a) $\frac{8}{15}\, x\sqrt[8]{x^7}$; (b) $\frac{4^x}{\ln 4} + 2\frac{6^x}{\ln 6} + \frac{9^x}{\ln 9}$; (c) $\frac{\arcsin x}{2}$; (d) $\ln(1 + \sin x)$.

*6.99.* (a) $-\operatorname{cotg} x - x + C$; (b) $\operatorname{tg} x - \operatorname{cotg} x + C$.

*6.100.* $\mathrm{e}^x + 3\arcsin\frac{x}{2}$.

*6.101.* $\frac{1}{4}\ln\left(1 + x^4\right) + C$.

*6.102.* $2\sqrt{2}\operatorname{arctg}\frac{x-1}{\sqrt{2}} + C$.

*6.103.* $\ln\left|\frac{x^2-1}{x}\right| + \frac{3}{2}\arcsin x - 4\cos x - 5\sin x + C$.

*6.104.* (a) $x\operatorname{arctg} x - \frac{\ln(1+x^2)}{2} + C$; (b) $\frac{\ln^2 x}{2} + C$.

*6.106.* (a) $-x^2\cos x + 2x\sin x + 2\cos x + C$; (b) $\mathrm{e}^x\left(x^2 - 2x + 2\right) + C$.

*6.107.* $\frac{x^2}{4}\left(2\ln^2 x - 2\ln x + 1\right) + C$.

*6.108.* $\left(2x - x^2\right)\mathrm{e}^x + C$.

*6.109.* (a) $\frac{(2x+5)^{11}}{22} + C$; (b) $-\frac{1}{\ln x} + C$; (c) $-\frac{1}{3}\,\mathrm{e}^{-x^3} + C$; (d) $5\arcsin^3 x + C$; (e) $\frac{\ln^2 x}{2} + C$; (f) $\operatorname{arctg}^2\sqrt{x} + C$; (g) $\frac{\sqrt{3}}{3}\operatorname{arctg}\left(\frac{\sqrt{3}}{3}\,\mathrm{e}^x\right) + C$; (h) $2\sin\sqrt{x} - 2\sqrt{x}\,\cos\sqrt{x} + C$.

*6.111.* Např. $1 - x = t^2 x$ dává $\int \frac{-2}{(1+t^2)^4}\,dt$; a $\sqrt{x^2+x+1} = x + y$ vede na $\int \frac{2\,dy}{y^2+2y-2}$.

*6.112.* $\frac{\sqrt{2}}{2}\operatorname{arctg}\left(\sqrt{2}\operatorname{tg} x\right) + C$.

*6.113.* $x - 2\sqrt{x} + 2\ln\left(1 + \sqrt{x}\right) + C$.

*6.114.* (a) $\frac{x^{n+1}}{n+1}\ln x - \frac{x^{n+1}}{(n+1)^2} + C$; (b) $\frac{\operatorname{arctg} x^2}{2} + C$.

*6.117.* $2x^3 + 3x^2 - 2x - 13 + \frac{-19x+53}{x^2-2x+4}$.

*6.118.* $x^3 - \frac{1}{3}x + \frac{2}{9} + \frac{5}{9(3x+2)}$.

*6.119.* (a) $\frac{2}{x-2} + \frac{3}{x+2} - \frac{1}{x+3}$; (b) $\frac{2}{x} - \frac{1}{x^2} + \frac{1}{x^2+1} + \frac{x}{(x^2+1)^2}$.

*6.120.* $\frac{5}{x-2} + \frac{3}{x^3} - \frac{3}{x}$.

*6.121.* $\frac{3}{x+1} + \frac{4x-2}{x^2-4x+13}$.

*6.122.* $\frac{1}{x^2} - \frac{2}{x} + \frac{2x-3}{x^2-x+2}$.

*6.123.* $\frac{1}{x} - \frac{1}{x^2} + \frac{1}{x^3} - \frac{1}{x+1}$.

*6.124.* $\frac{A}{x-2} + \frac{B}{x^2} + \frac{C}{x} + \frac{Dx+E}{(3x^2+x+4)^2} + \frac{Fx+G}{3x^2+x+4}$.

*6.125.* $1 + \frac{1}{x^3} - \frac{3}{x} + \frac{5}{x-2}$.

*6.126.* (a) $3 \ln |x-2|$; (b) $\frac{1}{(x-2)^2}$.

*6.127.* $\frac{3}{2} \ln\left(x^2+4x+8\right) - \frac{1}{2} \operatorname{arctg} \frac{x+2}{2} + C$.

*6.128.* $\frac{4}{3\sqrt{3}} \operatorname{arctg} \frac{2x+1}{\sqrt{3}} + \frac{2x+1}{3\left(x^2+x+1\right)} + C$.

*6.129.* $\frac{1}{6} \ln \frac{(x+1)^2}{x^2-x+1} + \frac{\sqrt{3}}{3} \operatorname{arctg} \frac{2x-1}{\sqrt{3}} + C$.

*6.130.* $\frac{1}{3} \ln|x-1| - \frac{1}{6} \ln\left(x^2+x+1\right) - \frac{1}{\sqrt{3}} \operatorname{arctg} \frac{2x+1}{\sqrt{3}} + C$.

*6.131.* $\ln\left(|x-1|\,(x-2)^4\right) - \frac{8}{x-2} + x + C$.

*6.132.* (a) $\frac{\cos^7 x}{7} - \frac{\cos^5 x}{5} + C$;

(b) $\frac{\operatorname{tg} x}{2} + \frac{x}{2} + C$;

(c) $x - \sin x + C$;

(d) $\frac{x}{2} + \frac{\sin 2x}{4} + C$;

(e) $\frac{2}{3} \sin^{\frac{3}{2}} x - \frac{4}{7} \sin^{\frac{7}{2}} x + \frac{2}{11} \sin^{\frac{11}{2}} x + C$;

$\frac{\operatorname{tg}^3 x}{3} + 2 \operatorname{tg} x - \frac{1}{\operatorname{tg} x} + C$;

(g) $\frac{1}{2} \ln\left|\operatorname{tg} \frac{x}{2}\right| - \frac{\cos x}{2 \sin^2 x} + C$;

(h) $\ln\left|\operatorname{tg} \frac{x}{2}\right| + C$.

*6.133.* $S_{\Xi_n,\,\sup} = \frac{n+1}{n}$, $S_{\Xi_n,\,\inf} = \frac{n-1}{n}$; ano, je.

*6.134.* $\int_1^2 \sqrt{x}\,dx = \frac{2}{3}\left(2\sqrt{2}-1\right)$.

*6.135.* Nekonečně mnoho.

*6.136.* Např. funkce $f$ může nabývat hodnoty 1 v racionálních bodech intervalu $I$ a být nulová v iracionálních bodech.

*6.137.* (a) 2; (b) $\frac{\pi}{4} - \frac{\ln 2}{2}$; (c) $2 \ln\left(1+\sqrt{2}\right)$; (d) $2 - \frac{2}{\mathrm{e}}$.

*6.138.* $\sqrt{5} - \sqrt{2}$.

*6.139.* $|b| - |a|$.

*6.140.* $\frac{1}{4} \ln 2$.

*6.141.* $\frac{1}{5}\left(\mathrm{e}^{\pi} - 2\right)$.

*6.142.* $\mathrm{e} - 5\mathrm{e}^{-1}$.

*6.143.* $\frac{1}{6}$.

*6.144.* (a) 4; (b) $\frac{1-\ln 2}{2}$.

*6.145.* $p < q$.

*6.146.* $a > 0$; $b = 0$; $c > 0$.

*6.147.* $C < D = 0 < A < B$.

*6.148.* (a) 5; (b) 0; (c) 0.

*6.149.* 1.

*6.150.* 0.

*6.151.* $0 < \int_1^2 \frac{\cos^{10} x}{10} \ln x\,dx < \frac{1}{10}$, $\int_1^2 x \ln x\,dx = \ln 4 - \frac{3}{4}$.

*6.152.* $-6x^5 \cos x^2$.

*6.153.* $\frac{1}{2}\ln(x^2+2x+2)-\frac{1}{2}\ln(x^2+x+1)+\frac{1}{3}\sqrt{3}\arctan\left(\frac{(2x+1)\sqrt{3}}{3}\right)+C$.

*6.154.* $\frac{1}{2}\ln\left(3+2\sqrt{2}\right)$.

*6.155.* $-\frac{1}{6}-\frac{2}{9}\ln 2$.

*6.156.*

(i) $\frac{2}{3}$,

(ii) $\frac{1}{2}\sin^4 x$.

*6.157.* (a) $\pi$; (b) $+\infty$; (c) 20; (d) $-2$.

*6.158.* $-\infty$.

*6.159.* $\frac{2}{\sqrt{3}}\pi$.

*6.160.* $\frac{2\sqrt{3}}{9}\,\pi$.

*6.161.* $-\frac{1}{2}$; 1.

*6.162.* $2-\frac{2}{\mathrm{e}}$; $\frac{2}{\mathrm{e}}-\frac{2}{\mathrm{e}^2}$; $\frac{2}{\mathrm{e}^2}$.

*6.163.* (a) $\alpha>1$; (b) $\alpha<1$; (c) $\alpha=0$.

*6.164.* Právě pro $p>1$, $q\in\mathbb{R}$ a pro $p=1$, $q>1$.

*6.165.* (a) platí; (b) neplatí; (c) platí.

*6.166.* $1-\frac{\pi^2}{10^2\cdot 2}+\frac{\pi^4}{10^4\cdot 4!}$.

*6.167.* Chyba náleží do intervalu $(0,\,1/200)$.

*6.168.* $1-3x+\frac{7}{24}x^4$; nad tečnou.

*6.169.* $\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\,x^{2n}$.

*6.170.* $y=\operatorname{arctg} x$.

*6.171.* Právě pro $x\in\left(-\frac{5}{2},\,\frac{5}{2}\right)$ je

$$\frac{1}{5+2x}=\frac{1}{5}\sum_{n=0}^{\infty}\left(-\frac{2}{5}\right)^n x^n.$$

*6.172.* $\frac{1}{3}\sum_{n=0}^{\infty}\frac{2^n}{3^n}x^n$.

*6.173.*

$$f(x)=1/2+\sum_{i=0}^{\infty}\frac{(-1)^{i+1}2^{2i}}{(2i+1)!}\left(x-\frac{\pi}{4}\right)^{2i+1}.$$

Řada konverguje pro všechna $x\in R$.

*6.174.* $\sum_{n=0}^{\infty}\frac{\mathrm{e}}{n!}\,(x-1)^n$; $\sum_{n=0}^{\infty}\frac{\ln^n 2}{n!}\,x^n$.

*6.175.* $f(x)=x$, $x\in\mathbb{R}$; ano.

*6.176.* Nikoli.

*6.177.* $\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\,x^{2n}$.

*6.178.* (a) $1-\frac{\pi^2}{18^2\cdot 2!}+\frac{\pi^4}{18^4\cdot 4!}$; (b) $\frac{1}{2}-\frac{1}{5\cdot 2^5}$.

*6.179.* $\sum_{n=0}^{\infty}\frac{1}{(2n+1)\,n!}\,x^{2n+1}$.

*6.180.* $y=\operatorname{arctg} x$.

*6.181.* Právě pro $x\in\left(-\frac{5}{2},\,\frac{5}{2}\right)$ je

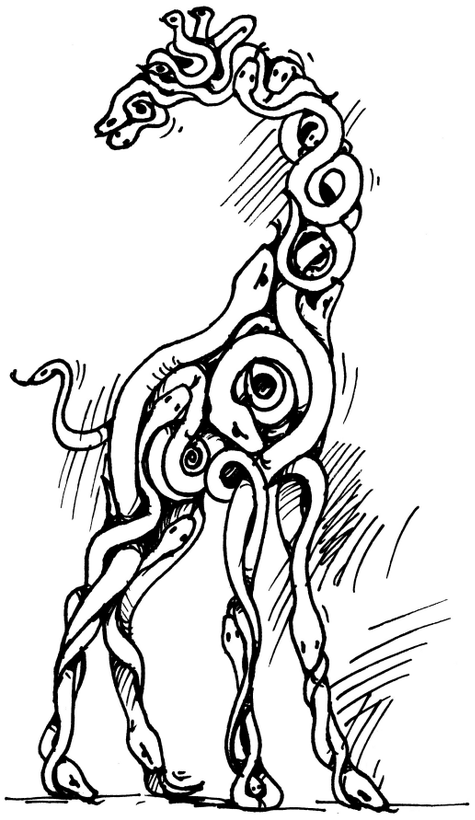
$$\frac{1}{5+2x}=\frac{1}{5}\sum_{n=0}^{\infty}\left(-\frac{2}{5}\right)^n x^n.$$

*6.182.* (a) $v(0)=6\,\mathrm{m/s}$; (b) $t=3\,\mathrm{s}$, $s(3)=16\,\mathrm{m}$; (c) $v(4)=-2\,\mathrm{m/s}$, $a(4)=-2\,\mathrm{m/s^2}$.

KAPITOLA 7

# Spojité modely

*Jak zvládáme nelineární objekty?*
*– zase lineárními nástroji ...*



## A. Ortogonální systémy funkcí

Chceme-li zobrazit nějaký trojrozměrný objekt v rovině, uvážíme jeho (například kolmou) projekci do této roviny. Obdobně, chceme-li „vyjádřit“ nějakou složitější funkci pomocí jednodušších, můžeme uvážit její projekci do (reálného) vektorového prostoru generovaného těmito jednoduššími funkcemi. Potom budeme schopni například integrovat složitější funkce stejně, jako jsme integrovali (či derivovali) funkce vyjádřené pomocí mocninných řad (pokud bude prostor jednodušších funkcí „dostatečně“ velký, tak s libovolnou přesností).

V této kapitole ukážeme využití nástrojů diferenciálního a integrálního počtu ve vybraných problémech, ve kterých si vystačíme s funkcemi jedné reálné nezávislé proměnné.

Půjde o postupy a nástroje docela podobné těm z kapitoly třetí, tj. manipulace s lineárními kombinacemi vybraných generátorů a lineárními transformacemi (např. hledání jejich jader nebo vzorů předepsaných obrazů). Jen místo konečně rozměrných vektorů budeme pracovat s prostory funkcí, tzn. uvažované vektorové prostory často nebudou mít konečnou dimenzi. K těmto i dalším praktickým oblastem se vrátíme v příští kapitole v kontextu funkcí více proměnných a diferenciálních rovnic.

Nejprve budeme aproximovat funkce pomocí lineárních kombinací z předem pevně zvolených sad generátorů. Po cestě si ale budeme muset ujasnit, jak vlastně lze pracovat s pojmy jako je vzdálenost. Půjde o náznaky teorie tzv. metrických prostorů a tato část je zároveň přípravou na analýzu v euklidovských prostorech $\mathbb{R}^n$. V zásadě přitom budeme pokračovat v postupech, které již z euklidovských vektorových prostorů dobře známe. Zjistíme, že naše intuice z euklidovských prostorů nízké dimenze se docela dobře hodí i obecně.

Pak se budeme stručně zabývat integrálními operátory, tj. lineárními zobrazeními na funkcích, které jsou definovány pomocí integrování. Půjde zejména o tzv. Fourierovu analýzu. Při našich úvahách se přitom budeme jako obvykle zamýšlet i nad diskrétními variantami dříve diskutovaných spojitých operací.

V celé kapitole budeme pracovat s funkcemi jedné reálné proměnné, které ale budou mít buď reálné nebo (velmi často) komplexní hodnoty.

### 1. Fourierovy řady

**7.1. Prostory funkcí.** Jako obvykle začneme výběrem vhodných množin funkcí, se kterými chceme pracovat. Přitom chceme mít dost funkcí pro praktickou použitelnost našich modelů, ale také musí být dostatečně „pěkné“, abychom je uměli integrovat a derivovat tak, jak bude třeba.



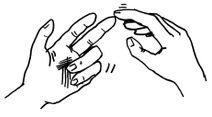
Budeme vesměs pracovat s funkcemi definovanými na nějakém intervalu $I = [a, b] \subset \mathbb{R}$, případně nekonečném intervalu (tj. krajní hodnoty $a$ i $b$ mohou také nabývat hodnot $\pm\infty$, stále však půjde o uzavřené množiny).

PROSTORY PO ČÁSTECH HLADKÝCH FUNKCÍ

Množina funkcí $\mathcal{S}^0 = \mathcal{S}^0[a, b]$ obsahuje právě všechny po částech spojité funkce na $I = [a, b]$ s reálnými nebo komplexními hodnotami, tj. předpokládáme, že v každém bodě intervalu

Na vhodném (nekonečném) vektorovém prostoru funkcí na daném intervalu, můžeme zavést i skalární součin (takovým vhodným prostorem je například prostor $L_2$, viz 7.3). Skalární součin tedy nezavedeme na prostoru všech funkcí na daném intervalu, ale na jistém jeho podprostoru, který však bude dostatecně veliký pro naše výpočty (mimo jiné bude obsahovat všechny spojité funkce na daném intervalu). Skalární součin nám umožní počítat projekce tak, jak jsme byli zvyklí u vektorových prostorů. Pokud máme dán konečně rozměrný vektorový (pod)prostor funkcí a chceme určit projekci nějaké funkce na něj, tak Gramovým-Schmidtovým ortogonalizačním procesem (viz 2.42) nejprve spočítáme ortogonální (či ortonormální) bázi tohoto podprostoru a pak známým způsobem (2.3) dopočítáme kolmou projekci.

**7.1.** V prostoru reálných funkcí na intervalu $[1, 2]$, je dán vektorový podprostor $\langle x^2, 1/x\rangle$. Doplňte funkci $1/x$ na jeho ortogonální bázi, určete kolmou projekci funkce $x$ na tento podprostor a spočítejte její vzdálenost od tohoto podprostoru.



**Řešení.** Nejprve doplníme funkci $1/x$ na ortogonální bázi. Jedním z vektorů báze tedy bude funkce $1/x$. Uvažovaný vektorový prostor je generován dvěma lineárně nezávislými funkcemi, bude tedy mít dimenzi 2 (a všechny vektory v něm jsou tvaru $a\cdot\frac{1}{x}+b\cdot x^2$, kde $a, b \in \mathbb{R}$). Zbývá nám tedy najít pouze ještě jeden vektor báze, který bude kolmý na funkci $f_1 = 1/x$. Podle Gramova-Schmidtova ortogonalizačního procesu ho hledáme ve tvaru $f_2 = x^2 + k \cdot \frac{1}{x}$, $k \in \mathbb{R}$. Reálnou konstantu $k$ určíme z podmínky kolmosti:

$$0 = \left\langle \frac{1}{x}, x^2 + k \cdot \frac{1}{x} \right\rangle = \left\langle \frac{1}{x}, x^2 \right\rangle + k \left\langle \frac{1}{x}, \frac{1}{x} \right\rangle,$$

tedy

$$k = -\frac{\langle \frac{1}{x}, x^2 \rangle}{\langle \frac{1}{x}, \frac{1}{x} \rangle} = -\frac{\int_1^2 \frac{1}{x} \cdot x^2 \,\mathrm{d}x}{\int_1^2 \frac{1}{x} \cdot \frac{1}{x} \,\mathrm{d}x} = -3.$$

Hledaná ortogonální báze tedy je $\left(\frac{1}{x}, x^2 - \frac{3}{x}\right)$. Nyní spočítáme projekci $p_x$ funkce $x$ na tento podprostor (viz (2.3)):

$$p_x = \frac{\langle x, \frac{1}{x} \rangle}{\langle \frac{1}{x}, \frac{1}{x} \rangle} \cdot \frac{1}{x} + \frac{\langle x, x^2 - \frac{3}{x} \rangle}{\langle x^2 - \frac{3}{x}, x^2 - \frac{3}{x} \rangle} \cdot \left(x^2 - \frac{3}{x}\right) = \\ = \frac{2}{x} + \frac{15}{34}\left(x^2 - \frac{3}{x}\right).$$

Vzdálenost vektoru od vektorového podprostoru je dána velikostí rozdílu vektoru a jeho projekce do uvažovaného podprostoru. V našem

má funkce $f \in \mathcal{S}^0$ příslušné konečné jednostranné limity zprava i zleva, přičemž bodů nespojitosti je nejvýše konečně mnoho na každém konečném intervalu. Zejména jsou tedy všechny takové funkce na omezených intervalech omezené.

Pro každé přirozené číslo $k \geq 1$ budeme také uvažovat množinu všech po částech spojitých funkcí $f$ jejichž všechny derivace až do řádu $k$ včetně patří do $S^0$ (tj. nemusí existovat ve všech bodech, ale existují jejich jednostranné limity ve všech bodech). Budeme pro ni používat značení $\mathcal{S}^k$.

V případě neomezeného intervalu $I$ budeme také pracovat často s podmnožinou $\mathcal{S}^k_c \subset \mathcal{S}^k$ všech funkcí s kompaktním nosičem (tzn. že funkce jsou identicky nulové vně nějakého konečného uzavřeného intervalu).

Na ohraničených intervalech samozřejmě mají všechny funkce kompaktní nosič v tomto smyslu. Když nás nebude zajímat, na jakém intervalu pracujeme, budeme proto psát jen $\mathcal{S}^k_c$ ve všech případech. V případě konečného intervalu $[a, b]$ nebo za předpokladu kompaktního nosiče jsou naše funkce z $\mathcal{S}^0$ vždy riemannovsky integrovatelné na zvoleném intervalu $I$ jak v absolutní hodnotě tak v kvadrátu, tzn.

$$\int_a^b |f(x)|dx < \infty, \quad \int_a^b (f(x))^2 dx < \infty.$$

Naše úvahy lze rozšiřovat na podstatně větší definiční obory funkcí, často ale za cenu značné technické námahy. Budeme občas zmiňovat prostory kurzweilovsky (nebo lebesgueovsky) integrovatelných funkcí, pro které jsou výsledky daleko ucelenější a pěknější. Zájemce odkazujeme na rozsáhlou specializovanou literaturu. Ve skutečnosti se budeme držet stejné strategie jako u racionálních a reálných čísel – počítáme jen s pěknými funkcemi a máme „nějak zvládnuto“, jak vypadají limity cauchyovských posloupností ve zvolených metrikách (které většinou potřebujeme jen formálně).

**7.2. Vzdálenost funkcí.** Z námi již dokázaných vlastností limit a derivování je okamžitě vidět, že $\mathcal{S}^k$, resp. $\mathcal{S}^k_c$, jsou vektorové prostory. Na konečnědimenzionálních prostorech jsme uvažovali vzdálenost vektorů pomocí rozdílů hodnot jednotlivých jejich souřadnic. Na prostorech funkcí můžeme postupovat podobě a využít absolutní hodnoty reálných nebo komplexních čísel (resp. euklidovské vzdálenosti) následujícím způsobem:



VZDÁLENOST FUNKCÍ

**Definice.** Pro funkce $f$ a $g$ z $\mathcal{S}^0_c$ je jejich $L_1$–vzdálenost definována vztahem

$$\|f - g\|_1 = \int_a^b |f(x) - g(x)|dx\,.$$

Obdobně je $L_2$–vzdálenost funkcí $f$ a $g$ definována vztahem

$$\|f - g\|_2 = \left(\int_a^b |f(x) - g(x)|^2 dx\right)^{1/2}.$$

Velikostí funkce $\|f\|_1$ nebo $\|f\|_2$ rozumíme její vzdálenost od funkce nulové.

případě

$$\begin{aligned}\|x - p_x\| &= \left[\int_1^2 \left(x - \frac{2}{x} - \frac{15}{34}\left(x^2 - \frac{3}{x}\right)\right)^2 \mathrm{d}x\right]^{\frac{1}{2}} \\ &= \frac{\sqrt{102}}{204} \doteq 0{,}495.\end{aligned}$$

□

**7.2.** Uvažujme reálný vektorový prostor funkcí na intervalu $[1, 2]$ generovaný funkcemi $\frac{1}{x}, \frac{1}{x^2}, \frac{1}{x^3}$. Doplňte funkci $\frac{1}{x}$ na ortogonální bázi tohoto prostoru. Dále určete projekce funkcí $\frac{1}{x^4}$ a $x$ na tento vektorový prostor a určete jejich vzdálenosti od tohoto vektorového prostoru.

**Řešení.** Analogicky jako v předcházejícím příkladu, použijeme Gramova-Schmidtova ortogonalizačního procesu (s daným skalárním součinem). Dostáváme tak postupně

$$\begin{aligned}f_1(x) &= \tfrac{1}{x}, \\ f_2(x) &= \tfrac{1}{x^2} - \tfrac{3}{4x}, \\ f_3(x) &= \tfrac{1}{x^3} - \tfrac{3}{2x^2} + \tfrac{13}{24x}.\end{aligned}$$

Pomocí získané ortonormální báze pak již snadno zapíšeme hledané projekce:

$$\begin{aligned}p_x &= \frac{\langle x, f_1\rangle}{\langle f_1, f_1\rangle}\cdot f_1 + \frac{\langle x, f_2\rangle}{\langle f_2, f_2\rangle}\cdot f_1 + \frac{\langle x, f_3\rangle}{\langle f_3, f_3\rangle}\cdot f_1 = \\ &= 2f_1 + 96\cdot\left(\ln 2 - \frac{3}{4}\right)\cdot f_2 + 5760\left(\frac{25}{24} - \frac{3}{2}\ln 2\right) f_3 = \\ &\doteq 0{,}058.\end{aligned}$$

Pro projekci funkce $\frac{1}{x^4}$ pak dostáváme

$$\begin{aligned}p_{\frac{1}{x^4}} &= \frac{15}{32}f_1 + \frac{69}{40}f_2 + \frac{9}{4}f_3 = \\ &= \frac{\sqrt{14}}{2240} \doteq 0{,}002.\end{aligned}$$

Vidíme, že vzdálenost funkce, která má podobný průběh jako generátory, je menší. □

*7.3.* V prostoru reálných funkcí na intervalu $[0, \pi]$, je dán vektorový podprostor $\langle \sin(x), x\rangle$. Doplňte funkci $x$ na jeho ortogonální bázi a určete kolmou projekci funkce $\frac{1}{2}\sin(x)$ na tento podprostor. ○

*7.4.* V prostoru reálných funkcí na intervalu $[0, \pi]$, je dán vektorový podprostor $\langle \cos(x), x\rangle$. Doplňte funkci $\cos(x)$ na jeho ortogonální bázi a určete kolmou projekci funkce $\frac{1}{3}\cos(x)$ na tento podprostor ○

V prvním případě $L_1$–vzdálenost funkcí $f$ a $g$ s pouze reálnými hodnotami vyjadřuje plochu uzavřenou mezi grafy těchto funkcí, nezávisle na tom, která funkce má větší či menší hodnoty. Protože uvažujeme po částech spojité funkce $f$ a $g$, může být jejich vzdálenost rovna nule pouze když se od sebe liší nanejvýš svými hodnotami v bodech nespojitosti, tj. v nejvýše konečně mnoha bodech na ohraničených intervalech. Skutečně, jestliže se dvě naše funkce liší v jednom bodě $x_0$, ve kterém jsou spojité, liší se i na nějakém dostatečně malém okolí tohoto bodu a toto okolí přispěje do vzdálenosti nenulovou hodnotou integrálu.

Máme-li tři funkce $f$, $g$ a $h$, pak samozřejmě

$$\begin{aligned}\int_a^b |h(x) - f(x)|dx &= \int_a^b |h(x) - g(x) + g(x) - f(x)|dx \leq \\ &\leq \int_a^b |h(x) - g(x)|dx + \int_a^b |g(x) - f(x)|dx,\end{aligned}$$

a platí tedy obvyklá trojúhelníková nerovnost. Všimněme si, že odvození této nerovnosti využívá pouze trojúhelníkovou nerovnost platnou pro velikost skalárů, platí proto i pro funkce $f, g \in \mathcal{S}_c^0$ s komplexními hodnotami.

Podobné je to pro druhou definici. Čtverec velikosti $\|f\|_2$ funkce $f$ je

$$(\|f\|_2)^2 = \int_a^b |f(x)|^2\,dx$$

a je odvozen z dobře definovaného symetrického bilineárního zobrazení reálných funkcí do skalárů

$$\langle f, g\rangle = \int_a^b f(x)g(x)\,dx$$

dosazením $f$ za obě funkce. U komplexních hodnot ale obdržíme podobně tuto velikost ze skalárního součinu s použitím komplexní konjugace,

$$\langle f, g\rangle = \int_a^b f(x)\overline{g(x)}\,dx,$$

jak jsme viděli u unitárních prostorů v třetí kapitole.

Určitě tedy bude platit i trojúhelníková nerovnost, protože celou diskusi můžeme odehrát v maximálně třírozměrném prostoru se skalárním součinem generovaným danými funkcemi $f$, $g$ a $h$.

**7.3. (Ne)konečnost dimenze a ortogonalita.** Zůstaňme na chvíli



u naší definice $L_2$–normy $\|\ \|_2$ na vektorovém prostoru $\mathcal{S}_c^0$. Zjevně operace na konci posledního odstavce splňuje jak linearitu v prvním argumentu, tak symetrii

$$\langle f, g\rangle = \overline{\langle g, f\rangle},$$

tj. v reálném případě je to symetrické bilineární zobrazení. Zároveň je pro spojité funkce splněna i podmínka nenulovosti velikosti pro nenulové funkce, zatímco pro naše po částech spojité funkce znamená nulovost velikosti nulovost funkce až na nejvýše spočetnou množinu bodů (konečnou na každém konečném intervalu). Pro vektorový podprostor spojitých funkcí jsme tedy skutečně definovali skalární součin.

U obecnějších funkcí bychom, technicky vzato, měli ztotožňovat funkce, které se liší na konečných intervalech jen v konečně mnoha hodnotách. V našich dalších úvahách ale tato technická nepříjemnost nebude hrát podstatnou roli (a příležitostně se k ní budeme vracet v poznámkách).

### B. Fourierovy řady

Základním studovaným periodickým dějem, s nímž se setkáváme v aplikacích, je obecné jednoduché harmonické kmitání v mechanice. Jedná se o pohyb hmotného bodu po přímce. Je dobře známo, že funkce $f$, jež udává polohu kmitajícího hmotného bodu na přímce v závislosti na čase $t$, má tvar

$$f(t) = a\sin(\omega t + b) \tag{7.1}$$

pro jisté konstanty $a, \omega > 0, b \in \mathbb{R}$ určené polohou a rychlostí bodu v počátečním čase. Funkci $y \equiv f(t)$ lze získat např. vyřešením homogenní lineární diferenciální rovnice

$$y'' + \omega^2 y = 0 \tag{7.2}$$

vyplývající z aplikace Newtonova zákonu síly pro daný pohyb. Doplňme, že funkce $f$ má zřejmě periodu $T = 2\pi/\omega$ (v mechanice se však častěji mluví o kmitočtu neboli frekvenci $1/T$) a že kladná hodnota $a$ (vyjadřující maximální výchylku kmitajícího bodu od počátku) se nazývá amplituda, hodnota $b$ (vyjadřující polohu bodu v počátečním čase) počáteční fáze a hodnota $\omega$ pak úhlová frekvence kmitavého pohybu.

Podobně se můžeme zabývat funkcí $z \equiv g(t)$, která udává napětí v závislosti na čase $t$ v elektrickém obvodu s indukčností $L$ a kapacitou $C$ a která je řešením diferenciální rovnice

$$z'' + \omega^2 z = 0. \tag{7.3}$$

Rozdíl mezi rovnicemi (‖7.2‖) a (‖7.3‖) (kromě odlišné fyzikální interpretace) je pouze v konstantě $\omega$. Pro rovnici (‖7.2‖) je $\omega^2 = k/m$, kde $k$ je konstanta úměrnosti a $m$ je hmotnost hmotného bodu; a pro rovnici (‖7.3‖) je $\omega^2 = (LC)^{-1}$.

Ve skutečnosti každý periodický děj, který lze zadat funkcí ve tvaru (‖7.1‖), se označuje jako harmonické kmitání a pro konstanty $a, \omega, b$ se používá takřka výhradně výše zmíněné označení převzaté z jednoduchého harmonického kmitání hmotného bodu v mechanice.

Když využijeme jednoho ze součtových vzorců

$$\sin(\alpha + \beta) = \cos\alpha\sin\beta + \sin\alpha\cos\beta, \quad \alpha, \beta \in \mathbb{R},$$

můžeme funkci $f$ (viz (‖7.1‖)) zapsat jako

$$f(t) = c\cos(\omega t) + d\sin(\omega t)\,, \tag{7.4}$$

přičemž $c = a\sin b$, $d = a\cos b$. Rovněž tedy funkce $f$ z (‖7.4‖) vystihuje harmonické kmitání s amplitudou $a = \sqrt{c^2 + d^2}$ a s počáteční fází $b \in [0, 2\pi)$ splňující $\sin b = c/a$, $\cos b = d/a$.

V konečněrozměrném případě reálných nebo komplexních vektorových prostorů jsme uvažovali skalární součiny a velikost vektorů již ve druhé a třetí kapitole.

Všimněme si teď, že při odvozování vlastností jsme vždy pracovali s dvojicemi nebo konečnými množinami vektorů. Nyní to ale můžeme dělat s funkcemi naprosto stejně a pokud zúžíme naši definici skalárního součinu na vektorový podprostor generovaný (podle potřeby nad reálnými nebo komplexními čísly) jen konečně mnoha funkcemi $f_1, \ldots, f_k$. Dostaneme opět dobře definovaný skalární součin na tomto konečněrozměrném vektorovém podprostoru.

Jako příklad uvažme funkce $f_i = x^i$, $i = 0, \ldots, k$. Jimi je v $\mathcal{S}^0$ generován $(k+1)$–rozměrný vektorový podprostor $\mathbb{R}_k[x]$ všech polynomů stupně nejvýše $k$. Skalární součin dvou takových polynomů je dán integrálem. Každý polynom stupně nejvýše $k$ je vyjádřen jednoznačným způsobem jako lineární kombinace generátorů $f_0, \ldots, f_k$. Pokud by navíc naše generátory měly tu vlastnost, že

$$\langle f_i, f_j\rangle = \begin{cases} 0 & \text{pro } i \neq j, \\ 1 & \text{pro } i = j, \end{cases} \tag{7.1}$$

jde o tzv. *ortonormální bázi*. Připomeňme si v této souvislosti proceduru Gramovy–Schmidtovy ortogonalizace, viz 2.42, která z libovolného systému lineárně nezávislých generátorů $f_i$ vytvoří nové (opět lineárně nezávislé) ortogonální generátory $g_i$ téhož prostoru, tj. $\langle g_i, g_j\rangle = 0$ pro všechny $i \neq j$. Spočteme je přitom postupně jako $g_1 = f_1$ a vzorci

$$g_{\ell+1} = f_{\ell+1} + a_1 g_1 + \cdots + a_\ell g_\ell, \quad a_i = -\frac{\langle f_{\ell+1}, g_i\rangle}{\|g_i\|^2}$$

pro $\ell \geq 1$.

Aplikujme tuto proceduru pro ilustraci na tři polynomy $1, x, x^2$ na intervalu $[-1, 1]$. Dostaneme $g_1 = 1$,

$$\begin{aligned} g_2 &= x - \frac{1}{\|g_1\|^2}\left(\int_{-1}^{1} x\cdot 1\,dx\right)\cdot 1 = x - 0 = x \\ g_3 &= x^2 - \frac{1}{\|g_1\|^2}\left(\int_{-1}^{1} x^2\cdot 1\,dx\right)\cdot 1 - \\ &\quad - \frac{1}{\|g_2\|^2}\left(\int_{-1}^{1} x^2\cdot x\,dx\right)\cdot x = \\ &= x^2 - \frac{1}{3}. \end{aligned}$$

Příslušná ortogonální báze prostoru $\mathbb{R}_2[x]$ všech polynomů stupně nejvýše tři na intervalu $[-1, 1]$ je tedy $1, x, x^2 - 1/3$. Normalizací, tj. vhodným násobením skalárem tak, aby prvky v bázi měly velikost jedna, dostaneme ortonormální bázi

$$h_1 = \sqrt{\frac{1}{2}}, \quad h_2 = \sqrt{\frac{3}{2}}x, \quad h_3 = \frac{1}{2}\sqrt{\frac{5}{2}}(3x^2 - 1/3).$$

Takovým ortonormálním generátorům $\mathbb{R}_k[x]$ se říká *Legendreovy polynomy*.

**7.4. Ortogonální systémy funkcí.** Právě jsme si připomněli



výhody, které ortonormální báze podprostorů mají pro konečněrozměrné vektorové prostory. V předchozím příkladu Legendreových polynomů generujících $\mathbb{R}_2[x] \subset V = \mathbb{R}_k[x]$, $k \geq 2$, bude pro libovolný polynom $h \in V$ funkce

Důležitou úlohou v aplikačních problémech je skládání (tzv. superpozice) různých harmonických kmitání. Klíčovou pozici potom zaujímá superpozice konečného počtu harmonických kmitání vyjádřených funkcemi ve tvaru

$$f_n(x) = a_n \cos(n\omega x) + b_n \sin(n\omega x)$$

pro $n \in \{1, \dots, m\}$. Tyto jednotlivé funkce mají základní periodu $2\pi/(n\omega)$. Jejich součet

$$\sum_{n=1}^{m} [a_n \cos(n\omega x) + b_n \sin(n\omega x)] \tag{7.5}$$

je proto periodickou funkcí s periodou $2\pi/\omega$. Obecně platí, že superpozicí libovolných konečně mnoha jednoduchých harmonických kmitání majících souměřitelné periody je periodický proces, jehož periodou je nejmenší společný násobek primitivních period jednotlivých kmitání.

Součet (‖7.5‖) doplněný o vhodné posunutí

$$\frac{a_0}{2} + \sum_{n=1}^{m} [a_n \cos(n\omega x) + b_n \sin(n\omega x)] \tag{7.6}$$

je právě $m$-tým částečným součtem funkcionální řady

$$\frac{a_0}{2} + \sum_{n=1}^{\infty} [a_n \cos(n\omega x) + b_n \sin(n\omega x)]\,. \tag{7.7}$$

Z fyzikálního hlediska jde o složený periodický proces, jenž může sloužit jako přirozená aproximace superpozice nekonečného počtu jednoduchých harmonických kmitání (tzv. harmonických složek) funkcionální řady (‖7.7‖).

Nabízí se zde otázka, zda je možné naopak každý periodický proces „rozumně“ vyjádřit superpozicí konečného a případně nekonečného počtu jednoduchých harmonických kmitání – zda každý periodický proces je výsledkem takové superpozice. Formulováno přesněji z pohledu matematiky, zda lze každou periodickou funkci vyjádřit jako konečný součet (‖7.6‖), příp. alespoň jako součet řady (‖7.7‖). Kladnou odpověď pro významnou a širokou třídu periodických funkcí samozřejmě dostáváme pouze pro součet nekonečný (viz teoretická část).

Již jsme řekli, že periodické procesy hrají důležitou roli ve většině fyzikálních i technických oborů. Tradičně vyzdvihněme alespoň akustiku, mechaniku, elektrotechniku, kde se nepopiratelně ukazuje nutnost zodpovězení uvedené otázky. Kromě toho však hledání odpovědi vedlo ke vzniku svébytné matematické partie – teorie Fourierových řad. Ta se poté začala využívat při řešení dalších tříd problémů (mj. k řešení většiny důležitých typů obyčejných a parciálních diferenciálních rovnic) a přispěla k rozvoji samotných teoretických základů matematiky

$$H = \langle h, h_1\rangle h_1 + \langle h, h_2\rangle h_2 + \langle h, h_3\rangle h_3$$

jednoznačně určenou funkcí, která minimalizuje naši $L_2$–vzdálenost $\|h - H\|$ mezi všemi funkcemi v $\mathbb{R}_k[x]$, viz 3.25.

Koeficienty pro nejlepší aproximaci zadané funkce pomocí funkce z vybraného podprostoru je možné tedy získat prostě integrací v definici skalárního součinu.

Uvedený příklad podbízí následující zobecnění: Když provedeme proceduru Gramovy–Schmidtovy ortogonalizace pro všechny monomy $1, x, x^2, \dots$, tj. pro spočetný systém generátorů, co z toho vznikne?

### Ortogonální systémy funkcí

Libovolný konečný nebo spočetný systém lineárně nezávislých funkcí v $\mathcal{S}^0_c[a, b]$ takový, že každé dvě různé z nich mají nulový skalární součin, se nazývá *ortogonální systém funkcí*. Jestliže jsou všechny funkce $f_n$ v posloupnosti po dvou ortogonální a zároveň je pro všechna $n$ velikost $\|f_n\|_2 = 1$, hovoříme o *ortonormálním systému funkcí*.

Uvažme tedy jakýkoliv ortogonální systém funkcí $f_n \in \mathcal{S}^0[a, b]$ a předpokládejme, že pro (reálné nebo komplexní) konstanty $c_n$ konverguje řada

$$F(x) = \sum_{n=1}^{\infty} c_n f_n$$

stejnoměrně na konečném intervalu $[a, b]$. Pak snadno vyjádříme skalární součin $\langle F, f_n\rangle$ po jednotlivých sčítancích (viz důsledek 6.43) a dostaneme

$$\langle F, f_n\rangle = \sum_{m=1}^{\infty} c_m \int_a^b f_m(x)\overline{f_n(x)}\,dx = c_n \|f_n\|^2,$$

kde normou myslíme (stejně jako v dalších odstavcích) naši $L_2$–velikost.



Jistě teď už tušíme, v jakém smyslu lze případně rozšiřovat postupy z konečněrozměrných prostorů: Místo konečných lineárních kombinací bázových vektorů budeme pracovat s nekonečnými řadami po dvou ortogonálních funkcí. Následující věta nám přitom dává přehlednou a velmi obecnou odpověď na otázku, jak dobře se konečnými součty takové řady umíme k dané funkci přiblížit:

**7.5. Věta.** *Nechť $f_n$, $n = 1, 2, \dots$, je ortogonální posloupnost (reálných nebo komplexních) funkcí v prostoru $\mathcal{S}^0[a, b]$, nechť $g \in \mathcal{S}^0[a, b]$ je libovolná taková funkce a označme*

$$c_n = \|f_n\|^{-2} \int_a^b g(x)\overline{f_n(x)}\,dx.$$

*(1) Pro libovolné pevné $n \in \mathbb{N}$ má ze všech lineárních kombinací funkcí $f_1, \dots, f_n$ nejmenší $L_2$–vzdálenost od $g$ funkce*

$$h_n(x) = \sum_{i=1}^{n} c_i f_i(x).$$

*(2) Číselná řada $\sum_{n=1}^{\infty} |c_n|^2 \|f_n\|^2$ vždy konverguje a platí*

$$\sum_{n=1}^{\infty} |c_n|^2 \|f_n\|^2 \le \|g\|^2.$$

(např. k přesnému vymezení tak fundamentálních pojmů, jakými jsou funkce a integrál).

Název Fourierovy řady je pak na počest francouzského matematika a fyzika Jeana B. J. Fouriera, který jako první prakticky využil trigonometrické výrazy (‖7.6‖) ve své práci z roku 1822 věnované problematice vedení tepla (problematikou se začal zabývat v roce 1804 a práci sepsal již v roce 1811). Význam tohoto Fourierova počinu pro teoretickou fyziku, přestože se fyzice věnoval spíše okrajově, byl nesmírný: zavedl tím do oboru matematické metody, které dodnes patří ke klasickým nástrojům teoretické fyziky. Fourierova matematická teorie tepla se také stala základem pro George S. Ohma při odvození jeho slavného zákonu vedení elektrického proudu. Upozorněme ještě, že jiní matematici studovali vlastnosti součtů (‖7.6‖) o mnoho let dříve než Fourier (kupř. L. Euler). Nedosáhli však zásadního výsledku směrem k možnému praktickému využití jako on.

**7.5.** Určete Fourierovy koeficienty funkce

(a) $g(x) = \sin(2x)\cos(3x)\,,\ x \in [-\pi, \pi]$;

(b) $g(x) = \cos^4 x,\ x \in [-\pi, \pi]$.

**Řešení.** Případ (a). Neboť pro $x \in \mathbb{R}$ je

$$\begin{aligned}\sin(2x)\cos(3x) &= \sin(2x)\,[\cos(2x)\cos x - \sin(2x)\sin x] = \\ &= \tfrac{1}{2}\sin(4x)\cos x - \sin^2(2x)\sin x = \\ &= \tfrac{1}{2}\cos x \sin(4x) - \tfrac{1-\cos(4x)}{2}\sin x = \\ &= -\tfrac{1}{2}\sin x + \tfrac{1}{2}\cos x \sin(4x) + \tfrac{1}{2}\sin x \cos(4x) = \\ &= -\tfrac{1}{2}\sin x + \tfrac{1}{2}\sin(5x)\,,\end{aligned}$$

vidíme, že Fourierovy koeficienty jsou nulové s výjimkou $b_1 = -1/2$, $b_5 = 1/2$.

Případ (b). Podobně z

$$\begin{aligned}\cos^4 x = \left[\cos^2 x\right]^2 &= \left[\tfrac{1+\cos(2x)}{2}\right]^2 = \\ &= \tfrac{1}{4}\left[1 + 2\cos(2x) + \cos^2(2x)\right] = \\ &= \tfrac{1}{4}\left[1 + 2\cos(2x) + \tfrac{1+\cos(4x)}{2}\right] = \\ &= \tfrac{3}{8} + \tfrac{1}{2}\cos(2x) + \tfrac{1}{8}\cos(4x)\,, \quad x \in \mathbb{R}\end{aligned}$$

plyne, že $a_0 = 3/4$, $a_2 = 1/2$, $a_4 = 1/8$ a že ostatní koeficienty jsou nulové.

V této úloze jsme si ukázali, že výpočet Fourierovy řady nemusí nutně vést na počítání integrálů (obvykle metodou per partes). Zvláště v situacích, kdy funkce $g$ má tvar součinu (mocniny) funkcí $y = \sin(mx)$, $y = \cos(nx)$ pro $m, n \in \mathbb{N}$, stačí aplikovat středoškolské učivo (známé goniometrické vzorce). □

**7.6.** Najděte Fourierovu řadu pro periodické prodloužení funkce

(a) $g(x) = 0,\ x \in [-\pi, 0), \quad g(x) = \sin x,\ x \in [0, \pi)$;

*(3) $L_2$–vzdálenost funkce $g$ od částečných součtů $s_k = \sum_{n=1}^{k} c_n f_n$ jde v limitě k nule, tj.*

$$\lim_{k\to\infty} \|g - s_k\| = 0,$$

*tehdy a jen tehdy, když*

$$\sum_{n=1}^{\infty} c_n^2 \|f_n\|^2 = \|g\|^2.$$

Ještě než se pustíme do důkazu, zkusme lépe porozumět významu jednotlivých tvrzení této věty. Protože pracujeme s úplně libovolně zvoleným ortogonálním systémem funkcí, nemůžeme očekávat, že lze dobře aproximovat jakoukoliv funkci pomocí lineárních kombinací funkcí $f_i$.

Např. když se omezíme u Legendreových ortogonálních polynomů na intervalu $[-1, 1]$ pouze na sudé stupně, určitě budeme dobře aproximovat pouze nanejvýš sudé funkce. Nicméně hned první tvrzení věty nám říká, že vždycky budeme dosahovat nejlepší možné aproximace částečnými součty (v $L_2$–vzdálenosti).

Druhé a třetí tvrzení pak můžeme vnímat jako analogii ke kolmým průmětům do podprostorů vyjádřeným pomocí kartézských souřadnic. Skutečně, pokud pro danou funkci $g$ bodově konverguje řada $F(x) = \sum_{n=1}^{\infty} c_n f_n(x)$, pak je funkce $F(x)$ v jistém smyslu kolmým průmětem $g$ do vektorového podprostoru všech takovýchto řad.

Druhému tvrzení se říká *Besselova nerovnost* a je obdobou konečněrozměrného tvrzení, že kolmý průmět vektoru nemůže být větší než původní vektor. Rovnost ze třetího tvrzení se nazývá *Parsevalova rovnost* a říká, že jestliže se vektor kolmým průmětem do podprostoru ostře nezmenší, pak do tohoto podprostoru jistě sám patří.

Na druhé straně ale naše věta neříká, že by částečné součty uvažované řady musely bodově konvergovat k nějaké funkci. To je jev, který v konečněrozměrném světě nemá obdobu. Řada $F(x)$ obecně nemusí být konvergentní (tj. pokud bychom uvažovali obecnější funkce než je náš prostor $\mathcal{S}^0[a, b]$) ani v případě, kdy nastane rovnost v (3). Pokud ale např. existuje konečná hodnota $\sum_{n=1}^{\infty} |c_n|$ a všechny funkce $f_n$ jsou stejnoměrně omezené na $I$, pak zřejmě řada $F(x) = \sum_{n=1}^{\infty} c_n f_n(x)$ konverguje v každém $x$. Nemusí ale přitom konvergovat všude k funkci $g$. K těmto úvahám se brzy vrátíme.

Důkaz všech třech tvrzení věty je velmi podobný jako u konečněrozměrných euklidovských prostorů. Není divu, protože odhady vzdálenosti $g$ od částečného součtu $f$ se vlastně dělají jen v konečněrozměrném lineárním obalu dotčených funkcí:

Důkaz Věty 7.5. Zvolme libovolnou lineární kombinaci $f = \sum_{n=1}^{k} a_n f_n$ a spočtěme její vzdálenost od $g$. Dostáváme

$$\begin{aligned}\|g - \sum_{n=1}^{k} a_n f_n\|^2 &= \int_a^b \left|g(x) - \sum_{n=1}^{k} a_n f_n(x)\right|^2 dx = \\ &= \int_a^b |g(x)|^2\,dx - \int_a^b \sum_{n=1}^{k} g(x)\overline{a_n f_n(x)}\,dx - \\ &\quad - \int_a^b \sum_{n=1}^{k} a_n f_n(x)\overline{g(x)}\,dx + \int_a^b \left|\sum_{n=1}^{k} a_n f_n(x)\right|^2 dx =\end{aligned}$$

(b) $g(x) = |x|,\ x \in [-\pi, \pi)$;

(c) $g(x) = 0,\ x \in [-1, 0), \quad g(x) = x + 1,\ x \in [0, 1)$.

**Řešení.** Případ (a). Přímými výpočty získáváme

$$\begin{aligned}
a_0 &= \tfrac{1}{\pi} \int_{x_0}^{x_0+2\pi} g(x)\,dx = \tfrac{1}{\pi} \int_{-\pi}^{0} 0\,dx + \tfrac{1}{\pi} \int_{0}^{\pi} \sin x\,dx = \\
&= \tfrac{1}{\pi} [-\cos x]_0^{\pi} = \tfrac{2}{\pi}, \\
a_n &= \tfrac{1}{\pi} \int_{x_0}^{x_0+2\pi} g(x) \cos(nx)\ dx = \\
&= \tfrac{1}{\pi} \int_{-\pi}^{0} 0\,dx + \tfrac{1}{\pi} \int_{0}^{\pi} \sin x \cos(nx)\ dx = \\
&= \tfrac{1}{2\pi} \int_{0}^{\pi} \sin([1+n]x) + \sin([1-n]x)\ dx = \\
&= \tfrac{1}{2\pi} \left[ -\tfrac{\cos([1+n]x)}{1+n} - \tfrac{\cos([1-n]x)}{1-n} \right]_0^{\pi} = \\
&= \tfrac{1}{2\pi} \left( -\tfrac{\cos([1+n]\pi)}{1+n} - \tfrac{\cos([1-n]\pi)}{1-n} + \tfrac{1}{1+n} + \tfrac{1}{1-n} \right), \quad n \in \mathbb{N}, \\
b_1 &= \tfrac{1}{\pi} \int_{x_0}^{x_0+2\pi} g(x) \sin x\,dx = \tfrac{1}{\pi} \int_{-\pi}^{0} 0\,dx + \tfrac{1}{\pi} \int_{0}^{\pi} \sin^2 x\,dx = \\
&= \tfrac{1}{2\pi} \int_{0}^{\pi} 1 - \cos(2x)\ dx = \tfrac{1}{2\pi} \left[ x - \tfrac{\sin(2x)}{2} \right]_0^{\pi} = \tfrac{1}{2}, \\
b_n &= \tfrac{1}{\pi} \int_{x_0}^{x_0+2\pi} g(x) \sin(nx)\ dx = \\
&= \tfrac{1}{\pi} \int_{-\pi}^{0} 0\,dx + \tfrac{1}{\pi} \int_{0}^{\pi} \sin x \sin(nx)\ dx = \\
&= \tfrac{1}{2\pi} \int_{0}^{\pi} \cos([1-n]x) - \cos([1+n]x)\ dx = \\
&= \tfrac{1}{2\pi} \left[ \tfrac{\sin([1-n]x)}{1-n} - \tfrac{\sin([1+n]x)}{1+n} \right]_0^{\pi} = 0, \text{ pro } n \in \mathbb{N} \setminus \{1\}
\end{aligned}$$

Dostáváme tak Fourierovu řadu

$$\tfrac{1}{\pi} + \tfrac{\sin x}{2} + \tfrac{1}{2\pi} \sum_{n=1}^{\infty} \left[ \left( -\tfrac{\cos([1+n]\pi)}{1+n} - \tfrac{\cos([1-n]\pi)}{1-n} + \tfrac{1}{1+n} + \tfrac{1}{1-n} \right) \cos(nx) \right].$$

Upravme ještě získaný výsledek. Pro sudá $n$ totiž platí

$$\begin{aligned}
-\tfrac{\cos([1+n]\pi)}{1+n} - \tfrac{\cos([1-n]\pi)}{1-n} + \tfrac{1}{1+n} + \tfrac{1}{1-n} = \\
= \tfrac{1}{1+n} + \tfrac{1}{1-n} + \tfrac{1}{1+n} + \tfrac{1}{1-n} = -\tfrac{4}{n^2-1}
\end{aligned}$$

a pro lichá $n$ pak

$$\begin{aligned}
-\tfrac{\cos([1+n]\pi)}{1+n} - \tfrac{\cos([1-n]\pi)}{1-n} + \tfrac{1}{1+n} + \tfrac{1}{1-n} = \\
= -\tfrac{1}{1+n} - \tfrac{1}{1-n} + \tfrac{1}{1+n} + \tfrac{1}{1-n} = 0.
\end{aligned}$$

Celkem tedy

$$-\tfrac{\cos([1+n]\pi)}{1+n} - \tfrac{\cos([1-n]\pi)}{1-n} + \tfrac{1}{1+n} + \tfrac{1}{1-n} = 2\,\tfrac{(-1)^{n+1}-1}{n^2-1}, \quad n \in \mathbb{N},$$

a tudíž můžeme výslednou řadu zapsat ve tvaru

$$\tfrac{1}{\pi} + \tfrac{\sin x}{2} + \tfrac{1}{\pi} \sum_{n=1}^{\infty} \left[ \tfrac{(-1)^{n+1}-1}{n^2-1} \cos(nx) \right] = \tfrac{1}{\pi} + \tfrac{\sin x}{2} - \tfrac{2}{\pi} \sum_{n=1}^{\infty} \tfrac{\cos(2nx)}{4n^2-1}.$$

Případ (b). Nejprve poznamenejme, že o zadané funkci se často hovoří jako o funkci pilovitých kmitů a že její vyjádření Fourierovou řadou je velmi důležité v aplikacích. Využijeme-li sudosti funkce $g$ na $(-\pi, \pi)$, ihned víme, že je $b_n = 0$ pro všechna $n \in \mathbb{N}$. Stačí nám tedy vypočítat

$$\begin{aligned}
&= \|g\|^2 - \sum_{n=1}^{k} \overline{a_n} c_n \|f_n\|^2 - \sum_{n=1}^{k} a_n \overline{c_n} \|f_n\|^2 + \sum_{n=1}^{k} a_n^2 \|f_n\|^2 = \\
&= \|g\|^2 + \sum_{n=1}^{k} \|f_n\|^2 \big( (c_n - a_n)\overline{(c_n - a_n)} - |c_n|^2 \big).
\end{aligned}$$

Evidentně lze poslední výraz minimalizovat právě volbou $a_n = c_n$, čímž je první tvrzení dokázáno.

Dosazením této volby dostáváme tzv. *Besselovu identitu*

$$\|g - \sum_{n=1}^{k} c_n f_n\|^2 = \|g\|^2 - \sum_{n=1}^{k} |c_n|^2 \|f_n\|^2,$$

ze které okamžitě díky nezápornosti levé strany vyplývá dokazovaná Besselova nerovnost

$$\sum_{n=1}^{k} c_n^2 \|f_n\|^2 \le \|g\|^2.$$

Tím je dokázáno i celé druhé tvrzení, protože každá neklesající a shora omezená posloupnost reálných čísel má limitu (a je jí supremum celé množiny hodnot prvků posloupnosti).

Jestliže v Besselově nerovnosti nastane rovnost, pak přímo z definic a výše dokázané Besselovy identity vyplývá tvrzení (3). □

Ortogonální systém funkcí nazveme *úplný ortogonální systém* na intervalu $I = [a, b]$ pro nějaký prostor funkcí na $I$, jestliže platí Parsevalova rovnost pro každou funkci $g$ z tohoto prostoru.

**7.6. Fourierovy řady.** Předchozí věta naznačuje, že umíme se



spočetnými ortogonálními systémy funkcí $f_n$ pracovat velice podobně jako s konečnými ortogonálními bázemi vektorových prostorů, jsou tu ale zásadní rozdíly:

- Není snadné říci, jak vypadá celý prostor konvergentních nebo stejnoměrně konvergentních řad
$$F(x) = \sum_{n=1}^{\infty} c_n f_n(x).$$
- Pro danou integrovatelnou funkci umíme najít jen „nejlepší možné přiblížení“ takovou řadou $F(x)$ ve smyslu $L_2$–vzdálenosti.

Hovoříme o (abstraktních) *Fourierových řadách* a koeficientům $c_n$ z předchozí věty říkáme *Fourierovy koeficienty* dané funkce.

V případě, že místo ortogonálního systému $f_n$ máme systém ortonormální, jsou formulky ve větě o něco jednodušší, žádné další zlepšení ale nenastane.

Výběr ortogonálního systému funkcí musí pro praktické použití sledovat účel, pro který chceme aproximace a další nástroje použít. Samotný název „Fourierovy řady“ odkazuje na následující volbu systému reálných funkcí:

FOURIERŮV ORTOGONÁLNÍ SYSTÉM

Systém reálných funkcí

$$1,\ \sin x,\ \cos x,\ \sin 2x,\ \cos 2x,\ \ldots,\ \sin nx,\ \cos nx,\ \ldots$$

nazýváme *Fourierův ortogonální systém*.

$$a_0 = \tfrac{1}{\pi}\int_{x_0}^{x_0+2\pi} g(x)\,dx = \tfrac{2}{\pi}\int_0^{\pi} x\,dx = \tfrac{2}{\pi}\left[\tfrac{x^2}{2}\right]_0^{\pi} = \pi$$

a pro libovolné $n \in \mathbb{N}$ pomocí metody per partes dále

$$\begin{aligned} a_n &= \tfrac{1}{\pi}\int_{x_0}^{x_0+2\pi} g(x)\cos(nx)\;dx = \tfrac{2}{\pi}\int_0^{\pi} x\cos(nx)\;dx = \\ &= \tfrac{2}{\pi}\left[\tfrac{x}{n}\sin(nx)\right]_0^{\pi} - \tfrac{2}{n\pi}\int_0^{\pi}\sin(nx)\;dx = \\ &= \tfrac{2}{n^2\pi}\left[\cos(nx)\right]_0^{\pi} = \tfrac{2}{n^2\pi}\left[(-1)^n - 1\right], \text{ tedy} \\ &\quad a_n = -\tfrac{4}{n^2\pi} \text{ pro } n \text{ liché}, \quad a_n = 0 \text{ pro } n \text{ sudé}. \end{aligned}$$

Nyní již známe Fourierovu řadu funkce pilovitých kmitů

$$\begin{aligned} &\tfrac{\pi}{2} + \tfrac{2}{\pi}\sum_{n=1}^{\infty}\left[\tfrac{(-1)^n-1}{n^2}\cos(nx)\right] = \tfrac{\pi}{2} - \tfrac{4}{\pi}\sum_{n=1}^{\infty}\tfrac{\cos([2n-1]x)}{(2n-1)^2} = \\ &\quad = \tfrac{\pi}{2} - \tfrac{4}{\pi}\left[\cos x + \tfrac{\cos(3x)}{3^2} + \tfrac{\cos(5x)}{5^2} + \cdots\right]. \end{aligned}$$

Tuto řadu bylo možné nalézt i jednodušším způsobem – pomocí integrování Fourierovy řady Heavisideovy funkce (viz 7.9).

Případ (c). Funkce má periodu $T = 2$, a proto použijeme obecnější vzorce

$$a_0 = \frac{2}{T}\int_{x_0}^{x_0+T} g(x)\,dx = \int_{-1}^{1} g(x)\,dx = \int_{-1}^{0} 0\,dx + \int_0^1 (x+1)\,dx = \frac{3}{2},$$

$$\begin{aligned} a_n &= \frac{2}{T}\int_{x_0}^{x_0+T} g(x)\cos(n\omega x)\;dx = \int_{-1}^{1} g(x)\cos(n\pi x)\;dx = \\ &= \int_{-1}^{0} 0\,dx + \int_0^1 (x+1)\cos(n\pi x)\;dx = \frac{(-1)^n - 1}{n^2\pi^2}, \quad n \in \mathbb{N}, \end{aligned}$$

$$\begin{aligned} b_n &= \frac{2}{T}\int_{x_0}^{x_0+T} g(x)\sin(n\omega x)\;dx = \int_{-1}^{1} g(x)\sin(n\pi x)\;dx = \\ &= \int_{-1}^{0} 0\,dx + \int_0^1 (x+1)\sin(n\pi x)\;dx = \frac{1-2(-1)^n}{n\pi}, \quad n \in \mathbb{N}. \end{aligned}$$

Výpočet $a_0$ byl snadný a netřeba jej komentovat. K vyčíslení integrálů u $a_n$ a $b_n$ raději doplňme, že opět stačilo jedenkrát použít metodu per partes (derivovat polynom $u = x + 1$). Hledaná Fourierova řada tak je

$$\tfrac{3}{4} + \sum_{n=1}^{\infty}\left(\tfrac{(-1)^n-1}{n^2\pi^2}\cos(n\pi x) + \tfrac{1-2(-1)^n}{n\pi}\sin(n\pi x)\right).$$

Dílčích zjednodušení zápisu můžeme docílit, když si např. uvědomíme, že pro $n \in \mathbb{N}$ platí

$$a_n = -\tfrac{2}{n^2\pi^2} \text{ pro } n \text{ liché}, \quad a_n = 0 \text{ pro } n \text{ sudé}$$

a podobně

$$b_n = \tfrac{3}{n\pi} \text{ pro } n \text{ liché}, \quad b_n = -\tfrac{1}{n\pi} \text{ pro } n \text{ sudé}.$$

Jako elementární cvičení na integraci per partes si můžeme spočíst, že skutečně jde o ortogonální systém funkcí na intervalu $[-\pi, \pi]$. Ukážeme si vzápětí i jiné ověření této skutečnosti.

Jde o tzv. periodické funkce se společnou periodou $2\pi$ (viz definice níže) a tzv. „Fourierova analýza“ opřená o tento ortogonální systém nám umožní mimořádně účinně pracovat se všemi (po částech spojitými) periodickými funkcemi. Vzhledem k tomu, že mnoho fyzikálních, chemických i biologických dat vnímáme, přijímáme nebo měříme ve skutečnosti prostřednictvím frekvencí tzv. signálů (tj. měřených veličin), jde o skutečně základní matematický nástroj. Biologové a inženýři dokonce často používají slovo „signál“ v našem smyslu „funkce“.

### Periodické funkce

Funkce $f$ s reálnými nebo komplexními hodnotami definovaná na celém $\mathbb{R}$ se nazývá *periodická funkce* s periodou $T > 0$, jestliže pro každé $x \in \mathbb{R}$ platí $f(x+T) = f(x)$. Nejmenší perioda $T$ (pokud existuje) se nazývá základní perioda funkce $f$.

Je zjevné, že součty a skalární násobky periodických funkcí se stejnými periodami jsou opět periodické funkce s touž periodou.

Integrál $\int_{x_0}^{x_0+T} f(x)\,dx$ periodické funkce $f$ přes interval délky periody $T$ nezávisí na volbě $x_0 \in \mathbb{R}$.

Poslední tvrzení se dokáže snadno:

Zvolme si dva takové levé hraniční body integrace $x_0$ a $y_0$. Pomocí substituce $t = x + kT$ s vhodným $k$ převedeme $\int_{y_0}^{y_0+T} f(x)\,dx$ na případ, kdy $y_0 \in [x_0, x_0+T]$. Nyní rozdělením intervalu integrace na tři části dokončíme důkaz.

Ortogonalitu Fourierova systému funkcí si můžeme spočíst docela snadno pomocí výletu do komplexních čísel, který se nám bude velice hodit později:



Připomeňme, že pro reálná $x$ je $e^{ix} = \cos(x) + i\sin(x)$. Přímým derivováním součinu reálných funkcí ověříme, že pro funkce $z(x)$ a $\varphi(x)$ s reálnou proměnnou $x$ a s reálnými hodnotami platí

$$\left(z(x)\,e^{i\varphi(x)}\right)' = z'(x)\,e^{i\varphi(x)} + i\,z(x)\,\varphi'(x)\,e^{i\varphi(x)}.$$

Primitivní funkce ke komplexní funkci $f(x)$ s reálnou proměnnou $x$ samozřejmě dostaneme pomocí primitivních funkcí k reálné a imaginární komponentě funkce $f$.

Můžeme si tedy velmi snadno spočíst integrál (předpokládáme $m \neq n$)

$$\int_{-\pi}^{\pi} e^{imx}\,e^{-inx}\,dx = \int_{-\pi}^{\pi} e^{i(m-n)x}\,dx = \tfrac{1}{i(m-n)}[e^{i(m-n)x}]_{-\pi}^{\pi},$$

což je vždy nula, protože je jedno jestli o násobky $\pi$ obíháme po jednotkové kružnici v jednom nebo druhém směru.

Právě spočtený integrál vyjadřuje skalární součin $\langle e^{imx}, e^{inx}\rangle$. Vidíme tedy, že skutečně všechny dvojice našich funkcí $e^{inx}$ (s komplexními hodnotami) jsou na sebe kolmé.

Můžeme ale tento skalární součin rozepsat:

$$\begin{aligned} \langle e^{imx}, e^{inx}\rangle &= \langle \cos(mx) + i\sin(mx), \cos(nx) + i\sin(nx)\rangle = \\ &= \big(\langle\cos(mx), \cos(nx)\rangle + \langle\sin(mx), \sin(nx)\rangle\big) \\ &\quad + i\big(\langle\sin(mx), \cos(nx)\rangle - \langle\cos(mx), \sin(nx)\rangle\big). \end{aligned}$$

Všimněme si, že v imaginární části tohoto výrazu budeme integrovat liché funkce přes interval $[-\pi, \pi]$ a tedy dostaneme zaručeně nulu.

□

**7.7.** Nechť je dána Fourierova řada funkce $f$ na intervalu $[-\pi, \pi]$ s koeficienty $a_m, b_n$, $m \in \mathbb{N} \cup \{0\}$, $n \in \mathbb{N}$. Dokažte následující tvrzení:

(a) Jestliže $f(x) = f(x + \pi)$, $x \in [-\pi, 0]$, potom $a_{2k-1} = b_{2k-1} = 0$ pro každé $k \in \mathbb{N}$.

(b) Jestliže $f(x) = -f(x + \pi)$, $x \in [-\pi, 0]$, potom $a_0 = a_{2k} = b_{2k} = 0$ pro každé $k \in \mathbb{N}$.

**Řešení.** Případ (a). Tvrzení lze pro libovolné $k \in \mathbb{N}$ dokázat přímo výpočty

$$
\begin{aligned}
a_{2k-1} &= \tfrac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos([2k-1]x)\ dx = \\
&= \tfrac{1}{\pi} \int_{-\pi}^{0} f(x) \cos([2k-1]x)\ dx + \tfrac{1}{\pi} \int_{0}^{\pi} f(x) \cos([2k-1]x)\ dx = \\
&= |\, x = y + \pi \,| = \tfrac{1}{\pi} \int_{-2\pi}^{-\pi} f(y+\pi) \cos([2k-1][y+\pi])\ dy + \\
&\quad + \tfrac{1}{\pi} \int_{0}^{\pi} f(x) \cos([2k-1]x)\ dx = \\
&= \tfrac{1}{\pi} \int_{0}^{\pi} f(y) \cos([2k-1][y+\pi])\ dy + \\
&\quad + \tfrac{1}{\pi} \int_{0}^{\pi} f(x) \cos([2k-1]x)\ dx = \\
&= \tfrac{1}{\pi} \int_{0}^{\pi} f(y) \big[ \cos([2k-1]y) \cos([2k-1]\pi) - \\
&\quad - \sin([2k-1]y) \sin([2k-1]\pi) \big]\, dy + \\
&\quad + \tfrac{1}{\pi} \int_{0}^{\pi} f(x) \cos([2k-1]x)\ dx = \\
&= -\tfrac{1}{\pi} \int_{0}^{\pi} f(y) \cos([2k-1]y)\ dy + \\
&\quad + \tfrac{1}{\pi} \int_{0}^{\pi} f(x) \cos([2k-1]x)\ dx = 0, \\
b_{2k-1} &= \tfrac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin([2k-1]x)\ dx = \\
&= \tfrac{1}{\pi} \int_{-\pi}^{0} f(x) \sin([2k-1]x)\ dx + \tfrac{1}{\pi} \int_{0}^{\pi} f(x) \sin([2k-1]x)\ dx = \\
&= |\, x = y + \pi \,| = \tfrac{1}{\pi} \int_{-2\pi}^{-\pi} f(y+\pi) \sin([2k-1][y+\pi])\ dy + \\
&\quad + \tfrac{1}{\pi} \int_{0}^{\pi} f(x) \sin([2k-1]x)\ dx = \\
&= \tfrac{1}{\pi} \int_{0}^{\pi} f(y) \sin([2k-1][y+\pi]) + \tfrac{1}{\pi} \int_{0}^{\pi} f(x) \sin([2k-1]x)\ dx = \\
&= \tfrac{1}{\pi} \int_{0}^{\pi} f(y) \big[ \sin([2k-1]y) \cos([2k-1]\pi) + \\
&\quad + \sin([2k-1]\pi) \cos([2k-1]y) \big]\, dy + \\
&\quad + \tfrac{1}{\pi} \int_{0}^{\pi} f(x) \sin([2k-1]x)\ dx = \\
&= 0.
\end{aligned}
$$

Funkce $\sin(x)$ a $\cos(x)$ se liší jen o fázový posun, tj. $\cos(mx - \pi/2) = \sin(mx)$. Proto jsou oba sčítance v reálné části našeho výrazu stejné. Musí tedy dát nulu oba. Tím jsme ověřili ortogonalitu našeho systému funkcí.

Zároveň vidíme, že pro $m = n$ je výsledkem reálné číslo $\int_{-\pi}^{\pi} dx = 2\pi$ a přitom zjevně musí opět být velikosti jak $\sin(nx)$ tak $\cos(nx)$ stejné. Nutně proto pro kladná $n$ dostáváme velikosti

$$\|\cos(nx)\|^2 = \pi, \quad \|\sin(nx)\|^2 = \pi.$$

Jen pro $n = 0$ dostáváme $\|1\|^2 = 2\pi$.

### Fourierovy řady

Řadu funkcí

$$F(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} \big( a_n \cos(nx) + b_n \sin(nx) \big)$$

z Věty 7.5, s koeficienty

$$a_n = \frac{1}{\pi} \int_{x_0}^{\times_0 + 2\pi} g(x) \cos(nx)\, dx,$$

$$b_n = \frac{1}{\pi} \int_{x_0}^{\times_0 + 2\pi} g(x) \sin(nx)\, dx,$$

nazýváme *Fourierova řada* funkce $g$ na intervalu $[x_0, x_0 + 2\pi]$. Koeficienty $a_n$ a $b_n$ se nazývají *Fourierovy koeficienty funkce* $g$.



V praktickém použití chceme pracovat s Fourierovými řadami s libovolnou délkou periody funkcí $T$ místo hodnoty $2\pi$. Stačí k tomu jen přejít k funkcím $\cos(\frac{2\pi}{T} nx)$, $\sin(\frac{2\pi}{T} nx)$. Jednoduchou substitucí proměnných $t = \omega x$, kde $\omega = \frac{2\pi}{T}$, ověříme ortogonalitu našeho nového systému funkcí a přepočítáme koeficienty ve Fourierově řadě $F(x)$ funkce $g$ na intervalu $[x_0, x_0 + T]$:

$$F(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} \big( a_n \cos(n\omega x) + b_n \sin(n\omega x) \big),$$

které mají hodnoty

$$a_n = \frac{2}{T} \int_{x_0}^{\times_0 + T} g(x) \cos(n\omega x)\, dx,$$

$$b_n = \frac{2}{T} \int_{x_0}^{\times_0 + T} g(x) \sin(n\omega x)\, dx.$$

**7.7. Vyjádření s exponenciálou.** Před chvílí jsme při ověřování ortogonality funkcí $\cos(nx)$, $\sin(nx)$ vyšli ze základního vztahu pro parametrizaci jednotkové kružnice v komplexní rovině pomocí goniometrických funkcí. Uvažujeme-li $\omega = 2\pi/T$ jako rychlost obíhání kružnice, kde $T$ je čas jednoho oběhu, dostáváme tutéž parametrizaci ve tvaru:

$$\mathrm{e}^{i\omega t} = \cos \omega t + i \sin \omega t.$$

Pro (reálnou nebo komplexní) funkci $f(t)$ a všechna celá čísla $n$ si v tomto kontextu definujeme její *komplexní Fourierovy koeficienty* jako komplexní čísla

$$c_n = \frac{1}{T} \int_{-T/2}^{T/2} f(t)\, \mathrm{e}^{-i\omega n t}\ dt.$$

Přímo z definice jsou přitom jasné vztahy mezi koeficienty $a_n$ a $b_n$ Fourierových řad (po přepočtu formulí pro tyto koeficienty pro

$$= -\tfrac{1}{\pi}\int_0^{\pi} f(y)\sin([2k-1]y)\ dy +$$
$$+\ \tfrac{1}{\pi}\int_0^{\pi} f(x)\sin([2k-1]x)\ dx = 0.$$

Případ (b). Okamžitě máme

$$a_0 = \tfrac{1}{\pi}\int_{-\pi}^{\pi} f(x)\,dx = \tfrac{1}{\pi}\int_{-\pi}^{0} f(x)\,dx + \tfrac{1}{\pi}\int_0^{\pi} f(x)\,dx = 0$$

a poté analogicky jako v důkazu prvního tvrzení pro libovolné $k \in \mathbb{N}$ dostáváme

$$a_{2k} = \tfrac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos([2k]x)\ dx =$$
$$= \tfrac{1}{\pi}\int_{-\pi}^{0} f(x)\cos([2k]x)\ dx + \tfrac{1}{\pi}\int_0^{\pi} f(x)\cos([2k]x)\ dx =$$
$$= |\, x = y+\pi \,| =$$
$$= \tfrac{1}{\pi}\int_{-2\pi}^{-\pi} f(y+\pi)\cos([2k][y+\pi])\ dy + \tfrac{1}{\pi}\int_0^{\pi} f(x)\cos([2k]x)\ dx =$$
$$= -\tfrac{1}{\pi}\int_0^{\pi} f(y)\cos([2k][y+\pi])\ dy + \tfrac{1}{\pi}\int_0^{\pi} f(x)\cos([2k]x)\ dx =$$
$$= -\tfrac{1}{\pi}\int_0^{\pi} f(y)\big[\cos([2k]y)\cos([2k]\pi) - \sin([2k]y)\sin([2k]\pi)\big]\ dy +$$
$$+\ \tfrac{1}{\pi}\int_0^{\pi} f(x)\cos([2k]x)\ dx =$$
$$= -\tfrac{1}{\pi}\int_0^{\pi} f(y)\cos([2k]y)\ dy + \tfrac{1}{\pi}\int_0^{\pi} f(x)\cos([2k]x)\ dx = 0,$$
$$b_{2k} = \tfrac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin([2k]x)\ dx =$$
$$= \tfrac{1}{\pi}\int_{-\pi}^{0} f(x)\sin([2k]x)\ dx + \tfrac{1}{\pi}\int_0^{\pi} f(x)\sin([2k]x)\ dx =$$
$$= |\, x = y+\pi \,| =$$
$$= \tfrac{1}{\pi}\int_{-2\pi}^{-\pi} f(y+\pi)\sin([2k][y+\pi])\ dy + \tfrac{1}{\pi}\int_0^{\pi} f(x)\sin([2k]x)\ dx =$$
$$= -\tfrac{1}{\pi}\int_0^{\pi} f(y)\sin([2k][y+\pi])\ dy + \tfrac{1}{\pi}\int_0^{\pi} f(x)\sin([2k]x)\ dx =$$
$$= -\tfrac{1}{\pi}\int_0^{\pi} f(y)\big[\sin([2k]y)\cos([2k]\pi) + \sin([2k]\pi)\cos([2k]y)\big]\ dy +$$
$$+\ \tfrac{1}{\pi}\int_0^{\pi} f(x)\sin([2k]x)\ dx =$$
$$= -\tfrac{1}{\pi}\int_0^{\pi} f(y)\sin([2k]y)\ dy + \tfrac{1}{\pi}\int_0^{\pi} f(x)\sin([2k]x)\ dx = 0\,. \qquad \square$$

**7.8.** Rozhodněte o konvergenci a stejnoměrné konvergenci Fourierovy řady funkce $g(x) = \mathrm{e}^{-x}$ pro $x \in [-1, 1)$.

**Řešení.** K rozhodnutí o konvergenci není třeba příslušnou Fourierovu řadu počítat. Zaveďme funkci $s$ definovanou na $\mathbb{R}$ s periodou $T = 2$ předpisem

$$s(x) := g(x) = \mathrm{e}^{-x},\ x \in (-1,1),\ s(1) := \frac{g(-1) + \lim\limits_{x\to 1-} g(x)}{2} = \frac{\mathrm{e}+\mathrm{e}^{-1}}{2}.$$

O této funkci totiž víme, že je součtem uvažované Fourierovy řady. Jinými slovy, Fourierova řada konverguje k periodické funkci $s$. Navíc tato konvergence je stejnoměrná na každém uzavřeném intervalu, funkce s obecnou periodou délky $T$) a těmito komplexními koeficienty $c_n$. Pro přirozená $n$ dostáváme

$$c_n = \tfrac{1}{2}(a_n - ib_n), \quad c_{-n} = \tfrac{1}{2}(a_n + ib_n)$$

a při výhradně reálných hodnotách funkce $f$ jsou samozřejmě $c_n$ a $c_{-n}$ komplexně konjugované hodnoty.

Vyjádřili jsme tedy Fourierovu řadu $F(t)$ pro funkci $f(t)$ ve tvaru

$$F(t) = \sum_{n=-\infty}^{\infty} c_n\, \mathrm{e}^{i\omega n t}\,.$$

Takto lze psát Fourierovy řady pro funkce s reálnými i komplexními hodnotami, v obou případech ale budou obecně její koeficienty komplexní.

K tomuto vyjádření se ještě několikrát vrátíme, např. až budeme diskutovat prakticky mimořádně užitečnou Fourierovu transformaci.

Všimněme si ještě, že při pevně zvoleném $T$ vyjadřuje výraz $\omega = 2\pi/T$ právě změnu ve frekvenci způsobenou nárůstem $n$ o jedničku. Je to tedy právě diskrétní krok, se kterým při výpočtu koeficientů Fourierovy řady měníme frekvence.

V pozdější části této kapitoly ukážeme, že Fourierovy řady pracují s úplným ortogonálním systémem na $\mathcal{S}^0$. Budeme se na to ale muset napřed důkladně připravit. Proto zde teď zformulujeme užitečné výsledky předem a hned uvedeme několik praktičtěji orientovaných poznámek. K důkazům se vrátíme později.

**7.8. Věta.** *Uvažujme konečný interval $[a, b]$ s délkou $T = b - a$. Dále nechť $f$ je funkce s reálnými nebo komplexními hodnotami v $\mathcal{S}^1[a, b]$ (tj. po částech spojitá funkce s po částech spojitou první derivací), periodicky rozšířená na celé $\mathbb{R}$. Potom platí:*

*(1) Částečné součty $s_N$ její Fourierovy řady konvergují bodově k funkci*

$$g(x) = \tfrac{1}{2}\big(\lim_{y\to x_+} f(y) + \lim_{y\to x_-} f(y)\big).$$

*(2) Je-li navíc $f$ spojitá periodická funkce s po částech spojitou derivací, pak je bodová konvergence její Fourierovy řady stejnoměrná.*

*(3) $L_2$–vzdálenost $\|s_N - f\|_2$ částečných součtů $s_N$ Fourierovy řady od funkce $f$ na $\mathcal{S}^1[a, b]$ vždy konverguje k nule při $N \to \infty$.*

**7.9. Rozvoj periodických funkcí.** Konvergentní Fourierova řada



bude samozřejmě konvergovat i mimo původní interval $[-T/2, T/2]$ a bude periodickou funkcí na celém $\mathbb{R}$.

Jako příklad uveďme Fourierovu řadu pro periodickou funkci vzniklou z obdoby Heavisideovy funkce $g(x)$ zúžením na jednu periodu. Naše funkce $g$ nyní bude na intervalu $[-\pi, 0]$ rovna $-1$ a na intervalu $(0, \pi)$ bude rovna 1. Hodnotami v nule a v krajních bodech intervalu se nemusíme zabývat, protože stejně na koeficienty Fourierovy řady nebudou mít žádný vliv. Jejímu periodickému rozšíření na celé $\mathbb{R}$ se říkává „hranatá vlnová funkce“ (v angličtině „square wave function“).

Protože jde o funkci lichou, jistě budou všechny koeficienty u funkcí $\cos(nx)$ nulové. Pro koeficienty u funkcí $\sin(nx)$

který neobsahuje žádný z bodů $2k+1$, $k \in \mathbb{Z}$. To vyplývá ze spojitosti funkcí $g$ a $g'$ na $(-1, 1)$. Konvergence pak nemůže být stejnoměrná na žádném intervalu $(c, d)$ s vlastností $[c, d] \cap \{2k+1;\ k \in \mathbb{Z}\} \neq \emptyset$, protože stejnoměrnou limitou spojitých funkcí je vždy funkce spojitá. Zvláště tak řada konverguje k funkci $g$ na $(-1, 1)$, ale tato konvergence je stejnoměrná pouze na podintervalech $[c, d]$ splňujících omezení $-1 < c < d < 1$. □

**7.9.** Určete kosinovou Fourierovu řadu pro periodické prodloužení funkce

$$g(x) = 1,\ x \in [0, 1), \quad g(x) = 0,\ x \in [1, 4)$$

a sinovou Fourierovu řadu pro

$$f(x) = x - 1,\ x \in (0, 2), \quad f(x) = 3 - x,\ x \in [2, 4).$$

**Řešení.** S konstrukcí kosinové Fourierovy řady jsme se již vlastně setkali. Jedná se totiž o Fourierovy řady sudých funkcí. Nejprve tedy musíme funkci $g$ dodefinovat na intervalu $(-4, 0)$ tak, aby se stala sudou, což znamená položit

$$g(x) := 1 \text{ pro } x \in (-1, 0), \quad g(x) := 0 \text{ pro } x \in (-4, -1].$$

Nyní můžeme uvažovat její periodické rozšíření na celé $\mathbb{R}$ s periodou $T = 8$ a $\omega = \pi/4$.

V kosinové řadě vždy musí být $b_n = 0$ pro všechna $n \in \mathbb{N}$. Snadno stanovíme také Fourierovy koeficienty

$$a_0 = \frac{2}{T}\int_{x_0}^{x_0+T} g(x)\,dx = \frac{1}{2}\int_0^1 1\,dx = \frac{1}{2},$$

$$a_n = \frac{2}{T}\int_{x_0}^{x_0+T} g(x)\cos(n\omega x)\,dx = \frac{1}{2}\int_0^1 \cos\frac{n\pi x}{4}\,dx =$$

$$= \frac{2}{n\pi}\sin\frac{n\pi}{4},\ n \in \mathbb{N},$$

kde jsme si pomohli vztahem

$$\int_{-a}^{a} f(x)\,dx = 2\int_0^a f(x)\,dx \tag{7.8}$$

platným pro každou sudou funkci $f$ integrovatelnou na intervalu $[0, a]$.

Nahrazovat výraz $\sin(n\pi/4)$ podobně jako v dřívějších příkladech není dobrý nápad, protože bychom museli rozdělit přirozená čísla $n$ hned do 8 skupin podle jejich zbytku po dělení právě číslem 8. Tím bychom ale neobdrželi příliš přehledné vyjádření. Spokojíme se tudíž s tvarem kosinové Fourierovy řady

$$\tfrac{1}{4} + \sum_{n=1}^{\infty}\left[\tfrac{2}{n\pi}\sin\tfrac{n\pi}{4}\cos\tfrac{n\pi x}{4}\right].$$

spočteme

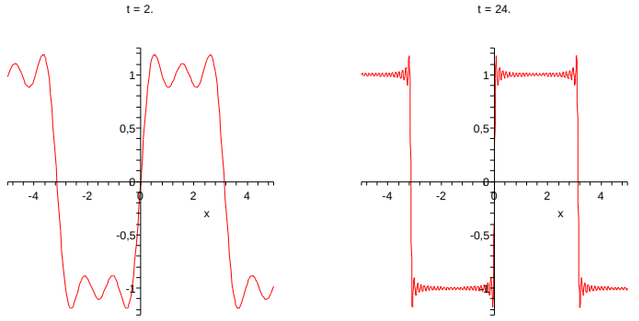
$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} g(x)\sin(nx)\,dx = \frac{2}{\pi}\int_0^{\pi}\sin(nx)\,dx =$$

$$= \frac{2}{n\pi}(1 - (-1)^n).$$

Výsledná Fourierova řada je tedy tvaru

$$g(x) = \frac{4}{\pi}\left(\sin(x) + \frac{1}{3}\sin(3x) + \frac{1}{5}\sin(5x) + \dots\right)$$

a součet jejích prvních pěti a prvních padesáti členů je na následujících dvou obrázcích.




Pokud za základní periodu pro takovou hranatou vlnovou funkci zvolíme interval $[-T/2, T/2]$, tj. chceme pracovat s periodickým rozšířením naší funkce s periodou $T$, jednoduše přepočítáme, že výsledná Fourierova řada je tvaru

$$g(x) = \frac{4}{\pi}\left(\sin(\omega x) + \frac{1}{3}\sin(3\omega x) + \frac{1}{5}\sin(5\omega x) + \dots\right),$$

kde číslu $\omega = \frac{2\pi}{T}$ se říká „fázová frekvence“ vlny. Vyjadřuje poměr skutečné základní periody k frekvenci jednotkové, tj. délce jednotkové kružnice $2\pi$.

Všimněme si, že se zvyšujícím se počtem členů řady se výrazně zpřesňuje aproximace s výjimkou stále se zmenšujícího okolí bodu nespojitosti, na němž je ale maximum odchylky stále zhruba stejné. Je to obecná vlastnost Fourierových řad, které se říká *Gibbsův jev*.

Povšimněme si také, že v samotném bodě nespojitosti je hodnota aproximující funkce právě v polovině mezi limitami zprava a zleva pro naši funkci $g$, přesně jak říká 7.8(1).

Samozřejmě nelze očekávat, že by konvergence Fourierových řad pro funkce $g$ s body nespojitosti mohla být stejnoměrná (to by totiž $g$ musela být coby stejnoměrná limita spojitých funkcí sama spojitá).

**7.10. Využití symetrie funkcí.** Zamysleme se, jak bychom mohli co nejlépe aproximovat Fourierovou řadou funkci $g(x) = x^2$ na intervalu $[0, 1]$. Kdybychom prostě periodicky rozšířili tuto funkci z daného intervalu $[0, 1]$, nebude spojitá a tedy i konvergence v celých číslech by byla podobně podivná jako u hranaté vlnové funkce. Můžeme ale snadno pracovat s Fourierovou řadou na základním intervalu $[-1, 1]$. Jde o sudou funkci, a tedy nenulové mohou být pouze koeficienty $a_n$.

Sinovou Fourierovu řadu funkce analogicky počítáme z lichého prodloužení zadaného úseku. Pro funkci $f$ je opět $T = 8$ a $\omega = \pi/4$. Tentokráte jsou však nulové koeficienty $a_n$, $n \in \mathbb{N} \cup \{0\}$. K nalezení zbývajících koeficientů užitím metody per partes a (‖7.8‖) (součinem 2 lichých funkcí je funkce sudá) získáme

$$\begin{aligned}
b_n &= \frac{2}{T}\int_{x_0}^{x_0+T} f(x)\sin(n\omega x)\,dx = \\
&= \frac{1}{2}\left[\int_0^2 (x-1)\sin\frac{n\pi x}{4}\,dx - \int_2^4 (x-3)\sin\frac{n\pi x}{4}\,dx\right] = \\
&= \left[-(x-1)\frac{2}{n\pi}\cos\frac{n\pi x}{4}\right]_0^2 + \left[\frac{8}{n^2\pi^2}\sin\frac{n\pi x}{4}\right]_0^2 - \\
&\quad - \left[-(x-3)\frac{2}{n\pi}\cos\frac{n\pi x}{4}\right]_2^4 - \left[\frac{8}{n^2\pi^2}\sin\frac{n\pi x}{4}\right]_2^4 = \\
&= \frac{2}{n\pi}\left[(-1)^n - 1\right] + \frac{16}{n^2\pi^2}\sin\frac{n\pi}{2}, \quad n \in \mathbb{N}.
\end{aligned}$$

Ihned odsud vidíme, že pro sudá $n$ je $b_n = 0$. Sinovu Fourierovou řadu díky tomu upravíme do tvaru $\sum_{n=1}^{\infty}\left[\left(\frac{2}{n\pi}\left[(-1)^n - 1\right] + \frac{16}{n^2\pi^2}\sin\frac{n\pi}{2}\right)\sin\frac{n\pi x}{4}\right] =$
$= \sum_{n=1}^{\infty}\left[\left(\frac{-4}{[2n-1]\pi} + \frac{(-1)^{n-1}16}{[2n-1]^2\pi^2}\right)\sin\frac{[2n-1]\pi x}{4}\right]$.

□

**7.10.** Funkci $g(x) = \cos x$, $x \in (0, \pi)$ zapište jako součet kosinové a sinové Fourierovy řady.

**Řešení.** Samozřejmě platí

$$\cos x = \cos x, \quad x \in (-\pi, \pi),$$

přičemž na kosinus na levé straně nahlížíme jako na sudé rozšíření funkce $g$ a na pravé straně jako na kosinovou Fourierovu řadu, která je dána jednoznačně.

Pro sinovou řadu pak musí být $a_n = 0, n \in \mathbb{N} \cup \{0\}$ a snadno také spočítáme

$$\begin{aligned}
b_1 &= \frac{2}{\pi}\int_0^{\pi}\cos x\sin x\,dx = \frac{1}{\pi}\int_0^{\pi}\sin(2x)\,dx = 0, \\
b_n &= \frac{2}{\pi}\int_0^{\pi}\cos x\sin(nx)\,dx = \\
&= \frac{1}{\pi}\int_0^{\pi}\sin([n+1]x) + \sin([n-1]x)\,dx =
\end{aligned}$$

Pro $n > 0$ dvojnásobným využitím metody per partes dostáváme:

$$\begin{aligned}
a_n &= \frac{2}{2}\int_{-1}^{1} x^2\cos\left(\tfrac{2\pi n x}{2}\right)dx = 2\int_0^1 x^2\cos(\pi n x)dx = \\
&= \frac{4}{\pi^2 n^2}(-1)^n.
\end{aligned}$$

Zbývající koeficient je

$$a_0 = \frac{2}{2}\int_{-1}^{1} x^2\,dx = 2\int_0^1 x^2\,dx = \frac{2}{3}.$$

Celá řada dávající periodické rozšíření $x^2$ z intervalu $[-1, 1]$ je tedy

$$f(x) = \frac{1}{3} + \frac{4}{\pi^2}\sum_{n=1}^{\infty}\frac{(-1)^n}{n^2}\cos(\pi n x).$$

Z Weierstrassova kritéria je přímo zřejmé, že tato řada konverguje stejnoměrně a tedy bude $f(x)$ spojitá. Z Věty 7.8 ale už víme, že ve skutečnosti je $f(x) = x^2$ na celém intervalu $[-1, 1]$, protože aproximujeme spojitou funkci na celém $\mathbb{R}$ a konvergence musí být stejnoměrná. Aproximuje tedy naše řada funkci $x^2$ na intervalu $[0, 1]$ výrazně lépe, než bychom to uměli s periodickým rozšířením dané funkce jen z tohoto intervalu.

Pojďme ale v našich ilustracích dále. Díky stejnoměrné konvergenci můžeme využít věty o derivování a integrování řad člen po členu a spočítat Fourierovy řady pro funkce $x$ a $x^3$. Jednodušší bude derivování:

$$\frac{1}{2}(x^2)' = x = \frac{2}{\pi}\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\sin(\pi n x).$$

Tato řada už evidentně nemůže konvergovat stejnoměrně, protože periodické rozšíření funkce $x$ není spojitou funkcí. Docela snadno lze ale přímo odvodit, že bodově konvergovat bude (viz naše úvahy o alternujících řadách v 5.48), proto jsme skutečně dostali rovnost (viz věta 5.48 na straně 280).

Obdobně můžeme člen po členu integrovat a dostaneme

$$\frac{1}{3}x^3 = \frac{2}{3}x + \frac{4}{\pi^3}\sum_{n=1}^{\infty}\frac{(-1)^n}{n^3}\sin(\pi n x)$$

a výslednou Fourierovu řadu dostaneme dosazením za $x$ z předchozí rovnosti.

**7.11. Obecné Fourierovy řady a wavelety.** V případě obecného ortogonálního systému funkcí $f_n$ a z něj vytvářených řad se často hovoří o *obecných Fourierových řadách* vzhledem k ortogonálnímu systému funkcí $f_n$.



Fourierovy řady a další z nich vycházející nástroje jsou využívány ke zpracování různých signálů, obrázků apod. Povaha použitých periodických goniometrických funkcí v klasických Fourierových řadách a jejich prosté škálování pomocí zvětšující se frekvence zároveň omezují jejich použitelnost. V mnoha oblastech aplikací proto vyvstala přirozená potřeba nalézt šikovnější úplné ortogonální systémy funkcí, které budou vycházet z předpokládané povahy dat a které bude možné efektivněji zpracovávat.

Obvyklým požadavkem pro rychlá numerická zpracování bývá rychlá škálovatelnost měřítek a možnost snadného posuvu o konstantní hodnoty. V takový systém lze například doufat, jestliže zvolíme vhodnou spojitou funkci $\psi$ s kompaktním nosičem,

$$= -\frac{1}{\pi}\left[\frac{\cos([n+1]x)}{n+1} + \frac{\cos([n-1]x)}{n-1}\right]_0^{\pi} =$$
$$= \frac{2n\,[(-1)^n+1]}{(n^2-1)\pi}, \quad n \in \mathbb{N} \setminus \{1\}.$$

Jestliže uvážíme, že

$$b_n = 0 \text{ pro lichá } n \in \mathbb{N} \quad \text{a} \quad b_n = \tfrac{4n}{(n^2-1)\pi} \text{ pro sudá } n,$$

získáme

$$\cos x = \sum_{n=1}^{\infty}\left[\tfrac{8n}{(4n^2-1)\pi}\sin(2nx)\right], \quad x \in (0,\pi).$$

□

**7.11.** Napište Fourierovu řadu $\pi$-periodické funkce, která se rovná kosinu na intervalu $(-\pi/2, \pi/2)$, a kosinovou Fourierovu řadu $2\pi$-periodické funkce $y = |\cos x|$.

**Řešení.** Není obtížné si uvědomit, že hledáme pouze jednu Fourierovu řadu (druhá část zadání je reformulací té první). Sestrojme tedy Fourierovu řadu pro funkci $g(x) = \cos x$, $x \in [-\pi/2, \pi/2]$. Ze sudosti $g$ plyne $b_n = 0$, $n \in \mathbb{N}$. Současně máme

$$a_0 = \tfrac{2}{\pi}\int_{-\pi/2}^{\pi/2} \cos x\,dx = \tfrac{4}{\pi},$$
$$a_n = \tfrac{2}{\pi}\int_{-\pi/2}^{\pi/2} \cos x\cos(2nx)\,dx =$$
$$= \tfrac{2}{\pi}\int_{-\pi/2}^{\pi/2} \tfrac{1}{2}[\cos([2n+1]x) + \cos([2n-1]x)]\,dx =$$
$$= \tfrac{1}{\pi}\left[\tfrac{\sin([2n+1]x)}{2n+1} + \tfrac{\sin([2n-1]x)}{2n-1}\right]_{-\pi/2}^{\pi/2} = \tfrac{2}{\pi}\left[\tfrac{(-1)^n}{2n+1} + \tfrac{(-1)^{n+1}}{2n-1}\right] =$$
$$= \tfrac{4}{\pi}\tfrac{(-1)^{n+1}}{4n^2-1}$$

pro každé $n \in \mathbb{N}$. Všimněme si, že výpočet $a_0$ bylo možné zahrnout do výpočtu obecného $a_n$. Hledanou Fourierovou řadou je

$$\tfrac{2}{\pi} + \tfrac{4}{\pi}\sum_{n=1}^{\infty}\left[\tfrac{(-1)^{n+1}}{4n^2-1}\cos(2nx)\right].$$

□

**7.12.** Funkci $g(x) = e^x$ rozviňte do

(a) Fourierovy řady na intervalu $[0, 1)$;

(b) kosinové Fourierovy řady na intervalu $[0, 1]$;

(c) sinové Fourierovy řady na intervalu $(0, 1]$.

**Řešení.** V celé úloze budeme využívat vztahů

(7.9)
$$\int e^x\cos(\alpha x)\,dx = \frac{e^x[\alpha\sin(\alpha x) + \cos(\alpha x)]}{1+\alpha^2} + C, \quad \alpha \in \mathbb{R},$$

(7.10)
$$\int e^x\sin(\beta x)\,dx = \frac{e^x[\sin(\beta x) - \beta\cos(\beta x)]}{1+\beta^2} + C, \quad \beta \in \mathbb{R},$$

které lze obdržet dvojí aplikací metody per partes.

S jejich pomocí postupně vypočítáme

ze které sestrojíme spočetně mnoho funkcí $\psi_{jk}$, $j, k \in \mathbb{Z}$, pomocí translací a dilatací:

$$\psi_{jk}(x) = 2^{j/2}\psi(2^j x - k).$$

Pokud zároveň vyhovíme dvěma podmínkám:

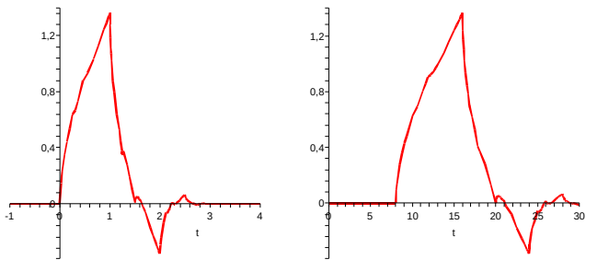
- tvar *mateřské funkce* $\psi$ dobře vystihuje možné chování dat,
- její potomci $\psi_{jk}$ tvoří úplný ortogonální systém,

pak bude dobře stačit k aproximaci konkrétního zpracovávaného signálu jen několika málo funkcí. Hovoříme o tzv. *waveletech*.

Nemáme zde prostor pro podrobnosti, jde o mimořádně živý směr výzkumu i základ komerčních aplikací. Zájemce snadno najde spoustu literatury.

Poznamenejme však, že ve skutečnosti se velmi často používají pouze diskrétní verze našich objektů, tzn. hodnoty všech funkcí $\psi_{jk}$ jsou pouze tabelovány v diskrétní (hodně velké) množině bodů a jsou v tomto smyslu i ortogonální. Dobrým příkladem jsou standardy JPEG2000, které tuto techniku používají a jsou nástrojem pro profesionální komprimaci obrazových dat ve filmovém průmyslu, nebo formát DjVu komprimace publikací.

Jedny z prvních waveletů sestrojila Ingrid Daubechies na začátku devadesátých let. Na obrázku níže je tzv. Daubechies mateřská wavelet $D4(x)$ a její dcera $D4(2^{-3}x - 1)$.




Průběh funkce $D4$ není popsán analytickým způsobem. Funkce je zadána pouze tabelovanými hodnotami pro konečnou (byť velmi velkou) množinu argumentů. Je zvolena tak, aby měla ve svých různých částech všechny vlastnosti, které jsou třeba pro grafická data potřebné — pomalý i rychlý růst, ostrý zlom v obou extrémech apod. Složitost konstrukce spočívá samozřejmě v tom, abychom skutečně dostali pomocí výše uvedené konstrukce ortogonální systém!

## 2. Metrické prostory

V této části kapitoly se abstraktně zamyslíme nad pojmy vzdálenost a konvergence. Bude se nám to hodit vzápětí při důkazech již formulovaných výsledků o Fourierových řadách a v nejrůznějších kontextech se k těmto pojmům budeme vracet. Berme proto další stránky jako velmi užitečný (a snad ještě stále stravitelný) výlet do matematiky pro zdatné či odvážné.

**7.12. Metriky a normy.** 
Při odvozování techniky Fourierových řad jsme volně hovořili o vzdálenosti na prostoru funkcí. Nyní se u tohoto pojmu zastavíme pořádněji. Euklidovská vzdálenost ve vektorových prostorech $\mathbb{R}^n$ splňuje, stejně jako tomu bylo u naší $L_1$–vzdálenosti $d(f,g) = \|f-g\|_1$ na prostoru spojitých absolutně integrovatelných funkcích, následující tři abstraktní požadavky. Mějme v dalších odstavcích pořád na paměti tyto dva příklady.

$$a_0 = 2\int_0^1 \mathrm{e}^x\,dx = 2(\mathrm{e}-1),$$

$$a_n = 2\int_0^1 \mathrm{e}^x\cos(2n\pi x)\,dx = 2\left[\frac{\mathrm{e}^x[2n\pi\sin(2n\pi x)+\cos(2n\pi x)]}{1+4n^2\pi^2}\right]_0^1 =$$

(a)

$$= \frac{2(\mathrm{e}-1)}{1+4n^2\pi^2}, \quad n\in\mathbb{N},$$

$$b_n = 2\int_0^1 \mathrm{e}^x\sin(2n\pi x)\,dx = 2\left[\frac{\mathrm{e}^x[\sin(2n\pi x)-2n\pi\cos(2n\pi x)]}{1+4n^2\pi^2}\right]_0^1 =$$

$$= \frac{4n\pi(1-\mathrm{e})}{1+4n^2\pi^2}, \quad n\in\mathbb{N};$$

(b)

$$a_0 = 2\int_0^1 \mathrm{e}^x\,dx = 2(\mathrm{e}-1),$$

$$a_n = 2\int_0^1 \mathrm{e}^x\cos(n\pi x)\,dx = 2\left[\frac{\mathrm{e}^x[n\pi\sin(n\pi x)+\cos(n\pi x)]}{1+n^2\pi^2}\right]_0^1 =$$

$$= \frac{2\left[(-1)^n\mathrm{e}-1\right]}{1+n^2\pi^2}, \quad n\in\mathbb{N};$$

(c)

$$b_n = 2\int_0^1 \mathrm{e}^x\sin(n\pi x)\,dx = 2\left[\frac{\mathrm{e}^x[\sin(n\pi x)-n\pi\cos(n\pi x)]}{1+n^2\pi^2}\right]_0^1 =$$

$$= \frac{2n\pi\left[1+(-1)^{n+1}\mathrm{e}\right]}{1+n^2\pi^2}, \quad n\in\mathbb{N}$$

a následně pouhým dosazením získáme příslušné Fourierovy řady

(a)

$$\mathrm{e}-1+2(\mathrm{e}-1)\sum_{n=1}^{\infty}\frac{\cos(2n\pi x)}{1+4n^2\pi^2}+4\pi(1-\mathrm{e})\sum_{n=1}^{\infty}\frac{n\sin(2n\pi x)}{1+4n^2\pi^2};$$

(b)

$$\mathrm{e}-1+2\sum_{n=1}^{\infty}\frac{\left[(-1)^n\mathrm{e}-1\right]\cos(n\pi x)}{1+n^2\pi^2};$$

(c)

$$2\pi\sum_{n=1}^{\infty}\frac{n\left[1+(-1)^{n+1}\mathrm{e}\right]\sin(n\pi x)}{1+n^2\pi^2}.$$

□

**7.13.** Funkci $g(x)=\pi^2-x^2$ na intervalu $[-\pi,\pi]$ vyjádřete jako součet Fourierovy řady. Pomocí tohoto vyjádření sečtěte číselné řady

$$\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^2}, \qquad \sum_{n=1}^{\infty}\frac{1}{n^2}.$$

**Řešení.** Také nyní bychom mohli využít sudosti zadané funkce $g$ a metodou per partes spočítat nenulové koeficienty $a_n$. V teoretické části je však odvozena Fourierova řada pro funkci $f(x)=x^2$ na intervalu $[-1,1]$. Tím je vlastně dokázána identita

$$f(x)=\tfrac{1}{3}+\tfrac{4}{\pi^2}\sum_{n=1}^{\infty}\frac{(-1)^n\cos(n\pi x)}{n^2}, \quad x\in(-1,1).$$

Odtud pak (s přihlédnutím k rovnosti $g(-\pi)=g(\pi)$) plyne

$$g(x) = \pi^2-\left(\tfrac{1}{3}+\tfrac{4}{\pi^2}\sum_{n=1}^{\infty}\frac{(-1)^n\cos\frac{n\pi x}{\pi}}{n^2}\right)\pi^2 =$$

$$= \tfrac{2}{3}\pi^2+4\sum_{n=1}^{\infty}\frac{(-1)^{n+1}\cos(nx)}{n^2}, \quad x\in[-\pi,\pi].$$

Stačilo přičíst $\pi^2$ a původní řadu vynásobit $-1$. Dále je třeba si uvědomit, že v argumentu kosinů bude pouze $nx$ místo $n\pi x$. Perioda je tak $\pi$-násobná (mění se $2/T$ a meze integrálu ve vzorci pro $a_n$) a při integrování kosinů nyní nedostáváme $\pi$ ve jmenovatelích (při výpočtu $a_0$ se projeví změna horní meze). Proto jsme museli původní řadu ještě

### Axiomy metriky a normy

Množina $X$ spolu se zobrazením $d: X\times X\to\mathbb{R}$ splňující pro všechny prvky $x, y, z\in X$ podmínky

(7.2) $d(x,y)\geq 0$ a $d(x,y)=0$, právě když $x=y$,

(7.3) $d(x,y)=d(y,x)$,

(7.4) $d(x,z)\leq d(x,y)+d(y,z)$

se nazývá *metrický prostor*. Zobrazení $d$ je *metrika* na $X$.

Je-li $X$ vektorový prostor nad $\mathbb{R}$ a $\|\ \|: X\to\mathbb{R}$ je funkce splňující

(7.5) $\|x\|\geq 0$, přičemž $\|x\|=0$, právě když $x=0$,

(7.6) $\|\lambda x\|=|\lambda|\,\|x\|$, pro všechny skaláry $\lambda$,

(7.7) $\|x+y\|\leq\|x\|+\|y\|$,

pak funkci $\|\ \|$ nazýváme *norma* na $X$ a prostor $X$ je *normovaný vektorový prostor*.

Norma vždy zadává metriku $d(x,y)=\|x-y\|$.

Na začátku předchozí části této kapitoly jsme tedy ve skutečnosti definovali vzdálenost funkcí pomocí tzv. $L_1$–normy. V euklidovských vektorových prostorech pak šlo také o normu $\|x\|$, která je indukována z bilineárního skalárního součinu vztahem $\|x\|^2=\langle x,x\rangle$, a obdobně jsme pracovali s normou na prostorech unitárních. Úplně stejně jsme pak obdrželi na spojitých funkcích $L_2$–normu.

Samozřejmě metriky zadané normou mají velmi specifické vlastnosti, protože jejich chování lze na celém prostoru $X$ odvodit z vlastností v libovolně malém okolí nulového prvku $x=0\in X$.

**7.13. Konvergence.** Na zcela abstraktních metrických prostorech lze zavést pojem (blízkých) okolí jednotlivých prvků, konvergence posloupností prvků a související „topologické“ pojmy prakticky úplně stejně, jako jsme to udělali pro reálná a komplexní čísla a jejich posloupnosti na začátku páté kapitoly, viz 5.12–5.17.



Můžeme tyto odstavce skoro zkopírovat, jen u věty 5.17 narazíme na výrazně složitější důkazy. Začneme konceptem konvergentních posloupností v metrickém prostoru $X$ s metrikou $d$:

### Cauchyovské posloupnosti

Uvažme libovolnou posloupnost prvků $x_0, x_1, \ldots$ v $X$ takovou, že pro libovolné pevně zvolené kladné reálné číslo $\varepsilon$ platí pro všechny dvojice prvků $x_i, x_j$ posloupnosti, až na konečně mnoho výjimek (které závisí na volbě $\varepsilon$),

$$d(x_i,x_j)<\varepsilon.$$

Jinak řečeno, pro každé pevné $\varepsilon>0$ existuje index $N$ takový, že předcházející nerovnost platí pro všechna $i, j>N$. Takové posloupnosti prvků se říká *cauchyovská posloupnost*.

Stejně jako u reálných či komplexních čísel bychom rádi, aby každá cauchyovská posloupnost prvků $x_i\in X$ konvergovala k nějaké hodnotě $x$ v následujícím smyslu:

### Konvergentní posloupnosti

Jestliže pro posloupnost prvků $x_0, x_1, \ldots\in X$, pevně zvolený prvek $x\in X$ a pro libovolné kladné reálné číslo $\varepsilon$ platí pro všechna $i$, až na konečně mnoho výjimek (závisejících na volbě $\varepsilon$),

$$d(x_i,x)<\varepsilon,$$

vynásobit $\pi^2$. Jestliže čtenář není schopen projít si příslušné výpočty v hlavě a hned si uvědomit, kde vzniknou odlišnosti, doporučujeme mu, aby Fourierovu řadu funkce $g$ raději vypočítal přímo.

Když dosadíme $x = 0$ a $x = \pi$, obdržíme již

$$\pi^2 = \tfrac{2}{3}\pi^2 + 4\sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}}{n^2}, \quad \text{tj.} \quad \sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}}{n^2} = \tfrac{\pi^2}{12},$$

a

$$0 = \tfrac{2}{3}\pi^2 + 4\sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}(-1)^n}{n^2}, \quad \text{tj.} \quad \sum_{n=1}^{\infty} \tfrac{1}{n^2} = \tfrac{\pi^2}{6}.$$

Jinak řečeno, nalezli jsme další způsob, jak lze vyjádřit

$$\pi^2 = 12\left(1 - \tfrac{1}{2^2} + \tfrac{1}{3^2} - \tfrac{1}{4^2} + \cdots\right) = 6\left(1 + \tfrac{1}{2^2} + \tfrac{1}{3^2} + \tfrac{1}{4^2} + \cdots\right).$$

□

**7.14.** Pomocí Fourierovy řady funkce $g(x) = \mathrm{e}^x, x \in [0, 2\pi)$, vyčíslete $\sum_{n=1}^{\infty} \frac{1}{1+n^2}$.

**Řešení.** Platí (viz také (‖7.9‖), (‖7.10‖))

$$\begin{aligned}
a_0 &= \tfrac{1}{\pi}\int_0^{2\pi} \mathrm{e}^x\,dx = \tfrac{1}{\pi}\left(\mathrm{e}^{2\pi} - 1\right), \\
a_n &= \tfrac{1}{\pi}\int_0^{2\pi} \mathrm{e}^x \cos(nx)\,dx = \tfrac{1}{\pi}\left[\tfrac{\mathrm{e}^x[\cos(nx)+n\sin(nx)]}{1+n^2}\right]_0^{2\pi} = \\
&= \tfrac{\mathrm{e}^{2\pi}-1}{(1+n^2)\pi}, \quad n \in \mathbb{N}, \\
b_n &= \tfrac{1}{\pi}\int_0^{2\pi} \mathrm{e}^x \sin(nx)\,dx = \\
&= \tfrac{1}{\pi}\left[\tfrac{\mathrm{e}^x[\sin(nx)-n\cos(nx)]}{1+n^2}\right]_0^{2\pi} = -\tfrac{n(\mathrm{e}^{2\pi}-1)}{(1+n^2)\pi}, \quad n \in \mathbb{N}.
\end{aligned}$$

Proto je

$$\mathrm{e}^x = \tfrac{\mathrm{e}^{2\pi}-1}{\pi}\left(\tfrac{1}{2} + \sum_{n=1}^{\infty} \tfrac{\cos(nx)-n\sin(nx)}{1+n^2}\right), \quad x \in (0, 2\pi).$$

Žádnou volbou $x \in (0, 2\pi)$ ale nelze na pravé straně získat řadu $\sum_{n=1}^{\infty} \frac{1}{1+n^2}$. Tu bychom obdrželi pro $x = 0$. V tomto bodě zjevně není periodické prodloužení $g$ na $\mathbb{R}$ spojité, a tak dostáváme

$$\tfrac{\mathrm{e}^0+\mathrm{e}^{2\pi}}{2} = \tfrac{g(0)+\lim\limits_{x\to 2\pi-} g(x)}{2} = \tfrac{\mathrm{e}^{2\pi}-1}{\pi}\left(\tfrac{1}{2} + \sum_{n=1}^{\infty} \tfrac{\cos 0 - n\sin 0}{1+n^2}\right),$$

odkud plyne

$$\tfrac{\mathrm{e}^{2\pi}+1}{2} \cdot \tfrac{\pi}{\mathrm{e}^{2\pi}-1} = \tfrac{1}{2} + \sum_{n=1}^{\infty} \tfrac{1}{1+n^2}$$

a po úpravě

$$\sum_{n=1}^{\infty} \tfrac{1}{1+n^2} = \tfrac{(\pi-1)\,\mathrm{e}^{2\pi}+\pi+1}{2(\mathrm{e}^{2\pi}-1)}.$$

□

**7.15.** Určete součet řady

$$\sum_{n=1}^{\infty} \tfrac{1}{(2n-1)^2}.$$

říkáme, že posloupnost $x_i$, $i = 0, 1, \ldots$, *konverguje* k prvku $x$, kterému říkáme *limita* posloupnosti $x_i$, $i = 0, 1, \ldots$ v metrickém prostoru $X$.

Díky trojúhelníkové nerovnosti dostáváme pro každou dvojici prvků $x_i$, $x_j$ z konvergentní posloupnosti, s dostatečně velikými indexy (značení jako v definici výše),

$$d(x_i, x_j) \le d(x_i, x) + d(x, x_j) < 2\varepsilon,$$

a proto je každá konvergentní posloupnost také cauchyovská. Metrické prostory, kde platí i obrácené tvrzení, tj. že *každá cauchyovská posloupnost je konvergentní*, nazýváme *úplné metrické prostory*.

**7.14. Topologie, konvergence a spojitost.** Stejně jako v případě reálných čísel můžeme zformulovat konvergenci pomocí „otevřených okolí".

### Otevřené a uzavřené množiny

*Otevřené $\varepsilon$–okolí* prvku $x$ v metrickém prostoru $X$ (stručně $\varepsilon$–okolí) je množina

$$\mathcal{O}_\varepsilon(x) = \{y \in X;\ d(x, y) < \varepsilon\}.$$

Podmnožina $U \subset X$ je *otevřená*, jestliže obsahuje s každým svým bodem i nějaké jeho $\varepsilon$–okolí. Podmnožina $W \subset X$ je *uzavřená*, jestliže je její doplněk $X \setminus W$ otevřenou množinou.

Namísto $\varepsilon$–okolí hovoříme také o (otevřené) $\varepsilon$–kouli se středem v $x$. V případě normovaného prostoru si vystačíme s $\varepsilon$–koulemi se středem v nule, jejichž přičtením k danému prvku $x$ dostaneme právě jeho $\varepsilon$–okolí.

*Hromadné body podmnožiny* $A \subset X$ opět definujeme jako takové prvky $x \in X$, ke kterým konverguje nějaká posloupnost bodů z $A$ neobsahující samotný bod $x$. Snadno uvidíme, že množina je uzavřená, právě když obsahuje všechny své hromadné body:

Skutečně, přímo z definice plyne, že množina $A$ je uzavřená, právě když pro každý bod $x \notin A$ existuje nějaké $\varepsilon > 0$ takové, že celé $\varepsilon$–okolí $\mathcal{O}_\varepsilon(x)$ má s $A$ prázdný průnik. Pokud by tedy $A$ byla uzavřená a $x$ byl hromadný bod množiny $A$, který do $A$ nepatří, pak jistě v libovolném takovém $\varepsilon$–okolí takového $x$ leží nekonečně mnoho bodů množiny $A$, což je spor.

Naopak předpokládejme, že $A$ obsahuje všechny své hromadné body a uvažme $x \in X \setminus A$. Pokud by v každém $\varepsilon$–okolí bodu $x$ existoval bod $x_\varepsilon \in A$, pak postupně volbami $\varepsilon = 1/n$ dostaneme posloupnost bodů $x_n \in A$ konvergující k $x$. Pak by ovšem $x$ musel být hromadným bodem, a tedy v $A$, takže opět máme spor.

Pro každou podmnožinu $A$ v metrickém prostoru $X$ definujeme její *vnitřek* jako množinu těch bodů v $A$, které do $A$ patří i s celým svým nějakým okolím. Dále definujeme uzávěr $\bar{A}$ množiny $A$ jako sjednocení původní množiny $A$ s množinou všech jejích hromadných bodů.

Snadno jako u reálných čísel ověříme, že libovolný průnik a libovolné konečné sjednocení uzavřených množin v metrickém prostoru je opět uzavřená množina.

U otevřených množin je to opět naopak: libovolné sjednocení otevřených množin je opět otevřená množina, ale jen konečný průnik otevřených množin je obecně opět otevřená množina. Dokažte si obě tvrzení podrobně sami!

**Řešení.** Ke stanovení součtu této řady lze s úspěchem využít známých Fourierových řad mnoha různých funkcí. Připomeňme např. Fourierovu řadu

$$\tfrac{\pi}{2} - \tfrac{4}{\pi}\sum_{n=1}^{\infty} \tfrac{\cos([2n-1]x)}{(2n-1)^2},$$

kterou jsme vypočítali pro funkci $g(x) = |\,x\,|$, $x \in [-\pi, \pi)$. Protože je tato funkce spojitá na $[-\pi, \pi)$ a $|\,-\pi\,| = |\,\pi\,|$, víme, že dokonce platí

$$|\,x\,| = \tfrac{\pi}{2} - \tfrac{4}{\pi}\sum_{n=1}^{\infty} \tfrac{\cos([2n-1]x)}{(2n-1)^2}, \quad x \in [-\pi, \pi].$$

Dosazení $x = 0$ nám dává

$$0 = \tfrac{\pi}{2} - \tfrac{4}{\pi}\sum_{n=1}^{\infty} \tfrac{1}{(2n-1)^2}, \quad \text{tj.} \quad \sum_{n=1}^{\infty} \tfrac{1}{(2n-1)^2} = \tfrac{\pi^2}{8}.$$

□

**7.16.** Sečtěte řady

$$\sum_{n=1}^{\infty} \tfrac{1}{n^4}, \quad \sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}}{n^4}.$$

**Řešení.** Nejdříve připomeňme, že součty řad

$$\sum_{n=1}^{\infty} \tfrac{1}{n^2} = \tfrac{\pi^2}{6}, \quad \sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}}{n^2} = \tfrac{\pi^2}{12}$$

jsme určili už dříve. V této úloze naznačíme, jakým způsobem lze postupovat při počítaní součtů řad

$$\sum_{n=1}^{\infty} \tfrac{1}{n^{2k}}, \quad \sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}}{n^{2k}}$$

pro obecné $k \in \mathbb{N}$. Využijeme identit

$$x = \pi - 2\sum_{n=1}^{\infty} \frac{\sin(nx)}{n}, \quad x \in (0, 2\pi), \tag{7.11}$$

$$x^2 = \frac{4\pi^2}{3} + 4\sum_{n=1}^{\infty} \frac{\cos(nx)}{n^2} - 4\pi\sum_{n=1}^{\infty} \frac{\sin(nx)}{n}, \quad x \in (0, 2\pi), \tag{7.12}$$

které vyplývají z konstrukcí Fourierových řad postupně pro funkce $g(x) = x$ a $g(x) = x^2$ na intervalu $[0, 2\pi)$.

Podle (‖7.11‖) je

$$\sum_{n=1}^{\infty} \tfrac{\sin(nx)}{n} = \tfrac{\pi - x}{2}, \quad x \in (0, 2\pi).$$

Dosazením do (‖7.12‖) získáme

$$\sum_{n=1}^{\infty} \tfrac{\cos(nx)}{n^2} = \tfrac{3x^2 - 6\pi x + 2\pi^2}{12}, \quad x \in (0, 2\pi).$$

Pouhé dosazení pak dokáže platnost tohoto vztahu také v krajních bodech $x = 0$, $x = 2\pi$. Řada na levé straně má zjevně majorantu $\sum_{n=1}^{\infty} \frac{1}{n^2}$, a proto konverguje absolutně a stejnoměrně na $[0, 2\pi]$. Můžeme ji tak integrovat člen po členu:

Sami si také podrobně ověřte, že vnitřek množiny $A$ je právě sjednocením všech otevřených množin v $A$ obsažených, zatímco uzávěr $A$ je průnikem všech uzavřených množin obsahujících $A$.

Uzavřené a otevřené množiny představují základní pojmy tzv. *topologie*. Aniž bychom zacházeli do hlubších podrobností a souvislostí, seznámili jsme se právě s *topologií metrických prostorů*.

Pojem konvergence můžeme nyní zformulovat tak, že posloupnost prvků $x_i$ v metrickém prostoru $X$, $i = 0, 1, \ldots$, konverguje k $x \in X$, právě když pro každou otevřenou množinu $U$ obsahující $x$ jsou všechny body naší posloupnosti, až na konečně mnoho výjimek, obsaženy v $U$.

Stejně jako u reálných čísel můžeme také definovat *spojitá zobrazení* mezi metrickými prostory:

Zobrazení $f : W \to Z$ je spojité jestliže vzor $f^{-1}(V)$ každé otevřené množiny $V \subset Z$ je otevřená množina ve $W$. Samozřejmě to neznamená nic jiného než tvrzení, že pro všechny prvky $z = f(x) \in Z$, $x \in W$ a kladné číslo $\varepsilon$ existuje kladné číslo $\delta$ tak, že pro všechny prvky $y \in W$ se vzdáleností $d_W(x, y) < \delta$ je také $d_Z(z, f(y)) < \varepsilon$.

Zcela stejně jako u reálných funkcí je zobrazení $f$ mezi metrickými prostory spojité právě tehdy, když respektuje konvergence posloupností.

**7.15. $L_p$–normy.** Nyní máme k dispozici obecné nástroje, se kterými se můžeme podívat na příklady metrických prostorů tvořených konečněrozměrnými vektory nebo funkcemi. Omezíme se na obzvlášť užitečnou třídu norem. Začneme na reálných nebo komplexních konečněrozměrných vektorových prostorech $\mathbb{R}^n$ a $\mathbb{C}^n$ a definujeme pro pevné reálné číslo $p \geq 1$ a libovolný vektor $z = (z_1, \ldots, z_n)$

$$\|z\|_p = \left(\sum_{i=1}^{n} |z_i|^p\right)^{1/p}.$$

Dokážeme, že takto je definována norma. První dvě vlastnosti z definice jsou zřejmé. Zbývá dokázat trojúhelníkovou nerovnost. Vyjdeme přitom z tzv. *Hölderovy nerovnosti*:

**Lemma.** *Pro pevné reálné číslo $p > 1$ a každé dvě $n$–tice nezáporných reálných čísel $x_i$ a $y_i$ platí*

$$\sum_{i=1}^{n} x_i y_i \leq \left(\sum_{i=1}^{n} x_i^p\right)^{1/p} \cdot \left(\sum_{i=1}^{n} y_i^q\right)^{1/q},$$

*kde $1/q = 1 - 1/p$.*



Důkaz. Označme si $X$ a $Y$ výrazy v součinu na pravé straně dokazované nerovnosti. Pokud jsou všechna čísla $x_i$ nebo všechna $y_i$ nulová, pak tvrzení platí. Předpokládejme tedy $X \neq 0$ a $Y \neq 0$.

Hölderova nerovnost je užitečným přímým důsledkem konvexity exponenciální funkce. Definujme čísla $v_k$ a $w_k$ tak, aby platilo

$$x_k = X\,\mathrm{e}^{v_k/p}, \quad y_k = Y\,\mathrm{e}^{w_k/q}.$$

Protože $1/p + 1/q = 1$, můžeme uvažovat afinní kombinaci hodnot $\frac{1}{p}v_k + \frac{1}{q}w_k$ a díky konvexitě exponenciály dostáváme

$$\mathrm{e}^{v_k/p + w_k/q} \leq \tfrac{1}{p}\,\mathrm{e}^{v_k} + \tfrac{1}{q}\,\mathrm{e}^{w_k}.$$

Odtud již přímo dopočítáme

$$\frac{1}{XY}x_k y_k \leq \frac{1}{p}\left(\frac{x_k}{X}\right)^p + \frac{1}{q}\left(\frac{y_k}{Y}\right)^q$$

$$\sum_{n=1}^{\infty}\frac{\sin(nx)}{n^3} = \sum_{n=1}^{\infty}\left[\frac{\sin(ny)}{n^3}\right]_0^x = \int_0^x \sum_{n=1}^{\infty}\frac{\cos(ny)}{n^2}\,dy =$$
$$= \int_0^x \frac{3y^2-6\pi y+2\pi^2}{12}\,dy = \frac{x^3-3\pi x^2+2\pi^2 x}{12},\ x\in[0,2\pi].$$

Upozorněme, že ve skutečnosti lze člen po členu integrovat každou Fourierovu řadu. Analogicky dalším integrováním obdržíme

$$\sum_{n=1}^{\infty}\frac{1-\cos(nx)}{n^4} = \sum_{n=1}^{\infty}\left[-\frac{\cos(ny)}{n^4}\right]_0^x = \int_0^x \sum_{n=1}^{\infty}\frac{\sin(ny)}{n^3}\,dy =$$
$$= \int_0^x \frac{y^3-3\pi y^2+2\pi^2 y}{12}\,dy = \frac{x^4-4\pi x^3+4\pi^2 x^2}{48},\quad x\in[0,2\pi].$$

Dosazení $x=\pi$ vede na

$$\sum_{n=1}^{\infty}\frac{1+(-1)^{n+1}}{n^4} = \sum_{n=1}^{\infty}\frac{1-\cos(n\pi)}{n^4} = \frac{\pi^4}{48}.$$

S přihlédnutím k tomu, že čitatel na levé straně je nulový pro sudá $n$ a je roven 2 pro lichá $n$, lze obdrženou řadu zapsat jako

$$\sum_{n=1}^{\infty}\frac{2}{(2n-1)^4} = \frac{\pi^4}{48}. \tag{7.13}$$

Z vyjádření

$$\sum_{n=1}^{\infty}\frac{1}{n^4} = \sum_{n=1}^{\infty}\frac{1}{(2n)^4} + \sum_{n=1}^{\infty}\frac{1}{(2n-1)^4} = \frac{1}{16}\sum_{n=1}^{\infty}\frac{1}{n^4} + \sum_{n=1}^{\infty}\frac{1}{(2n-1)^4}$$

pak plyne

$$\sum_{n=1}^{\infty}\frac{1}{n^4} = \frac{16}{15}\sum_{n=1}^{\infty}\frac{1}{(2n-1)^4} = \frac{16}{15}\cdot\frac{1}{2}\cdot\frac{\pi^4}{48} = \frac{\pi^4}{90},$$

čímž jsme sečetli první řadu. Součet druhé je

$$\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^4} = \sum_{n=1}^{\infty}\frac{1}{(2n-1)^4} - \sum_{n=1}^{\infty}\frac{1}{(2n)^4} = \sum_{n=1}^{\infty}\frac{1}{(2n-1)^4} - \frac{1}{16}\sum_{n=1}^{\infty}\frac{1}{n^4} =$$
$$= \frac{1}{2}\cdot\frac{\pi^4}{48} - \frac{1}{16}\cdot\frac{\pi^4}{90} = \frac{7\pi^4}{720}.$$

Jak jsme řekli, obdobně lze postupovat při sčítání řad

$$\sum_{n=1}^{\infty}\frac{1}{n^{2k}},\qquad \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^{2k}}$$

pro další $k\in\mathbb{N}$. Je proto přirozené ptát se např. na součet řady $\sum_{n=1}^{\infty}\frac{1}{n^3}$. O nalezení jejího součtu se však matematici marně pokoušejí (bez přehánění) už celá staletí. To může čtenáře oprávněně překvapit, neboť naznačený postup bychom měli být schopni provést i pro všechny liché mocniny.

Můžeme třeba vyjít z identity

$$\sum_{n=1}^{\infty}\frac{\cos(nx)}{n} = -\ln\left(2\sin\tfrac{x}{2}\right),\quad x\in(0,2\pi),$$

kterou lze mimochodem opět dokázat tím, že funkci na pravé straně rozvineme do Fourierovy řady. Kdybychom stejně jako výše dvakrát integrovali člen po členu řadu na levé straně a v limitě dosadili $x\to 0+$, získali bychom právě řadu $\sum_{n=1}^{\infty}\frac{1}{n^3}$. Mělo by tedy stačit dvojí integrování funkce na pravé straně a výpočet jedné limity. Integrování pravé strany ovšem vede na tzv. vyšší funkci, kterou není možné běžným způsobem vyjádřit pomocí funkcí elementárních, s nimiž pracujeme. [1] □

[1] Funkce $\zeta(p)=\sum_{n=1}^{\infty}\frac{1}{n^p}$ se nazývá Riemannova zeta funkce.

a sečtením přes $k=1,\dots,n$

$$\frac{1}{XY}\sum_{i=1}^{n}x_i y_i \le \frac{1}{pX^p}\sum_{i=1}^{n}x_i^p + \frac{1}{qY^p}\sum_{i=1}^{n}y_i^q.$$

Na pravé straně ovšem jednotlivé sumy dávají právě $X^p$ a $Y^q$ a celý výraz je tedy roven $1/p+1/q=1$. Vynásobením této nerovnosti číslem $XY$ dostáváme právě dokazovanou nerovnost. □

Teď už budeme umět dokázat, že $\|\ \|_p$ je skutečně norma:

**Minkowského nerovnost**

Pro každé $p>1$ a všechny $n$–tice nezáporných reálných čísel $(x_1,\dots,x_n)$ a $(y_1,\dots,y_n)$ platí

$$\left(\sum_{i=1}^{n}(x_i+y_i)^p\right)^{1/p} \le \left(\sum_{i=1}^{n}x_i^p\right)^{1/p} + \left(\sum_{i=1}^{n}y_i^p\right)^{1/p}.$$

K ověření této praktické nerovnosti vede následující trik využívající Hölderovu nerovnost. Jistě platí (všimněme si, že $p>1$)

$$\sum_{i=1}^{n}x_i(x_i+y_i)^{p-1} \le \left(\sum_{i=1}^{n}x_i^p\right)^{1/p}\cdot\left(\sum_{i=1}^{n}(x_i+y_i)^{(p-1)q}\right)^{1/q}$$

a stejně tak

$$\sum_{i=1}^{n}y_i(x_i+y_i)^{p-1} \le \left(\sum_{i=1}^{n}y_i^p\right)^{1/p}\cdot\left(\sum_{i=1}^{n}(x_i+y_i)^{(p-1)q}\right)^{1/q}.$$

Nyní sečtením posledních dvou nerovností, s využitím skutečnosti, že $p+q=pq$ a tedy $(p-1)q=pq-q=p$, dostaneme

$$\frac{\sum_{i=1}^{n}(x_i+y_i)^p}{\left(\sum_{i=1}^{n}(x_i+y_i)^p\right)^{1/q}} \le \left(\sum_{i=1}^{n}x_i^p\right)^{1/p} + \left(\sum_{i=1}^{n}y_i^p\right)^{1/p},$$

ale $1-1/q=1/p$, takže jde právě o dokazovanou *Minkowského nerovnost*.

Ověřili jsme si tedy, že na každém konečněrozměrném reálném nebo komplexním vektorovém prostoru máme třídu norem $\|\ \|_p$ pro všechna $p\ge 1$. Kromě toho ještě klademe

$$\|z\|_\infty = \max\{|z_i|,\ i=1,\dots,n\},$$

což je zjevně také norma.

Všimněme si, že Hölderovu nerovnost můžeme v kontextu těchto norem zapsat pro všechna $x=(x_1,\dots,x_n)$, $y=(y_1,\dots,y_n)$ jako

$$\sum_{i=1}^{n}|x_i|\cdot|y_i| \le \|x\|_p\cdot\|y\|_q$$

pro všechna $p\ge 1$ a $q$ splňující $1/p+1/q=1$, přičemž pro $p=1$ klademe $q=\infty$.

**7.16. $L_p$–normy pro posloupnosti a funkce.** Nyní docela snadno zavedeme normy i na vhodných nekonečněrozměrných vektorových prostorech. Začněme posloupnostmi. Vektorový prostor $\ell_p$, $p\ge 1$, je množina všech posloupností reálných nebo komplexních posloupností $x_0, x_1, \dots$ takových, že



$$\sum_{i=0}^{\infty}|x_i|^p < \infty.$$

**7.17.** Pomocí Parsevalovy rovnosti pro Fourierův ortogonální systém ověřte, že

$$\sum_{n=1}^{\infty} \tfrac{1}{(2n-1)^4} = \tfrac{\pi^4}{96}.$$

**Řešení.** Součet uvedené řady jsme již stanovili (viz (‖7.13‖)). Nyní odhalíme, že číselné řady lze pomocí Fourierových řad sčítat ještě snadněji. Tato cesta však podmiňuje znalost nemalého počtu Fourierových řad a může být pro čtenáře o něco náročnější. (Doporučujeme tak každému, aby porovnal řešení tohoto a předchozího příkladu.)

Základem je volba vhodné Fourierovy řady. Vezměme kupř. Fourierovu řadu

$$\tfrac{\pi}{2} - \tfrac{4}{\pi} \sum_{n=1}^{\infty} \tfrac{\cos([2n-1]x)}{(2n-1)^2},$$

kterou jsme obdrželi pro funkci $g(x) = |x|$, $x \in [-\pi, \pi)$ a kterou jsme k určení součtu číselné řady již jednou použili. Parsevalova rovnost

$$\tfrac{a_0^2}{2} + \sum_{n=1}^{\infty} a_n^2 + \sum_{n=1}^{\infty} b_n^2 = \tfrac{2}{T} \int_{x_0}^{x_0+T} [g(x)]^2\, dx$$

pro ni říká

$$\tfrac{\pi^2}{2} + \tfrac{16}{\pi^2} \sum_{n=1}^{\infty} \tfrac{1}{(2n-1)^4} = \tfrac{1}{\pi} \int_{-\pi}^{\pi} |x|^2\, dx = \tfrac{2}{\pi} \int_0^{\pi} x^2\, dx = \tfrac{2\pi^2}{3},$$

tj.

$$\sum_{n=1}^{\infty} \tfrac{1}{(2n-1)^4} = \left(\tfrac{2\pi^2}{3} - \tfrac{\pi^2}{2}\right) \tfrac{\pi^2}{16} = \tfrac{\pi^4}{96}.$$

□

Nyní budeme ilustrovat, jak lze použít Fourierovy řady v teorii diferenciálních rovnic. Diferenciální rovnice budeme podrobněji studovat v další kapitole, viz 3. Pro jednoduchost uvažujme pouze nehomogenní (srovnej s (‖7.2‖)) diferenciální rovnici

$$y'' + a^2 y = f(x) \tag{7.14}$$

s neznámou $y$ v proměnné $x \in \mathbb{R}$, s periodickou spojitě diferencovatelnou funkcí $f : \mathbb{R} \to \mathbb{R}$ na pravé straně a konstantou $a > 0$. Nechť je $T > 0$ primitivní perioda funkce $f$ a nechť je na $[-T/2, T/2]$ známa její Fourierova řada, tj. identita

$$f(x) = \frac{A_0}{2} + \sum_{n=1}^{\infty} \left[ A_n \cos \frac{2\pi n x}{T} + B_n \sin \frac{2\pi n x}{T} \right], \quad x \in \mathbb{R}. \tag{7.15}$$

**7.18.** Dokažte, že má-li rovnice (‖7.14‖) periodické řešení na $\mathbb{R}$, pak perioda tohoto řešení musí být rovněž periodou funkce $f$. Dále dokažte, že rovnice (‖7.14‖) má právě jedno periodické řešení s periodou $T$ právě tehdy, když je

$$a \neq \frac{2\pi n}{T} \quad \text{pro každé } n \in \mathbb{N}. \tag{7.16}$$

Všechny posloupnosti s omezenými absolutními hodnotami členů tvoří prostor $\ell_\infty$. Limitním přechodem pro $n \to \infty$ okamžitě z Minkowského nerovnosti vidíme, že výraz

$$\|x\|_p = \left( \sum_{i=0}^{\infty} |x_i|^p \right)^{1/p}$$

je norma na $\ell_p$. Obdobně klademe na $\ell_\infty$

$$\|x\|_\infty = \sup\{|x_i|, i = 0, 1, \dots\}$$

a opět dostáváme normu.

Konečně, vraťme se k prostorům funkcí $\mathcal{S}^0[a, b]$ na konečném intervalu $[a, b]$ nebo $\mathcal{S}_c^0[a, b]$ na neohraničeném intervalu. S normou $\| \ \|_1$ jsme se již setkali. Zjevně ale pro každé $p > 1$ a pro všechny funkce v takovém prostoru funkcí existují Riemannovy integrály

$$\int_a^b |f(x)|^p dx$$

a můžeme tedy definovat

$$\|f\|_p = \left( \int_a^b |f(x)|^p dx \right)^{1/p}.$$

Riemannův integrál jsme definovali pomocí limitního přechodu vycházejícího z tzv. Riemannových součtů, které odpovídají dělením $\Xi$ s reprezentanty $\xi_i$. V našem případě tedy jde o konečné součty

$$S_{\Xi,\xi} = \sum_{i=1}^{n} |f(\xi_i)|^p (x_i - x_{i-1}).$$

Hölderova nerovnost použitá na Riemannovy součty součinu dvou funkcí $f(x)$ a $g(x)$ dá

$$\sum_{i=1}^{n} |f(\xi_i)||g(\xi_i)|(x_i - x_{i-1}) =$$

$$= \sum_{i=1}^{n} |f(\xi_i)|(x_i - x_{i-1})^{1/p} |g(\xi_i)|(x_i - x_{i-1})^{1/q} \leq$$

$$\leq \left( \sum_{i=1}^{n} |f(\xi_i)|^p (x_i - x_{i-1}) \right)^{1/p} \cdot \left( \sum_{i=1}^{n} |g(\xi_i)|^q (x_i - x_{i-1}) \right)^{1/q},$$

přičemž napravo máme zjevně právě součin Riemannových součtů pro integrály $\|f\|_p$ a $\|g\|_q$.

Limitním přechodem tak ověřujeme tzv. *Hölderovu nerovnost pro integrály*:

$$\int_a^b f(x) g(x)\, dx \leq \left( \int_a^b f(x)^p\, dx \right)^{1/p} \left( \int_a^b g(x)^q\, dx \right)^{1/q}$$

platnou pro všechny nezáporné reálné funkce $f$ a $g$ v našem prostoru po částech spojitých funkcí s kompaktním nosičem

Přesně stejným postupem jako v předchozím odstavci odvodíme z Hölderovy nerovnosti nerovnost Minkowského v její integrální formě:

$$\|f + g\|_p \leq \|f\|_p + \|g\|_p.$$

Je tedy $\| \ \|_p$ je skutečně norma na vektorovém prostoru všech spojitých funkcí s kompaktními nosiči pro všechna $p > 1$ (a pro $p = 1$ jsme tuto skutečnost ověřili už dávno). Pro celý prostor $\mathcal{S}^0[a, b]$ po částech spojitých funkcí budeme sice také slovo norma v tomto kontextu používat, měli bychom ale přitom vědět, že musíme ztotožňovat funkce, které se od sebe liší jen hodnotami v bodech nespojitosti.

**Řešení.** Nechť je funkce $y = g(x)$, $x \in \mathbb{R}$ řešením rovnice (‖7.14‖) a má periodu $p > 0$. Aby bylo vůbec možné dosadit funkci $g$ do diferenciální rovnice druhého řádu, musí existovat její druhá derivace $g''$. Protože funkce $g, g', g'', \ldots$ mají stejnou periodu, také funkce

$$g''(x) + a^2 g(x) = f(x)$$

je periodická s periodou $p$. Jinak řečeno, funkce $f$ je periodická jako lineární kombinace funkcí s periodou $p$. Tím jsme dokázali první tvrzení říkající, že $p = lT$ pro jisté $l \in \mathbb{N}$.

Nyní předpokládejme, že funkce $y = g(x), x \in \mathbb{R}$ je periodickým řešením rovnice (‖7.14‖) s periodou $T$ a s vyjádřením Fourierovou řadou

$$g(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} \left[a_n \cos(\omega n x) + b_n \sin(\omega n x)\right], \quad x \in \mathbb{R}, \tag{7.17}$$

kde $\omega = 2\pi/T$. Vyhovuje-li $g$ rovnici (‖7.14‖), musí mít tato funkce spojitou druhou derivaci na $\mathbb{R}$. Platí tedy

$$g'(x) = \sum_{n=1}^{\infty} \left[\omega n b_n \cos(\omega n x) - \omega n a_n \sin(\omega n x)\right], \quad x \in \mathbb{R},$$

(7.18)

$$g''(x) = \sum_{n=1}^{\infty} \left[-\omega^2 n^2 a_n \cos(\omega n x) - \omega^2 n^2 b_n \sin(\omega n x)\right], \quad x \in \mathbb{R}.$$

Dosazení (‖7.15‖), (‖7.17‖) a (‖7.18‖) do (‖7.14‖) dává

$$\begin{aligned} a^2 \tfrac{a_0}{2} + \sum_{n=1}^{\infty} \big[ &\left(-\omega^2 n^2 a_n + a^2 a_n\right) \cos(n\omega x) + \\ &+ \left(-\omega^2 n^2 b_n + a^2 b_n\right) \sin(n\omega x)\big] = \\ = \tfrac{A_0}{2} + \sum_{n=1}^{\infty} &\left[A_n \cos(n\omega x) + B_n \sin(n\omega x)\right]. \end{aligned}$$

Odsud vyplývá, že

$$a^2 \frac{a_0}{2} = \frac{A_0}{2}, \quad \text{tj.} \quad a_0 = \frac{A_0}{a^2}, \tag{7.19}$$

a

$$\left(-\omega^2 n^2 + a^2\right) a_n = A_n, \quad \left(-\omega^2 n^2 + a^2\right) b_n = B_n, \quad n \in \mathbb{N}. \tag{7.20}$$

Je vidět, že těmto podmínkám vyhovuje právě jedna dvojice posloupností $\{a_n\}_{n\in\mathbb{N}\cup\{0\}}$, $\{b_n\}_{n\in\mathbb{N}}$ tehdy a jenom tehdy, když je

$$-\omega^2 n^2 + a^2 = -\left(\tfrac{2\pi n}{T}\right)^2 + a^2 \neq 0 \quad \text{pro každé } n \in \mathbb{N},$$

tj. když platí (‖7.16‖). V tomto případě je jediné řešení (‖7.14‖) s periodou $T$ určeno jediným řešením

$$a_n = \frac{A_n}{-\omega^2 n^2 + a^2}, \quad b_n = \frac{B_n}{-\omega^2 n^2 + a^2}, \quad n \in \mathbb{N} \tag{7.21}$$

soustavy rovnic (‖7.20‖). Podotkněme, že jsme mlčky využili stejnoměrnou konvergenci řady v (‖7.18‖). Ta mj. vyplývá z hlubších výsledků obecné teorie Fourierových řad, kterým se však nebudeme podrobněji věnovat. □

Mezi těmito normami je výjimečný případ $p = 2$, který jsme již dříve realizovali pomocí skalárního součinu. V tomto případě jsme mohli odvodit trojúhelníkovou nerovnost daleko jednodušeji pomocí Schwarzovy nerovnosti.

Pro funkce z $\mathcal{S}^0[a, b]$ můžeme definovat i obdobu $L_\infty$–normy na $n$–rozměrných vektorech. Protože jsou naše funkce po částech spojité, budou pro ně na konečném uzavřeném intervalu vždy existovat suprema absolutních hodnot a klademe tedy pro takovou funkci $f$

$$\|f\|_\infty = \sup\{f(x),\ x \in [a, b]\}.$$

Všimněme si, že kdybychom za hodnoty $f(x)$ v bodech nespojitosti považovali jak jednostranné limity (které podle naší definice vždy existují), tak samotnou hodnotu funkce, pak můžeme pracovat s maximy místo suprem. Opět je zřejmé, že jde o normu (až na problémy s hodnotami v bodech nespojitosti).

**7.17. Zúplnění metrických prostorů.** Samotná reálná čísla $\mathbb{R}$ nebo komplexní čísla $\mathbb{C}$ jsou (s metrikou danou absolutní hodnotou) úplným metrickým prostorem. To je vlastně obsahem axiomu o existenci suprema a připomeňme, že jsme reálná čísla vytvořili jako „zúplnění“ prostoru racionálních čísel, který sám úplný naopak není. Je přitom zjevné, že uzávěrem množiny $\mathbb{Q} \subset \mathbb{R}$ je už celé $\mathbb{R}$.



Husté a řídké podmnožiny

Říkáme, že podmnožina $A \subset X$ v metrickém prostoru $X$ je *hustá*, jestliže je uzávěrem $A$ celý prostor $X$. Množina $A$ je *řídká* v $X$, jestliže je $X \setminus \bar{A}$ hustá.

Zjevně je $A$ hustá v $X$, jestliže každá otevřená množina v celém prostoru $X$ má s $A$ neprázdný průnik.

Ve všech případech norem na funkcích z předchozího odstavce je vcelku snadné vidět, že takto definované metrické prostory nebudou patrně úplné. Snadno se totiž stane, že cauchyovská posloupnost funkcí z našeho vektorového prostoru $\mathcal{S}^0[a, b]$ by měla mít za limitu funkci, která již v tomto prostoru nebude. Vezměme si třebas na intervalu $[0, 1]$ funkce $f_n$, které jsou nulové na $[0, 1/n)$ a rovny $\sin(1/x)$ na $[1/n, 1]$. Zjevně budou konvergovat ve všech $L_p$ normách k funkci $\sin(1/x)$, ta ale do našich prostorů již nepatří.

Zúplnění metrického prostoru

Nechť $X$ je metrický prostor s metrikou $d$, který není úplný. Metrický prostor $\tilde{X}$ s metrikou $\tilde{d}$ takový, že $X \subset \tilde{X}$, $d$ je zúžením $\tilde{d}$ na podmnožinu $X$ a uzávěrem $\tilde{X}$ je celý prostor $\tilde{X}$, se nazývá *zúplnění metrického prostoru* $X$.

Následující věta říká, že prakticky stejným postupem, jak jsme vytvořili reálná čísla z racionálních, můžeme nyní najít zúplnění libovolného (neúplného) metrického prostoru $X$. Ještě než se do docela složitého důkazu tohoto mimořádně důležitého a užitečného výsledku pustíme, všimněme si, že takové „zúplnění“ $\tilde{X}$ prostoru $X$ může být dané v rozumném smyslu jediným způsobem:

O zobrazení $\varphi : X_1 \to X_2$ mezi metrickými prostory s metrikami $d_1$ a $d_2$ řekneme, že je *izometrie*, jestliže pro všechny prvky $x, y \in X$ platí $d_2(\varphi(x), \varphi(y)) = d_1(x, y)$.

Každá izometrie je samozřejmě bijekcí na svůj obraz (plyne z vlastnosti, že vzdálenost libovolných různých prvků je nenulová) a příslušné inverzní zobrazení je také izometrie.

**7.19.** Pomocí řešení předchozí úlohy nalezněte všechna $2\pi$-periodická řešení diferenciální rovnice

$$y'' + 2y = \sum_{n=1}^{\infty} \frac{\sin(nx)}{n^2}, \quad x \in \mathbb{R}.$$

**Řešení.** Rovnice je ve tvaru (‖7.14‖) pro $a = \sqrt{2}$ a spojitě diferencovatelnou funkci

$$f(x) = \sum_{n=1}^{\infty} \frac{\sin(nx)}{n^2}, \quad x \in \mathbb{R}$$

s primitivní periodou $T = 2\pi$. Podle úlohy ‖7.18‖ podmínka $\sqrt{2} \notin \mathbb{N}$ implikuje, že $2\pi$-periodické řešení existuje právě jedno. Budeme-li jej hledat jako součet řady

$$\frac{a_0}{2} + \sum_{n=1}^{\infty} [a_n \cos(nx) + b_n \sin(nx)], \quad x \in \mathbb{R},$$

protože platí (‖7.19‖) je

$$a_0 = a_n = 0, \quad b_n = \frac{1}{n^2(2-n^2)}, \quad n \in \mathbb{N}.$$

Zadaná rovnice má tedy jediné $2\pi$-periodické řešení

$$y = \sum_{n=1}^{\infty} \frac{\sin(nx)}{n^2(2-n^2)}, \quad x \in \mathbb{R}.$$

□

## C. Metrické prostory

**7.20.** Ukažte, že definice metriky jakožto reálné funkce $d$ definované na $X \times X$, pro neprázdnou množinu $X$ splňující

$$d(x, y) = 0, \text{ právě když } x = y, \quad x, y \in X, \tag{7.22}$$

$$d(x, z) \leq d(y, x) + d(y, z), \quad x, y, z \in X, \tag{7.23}$$

je ekvivalentní definici metriky, která je uvedena v teoretické části, v odstavci 7.12.

**Řešení.** Zdánlivě se v této definici klade na metriku méně požadavků než v definici z teoretické části. Definice jsou potom ekvivalentní právě tehdy, když podmínky (‖7.22‖), (‖7.23‖) implikují

$$d(y, x) \geq 0, \quad x, y \in X, \tag{7.24}$$

$$d(x, y) = d(y, x), \quad x, y \in X. \tag{7.25}$$

Položíme-li však $x = z$ v (‖7.23‖), z (‖7.22‖) dostaneme (‖7.24‖). Podobně z volby $y = z$ v (‖7.23‖) s použitím (‖7.22‖) plyne $d(x, y) \leq d(y, x)$ pro všechny body $x, y \in X$. Záměnou proměnných $x$ a $y$ dále obdržíme $d(y, x) \leq d(x, y)$, tj. (‖7.25‖). Dokázali jsme, že definice jsou ekvivalentní.

V literatuře lze nalézt i další ekvivalentní způsoby pro zavedení metrik. Stejně tak lze dohledat mnoho mírně odlišných definic, které ovšem vedou na jiné objekty než metriky (nejdůležitější mezi nimi jsou pseudometriky, ultrametriky a semimetriky). První axiomatickou

Uvažme nyní dvě vložení hustých podmnožin $\iota_1 : X \to \tilde{X}_1$ a $\iota_2 : X \to \tilde{X}_2$ do dvou zúplnění prostoru $X$. Evidentně je na husté podmnožině $\iota_1(X) \subset \tilde{X}_1$ dobře definované zobrazení

$$\varphi : \iota_1(X) \xrightarrow{\iota_1^{-1}} X \xrightarrow{\iota_2} \tilde{X}_2 .$$

Jeho obrazem je hustá podmnožina $\iota_2(X) \subset \tilde{X}_2$ a toto zobrazení je navíc zjevně izometrií. Stejně tak funguje i opačné zobrazení $\iota_1 \circ \iota_2^{-1}$.

Každé izometrické zobrazení samozřejmě zobrazuje cauchyovské posloupnosti na cauchyovské posloupnosti. Zároveň budou takové cauchyovské posloupnosti konvergovat ke stejnému prvku v zúplnění právě, když totéž bude platit o jejich obrazech v izometrii $\varphi$. Je-li tedy takové $\varphi$ definované na husté podmnožině $X$ metrického prostoru $\tilde{X}_1$, jistě bude mít jednoznačné rozšíření na celé $\tilde{X}_1$ s hodnotami v uzávěru obrazu $\varphi(X)$, tj. $\tilde{X}_2$.

Podle předchozí úvahy tedy existuje jediné rozšíření $\varphi$ na zobrazení $\tilde{\varphi} : \tilde{X}_1 \to \tilde{X}_2$, které je bijektivní izometrií. Jsou tedy skutečně $\tilde{X}_1$ a $\tilde{X}_2$ stejné v tomto smyslu.

**7.18. Věta.** *Nechť $X$ je metrický prostor s metrikou $d$, který není úplný. Pak existuje jeho zúplnění $\tilde{X}$ s metrikou $\tilde{d}$, které je jednoznačné až na bijektivní izometrie.*



Důkaz. Myšlenka konstrukce je zcela identická jako u konstrukce reálných čísel. Dvě cauchyovské posloupnosti $x_i$ a $y_i$ bodů v $X$ považujeme za ekvivalentní, jestliže $d(x_i, y_i)$ konverguje k nule pro $i$ jdoucí do nekonečna. Tady jde o konvergenci reálných čísel, tedy korektní definici.

Je vcelku zřejmé z vlastností konvergence na reálných číslech, že jde skutečně o relaci ekvivalence (ověřte si podrobně – např. tranzitivita plyne z toho, že součet dvou posloupností konvergujících k nule také konverguje k nule).

Definujeme nyní $\tilde{X}$ jako množinu tříd ekvivalence cauchyovských posloupností. Původní body $x \in X$ můžeme ztotožnit s třídou posloupností ekvivalentních s konstantní posloupností $x_i = x, i = 0, 1, \ldots$.

Nyní je nasnadě, jak zadefinovat metriku $\tilde{d}$. Nabízí se uvažovat pro posloupnosti $\tilde{x} = \{x_0, x_1, \ldots\}$ a $\tilde{y} = \{y_0, y_1, \ldots\}$

$$\tilde{d}(\tilde{x}, \tilde{y}) = \lim_{i \to \infty} d(x_i, y_i).$$

Předně je třeba ověřit, že tato limita skutečně existuje a je konečná. Přímo z trojúhelníkové nerovnosti pro absolutní hodnotu na reálných číslech a skutečnosti, že obě posloupnosti $\tilde{x}$ a $\tilde{y}$ jsou cauchyovské, plyne, že jde o cauchyovskou posloupnost reálných čísel $d(x_i, y_i)$ a tedy její limita skutečně existuje.

Pokud vybereme jiné reprezentanty $\tilde{x} = \{x'_0, x'_1, \ldots\}$ a $\tilde{y} = \{y'_0, y'_1, \ldots\}$, pak z trojúhelníkové nerovnosti pro vzdálenost reálných čísel (je třeba uvážit důsledky pro rozdíly vzdáleností) vidíme, že

$$\begin{aligned} |d(x'_i, y'_i) - d(x_i, y_i)| &\leq |d(x'_i, y'_i) - d(x'_i, y_i)| + \\ &\quad + |d(x'_i, y_i) - d(x_i, y_i)| \leq \\ &\leq d(x_i, x'_i) + d(y_i, y'_i). \end{aligned}$$

Skutečně tedy na výběru reprezentantů v definici nezáleží.

definici „tradiční“ metriky pak vyslovil Maurice Fréchet v roce 1906. Název metrika pochází ale od Felixe Hausdorffa, který tento pojem poprvé použil ve své práci z roku 1914. □

**7.21.** Uvažujte množinu všech podmnožin libovolné konečné množiny a rozhodněte, zda je zobrazení pro všechny uvažované podmnožiny $X, Y$ definované vztahem

(a) $d_1(X,Y) := |\,(X \cup Y) \setminus (X \cap Y)\,|$;

(b) $d_2(X,Y) := \frac{|\,(X\cup Y)\setminus(X\cap Y)\,|}{|\,X\cup Y\,|}$, $X \cup Y \neq \emptyset$, $\quad d_2(\emptyset,\emptyset) := 0$

metrikou. (Symbolem $|\,X\,|$ se rozumí počet prvků množiny $X$.)

**Řešení.** V konkrétních úlohách o rozhodnutí, zda je nějaké zobrazení metrikou, budeme ověřování prvních dvou podmínek z definice metriky vynechávat. Čtenář by si měl sám hned uvědomit, že jsou splněny pro $d_1$ i $d_2$. Omezíme se tedy pouze na rozbor trojúhelníkové nerovnosti.

Případ (a). Pro libovolné množiny $X, Y, Z$ platí

(7.26)

$$(X \cup Z) \setminus (X \cap Z) \subseteq [(X \cup Y) \setminus (X \cap Y)] \cup [(Y \cup Z) \setminus (Y \cap Z)]\,.$$

Pokud totiž $x \in (X\cup Z)\setminus(X\cap Z)$, pak nastává právě jedna z možností

$$x \in X \text{ a současně } x \notin Z, \quad x \notin X \text{ a současně } x \in Z.$$

Má tak smysl zvažovat tyto 4 možnosti

$$x \in X,\ x \notin Z,\ x \in Y, \quad x \in X,\ x \notin Z,\ x \notin Y,$$

$$x \notin X,\ x \in Z,\ x \in Y, \quad x \notin X,\ x \in Z,\ x \notin Y,$$

které mohou nastat pro $x \in (X \cup Z) \setminus (X \cap Z)$. Ve všech těchto 4 případech je však $x$ prvkem právě jedné z množin $(X \cup Y) \setminus (X \cap Y)$, $(Y \cup Z) \setminus (Y \cap Z)$. Tím jsme obdrželi inkluzi (‖7.26‖), z níž ihned plyne požadovaná trojúhelníková nerovnost

$$\begin{aligned} d_1(X,Z) &= |\,(X \cup Z) \setminus (X \cap Z)\,| \leq \\ &\leq |\,[(X \cup Y) \setminus (X \cap Y)] \cup [(Y \cup Z) \setminus (Y \cap Z)]\,| \leq \\ &\leq |\,(X \cup Y) \setminus (X \cap Y)\,| + |\,(Y \cup Z) \setminus (Y \cap Z)\,| = \\ &= d_1(X,Y) + d_1(Y,Z). \end{aligned}$$

Případ (b). Lze postupovat podobně jako pro $d_1$. Symbolem $X'$ budeme označovat doplněk (komplement) množiny $X$. Z rovností

$$(X \cup Y) \setminus (X \cap Y) =$$
$$= (X \cap Y' \cap Z) \cup (X \cap Y' \cap Z') \cup (X' \cap Y \cap Z) \cup (X' \cap Y \cap Z'),$$
$$(Y \cup Z) \setminus (Y \cap Z) =$$
$$= (X \cap Y \cap Z') \cup (X \cap Y' \cap Z) \cup (X' \cap Y \cap Z') \cup (X' \cap Y' \cap Z),$$
$$[(X \cup Z) \setminus (X \cap Z)] \cup [Y \setminus (X \cup Z)] =$$
$$= (X \cap Y \cap Z') \cup (X \cap Y' \cap Z') \cup (X' \cap Y \cap Z) \cup (X' \cap Y' \cap Z) \cup$$
$$\cup (X' \cap Y \cap Z'),$$

Dále ověříme, že $\tilde{d}$ je metrikou na $\tilde{X}$. První dvě vlastnosti jsou zřejmé. Pro odvození trojúhelníková nerovnosti zvolme tři cauchyovské reprezentanty prvků $\tilde{x}, \tilde{y}, \tilde{z}$ a opět dostaneme snadno:

$$\begin{aligned} \tilde{d}(\tilde{x},\tilde{z}) &= \lim_{i\to\infty} d(x_i, z_i) \leq \\ &\leq \lim_{i\to\infty} d(x_i, y_i) + \lim_{i\to\infty} d(y_i, z_i) = \\ &= \tilde{d}(\tilde{x},\tilde{y}) + \tilde{d}(\tilde{y},\tilde{z}\,). \end{aligned}$$

Zjevně je také zúžení právě zadefinované metriky $\tilde{d}$ na původní prostor $X$ shodný s původní metrikou, protože původní body jsou reprezentovány konstantními posloupnostmi.

Zbývá nám ještě dokázat hustota $X$ v $\tilde{X}$ a úplnost nově zkonstruovaného metrického prostoru. Chceme tedy dokázat, že pro pevně vybranou cauchyovskou posloupnost $\tilde{x} = \{x_i\}$ vždy ke každému sebemenšímu $\varepsilon > 0$ najdeme v původním prostoru nějaké $y$ takové, že vzdálenost konstantní posloupnosti prvků $y$ od zvolené posloupnosti $x_i$ nebude větší než $\varepsilon$. Protože je však posloupnost $x_i$ cauchyovská, budou všechny dvojice $x_n$, $x_m$ jejích členů sobě blíže než o $\varepsilon$ pro dostatečně veliké indexy $m$ a $n$. Pak ale nutně také výběrem $y = x_n$ pro jeden takový index budou již sobě prvky $y$ a $x_m$ blíže než o $\varepsilon$ a tedy i v limitě bude platit, že $\tilde{d}(\tilde{y},\tilde{x}) \leq \varepsilon$.

Závěrem je tedy ještě třeba ukázat, že cauchyovské posloupnosti bodů rozšířeného prostoru $\tilde{X}$ vzhledem k metrice $\tilde{d}$ jsou už nutně konvergentní. Jinak řečeno, chceme ukázat, že opakováním předchozí konstrukce již nedostaneme nové body. To uděláme tak, že budeme umět postupně body cauchyovské posloupnosti $\tilde{x}_k$ přiblížit body $y_k$ z původního prostoru $X$ tak, aby výsledná posloupnost $\tilde{y} = \{y_i\}$ byla limitou původní posloupnosti vzhledem k metrice $\tilde{d}$.

Protože již víme, že je $X$ v $\tilde{X}$ hustou podmnožinou, můžeme pro každý prvek $\tilde{x}_k$ z naší dané posloupnosti vybrat prvek $z_k \in X$ tak, aby pro konstantní posloupnost $\tilde{z}_k$ platilo $\tilde{d}(\tilde{x}_k,\tilde{z}_k) < 1/k$. Uvažme nyní posloupnost $\tilde{z} = \{z_0, z_1, \dots\}$. Původní posloupnost $\tilde{x}$ je cauchyovská, tj. pro pevně zvolené číslo $\varepsilon > 0$ najdeme index $n(\varepsilon)$ takový, že $\tilde{d}(\tilde{x}_n,\tilde{x}_m) < \varepsilon/2$, kdykoliv budou $m$ i $n$ větší než $n(\varepsilon)$. Bez obav můžeme přitom předpokládat, že námi zvolený index $n(\varepsilon)$ je větší nebo roven číslu $4/\varepsilon$. Nyní dostáváme pro $m$ i $n$ větší než $n(\varepsilon)$:

$$\begin{aligned} d(z_m, z_n) &= \tilde{d}(\tilde{z}_m,\tilde{z}_n) \leq \\ &\leq \tilde{d}(\tilde{z}_m,\tilde{x}_m) + \tilde{d}(\tilde{x}_m,\tilde{x}_n) + \tilde{d}(\tilde{x}_n,\tilde{z}_n) \leq \\ &\leq 1/m + \varepsilon/2 + 1/n \leq 2\frac{\varepsilon}{4} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Jde tedy o cauchyovskou posloupnost $z_i$ prvků v $X$ a tedy $\tilde{z} \in \tilde{X}$. Zkoumejme, zda vzdálenost $\tilde{d}(\tilde{x}_n,\tilde{z})$ skutečně jde k nule, jak jsme se snažili konstrukcí zajistit. Z trojúhelníkové nerovnosti

$$\tilde{d}(\tilde{z},\tilde{x}_n) \leq \tilde{d}(\tilde{z},\tilde{z}_n) + \tilde{d}(\tilde{z}_n,\tilde{x}_n).$$

Podle našich předchozích odhadů ale jdou oba sčítanci napravo k nule a tím je důkaz ukončen. □

V dalších třech odstavcích si uvedeme tři docela jednoduché věty o úplných metrických prostorech, které mají spoustu důležitých aplikací jak v samotné matematické analýze, tak v ověřování konvergence numerických metod.

které lze opět snadno dokázat výčtem možností, plyne zesílení (‖7.26‖) ve tvaru

$$[(X \cup Z) \setminus (X \cap Z)] \cup [Y \setminus (X \cup Z)] \subseteq$$
$$\subseteq [(X \cup Y) \setminus (X \cap Y)] \cup [(Y \cup Z) \setminus (Y \cap Z)] .$$

Dále využijeme nerovnost

$$\frac{|\,(X\cup Z)\setminus(X\cap Z)\,|}{|\,X\cup Z\,|} \le \frac{|\,[(X\cup Z)\setminus(X\cap Z)]\cup[Y\setminus(X\cup Z)]\,|}{|\,X\cup Z\cup[Y\setminus(X\cup Z)]\,|}, \quad X \cup Z \neq \emptyset.$$

Ta je založena pouze na počítání s nezápornými čísly, neboť obecně platí

$$\frac{x}{z} \le \frac{x+y}{z+y}, \quad y \ge 0,\ z > 0,\ x \in [0, z].$$

Ze zřejmého vztahu

$$X \cup Z \cup [Y \setminus (X \cup Z)] = X \cup Y \cup Z$$

tak již dostáváme

$$d_2(X, Z) = \frac{|\,(X\cup Z)\setminus(X\cap Z)\,|}{|\,X\cup Z\,|} \le \frac{|\,[(X\cup Z)\setminus(X\cap Z)]\cup[Y\setminus(X\cup Z)]\,|}{|\,X\cup Z\cup[Y\setminus(X\cup Z)]\,|} \le$$
$$\le \frac{|\,[(X\cup Y)\setminus(X\cap Y)]\cup[(Y\cup Z)\setminus(Y\cap Z)]\,|}{|\,X\cup Y\cup Z\,|} \le \frac{|\,(X\cup Y)\setminus(X\cap Y)\,|+|\,(Y\cup Z)\setminus(Y\cap Z)\,|}{|\,X\cup Y\cup Z\,|} \le$$
$$\le \frac{|\,(X\cup Y)\setminus(X\cap Y)\,|}{|\,X\cup Y\,|} + \frac{|\,(Y\cup Z)\setminus(Y\cap Z)\,|}{|\,Y\cup Z\,|} = d_2(X, Y) + d_2(Y, Z),$$

pokud $X \cup Z \neq \emptyset$ a $Y \neq \emptyset$. Pro $X = Z = \emptyset$ nebo $Y = \emptyset$ je však očividně trojúhelníková nerovnost splněna také.

V obou případech se tudíž jedná o metriky. Metrika $d_1$ má spíše pomocný charakter a nelze říci, že by měla tak široké uplatnění jako $d_2$, kterou lze dohledat v literatuře pod názvem Jaccardova metrika. Pojmenována byla podle biologa Paula Jaccarda, který v roce 1908 pomocí funkce $1 - d_2$ účinně vystihl míru podobnosti mezi hmyzími populacemi. □

**7.22.** Nechť je

$$d(x, y) := \frac{|\,x-y\,|}{1+|\,x-y\,|}, \quad x, y \in \mathbb{R}.$$

Dokažte, že $d$ je metrika na $\mathbb{R}$.

**Řešení.** Opět dokážeme jenom trojúhelníkovou nerovnost (ostatní je zřejmé). Zaveďme pomocnou rostoucí funkci

$$f(t) := \frac{t}{1+t}, \quad t \ge 0. \tag{7.27}$$

Skutečnost, že $f$ je rostoucí, ani není třeba ověřovat výpočtem první derivace. Stačí úvaha nebo jednoduchá úprava

$$f(s) - f(r) = \frac{s}{1+s} - \frac{r}{1+r} = \frac{s-r}{(1+s)(1+r)} > 0, \quad s > r \ge 0.$$

Platí proto

$$d(x, z) = \frac{|\,x-z\,|}{1+|\,x-z\,|} = \frac{|\,x-y+y-z\,|}{1+|\,x-y+y-z\,|} \le \frac{|\,x-y\,|+|\,y-z\,|}{1+|\,x-y\,|+|\,y-z\,|} =$$
$$= \frac{|\,x-y\,|}{1+|\,x-y\,|+|\,y-z\,|} + \frac{|\,y-z\,|}{1+|\,x-y\,|+|\,y-z\,|} \le \frac{|\,x-y\,|}{1+|\,x-y\,|} + \frac{|\,y-z\,|}{1+|\,y-z\,|} =$$
$$= d(x, y) + d(y, z), \quad x, y, z \in \mathbb{R} . \qquad \square$$

**7.19. Banachova věta o kontrakci.** Zobrazení $F : X \to X$ na



metrickém prostoru $X$ s metrikou $d$ se nazývá *kontrahující zobrazení*, jestliže pro nějakou reálnou konstantu $0 \le C < 1$ a všechny prvky $x$, $y$ v $X$ platí

$$d(F(x), F(y)) \le C\, d(x, y).$$

**Věta.** *Je-li $F$ kontrahující zobrazení na úplném metrickém prostoru $X$, pak existuje právě jeden jeho pevný bod $z \in X$, tj. $F(z) = z$.*

Důkaz. Důkaz docela přímočaře sleduje intuitivní představy, že když je zobrazení kontrahující, mělo by se jeho iterované působení na nějaké počáteční hodnotě $z_0 \in X$ „hromadit“ k nějakému bodu. K tomu pochopitelně potřebujeme úplnost, jinak by limitní bod už nemusel v $X$ existovat.

Zvolme tedy libovolné $z_0 \in X$ a uvažme posloupnost $z_i$, $i = 0, 1, \ldots$

$$z_1 = F(z_0),\ z_2 = F(z_1), \ldots, z_{i+1} = F(z_i), \ldots$$

Podle předpokladů platí

$$d(z_{i+1}, z_i) = d(F(z_i), F(z_{i-1})) \le$$
$$\le C\, d(z_i, z_{i-1}) \le \cdots \le C^i\, d(z_1, z_0).$$

Z trojúhelníkové nerovnosti pak pro všechna přirozená čísla $j$ dostáváme

$$d(z_{i+j}, z_i) \le \sum_{k=1}^{j} d(z_{i+k}, z_{i+k-1}) \le$$
$$\le \sum_{k=1}^{j} C^{i+k-1}\, d(z_1, z_0) = C^i\, d(z_1, z_0) \sum_{k=1}^{j} C^{k-1} \le$$
$$\le C^i\, d(z_1, z_0) \sum_{k=1}^{\infty} C^{k-1} = \frac{C^i}{1-C}\, d(z_1, z_0).$$

Nyní pro každé kladné sebemenší $\varepsilon$ jistě bude výraz na pravé straně menší než $\varepsilon$ pro dostatečně velké indexy $i$, tj.

$$d(z_i, z_{i+j}) \le \frac{C^i}{1-C}\, d(z_1, z_0) \le \varepsilon.$$

To ale přesně říká, že je naše posloupnost $z_i$ cauchyovská. Díky úplnosti prostoru $X$ bude tedy existovat její limita $z$ a k dokončení důkazu je již jen třeba ověřit, že $F(z) = z$.

Každé kontrahující zobrazení je ale zcela evidentně spojité. Je tedy

$$F(z) = F(\lim_{n\to\infty} z_n) = \lim_{n\to\infty} F(z_n) = z\ .$$

Zbývá dokázat jednoznačnost. Je-li $F(y) = y$ a $F(z) = z$, pak je

$$d(y, z) = d(F(y), F(z)) \le C\, d(y, z).$$

Tím je tvrzení dokázáno. □

**7.20. Cantorova věta o průniku.** Pro libovolnou množinu $A$ v metrickém prostoru $X$ s metrikou $d$ nazýváme reálné číslo

$$\operatorname{diam} A = \sup_{x,y\in A} d(x, y)$$

*průměrem množiny $A$*. O množině $A$ říkáme, že je *omezená*, jestliže $\operatorname{diam} A < \infty$.

**7.23.** Určete vzdálenost funkcí

$$f(x) = x, \quad g(x) = -\tfrac{x}{\sqrt{1+x^2}}, \quad x \in [1,2]$$

jako prvků normovaného vektorového prostoru $\mathcal{S}[1,2]$ po částech spojitých funkcí na intervalu $[1,2]$ s normou

(a) $\| f \|_1 = \int_1^2 | f(x) | \, dx$;

(b) $\| f \|_\infty = \max \{ | f(x) |; \ x \in [1,2] \}$.

**Řešení.** Případ (a). Stačí vypočítat

$$\int_1^2 | f(x) - g(x) | \ dx = \int_1^2 x + \tfrac{x}{\sqrt{1+x^2}} \, dx = \left[ \tfrac{x^2}{2} + \sqrt{1+x^2} \right]_1^2 = \\ = \tfrac{3}{2} + \sqrt{5} - \sqrt{2}.$$

Případ (b). Nyní chceme určit

$$\max_{x \in [1,2]} | f(x) - g(x) | = \max_{x \in [1,2]} \left( x + \tfrac{x}{\sqrt{1+x^2}} \right).$$

Při hledání extrémů funkcí je velmi silným a účinným nástrojem jejich derivování. Ihned z nerovnosti

$$\left( x + \tfrac{x}{\sqrt{1+x^2}} \right)' = 1 + \tfrac{1}{\left( \sqrt{1+x^2} \right)^3} > 0, \quad x \in [1,2]$$

vidíme, že

$$\max_{x \in [1,2]} \left( x + \tfrac{x}{\sqrt{1+x^2}} \right) = 2 + \tfrac{2}{\sqrt{1+2^2}} = 2 + \tfrac{2}{\sqrt{5}}.$$

Rostoucí funkce na uzavřeném intervalu totiž nabývá své maximální hodnoty v jeho pravém krajním bodě. □

**7.24.** Zjistěte, jestli je posloupnost $\{x_n\}_{n \in \mathbb{N}}$, kde

$$x_1 = 1, \quad x_n = 1 + \tfrac{1}{2} + \cdots + \tfrac{1}{n}, \ n \in \mathbb{N} \setminus \{1\},$$

cauchyovská v $\mathbb{R}$. Uvažujte nejprve běžnou metriku danou rozdílem v absolutní hodnotě (tj. indukovanou normou, kterou je absolutní hodnota) a poté metriku

$$d(x,y) := \tfrac{| x-y |}{1+| x-y |}, \quad x, y \in \mathbb{R}.$$

**Řešení.** Připomeňme, že

$$\sum_{k=1}^{\infty} \frac{1}{k} = \infty, \quad \text{tj.} \quad \sum_{k=m}^{\infty} \frac{1}{k} = \infty, \ m \in \mathbb{N}. \tag{7.28}$$

Platí tak

$$\lim_{n \to \infty} | x_n - x_m | = \sum_{k=m+1}^{\infty} \tfrac{1}{k} = \infty, \quad m \in \mathbb{N}.$$

Odsud je vidět, že posloupnost $\{x_n\}$ nemůže být cauchyovská. Nalezli jsme odpověď pro běžnou metriku. Mohli jsme však hned využít toho, že posloupnost $\{x_n\}$ není podle (‖7.28‖) konvergentní, a vzpomenout si, že se nacházíme v úplném metrickém prostoru, kde cauchyovské a konvergentní posloupnosti splývají.

Pro metriku $d$ si stačí uvědomit, že zobrazení $f$ zavedené v (‖7.27‖) je spojitou bijekcí mezi množinami $[0,\infty)$ a $[0,1)$ s vlastností, že $f(0) = 0$. Libovolná posloupnost je tak konvergentní

**Věta.** *Je-li $A_1 \supset A_2 \supset \cdots \supset A_i \supset \ldots$ neklesající řetězec neprázdných uzavřených podmnožin v úplném metrickém prostoru $X$ a* diam $A_i \to 0$, *pak existuje právě jeden bod $x \in X$ patřící do průniku všech $A_i$.*

Důkaz. Vyberme z každé množiny $A_i$ jeden bod $z_i$. Protože diam $A_i \to 0$, můžeme pro sebemenší kladné $\varepsilon$ najít index $n(\varepsilon)$ tak, aby všechny $A_i$ s indexy $i \geq n(\varepsilon)$ už měly průměr menší než $\varepsilon$. Pak ale nutně pro takto veliké indexy $i, j$ bude také $d(z_i, z_j) \leq \varepsilon$ a tedy je naše posloupnost cauchyovská. Bude proto mít limitní bod $z \in X$, který pochopitelně musí být hromadným bodem všech $A_i$, a proto patří do všech $A_i$ (když jsou všechny uzavřené) a tedy patří do jejich průniku.

Dokázali jsme tedy existenci $z$, zbývá odůvodnit jednoznačnost. Předpokládejme tedy, že máme body $z$ a $y$, oba v průniku všech $A_i$. Jejich vzdálenost pak ale musí být menší než průměr všech $A_i$, ten ale konverguje k nule. Tím je důkaz ukončen. □

**7.21. Věta** (Bairova věta)**.** *Je-li $X$ úplný metrický prostor, pak průnik libovolného spočetného systému otevřených hustých množin $A_i$ je množina hustá v metrickém prostoru $X$.*

Důkaz. Máme dán systém hustých a otevřených množin $A_i$ v $X$, $i = 1, 2 \ldots$, a chceme ukázat, že množina $A = \cap_{i=1}^{\infty} A_i$ má s libovolnou otevřenou množinou $U \subset X$ neprázdný průnik. Budeme postupovat induktivně s pomocí předchozí věty.



Jistě existuje $z_1 \in A_1 \cap U$, protože je ale množina $A_1$ otevřená, patří bod $z_1$ do tohoto průniku i s uzávěrem svého $\varepsilon_1$ okolí $U_1$ pro dostatečně malé $\varepsilon_1$. Označme si uzávěr této $\varepsilon_1$–koule $U_1$ jako $B_1$. Předpokládejme dále, že již jsou vybrány body $z_i$ a jejich otevřená $\varepsilon_i$–okolí $U_i$ pro $i = 1, \ldots, n$. Protože je množina $A_{n+1}$ otevřená a hustá v $X$, jistě existuje bod $z_{n+1} \in A_{n+1} \cap \bar{U}_n$, protože je ale $A_{n+1} \cap U_n$ otevřená, patří do ní bod $z_{n+1}$ i s dostatečně malým $\varepsilon_{n+1}$ okolím $U_{n+1}$. Pak jistě také pro uzávěry platí $B_{n+1} = \bar{U}_{n+1} \subset \bar{U}_n$ a tedy uzavřená množina $B_{n+1}$ je obsažena v $A_{n+1} \cap \bar{U}_n$. Jistě přitom můžeme předpokládat i $\varepsilon_n \leq 1/n$.

Jestliže takto induktivně postupujeme od původního bodu $z_1$ a množiny $B_1$, dostáváme neklesající posloupnost neprázdných uzavřených množin $B_n$, jejichž průměr jde k nule. Existuje tedy společný bod $z$ všech těchto množin, tj.

$$z \in \cap_{i=1}^{\infty} \bar{U}_i = \cap_{i=1}^{\infty} B_i \subset \cap_{i=1}^{\infty} A_n \cap U \ ,$$

což jsme chtěli dokázat. □

**7.22. Ohraničené a kompaktní množiny.** Pro reálná čísla se nám osvědčily následující pojmy, které nám ulehčovaly vyjadřování. Pro metrické prostory je můžeme převzít skoro beze změn:



*Vnitřním bodem podmnožiny $A$* v metrickém prostoru je takový prvek, který do $A$ patří i s nějakým svým $\varepsilon$–okolím.

*Hraniční bod* množiny $A$ je takový prvek $x \in X$, jehož každé okolí má neprázdný průnik jak s $A$, tak s doplňkem $X \setminus A$. Hraniční bod tedy může, ale nemusí patřit do samotné množiny $A$.

*Otevřené pokrytí* množiny $A$ je takový systém otevřených množin $U_i \subset X$, $i \in I$, že jejich sjednocení obsahuje celé $A$.

*Izolovaným bodem* množiny $A$ rozumíme prvek $a \in A$, který má v metrickém prostoru $X$ $\varepsilon$–okolí, jehož průnik s $A$ je právě jednobodová množina $\{a\}$.

„v původním významu“, právě když konverguje v metrickém prostoru $\mathbb{R}$ s metrikou $d$. Stejně tak platí, že posloupnost je cauchyovská v $\mathbb{R}$ vzhledem k běžné metrice právě tehdy, když je cauchyovská vzhledem k $d$. □

**7.25.** Je metrický prostor $\mathcal{S}[-1, 1]$ spojitých funkcí na intervalu $[-1, 1]$ s metrikou danou normou

(a) $\| f \|_p = \left( \int_{-1}^{1} | f(x) |^p \, dx \right)^{1/p}$ pro $p \geq 1$;

(b) $\| f \|_\infty = \max \{ | f(x) | ; \; x \in [-1, 1] \}$

úplný?

**Řešení.** Případ (a). Pro každé $n \in \mathbb{N}$ definujme funkci

$$f_n(x) = 0, \;\; x \in [-1, 0) \,, \qquad f_n(x) = 1, \;\; x \in \left[ \tfrac{1}{n}, 1 \right] ,$$
$$f_n(x) = nx, \;\; x \in \left[ 0, \tfrac{1}{n} \right) .$$

Takto získaná funkční posloupnost $\{f_n\}_{n \in \mathbb{N}} \subset \mathcal{S}[-1, 1]$ je cauchyovská. K ověření její cauchyovskosti stačí s pomocí geometrického významu určitého integrálu vyjádřit

$$\left( \int_{-1}^{1} | f_m(x) - f_n(x) |^p \, dx \right)^{1/p} < \left( \int_{0}^{1/n} 1 \, dx \right)^{1/p} = \left( \tfrac{1}{n} \right)^{1/p}$$

pro libovolné $m \geq n, m, n \in \mathbb{N}$.

Zabývejme se případnou limitou posloupnosti $\{f_n\}$ v $\mathcal{S}[-1, 1]$. Předpokládejme její existenci a označme ji jako $f$. Pro každé $\varepsilon \in (0, \; 1)$ zřejmě existuje $n(\varepsilon) \in \mathbb{N}$ takové, že

$$f_n(x) = 0, \;\; x \in [-1, 0], \qquad f_n(x) = 1, \;\; x \in [\varepsilon, 1]$$

pro všechna $n \geq n(\varepsilon)$. Spojitá funkce $f$ proto musí splňovat

$$f(x) = 0, \;\; x \in [-1, 0], \qquad f(x) = 1, \;\; x \in [\varepsilon, 1]$$

pro libovolně malé $\varepsilon > 0$. Tedy nutně

$$f(x) = 0, \;\; x \in [-1, 0], \qquad f(x) = 1, \;\; x \in (0, 1].$$

Tato funkce však není spojitá na $[-1, 1]$ – nepatří do uvažovaného metrického prostoru. Posloupnost $\{f_n\}$ tak nemá limitu v $\mathcal{S}[-1, 1]$ a tento prostor není úplný.

Případ (b). Nechť je libovolně dána cauchyovská posloupnost $\{f_n\}_{n \in \mathbb{N}} \subset \mathcal{S}[-1, 1]$. Členy této posloupnosti jsou spojité funkce $f_n$ na $[-1, 1]$ s vlastností, že ke každému $\varepsilon > 0$ (chcete-li, ke každému $\varepsilon/2$) existuje $n(\varepsilon) \in \mathbb{N}$, pro které platí

$$\max_{x \in [-1,1]} | f_m(x) - f_n(x) | < \frac{\varepsilon}{2}, \qquad m, n \geq n(\varepsilon). \tag{7.29}$$

Zvláště tak pro každé $x \in [-1, 1]$ dostáváme cauchyovskou číselnou posloupnost $\{f_n(x)\}_{n \in \mathbb{N}} \subset \mathbb{R}$. Neboť metrický prostor $\mathbb{R}$ s běžnou metrikou je úplný, každá (pro $x \in [-1, 1]$) posloupnost $\{f_n(x)\}$ je konvergentní. Označme

$$f(x) := \lim_{n \to \infty} f_n(x), \qquad x \in [-1, 1].$$

Množina $A$ prvků metrického prostoru se nazývá *ohraničená* nebo *omezená*, jestliže je její průměr konečný, tj. existuje kladné reálné číslo $r$ takové, že $d(x, y) \leq r$ pro všechny prvky $x, y \in A$. V opačném případě je *neohraničená* nebo *neomezená*.

Metrický prostor $X$ se nazývá *kompaktní*, jestliže v něm má každá posloupnost $x_i \in X$ podposloupnost konvergující k nějakému bodu $x \in X$.

U reálných čísel jsme si uváděli několik charakterizací kompaktnosti. U metrických prostorů to je o něco složitější s pojmem ohraničenosti. Pro libovolné podmnožiny $A$, $B \subset X$ v metrickém prostoru $X$ s metrikou $d$ definujeme *vzdálenost*



$$\operatorname{dist}(A, B) = \sup_{x \in A, y \in B} \{ d(x, y) \}.$$

Je-li $A = \{x\}$ jednobodová množina, hovoříme o vzdálenosti $\operatorname{dist}(x, B)$ bodu od množiny. Řekneme, že je metrický prostor $X$ *totálně omezený*, jestliže ke každému kladnému číslu $\varepsilon$ existuje konečná množina $A$ taková, že

$$\operatorname{dist}(x, A) < \varepsilon$$

pro všechny body $x \in X$. Připomeňme, že metrický prostor je *omezený*, jestliže má celé $X$ konečný průměr.

Je okamžitě vidět, že totálně omezený prostor je také omezený. Skutečně, průměr konečné množiny je vždy konečný a jeli $A$ množina z definice totální omezenosti příslušná k $\varepsilon$, pak vzdálenost dvou bodů $d(x, y)$ můžeme vždy shora odhadnout součtem $\operatorname{dist}(x, A)$, $\operatorname{dist}(y, A)$ a $\operatorname{diam} A$, což je konečné číslo. V případě metriky na podmnožině konečněrozměrného euklidovského prostoru tyto pojmy splývají, neboť omezenost množiny zaručuje omezenost všech jednotlivých souřadnic v pevně vybrané ortonormální bázi a odtud již plyne i totální omezenost (ověřte si podrobně samostatně).

**Věta.** *Následující podmínky na metrický prostor $X$ jsou ekvivalentní*

*(1) $X$ je kompaktní,*

*(2) každé otevřené pokrytí $X$ obsahuje konečné podpokrytí,*

*(3) $X$ je úplný a totálně omezený.*

Důkaz zde v detailech neuvádíme. Lze jej provést např. implikacemi (2) $\Longrightarrow$ (3), (3) $\Longrightarrow$ (1) a (1) $\Longrightarrow$ (2) a vcelku snadno jej lze dohledat v dostupné literatuře.

Zastavíme se alespoň u prvního kroku, kde se zásadním způsobem objevuje pojem totální omezenosti. Je-li splněna druhá podmínka věty, pak je vcelku snadno vidět, že musí být prostor $X$ totálně omezený. Skutečně, stačí si vybrat pokrytí $X$ pomocí všech $\varepsilon$–koulí se středy v bodech $x \in X$. Z něho musí jít vybrat konečné pokrytí a množina středů $x_i$ koulí, které se v tomto konečném pokrytí vyskytují, již naplňuje podmínku z definice totální omezenosti. K důkazu implikace (2) $\Longrightarrow$ (3) ale ještě chybí důkaz úplnosti.

**7.23. Kompaktnost na spojitých funkcích.** Jako příklad odlišného chování pojmu kompaktnosti v euklidovských prostorech a v prostorech funkcích si uvedeme velice užitečné tvrzení známé pod jménem *Arzelaova-Ascoliho věta*.

Říkáme, že jsou funkce $f$ z nějaké množiny funkcí $M$ na společném definičním oboru $A$ *rovnomocně spojité*, jestliže pro každé $x \in A$ a každé kladné $\varepsilon$ existuje (nezávisle na funkci $f$)

Limitním přechodem pro $m \to \infty$ v (‖7.29‖) obdržíme

$$\max_{x\in[-1,1]} |\, f(x) - f_n(x)\,| \le \tfrac{\varepsilon}{2} < \varepsilon, \quad n \ge n(\varepsilon).$$

To ovšem znamená, že posloupnost $\{f_n\}_{n\in\mathbb{N}}$ stejnoměrně konverguje k funkci $f$ na $[-1, 1]$. Jinak řečeno, $\{f_n\}_{n\in\mathbb{N}}$ konverguje k $f$ vzhledem k zadané normě. Již dříve jsme navíc zjistili, že stejnoměrnou limitou spojitých funkcí je funkce spojitá. Díky tomu nemusíme dokazovat, že $f \in \mathcal{S}[-1, 1]$. Metrický prostor je tudíž úplný.

Doplňme, že ke stejným závěrům (pomocí stejných úvah v obou variantách) bychom pochopitelně dospěli také pro obecnější metrický prostor $\mathcal{S}[a, b]$ spojitých funkcí na $[a, b]$. □

**7.26.** Jednu z nejdůležitějších charakteristik úplných metrických prostorů poskytuje tzv. princip vložených koulí. Ten říká, že metrický prostor $(X, d)$ je úplný právě tehdy, když pro každou posloupnost $\{A_n\}_{n\in\mathbb{N}}$ do sebe vnořených (tj. $A_{n+1} \subseteq A_n$, $n \in \mathbb{N}$) neprázdných uzavřených množin $A_n$ platí

$$\bigcap_{n\in\mathbb{N}} A_n \neq \emptyset. \tag{7.30}$$

Součástí tohoto tvrzení však je ještě jedna podmínka na uvažované posloupnosti $\{A_n\}$. Požaduje se, aby

$$\lim_{n\to\infty} \sup\{d(x, y);\ x, y \in A_n\} = 0. \tag{7.31}$$

Zjistěte, zda lze tuto podmínku vynechat.

**Řešení.** Pravděpodobně v rozporu s očekáváním většiny čtenářů nelze podmínku (‖7.31‖) vynechat: při jejím vynechání se tvrzení stane neplatným. Potřebujeme uvést jediný protipříklad dokládající, že bez této podmínky tvrzení neplatí.

Uvažujme proto množinu $X = \mathbb{N}$ s metrikou

$$d(m, n) = 1 + \tfrac{1}{m+n},\ m \neq n, \quad d(m, n) = 0,\ m = n.$$

První dvě vlastnosti metriky jsou očividně splněny. K dokázaní trojúhelníkové nerovnosti si stačí všimnout, že $d(m, n) \in (1, 4/3]$, je-li $m \neq n$. Stejně lehce lze najít všechny cauchyovské posloupnosti. Těmi jsou tzv. skorostacionární posloupnosti – od jistého indexu konstantní (konstantní až na konečně mnoho výjimek). Každá cauchyovská posloupnost je tedy konvergentní a uvažovaný prostor úplný.

Zaveďme množiny

$$A_n := \left\{m \in \mathbb{N};\ d(m, n) \le 1 + \tfrac{1}{2n}\right\}, \quad n \in \mathbb{N}.$$

Neostrá nerovnost v jejich definici zaručuje, že se jedná o uzavřené množiny. Neboť $A_n = \{n, n + 1, \dots\}$, (‖7.30‖) neplatí. Při vynechání podmínky (‖7.31‖) by to znamenalo, že metrický prostor není úplný, což není pravda. Pro jistotu dodejme, že

$$\lim_{n\to\infty} \sup\{d(x, y);\ x, y \in A_n\} = \lim_{n\to\infty} \left(1 + \tfrac{1}{2n+1}\right) = 1 \neq 0\,. \qquad \square$$

číslo $\delta > 0$, takové že pro všechna $y$ z $\delta$-okolí bodu $x$ bude $d(f(y), f(x)) < \varepsilon$.

**Věta.** *Množina $M \subset C[a, b]$ spjitých funkcí je kompaktní, právě když je omezená, uzavřená a rovnomocně spojitá.*

Důkaz zde nebudeme uvádět. Všimněte si rozdílu mezi použitou rovnomocnou a stejnoměrnou konvergencí!

**7.24. Důkaz věty 7.8 o Fourierových řadách.** Obecný kontext



metrik a konvergencí nám nyní umožní vrátit se k důkazu věty, ve které jsme dali částečný obrázek o bodové i jiné konvergenci Fourierových řad. Nejde nám přitom o nutné podmínky konvergencí a v literatuře lze najít mnoho jiných formulací. Naše věta 7.8 ale byla docela jednoduchá a postihla velké množství užitečných případů.

Pro začátek si bude dobré uvědomit, jak se mohou lišit konvergence vůči různým $L_p$ normám. Pro zjednodušení budeme vždy pracovat v zúplnění prostoru $S_c^0$ nebo $S_c^1$ vzhledem k příslušné normě, aniž bychom dumali nad tím, o jaké přesně prostory jde (i když bychom je mohli popisovat docela snadno pomocí Kurzweilova integrálu).

Hölderova nerovnost (použitá na funkce $f$ a konstantu 1) dává na $\mathcal{S}^0[a, b]$ první z následujících odhadů

$$\int_a^b |f(x)|dx \le |a-b|^{1/q}\left(\int_a^b |f(x)|^p\,dx\right)^{1/p} \le$$
$$\le |a-b|^{1/q} C^{1/q}\left(\int_a^b |f(x)|\,dx\right)^{1/p},$$

kde $p > 1$ a $1/p + 1/q = 1$, $C \ge |f(x)|$ na celém intervalu $[a, b]$ (takové stejnoměrné omezení konstantou vždy existuje, když je $f \in \mathcal{S}^0[a, b]$). Druhý odhad okamžitě plyne z odhadu $|f(x)|^p \le C^{p-1}|f(x)|$ a vztahu $1 - 1/p = 1/q$.

Je tedy z prvního odhadu zjevné, že $L_p$–konvergence $f_n \to f$ bude pro jakékoliv $p > 1$ vždy silnější než $L_1$–konvergence (a drobně upraveným odhadem ukážeme i obdobné silnější tvrzení, že $L_q$ konvergence je silnější než $L_p$ konvergence, kdykoliv je $q > p$, zkuste si sami). Pro použití druhého odhadu ale musíme požadovat stejnoměrnou omezenost posloupnosti funkcí $f_n$, tj. omezení funkcí $f_n$ konstantou $C$ musí být nezávislé na $n$. Pak totiž můžeme odhadnout $|f_n(x) - f(x)| \le 2C$ a dostáváme z našeho odhadu, že $L_1$–konvergence je silnější než $L_p$–konvergence.

Jsou tedy všechny $L_p$–normy na našem prostoru $S^0[a, b]$ rovnocenné z hlediska konvergence stejnoměrně omezených posloupností funkcí.

Nejtěžší (a také nejzajímavější) bude dokázat první tvrzení věty 7.8, které bývá v literatuře označováno jako *Dirichletova podmínka* (byla údajně odvozena již v roce 1824). Dokážeme proto nejprve, jak z této vlastnosti bodové konvergence vyplývají tvrzení (2) a (3) dokazované věty. Bez újmy na obecnosti můžeme předpokládat, že pracujeme na intervalu $[-\pi, \pi]$, tj. s periodou $T = 2\pi$.

Jako první krok si připravíme jednoduché odhady pro koeficienty Fourierovy řady. Samozřejmý je odhad

$$|a_n| \le \frac{1}{\pi}\int_{-\pi}^{\pi} |f(x)|\,dx$$

a totéž pro všechna $b_n$, neboť jak $\cos(x)$, tak $\sin(x)$ jsou v absolutní hodnotě ohraničené jedničkou. Pokud je ale $f$ spojitá funkce

**7.27.** Dokažte, že metrický prostor $l_2$ je úplný.

**Řešení.** Uvažujme libovolnou cauchyovskou posloupnost $\{x_n\}_{n\in\mathbb{N}}$ v prostoru $l_2$. Každým členem této posloupnosti je ovšem zase posloupnost, tj. $x_n = \{x_n^k\}_{k\in\mathbb{N}}$, $n \in \mathbb{N}$. Poznamenejme, že samozřejmě nezáleží na rozsahu indexování – zda $n, k \in \mathbb{N}$, resp. $n, k \in \mathbb{N} \cup \{0\}$. Zaveďme pomocné posloupnosti $y_k$ pro $k \in \mathbb{N}$ tak, že

$$y_k = \{y_k^n\}_{n\in\mathbb{N}} = \left\{x_n^k\right\}_{n\in\mathbb{N}}.$$

Je-li $\{x_n\}$ cauchyovská v $l_2$, pak tím spíše musí být cauchyovská každá z posloupností $y_k$ v $\mathbb{R}$ (posloupnosti $y_k$ jsou posloupnostmi reálných čísel). Z úplnosti $\mathbb{R}$ (vzhledem k běžné metrice) plyne, že všechny posloupnosti $y_k$ jsou konvergentní. Jejich limity označme jako $z_k$, $k \in \mathbb{N}$.

Stačí nám dokázat, že $z = \{z_k\}_{k\in\mathbb{N}} \in l_2$ a že posloupnost $\{x_n\}$ konverguje pro $n \to \infty$ v $l_2$ právě k posloupnosti $z$. Posloupnost $\{x_n\}_{n\in\mathbb{N}} \subset l_2$ je cauchyovská, a tak ke každému $\varepsilon > 0$ existuje $n(\varepsilon) \in \mathbb{N}$ s vlastností, že

$$\sum_{k=1}^{\infty}\left(x_m^k - x_n^k\right)^2 < \varepsilon, \quad m, n \geq n(\varepsilon),\ m, n \in \mathbb{N}.$$

Zvláště je

$$\sum_{k=1}^{l}\left(x_m^k - x_n^k\right)^2 < \varepsilon, \quad m, n \geq n(\varepsilon),\ m, n, l \in \mathbb{N},$$

odkud limitním přechodem pro $m \to \infty$ lze obdržet

$$\sum_{k=1}^{l}\left(z_k - x_n^k\right)^2 \leq \varepsilon, \quad n \geq n(\varepsilon),\ n, l \in \mathbb{N},$$

tj. (tentokráte $l \to \infty$)

$$\sum_{k=1}^{\infty}\left(z_k - x_n^k\right)^2 \leq \varepsilon, \quad n \geq n(\varepsilon),\ n \in \mathbb{N}. \tag{7.32}$$

Speciálně máme

$$\sum_{k=1}^{\infty}\left(z_k - x_n^k\right)^2 < \infty, \quad n \geq n(\varepsilon),\ n \in \mathbb{N}$$

a současně

$$\sum_{k=1}^{\infty}\left(x_n^k\right)^2 < \infty, \quad n \in \mathbb{N},$$

což plyne přímo z $\{x_n\}_{n\in\mathbb{N}} \subset l_2$. Protože

$$\sum_{k=1}^{\infty}\left(z_k x_n^k\right) \leq \sqrt{\sum_{k=1}^{\infty} z_k^2} \cdot \sqrt{\sum_{k=1}^{\infty}\left(x_n^k\right)^2}, \quad n \in \mathbb{N}$$

a

$$\sum_{k=1}^{\infty}\left(z_k - x_n^k\right)^2 = \sum_{k=1}^{\infty}\left[z_k^2 - 2z_k x_n^k + \left(x_n^k\right)^2\right], \quad n \in \mathbb{N},$$

musí být

$$\sum_{k=1}^{\infty} z_k^2 < \infty.$$

Tím jsme dokázali, že $z \in l_2$. Skutečnost, že $\{x_n\}$ konverguje pro $n \to \infty$ k $z$ v $l_2$, vyplývá z (‖7.32‖). □

v $\mathcal{S}^1[a, b]$, můžeme integrovat per partes a dostaneme

$$\begin{aligned} a_n(f) &= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(nx)dx = \\ &= \frac{1}{n\pi}[f(x)\sin(nx)]_{-\pi}^{\pi} - \frac{1}{n\pi}\int_{-\pi}^{\pi} f'(x)\sin(nx)\,dx = \\ &= -\frac{1}{n}b_n(f'). \end{aligned}$$

Píšeme zde $a_n(f)$ pro příslušný koeficient funkce $f$ atd.

Vidíme tedy, že čím „hladší“ funkce, tím rychleji se blíží Fourierovy koeficienty k nule. Iterací této procedury skutečně dostaneme odhad pro funkce $f$ v $\mathcal{S}^{k+1}[-\pi, \pi]$ se spojitými derivacemi až do řádu $k$ včetně:

$$|a_n(f)| \leq \frac{1}{n^{k+1}\pi}\int_{-\pi}^{\pi} |f^{(k+1)}(x)|dx$$

a totéž pro $b_n(f)$. Jinak řečeno, pro dostatečně hladké funkce $f$ jsou $n^k$–násobky jejich Fourierových koeficientu $a_n$ a $b_n$ ohraničeny $L_1$-normou jejich $k$–té derivace $f^{(k)}$.

Předpokládejme tedy, že máme spojitou funkci $f$ v prostoru $\mathcal{S}^1[a, b]$, jejíž částečné součty Fourierovy řady bodově konvergují k $f$. Můžeme pak odhadnout

$$\begin{aligned} |s_N(x) - f(x)| &= \left|\sum_{k=N+1}^{\infty}(a_k\cos(kx) + b_k\sin(kx))\right| \leq \\ &\leq \sum_{k=N+1}^{\infty}(|a_k| + |b_k|). \end{aligned}$$

Pravou stranu můžeme dále odhadnout pomocí koeficientů $a_n'$ a $b_n'$ derivace $f'$ (s použitím Hölderovy nerovnosti pro $L_p$ a $L_q$ normy pro nekonečné řady s $p = q = 2$, viz 7.15, a Besselovy nerovnosti pro obecné Fourierovy řady. viz 7.5.(2))

$$\begin{aligned} |s_N(x) - f(x)| &\leq \sum_{k=N+1}^{\infty}\frac{1}{k}(|a_k'| + |b_k'|) \leq \\ &\leq \left(2\sum_{k=N+1}^{\infty}\frac{1}{k^2}\right)^{1/2}\left(\sum_{k=N+1}^{\infty}(|a_k'|^2 + |b_k'|^2)\right)^{1/2} \leq \\ &\leq \sqrt{2}\left(\int_N^{\infty}\frac{1}{x^2}\,dx\right)^{1/2}\frac{1}{\sqrt{\pi}}\|f'\|_2 = \\ &= \left(\frac{\sqrt{2}}{\sqrt{\pi}}\|f'\|_2\right)\cdot\frac{1}{\sqrt{N}}. \end{aligned}$$

Dostali jsme takto nejen důkaz stejnoměrné konvergence naší řady k předjímané hodnotě, ale také odhad rychlosti konvergence:

$$\sup_{x\in\mathbb{R}}|s_N(x) - f(x)| \leq \left(\frac{\sqrt{2}}{\sqrt{\pi}}\|f'\|_2\right)\cdot\frac{1}{\sqrt{N}}.$$

Tím je dokázáno tvrzení 7.8.(2) za předpokladu platnosti Dirichletovy podmínky 7.8.(1).

**7.25. $L_2$–konvergence.** V dalším kroku našeho důkazu odvodíme $L_2$–konvergenci Fourierových řad za předpokladu stejnoměrné konvergence. Důkaz se opírá o obvyklou techniku aproximace nespojitých objektů spojitými, kterou popíšeme jen bez podrobností. V případě zájmu či potřeby by mělo být vcelku snadné detaily doplnit. Zformulujeme si napřed potřebné tvrzení obecně:



**7.28.** V metrickém prostoru $\mathcal{S}[-1,1]$ s metrikou danou normou $\|\cdot\|_\infty$ uvažujte množiny

$$A = \{f \in \mathcal{S}[-1,1];\ f(0) \in (0,2)\},$$
$$B = \{f \in \mathcal{S}[-1,1];\ \int_{-1}^{1} f(x)\,dx = 0\}.$$

Jsou tyto množiny otevřené, uzavřené?

**Řešení.** Vnitřkem množiny $M$ rozumíme množinu všech vnitřních bodů a značíme jej $M^0$. Libovolná množina $M$ je pak otevřená, právě když $M = M^0$. Podobně zavádíme uzávěr množiny $M$ jako množinu všech bodů majících nulovou vzdálenost od množiny $M$ a značíme ho $\overline{M}$. Stejně snadno vidíme, že libovolná množina $M$ je uzavřená právě tehdy, když $M = \overline{M}$. Protože platí

$$A^0 = A,\ \overline{A} = \{f \in \mathcal{S}[-1,1];\ f(0) \in [0,2]\},\quad B^0 = \emptyset,\ \overline{B} = B,$$

je množina $A$ otevřená a není uzavřená a množina $B$ je naopak uzavřená a není otevřená. □

**7.29.** Nechť je dána libovolná množina $X \neq \emptyset$. Zobrazení $d : X \times X \to \mathbb{R}$ definované předpisem

$$d(x,y) = 1,\ x \neq y,\quad d(x,y) = 0,\ x = y$$

je zjevně metrikou na $X$. Hovoří se o tzv. triviálním nebo častěji o diskrétním metrickém prostoru $(X,d)$.

(a) Popište všechny cauchyovské a konvergentní posloupnosti v $(X,d)$.

(b) Popište všechny otevřené, uzavřené a ohraničené množiny v $(X,d)$.

(c) Popište vnitřní, hraniční, hromadné a izolované body libovolné množiny v $(X,d)$.

(d) Popište všechny kompaktní množiny v $(X,d)$.

**Řešení.** (a) K tomu, aby mohla být jakákoli posloupnost $\{x_n\}_{n\in\mathbb{N}}$ cauchyovská, je v tomto prostoru nutné, aby existoval index $n \in \mathbb{N}$ takový, že $x_n = x_{n+m}$ pro všechna $m \in \mathbb{N}$. Posloupnost s touto vlastností pak nutně konverguje ke společné hodnotě $x_n = x_{n+1} = \cdots$ (mluvíme o skorostacionárních posloupnostech). Mimo jiné jsme tak dokázali, že metrický prostor $(X,d)$ je úplný.

(b) Otevřené 1-okolí libovolného prvku obsahuje pouze tento prvek. Každá jednoprvková množina je tedy otevřená. Neboť sjednocení libovolného počtu otevřených množin je otevřená množina, je každá množina v $(X,d)$ otevřená. To ale rovněž znamená, že každá množina je současně uzavřená. Skutečnost, že 2-okolí libovolného

**Lemma.** *Podmnožina spojitých funkcí $f$ v $\mathcal{S}^0[a,b]$ na konečném intervalu $[a,b]$ je v tomto prostoru hustá podmnožina vzhledem k $L_2$–normě.*

Myšlenka důkazu je dobře vidět na příkladu aproximace po částech konstantní funkce $h$ na $[-\pi,\pi]$ z odstavce 7.9. Pro každé $\pi > \delta > 0$ definujeme funkci $f_\delta$ jako $x/\delta$ pro $|x| \le \delta$ a $f_\delta(x) = h(x)$ jinak. Zjevně jsou všechny funkce $f_\delta$ spojité, protože jsme bod nespojitosti překlenuli pomocí vhodné lineární funkce na intervalu, jehož velikost je kontrolována pomocí $\delta$. Velmi jednoduše se spočte, že $\|h - f_\delta\|_2 \to 0$, neboť funkce $f$ je omezená v absolutní hodnotě a tedy příspěvek integrace přes stále se zmenšující interval musí jít k nule.

Zcela stejným způsobem můžeme ošetřit všechny body nespojitosti obecné funkce $f$, kterých je maximálně konečně mnoho a tedy jsou skutečně všechny uvažované funkce hromadnými body posloupností spojitých funkcí.

Nyní je již náš důkaz jednoduchý, protože pro zadanou funkci $f$ můžeme odhadnout vzdálenost od částečných součtů její Fourierovy řady pomocí spojitého přiblížení $f_\varepsilon$ takto (všechny normy v tomto odstavci jsou $L_2$ normy):

$$\|f - s_N(f)\| \le \|f - f_\varepsilon\| + \|f_\varepsilon - s_N(f_\varepsilon)\| + \|s_N(f_\varepsilon) - s_N(f)\|$$

a jednotlivé sčítance napravo umíme kontrolovat.

První z nich je nejvýše $\varepsilon$, podle předpokladu o stejnoměrné konvergenci pro spojité funkce můžeme dosáhnout stejně malého ohraničení i druhého sčítance. U třetího je dobré si všimnout, že jde vlastně o velikost částečného součtu Fourierovy řady pro $f - f_\varepsilon$. Je tedy jistě

$$\|f - f_\varepsilon - s_N(f - f_\varepsilon)\| \le \|f - f_\varepsilon\|,$$

a proto také (díky trojúhelníkové nerovnosti)

$$\|s_N(f - f_\varepsilon)\| \le 2\|f - f_\varepsilon\| \le 2\varepsilon.$$

Celkem jsme tedy odhadli celou vzdálenost pro dostatečně blízké spojité funkce a dostatečně velká $N$ číslem $4\varepsilon$. Tím je dokazovaná $L_2$ konvergence potvrzena.

**7.26. Dirichletovo jádro.** A konečně se dáme do důkazu prvního tvrzení věty 7.8. Přímo z definice Fourierovy řady $F(t)$ funkce $f(t)$ a s využitím jejího vyjádření s komplexní exponenciálou v 7.7 dostáváme pro částečné součty $s_N(t)$ výraz



$$s_N(t) = \frac{1}{T}\sum_{k=-N}^{N} \int_{-T/2}^{T/2} f(x)\,\mathrm{e}^{-i\omega kx}\,\mathrm{e}^{i\omega kt}\,dx,$$

kde $T$ je základní perioda, se kterou pracujeme, a $\omega = 2\pi/T$. Tento výraz můžeme přepsat jako

$$s_N(t) = \int_{-T/2}^{T/2} K_N(t-x) f(x)\,dx$$

a funkci

$$K_N(y) = \frac{1}{T}\sum_{k=-N}^{N} \mathrm{e}^{i\omega ky}$$

nazýváme *Dirichletovo jádro*. Všimněme si, že součet je částí geometrické řady s poměrem členů $\mathrm{e}^{i\omega y}$. Můžeme ji tedy přímo vyjádřit pro všechna $y \neq 0$ následujícím způsobem (po cestě násobíme čitatel i jmenovatel výrazem $-\mathrm{e}^{-i\omega y/2}$, abychom uměli

prvku splývá s celým prostorem, pak znamená, že každá množina v $(X, d)$ je ohraničená.

(c) Znovu využijeme toho, že otevřené 1-okolí každého prvku obsahuje pouze tento prvek. Odsud vyplývá, že každý bod libovolné množiny je jejím vnitřním a současně izolovaným bodem a že žádná množina nemá ani jeden hraniční nebo hromadný bod.

(d) Každá konečná množina v libovolném metrickém prostoru je zřejmě kompaktní (zadává kompaktní metrický prostor zúžením definičního oboru $d$). Z popisu konvergentních posloupností (viz (a)) plyne, že žádná nekonečná množina nemůže být kompaktní v $(X, d)$. □

**7.30.** Rozhodněte, zda je množina (nazývaná Hilbertova krychle)

$$A = \left\{\{x_n\}_{n\in\mathbb{N}} \in l_2;\ |x_n| \le \tfrac{1}{n},\ n \in \mathbb{N}\right\}$$

kompaktní v $l_2$. Poté rozhodněte o kompaktnosti množiny

$$B = \left\{\{x_n\}_{n\in\mathbb{N}} \in l_\infty;\ |x_n| < \tfrac{1}{n},\ n \in \mathbb{N}\right\}$$

v prostoru $l_\infty$.

**Řešení.** Víme, že prostor $l_2$ je úplný. Každá uzavřená podmnožina úplného metrického prostoru sama zadává úplný metrický prostor. Množina $A$ je očividně uzavřená v $l_2$, a tak k její kompaktnosti stačí ukázat, že je totálně omezená.

Vyjděme z nám dobře známého součtu

$$\sum_{k=1}^{\infty} \tfrac{1}{k^2} = \tfrac{\pi^2}{6}.$$

Pro každé $\varepsilon > 0$ tak existuje $n(\varepsilon) \in \mathbb{N}$ splňující

$$\sqrt{\sum_{k=n(\varepsilon)+1}^{\infty} \tfrac{1}{k^2}} < \tfrac{\varepsilon}{2}.$$

Z každého z intervalů $[-1/n, 1/n]$ pro $n \in \{1, \dots, n(\varepsilon)\}$ můžeme vybrat konečně mnoho bodů $x_1^n, \dots, x_{m(n)}^n$ tak, aby pro libovolné $x \in [-1/n,\ 1/n]$ bylo

$$\min_{j\in\{1,\dots,m(n)\}} \left| x - x_j^n \right| < \tfrac{\varepsilon}{\sqrt{5^n}}.$$

Uvažujme takové posloupnosti $\{y_n\}_{n\in\mathbb{N}}$ z $l_2$, jejichž členy s indexy $n > n(\varepsilon)$ jsou nulové a současně platí

$$y_1 \in \left\{x_1^1, \dots, x_{m(1)}^1\right\}, \dots, y_{n(\varepsilon)} \in \left\{x_1^{n(\varepsilon)}, \dots, x_{m(n(\varepsilon))}^{n(\varepsilon)}\right\}.$$

Všech takových posloupností je konečně mnoho a tvoří $\varepsilon$-síť pro $A$, neboť

$$\sqrt{\tfrac{\varepsilon^2}{5} + \tfrac{\varepsilon^2}{5^2} + \dots + \tfrac{\varepsilon^2}{5^{n(\varepsilon)}}} + \tfrac{\varepsilon}{2} < \varepsilon \cdot \sqrt{\tfrac{1}{1-\frac{1}{5}} - 1} + \tfrac{\varepsilon}{2} = \varepsilon.$$

Libovolnost $\varepsilon > 0$ potom implikuje, že množina $A$ je totálně omezená, což již dává její kompaktnost.

Rozhodnout o kompaktnosti množiny $B$ je velmi snadné. Každá kompaktní množina totiž musí být uzavřená, a to množina $B$ není. Jejím uzávěrem je

přepsat následně pomocí reálné funkce sin):

$$\begin{aligned} K_N(y) &= \frac{1}{T}\frac{\mathrm{e}^{-iN\omega y} - \mathrm{e}^{i(N+1)\omega y}}{1 - \mathrm{e}^{i\omega y}} = \\ &= \frac{1}{T}\frac{-\mathrm{e}^{-i(N+1/2)\omega y} + \mathrm{e}^{i(N+1/2)\omega y}}{\mathrm{e}^{i\omega y/2} - \mathrm{e}^{-i\omega y/2}} = \\ &= \frac{1}{T}\frac{\sin(\omega(N+1/2)y)}{\sin(\omega y/2)}. \end{aligned}$$

V bodě $y = 0$ samozřejmé přímo vidíme $K_N(0) = \frac{1}{T}(2N+1)$.

Z posledního výrazu je také vidět, že $K_N(y)$ je sudá funkce a pomocí L'Hospitalova pravidla přímo rychle spočteme, že je to funkce všude spojitá. Protože všechny částečné součty řady pro konstantní funkci $f(x) = 1$ jsou 1, dostáváme přímo z definice Dirichletova jádra

$$\int_{-T/2}^{T/2} K_N(x)dx = 1.$$

U periodických funkcí jsou jejich integrály přes intervaly délky periody nezávislé na volbě krajních bodů intervalu integrace. Proto můžeme pomocí změny souřadnic použít pro částečné součty též výraz

$$s_N(x) = \int_{-T/2}^{T/2} K_N(y)\, f(x+y)\, dy.$$

Teď konečně máme vše připraveno. Nejprve se budeme věnovat případu, kdy je funkce $f$ v bodě $x$ spojitá a diferencovatelná. Chceme pro tento případ dokázat, že Fourierova řada $F(x)$ v bodě $x$ konverguje k hodnotě $f(x)$. Dostáváme

$$s_N(x) - f(x) = \int_{-T/2}^{T/2} (f(x+y) - f(x))K_N(y)\, dy.$$

Integrovaný výraz můžeme přepsat do tvaru, který bude připomínat opět Fourierovy koeficienty pro vhodné funkce:

$$\begin{aligned} &\frac{f(x+y) - f(x)}{\sin(\omega y/2)} \sin((N+1/2)\omega y) = \\ &\quad = \varphi_x(y)\big(\cos(\omega y/2)\sin(N\omega y) + \sin(\omega y/2)\cos(N\omega y)\big), \end{aligned}$$

kde jsme si označili funkci

$$\varphi_x(y) = \frac{f(x+y) - f(x)}{\sin(\omega y/2)}$$

pro $y \neq 0$, zatímco $\varphi_x(0) = f'(x)$. Všimněme si, že pro tento krok jsme potřebovali diferencovatelnost a spojitost $f$ v bodě $x$.

Nyní ale můžeme skutečně chápat rozdíl $s_N(x) - f(x)$ jako součet Fourierových koeficientů $b_N(\psi_1)$ a $a_N(\psi_2)$, kde

$$\psi_1(y) = \frac{T}{2}\varphi_x(y)\cos(\omega y/2),\ \ \psi_2(y) = \frac{T}{2}\varphi_x(y)sin(\omega y/2).$$

To ale znamená, že s rostoucím $N$ nutně tento výraz $b_N(\psi_1 + a_N(\psi_2)$ konverguje k nule (viz 7.5.(2)).

Závěrem se podíváme na konvergenci v případě, že v bodě $x = 0$ má funkce $f$ nebo její derivace bod nespojitosti. Protože jde o funkci v $\mathcal{S}^1$, je v okolních bodech mimo $x = 0$ již spojitá a diferencovatelná. Rozložme si funkci $f$ na její sudou část $f_1$ a lichou část $f_2$, tj.

$$f(x) = \frac{1}{2}(f(x) + f(-x)) + \frac{1}{2}(f(x) - f(-x)).$$

$$\overline{B} = \left\{\{x_n\}_{n\in\mathbb{N}} \in l_\infty;\ |x_n| \le \tfrac{1}{n},\ n \in \mathbb{N}\right\}.$$

Množina $\overline{B}$ pak je kompaktní. Důkaz je výrazně jednodušší než pro množinu $A$, a proto jej přenecháváme čtenáři jako cvičení. □

### D. Integrální operátory

Konvoluce je jedním z nástrojů k vyhlazování funkcí. Zkusme spočítat konvoluci dvou funkcí, které mají obě konečný nosič (nosič je množina čísel, ve kterých je hodnota funkce nenulová).

**7.31.** Určete konvoluci $f_1 * f_2$, kde

$$f_1(x) = \begin{cases} 1-x^2 & \text{pro } x \in [-1,1], \\ 0 & \text{jinak,} \end{cases}$$

$$f_2(x) = \begin{cases} x & \text{pro } x \in [0,1], \\ 0 & \text{jinak.} \end{cases}$$

**Řešení.** Hodnota konvoluce $f_1 * f_2$ v bodě $t$ je dána integrálem přes všechna reálná čísla ze součinu funkce $f_1(x)$ a funkce $f_2(t-x)$ podle proměnné $x$ (viz 7.13). Je tedy tato hodnota nulová, jestliže je alespoň jedna z hodnot $f_1(x)$ a $f_2(t-x)$ nulová pro libovolné reálné $x$. Obráceně hodnota konvoluce může být v bodě $t$ nenulová, pouze pokud existují taková $x$, pro která $f_1(x) \neq 0 \neq f_2(t-x)$. Podle definice daných funkcí je to tehdy, pokud existují taková $x \in [-1,1]$ ($f_1(x) \neq 0$), že $(t-x) \in [0,1]$ ($f_2(t-x) \neq 0$). Neboli $f_1 * f_2(t)$ může být nenulové pokud $[t-1, t+1] \cap [0,1] \neq \emptyset$. To nastává pro $t \in [-1,2]$. Integrujeme pak přes $x$ náležící průniku intervalů $[t-1, t+1]$ a $[0,1]$. Tento průnik se dále liší v závislosti na $t \in [-1,2]$:

a) pro $t \in [-1,0]$ je $[t-1, t+1] \cap [0,1] = [0, t+1]$,
b) pro $t \in [0,1]$ je $[t-1, t+1] \cap [0,1] = [0,1]$,
c) pro $t \in [1,2]$ je $[t-1, t+1] \cap [0,1] = [t-1, 1]$.

V závislosti od průniku těchto intervalů je potom:
a)

$$\int_{-\infty}^{\infty} f_1(x) f_2(t-x)\,\mathrm{d}x = \int_0^{t+1} f_1(x) f_2(t-x)\,\mathrm{d}x =$$
$$= \int_0^{t+1} (1-x^2)(t-x)\,\mathrm{d}x = -\frac{1}{12}t^4 + t^2 + \frac{2}{3}t - \frac{1}{4},$$

b)

$$\int_{-\infty}^{\infty} f_1(x) f_2(t-x) = \int_0^{1} f_1(x) f_2(t-x) =$$
$$= \int_0^{1} (1-x^2)(t-x)\,\mathrm{d}x = \frac{2}{3}t - \frac{1}{4},$$

V bodě $x = 0$ přitom definujeme hodnotu $f_1(0)$ jako

$$\frac{1}{2}\left(\lim_{y\to 0_+} f(y) + \lim_{y\to 0_-} f(y)\right).$$

Pak se snadno přesvědčíme, že sudá část $f_1(x)$ je spojitá a diferencovatelná v bodě $x = 0$ (díky tomu, že jednostranné limity existují) a tedy i na celém okolí tohoto bodu. Zároveň nás nepřekvapí, že lichá část splňuje $f_2(0) = 0$ a stejně tak je v nule nulová i Fourierova řada, ve které jsou pouze členy se $\sin(n\omega x)$.

Můžeme proto využít předchozího spojitého případu a spočíst pro Fourierovu řadu $F(x)$ naší funkce $f$

$$F(0) = F_1(0) + F_2(0) = \tfrac{1}{2}\Big(\lim_{y\to 0_+} f(y) + \lim_{y\to 0_-} f(y)\Big) + 0,$$

což jsme chtěli dokázat.

V případě nespojitosti v obecném bodě můžeme postupovat obdobně a celý důkaz dirichletovy podmínky je ukončen (a tím i důkaz tvrzení (2) a (3) věty 7.8, v jejichž důkazech jsme předpokládali správnost Dirichletovy podmínky).

### 3. Integrální operátory

**7.27. Integrální operátory.** V případě konečněrozměrných vektorových prostorů jsme mohli vnímat vektory jako zobrazení z konečné množiny pevně zvolených generátorů do prostoru souřadnic. Sčítání vektorů a násobení vektorů skaláry pak bylo dáno odpovídajícími operacemi s takovými funkcemi. Stejným způsobem jsme pak pracovali i s vektorovými prostory funkcí jedné reálné proměnné, když jejich hodnotami byly skaláry (nebo případně i vektory).



Nejjednodušší lineární zobrazení $\alpha$ mezi vektorovými prostory zobrazovala vektory do skalárů (tzv. lineární formy). Byla definována jako součet součinů souřadnic $x_i$ vektorů s pevně zvolenými hodnotami $\alpha_i = \alpha(e_i)$ na generátorech $e_i$, tj. pomocí jednořádkových matic:

$$(x_1, \ldots, x_n)^T \mapsto (\alpha_1, \ldots, \alpha_n) \cdot (x_1, \ldots, x_n)^T.$$

Složitější zobrazení s hodnotami opět v tom samém prostoru pak byla obdobně zadána čtvercovými maticemi. Velice podobně umíme přistoupit k lineárním operacím na prostorech funkcí.

Budeme chvíli pro jednoduchost pracovat s reálným vektorovým prostorem $\mathcal{S}$ všech po částech spojitých reálných funkcí s kompaktním nosičem definovaných na celém $\mathbb{R}$ nebo na intervalu $I = [a,b]$. Lineárním zobrazením $\mathcal{S} \to \mathbb{R}$ budeme říkat (reálné) *lineární funkcionály*. Příklady takových funkcionálů můžeme velmi snadno zadat dvěma způsoby — pomocí vyčíslení funkce (případně jejích derivací) v jednotlivých pevně zvolených bodech nebo pomocí integrování. Příkladem funkcionálu $L$ tedy může být vyčíslení v jediném pevném bodě $x_0 \in I$

$$L(f) = f(x_0)$$

a příklad s integrováním může být zadán pomocí pevně zvolené funkce $g(x)$

$$L(f) = \int_a^b f(x)g(x)\,dx.$$

Funkce $g(x)$ zde hraje roli váhy, se kterou při definici Riemannova integrálu bereme jednotlivé hodnoty reprezentující funkci $f(x)$. Nejjednodušším příkladem takového funkcionálu je samozřejmě Riemannův integrál samotný, tj. případ s $g(x) = 1$ pro všechny body $x$.

c)

$$\int_{-\infty}^{\infty} f_1(x)\,f_2(t-x) = \int_{t-1}^{1} f_1(x)\,f_2(t-x) =$$
$$= \int_{t-1}^{1} (1-x^2)(t-x)\,\mathrm{d}x = \frac{1}{12}t^4 - t^2 + \frac{4}{3}t.$$

Celkem tak dostáváme:

$$f_1 * f_2(t) = \begin{cases} -\frac{1}{12}t^4 + t^2 + \frac{2}{3}t - \frac{1}{4} & \text{pro } t \in [-1,0], \\ \frac{2}{3}t - \frac{1}{4} & \text{pro } t \in [0,1], \\ \frac{1}{12}t^4 - t^2 + \frac{4}{3}t & \text{pro } t \in [1,2] \\ 0 & \text{jinak.} \end{cases}$$

□

**7.32.** Určete konvoluci $f_1 * f_2$, kde

$$f_1(x) = \frac{1}{x} \quad \text{pro } x \neq 0$$
$$f_2(x) = \begin{cases} x & \text{pro } x \in [-1,1] \\ 0 & \text{jinak} \end{cases}$$

**Řešení.** Hodnota konvoluce v bodě $t$ je dána integrálem $\int_{-\infty}^{\infty} f_1(x)\,f_2(t-x)\,\mathrm{d}x$. Integrovaná funkce je nenulová pokud je druhý z činitelů nenulový, tedy pokud $(t-x) \in [-1,1]$, tj. $x \in [t-1, t+1]$. Hodnotu konvoluce v bodě $t$ tak můžeme interpretovat jako integrální průměr funkce $f_1$ přes interval $(t-1, t+1)$. Při integrování přes tento interval musíme rozlišit, náleží-li číslo 0 tomuto intervalu, či nikoliv. V případě, že interval nulu obsahuje, tak musíme integrál rozdělit na dva integrály. Jeden bude typu $\int_{-a}^{a} 1/x dx$ a ten je jakožto integrál ve smyslu Cauchovy hlavní hodnoty nulový (intuitivně je plocha vymezená křivkou $1/x$ pro $x \in (-a, a)$ středově symetrická podle nuly, integrál jakožto plocha pod křivkou by měl být nulový). Zbude integrál $\int_{1-t}^{t+1} \frac{1}{x}\,\mathrm{d}x$ (rozmyslete si, že předpis funguje i pro záporné $t$). Dostáváme tak:

$$f_1 * f_2(t) = \begin{cases} \int_{t-1}^{t+1} \frac{1}{x}\,\mathrm{d}x = \ln\left|\frac{t+1}{t-1}\right| & \text{pro } t \in (-\infty,-1] \cup [1,\infty], \\ \int_{1-t}^{1+t} \frac{1}{x}\,\mathrm{d}x = \ln\left|\frac{1+t}{1-t}\right| & \text{pro } t \in [-1,1]. \end{cases}$$

□

*7.33.* Určete konvoluci $f_1 * f_2$ funkcí

$$f_1 = \begin{cases} 1-x & \text{pro } x \in [-2,1], \\ 0 & \text{jinak,} \end{cases}$$
$$f_2 = \begin{cases} 1 & \text{pro } x \in [0,1], \\ 0 & \text{jinak.} \end{cases}$$

○

Dobrou představu dává volba funkce

$$g(x) = \begin{cases} 0 & \text{je-li } |x| \geq \varepsilon, \\ \frac{1}{2\varepsilon} & \text{je-li } |x| < \varepsilon. \end{cases}$$

pro jakákoliv $\varepsilon > 0$. Integrál funkce $g$ přes $\mathbb{R}$ je jednotkový a náš lineární funkcionál můžeme vnímat jako (rovnoměrné) zprůměrování hodnot funkce $f$ přes $\varepsilon$–okolí počátku. Obdobně můžeme pracovat s funkcí

$$g(x) = \begin{cases} 0 & \text{je-li } |x| \geq \varepsilon \\ \mathrm{e}^{\frac{1}{x^2-\varepsilon^2}+\frac{1}{\varepsilon^2}} & \text{je-li } |x| < \varepsilon \end{cases}$$

se kterou jsme se setkali v odstavci 6.6 na straně 6.6. To je funkce hladká na celém $\mathbb{R}$ s kompaktním nosičem v intervalu $(-\varepsilon, \varepsilon)$. Náš funkcionál má tentokrát význam vážené kombinace hodnot, tentokrát však bereme rychle se zmenšující váhy jednotlivých argumentů se vzrůstající vzdáleností od počátku. Jistě má $g$ konečný integrál přes celé $\mathbb{R}$, nebude to ale jednička. Vydělením $g$ tímto integrálem bychom opět obdrželi funkcionál, který bude mít význam nerovnoměrného průměrování dané funkce $f$.

Jiný velice obvyklý příklad je tzv. Gaussova funkce

$$g(x) = \frac{1}{\pi}\,\mathrm{e}^{-x^2},$$

což je funkce opět s jedničkovým integrálem přes celé $\mathbb{R}$ (což časem také ukážeme), tentokrát mají všechny argumenty $x$ v příslušném „průměru“ nenulovou váhu, byť s rostoucí vzdáleností od počátku velmi rychle zanedbatelně malou.

Další takový příklad s jedničkovým integrálem přes celé $\mathbb{R}$ jsme viděli před chvílí při diskusi Dirichletových jader $g(x) = K_N(x)$ u Fourierových řad.

**7.28. Konvoluce funkcí.** Integrální funkcionály z předchozího odstavce můžeme lehce modifikovat, abychom obdrželi „rozmlžené zprůměrování“ hodnot funkce $f$ kolem daného bodu $y \in \mathbb{R}$:



$$L_y(f) = \int_{-\infty}^{\infty} f(x)g(y-x)\,dx$$

KONVOLUCE FUNKCÍ JEDNÉ REÁLNÉ PROMĚNNÉ

Volný parametr $y$ v naší definici funkcionálu $L_y(f)$ může být vnímán jako nová nezávislá proměnná a naše operace $L_y$ tedy ve skutečnosti zobrazuje funkce opět na funkce $f \mapsto \tilde{f}$:

$$\tilde{f}(y) = L_y(f) = \int_{-\infty}^{\infty} f(x)g(y-x)\,dx.$$

Této operaci se říká *konvoluce funkcí* $f$ a $g$, značíme ji $f * g$.

Budeme s konvolucí většinou používat pro reálné nebo komplexní funkce na $\mathbb{R}$ s kompaktním nosičem.

Pomocí transformace $t = z - x$ se snadno spočte

$$(f * g)(z) = \int_{-\infty}^{\infty} f(x)g(z-x)\,dx =$$
$$= -\int_{\infty}^{-\infty} f(z-t)g(t)\,dt = (g * f)(z).$$

Je tedy konvoluce coby binární operace

$$* : \mathcal{S}_c \times \mathcal{S}_c \to \mathcal{S}_c$$

**7.34.** Nalezněte Fourierovu transformaci $\mathcal{F}(f) = \tilde{f}$ funkce

$$f(t) = \operatorname{sgn} t, \quad t \in (-1,1); \qquad f(t) = 0, \quad t \in \mathbb{R} \setminus (-1,1),$$

tj. $f(0) = 0$, $f(t) = 1$ pro $t \in (0,1)$ a $f(t) = -1$ pro $t \in (-1,0)$.

**Řešení.** Fourierova transformace uvedené funkce je

$$\mathcal{F}(f)(\omega) = \tfrac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(t)\, \mathrm{e}^{-i\omega t}\, dt =$$

$$= \tfrac{1}{\sqrt{2\pi}} \int_{-1}^{1} \operatorname{sgn} t\ [\cos(\omega t) - i \sin(\omega t)]\ dt.$$

Protože součin dvou lichých funkcí je sudá funkce, součin sudé a liché je lichá funkce a protože integrál liché funkce přes interval $[-1, 1]$ je 0 (pokud tento integrál existuje) a integrál sudé funkce přes interval $[-1, 1]$ je roven dvojnásobku integrálu přes $[0, 1]$, dostáváme dále

$$\mathcal{F}(f)(\omega) = \tfrac{2}{\sqrt{2\pi}} \int_0^1 -i \sin(\omega t)\ dt = \tfrac{2i}{\sqrt{2\pi}} \left[\tfrac{\cos(\omega t)}{\omega}\right]_0^1 = i\sqrt{\tfrac{2}{\pi}}\, \tfrac{\cos\omega - 1}{\omega}.$$

Kdybychom přímo využili známé vyjádření Fourierovy transformace liché funkce $f$, snadněji bychom obdrželi

$$\mathcal{F}(f)(\omega) = \tfrac{-2i}{\sqrt{2\pi}} \int_0^{\infty} f(t)\, \sin(\omega t)\ dt = \tfrac{-2i}{\sqrt{2\pi}} \int_0^1 \sin(\omega t)\ dt = \cdots =$$

$$= i\sqrt{\tfrac{2}{\pi}}\, \tfrac{\cos\omega - 1}{\omega}\,. \qquad \square$$

**7.35.** Vyřešte integrální rovnici

$$\int_0^{\infty} f(x)\, \sin(xt)\ dt = \mathrm{e}^{-x}, \quad x > 0$$

pro neznámou funkci $f$.

**Řešení.** Pokud obě strany rovnice vynásobíme číslem $\sqrt{2/\pi}$, obdržíme na levé straně právě sinovou Fourierovu transformaci. Stačí tedy aplikovat na rovnici inverzní transformaci. Takto dostaneme

$$f(t) = \tfrac{2}{\pi} \int_0^{\infty} \mathrm{e}^{-x}\, \sin(xt)\ dx, \quad t > 0.$$

Dvojnásobným použitím metody per partes pak lze spočítat

$$\int \mathrm{e}^{-x}\, \sin(xt)\ dx = = \tfrac{\mathrm{e}^{-x}}{1+t^2}\, [-\sin(xt) - t\cos(xt)] + C,$$

a tudíž je

$$\int_0^{\infty} \mathrm{e}^{-x}\, \sin(xt)\ dx =$$

$$\lim_{x\to\infty} \left(\tfrac{\mathrm{e}^{-x}}{1+t^2}\, [-\sin(xt) - t\cos(xt)]\right) - \tfrac{\mathrm{e}^0}{1+t^2}\, (-t) = \tfrac{t}{1+t^2}.$$

Řešením rovnice je proto funkce

$$f(t) = \tfrac{2}{\pi}\, \tfrac{t}{1+t^2}, \quad t > 0\,. \qquad \square$$

**7.36.** Popište Fourierovu transformaci $\mathcal{F}(f)$ funkce

$$f(t) = \mathrm{e}^{-at^2}, \quad t \in \mathbb{R},$$

kde $a > 0$.

**Řešení.** Naším úkolem je vypočítat

$$\mathcal{F}(f)(\omega) = \tfrac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{e}^{-at^2}\, \mathrm{e}^{-i\omega t}\, dt.$$

na dvojicích funkcí s kompaktními nosiči komutativní. Stejně tak můžeme konvoluce uvažovat s pomocí integrace přes konečný interval, musíme se jen postarat o to, aby byly dobře definovány funkce, které v nich vystupují. Zejména je to tedy dobře možné u periodických funkcí a integrování přes interval délky periody.

Konvoluce je mimořádně užitečný nástroj pro modelování způsobu, jak pozorujeme data měřená v experimentu nebo jak se projevuje prostředí při přenosu informací (např. analogový audio nebo video signál ovlivňovaný šumy apod.). Argument $f$ je přenášenou informací, funkce $g$ je volena tak, aby co nejlépe vystihovala vlivy prostředí či zvoleného technického postupu při zpracovávání signálu, resp. jakýchkoliv dat.

**7.29. Gibbsův efekt.** Jeden velmi užitečný případ konvoluce



jsme vlastně již viděli dříve. V odstavci 7.26 jsme interpretovali částečný součet Fourierovy řady pro funkci $f$ jako konvoluci s Dirichletových jádrem $K_N(y) = \sum_{-T/2}^{T/2} \mathrm{e}^{i\omega k y}$.

Tato interpretace umožňuje také vysvětlit tzv. Gibbsův jev zmíněný v odstavci 7.9. Jestliže totiž máme možnost předem omezit/odhadnout rozložení vah kolem nuly a zároveň víme, že je funkce $f$ ohraničená, lze vcelku snadno odvodit, do jaké míry je efekt konvoluce na na funkci $f$ lokální. Pomocí takového odhadu lokálnosti konvoluce lze totiž ověřit, že se konvoluce s Dirchletovými jádry budou kolem skoku chovat obdobně jako je tomu u skokové funkce z odstavce 7.9 a pro ni lze snadno spočíst pozorovaný efekt explicitně.

Nebudeme tu uvádět podrobnosti, čtenář může buď dohledat jinde nebo si provést sám jako netriviální cvičení.

**7.30. Fourierova transformace.** Konvoluce jsou jedním



z mnoha případů obecných integrálních operátorů na prostorech funkcí ve tvaru

$$L(f)(y) = \int_a^b f(x) k(y,x)\, dx.$$

Funkce $k(y, x)$ závislá na dvou proměnných,

$$k : \mathbb{R}^2 \to \mathbb{R},$$

se nazývá *jádro integrálního operátoru* $L$. Definiční obor takových funkcionálů je nutné volit s ohledem na vlastnosti jádra tak, aby vždy existoval použitý integrál.

Teorie integrálních operátorů s jádry a rovnic, které je obsahují, je velice užitečná a zajímavá zároveň, bohužel pro ni zde teď ale nemáme dost prostoru. Zaměříme se alespoň na jeden mimořádně důležitý případ, tzv. *Fourierovu transformaci* $\mathcal{F}$, která úzce souvisí s Fourierovými řadami.

Připomeňme, že funkce $f(t)$, která je dána svojí konvergující Fourierovou řadou, je rovna

$$f(t) = \sum_{n=-\infty}^{\infty} c_n\, \mathrm{e}^{i\omega_n t},$$

kde $c_n$ jsou komplexní Fourierovy koeficienty, $\omega_n = n2\pi/T$ se základní periodou $T$, viz odstavec 7.7.

Při pevně zvoleném $T$ vyjadřuje výraz $\Delta\omega = 2\pi/T$ právě změnu ve frekvenci způsobenou nárůstem $n$ o jedničku. Je to tedy právě diskrétní krok, se kterým při výpočtu koeficientů Fourierovy

Derivování (podle $\omega$) a poté užití metody per partes (pro $F' = -it\,\mathrm{e}^{-at^2}, G = \mathrm{e}^{-i\omega t}$) dává

$$(\mathcal{F}(f)(\omega))' = \tfrac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} -it\,\mathrm{e}^{-at^2}\,\mathrm{e}^{-i\omega t}\,dt =$$

$$= \tfrac{1}{\sqrt{2\pi}} \left( \lim_{t\to\infty} \tfrac{i}{2a}\,\mathrm{e}^{-at^2-i\omega t} - \lim_{t\to-\infty} \tfrac{i}{2a}\,\mathrm{e}^{-at^2-i\omega t} - \right.$$

$$\left. - \int_{-\infty}^{\infty} \tfrac{i(-i\omega)}{2a}\,\mathrm{e}^{-at^2}\,\mathrm{e}^{-i\omega t}\,dt \right) =$$

$$= \tfrac{1}{\sqrt{2\pi}} \left( \tfrac{i}{2a} \lim_{t\to\infty} \mathrm{e}^{-at^2} - \tfrac{i}{2a} \lim_{t\to-\infty} \mathrm{e}^{-at^2} - \int_{-\infty}^{\infty} \tfrac{\omega}{2a}\,\mathrm{e}^{-at^2}\,\mathrm{e}^{-i\omega t}\,dt \right) =$$

$$= -\tfrac{\omega}{2a} \left( \tfrac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{e}^{-at^2}\,\mathrm{e}^{-i\omega t}\,dt \right) = -\tfrac{\omega}{2a}\,\mathcal{F}(f)(\omega)\,.$$

Hledejme proto funkce $y(\omega) = \mathcal{F}(f)(\omega)$, které vyhovují diferenciální rovnici

$$y' = -\frac{\omega}{2a}\,y. \tag{7.33}$$

Při zápisu $y' = dy/d\omega$ je

$$\tfrac{dy}{d\omega} = -\tfrac{\omega}{2a}\,y, \quad \text{tj.} \quad \tfrac{1}{y}\,dy = -\tfrac{\omega}{2a}\,d\omega,$$

není-li funkce $y$ rovna nule (zjevně $y \equiv 0$ je řešením (‖7.33‖)). Integrováním dostáváme

$$\ln|y| = -\tfrac{\omega^2}{4a} - \ln|C|, \quad \text{tj.} \quad y = \pm\tfrac{1}{C}\,\mathrm{e}^{-\frac{\omega^2}{4a}},$$

přičemž $C \in \mathbb{R}\setminus\{0\}$. Zahrnutím nulového řešení tak můžeme vyjádřit všechna řešení diferenciální rovnice (‖7.33‖) jako funkce

$$y(\omega) = K\,\mathrm{e}^{-\frac{\omega^2}{4a}}, \quad K \in \mathbb{R}.$$

Doplňme určení konstanty $K$, pro niž získáváme právě $\mathcal{F}(f)(\omega)$. Později (v souvislosti s tzv. normálním rozdělením ve statistických metodách) se dozvíme, že

$$\int_{-\infty}^{\infty} \mathrm{e}^{-x^2}\,dx = \sqrt{\pi},$$

z čehož plyne

$$\int_{-\infty}^{\infty} \mathrm{e}^{-at^2}\,dt = \tfrac{1}{\sqrt{a}} \int_{-\infty}^{\infty} \mathrm{e}^{-x^2}\,dx = \tfrac{\sqrt{\pi}}{\sqrt{a}}.$$

Platí proto

$$\mathcal{F}(f)(0) = \tfrac{1}{\sqrt{2\pi}}\,\tfrac{\sqrt{\pi}}{\sqrt{a}} = \tfrac{1}{\sqrt{2a}} \quad \text{a současně} \quad \mathcal{F}(f)(0) = K\,\mathrm{e}^0 = K.$$

Celkem máme

$$\mathcal{F}(f)(\omega) = \tfrac{1}{\sqrt{2a}}\,\mathrm{e}^{-\frac{\omega^2}{4a}}\,. \qquad \square$$

**7.37.** Stanovte funkci $f$, jejíž Fourierovou transformací je funkce

$$\tilde{f}(\omega) = \tfrac{1}{\sqrt{2\pi}}\,\tfrac{\sin\omega}{\omega}, \quad \omega \neq 0.$$

**Řešení.** Inverzní Fourierova transformace dává

$$f(t) = \tfrac{1}{2\pi} \int_{-\infty}^{\infty} \tfrac{\sin\omega}{\omega}\,\mathrm{e}^{i\omega t}\,d\omega =$$

$$= \tfrac{1}{2\pi} \left( \int_{-\infty}^{0} \tfrac{\sin\omega}{\omega}\,\mathrm{e}^{i\omega t}\,d\omega + \int_{0}^{\infty} \tfrac{\sin\omega}{\omega}\,\mathrm{e}^{i\omega t}\,d\omega \right).$$

řady měníme frekvence. Koeficient $1/T$ ve vztahu

$$c_n = \frac{1}{T} \int_{-T/2}^{T/2} f(t)\,\mathrm{e}^{-i\omega_n t}\,dt$$

je pak roven $\Delta\omega/2\pi$, takže můžeme řadu pro $f(t)$ přepsat jako

$$f(t) = \sum_{n=-\infty}^{\infty} \frac{1}{2\pi} \left( \Delta\omega \int_{-T/2}^{T/2} f(x)\,\mathrm{e}^{-i\omega_n x}\,dx\,\mathrm{e}^{i\omega_n t} \right).$$



Představme si nyní hodnoty $\omega_n$ pro všechna $n \in \mathbb{Z}$ jako vybrané reprezentanty pro malé intervaly $[\omega_n, \omega_{n+1}]$ o délce $\Delta\omega$. Pak náš výraz ve vnitřní velké závorce v posledním vztahu pro $f(t)$ ve skutečnosti vyjadřuje sčítance Riemannových součtů pro nevlastní integrál

$$\frac{1}{2\pi} \int_{-\infty}^{\infty} g(\omega)\,\mathrm{e}^{i\omega t}\,d\omega$$

kde $g(\omega)$ je funkce nabývající v bodech $\omega_n$ hodnoty

$$g(\omega_n) = \int_{-T/2}^{T/2} f(x)\,\mathrm{e}^{-i\omega_n x}\,dx.$$

Pracujeme s po částech spojitými funkcemi s kompaktním nosičem, proto je naše funkce $f$ integrovatelná v absolutní hodnotě přes celé $\mathbb{R}$. Limitním přechodem $T \to \infty$ dojde ke zjemňování normy $\Delta\omega$ našich dělících intervalů v Riemannově součtu. Zároveň se dostaneme v posledním výrazu k integrálu

$$g(\omega) = \int_{-\infty}^{\infty} f(x)\,\mathrm{e}^{-i\omega x}\,dx.$$

Předchozí úvahy ukazují, že pro docela velkou množinu Riemannovsky integrovatelných funkcí $f$ na $\mathbb{R}$ umíme zadefinovat dvojici vzájemně inverzních integrálních operátorů:



FOURIEROVA TRANSFORMACE

Pro každou po částech spojitou reálnou nebo kompaktní funkci $f$ na $\mathbb{R}$ s kompaktním nosičem definujeme

$$\mathcal{F}(f)(\omega) = \tilde{f}(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(t)\,\mathrm{e}^{-i\omega t}\,dt.$$

Této funkci $\tilde{f}$ říkáme Fourierova transformace funkce $f$. Předchozí úvahy ukazují, že bude také platit

$$f(t) = \mathcal{F}^{-1}(\tilde{f})(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \tilde{f}(\omega)\,\mathrm{e}^{i\omega t}\,d\omega.$$

Tím říkáme, že k právě definované *Fourierově transformaci* $\mathcal{F}$ existuje inverzní operace $\mathcal{F}^{-1}$, které říkáme *inverzní Fourierova transformace*.

Všimněme si, že Fourierova transformace a její inverze jsou integrální operátory se skoro shodným jádrem

$$k(\omega, t) = \mathrm{e}^{\pm i\omega t}\,.$$

Samozřejmě tyto transformace mají smysl pro mnohem větší definiční obory, zájemce odkazujeme na speciální literaturu.

Jestliže použijeme substituci, kdy nahradíme $-\omega$ za $\omega$ v integrálu přes interval $(-\infty, 0]$, získáme

$$f(t) = \tfrac{1}{2\pi}\left(\int_0^\infty \tfrac{\sin\omega}{\omega}\,\mathrm{e}^{-i\omega t}\,d\omega + \int_0^\infty \tfrac{\sin\omega}{\omega}\,\mathrm{e}^{i\omega t}\,d\omega\right) =$$

$$= \tfrac{1}{2\pi}\int_0^\infty \tfrac{\sin\omega}{\omega}\,[\cos(\omega t) - i\sin(\omega t) + \cos(\omega t) + i\sin(\omega t)]\,d\omega =$$

$$= \tfrac{1}{\pi}\int_0^\infty \tfrac{\sin\omega}{\omega}\,\cos(\omega t)\,d\omega.$$

Poznamenejme, že předchozí vyjádření lze obdržet už z toho, že funkce $y = \frac{\sin\omega}{\omega}$ s maximálním definičním oborem je sudá.

Pomocí identity

$$\sin x\cdot\cos(xy) = \tfrac{1}{2}\left(\sin\left[x(1+y)\right] + \sin\left[x(1-y)\right]\right), \quad x, y\in\mathbb{R},$$

která mj. vyplývá ze součtových vzorců (pro sinus), dostáváme

$$f(t) = \tfrac{1}{2\pi}\left(\int_0^\infty \tfrac{\sin[\omega(1+t)]}{\omega}\,d\omega + \int_0^\infty \tfrac{\sin[\omega(1-t)]}{\omega}\,d\omega\right).$$

Substituce $u = \omega(1+t)$, $v = \omega(1-t)$ potom dávají

$$f(t) = \tfrac{1}{2\pi}\left(\int_0^\infty \tfrac{\sin u}{u}\,du - \int_0^\infty \tfrac{\sin v}{v}\,dv\right) = 0, \quad t > 1;$$

$$f(t) = \tfrac{1}{2\pi}\left(\int_0^\infty \tfrac{\sin u}{u}\,du + \int_0^\infty \tfrac{\sin v}{v}\,dv\right) = \tfrac{1}{\pi}\int_0^\infty \tfrac{\sin u}{u}\,du, \quad t\in(-1,1);$$

$$f(t) = \tfrac{1}{2\pi}\left(-\int_0^\infty \tfrac{\sin u}{u}\,du + \int_0^\infty \tfrac{\sin v}{v}\,dv\right) = 0, \quad t < -1.$$

Dokázali jsme tak, že funkce $f$ je nulová pro $|t| > 1$ a konstantní (nutně nenulová) pro $|t| < 1$. (Po celou dobu předpokládáme, že inverzní Fourierova transformace existuje.)

Určeme funkční hodnotu $f(0)$. Pro funkci

$$g(t) = 1, \quad |t| < 1; \qquad g(t) = 0, \quad |t| > 1$$

platí

$$\mathcal{F}(g)(\omega) = \tfrac{1}{\sqrt{2\pi}}\int_{-1}^{1}\mathrm{e}^{-i\omega t}\,dt = \tfrac{2}{\sqrt{2\pi}}\int_0^1\cos(\omega t)\,dt = \tfrac{2}{\sqrt{2\pi}}\tfrac{\sin\omega}{\omega}.$$

Odtud plyne, že $f(0) = g(0)/2 = 1/2$. Ještě vyzdvihněme vyčíslení integrálu

$$\int_0^\infty \tfrac{\sin u}{u}\,du = \tfrac{\pi}{2},$$

které jsme rovněž obdrželi. □

## E. Laplaceova transformace

**7.38.** Stanovte Laplaceovu transformaci $\mathcal{L}(f)(s)$ funkce

(a) $f(t) = \mathrm{e}^{at}$;
(b) $f(t) = c_1\,\mathrm{e}^{a_1 t} + c_2\,\mathrm{e}^{a_2 t}$;
(c) $f(t) = \cos(bt)$;
(d) $f(t) = \sin(bt)$;
(e) $f(t) = \cosh(bt)$;
(f) $f(t) = \sinh(bt)$,

**7.31. Jednoduché vlastnosti.** Fourierova transformace zajímavým způsobem převrací lokální a globální chování funkcí. Začněme jednoduchým příkladem, ve kterém najdeme funkci $f(t)$, která se transformuje na charakteristickou funkci intervalu $[-\Omega, \Omega]$, tj. $\tilde f(\omega) = 0$ pro $|\omega| > \Omega$ a $\tilde f = 1$ pro $|\omega| \le \Omega$. Inverzní transformace $\mathcal{F}^{-1}$ nám dává

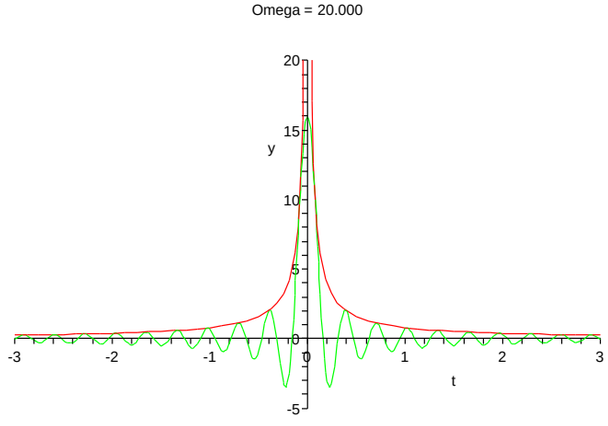
$$f(t) = \frac{1}{\sqrt{2\pi}}\int_{-\Omega}^{\Omega}\mathrm{e}^{i\omega t}\,d\omega = \frac{1}{\sqrt{2\pi}}\left[\frac{1}{it}\,\mathrm{e}^{i\omega t}\right]_{-\Omega}^{\Omega} =$$

$$= \frac{2}{\sqrt{2\pi}\,t}\,\frac{1}{2i}(\mathrm{e}^{i\Omega t} - \mathrm{e}^{-i\Omega t}) =$$

$$= \frac{2\Omega}{\sqrt{2\pi}}\,\frac{\sin(\Omega t)}{\Omega t}.$$

Až na konstantní násobek a škálování proměnné, jde tedy o velice důležitou funkci $\mathrm{sinc}(x) = \frac{\sin x}{x}$.

Přímým výpočtem limity v nule (L'Hospitalovo pravidlo) spočteme, že $f(0) = 2\Omega(2\pi)^{-1/2}$, nejbližší nulové body jsou v $t = \pm\pi/\Omega$ a funkce poměrně rychle klesá k nule mimo počátek $x = 0$. Na obrázku je tato funkce znázorněná rozvlněnou křivkou pro $\Omega = 20$. Zároveň je vynesena křivkou oblast, ve které se s rostoucím $\Omega$ naše funkce $f(t)$ stále vlní.




Vidíme, že charakteristická funkce intervalu $[-\Omega, \Omega]$ přechází Fourierovou transformací na funkci $f$, která má velmi výraznou kladnou hodnotu v malém okolí nuly, přičemž hodnota v nule je pevným násobkem $\Omega$. Čím je tedy $\Omega$ větší, tím více se soustředí $f$ do okolí počátku.

Dále si spočteme Fourierovu transformaci derivace $f'(t)$ pro nějakou funkci $f$. Stále předpokládáme, že $f$ má kompaktní nosič, tj, zejména $\mathcal{F}(f')$ i $\mathcal{F}(f)$ skutečně existují. Počítejme metodou per partes:

$$\mathcal{F}(f')(\omega) = \frac{1}{\sqrt{2\pi}}\int_{\infty}^{\infty} f'(t)\,\mathrm{e}^{-i\omega t}\,dt =$$

$$= \frac{1}{\sqrt{2\pi}}\left[\mathrm{e}^{-i\omega t}\,f(t)\right]_{-\infty}^{\infty} + \frac{i\omega}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(t)\,\mathrm{e}^{-i\omega t}\,dt =$$

$$= i\omega\mathcal{F}(f)(\omega).$$

Vidíme tedy, že Fourierova transformace převádí (limitní) operaci derivování na (algebraickou) operaci prostého násobení proměnnou. Samozřejmě můžeme tento vzorec iterovat a dostáváme

$$\mathcal{F}(f'')(\omega) = -\omega^2\mathcal{F}(f), \ldots, \mathcal{F}(f^{(n)}) = i^n\,\omega^n\,\mathcal{F}(f).$$

přičemž hodnoty $b \in \mathbb{R}$ a $c_1, c_2 \in \mathbb{C}$ jsou libovolné a kladné $s \in \mathbb{R}$ je větší než reálné části čísel $a, a_1, a_2 \in \mathbb{C}$ a rovněž je větší než $b$ ve variantách (e) a (f).

**Řešení.** Případ (a). Bezprostředně z definice Laplaceovy transformace plyne

$$\mathcal{L}(f)(s) = \int_0^\infty \mathrm{e}^{at}\,\mathrm{e}^{-st}\,dt = \int_0^\infty \mathrm{e}^{-(s-a)t}\,dt = \\ = \lim_{t\to\infty}\left(\tfrac{\mathrm{e}^{-(s-a)t}}{-(s-a)}\right) - \tfrac{\mathrm{e}^0}{-(s-a)} = \tfrac{1}{s-a}.$$

Případ (b). Pomocí výsledku varianty (a) a linearity nevlastního integrálu dostáváme

$$\mathcal{L}(f)(s) = c_1 \int_0^\infty \mathrm{e}^{a_1 t}\,\mathrm{e}^{-st}\,dt + c_2 \int_0^\infty \mathrm{e}^{a_2 t}\,\mathrm{e}^{-st}\,dt = \tfrac{c_1}{s-a_1} + \tfrac{c_2}{s-a_2}.$$

Případ (c). Protože

$$\cos(bt) = \tfrac{1}{2}\left(\mathrm{e}^{ibt} + \mathrm{e}^{-ibt}\right),$$

volba $c_1 = 1/2 = c_2, a_1 = ib, a_2 = -ib$ v předchozí variantě již dává

$$\mathcal{L}(f)(s) = \int_0^\infty \left(\tfrac{1}{2}\mathrm{e}^{ibt} + \tfrac{1}{2}\mathrm{e}^{-ibt}\right)\mathrm{e}^{-st}\,dt = \tfrac{1}{2(s-ib)} + \tfrac{1}{2(s+ib)} = \tfrac{s}{s^2+b^2}.$$

Případy (d), (e), (f). Analogicky volby

(d) $c_1 = -i/2, c_2 = i/2, a_1 = ib, a_2 = -ib$;

(e) $c_1 = 1/2 = c_2, a_1 = b, a_2 = -b$;

(f) $c_1 = 1/2, c_2 = -1/2, a_1 = b, a_2 = -b$

vedou na

(d) $\mathcal{L}(f)(s) = \frac{b}{s^2+b^2}$;

(e) $\mathcal{L}(f)(s) = \frac{s}{s^2-b^2}$;

(f) $\mathcal{L}(f)(s) = \frac{b}{s^2-b^2}$.

□

**7.39.** Pomocí vztahu

$$\mathcal{L}\left(f'\right)(s) = s\,\mathcal{L}(f)(s) - \lim_{t\to 0+} f(t) \tag{7.34}$$

odvoďte Laplaceovy transformace funkcí $y = \cos t$ a $y = \sin t$.

**Řešení.** Nejprve si uvědomme, že z (‖7.34‖) plyne

$$\mathcal{L}\left(f''\right)(s) = s\,\mathcal{L}\left(f'\right)(s) - \lim_{t\to 0+} f'(t) = \\ = s\left(s\mathcal{L}(f)(s) - \lim_{t\to 0+} f(t)\right) - \lim_{t\to 0+} f'(t) = \\ = s^2\,\mathcal{L}(f)(s) - s\lim_{t\to 0+} f(t) - \lim_{t\to 0+} f'(t).$$

Platí tedy

$$-\mathcal{L}(\sin t)(s) = \mathcal{L}(-\sin t)(s) = \mathcal{L}\left((\sin t)''\right)(s) = \\ = s^2\,\mathcal{L}(\sin t)(s) - s\lim_{t\to 0+}\sin t - \lim_{t\to 0+}\cos t = s^2\,\mathcal{L}(\sin t)(s) - 1,$$

odkud dostáváme

$$-\mathcal{L}(\sin t)(s) = s^2\,\mathcal{L}(\sin t)(s) - 1, \quad \text{tj.} \quad \mathcal{L}(\sin t)(s) = \tfrac{1}{s^2+1}.$$

**7.32. Vztah ke konvolucím.** Další mimořádně důležitou vlastností je vztah mezi konvolucemi a Fourierovou transformací. Spočtěme, jak dopadne transformace konvoluce $h = f * g$, kde opět pro jednoduchost předpokládáme, že funkce mají kompaktní nosiče. Při výpočtu prohodíme pořadí integrování, což je krok, který ověříme teprve v diferenciálním a integrálním počtu později, viz 8.28. V dalším krůčku pak zavedeme substituci $t - x = u$.

$$\mathcal{F}(h)(\omega) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty\left(\int_{-\infty}^\infty f(x)g(t-x)\,dx\right)\mathrm{e}^{-i\omega t}\,dt = \\ = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty f(x)\left(\int_{-\infty}^\infty g(t-x)\,\mathrm{e}^{-i\omega t}\,dt\right)dx = \\ = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty f(x)\left(\int_{-\infty}^\infty g(u)\,\mathrm{e}^{-i\omega(u+x)}\,du\right)dx = \\ = \frac{1}{\sqrt{2\pi}}\left(\int_{-\infty}^\infty f(x)\,\mathrm{e}^{-i\omega x}\,dx\right)\cdot\left(\int_{-\infty}^\infty g(u)\,\mathrm{e}^{-i\omega u}\,du\right) = \\ = \sqrt{2\pi}\,\mathcal{F}(f)\cdot\mathcal{F}(g)$$

Podobný výpočet ukazuje i obrácené tvrzení, že Fourierova transformace součinu je, až na konstantu, konvoluce transformací.

$$\mathcal{F}(f\cdot g) = \frac{1}{\sqrt{2\pi}}\mathcal{F}(f) * \mathcal{F}(g).$$

Jak jsme si uváděli výše, konvoluce $f*g$ velice často modeluje proces našeho pozorování nějaké sledované veličiny $f$. Pomocí Fourierovy transformace a její inverze nyní můžeme snadno rozpoznat původní hodnoty této veličiny, pokud známe konvoluční jádro $g$. Prostě spočteme $\mathcal{F}(f*g)$ a podělíme obrazem $\mathcal{F}(g)$. Tak získáme Fourierovu transformaci původní funkce $f$, kterou obdržíme explicitně pomocí inverzní Fourierovy transformace. Hovoříme o *dekonvoluci*.

**7.33. Diracova delta–funkce.** Vraťme se nyní ještě k prvnímu příkladu s inverzní transformací k charakteristické funkci $f_\Omega$ intervalu $[-\Omega, \Omega]$. Zkusme provést limitní přechod pro $\Omega$ jdoucí k nekonečnu a označme $\sqrt{2\pi}\delta(t)$ kýženou limitní „funkci“ pro $\mathcal{F}^{-1}(f_\Omega)(t)$. Inverzní obraz součinu s libovolným obrazem $\mathcal{F}(g)$ umíme vyjádřit pomocí konvoluce:

$$\mathcal{F}^{-1}(f_\Omega\cdot\mathcal{F}(g))(z) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty g(t)\mathcal{F}^{-1}(f_\Omega)(z-t)\,dt.$$

Při limitním přechodu $\Omega\to\infty$ přejde výraz nalevo k hodnotě $\mathcal{F}^{-1}(\mathcal{F}(g))(z) = g(z)$, zatímco napravo dostáváme

$$g(z) = \int_{-\infty}^\infty g(t)\delta(z-t)\,dt.$$

Naše hledaná $\delta(t)$ tedy vypadá na „funkci“, která je všude nulová, kromě jediného bodu $t = 0$, kde je tak „nekonečná“, že integrováním jejího součinu s libovolnou integrovatelnou funkcí $g$ dostaneme právě hodnotu $g$ v bodě $t = 0$. Není to samozřejmě funkce v našem smyslu, nicméně jde o objekt často používaný. Říká se jí *Diracova funkce* $\delta$ a korektně ji lze popsat jako tzv. distribuci.

Z nedostatku času nebudeme distribuce podrobněji rozebírat a omezíme se na konstatování, že si lze dobře Diracovo $\delta$ představit jako jednotkový impulz v jediném bodě. Fourierova transformace jej pak přetransformuje na konstantní funkci $\mathcal{F}(\delta)(\omega) = \frac{1}{\sqrt{2\pi}}$.

Nyní užitím vzorce (‖7.34‖) snadno určíme
$\mathcal{L}(\cos t)(s) = \mathcal{L}\left((\sin t)'\right)(s) = s\,\frac{1}{s^2+1} - \lim_{t\to 0+} \sin t = \frac{s}{s^2+1}$. □

**7.40.** Pro $s > -1$ spočtěte Laplaceovu transformaci $\mathcal{L}(g)(s)$ funkce

$$g(t) = t\,\mathrm{e}^{-t}$$

a pro $s > 1$ Laplaceovu transformaci $\mathcal{L}(h)(s)$ funkce

$$h(t) = t \sinh t.$$

**Řešení.** Užitím metody per partes získáváme

$$\mathcal{L}(g)(s) = \int_0^\infty t\,\mathrm{e}^{-t}\,\mathrm{e}^{-st}\,dt = \int_0^\infty t\,\mathrm{e}^{-(s+1)t}\,dt = \lim_{t\to\infty}\left(\frac{t\,\mathrm{e}^{-(s+1)t}}{-(s+1)}\right) - 0 -$$
$$- \int_0^\infty \frac{\mathrm{e}^{-(s+1)t}}{-(s+1)}\,dt = -\left(\lim_{t\to\infty}\frac{\mathrm{e}^{-(s+1)t}}{(s+1)^2} - \frac{\mathrm{e}^0}{(s+1)^2}\right) = \frac{1}{(s+1)^2}.$$

Derivování Laplaceovy transformace obecné funkce $-f$ (tj. nevlastního integrálu) podle parametru $s$ dává

$$\left(\int_0^\infty -f(t)\,\mathrm{e}^{-st}\,dt\right)' = \int_0^\infty -f(t)\,\left(\mathrm{e}^{-st}\right)'\,dt = \int_0^\infty t\,f(t)\,\mathrm{e}^{-st}\,dt.$$

To znamená, že derivace Laplaceovy transformace $\mathcal{L}(-f)(s)$ je Laplaceova transformace funkce $tf(t)$. Laplaceovu transformaci funkce $y = \sinh t$ jsme ale dříve určili jako funkci $y = \frac{1}{s^2-1}$. Proto platí

$$\mathcal{L}(h)(s) = \left(-\frac{1}{s^2-1}\right)' = \frac{2s}{(s^2-1)^2}.$$

Povšimněme si, že tímto způsobem jsme rovněž mohli určit $\mathcal{L}(g)(s)$. □

Základní Laplaceovy transformace uvádíme v následující tabulce:

| $y(t)$ | $\mathcal{L}(y)(s)$ |
|---|---|
| $e^{at}$ | $\frac{1}{s-a}$ |
| $te^{at}$ | $\frac{1}{(s-a)^2}$ |
| $t^n e^{at}$ | $\frac{n!}{(s-a)^{n+1}}$ |
| $\sin \omega t$ | $\frac{\omega}{s^2+\omega^2}$ |
| $\cos \omega t$ | $\frac{s}{s^2+\omega^2}$ |
| $e^{at}\sin \omega t$ | $\frac{\omega}{(s-a)^2+\omega^2}$ |
| $e^{at}(\cos \omega t + \frac{a}{\omega}\sin \omega t)$ | $\frac{s}{(s-a)^2+\omega^2}$ |
| $t \sin \omega t$ | $\frac{2\omega s}{(s^2+\omega^2)^2}$ |
| $\sin \omega t - \omega t \cos \omega t$ | $\frac{2\omega^3}{(s^2+\omega^2)^2}$ |

**7.41.** Dokažte 4. a 5. řádek tabulky pomocí Eulerova vztahu $e^{i\omega t} = \cos \omega t + i \sin \omega t$.

**Řešení.** $\mathcal{L}(\cos \omega t)(s) + i\mathcal{L}(\sin \omega t)(s) = \mathcal{L}(e^{i\omega t})(s) =$
$= \int_0^\infty e^{i\omega t} e^{-st}\,\mathrm{d}t = \int_0^\infty e^{(i\omega - s)t}\,\mathrm{d}t =$
$= -\frac{1}{s-i\omega}\left[e^{(i\omega-s)t}\right]_0^\infty =$
$= -\frac{1}{s-i\omega}(\lim_{t\to\infty}\frac{e^{i\omega t}}{e^{st}} - 1) = \frac{1}{s-i\omega} = \frac{s+i\omega}{(s-i\omega)(s+i\omega)} =$
$= \frac{s}{s^2+\omega^2} + i\,\frac{\omega}{s^2+\omega^2}$. □

Naopak mnohé funkce, které nejsou integrovatelné v absolutní hodnotě na $\mathbb{R}$ transformuje Fourierova transformace na výrazy s Diracovým $\delta$. Např.

$$\mathcal{F}(\cos(nt))(\omega) = \sqrt{\frac{\pi}{2}}(\delta(n-\omega) + \delta(n+\omega)),$$

což můžeme docela snadno vidět výpočtem Fourierovy transformace funkce $f_\Omega \cos(nx)$ a následným limitním přechodem $\Omega \to \infty$.

Obdobně dostaneme Fourierovu transformaci pro funkci sinus, můžeme pro to využít také skutečnost, že transformace derivace této funkce se bude lišit jen o násobek imaginární jednotkou a proměnnou.

Tyto transformace jsou základem Fourierovy analýzy signálů. Jestliže totiž signál je čistou sinusoidou na dané frekvenci, pak to pomocí Fourierovy transformace identifikujeme jako dva bodové impulzy právě v kladné a záporné hodnotě frekvence. Pokud je signál lineární kombinací několika takových čistých signálů, dostaneme stejnou lineární kombinaci bodových impulzů. Protože ale vždycky zpracováváme signál jen v nějakém konečném časovém intervalu, dostáváme ve skutečnosti místo bodových impulzů rozvlněnou křivku podobnou funkci sinc s výrazným maximem právě v hodnotě příslušné frekvence. Z velikosti tohoto maxima přitom umíme také přímo vyčíst původní amplitudu signálu.

**7.34. Fourierova sinová a cosinová transformace.** Pokud použijeme Fourierovu transformaci na lichou funkci $f(t)$, tj. $f(-t) = -f(t)$, příspěvek integrace součinu $f(t)$ a funkce $\cos(\pm\omega t)$ se pro kladná a záporná $t$ vyruší. Dostaneme proto přímým výpočtem

$$\mathcal{F}(f)(\omega) = \frac{-2i}{\sqrt{2\pi}}\int_0^\infty f(t)\sin \omega t\,dt.$$

Výsledná funkce je opět lichá, proto ze stejného důvodu i inverzní transformaci lze spočíst obdobně:

$$\tilde{\mathcal{F}}(f)(\omega) = \frac{2i}{\sqrt{2\pi}}\int_0^\infty f(t)\sin \omega t\,dt.$$

Vynecháním imaginární jednotky $i$ dostáváme vzájemně inverzní transformace, kterým se říká *Fourierova sinusová transformace* pro liché funkce:

$$\tilde{f}_s(\omega) = \sqrt{\frac{2}{\pi}}\int_0^\infty f(t)\sin(\omega t)\,dt,$$
$$f(t) = \sqrt{\frac{2}{\pi}}\int_0^\infty \tilde{f}_s(t)\sin(\omega t)\,dt.$$

Obdobně se definuje *Fourierova kosinusová transformace* pro sudé funkce:

$$\tilde{f}_c(\omega) = \sqrt{\frac{2}{\pi}}\int_0^\infty f(t)\cos(\omega t)\,dt,$$
$$f(t) = \sqrt{\frac{2}{\pi}}\int_0^\infty \tilde{f}_s(t)\sin \omega t\,dt.$$

**7.35. Laplaceova transformace.** Fourierovu transformaci nelze dobře využít pro funkce, které nejsou integrovatelné v absolutní hodnotě přes celé $\mathbb{R}$ (minimálně nedostáváme opravdové funkce).

**7.42.** Nalezněte Laplaceovu transformaci Heavisideovy funkce $H(t)$ a posunuté Heavisideovy funkce $H_a(t) = H(t-a)$:

$$H(t) = \begin{cases} 0 & \text{pro } t < 0, \\ \frac{1}{2} & \text{pro } t = 0, \\ 1 & \text{pro } t > 0. \end{cases}$$

**Řešení.**

$$\begin{aligned} \mathcal{L}(H(t))(s) &= \int_0^\infty H(t)e^{-st}\,\mathrm{d}t = \int_0^\infty e^{-st}\,\mathrm{d}t = \\ &= \left[-\frac{e^{-st}}{s}\right]_0^\infty = -\tfrac{1}{s}(0-1) = \tfrac{1}{s}, \\ \mathcal{L}(H_a(t))(s) &= \mathcal{L}(H(t-a))(s) = \int_0^\infty H(t-a)e^{-st}\,\mathrm{d}t = \\ &= \int_a^\infty e^{-st}\,\mathrm{d}t = \int_0^\infty e^{-s(t+a)}\,\mathrm{d}t = \\ &= e^{-as}\mathcal{L}(H(t))(s) = \frac{e^{-as}}{s}. \end{aligned}$$

□

**7.43.** Ukažte, že platí

$$\mathcal{L}(f(t)\cdot H_a(t))(s) = e^{-as}\mathcal{L}(f(t+a))(s) \tag{7.35}$$

**Řešení.**

$$\begin{aligned} \mathcal{L}(f(t)\cdot H_a(t))(s) &= \textstyle\int_0^\infty f(t)H(t-a)e^{-st}\,\mathrm{d}t = \int_a^\infty f(t)e^{-st}\,\mathrm{d}t = \\ &= \textstyle\int_0^\infty f(t+a)e^{-s(t+a)}\,\mathrm{d}t = \\ &= e^{-as}\textstyle\int_0^\infty f(t+a)e^{-st}\,\mathrm{d}t = \\ &= e^{-as}\mathcal{L}(f(t+a))(s)\,. \end{aligned}$$

□

Laplaceovy transformace lze také užít pro řešení diferenciálních rovnic a jejich systémů. Více naleznete v další kapitole od strany 505.

**7.44. Diskrétní kosinová transformace.** Základem JPEG komprese dat je tzv. diskrétní kosinová transformace. Ta je dána ortogonální maticí $C = (c_{kl})_{k,l=1}^n$ definovanou následovně

$$c_{kl} = \alpha_{kl}\cos\left(\frac{(2k-1)(l-1)\pi}{2n}\right)$$

kde $\alpha_{k1} = \frac{1}{\sqrt{n}}$ $\alpha_{kl} = \sqrt{\frac{2}{n}}$ pro $l > 1$. Vektor reprezentující data pak ortogonálně rozložíme a některé bázové vektory (sloupce matice $C$) vypustíme. Tím je provedena redukce dat s rozumnou aproximací původních dat. Zpětná transformace je jednoduchá. Protože je $C$ ortogonální, je dána násobením transponovanou maticí.

Ukažte, že pro $n = 2$ je matice $C$ rovna $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ a že je ortogonální. Spočítejte ortogonální rozklad vektoru $(3,4)$ vzhledem k bázi tvořené sloupci matice a určete vlastní čísla a vlastní vektory.

*Laplaceova transformace* se chová docela podobně jako Fourierova a tuto vadu nemá:

$$\mathcal{L}(f)(s) = \bar{f}(s) = \int_0^\infty f(t)\,\mathrm{e}^{-st}\,dt.$$

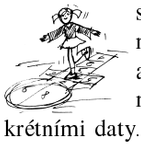
Integrální operátor $\mathcal{L}$ má velice rychle se zmenšující jádro, pokud je $s$ kladné reálné číslo. Obvykle proto Laplaceovu transformaci chápeme jako zobrazení vhodných funkcí na intervalu $[0,\infty)$ do funkcí na témž nebo menším intervalu. Obraz $\mathcal{L}(p)$ bude existovat například pro každý polynom $p(t)$ a všechna kladná $s$.

Obdobně jako pro Fourierovu transformaci dostaneme prostým výpočtem per partes vztah pro Laplaceovu transformaci derivované funkce při $s > 0$:

$$\begin{aligned} \mathcal{L}(f'(t))(s) &= \int_0^\infty f'(t)\,\mathrm{e}^{-st}\,dt = \\ &= [f(t)\,\mathrm{e}^{-st}]_0^\infty + s\int_0^\infty f(t)\,\mathrm{e}^{-st}\,dt = \\ &= -f(0) + s\mathcal{L}(f)(s). \end{aligned}$$

Vlastnosti Laplaceovy transformace a řadu dalších zejména v technické praxi používaných transformací je možné snadno dohledat v literatuře.

**7.36. Diskrétní Fourierovy transformace.** Fourierova analýza signálů naznačená v předchozím odstavci byla dříve např. v radiotechnice realizována pomocí speciálních analogových obvodů. Dnes při zpracování signálů pomocí počítačových obvodů pracujeme pouze s diskrétními daty. Předpokládáme, že v (diskrétní) časové proměnné je dán nějaký pevný (malinký) *vzorkovací interval* $\tau$ a že se naše vzorkovací signály opakují s periodou $N\tau$ (pro hodně veliké přirozené $N$), což je maximální perioda zachytitelná v našem diskrétním modelu).



Jistě nás nepřekvapí, že diskrétní aproximací našich spojitých metod dostaneme velmi podobně účinné nástroje.

Budeme pracovat s $N$–rozměrným vektorem, který si můžeme představit jako funkci $r \mapsto f(r) \in \mathbb{C}$ pro $r = 0, 1, \ldots, N-1$. Označme si $\Delta\omega = \frac{2\pi}{N}$ a $\omega_k = k\Delta\omega$. Diskrétní přiblížení integrálu z definice Fourierovy transformace napovídá, že definice

$$\tilde{f}(k) = \frac{1}{N}\sum_{r=0}^{N-1} f(r)\,\mathrm{e}^{-i\frac{2\pi}{N}kr}$$

povede na transformaci $f \mapsto \tilde{f}$, pro kterou bychom mohli zkusit napsat něco blízkého inverzní transformaci pomocí vztahu

$$\hat{f}(k) = \sum_{r=0}^{N-1} f(r)\,\mathrm{e}^{i\frac{2\pi}{N}kr}\,.$$

Ve skutečnosti dostáváme skutečně dvě vzájemně inverzní transformace:

**Věta.** *Pro výše definované transformace platí* $\hat{\tilde{f}}(k) = f(k)$ *pro všechna* $k = 0, 1, \ldots, N-1$.

Důkaz. Důkaz je založen na jednoduchém lemmatu, které přesně vyjadřuje naši (již ve spojitém případě používanou) intuici, že sčítání hodnot $\mathrm{e}^{ir\omega_k}$ se vzájemně úplně vyruší, pokud není

**Řešení.** Počítejme

$$CC^T = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix} = 1.$$

Matice $C$ je tedy ortogonální a její sloupce tvoří ortonormální bázi $e_1 = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$, $e_2 = (\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$. Koeficienty ortogonálního rozkladu vektoru $u = (3, 4)$ dostaneme jednoduše použitím transponované matice

$$C^T u = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}3\\ 4\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}7\\ -1\end{pmatrix}$$

Ortogonální rozklad má tedy následující tvar

$$\begin{pmatrix}3\\ 4\end{pmatrix} = \frac{7}{\sqrt{2}}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} - \frac{1}{\sqrt{2}}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}$$

Charakteristický polynom matice $C$ je $(\lambda+\frac{1}{\sqrt{2}})(\lambda-\frac{1}{\sqrt{2}})-\frac{1}{2} = 0$ a vlastní čísla jsou tedy $\lambda_{1,2} = \pm 1$ (jiná ani ortogonální matice nemůže mít). Příslušné vlastní vektory jsou určeny po řadě rovnicemi

$$(\tfrac{1}{\sqrt{2}} - 1)x + \tfrac{1}{\sqrt{2}}y = 0, \quad (\tfrac{1}{\sqrt{2}} + 1)x + \tfrac{1}{\sqrt{2}}y = 0$$

a jsou to tedy například vektory $(\frac{1}{\sqrt{2}}, 1 - \frac{1}{\sqrt{2}})$, $(\frac{1}{\sqrt{2}}, -1 - \frac{1}{\sqrt{2}})$ (které jsou automaticky ortogonální). □

**Poznámka.** Zkuste si nakreslit obrázek působení zobrazení určeného maticí $A$ na nějaký vektor v rovině.

$k$ násobkem čísla $N$. Naopak, v případě, že $k$ je násobek čísla $N$, dostáváme hodnotu $N$:

$$\sum_{r=0}^{N-1} \mathrm{e}^{ir\frac{2\pi}{N}k} = \begin{cases} N & \text{je-li } k \text{ je násobek } N\\ 0 & \text{jinak.}\end{cases}$$



Doporučujeme provést si podrobný důkaz na základě náčrtku (všimněme si, že pro obecné $N$ a dané $k$ se všechny sčítance rozpadnou do „cyklů“ na jednotkové kružnici a je třeba odlišně diskutovat cykly o sudé a liché délce; v obou případech ale tyto cykly dají nulové součty, pokud nejde o triviální jednoprvkový cyklus $\mathrm{e}^0 = 1$).

Nyní můžeme velmi snadno přímo spočíst:

$$\begin{aligned}\hat{\tilde{f}}(k) &= \sum_{r=0}^{N-1}\frac{1}{N}\Big(\sum_{s=0}^{N-1} f(s)\,\mathrm{e}^{-i\frac{2\pi}{N}rs}\Big)\mathrm{e}^{i\frac{2\pi}{N}rk} =\\ &= \frac{1}{N}\sum_{r=0}^{N-1}\sum_{s=0}^{N-1} f(s)\,\mathrm{e}^{-i\frac{2\pi}{N}r(k-s)} =\\ &= \frac{1}{N}\sum_{r=0}^{N-1}\sum_{s=0}^{N-1} f(s)\delta_{ks}N = f(k),\end{aligned}$$

kde $\delta_{ks}$ je nula pro $k \neq s$ a 1 pro $k = s$ (je nutné si všimnout, že mezi všemi možnostmi hodnot $(k - s)$ jediná nula je násobkem $N$). □

Výpočet použitý v důkazu zároveň ukazuje, že při diskrétní Fourierově transformaci komplexního periodického signálu s jednou ze vzorkovacích period dostaneme jako diskrétní Fourierův obraz právě jeho amplitudu. Pokud tedy vznikne signál superpozicí vzorkovacích frekvencí, dostáváme dokonalý výsledek. Pokud bude ale frekvence mimo použité vzorky, dostaneme nenulové amplitudy u všech vzorkovacích frekvencí. V technické literatuře se tomuto jevu říká „prosakování frekvencí“.

Vlastnostem, využitím a rychlé implementaci diskrétní Fourierovy transformace a dalších obdobných diskrétních nástrojů se věnuje obrovské množství literatury a jde o aktivní oblast současného výzkumu. Nemáme tu prostor pro podrobnější diskusi.

### F. Doplňující příklady k celé kapitole

*7.45.* Rozviňte do Furierovy řady funkci $\sin^2(x)$ na intervalu $[-\pi, \pi]$. ○

*7.46.* Rozviňte do Furierovy řady funkci $\cos^2(x)$ na intervalu $[-\pi, \pi]$. ○

*7.47.* Určete konvoluci funkcí $f_1$ a $f_2$, kde

$$f_1 = \begin{cases} 1 & \text{pro } x \in [-1, 0] \\ 0 & \text{jinak} \end{cases}$$

$$f_2 = \begin{cases} x & \text{pro } x \in [0, 1] \\ 0 & \text{jinak} \end{cases}$$

○

*7.48.* Určete konvoluci funkce

$$f_1 = \begin{cases} 1 & \text{pro } x \in \langle 0, 1 \rangle \\ 0 & \text{jinak} \end{cases}$$

se sebou. ○

### Řešení cvičení

*7.3.* $x, -\frac{3}{\pi^2}x + \sin(x)$, projekce funkci $\frac{1}{2}\sin(x)$ nezmění, neboť leží v prostoru samotném.

*7.4.* $\cos(x), \frac{4}{\pi}\cos(x) + x$. Projekce funkci $\frac{1}{3}\cos(x)$ nezmění, neboť leží v prostoru samotném.

*7.33.*

$$f_1 * f_2(t) = \begin{cases} t - \frac{t^2}{2} + 4 & \text{pro } t \in [-2,-1] \\ 1 - t + \frac{1}{2} & \text{pro } t \in [-1,1] \\ \frac{t^2}{2} - 2t + 2 & \text{pro } t \in [1,2] \\ 0 & \text{jinak} \end{cases}$$

*7.45.* $\frac{1}{2} - \frac{1}{2}\cos(2x)$.

*7.46.* $\frac{1}{2} + \frac{1}{2}\cos(2x)$.

*7.47.*

$$f_1 * f_2(t) = \begin{cases} \frac{(t+1)^2}{2} & \text{pro } t \in [-1,0] \\ \frac{1-t^2}{2} & \text{pro } t \in [0,1] \\ 0 & \text{jinak} \end{cases}$$

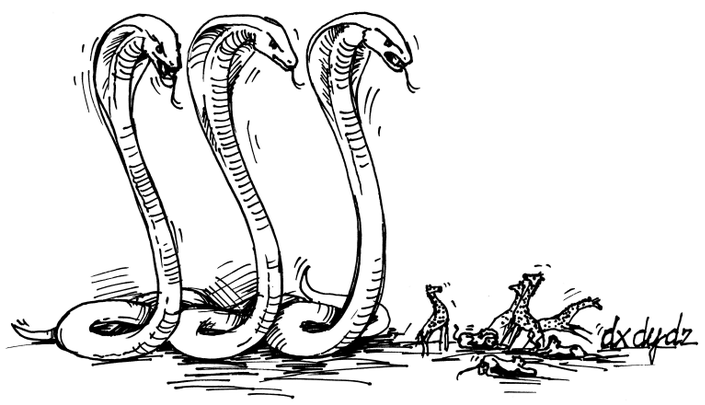
*7.48.*

$$f_1 * f_1 = \begin{cases} x & \text{pro } x \in \langle 0,1\rangle \\ 2 - x & \text{pro } x \in \langle 1,2\rangle \\ 0 & \text{jinak} \end{cases}$$

KAPITOLA 8

# Spojité modely s více proměnnými

*jedna proměnná nám k modelování nestačí?*
*– nevadí, stačí vzpomenout na vektory!*




## A. Funkce více proměnných

**8.1.** Určete definiční obor funkcí $\mathbb{R}^2 \to \mathbb{R}$, které jsou zadány následujícími předpisy:

a)
$$\frac{xy}{y(x^3+x^2+x+1)},$$

b)
$$\ln(x^2-y^2),$$

c)
$$\ln(-x^2-y^2),$$

d)
$$\arcsin(2\,\mathrm{sgn}(\chi_{\mathbb{Q}}(x)),$$

kde $\chi_{\mathbb{Q}}$ značí charakteristickou funkci racionálních čísel,

e)
$$f(x,y,z)=\sqrt{\ln x\cdot\arcsin(y^2z)}.$$

**Řešení.** a) Jedinou podmínkou proto, aby byl předpis korektně zadával nějakou hodnotu, je, aby jmenovatel uvedeného zlomku byl nenulový.

Na samotném počátku našeho putování matematickou krajinou jsme hned viděli, že pracovat současně s více parametry nebylo obtížné, protože s vektory šlo počítat velice podobně jako se skaláry. Jen je třeba si věci dobře rozmyslet. Budeme se nyní znovu zabývat situacemi, kdy matematicky vyjádřené vztahy závisí na více (ale zatím konečně mnoha) parametrech. Uvidíme, že vlastně ani není třeba překvapivých nových nápadů, stačí vždy šikovně redukovat problémy na takové, které už řešit umíme.

Zároveň se konečně budeme umět vrátit k diskusi situací, kdy hodnoty funkcí popisujeme pomocí jejich okamžitých změn – tj. malinko se zastavíme i u obyčejných a parciálních diferenciálních rovnic. Úplně závěrem zmíníme tzv. variační problémy.

Průběžně se budeme také jako obvykle snažit komentovat diskrétní varianty přístupů či problémů.

## 1. Funkce a zobrazení na $\mathbb{R}^n$



**8.1. Funkce více proměnných.** Pro praktické modelování procesů (nebo objektů v grafice) jen velice zřídka vystačíme s funkcemi $\mathbb{R} \to \mathbb{R}$ jedné proměnné. Přinejmenším bývají potřebné funkce závislé na parametrech a často právě změna výsledků v závislosti na parametrech bývá důležitější než výsledek samotný. Budeme proto uvažovat funkce $f : \mathbb{R}^n \to \mathbb{R}$, které budeme také psát ve tvaru zdůrazňujícím označení proměnných,

$$f(x_1, x_2, \ldots, x_n) : \mathbb{R}^n \to \mathbb{R}$$

a budeme se snažit co nejlépe rozšířit naše metody pro sledování hodnot a jejich změn do této situace. Říkáme jim *funkce více proměnných.*

Pro snazší pochopení pojmů budeme často pracovat s případy $n = 2$ nebo $n = 3$ a přitom budeme místo číslovaných proměnných používat písmena $x, y, z$. To znamená, že funkce $f$ definované v „rovině“ $\mathbb{R}^2$ budou značeny

$$f : \mathbb{R}^2 \ni (x, y) \mapsto f(x, y) \in \mathbb{R}$$

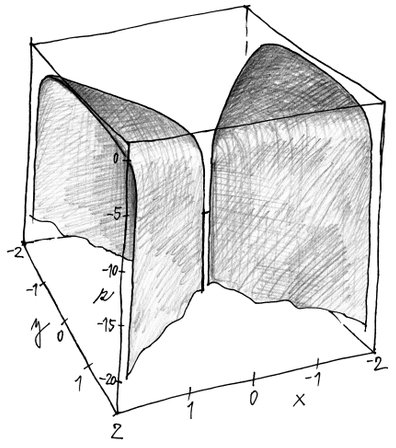
a podobně v „prostoru“ $\mathbb{R}^3$

$$f : \mathbb{R}^3 \ni (x, y, z) \mapsto f(x, y, z) \in \mathbb{R}.$$

Podobně jako u funkcí jedné proměnné hovoříme o definičním oboru $A \subset \mathbb{R}^n$, na kterém je příslušná funkce definována. Při zkoumání funkce zadané konkrétním výrazem bývá prvním úkolem zjistit co největší definiční obor, na kterém má tento výraz smysl.

Předpis tak definuje funkci na množině $\mathbb{R}^2 \setminus \{(x, 0), (-1, y), x, y \in \mathbb{R}\}$.

b) Předpis je korektní, pokud je argument logaritmu kladný, tj. $|x| > |y|$. Definiční obor takto zadané funkce je tedy $\{(x, y) \in \mathbb{R}^2, |x| > |y|\}$. Na obrázku můžete vidět graf této funkce.




c) Opět skládáme funkci logaritmus s polynomem více proměnných. Obor hodnot mnohočlenu $-x^2 - y^2$ jsou však nekladná reálná čísla, na nichž není logaritmus definován (jakožto funkce $\mathbb{R} \to \mathbb{R}$).

d) Aby předpis zadával nějakou hodnotu, musí být argument funkce arcsin v intervalu $[-1, 1]$, což je porušeno právě pro ty dvojice $(x, y) \in R^2$, které mají první složku racionální. Předpis tedy korektně definuje funkci na množině $\{(x, y), x \in \mathbb{R} \setminus \mathbb{Q}\}$.

e) Argument odmocniny musí být nezáporný, tj. argument funkce ln z intervalu $[1, \infty]$, tj. $1 \leq x \arcsin(y^2 z)$ a argument funkce arcsin, tj. $y^2 z$, z intervalu $[-1, 1]$. Představení dané plochy v prostoru $\mathbb{R}^3$ ponecháme na laskavém čtenáři. □

### B. Topologie $E_n$

**8.2.** Známým faktem o prostoru $E_n$ je, že nejkratší možná spojnice dvou bodů je přímka. Na prostoru $\mathbb{R}^n$ (či jeho podmnožinách) můžeme však definovat různé metriky, které tuto vlastnost nemají. Uvážíme-li mapu nějakého státu jako podmnožinu $\mathbb{R}^2$, lze definovat vzdálenost dvou bodů, jako dobu, za kterou se lze nejrychleji dostat z jednoho do druhého pomocí použití veřejné dopravy či pěšky. Například ve Francii má takto definovaná metrika hodně daleko k tomu, aby nejkratší spojnicí dvou bodů byla přímka.

**8.3.** Ukažte že každá vlastní podmnožina $E_n$ má nějaký hraniční bod. (Ne nutně v ní ležící.)

**Řešení.** Nechť $U \subset E_n$ nemá hraniční bod. Uvažme bod $X \in U$ a $Y \in U' := E_n \setminus U$ a úsečku $XY \in E_n$. Populárně řečeno, tato úsečka

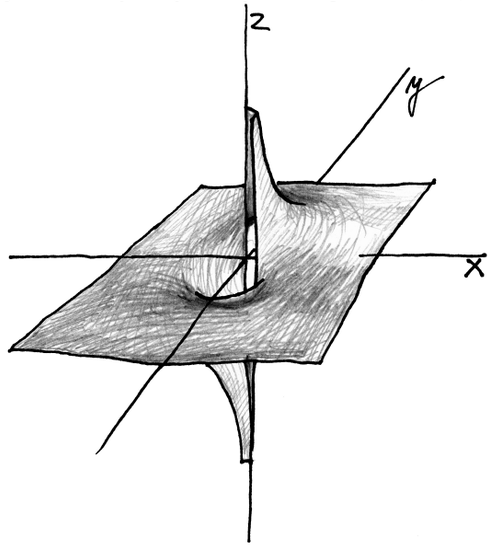
S každou takovou funkcí více proměnných bývá užitečné uvažovat její *graf*, tj. podmnožinu $G_f \subset \mathbb{R}^n \times \mathbb{R} = \mathbb{R}^{n+1}$ definovanou vztahem

$$G_f = \{(x_1, \ldots, x_n, f(x_1, \ldots, x_n));\ (x_1, \ldots, x_n) \in A\},$$

kde $A$ je definiční obor $f$. Např. grafem funkce definované v rovině vztahem

$$f(x, y) = \frac{x + y}{x^2 + y^2}$$

je docela pěkná plocha na obrázku a jejím maximálním definičním oborem jsou všechny body roviny kromě počátku $(0, 0)$.




Při definici a zejména při kreslení obrázku grafu jsme použili pevně zvolené *souřadnice* v rovině. Pokud pro některou z nich zvolíme pevnou hodnotu, zbude nám jen jedna proměnná. Pro pevně zvolenou hodnotu $x$ tak např. dostáváme zobrazení

$$\mathbb{R} \to \mathbb{R}^3,\ y \mapsto (x, y, f(x, y)),$$

tj. *křivku* v prostoru $\mathbb{R}^3$. Křivky jsou vektorové funkce jediné proměnné, se kterými jsme již pracovali v šesté kapitole (viz 6.14). Často jsou na obrázcích grafů funkcí čarami vyneseny obrazy takovýchto křivek pro některé pevně zvolené hodnoty souřadnic $x$ a $y$.

Křivky $c : \mathbb{R} \to \mathbb{R}^n$ jsou vedle funkcí více proměnných nejjednoduššími příklady *zobrazení* $F : \mathbb{R}^m \to \mathbb{R}^n$, ke kterým se dostaneme brzy také.

U funkcí jedné proměnné jsme celý diferenciální a integrální počet vybudovali na základě pojmů konvergence, otevřených okolí, spojitosti atd. Tyto pojmy jsme poté v druhé části sedmé kapitoly zobecnili nejen pro euklidovské prostory $\mathbb{R}^n$, ale i obecněji pro tzv. metrické prostory. Před čtením následujících odstavců bude vhodné si tyto pasáže pečlivě připomenout, případně dohledávat si tam potřebné pojmy a výsledky průběžně. Pro jistotu tady jen velice rychle shrneme aspoň něco málo.

**8.2. Euklidovské prostory.** Euklidovský prostor $E_n$ vnímáme jako množinu bodů v $\mathbb{R}^n$ bez volby souřadnic a na jeho zaměření $\mathbb{R}^n$ pohlížíme jako na vektorový prostor možných přírůstků, které umíme k bodům prostoru $E_n$ přičítat.



musí někdy „přejít“ z $U$ do $\overline{U}'$ a tento přechod je možný jen na hranici (jak čtenář jistě zjistil při návštěvě cizích zemí). Formálně zvolme na úsečce $XY$ bod $A$ tak, aby $|XA| = \sup\{|XZ|,\, XZ \in U\}$ (takový bod $A$ je na úsečce $XY$ právě jeden). Tento bod je zjevně hraničním bodem množiny $U$: z definice $A$ leží libovolná úsečka $XB$, kde $B \in XA$ celá v $U$, zejména tedy bod $B$. Pokud by ovšem existovalo okolí $A$ ležící celé v $U$, tak by existovala úsečka delší než úsečka $XA$, ležící celá v $U$, což by byl také spor s definicí bodu $A$. Libovolné okolí bodu $X$ tak obsahuje jak bod z $U$ tak z $E_n \setminus U$. □

**8.4.** Dokažte, že jedinou podmnožinou $E_n$, která je uzavřená i otevřená, je $E_n$ samotné.

**Řešení.** Podle předchozího příkladu ‖8.3‖ by taková množina $U$ měla hraniční bod. Protože předpokládáme uzavřenost, tak by množina $U$ byla rovna svému uzávěru, tedy obsahovala svůj libovolný hraniční bod. Otevřená množina však z definice nemůže obsahovat žádné hraniční body. □

**8.5.** Ukažte, že prostor $E_n$ nelze zapsat jako sjednocení (alespoň dvou) disjunktních neprázdných otevřených množin.

**Řešení.** Předpokládejme, že $E_n$ takovým sjednocením vyjádřit lze, tedy $E_n = \bigcup_{i\in I} U_i$, kde $I$ je nějaká indexová množina. Vyberme pevně nějakou množinu $U$ z tohoto sjednocení. Pak můžeme psát $E_n = U \cup \overline{U}$, kde jak $U$, tak $\overline{U}$ (jakožto sjednocení otevřených) jsou obě otevřené. Tedy jsou obě, protože jsou doplňky otevřených, i uzavřené a dostáváme spor s tvrzením předchozího příkladu ‖8.4‖. □

**8.6.** Dokažte nebo vyvraťte: sjednocení (případně i nekonečně mnoha) uzavřených podmnožin v $E^n$ je uzavřená podmnožina v $E^n$.

**Řešení.** Tvrzení neplatí. Protipříkladem je sjednocení

$$\bigcup_{i=3}^{\infty}\left[\frac{1}{i}, 1-\frac{1}{i}\right]$$

uzavřených podmnožin $\mathbb{R}$, které je rovno otevřené množině $(0, 1)$. □

**8.7.** Dokažte nebo vyvraťte: průnik (případně i nekonečně mnoha) otevřených podmnožin v $E^n$ je otevřená podmnožina v $E^n$.

**Řešení.** Tvrzení neplatí. Protipříkladem je průnik

$$\bigcap_{i=2}^{\infty}\left(1-\frac{1}{i}, 1+\frac{1}{i}\right)$$

otevřených podmnožin $\mathbb{R}$, který je roven uzavřené množině $\{1\}$. □

Navíc je na $\mathbb{R}^n$ zvolen standardní skalární součin

$$u \cdot v = \sum_{i=1}^{n} x_i y_i,$$

kde $u = (x_1, \ldots, x_n)$ a $v = (y_1, \ldots, y_n)$ jsou libovolné vektory. Tím je na $E_n$ dána *metrika*, tj. funkce vzdálenosti $\|P - Q\|$ dvojic bodů $P$, $Q$ předpisem

$$\|P - Q\|^2 = \|u\|^2 = \sum_{i=1}^{n} x_i^2,$$

kde $u$ je vektor, jehož přičtením k bodu $Q$ obdržíme bod $P$. Např. v rovině $E_2$ je tedy vzdálenost bodů $P_1 = (x_1, y_1)$ a $P_2 = (x_2, y_2)$ dána

$$\|P_1 - P_2\|^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2.$$

Takto definovaná metrika splňuje trojúhelníkovou nerovnost pro každé tři body $P$, $Q$, $R$

$$\|P - R\| = \|(P - Q) + (Q - R)\| \le \|(P - Q)\| + \|(Q - R)\|,$$

viz 3.25(1) v geometrii, resp. axiomy metriky v 7.12 nebo stejnou nerovnost (5.4) pro skaláry. Můžeme proto bez problému přenést (rozšířit) pro body $P_i$ libovolného Euklidovského prostoru pojmy zavedené dosud pro reálné a komplexní skaláry a podrobně diskutované pro metrické prostory:

### Topologie euklidovského prostoru

- *Cauchyovská posloupnost*: posloupnost bodů $P_i$ taková, že pro každé pevně zvolené $\varepsilon > 0$ je $\|P_i - P_j\| < \varepsilon$ pro všechny indexy, až na konečně mnoho výjimečných hodnot $i$, $j$,
- *konvergentní posloupnost*: posloupnost bodů $P_i$ konverguje k bodu $P$, jestliže pro každé pevně zvolené $\varepsilon > 0$ je $\|P_i - P\| < \varepsilon$, až na konečně mnoho výjimečných hodnot $i$, $j$; bod $P$ pak nazýváme *limitou* posloupnosti $P_i$,
- *hromadný bod $P$ množiny $A \subset E_n$*: existuje posloupnost bodů $X_n \neq P$ v $A$ konvergující k $P$,
- *uzavřená množina*: obsahuje všechny své hromadné body,
- *otevřená množina*: její doplněk je uzavřený,
- *otevřené $\delta$–okolí bodu $P$*: množina $\mathcal{O}_\delta(P) = \{Q \in E_n;\ \|P - Q\| < \delta\}$, $\delta \in \mathbb{R}$, $\delta > 0$,
- *hraniční bod $P$ množiny $A$*: každé $\delta$–okolí bodu $P$ má neprázdný průnik s $A$ i s komplementem $E_n \setminus A$,
- *vnitřní bod $P$ množiny $A$*: existuje $\delta$–okolí bodu $P$, které celé leží uvnitř $A$,
- *ohraničená množina*: leží celá v nějakém $\delta$–okolí některého svého bodu (pro dostatečně velké $\delta$),
- *kompaktní množina*: uzavřená a ohraničená množina.



Čtenář by měl investovat přiměřené úsilí do pročtení odstavců 3.25, 5.14–5.17 a 7.14–7.16 a 7.22 a zkusit si promyslet/připomenout definice a souvislosti všech těchto pojmů.

Zejména by mělo být z definic přímo zřejmé, že posloupnosti bodů $P_i$ mají vlastnosti zmiňované v prvních dvou bodech předchozího výčtu tehdy a jen tehdy, když stejně nazvané vlastnosti mají reálné posloupnosti vzniklé z jednotlivých souřadnic bodů $P_i$ ve kterékoliv kartézské souřadné soustavě. Proto také z lemma 5.12 vyplývá, že každá cauchyovská posloupnost bodů v $E_n$ je konvergentní. Zejména je tedy $E_n$ vždy úplným metrickým prostorem.

**8.8.** Uvažme graf spojité funkce $f : \mathbb{R}^2 \to \mathbb{R}$ jako podmnožinu $E_3$. Rozhodněte o této množině, zda je otevřená, uzavřená, či kompaktní.

**Řešení.** Množina není otevřená, neboť libovolné okolí bodu $[x_0, y_0, f(x_0, y_0)]$ obsahuje nějakou úsečku ležící na přímce $x = x_0$, $y = y_0$. Na této úsečce však leží jediný bod grafu funkce a to právě bod $[x_0, y_0, f(x_0, y_0)]$.

Množina je uzavřená díky spojitosti funkce $f$: ukážeme, že libovolná konvergentní posloupnost bodů na grafu funkce $f$ konverguje k bodu ležícím rovněž na tomto grafu. Totiž je-li nějaká v $E_3$ konvergující posloupnost bodů na grafu funkce, tak konverguje každá její složka, tudíž posloupnost $\{[x_n, y_n]\}_{n=1}^{\infty}$ musí být konvergentní posloupnost v $\mathbb{R}^2$. Označme tuto limitu $[a, b]$. Potom z definice spojitosti funkce $f$ musejí její funkční hodnoty v bodech $[x_n, y_n]$ konvergovat k hodnotě $f(a, b)$. To však znamená, že posloupnost $\{[x_n, y_n, f(x_n, y_n)]\}_{n=1}^{\infty}$ konverguje k bodu $[a, b, f(a, b)]$. To je bod na grafu funkce $f$. Graf je tedy uzavřená množina.

Množina je sice uzavřená, ale není kompaktní, neboť není omezená (její kolmý průmět do souřadnicové roviny $xy$ je celé $\mathbb{R}^2$. (Kompaktní množiny v $E_n$ jsou právě právě množiny, které jsou současně uzavřené a omezené) □

### C. Tečny, tečné roviny, grafy funkcí více proměnných

**8.9.** V bodě $[1, 0, 0]$ se nachází v čase $t = 0$ auto o rychlosti dané vektorem $(0, 1, 1)$. Auto se pohybuje se zrychlením dané v čase $t$ vektorem $(-\cos t, -\sin t, 0)$. Popište dráhu auta v čase $t$.

**Řešení.** Jak bylo diskutováno v odstavci 8.4, s prostředky k řešení této úlohy jsme se již seznámili v kapitole 6. Všimněme si, že „integrální křivka“ $C(t)$ z věty z odstavce 8.4, začíná v bodě $(0, 0, 0)$. (resp. je $C(0) = (0, 0, 0)$). V afinním prostoru $\mathbb{R}^n$ ji můžeme posunout do libovolného bodu a na její derivaci se nic nemění (jde o přičtení konstanty v každé složce, v parametrickém vyjádření křivky). Až na toto posunutí je tak tato integrální křivka dána jednoznačně (nic jiného než konstanty v každé složce přičítat beze změny derivace nelze). Integrací křivky zrychlení, dostaneme křivku rychlostí $(-\sin t, \cos t - 1, 0)$, uvážením počáteční rychlosti, dostáváme křivku rychlostí auta: $(-\sin t, \cos t, 1)$ (posouvali jsme o vektor $(0, 1, 1)$, tedy tak, aby v čase $t = 0$ křivka rychlostí souhlasila se zadanou počáteční rychlostí). Další integrací dostáváme křivku $(\cos t - 1, \sin t, t)$. Posunutím o vektor $(1, 0, 0)$ se pak dostáváme do počáteční polohy auta. Auto se tedy pohybuje po křivce $[\cos t, \sin t, t]$ (této křivce se říká šroubovice, někdy též převzatým slovem helix). □

**8.3. Kompaktní množiny.** Naše hrátky s otevřenými, uzavřenými nebo kompaktními množinami mohly v případě reálné přímky $E_1$ vypadat jako zbytečné, protože nakonec jsme stejně skoro vždy mluvili jen o intervalech.

U metrických prostorů ve ve druhé části kapitoly sedmé to možná bylo až moc složité. Stejný přístup je ale v případě euklidovských prostorů $\mathbb{R}^n$ docela jednoduchý a zároveň velmi užitečný a podstatný (a je to samozřejmě speciální případ obecných metrických prostorů).

Stejně jako v případě $E_1$ definujeme otevřené pokrytí množiny (tj. systém otevřených množin, v jejichž sjednocení je daná množina obsažena) a platí s drobnými formulačními úpravami i Věta 5.17:

**Věta.** *Pro podmnožiny $A \subset E_n$ v euklidovských prostorech platí:*

*(1) A je otevřená, právě když je sjednocením nejvýše spočetného systému $\delta$–okolí,*
*(2) každý bod $a \in A$ je buď vnitřní nebo hraniční,*
*(3) každý hraniční bod je buď izolovaným nebo hromadným bodem A,*
*(4) A je kompaktní, právě když každá v ní obsažená nekonečná posloupnost má podposloupnost konvergující k bodu v A,*
*(5) A je kompaktní, právě když je uzavřená a omezená,*
*(6) A je kompaktní, právě když každé její otevřené pokrytí obsahuje konečné podpokrytí.*



Důkaz. Důkaz z 5.17 lze bez úprav použít v případě tvrzení (1)–(3), byť s novým chápání pojmů a nahrazením „otevřených intervalů“ jejich vícerozměrnými $\delta$–okolími vhodných bodů.

První charakterizace kompaktnosti je vlastně definice tohoto pojmu, kterou jsme použili v metrických prostorech. Zbylé dvě charakterizace kompaktnosti jsou speciálním případem obecných tvrzení pro metrické prostory, viz 7.22, které lze i přímo obdržet vhodnou modifikací našeho postupu z případu prostorů jednorozměrných. □

**8.4. Křivky v $E_n$.** Skoro celá naše diskuse kolem limit, derivací a integrálů funkcí v páté a šesté kapitole se týkala funkcí s jednou reálnou proměnnou a reálnými nebo komplexními hodnotami s odůvodněním, že používáme pouze trojúhelníkovou nerovnost platnou pro velikosti reálných i komplexních čísel. Již tehdy jsme si povšimli, že se tento argument do značné míry přenáší na jakékoliv funkce jedné reálné proměnné s hodnotami v euklidovském prostoru $\mathbb{R}^n$ a uvedli jsme několik nástrojů pro práci s křivkami v odstavcích 6.14–6.17.



Připomeňme proto, že pro každou (parametrizovanou) křivku[1], tj. zobrazení $c : \mathbb{R} \to \mathbb{R}^n$ v $n$–rozměrném prostoru, můžeme pracovat s pojmy, které jednoduše rozšiřují naše úvahy z funkcí jedné proměnné:

- *limita:* $\lim_{t \to t_0} c(t) \in \mathbb{R}^n$,
- *derivace:* $c'(t_0) = \lim_{t \to t_0} \frac{1}{|t - t_0|} \cdot (c(t) - c(t_0)) \in \mathbb{R}^n$,
- *integrál:* $\int_a^b c(t)dt \in \mathbb{R}^n$.

[1] V geometrii se většinou rozlišuje mezi křivkou jakožto podmnožinou v $E_n$ a její parametrizací $\mathbb{R} \to \mathbb{R}^n$. My zde pod pojmem „křivka“ rozumíme výhradně parametrizované křivky. Těm se v české geometrické literatuře často říká „dráha“.

**8.10.** Určete parametrické i implicitní rovnice tečny ke křivce $c : \mathbb{R} \to \mathbb{R}^3$, $c(t) = (c_1(t), c_2(t), c_3(t)) = (t, t^2, t^3)$ v bodě odpovídajícím hodnotě parametru $t = 1$.

**Řešení.** Parametru $t = 1$ odpovídá bod $c(1) = [1, 1, 1]$. Derivace jednotlivých složek jsou $c_1'(t) = 1$, $c_2'(t) = 2t$, $c_3(t) = 3t^2$. Hodnoty derivací v bodě $t = 1$ jsou 1, 2, 3. Parametrické rovnice tečny tak jsou:

$$\begin{aligned} x &= c_1'(1)t + c_1(1) = t + 1, \\ y &= c_2'(1)t + c_2(1) = 2t + 1, \\ z &= c_3'(1)t + c_3(1) = 3t + 1. \end{aligned}$$

Vyloučením parametru $t$ dostáváme implicitní rovnice tečny (nejsou dány kanonicky):

$$\begin{aligned} 2x - y &= 1, \\ 3x - z &= 2. \end{aligned}$$

□

**8.11. Množina diferencovatelných funkcí.** Všimněme si, že



mnohočleny více proměnných jsou diferencovatelné na celém svém oboru. Rovněž tak složení diferencovatelné funkce jedné proměnné s diferencovatelnou funkcí více proměnných je opět diferencovatelná funkce více proměnných. Je tedy například funkce $\sin(x + y)$ diferencovatelnou funkcí na celém $\mathbb{R}^2$, $\ln(x + y)$ je diferencovatelnou funkcí na množině $x > y$ (polorovině bez hraniční přímky). Důkazy zmíněných tvrzení jsou cvičením na skládání limit.

**Poznámka. Značení parciálních derivací.** Parciální derivaci funkce $f : \mathbb{R}^n \to \mathbb{R}$ proměnných $x_1, \ldots, x_n$ podle proměnné $x_1$ budeme značit jak $\frac{\partial f}{\partial x_1}$, tak kratším zápisem $f_{x_1}$. V příkladové části se budeme spíše držet druhého způsobu. Zápis $\frac{\partial f}{\partial x_1}$ pak lépe vystihuje fakt, že se jedná o derivaci funkce $f$ ve směru vektorového pole $\frac{\partial}{\partial x_1}$ (co je vektorové pole se dozvíte v odstavci 8.34).

**8.12.** Určete definiční obor funkce $f : \mathbb{R}^2 \to R$, $f(x, y) = x^2\sqrt{y}$.



Určete parciální derivace tam, kde jsou na tomto oboru definovány.

**Řešení.** Definičním oborem dané funkce je v $\mathbb{R}^2$ polorovina $\{(x, y), y \geq 0\}$. Při určení parciální derivace podle některé z proměnných postupujeme tak, že v předpisu pro funkci považujeme za proměnnou pouze tu, podle níž derivujeme. Ostatní proměnné pak považujeme za konstanty a derivujeme podle pravidel o derivování funkce jedné proměnné. Dostáváme tak:

$$f_x = 2x\sqrt{y} \text{ a } f_y = \frac{1}{2}\frac{x^2}{\sqrt{y}}.$$

Parciální derivace existují ve všech bodech definičního oboru mimo hraniční přímky $y = 0$. □

Všimněme si také, že jak limita tak derivace křivek mají smysl v afinním prostoru, aniž bychom volili souřadnice (přičemž limitou posloupnosti je opět bod v původním prostoru, zatímco derivace je vektor v zaměření!). V případě integrálu ale musíme uvažovat křivky ve vektorovém prostoru $\mathbb{R}^n$. Důvod je vidět už v jednorozměrném případě, kde potřebujeme znát počátek, abychom mohli vidět „plochu pod grafem funkce".

Opět je přímo z definice zjevné, že limity, derivace i integrály lze spočíst po jednotlivých $n$ souřadných složkách v $\mathbb{R}^n$ a stejně se rozpozná i jejich existence.

U integrálu můžeme také přímo formulovat pro křivky analogii souvislosti Riemannova integrálu a primitivní funkce (viz 6.25):

**Tvrzení.** *Nechť $c$ je křivka v $\mathbb{R}^n$, spojitá na intervalu $[a, b]$. Pak existuje její Riemannův integrál $\int_a^b c(t)dt$. Navíc je křivka*

$$C(t) = \int_a^t c(s)ds \in \mathbb{R}^n$$

*dobře definovaná, diferencovatelná a platí $C'(t) = c(t)$ pro všechny hodnoty $t \in [a, b]$.*

Horší je to s větou o střední hodnotě a obecněji s Taylorovou větou, viz 5.38 a 6.4. Ve zvolených souřadnicích je můžeme aplikovat na jednotlivé souřadné funkce diferencovatelné křivky $c(t) = (c_1(t), \ldots, c_n(t))$ na konečném intervalu $[a, b]$. Dostaneme např. u věty o střední hodnotě existenci čísel $t_i$ takových, že

$$c_i(b) - c_i(a) = (b - a) \cdot c_i'(t_i).$$

Tato čísla $t_i$ ale budou obecně různá, nemůžeme proto vyjádřit rozdílový vektor koncových bodů $c(b) - c(a)$ jako násobek derivace křivky v jediném bodě. Např. v rovině $E_2$ pro diferencovatelnou křivku $c(t) = (x(t), y(t))$ takto dostáváme

$$\begin{aligned} c(b) - c(a) &= (x'(\xi)(b - a), y'(\eta)(b - a)) \\ &= (b - a) \cdot (x'(\xi), y'(\eta)) \end{aligned}$$

pro dvě (obecně různé) hodnoty $\xi, \eta \in [a, b]$. Pořád nám ale tato úvaha stačí na následující odhad.

**Lemma.** *Je-li $c$ křivka v $E_n$ se spojitou derivací na kompaktním intervalu $[a, b]$, pak pro všechny $a \leq s \leq t \leq b$ platí*

$$\|c(t) - c(s)\| \leq \sqrt{n}\left(\max_{r\in[a,b]} \|c'(r)\|\right) \cdot |t - s|.$$

Důkaz. Přímým použitím věty o střední hodnotě dostáváme pro vhodné body $r_i$ uvnitř intervalu $[s, t]$:

$$\begin{aligned} \|c(t) - c(s)\|^2 &= \sum_{i=1}^{n} (c_i(t) - c_i(s))^2 \leq \sum_{i=1}^{n} (c_i'(r_i)(t - s))^2 \\ &\leq (t - s)^2 \sum_{i=1}^{n} \max_{r\in[s,t]} c_i'(r)^2 \\ &\leq n(\max_{r\in[s,t],\ i=1,\ldots,n} |c_i'(r)|)^2 (t - s)^2 \\ &\leq n \max_{r\in[s,t]} \|c'(r)\|^2 (t - s)^2. \end{aligned}$$

□

Důležitým pojmem je *tečný vektor* ke křivce $c : \mathbb{R} \to E_n$ v bodě $c(t_0) \in E_n$, který definujeme jako vektor v prostoru zaměření $\mathbb{R}^n$ daný derivací $c'(t_0) \in \mathbb{R}^n$.

**8.13.** Určete směrovou derivaci funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x, y, z) = x^2 yz$ v bodě $[1, -1, 2]$ ve směru $v = (3, 2, -1)$.

**Řešení.** Směrovou derivaci spočítáme dvěma různými způsoby. Jednak přímo z definice (viz odstavec 8.5), a také pomocí diferenciálu dané funkce, viz 8.6 a věta 8.7. Daná funkce je totiž mnohočlenem, tudíž diferencovatelnou funkcí na celém $\mathbb{R}^3$.

Počítejme podle definice:

$$\begin{aligned} f_v(x, y, z) &= \lim_{t\to 0} \frac{1}{t}[f(x + 3t, y + 2t, z - t) - f(x, y, z)] = \\ &= \lim_{t\to 0} \frac{1}{t}[(x + 3t)^2(y + 2t)(z - t) - x^2 yz] = \\ &= \lim_{t\to 0} \frac{1}{t}[t(6xyz + 2x^2 z - x^2 y) + t^2(\dots)] = \\ &= 6xyz + 2x^2 z - x^2 y. \end{aligned}$$

Odvodili jsme tak směrovou derivaci ve směru vektoru $(3, 2, -1)$ jakožto funkci tří reálných proměnných, udávající bod, ve kterém derivaci zkoumáme. Pro zadaný bod pak dosazením získáme $f_v(1, -1, 2) = -7$.

Pro výpočet směrové derivace z diferenciálu dané funkce budeme nejprve muset spočítat parciální derivace dané funkce:

$$f_x = 2xyz, \;\; f_y = x^2 z, \;\; f_z = x^2 y.$$

Podle poznámky za větou 8.7 pak můžeme vyjádřit

$$\begin{aligned} f_v(1, -1, 2) &= 3f_x(1, -1, 2) + 2f_y(1, -1, 2) + \\ &\quad + (-1)f_z(1, -1, 2) = \\ &= 3 \cdot (-4) + 2 \cdot 2 + (-1) \cdot (-1) = -7. \end{aligned}$$ □

**8.14.** Určete směrovou derivaci funkce $f : \mathbb{R}^3 \to R$, $f(x, y, z) = \frac{\cos(x^2 y)}{z}$ v bodě $[0, 0, 2]$ ve směru vektoru $(1, 2, 3)$.

**Řešení.** Definičním oborem dané funkce je $\mathbb{R}^3$ mimo roviny $z = 0$. Další výpočty budeme uvažovat pouze na tomto oboru. Funkce je v bodě $[0, 0, 2]$ diferencovatelná (podle poznámky ‖8.11‖). Hodnotu zkoumané směrové derivace určíme podle 8.6 pomocí parciálních derivací.

Určíme parciální derivace dané funkce (Jak jsme již popsali v příkladě ‖8.12‖, pro určení parciální derivace podle $x$, derivujeme danou funkci jako funkci jedné proměnné $x$, používáme pravidlo o derivaci složené funkce. Obdobně pro další parciální derivace.):

$$f_x = -\frac{2xy \sin(x^2 y)}{z}, \;\; f_y = -\frac{x^2 \sin(x^2 y)}{z}, \;\; f_z = -\frac{\cos(x^2 y)}{z^2}.$$

Pokud si představíme $c$ jako dráhu nějakého předmětu v prostoru, pak tečný vektor v bodě $t_0$ lze fyzikálně chápat jako okamžitou rychlost v tomto bodě.

Přímka $T$ zadaná parametricky

$$T: \quad c(t_0) + t \cdot c'(t_0)$$

se nazývá *tečna ke křivce* $c$ v bodě $t_0$. Na rozdíl od tečného vektoru, tečna $T$ coby neparametrizovaná přímka zjevně nezávisí na parametrizaci křivky $c$, protože při změně parametrizace dostaneme díky větě o derivování složených funkcí znovu stejný tečný vektor, až na násobek.

**8.5. Parciální derivace.** Pro každou funkci $f : \mathbb{R}^n \to \mathbb{R}$ a libovolnou křivku $c : \mathbb{R} \to \mathbb{R}^n$ máme k dispozici jejich kompozici $(f \circ c)(t) : \mathbb{R} \to \mathbb{R}$. Tato složená funkce $F \circ c$ vypovídá o chování funkce $f$ podél křivky $c$. Nejjednodušší bude použít přímky.



SMĚROVÉ A PARCIÁLNÍ DERIVACE

**Definice.** Řekneme, že $f : \mathbb{R}^n \to \mathbb{R}$ má *derivaci ve směru vektoru* $v \in \mathbb{R}^n$ v bodě $x \in E_n$, jestliže existuje derivace $d_v f(x)$ složeného zobrazení $t \mapsto f(x + tv)$ v bodě $t = 0$, tj.

$$d_v f(x) = \lim_{t\to 0} \frac{1}{t}(f(x + tv) - f(x)).$$

Hodnotě $d_v f$ také říkáme *směrová derivace*.

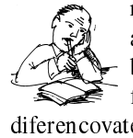
Speciální volbou přímek ve směru souřadných os dostáváme tzv. *parciální derivace funkce* $f$, které značíme $\frac{\partial f}{\partial x_i}$, $i = 1, \dots, n$, nebo bez odkazu na samotnou funkci jako operace $\frac{\partial}{\partial x_i}$.

Pro funkce v rovině tak dostáváme

$$\begin{aligned} \frac{\partial}{\partial x} f(x, y) &= \lim_{t\to 0} \frac{1}{t}(f(x + t, y) - f(x, y)), \\ \frac{\partial}{\partial y} f(x, y) &= \lim_{t\to 0} \frac{1}{t}(f(x, y + t) - f(x, y)). \end{aligned}$$

Zejména je vidět, že parciálně podle vybrané proměnné derivujeme tak, že prostě všechny ostatní proměnné považujeme za konstanty a postupujeme jako u funkcí jedné proměnné.

**8.6. Diferenciál funkce** $f : \mathbb{R}^n \to \mathbb{R}$**.** Se samotnými parciálními nebo směrovými derivacemi nevystačíme pro dobrou aproximaci chování funkce lineárními výrazy. Asi bychom přirozeně očekávali, že „diferencovatelná“ funkce více proměnných bude složením s jakoukoliv diferencovatelnou křivkou dávat diferencovatelné funkce jedné proměnné, které už dobře známe.



Podívejme se ale např. na funkce v rovině zadané výrazy

$$g(x, y) = \begin{cases} 1 & \text{když } yx = 0 \\ 0 & \text{jinak,} \end{cases}$$

$$h(x, y) = \begin{cases} 1 & \text{když } y = x^2 \neq 0 \\ 0 & \text{jinak.} \end{cases}.$$

Evidentně žádná z nich neprodlužuje všechny hladké křivky procházející bodem $(0, 0)$ na hladké funkce, protože už zúžení na přímky procházejících počátkem nejsou ani spojité. Přitom ale pro $g$ existují obě parciální derivace v $(0, 0)$ (a jsou nulové), ale jiné

Dosazením konkrétních hodnot pak obdržíme

$$f_x(0,0,2) + 2 \cdot f_y(0,0,2) + 3 \cdot f_z(0,0,2) = 1 \cdot 0 + 2 \cdot 0 + 3 \cdot \left(-\frac{1}{4}\right) = -\frac{3}{4}.$$

□

**8.15.** Pro funkci $f : \mathbb{R}^n \to \mathbb{R}$ s diferenciálem $df(x)$ určete v bodě $x \in \mathbb{R}^n$ jednotkový směr $v \in \mathbb{R}_n$, ve kterém je směrová derivace $d_v(x)$ maximální.

**Řešení.** Podle poznámky za větou 8.4 jde o maximalizaci funkce $f_v(x) = v_1 f_{x_1}(x) + v_2 f_{x_2}(x) + \cdots + v_n f_{x_n}(x)$. v závislosti na proměnných $v_1, \ldots, v_n$, které jsou vázány podmínkou $v_1^2 + \cdots + v_n^2 = 1$. Stejný problém už jsme řešili kapitole 3, při lineární optimalizaci (viz ‖3.1‖). Hodnotu $f_v(x)$ totiž můžeme interpretovat jako skalární součin vektorů $(f_{x_1}, \ldots, f_{x_n})$ a $(v_1, \ldots, v_n)$. No a ten je maximální, pokud jsou vektory stejného směru. Vektor $v$ tedy získáme normováním vektoru $(f_{x_1}, \ldots, f_{x_n})$. Obecně říkáme, že funkce roste maximálně ve směru $(f_{x_1}, \ldots, f_{x_n})$. Tento vektor pak nazýváme gradientem funkce $f$. Podrobněji se jím budeme zabývat a tuto úvahu si ještě připomeneme v odstavci 8.19. □

**8.16.** Rozhodněte, zda tečná rovina ke grafu funkce $f : \mathbb{R} \times \mathbb{R}^+ \to \mathbb{R}$, $f(x,y) = x \cdot \ln(y)$ v bodě $[1, \frac{1}{e}]$ prochází bodem $[1,2,3] \in \mathbb{R}^3$.

**Řešení.** Určíme nejdříve parciální derivace: $f_x(x,y) = \ln(y)$, $f_y(x,y) = \frac{x}{y}$, jejich hodnoty v bodě $[1, \frac{1}{e}]$ jsou $-1$, $e$, dále $f(1, \frac{1}{e}) = -1$. Rovnice tečné roviny je tedy

$$\begin{aligned} z &= f\left(1,\frac{1}{e}\right) + f_x\left(1,\frac{1}{e}\right)(x-1) + f_y\left(1,\frac{1}{e}\right)\left(y-\frac{1}{e}\right) \\ &= -1 - x + ey. \end{aligned}$$

Této rovnici daný bod nevyhovuje, v tečné rovině tedy neleží. □

**8.17.** Určete parametrické vyjádření tečny k průsečnici grafů funkcí $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x,y) = x^2 + xy - 6$, $g : \mathbb{R} \times \mathbb{R}^+ \to \mathbb{R}$, $g(x,y) = x \cdot \ln(y)$ v bodě $[2,1]$.

**Řešení.** Tečna k průsečnici je průsečnicí tečných rovin v daném bodě. Tečná rovina ke grafu funkce $f$ procházející bodem $[2,1]$ je

$$\begin{aligned} z &= f(2,1) + f_x(2,1)(x - x_0) + f_y(2,1)(y - y_0) \\ &= 5x + 2y - 12. \end{aligned}$$

Tečná rovina k grafu $g$ je pak

$$\begin{aligned} z &= g(2,1) + g_x(x,y)(2,1)(x - x_0) + g_y(x,y)(2,1)(y - y_0) \\ &= 2y - 2. \end{aligned}$$

směrové derivace neexistují. Pro $h$ existují všechny směrové derivace v bodě $(0,0)$ a je dokonce $d_v h(0) = 0$ pro všechny směry $v$ (protože na každé přímce procházející počátkem je na aspoň malinkém okolí nuly funkce $h$ nulová), takže jde o lineární závislost na $v \in \mathbb{R}^2$.

Snadno si také představíme funkci $f$, která bude mít podél přímek $(r\cos\theta, r\sin\theta)$ s pevným úhlem $\theta$ hodnoty $k(\theta)r$, přičemž $k(\theta)$ je periodická lichá funkce v úhlu $\theta$, s periodou $2\pi$. Její směrové derivace $d_v f$ v $(0,0)$ všechny existují, ale pro obecné funkce $k(\theta)$ zcela jistě nepůjde o lineární výrazy v závislosti na směrech $v$.

Budeme proto napodobovat případ funkcí jedné proměnné co nejdůsledněji a podobné patologické chování funkcí vyloučíme přímo definicí:

### Diferenciál

**Definice.** Funkce $f : \mathbb{R}^n \to \mathbb{R}$ je *diferencovatelná v bodě* $x$, jestliže zároveň platí tři vlastnosti:

(1) v bodě $x$ existují směrové derivace $d_v f(x)$ pro všechny vektory $v \in \mathbb{R}^n$,
(2) $d_v f(x)$ je lineární v závislosti na přírůstku $v$,
(3) $\lim_{v\to 0} \frac{1}{\|v\|}\big(f(x+v) - f(x) - d_v f(x)\big) = 0$.

Lineární výraz $d_v f$ (ve vektorové proměnné $v$) nazýváme *diferenciál funkce* $f$ vyčíslený na přírůstku $v$.

Řečeno slovy, požadujeme, aby v bodě $x$ existovalo dobré přiblížení přírůstků funkce $f$ pomocí lineární funkce přírůstků proměnných veličin.

Přímo z definice směrových derivací vyplývá, že můžeme také diferenciál definovat pouze pomocí vlastnosti (3). Skutečně, pokud existuje nějaká lineární forma $df(x)$ taková, že pro přírůstky $v$ v bodě $x$ platí vlastnost (3) s $d_v f(x) = df(x)(v)$, pak je zjevně $df(x)(v)$ právě směrovou derivací funkce $f$ v bodě $x$ a vlastnosti (1) a (2) jsou tedy splněny automaticky.

Definici diferenciálu můžeme také přepsat ve tvaru

$$\|f(x+v) - f(x)\| \le \|d_v(x)\| + \|\alpha(v)\|,$$

kde funkce $\alpha$ splňuje $\lim_{v\to 0} \frac{\alpha(v)}{\|v\|} = 0$. Protože jsou lineární zobrazení $df$ spojitá, dovodili jsme:

**Lemma.** *Je-li funkce $f$ diferencovatelná v bodě $x$, pak je v tomto bodě spojitá.*



Podívejme se, co umíme říci o diferenciálu funkce $f(x,y)$ v rovině za předpokladu, že obě parciální derivace $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$ existují a jsou spojité v okolí bodu $(x_0, y_0)$.

Uvažme za tím účelem jakoukoliv hladkou křivku $t \mapsto (x(t), y(t))$ s $x_0 = x(0)$, $y_0 = y(0)$. S použitím věty o střední hodnotě na funkce jedné proměnné v obou sčítancích zvlášť dovodíme, že

$$\begin{aligned} &\tfrac{1}{t}\big(f(x(t),y(t)) - f(x_0,y_0)\big) = \\ &\tfrac{1}{t}\big(f(x(t),y(t)) - f(x_0,y(t))\big) + \tfrac{1}{t}\big(f(x_0,y(t)) - f(x_0,y_0)\big) \\ &= \tfrac{1}{t}(x(t) - x_0) \cdot \frac{\partial f}{\partial x}(x(\xi), y(t)) + \tfrac{1}{t}(y(t) - y_0) \cdot \frac{\partial f}{\partial y}(x_0, y(\eta)) \end{aligned}$$

pro vhodná čísla $\xi$ a $\eta$ mezi 0 a $t$.

Průsečnicí těchto dvou rovin je přímka daná parametricky jako $[2, t, 2t-2]$, $t \in \mathbb{R}$.

**Jiné řešení.** Normála k ploše určené rovnicí $f(x, y, z) = 0$ v bodě $b = [2, 1, 0]$ je $(f_x(b), f_y(b), f_z(b)) = (5, 2, -1)$, normála k ploše určené jako $g(x, y, z) = 0$ v tomtéž bodě je $(0, 2, -1)$. Tečna je kolmá na obě normály, její směrový vektor získáme tedy např. vektorovým součinem normál, což je $(0, 5, 10)$. Protože tečna prochází bodem $[2, 1, 0]$, je její parametrické vyjádření $[2, 1+t, 2t]$, $t \in \mathbb{R}$. □

**8.18.** Určete všechny druhé parciální derivace funkce $f$ dané předpisem $f(x, y, z) = \sqrt{xy \ln z}$.

**Řešení.** Nejprve určíme definiční obor dané funkce: argument odmocniny musí být nezáporný a argument logaritmu musí být kladný, je tedy $Df = \{(x, y, z) \in \mathbb{R}^3, (z \geq 1 \& (xy > 0)) \vee (0 < z < 1) \& (xy < 0)\}$.

Nyní spočteme první parciální derivace podle všech tří proměnných:

$$f_x = \frac{y \ln(z)}{2\sqrt{xy \ln(z)}},\ f_y = \frac{x \ln(z)}{2\sqrt{xy \ln(z)}},\ f_z = \frac{xy}{2z\sqrt{xy \ln(z)}}.$$

Každá z těchto tří parciálních derivací je opět funkcí tří proměnných, můžeme tedy uvážit (první) parciální derivace těchto funkcí. To jsou druhé parciální derivace funkce $f$. Jako index k funkci $f$ připíšeme proměnné, podle kterých derivujeme.

$$\begin{aligned}
f_{xx} &= -\frac{y^2 \ln^2 z}{4(xy \ln z)^{\frac{3}{2}}},\\
f_{xy} &= -\frac{xy \ln^2 z}{4(xy \ln z)^{\frac{3}{2}}} + \frac{\ln z}{2\sqrt{xy \ln z}},\\
f_{xz} &= -\frac{xy^2 \ln z}{4z(xy \ln z)^{\frac{3}{2}}} + \frac{y}{2z\sqrt{xy \ln z}},\\
f_{yy} &= -\frac{x^2 \ln^2 z}{4(xy \ln z)^{\frac{3}{2}}},\\
f_{yz} &= -\frac{x^2 y \ln z}{4z(xy \ln z)^{\frac{3}{2}}} + \frac{x}{2z\sqrt{xy \ln z}},\\
f_{zz} &= -\frac{x^2 y^2}{4z^2(xy \ln z)^{\frac{3}{2}}} - \frac{xy}{2z^2\sqrt{xy \ln z}}.
\end{aligned}$$

Podle věty o záměnnosti parciálních derivací (viz 8.10) víme, že $f_{xy} = f_{yx}$, $f_{xz} = f_{zx}$, $f_{yz} = f_{zy}$, smíšené parciální derivace (smíšená znamená, že parciálně derivujeme podle více než jedné proměnné) tedy stačí určit pro jedno konkrétní pořadí derivování. □

Zejména tedy pro každou posloupnost čísel $t_n$ jdoucí k nule získáme příslušné posloupnosti čísel $\xi_n$ a $\eta_n$, které také budou konvergovat k nule, a pro všechny bude platit vyjádření výše.

Limitním přechodem $t \to 0$ proto díky spojitosti parciálních derivací dostáváme (viz test konvergence funkce pomocí vybraných posloupností hodnot argumentů, 5.23, a Věta 5.22 o limitách součtů a součinů funkcí)

$$\frac{d}{dt} f(x(t), y(t))|_{t=0} = x'(0)\frac{\partial f}{\partial x}(x_0, y_0) + y'(0)\frac{\partial f}{\partial y}(x_0, y_0),$$

což je příjemné rozšíření platnosti věty o derivování složených funkcí jedné proměnné pro vektorově hodnotové funkce.

Samozřejmě, speciální volbou parametrizovaných přímek

$$(x(t), y(t)) = (x_0 + t\xi, y_0 + t\eta)$$

přechází náš výpočet při $v = (\xi, \eta)$ na rovnost

$$d_v f(x_0, y_0) = \frac{\partial f}{\partial x}(x_0, y_0)\xi + \frac{\partial f}{\partial y}(x_0, y_0)\eta$$

a tento vztah můžeme pěkně vyjádřit způsobem, kterým jsme v lineární algebře zapisovali souřadná vyjádření lineárních funkcí na vektorových prostorech:

$$df = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy.$$

Jinými slovy, směrová derivace $d_v f$ je skutečně lineární funkce $\mathbb{R}^n \to \mathbb{R}$ na přírůstcích, se souřadnicemi danými právě parciálními derivacemi.

Podobným postupem nyní budeme umět dokázat, že předpoklad spojitých parciálních derivací v daném bodě zajišťuje i aproximační vlastnosti diferenciálu.

Budeme už rovnou uvažovat obecné funkce více proměnných:

**8.7. Věta.** *Nechť $f : E_n \to \mathbb{R}$ je funkce $n$ proměnných, která má v okolí bodu $x \in E_n$ spojité parciální derivace. Pak existuje její diferenciál $df$ v bodě $x$ a jeho souřadné vyjádření je dáno výrazem.*

$$df = \frac{\partial f}{\partial x_1}dx_1 + \frac{\partial f}{\partial x_2}dx_2 + \cdots + \frac{\partial f}{\partial x_n}dx_n.$$

Důkaz. Odvození věty je naprosto analogické výše uvedenému postupu v případě $n = 2$. Musíme být jen opatrní v detailech a dokončit úvahu o aproximačních vlastnostech. Úplně stejně jako výše uvažujeme křivku



$$c(t) = (c_1(t), \ldots, c_n(t)),$$

$c(0) = (0, ..., 0)$, a bod $x \in \mathbb{R}^n$ a vyjádříme pro složenou funkci $f(c(t))$ rozdíl $f(x + c(t)) - f(x)$ takto

$$\begin{aligned}
&f(x_1 + c_1(t), \ldots, x_n + c_n(t)) - f(x_1, x_2 + c_2(t), \ldots)\\
&+ f(x_1, x_2 + c_2(t), \ldots)) - f(x_1, x_2, \ldots, x_n + c_n(t))\\
&\vdots\\
&+ f(x_1, x_2, \ldots, x_n + c_n(t)) - f(x_1, x_2, \ldots, x_n).
\end{aligned}$$

### D. Taylorovy polynomy

**8.19.** Napište Taylorův rozvoj druhého řádu funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = \ln(x^2 + y^2 + 1)$ v bodě $[1, 1]$.

**Řešení.** Nejprve spočítáme první parciální derivace:

$$f_x = \frac{2x}{x^2 + y^2 + 1},\ f_y = \frac{2y}{x^2 + y^2 + 1},$$

poté Hessián:

$$Hf(x, y) = \begin{pmatrix} \frac{2y^2-2x^2+2}{(x^2+y^2+1)^2} & -\frac{4xy}{(x^2+y^2+1)^2} \\ -\frac{4xy}{(x^2+y^2+1)^2} & \frac{2x^2-2y^2+2}{(x^2+y^2+1)^2} \end{pmatrix}.$$

Hodnota Hessiánu v bodě $[1, 1]$ je

$$\begin{pmatrix} \frac{2}{9} & -\frac{4}{9} \\ -\frac{4}{9} & \frac{2}{9} \end{pmatrix},$$

celkem tedy je Taylorův rozvoj druhého řádu v bodě $[1, 1]$:

$$\begin{aligned} T_2(x, y) &= f(1, 1) + f_x(1, 1)(x - 1) + f_y(1, 1)(y - 1) + \\ &\quad + \frac{1}{2}(x - 1, y - 1)Hf(1, 1)\begin{pmatrix} x - 1 \\ y - 1 \end{pmatrix} \\ &= \ln(3) + \frac{2}{3}(x - 1) + \frac{2}{3}(y - 1) + \frac{1}{9}(x - 1)^2 - \\ &\quad - \frac{4}{9}(x - 1)(y - 1) + \frac{1}{9}(y - 1)^2 \\ &= \frac{1}{9}(x^2 + y^2 + 8x + 8y - 4xy - 14) + \ln(3). \end{aligned}$$

□

**Poznámka.** Zejména je tedy Taylorův rozvoj (polynom) druhého stupně z libovolné diferencovatelné funkce v daném bodě mnohočlenem druhého stupně.

**8.20.** Určete Taylorův polynom druhého stupně funkce $f : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = xy \cos y$ v bodě $[\pi, \pi]$. Určete, zda tečná rovina ke grafu této funkce v bodě $[\pi, \pi, f(\pi, \pi)]$ prochází bodem $[0, \pi, 0]$.

**Řešení.** Jako v předchozích příkladech zjistíme, že

$$T(x, y) = \frac{1}{2}\pi^2 y^2 - xy - \pi^3 y + \frac{1}{2}\pi^4.$$

Rovnice tečné roviny ke grafu dané funkce v bodě $[\pi, \pi]$ je dána Taylorovým polynomem prvního stupně v bodě $[\pi, \pi]$, její obecná rovnice je tedy

$$z = -\pi y - \pi x + \pi^2,$$

které zadaný bod $[0, \pi, 0]$ vyhovuje. □

*8.21.* Určete Taylorův polynom třetího stupně funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x, y, z) = x^3 y + xz^2 + xy + 1$ v bodě $[0, 0, 0]$. ○

*8.22.* Určete Taylorův polynom druhého stupně funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^2 \sin y + y^2 \cos x$ v bodě $[0, 0]$. Rozhodněte, zda tečná

Na všech $n$ sčítanců teď můžeme uplatnit větu o střední hodnotě a stejně jako v případě dvou proměnných dostáváme

$$\begin{aligned} &(c_1(t) - c_1(0))\frac{\partial f}{\partial x_1}(x_1 + c_1(\theta_1), x_2 + c_2(t), \dots, x_n + c_n(t)) \\ &+ (c_2(t) - c_2(0))\frac{\partial f}{\partial x_2}(x_1, x_2 + c_2(\theta_2), \dots, x_n + c_n(t)) \\ &\vdots \\ &+ (c_n(t) - c_n(0))\frac{\partial f}{\partial x_n}(x_1, x_2, \dots, x_n + c_1(\theta_n)), \end{aligned}$$

pro vhodné hodnoty $0 \le \theta_i \le t$. Jde o konečný součet, proto stejnou argumentací jako v případě dvou proměnných ověříme

$$\frac{d}{dt} f(x + c(t))_{t=0} = c_1'(0)\frac{\partial f}{\partial x_1}(x) + \cdots + c_n'(0)\frac{\partial f}{\partial x_n}(x).$$

Speciální volbou křivek $c(t) = x + tv$ pro směrový vektor $v$ máme ověřeno tvrzení o existenci a linearitě směrových derivací v bodě $x$.

Zároveň ale můžeme úplně stejně aplikovat větu o střední hodnotě na rozdíl

$$\begin{aligned} f(x + v) - f(x) &= d_v f(x + \theta v) \\ &= v_1\frac{\partial f}{\partial x_1}(x + \theta v) + \cdots + v_n\frac{\partial f}{\partial x_n}(x + \theta v) \end{aligned}$$

s vhodným $0 \le \theta \le 1$, kde druhá rovnost platí, podle výše odvozeného výrazu pro směrové derivace, pro dostatečně malá $v$ díky spojitosti parciálních derivací na okolí bodu $x$.

Protože jsou všechny parciální derivace spojité v bodě $x$, víme, že pro libovolně malé $\varepsilon > 0$ můžeme najít okolí $U$ počátku v $\mathbb{R}^n$ takové, že se pro $w \in U$ budou všechny parciální derivace $\frac{\partial f}{\partial x_i}(x + w)$ lišit od $\frac{\partial f}{\partial x_i}(x)$ o méně než $\varepsilon$. Dostaneme pak odhad

$$\frac{1}{\|w\|}\big(f(x + w) - f(x) - d_w f(x + \theta w)\big) \le \frac{n}{\|w\|}\|w\|\varepsilon,$$

a tedy i aproximační vlastnost diferenciálu je splněna. □

**Funkce třídy $C^1$**

Říkáme, že je funkce $f : \mathbb{R}^n \to \mathbb{R}$ třídy $C^1$ na množině $A$, jestliže má ve všech bodech této množiny spojité parciální derivace, píšeme $f \in C^1(A)$.

Právě dokázaná věta tedy říká, že je-li funkce třídy $C^1$ na nějakém okolí bodu $x$, pak má v tomto bodě diferenciál.

**8.8. Tečná rovina ke grafu funkce.** Lineární přiblížení chování funkce diferenciálem můžeme také obdobně k funkcím jedné proměnné vyjádřit ve vztahu k jejímu grafu. Jen místo tečen musíme pracovat s nadrovinami.



Pro případ funkce na $E_2$ a pevně zvoleného bodu $(x_0, y_0) \in E_2$ uvažme rovinu v $E_3$ zadanou rovnicí

$$\begin{aligned} z &= f(x_0, y_0) + df(x_0, y_0)(x - x_0, y - y_0) \\ &= f(x_0, y_0) + \frac{\partial f}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial f}{\partial y}(x_0, y_0)(y - y_0). \end{aligned}$$

Již jsme viděli, že přírůstek funkčních hodnot diferencovatelné funkce $f : E_n \to \mathbb{R}$ v bodech $x + tv$ a $x$ je vždy vyjádřen pomocí směrové derivace $d_v f$ ve vhodném bodě na jejich spojnici.

rovina ke grafu této funkce v bodě $[0, 0, 0]$ prochází bodem $[\pi, \pi, \pi]$. ○

*8.23.* Určete Taylorův polynom druhého stupně funkce $\ln(xy + 1)$ v bodě $[1, 1]$. ○

*8.24.* Určete Taylorův rozvoj druhého stupně funkce $f : \mathbb{R}^2 \to \mathbb{R}$,

$$f(x, y) = \tan(xy + y)$$

v bodě $[0, 0]$. ○

### E. Extrémy funkcí více proměnných

**8.25.** Určete stacionární body funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^2 y + y^2 x - xy$, a rozhodněte, které z těchto bodů jsou lokální extrémy a jakého druhu.

**Řešení.** První derivace jsou $f_x = 2xy + y^2 - y$, $f_y = x^2 + 2xy - x$. Položíme-li obě parciální derivace současně nule, má soustava následující řešení: $\{x = y = 0\}$, $\{x = 0, y = 1\}$, $\{x = 1, y = 0\}$, $\{x = 1/3, y = 1/3\}$, což jsou čtyři stacionární body dané funkce.

Hessián funkce $f$ je $\begin{pmatrix} 2y & 2x + 2y - 1 \\ 2x + 2y - 1 & 2x \end{pmatrix}$.

Jeho hodnoty ve stacionárních bodech jsou postupně

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix},$$

tedy první tři Hessiány jsou indefinitní, poslední pak pozitivně definitní, bod $[1/3, 1/3]$ je tedy lokálním minimem. □

**8.26.** Určete bod v rovině $x + y + 3z = 5$ ležící v $\mathbb{R}^3$, který má nejmenší vzdálenost od počátku souřadnic. A to jak metodami lineární algebry, tak metodami diferenciálního počtu.

**Řešení.** Jde o patu kolmice spuštěné z bodu $[0, 0, 0]$ na rovinu. Normála k rovině je $(t, t, 3t)$, $t \in \mathbb{R}$. Dosazením do rovnice roviny dostaneme patu kolmice $[5/11, 5/11, 15/11]$.

Alternativně minimalizujeme vzdálenost (resp. její kvadrát) bodů v rovině od počátku, tj. funkci dvou proměnných,

$$(5 - y - 3z)^2 + y^2 + z^2.$$

Položením parciálních derivací rovných nule dostaneme soustavu

$$\begin{aligned} 3y + 10z - 15 &= 0 \\ 2y + 3z - 5 &= 0, \end{aligned}$$

která má řešení jako výše. Protože víme, že minimum existuje a jedná se o jediný stacionární bod, nemusíme už ani počítat Hessián. □

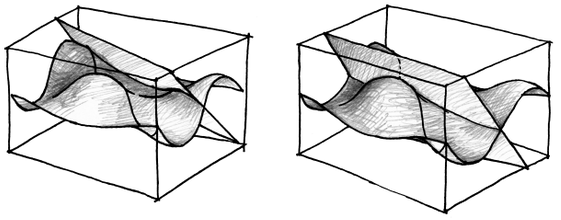
Tato rovina má tedy jako jediná ze všech rovin procházejících bodem $(x_0, y_0)$ vlastnost, že v ní leží derivace a tedy i tečny všech křivek

$$c(t) = (x(t), y(t), f(x(t), y(t))).$$

Říkáme jí *tečná rovina* ke grafu funkce $f$.

Na obrázku jsou zobrazeny dvě tečné roviny ke grafu funkce

$$f(x, y) = \sin(x)\cos(y).$$



Pro funkce $n$ proměnných definujeme tečnou rovinu jako analogii k tečné rovině k ploše v trojrozměrném prostoru. Místo zaplétání se do spousty indexů bude snad užitečná vzpomínka na afinní geometrii, kde jsme s tzv. nadrovinami již pracovali, viz odstavec 4.3.



TEČNÁ (NAD)ROVINA GRAFU FUNKCE V BODĚ

*Tečná nadrovina* ke grafu funkce $f : \mathbb{R}^n \to \mathbb{R}$ v bodě $x \in \mathbb{R}^n$ je nadrovina procházející bodem $(x, f(x))$ se zaměřením, které je grafem lineárního zobrazení $df(x) : \mathbb{R}^n \to \mathbb{R}$, tj. diferenciálu v bodě $x \in E_n$.

Definice vychází ze skutečnosti, že směrová derivace $d_v f$ je dána přírůstkem na tečné (nad)rovině odpovídajícím přírůstku argumentu $v$.

Z těchto úvah vyplývá řada analogií s funkcemi jedné proměnné. Zejména má diferencovatelná funkce $f$ na $E_n$ v bodě $x \in E_n$ nulový diferenciál tehdy a jen tehdy, když její složení s libovolnou křivkou procházející tímto bodem zde má stacionární bod, tj. ani neroste ani neklesá v lineárním přiblížení.

Jinak řečeno, tečná rovina je v takovém bodě rovnoběžná s nadrovinou proměnných (tj. její zaměření je $E_n \subset E_{n+1}$ s přidanou nulovou poslední souřadnicí). To samozřejmě neznamená, že v takovém bodě musí mít $f$ aspoň lokálně buď maximum nebo minimum. Stejně jako u funkcí jedné proměnné můžeme rozhodovat teprve podle derivací vyšších řádů.

**8.9. Derivace vyšších řádů.** Stejně jako v případě jedné proměnné, operaci derivování je možné iterovat. Tentokrát si můžeme pro každou iteraci vybrat jiný směr.



Jestliže vybereme pevný přírůstek $v \in \mathbb{R}^n$, zadává vyčíslení diferenciálů na tomto přírůstku (diferenciální) operaci na diferencovatelných funkcích $f : E_n \to \mathbb{R}$

$$f \mapsto d_v f = df(v)$$

a výsledkem je opět funkce $df(v) : E_n \to \mathbb{R}$. Jestliže je tato funkce opět diferencovatelná, může opakovat totéž s jiným přírůstkem atd. Zejména tedy můžeme pracovat s iteracemi parciálních derivací. Pro *parciální derivace druhého řádu* píšeme

$$\left(\frac{\partial}{\partial x_j} \circ \frac{\partial}{\partial x_i}\right) f = \frac{\partial^2}{\partial x_i \partial x_j} f = \frac{\partial^2 f}{\partial x_i \partial x_j}.$$

**8.27.** Určete všechny lokální extrémy funkce

$$f(x,y) = x^2 + \operatorname{arctg}^2 x + \left|\, y^3 + y \,\right|, \quad x, y \in \mathbb{R}.$$

**Řešení.** Funkci $f$ si vyjádříme jako součet $f_1 + f_2$, kde

$$f_1(x) = x^2 + \operatorname{arctg}^2 x, \quad x \in \mathbb{R}, \qquad f_2(y) = \left|\, y^3 + y \,\right|, \quad y \in \mathbb{R}.$$

Má-li mít funkce $f$ v nějakém bodě lokální extrém, pak jej musí mít také vzhledem k libovolné podmnožině svého definičního oboru. Jinak řečeno, pokud má např. v bodě $[a,b]$ maximum a my položíme $y = b$, potom funkce $f(x,b)$ jedné proměnné $x$ musí mít maximum v bodě $x = a$. Zvolme libovolně $y \in \mathbb{R}$. Pro toto pevné $y$ dostáváme funkci jedné proměnné, která je posunutím funkce $f_1$, což znamená, že má maxima a minima ve stejných bodech. Nalézt extrémy $f_1$ je ovšem snadné. Stačí si uvědomit, že tato funkce je sudá (je součtem dvou sudých funkcí, přičemž funkce $y = \operatorname{arctg}^2 x$ je součinem dvou lichých funkcí) a rostoucí pro $x \geq 0$ (kompozice i součet rostoucích funkcí je rostoucí funkce). Má proto jediný extrém, a to minimum v bodě $x = 0$. Podobně platí, že pro pevně zvolené $x$ je $f$ posunutím $f_2$ a že také funkce $f_2$ má minimum v bodě $y = 0$ jako svůj jediný extrém. Dokázali jsme tak, že $f$ může mít lokální extrém pouze v počátku. Protože zjevně

$$f(0,0) = 0, \qquad f(x,y) > 0, \quad [x,y] \in \mathbb{R}^2 \setminus \{[0,0]\},$$

funkce $f$ má v bodě $[0,0]$ ostré lokální (dokonce globální) minimum. □

**8.28.** Vyšetřete lokální extrémy funkce

$$f(x,y) = \left(x + y^2\right) \mathrm{e}^{\frac{x}{2}}, \quad x, y \in \mathbb{R}.$$

**Řešení.** Daná funkce má parciální derivace všech řádů na celém svém definičním oboru. Lokální extrém může proto nastat pouze ve stacionárních bodech, ve kterých jsou obě parciální derivace $f_x$, $f_y$ nulové. O tom, zda v těchto bodech extrém skutečně je, lze pak rozhodnout pomocí druhých derivací.

Snadno určíme

$$f_x(x,y) = \mathrm{e}^{\frac{x}{2}} + \tfrac{1}{2}\left(x + y^2\right)\mathrm{e}^{\frac{x}{2}}, \quad f_y(x,y) = 2y\,\mathrm{e}^{\frac{x}{2}}, \quad x, y \in \mathbb{R}.$$

Stacionární bod $[x,y]$ musí splňovat

$$f_y(x,y) = 0, \quad \text{tj.} \quad y = 0,$$

a dále

$$f_x(x,y) = f_x(x,0) = \mathrm{e}^{\frac{x}{2}}\left(1 + \tfrac{1}{2}x\right) = 0, \quad \text{tj.} \quad x = -2.$$

Vidíme, že existuje jediný stacionární bod $[-2,0]$.

Nyní spočítáme Hessián $Hf$ v tomto bodě. Bude-li tato matice (příslušná kvadratická forma) pozitivně definitní, jedná se o ostré lokální minimum; a při negativní definitnosti jde o ostré lokální maximum. Pokud bude indefinitní, nepůjde o extrém. Platí

V případě opakované volby $i = j$ píšeme také

$$\left(\frac{\partial}{\partial x_i} \circ \frac{\partial}{\partial x_i}\right) f = \frac{\partial^2}{\partial x_i^2} f = \frac{\partial^2 f}{\partial x_i^2}.$$

Úplně stejně postupujeme při dalších iteracích a hovoříme o *parciálních derivacích k-tého řádu*

$$\frac{\partial^k f}{\partial x_{i_1} \ldots \partial x_{i_k}}.$$

Obecněji můžeme iterovat (u dostatečně diferencovatelných funkcí) také libovolné směrové derivace, např. $d_v \circ d_w f$ pro dva pevné přírůstky $v, w \in \mathbb{R}^n$.

*k*–KRÁT DIFERENCOVATELNÉ FUNKCE

Řekneme, že je *funkce* $f : E_n \to \mathbb{R}$ *třídy* $C^k$ na množině $A$, jestliže má ve všech bodech $A$ spojité všechny parciální derivace až do řádu $k$ včetně, píšeme $f \in C^k(A)$.

Abychom si vše ukázali v co nejjednodušší formě, budeme opět pracovat chvíli v rovině $E_2$ za předpokladu spojitosti parciálních derivací druhého řádu. V rovině a prostoru se často stručně značí iterované derivace pouhými odkazy jmen proměnných v pozici indexů u funkce, např.

$$f_x = \frac{\partial f}{\partial x}, \quad f_{xx} = \frac{\partial^2 f}{\partial x^2}, \quad f_{xy} = \frac{\partial^2 f}{\partial x \partial y}, \quad f_{yx} = \frac{\partial^2 f}{\partial y \partial x}.$$



Ukážeme, že ve skutečnosti spolu za rozumných podmínek parciální derivace komutují, tzn. není potřeba dbát na pořadí, ve kterém je provádíme.

Dle předpokladu existence a spojitosti parciálních derivací existují limity

$$\begin{aligned} f_{xy}(x,y) &= \lim_{t\to 0} \frac{1}{t}\big(f_x(x,y+t) - f_x(x,y)\big) = \\ &= \lim_{t\to 0} \frac{1}{t}\Big(\lim_{s\to 0} \frac{1}{s}\big(f(x+s,y+t) - f(x,y+t) - \\ &\qquad - f(x+s,y) + f(x,y)\big)\Big). \end{aligned}$$

Protože ale limity můžeme vyjádřit pomocí libovolného výběru hodnot $t_n \to 0$ a $s_n \to 0$ a limit příslušných posloupností, bude jistě také platit

$$\begin{aligned} f_{xy}(x,y) &= \lim_{t\to 0} \frac{1}{t^2}\Big(\big(f(x+t,y+t) - f(x,y+t)\big) - \\ &\qquad - \big(f(x+t,y) - f(x,y)\big)\Big) \end{aligned}$$

a tato limitní hodnota je spojitá v $(x,y)$.

Označme si výraz, ze kterého bereme poslední limitu, jako funkci $\varphi(x,y,t)$ a zkusme jej vyjádřit pomocí parciálních derivací. Pro dočasně pevné $t$ si označme $g(x,y) = f(x+t,y) - f(x,y)$. Pak výraz v poslední velké závorce je díky větě o střední hodnotě roven

$$g(x,y+t) - g(x,y) = t \cdot g_y(x, y + t_0).$$

pro nějaké vhodné $t_0$, které je mezi nulou a $t$ (a hodnota $t_0$ závisí na $t$).

$$f_{xx}(x,y) = \tfrac{1}{2}\,\mathrm{e}^{\frac{x}{2}}\left(2+\tfrac{1}{2}\left(x+y^2\right)\right), \quad f_{yy}(x,y) = 2\,\mathrm{e}^{\frac{x}{2}},$$
$$f_{xy}(x,y) = f_{yx}(x,y) = y\,\mathrm{e}^{\frac{x}{2}}, \quad x,y \in \mathbb{R},$$

a tedy

$$Hf\,(-2,0) = \begin{pmatrix} f_{xx}\,(-2,0) & f_{xy}\,(-2,0) \\ f_{yx}\,(-2,0) & f_{yy}\,(-2,0) \end{pmatrix} = \begin{pmatrix} 1/2\mathrm{e} & 0 \\ 0 & 2/\mathrm{e} \end{pmatrix}.$$

Připomeňme, že vlastními čísly diagonální matice jsou právě hodnoty na diagonále a že pozitivní definitnost matice znamená, že všechna její vlastní čísla jsou kladná. Odtud již plyne, že v bodě $[-2,0]$ je ostré lokální minimum. □

**8.29.** Nalezněte lokální extrémy funkce

$$f(x,y,z) = x^3 + y^2 + \tfrac{z^2}{2} - 3xz - 2y + 2z, \quad x,y,z \in \mathbb{R}.$$

**Řešení.** Funkce $f$ je polynomem (mnohočlenem), a tudíž o ní víme, že má parciální derivace všech řádů. Hledejme proto stacionární body (jinde extrém být nemůže) tak, že zderivujeme $f$ postupně podle $x$, $y$, $z$ a tyto derivace položíme rovny nule. Takto dostaneme

$$3x^2 - 3z = 0, \quad \text{tj.} \quad z = x^2,$$
$$2y - 2 = 0, \quad \text{tj.} \quad y = 1,$$

a (s využitím první rovnice)

$$z - 3x + 2 = 0, \quad \text{tj.} \quad x \in \{1,2\}.$$

Existují tedy dva stacionární body $[1,1,1]$, $[2,1,4]$. Vypočtěme nyní všechny parciální derivace druhého řádu

$$f_{xx} = 6x, \quad f_{xy} = f_{yx} = 0, \quad f_{xz} = f_{zx} = -3,$$
$$f_{yy} = 2, \quad f_{yz} = f_{zy} = 0, \quad f_{zz} = 1.$$

S jejich pomocí ve stacionárních bodech snadno určíme Hessián ;

$$Hf\,(1,1,1) = \begin{pmatrix} 6 & 0 & -3 \\ 0 & 2 & 0 \\ -3 & 0 & 1 \end{pmatrix}, \quad Hf\,(2,1,4) = \begin{pmatrix} 12 & 0 & -3 \\ 0 & 2 & 0 \\ -3 & 0 & 1 \end{pmatrix}.$$

Potřebujeme zjistit, zda jsou tyto matice pozitivně definitní, negativně definitní, příp. indefinitní, abychom mohli rozhodnout, jestli a jaké jsou v nich extrémy. V případě první z matic (pro bod $[1,1,1]$) ihned vidíme vlastní číslo $\lambda = 2$. Neboť je její determinant roven $-6$ a jedná se o symetrickou matici (všechna vlastní čísla jsou reálná), matice musí mít také záporné vlastní číslo (determinant je součinem vlastních čísel). Matice $Hf\,(1,1,1)$ je tedy indefinitní – v bodě $[1,1,1]$ extrém není.

Pro matici $Hf\,(2,1,4)$ použijeme tzv. Sylvestrovo kritérium. Podle tohoto kritéria je reálná symetrická matice

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{12} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{13} & a_{23} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & a_{3n} & \cdots & a_{nn} \end{pmatrix}$$

Nyní $g_y(x,y) = f_y(x+t,y) - f_y(x,y)$, a proto můžeme psát $\varphi$ jako

$$\varphi(x,y,t) = \frac{1}{t} g_y(x, y+t_0) = \frac{1}{t}\big(f_y(x+t, y+t_0) - f_y(x, y+t_0)\big).$$

Opětovnou aplikací věty o střední hodnotě,

$$\varphi(x,y,t) = f_{yx}(x+t_1, y+t_0)$$

pro vhodné $t_1$ mezi nulou a $t$. Když ale velkou závorku rozdělíme na $(f(x+t,y+t) - f(x+t,y)) - (f(x,y+t) - f(x,y))$, dostaneme stejným postupem s funkcí $h(x,y) = f(x,y+t) - f(x,y)$ vyjádření

$$\varphi(x,y,t) = f_{xy}(x+s_0, y+s_1)$$

s obecně jinými konstantami $s_0$ a $s_1$. Protože jsou druhé parciální derivace podle našeho předpokladu spojité, musí i limita pro $t \to 0$ zaručit požadovanou rovnost

$$f_{xy}(x,y) = f_{yx}(x,y)$$

ve všech bodech $(x,y)$.

Stejný postup pro funkce $n$ proměnných dokazuje následující základní výsledek:

### Záměnnost parciálních derivací

**8.10. Věta** (Schwarzova). *Nechť $f : E_n \to \mathbb{R}$ je funkce třídy $C^k$ v okolí bodu $x \in \mathbb{R}^n$. Pak jsou všechny parciální derivace funkce $f$ v bodu $x$ až do řádu $k$ včetně nezávislé na pořadí derivování.*



Důkaz. Důkaz pro druhý řád byl proveden výše ve speciálním případě $n = 2$ a postup v obecném případě se nijak neliší.

Formálně můžeme celý důkaz vést tak, že pro každou pevnou volbu dvou souřadnic $x_i$ a $x_j$ se vždy celá diskuse jejich záměnnosti odehraje ve dvourozměrném afinním podprostoru, tj. všechny ostatní proměnné považujeme za konstantní a v argumentaci nijak aktivně nevystoupí.

U derivací vyššího řádu důkaz dokončíme indukcí podle řádu. Skutečně, každé pořadí indexů $i_1, \ldots, i_k$ lze vytvořit z pevně zvoleného záměnami sousedících dvojic. □

**8.11. Hessián.** Tak jako jsme u derivací prvního řádu zavedli diferenciál coby lineární formu $df(x)$ přibližující nejlépe v daném bodu $x$ funkci $f$, budeme nyní chtít porozumět kvadratickému přiblížení funkcí $f : E_n \to \mathbb{R}$.



### Hessián

Je-li $f : \mathbb{R}^n \to \mathbb{R}$ libovolná dvakrát diferencovatelná funkce, nazýváme symetrickou matici funkcí

$$Hf(x) = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}(x)\right) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1 \partial x_1}(x) & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n}(x) \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1}(x) & \cdots & \frac{\partial^2 f}{\partial x_n \partial x_n}(x) \end{pmatrix}$$

*Hessián funkce $f$* v bodě $x$.

pozitivně definitní, právě když všechny vedoucí hlavní minory $A$, tj. determinanty

$$d_1 = |a_{11}|\,,\ d_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix},\ d_3 = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{vmatrix},\ \ldots,\ d_n = |A|,$$

jsou kladné, a je negativně definitní tehdy a jenom tehdy, když je

$$d_1 < 0, \quad d_2 > 0, \quad d_3 < 0, \quad \ldots, \quad (-1)^n d_n > 0.$$

Z nerovností

$$|12| = 12 > 0, \quad \begin{vmatrix} 12 & 0 \\ 0 & 2 \end{vmatrix} = 24 > 0, \quad \begin{vmatrix} 12 & 0 & -3 \\ 0 & 2 & 0 \\ -3 & 0 & 1 \end{vmatrix} = 6 > 0,$$

vyplývá, že matice $Hf\,(2, 1, 4)$ je pozitivně definitní – v bodě $[2, 1, 4]$ je ostré lokální minimum. □

**8.30.** Stanovte lokální extrémy funkce

$$z = \left(x^2 - 1\right)\left(1 - x^4 - y^2\right), \quad x, y \in \mathbb{R}.$$

**Řešení.** Opět spočítáme parciální derivace $z_x$ a $z_y$ a položíme je rovny nule. Takto obdržíme rovnice

$$-6x^5 + 4x^3 + 2x - 2xy^2 = 0, \quad \left(x^2 - 1\right)(-2y) = 0$$

s řešeními $[x, y] = [0, 0]$, $[x, y] = [1, 0]$, $[x, y] = [-1, 0]$. Doplňme, že k nalezení řešení stačilo určit reálné kořeny $1, -1$ polynomu $-6x^4 + 4x^2 + 2$ pomocí substituce $u = x^2$. Nyní vypočítáme druhé parciální derivace

$$z_{xx} = -30x^4 + 12x^2 + 2 - 2y^2,\ z_{xy} = z_{yx} = -4xy,\ z_{yy} = -2\left(x^2 - 1\right)$$

a ve stacionárních bodech vyčíslíme Hessián:

$$Hz\,(0, 0) = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad Hz\,(1, 0) = Hz\,(-1, 0) = \begin{pmatrix} -16 & 0 \\ 0 & 0 \end{pmatrix}.$$

Vidíme, že první z matic je pozitivně definitivní, a tudíž je v počátku ostré lokální minimum.

Zbývající dvě matice jsou ale negativně semidefinitní. Nelze tedy na základě druhých parciálních derivací s určitostí říci, zda je v bodech $[1, 0]$, $[-1, 0]$ extrém. Zkoumejme proto funkční hodnoty v okolích těchto bodů. Platí

$$z\,(1, 0) = z\,(-1, 0) = 0, \qquad z\,(x, 0) < 0 \quad \text{pro } x \in (-1, 1).$$

Uvažujme dále $y$ v závislosti na $x \in (-1, 1)$ dané předpisem $y = \sqrt{2\left(1 - x^4\right)}$ splňujícím, že $y \to 0$ pro $x \to \pm 1$. Pro tuto volbu je však

$$z\left(x, \sqrt{2\left(1 - x^4\right)}\right) = \left(x^2 - 1\right)\left(x^4 - 1\right) > 0, \quad x \in (-1, 1).$$

Ukázali jsme, že v libovolně malých okolích bodů $[1, 0]$, $[-1, 0]$ nabývá $z$ hodnot větších i menších, než je funkční hodnota v těchto bodech. Nejedná se tak o extrémy. □

Z předchozích úvah jsme již viděli, že vynulování diferenciálu v bodě $(x, y) \in E_2$ zaručuje stacionární chování podél všech křivek v tomto bodu. Hessián

$$Hf(x, y) = \begin{pmatrix} f_{xx}(x, y) & f_{xy}(x, y) \\ f_{xy}(x, y) & f_{yy}(x, y) \end{pmatrix}$$

hraje roli druhé derivace. Pro každou parametrizovanou přímku

$$c(t) = (x(t), y(t)) = (x_0 + \xi t, y_0 + \eta t)$$

budou totiž mít funkce jedné proměnné

$$\alpha(t) = f(x(t), y(t))$$

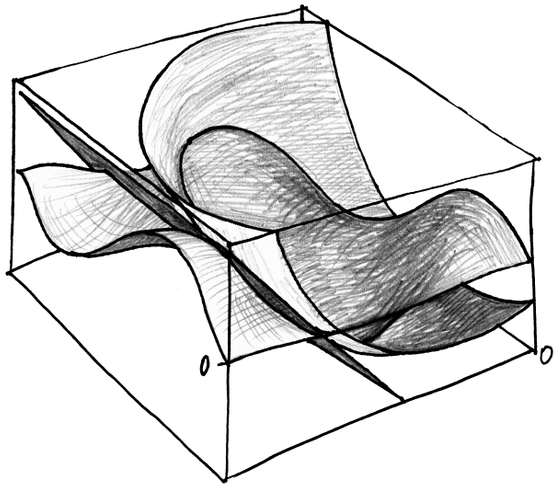
$$\beta(t) = f(x_0, y_0) + \frac{\partial f}{\partial x}(x_0, y_0)\xi t + \frac{\partial f}{\partial y}(x_0, y_0)\eta t + \frac{t^2}{2}\left(f_{xx}(x_0, y_0)\xi^2 + 2f_{xy}(x_0, y_0)\xi\eta + f_{yy}(x_0, y_0)\eta^2\right)$$

stejné derivace do druhého řádu včetně v bodě $t = 0$ (přepočtěte si!). Funkci $\beta$ přitom můžeme zapsat vektorově jako

$$\beta(t) = f(x_0, y_0) + df(x_0, y_0)\begin{pmatrix} \xi \\ \eta \end{pmatrix} t + \frac{1}{2}(\xi\ \eta)Hf(x_0, y_0)\begin{pmatrix} \xi \\ \eta \end{pmatrix} t^2$$

neboli $\beta(t) = f(x_0, y_0) + df(x_0, y_0)(v)t + \frac{1}{2}Hf(x_0, y_0)(v, v)t^2$, kde $v = (\xi, \eta)$ je přírůstek zadaný derivací křivky $c(t)$ a Hessián je použit jako symetrická 2–forma.

To je vyjádření, které již určitě připomíná Taylorovu větu funkcí jedné proměnné, přesněji řečeno kvadratické přiblížení funkce Taylorovým polynomem druhého řádu. Na následujícím obrázku je vynesena jak tečná rovina tak toto kvadratické přiblížení v jednom bodu pro funkci $f(x, y) = \sin(x)\cos(y)$.




**8.12. Taylorova věta.** Vícerozměrná verze Taylorovy věty je také příkladem matematického tvrzení, kde složitou částí je nalezení správné formulace. Důkaz je už pak docela snadný.



Budeme postupovat ve výše naznačeném směru a zavedeme si značení pro jednotlivé části $D^k f$ aproximací vyšších řádů pro funkce $f : E_n \to \mathbb{R}^n$. Budou to vždy $k$–lineární výrazy v přírůstcích a nás bude zajímat jen jejich vyčíslení na $k$ stejných hodnotách.

Již jsme diskutovali diferenciál $D^1 f = df$ v prvním řádu a Hessián $D^2 f = Hf$ v řádu druhém. Obecně pro funkce $f : E_n \to$

**8.31.** Rozhodněte, zda má polynom

$$p(x, y) = x^6 + y^8 + y^4x^4 - x^6y^5$$

ve stacionárním bodě $[0, 0]$ lokální extrém.

**Řešení.** Snadno lze ověřit, že parciální derivace $p_x$ a $p_y$ jsou v počátku skutečně nulové. Také všechny parciální derivace $p_{xx}, p_{xy}, p_{yy}$ jsou ale v bodě $[0, 0]$ rovny nule. Hessián $Hp\,(0, 0)$ je tudíž současně pozitivně i negativně semidefinitní. Jednoduchá úvaha však ihned dává výsledek. Všimněme si např., že je $p(0, 0) = 0$ a současně

$$p(x, y) = x^6\left(1 - y^5\right) + y^8 + y^4x^4 > 0$$

pro $[x, y] \in \mathbb{R} \times (-1, 1) \setminus \{[0, 0]\}$. Zadaný polynom má proto v počátku lokální minimum. □

*8.32.* Určete lokální extrémy funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x, y, z) = x^2y + y^2z + x - z$ na $\mathbb{R}^3$. ○

*8.33.* Určete lokální extrémy funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x, y, z) = x^2y - y^2z + 4x + z$ na $\mathbb{R}^3$. ○

*8.34.* Určete lokální extrémy funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x, y, z) = xz^2 + y^2z - x + y$ na $\mathbb{R}^3$. ○

*8.35.* Určete lokální extrémy funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x, y, z) = y^2z - xz^2 + x + 4y$ svého minima na $\mathbb{R}^3$. ○

*8.36.* Určete lokální extrémy funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^2y + x^2 + 2y^2 + y$ na $\mathbb{R}^2$ ○

*8.37.* Určete lokální extrémy funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^2y + 2y^2 + 2y$ na $\mathbb{R}^2$. ○

*8.38.* Určete lokální extrémy funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^2 + xy + 2y^2 + y$ na $\mathbb{R}^2$. ○

*8.39.* Určete lokální extrémy funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^2 + xy - 2y^2 + y$ na $\mathbb{R}^2$. ○

### F. Funkce a zobrazení dané implicitně

**8.40.** Buď dána funkce $F : \mathbb{R}^2 \to \mathbb{R}$, $F(x, y) = xy \sin\left(\frac{\pi}{2}xy^2\right)$. Ukažte, že rovnost $F(x, y) = 1$ zadává v nějakém okolí $U$ bodu $[1, 1]$ implicitně funkci $f : U \to \mathbb{R}$ tak, že platí $F(x, f(x)) = 1$ pro $x \in U$. Určete $f'(1)$.

**Řešení.** Funkce je diferencovatelná na celém $\mathbb{R}^2$, tím spíše na nějakém okolí bodu $[1, 1]$. Vyčísleme $F_y$ v bodě $[1, 1]$:

$$F_y(x, y) = x \sin\left(\frac{\pi}{2}xy^2\right) + \pi x^2y^2 \cos\left(\frac{\pi}{2}xy^2\right),$$

tedy $F_y(1, 1) = 1 \neq 0$, tudíž podle věty 8.18 předpis $F(x, y) = 1$ zadává implicitně na okolí bodu $(1, 1)$ funkci $f : U \to \mathbb{R}$, definovanou

$\mathbb{R}$, body $x = (x_1, \ldots, x_2) \in E_n$ a přírůstky $v = (\xi_1, \ldots, \xi_n)$ klademe

$$D^k f(x)(v) = \sum_{1 \le i_1, \ldots, i_k \le n} \frac{\partial^k f}{\partial x_{i_1} \ldots \partial x_{i_k}}(x_1, \ldots, x_n) \cdot \xi_{i_1} \cdots \xi_{i_k}.$$

Všimněme si, že skutečně jde v tomto výrazu o vyčíslení $k$–lineární formy na $k$ kopiích stejného argumentu $v$.

Názorným příkladem (s využitím symetrií parciálních derivací) je pro $E_2$ výraz třetího řádu

$$D^3 f(x, y)(\xi, \eta) = \frac{\partial^3 f}{\partial x^3}\xi^3 + 3\frac{\partial^3 f}{\partial x^2 \partial y}\xi^2\eta + 3\frac{\partial^3 f}{\partial x \partial y^2}\xi\eta^2 + \frac{\partial^3 f}{\partial y^3}\eta^3$$

a obecně

$$D^k f(x, y)(\xi, \eta) = \sum_{\ell=0}^{k} \binom{k}{\ell} \frac{\partial^k f}{\partial x^{k-\ell}\, \partial y^\ell} \xi^{k-\ell}\eta^\ell.$$

#### Taylorův rozvoj se zbytkem

**Věta.** *Nechť $f : E_n \to \mathbb{R}$ je funkce třídy $C^k$ v okolí $\mathcal{O}_\delta(x)$ bodu $x \in E_n$. Pro každý přírůstek $v \in \mathbb{R}^n$ s velikostí $\|v\| < \delta$ pak existuje číslo $0 \le \theta \le 1$ takové, že*

$$f(x + v) = f(x) + D^1 f(x)(v) + \frac{1}{2!}D^2 f(x)(v) + \cdots + \frac{1}{(k-1)!}D^{k-1} f(x)(v) + \frac{1}{k!}D^k f(x + \theta \cdot v)(v).$$

Důkaz. Pro přírůstek $v \in \mathbb{R}^n$ uvažujme parametrizovanou přímku $c(t) = x + tv$ v $E_n$ a zkoumejme funkci $\varphi : \mathbb{R} \to \mathbb{R}$ definovanou složením $\varphi(t) = (f \circ c)(t)$. Taylorova věta pro funkce jedné proměnné říká (viz Věta 6.4)



$$\varphi(t) = \varphi(0) + \varphi'(0)t + \ldots + \frac{1}{(k-1)!}\varphi^{(k-1)}(0)t^{k-1} + \frac{1}{k!}\varphi^{(k)}(\theta)t^k.$$

Zbývá nám tedy jen ověřit, že postupným derivováním složené funkce $\varphi$ dostaneme právě požadovaný vztah. To lze vcelku snadno provést indukcí přes řád $k$.

Pro $k = 1$ splývá Taylorova věta s již několikrát využitým důsledkem věty o střední hodnotě aplikované na směrovou derivaci. Při jeho odvození jsme vyšli ze vztahu

$$\frac{d}{dt}\varphi(t) = \frac{\partial f}{\partial x_1}(x(t)) \cdot x_1'(t) + \cdots + \frac{\partial f}{\partial x_n}(x(t)) \cdot x_n'(t),$$

který platí pro každou spojitě diferencovatelnou křivku a funkci $f$. To znamená, že

$$D^1 f(c(t))(v) = D^1 f(c(t))(c'(t))$$

pro všechna $t$ v okolí nuly. Stejně budeme postupovat pro funkce $D^\ell f$. Místo přírůstku $v$ můžeme psát $c'(t)$ a zapamatujme si, že další derivování $c(t)$ již vede identicky na nulu všude, tj. $c''(t) = 0$ pro všechna $t$ (protože jde o parametrizovanou přímku).

na nějakém okolí bodu (čísla) 1. Navíc je

$$F_x(x, y) = y \sin\left(\frac{\pi}{2}xy^2\right) + \frac{\pi}{2}xy^3 \cos\left(\frac{\pi}{2}xy^2\right),$$

a tak pro hodnotu derivace funkce $f$ v bodě 1 platí

$$f'(1) = -\frac{F_x(1, 1)}{F_y(1, 1)} = -\frac{1}{1} = -1. \qquad \square$$

**Poznámka.** Všimněte si, že i když neumíme z rovnice $F(x, f(x)) = 1$ explicitně vyjádřit funkci $f$, tak umíme vyčíslit hodnotu její derivace v bodě 1.

**8.41.** Ukažte, že funkce $F : \mathbb{R}^2 \to \mathbb{R}$,

$$F(x, y) = e^x \sin(y) + y - \pi/2 - 1$$

definuje předpisem $F(x, y) = 0$ v okolí bodu $[0, \pi/2]$ implicitně proměnnou $y$ jako funkci proměnné $x$, $y = f(x)$. Určete $f'(0)$.

**Řešení.** Funkce je diferencovatelná v okolí bodu $[0, \pi/2]$, navíc $F_y = e^x \cos y + 1$, $F(0, \pi/2) = 1 \neq 0$, tudíž daný předpis skutečně zadává na nějakém okolí bodu $[0, \pi/2]$ funkci $f : U \to \mathbb{R}$. Dále je $F_x = e^x \sin y$, $F_x(0, \pi/2) = 1$ a pro její derivaci v bodě 0 platí:

$$f'(0) = -\frac{F_x(0, \pi/2)}{F_y(0, \pi/2)} = -\frac{1}{1} = -1. \qquad \square$$

**8.42.** Buď

$$F(x, y, z) = \sin(xy) + \sin(yz) + \sin(xz).$$

Ukažte, že předpis $F(x, y, z) = 0$ zadává v okolí bodu $[\pi, 1, 0] \in \mathbb{R}^3$ implicitně funkci $z(x, y) : \mathbb{R}^2 \to \mathbb{R}$ takovou, že $F(x, y, z(x, y)) = 0$.

Určete $z_x(\pi, 1)$ a $z_y(\pi, 1)$.

**Řešení.** Určíme $F_z = y\cos(yz) + x\cos(xz)$, $F_z(\pi, 1, 0) = \pi + 1 \neq 0$ a funkce $z(x, y)$ je předpisem $F(x, y, z(x, y)) = 0$ na nějakém okolí bodu $[\pi, 1, 0]$ zadána. Pro hledané hodnoty parciálních derivací potřebujeme spočítat hodnoty obou zbylých parciálních derivací funkce $F$ v bodě $[\pi, 1, 0]$.

$$\begin{aligned} F_x(x, y, z) &= y\cos(xy) + z\cos(xz) \;\; F_x(\pi, 1, 0) = -1, \\ F_y(x, y, z) &= x\cos(xy) + z\cos(yz) \;\; F_y(\pi, 1, 0) = -\pi, \end{aligned}$$

odkud

$$\begin{aligned} z_x(\pi, 1) &= -\frac{F_x(\pi, 1, 0)}{F_z(\pi, 1, 0)} = \frac{1}{\pi + 1}, \\ z_y(\pi, 1) &= -\frac{F_y(\pi, 1, 0)}{F_z(\pi, 1, 0)} = \frac{\pi}{\pi + 1}. \end{aligned}$$

$\square$

Předpokládejme, že

$$D^\ell f(x)(v) = \sum_{1 \le i_1, \ldots, i_\ell \le n} \left( \frac{\partial^\ell f}{\partial x_{i_1} \ldots \partial x_{i_\ell}}(x_1(t), \ldots, x_n(t)) \cdot \right.$$
$$\left. \cdot\, x'_{i_1}(t) \cdots x'_{i_\ell}(t) \right)$$

a spočtěme totéž pro $\ell + 1$. Derivování složené funkce dá podle výše odvozeného vztahu pro derivaci prvního řádu v daném směru a podle pravidla o derivaci součinu (viz Věta 5.33)

$$\begin{aligned} &\frac{d}{dt} D^\ell f(c(t))(c'(t)) = \\ &= \frac{d}{dt} \sum_{1 \le i_1, \ldots, i_\ell \le n} \left( \frac{\partial^\ell f}{\partial x_{i_1} \ldots \partial x_{i_\ell}}(x_1(t), \ldots, x_n(t)) \right. \\ &\qquad \left. \cdot\, x'_{i_1}(t) \cdots x'_{i_\ell}(t) \right) = \\ &= \sum_{1 \le i_1, \ldots, i_\ell \le n} \left( \sum_{j=1}^{n} \frac{\partial^{\ell+1} f}{\partial x_{i_1} \ldots \partial x_{i_\ell} \partial x_j}(x_1(t), \ldots, x_n(t)) \right. \\ &\qquad \left. \cdot\, x'_j(t) \cdot x'_{i_1}(t) \cdots x'_{i_\ell}(t) \right) + 0 \end{aligned}$$

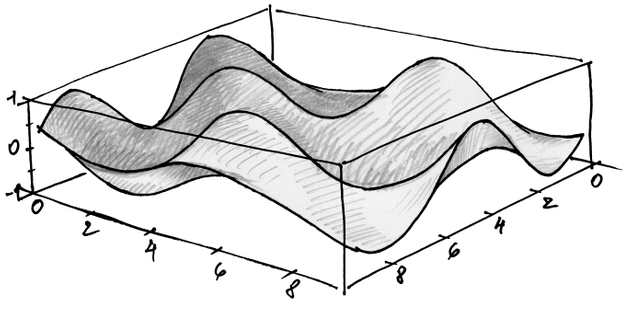
a to skutečně je požadovaný vztah pro řád $\ell + 1$. Taylorova věta nyní vyplývá z vyčíslení v bodě $t = 0$ a dosazení do rovnosti pro $\varphi$ na začátku tohoto důkazu. $\square$

**8.13. Lokální extrémy funkcí více proměnných.** Zkusme se nyní s pomocí diferenciálu a Hessiánu podívat na lokální maxima a minima funkcí na $E_n$. Stejně jako v případě funkce jedné proměnné řekneme o vnitřním bodu $x_0 \in E_n$ definičního oboru funkce $f$, že je (lokálním) *maximem* nebo *minimem*, jestliže existuje jeho okolí $U$ takové, že pro všechny body $x \in U$ splňuje funkční hodnota $f(x) \le f(x_0)$ nebo $f(x) \ge f(x_0)$. Pokud nastává v předchozích nerovnostech ostrá nerovnost pro všechny $x \neq x_0$, hovoříme o *ostrém extrému*.



Pro jednoduchost budeme nadále předpokládat, že naše funkce $f$ má spojité parciální derivace prvního i druhého řádu na svém definičním oboru. Nutnou podmínkou pro existenci maxima nebo minima v bodě $x_0$ je vymizení diferenciálu v tomto bodě, tj. $df(x_0) = 0$. Skutečně, pokud je $df(x_0) \neq 0$, pak existuje směr $v$, ve kterém je $d_v f(x_0) \neq 0$. Pak ovšem nutně podél přímky $x_0 + tv$ na jednu stranu od bodu $x_0$ hodnota funkce roste a na druhou klesá, viz odstavec 5.32 na straně 263.

Vnitřní bod $x \in E_n$ definičního oboru funkce $f$, ve kterém je diferenciál $df(x)$ nulový nazýváme *stacionární bod funkce* $f$.



**8.43.** Ukažte, že zobrazení $F : \mathbb{R}^3 \to \mathbb{R}^2$, $F(x, y, z) = (f(x, y, z), g(x, y, z)) = (e^{x \sin y}, xyz)$ zadává v okolí bodu $[1, \pi, 1]$ předpisem $F(x, c_1(x), c_2(x)) = (0, 0)$ křivku $c : \mathbb{R} \to \mathbb{R}^2$. Určete tečný vektor této křivky v bodě 1.

**Řešení.** Určeme čtvercovou matici parciálních derivací zobrazení $F$ podle proměnných $y$ a $z$:

$$H(x, y, z) = \begin{pmatrix} f_y & f_z \\ g_y & g_z \end{pmatrix} = \begin{pmatrix} x \cos y\, e^{x \sin y} & 0 \\ xz & xy \end{pmatrix},$$

tedy $H(1, \pi, 1) = \begin{pmatrix} -1 & 0 \\ 1 & \pi \end{pmatrix}$ a $\det H(1, \pi, 1) = -\pi \neq 0$, tudíž podle věty o implicitním zobrazení (viz 8.18) zadává předpis $F(x, c_1(x), c_2(x)) = (0, 0)$ na okolí bodu $[1, \pi, 1]$ křivku $(c_1(x), c_2(x))$ definovanou na nějakém okolí bodu $[1, \pi]$. Abychom vyčíslili její tečný vektor v tomto bodě, musíme ještě určit v tomto bodě (sloupcový) vektor $(f_x, g_x)$.

$$\begin{pmatrix} f_x \\ g_x \end{pmatrix} = \begin{pmatrix} \sin y\, e^{x \sin y} \\ yz \end{pmatrix}, \quad \begin{pmatrix} f_x(1, \pi, 1) \\ g_x(1, \pi, 1) \end{pmatrix} = \begin{pmatrix} 0 \\ \pi \end{pmatrix},$$

hledaný tečný vektor je tak

$$\begin{pmatrix} (c_1)_x(1) \\ (c_2)_x(1)) \end{pmatrix} = \begin{pmatrix} f_y(1, \pi, 1) & f_z(1, \pi, 1) \\ g_y(1, \pi, 1) & g_z(1, \pi, 1) \end{pmatrix}^{-1} \begin{pmatrix} f_x(1, \pi, 1 \\ g_x(1, \pi, 1) \end{pmatrix} =$$
$$= \begin{pmatrix} -1 & 0 \\ 1 & \pi \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ \pi \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ \frac{1}{\pi} & \frac{1}{\pi} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

□

## G. Vázané extrémy

Začněme s tak trochu netypickým optimalizačním problémem

**8.44.** Sázková kancelář vypisuje kurzy na výhru jednoho, či druhého hráče v tenisovém zápase. Hráč $A$ má kurz $a : 1$, hráč $B$ má kurz $b : 1$, tj. v případě sázky $x$ Kč na hráče $A$ obdrží v případě jeho výhry sázející $ax$ Kč, obdobně pro hráče $B$ (poplatky zanedbáváme). Jaká je nutná podmínka pro (kladná reálná) čísla $a$ a $b$, aby si sázející vhodným rozdělením vsazených peněz mezi sázky na výhru $A$ a na výhru $B$ nemohl zaručit zisk, ať vyhraje kdokoliv (např. při kurzu $1,4 : 1$ na výhru hráče $A$ a $5 : 1$ na výhru $B$ by si sázející při sázce 3 Kč na výhru $B$ a 7 Kč na výhru $A$ zajistil vždy zisk).

**Řešení.** Nechť má sázející k dispozici $P$ Kč. Svoji sázku může rozdělit na $kP$ a $(1-k)P$ korun, kde $k \in (0, 1)$. Jeho výhra pak bude buď $akP$ korun v případě výhry hráče $A$, nebo $b(1-k)P$ korun v případě výhry hráče $B$. Při daném rozdělení si sázející vždy zaručí výhru odpovídající menší z těchto částek, celkový zisk (ztráta) pak bude dána ještě odečtením částky $P$. Protože $a, b$ i $P$ jsou kladná reálná čísla, je funkce $akP$ rostoucí a funkce $b(1-k)P$ klesající vzhledem ke $k$. Pro $k = 0$ je větší $b(1-k)P$, pro $k = 1$ je pak větší $(1-k)P$. Maximum z minim

Budeme opět chvíli pracovat s jednoduchou funkcí v $E_2$ abychom závěry přímo mohli ilustrovat. Uvažme funkci $f(x, y) = \sin(x)\cos(y)$, která už byla předmětem diskuse a obrázků v odstavcích 8.9 a 8.8. Svým tvarem tato funkce připomíná známá kartonová plata na vajíčka, je tedy předem zřejmé, že najdeme řadu extrémů, ale ještě více stacionárních bodů, které ve skutečnosti extrémy nebudou (ta „sedýlka“ viditelná na obrázku).
Spočtěme si tedy první a poté potřebné druhé derivace:

$$f_x(x, y) = \cos(x)\cos(y), \quad f_y(x, y) = -\sin(x)\sin(y)$$

a obě derivace budou zároveň nulové pro dvě sady bodů

(1) $\cos(x) = 0$, $\sin(y) = 0$, to je $(x, y) = (\frac{2k+1}{2}\pi, \ell\pi)$, pro libovolné $k, \ell \in \mathbb{Z}$
(2) $\cos(y) = 0$, $\sin(x) = 0$, to je $(x, y) = (k\pi, \frac{2\ell+1}{2}\pi)$, pro libovolné $k, \ell \in \mathbb{Z}$.

Druhé parciální derivace jsou

$$Hf(x, y) = \begin{pmatrix} f_{xx} & f_{xy} \\ f_{xy} & f_{yy} \end{pmatrix}(x, y)$$
$$= = \begin{pmatrix} -\sin(x)\cos(y) & -\cos(x)\sin(y) \\ -\cos(x)\sin(y) & -\sin(x)\cos(y) \end{pmatrix}.$$

V našich dvou sadách stacionárních bodů tedy dostáváme následující Hessiány:

(1) $Hf(k\pi + \frac{\pi}{2}, \ell\pi) = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, přičemž znaménko $-$ nastává, když parity $k$ a $\ell$ jsou stejné a naopak pro $+$;
(2) $Hf(k\pi, \ell\pi + \frac{\pi}{2}) = \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, přičemž znaménko $-$ nastává, když parity $k$ a $\ell$ jsou stejné a naopak pro $+$.

Když se nyní podíváme na tvrzení Taylorovy věty pro řád $k = 2$, dostáváme v okolí jednoho ze stacionárních bodů $(x_0, y_0)$ pro body se souřadnicemi $x = x_0 + u$, $y = y_0 + v$

$$f(x, y) = f(x_0, y_0) + \frac{1}{2} Hf(x_0 + \theta u, y_0 + \theta v)(u, v),$$

kde $Hf$ nyní vnímáme jako kvadratickou formu vyčíslenou na přírůstku $(u, v)$. Protože naše funkce má spojitý Hessián (tj. spojité parciální derivace do druhého řádu včetně), a matice Hessiánu jsou nedegenerované, nastane lokální maximum tehdy a jen tehdy, když náš bod $(x_0, y_0)$ patří do první skupiny se stejnými paritami $k$ a $\ell$. Když budou parity opačné, pak bod z první skupiny bude naopak bodem lokálního minima.

Naopak, Hessián u druhé skupiny bodů se vždy vyčíslí kladně na některých přírůstcích a záporně na jiných. Proto se tak bude chovat i celá funkce $f$ v malém okolí daného bodu.



Abychom mohli zformulovat obecné tvrzení o Hessiánu a lokálních extrémech ve stacionárních bodech, musíme připomenout diskusi o kvadratických formách v odstavcích 4.31–4.32 v kapitole o afinní geometrii. Zavedli jsme tam pro kvadratickou formu $h : \mathbb{R}_n \to \mathbb{R}$ následující přívlastky

- *positivně definitní*, je-li $h(u) > 0$ pro všechny $u \neq 0$
- *positivně semidefinitní*, je-li $h(u) \geq 0$ pro všechny $u \in V$
- *negativně definitní*, je-li $h(u) < 0$ pro všechny $u \neq 0$
- *negativně semidefinitní*, je-li $h(u) \leq 0$ pro všechny $u \in V$
- *indefinitní*, je-li $h(u) > 0$ a $f(v) < 0$ pro vhodné $u, v \in \mathbb{R}^n$.

Zavedli jsme také nějaké metody, které umožňují přímo zjistit, zda daná forma má některý z těchto přívlastků.

z čísel $akP$ a $b(1-k)P$ tedy nastane pro $k \in (0,1)$ a to pro to $k_0$, pro které $ak_0P = b(1-k_0)P$, odkud $k_0 = \frac{b}{a+b}$. Sázková kancelář, aby nezkrachovala, pak musí volit $a, b$ tak, aby $ak_0P = b(1-k_0)P < P$, neboli $ak_0 < 1$, čili $ab < a+b$. □

Při této vázané optimalizaci jsme se obešli bez diferenciálního počtu. V dalších příkladech už tomu tak nebude.

**8.45.** Najděte extrémní hodnoty funkce

$$h(x,y,z) = x^3 + y^3 + z^3,$$

jednak na jednotkové sféře $S$ v $\mathbb{R}^3$ dané rovnicí

$$F(x,y,z) = x^2 + y^2 + z^2 - 1,$$

a také na kružnici dané průnikem této sféry s rovinou

$$G(x,y,z) = x + y + z.$$

**Řešení.** Začněme hledáním stacionárních bodů pro funkci $h$ na sféře $S$. Výpočtem příslušných gradientů (např. $\operatorname{grad} h(x,y,z) = (3x^2, 3y^2, 3z^2)$) dostaneme systém rovnic

$$\begin{aligned} 0 &= 3x^2 - 2\lambda x,\\ 0 &= 3y^2 - 2\lambda y,\\ 0 &= 3z^2 - 2\lambda z,\\ 0 &= x^2 + y^2 + z^2 - 1, \end{aligned}$$

což je systém čtyř rovnic o čtyřech proměnných. Před řešením tohoto systému si zkusme odhadnout, kolik lokálních vázaných extrémů bychom měli čekat. Určitě bude $h(P)$ v absolutní hodnotě rovno na jednotkové sféře nejvýše jedné a to nastane ve všech průnicích souřadných os s $S$. Máme tedy pravděpodobně 6 lokálních extrémů. Dále uvnitř každé osminy sféry vytčené souřadnými rovinami může, ale nemusí, být další extrém. Jednotlivé kvadranty lze snadno oparametrizovat a průběh funkce $h$ coby funkce dvou parametrů ověřit standardním způsobem (nebo si nechat vykreslit třeba programu v Maple).

Řešením systému (ať už algebraicky nebo opět v programu Maple) obdržíme ve skutečnosti spoustu stacionárních bodů. Kromě šesti, o kterých už víme (dvě souřadnice nulové a jedna $\pm 1$) a u kterých je $\lambda = \pm\frac{3}{2}$, jsou to např. ještě body

$$P_\pm = \pm\left(\frac{\sqrt{3}}{3}, \frac{\sqrt{3}}{3}, \frac{\sqrt{3}}{3}\right),$$

ve kterých skutečně nastává lokální extrém.

Jestliže omezíme náš zájem na body kružnice $K$, musíme přidat další funkci $G$ jeden další volný parametr $\eta$ coby koeficient u jejího

Taylorův rozvoj se zbytkem okamžitě dává platnost následující věty:

**Věta.** *Nechť $f : E_n \to \mathbb{R}$ je funkce třídy $C^2$ v okolí svého stacionárního bodu $x \in E_n$.*[2] *Potom*

*(1) $f$ má v $x$ ostré lokální minimum, je-li $Hf(x)$ positivně definitní,*

*(2) $f$ má v $x$ ostré lokální maximum, je-li $Hf(x)$ negativně definitní,*

*(3) $f$ nemá v bodě $x$ lokální extrém je-li $Hf(x)$ indefinitní.*

Důkaz. Taylorův rozvoj druhého řádu se zbytkem aplikovaný na naši funkci $f(x_1, \dots, x_n)$, libovolný bod $x = (x_1, \dots, x_n)$ a libovolný přírůstek $v = (v_1, \dots, v_n)$, takové že jak $x$ tak $x+v$ jsou v definičním oboru funkce $f$, říká



$$f(x+v) = f(x) + df(x)(v) + \frac{1}{2}Hf(x+\theta\cdot v)(v),$$

pro vhodné reálné $0 \le \theta \le 1$. Dle předpokladu o nulové hodnotě diferenciálu je tedy

$$f(x+v) = f(x) + \frac{1}{2}Hf(x+\theta\cdot v)(v).$$

Podle našeho předpokladu je kvadratická forma $Hf(x)$ spojitě závislá na bodu $x$ a definitnost, resp. indefinitnost, kvadratických forem je rozhodnutelná podle znaménka vedoucích hlavních subdeterminantů matice $Hf$, viz Sylvestrovo kritérium v odstavci 4.32. Samotný determinant je ale coby polynomiální výraz v koeficientech matice spojitou funkcí, proto nenulovost a znaménka zkoumaných determinantů v dostatečně malém okolí bodu $x$ budou stejná jako v bodě $x$ samotném.

Zejména tedy pro pozitivně definitní $Hf(x)$ máme ve stacionárním bodu $x$ zajištěno, že $f(x+v) > f(x)$ pro dostatečně malá $v$, jde tedy o ostré minimum funkce $f$ v bodě $x$. Analogicky pro negativní definitnost. V případě indefinitní formy $Hf(x)$ budou existovat směry $v, w$ ve kterých $f(x+v) > f(x)$ a $f(x+w) < f(x)$, a tedy v diskutovaném stacionárním bodu extrém žádný nenastává. □

Všimněme si, že věta nedává žádný výsledek, pokud je Hessián funkce ve zkoumaném bodě degenerovaný a přitom není indefinitní. Důvod je opět stejný jako u funkcí jedné proměnné. V takových případech totiž existují směry, ve kterých první i druhá derivace zmizí a my proto v tomto řádu přiblížení neumíme poznat, zda se funkce bude chovat jako $t^3$ nebo jako $\pm t^4$, dokud nespočteme alespoň v potřebných směrech derivace vyšší.

Zároveň si povšimněme, že i v bodech, kde je diferenciál nenulový, má definitnost Hessiánu $Hf(x)$ podobné důsledky jako nenulovost druhé derivace u funkce jedné proměnné. Skutečně, pro funkci $f : \mathbb{R}^n \to \mathbb{R}$ výraz

$$z(x+v) = f(x) + df(x)(v)$$

zadává tečnou nadrovinu ke grafu funkce $f$ v prostoru $\mathbb{R}^{n+1}$, a proto Taylorova věta druhého řádu se zbytkem, tak jak byla využita v důkazu, ukazuje, že při pozitivní definitnosti Hessiánu jsou všechny hodnoty funkce $f$ v dostatečně malém okolí bodu $x$ nad hodnotami na tečné nadrovině, tj. celý graf je v dostatečně malém okolí nad tečnou nadrovinou. V případě negativní definitnosti je

[2] Ve skutečnosti důkaz této věty vyžaduje jen dvakrát diferencovatelnou funkci $f$, bez předpokladu spojitosti derivací na okolí bodu $x$.

gradientu. Dostaneme tak větší systém rovnic

$$\begin{aligned}0 &= 3x^2 - 2\lambda x - \eta,\\ 0 &= 3y^2 - 2\lambda y - \eta,\\ 0 &= 3z^2 - 2\lambda z - \eta,\\ 0 &= x^2 + y^2 + z^2 - 1,\\ 0 &= x + y + z.\end{aligned}$$

Protože je i kružnice kompaktní množinou, nutně na ní musí mít $h$ globální maximum a globální minimum. Další rozbor ponecháme na čtenáři. □

**8.46.** Rozhodněte, zda funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x, y, z) = x^2 y$ nabývá extrémů na ploše $2x^2 + 2y^2 + z^2 = 1$. Pokud ano, tak tyto extrémy nalezněte a určete, o jaké extrémy se jedná.

**Řešení.** Protože vyšetřujeme extrémy spojité funkce na kompaktní množině (elipsoidu) – je to uzavřená a omezená množina v $\mathbb{R}^3$ – musí na něm daná funkce nabývat jak minima, tak maxima. Navíc, protože vazební podmínka je dána spojitě diferencovatelnou funkcí a zkoumaná funkce je diferencovatelná, extrémy musí nastat ve stacionárních bodech vyšetřované funkce na dané množině. Pro stacionární body sestavíme soustavu:

$$\begin{aligned}2xy &= 4kx,\\ x^2 &= 4ky,\\ 0 &= 2kz.\end{aligned}$$

Jejím řešením jsou body $[\pm\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}}, 0]$ a $[\pm\frac{1}{\sqrt{3}}, -\frac{1}{\sqrt{6}}, 0]$. Funkce nabývá pouze dvou funkčních hodnot v těchto čtyřech stacionárních bodech. Z výše uvedeného vyplývá, že první dva uvedené stacionární body jsou maxima dané funkce na uvedeném elipsoidu a druhé dva potom minima. □

**8.47.** Určete, zda existují maxima a minima funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x, y, z) = z - xy^2$ na sféře

$$x^2 + y^2 + z^2 = 1.$$

Pokud extrémy existují, určete je.

**Řešení.** Řešíme soustavu

$$\begin{aligned}x &= -ky^2,\\ y &= -2kxy,\\ z &= k.\end{aligned}$$

Z druhé rovnice dostáváme, že buď $y = 0$, nebo $x = -\frac{1}{2k}$. První možnost vede k bodům $[0, 0, 1]$, $[0, 0, -1]$. Druhá pak nemůže být tomu naopak. U indefinitních hodnot Hessiánu opět graf funkce přechází z jedné strany tečné nadroviny na druhou, to se ale obecně děje podél objektů nižší dimenze v tečné nadrovině, nemáme tedy k dispozici přímočaré zobecnění inflexních bodů.

**8.14. Diferenciál zobrazení.** Koncept derivace a diferenciálu lze snadno rozšířit na zobrazení $F : E_n \to E_m$. Při zvolených kartézských souřadnicích na obou stranách je takové zobrazení obyčejná $m$–tice



$$F(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$$

funkcí $f_i : E_n \to \mathbb{R}$. Řekneme, že zobrazení $F$ je *diferencovatelné* nebo *třídy* $C^k$, jestliže tuto vlastnost mají všechny funkce $f_1, \dots, f_m$.

Diferenciál a Jacobiho matice

Diferenciály $df_i(x)$ jednotlivých funkcí $f_i$ zobrazení

$$F(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$$

poskytují lineární přiblížení přírůstků jejich hodnot. Lze proto očekávat, že budou společně dávat také souřadné vyjádření lineárního zobrazení $D^1F(x) : \mathbb{R}^n \to \mathbb{R}^m$ mezi zaměřeními, které bude lineárně aproximovat přírůstky našeho zobrazení. Výsledná matice

$$D^1F(x) = \begin{pmatrix} df_1(x) \\ df_2(x) \\ \vdots \\ df_m(x) \end{pmatrix} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \frac{\partial f_m}{\partial x_2} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}(x)$$

se nazývá *Jacobiho matice zobrazení* $F$ v bodě $x$.

Lineární zobrazení $D^1F(x)$ definované na přírůstcích $v = (v_1, \dots, v_n)$ pomocí stejně značené Jacobiho matice nazýváme *diferenciál zobrazení* $F$ v bodě $x$ z definičního oboru, jestliže platí

$$\lim_{v \to 0} \frac{1}{\|v\|}\big(F(x + v) - F(x) - D^1F(x)(v)\big) = 0.$$

Již jsme několikrát použili skutečnost, že definice euklidovské vzdálenosti má za důsledek, že limity hodnot v $E_n$ existují tehdy a jen tehdy, když existují limity jednotlivých souřadných komponent.

Přímé použití věty 8.5 o existenci diferenciálu pro funkce $n$ proměnných na jednotlivé souřadné funkce zobrazení $F$ proto vede k následujícímu tvrzení (dokažte si případně podrobněji samostatně!):

**Důsledek.** *Nechť $F : E_n \to E_m$ je zobrazení třídy $C^1$ v okolí bodu $x \in E_n$. Pak existuje v tomto bodě diferenciál $D^1F(x)$ a je zadaný Jacobiho maticí $D^1F(x)$.*

**8.15. Transformace souřadnic.** Zobrazení $F : E_n \to E_n$, která mají inverzní zobrazení $G : E_n \to E_n$ definované na celém svém obrazu, se nazývají *transformace*. Každé takové zobrazení je možné vnímat jako změnu souřadnic. Zpravidla požadujeme, aby $F$ i $G$ bylo (spojitě) diferencovatelné zobrazení.



Stejně jako u vektorových prostorů, volba našeho „pohledu na věc“, tj. volba souřadnic, může zdánlivě zjednodušit nebo zhoršit naše porozumění studovanému objektu. Změnu souřadnic nyní

splněna (dosazením do rovnice koule dostaneme rovnici

$$\frac{1}{4k^2}+\frac{1}{2k^2}+k^2=1,$$

která nemá řešení. Ve dvou vypočtených bodech na dané sféře má funkce maximum, resp. minimum. □

**8.48.** Rozhodněte, zda existují extrémy funkce $f:\mathbb{R}^3\to\mathbb{R}$, $f(x,y,z)=xyz$, na elipsoidu určeném rovnicí

$$g(x,y,z)=kx^2+ly^2+z^2=1,\quad k,l\in\mathbb{R}^+.$$

Pokud extrémy existují, určete je.

**Řešení.** Nejprve sestavíme rovnice, které musí splňovat stacionární body dané funkce na elipsoidu:

$$\begin{aligned}\frac{\partial g}{\partial x}&=\lambda\frac{\partial f}{\partial x}: \quad yz &&=2\lambda kx,\\ \frac{\partial g}{\partial y}&=\lambda\frac{\partial f}{\partial y}: \quad xz &&=2\lambda ly,\\ \frac{\partial g}{\partial z}&=\lambda\frac{\partial f}{\partial z}: \quad xy &&=2\lambda z.\end{aligned}$$

Snadno nahlédneme, že řešením dané rovnice musí být trojice nenulových čísel. Po vydělení dvojic rovnic a dosazení do rovnice elipsy dostaneme osm řešení. Dostaneme osm stacionárních bodů $x=\pm\frac{1}{\sqrt{3k}}$, $y=\pm\frac{1}{\sqrt{3l}}$, $z=\pm\frac{1}{\sqrt{3}}$, v nichž ovšem funkce $f$ nabývá pouze dvou různých hodnot. Protože $f$ je spojitá a daný elipsoid je kompaktní, tak na něm $f$ nabývá jak svého minima, tak maxima. Neboť navíc jak $f$ tak $g$ jsou spojitě diferencovatelné, tak tyto extrémy musí nastat v stacionárních bodech. Není tedy jiné možnosti, než že čtyři z daných stacionárních bodů jsou lokálními maximy dané funkce s maximem $\frac{1}{3\sqrt{3kl}}$, zbývající čtyři pak minima s hodnotou $-\frac{1}{3\sqrt{3kl}}$. □

**8.49.** Stanovte globální extrémy funkce

$$f(x,y)=x^2-2y^2+4xy-6x-1$$

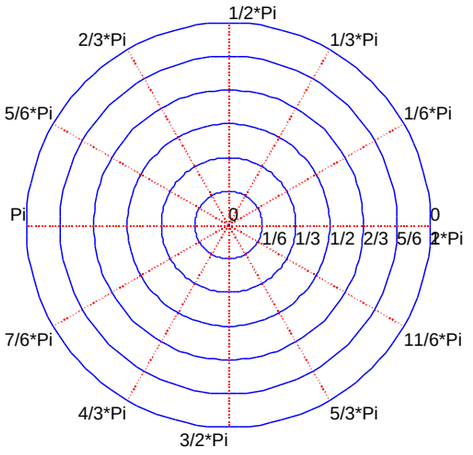
na množině bodů $[x,y]$ vyhovujících nerovnostem

$$x\geq 0,\quad y\geq 0,\quad y\leq -x+3. \tag{8.1}$$

**Řešení.** Máme zadán polynom se spojitými parciálními derivacemi na kompaktní (tj. uzavřené a ohraničené) množině. Taková funkce nutně nabývá své nejmenší a největší hodnoty na této množině, a to ve stacionárních bodech nebo na hranici. Stačí tedy najít stacionární body uvnitř množiny a stacionární body na konečném počtu otevřených (příp. jednobodových) částí hranice, vyčíslit v těchto bodech $f$ a vybrat největší a nejmenší hodnotu. Dodejme, že množina bodů určená nerovnostmi (‖8.1‖) je zřejmě trojúhelníkem s vrcholy $[0,0]$, $[3,0]$, $[0,3]$.

Určeme stacionární body uvnitř tohoto trojúhelníku jako řešení rovnic $f_x=0$, $f_y=0$. Neboť

diskutujeme v daleko obecnější formě než jen u afinních zobrazení v kapitole čtvrté. Někdy se v tomto obecném smyslu užívá označení „křivočaré souřadnice“. Velice názorný příklad je změna nejobvyklejších souřadnic v rovině na tzv. polární, tj. polohu bodu $P$ zadáváme pomocí jeho vzdálenosti od počátku souřadnic $r=\sqrt{x^2+y^2}$ a úhlu $\varphi=\arctan(y/x)$ mezi spojnicí s počátkem a osou $x$ (pokud je $x\neq 0$).




Přechod z polárních souřadnic do standardních je

$$P_{\text{polární}}=(r,\varphi)\mapsto(r\cos\varphi,r\sin\varphi)=P_{\text{kartézské}}$$

Je přitom zjevné, že je nutné polární souřadnice vhodně omezit na podmnožinu bodů $(r,\varphi)$ v rovině, aby existovalo i zobrazení inverzní. Kartézský obraz přímek v polárních souřadnicích s konstantními souřadnicemi $r$ nebo $\varphi$ je na obrázku výše.

Následující věta formuluje velmi užitečné zobecnění pravidla pro derivaci složených funkcí jedné proměnné. Je vlastně, až na složitější koncept samotného diferenciálu, úplně stejná, jako jsme už u jedné proměnné viděli. Pro funkce jedné proměnné je totiž Jacobiho matice jediné číslo a to derivace funkce v bodě, násobení Jacobiho matic je tedy prosté násobení derivací vnější a vnitřní složky funkce. Speciálním případem jsou samozřejmě také vztahy, které jsme odvodili pro derivaci kompozice funkce více proměnných s křivkou.

### Diferenciál složeného zobrazení

**8.16. Věta.** *Nechť $F:E_n\to E_m$ a $G:E_m\to E_r$ jsou dvě diferencovatelná zobrazení, přičemž definiční obor $G$ obsahuje celý obor hodnot $F$. Pak také složené zobrazení $G\circ F$ je diferencovatelné a jeho diferenciál je v každém bodě z definičního oboru $F$ kompozicí diferenciálů*

$$D^1(G\circ F)(x)=D^1G(F(x))\circ D^1F(x).$$

*Příslušná Jacobiho matice zobrazení $G\circ F$ je dána součinem příslušných Jacobiho matic zobrazení $G$ a $F$ v tomto pořadí.*

$$f_x(x,y) = 2x + 4y - 6, \quad f_y(x,y) = 4x - 4y,$$

těmto rovnicím vyhovuje pouze bod $[1,1]$. Hranici můžeme (nabízejícím se způsobem) vyjádřit jako sjednocení tří úseček výběrem dvojic vrcholů. Nejprve uvažujme $x = 0$, $y \in [0,3]$, kdy je $f(x,y) = -2y^2 - 1$. Graf této funkce (jedné proměnné) na intervalu $[0,3]$ ovšem známe. Není tudíž obtížné stanovit body, ve kterých nastávají globální extrémy. Jde o krajní body $[0,0]$, $[0,3]$. Podobně můžeme uvažovat $y = 0$, $x \in [0,3]$, přičemž také obdržíme jenom krajní body $[0,0]$, $[3,0]$. Zbývá úsečka $y = -x + 3$, $x \in [0,3]$, pro niž po úpravě dostáváme

$$f(x,y) = f(x,-x+3) = -5x^2 + 18x - 19, \quad x \in [0,3].$$

Potřebuje tedy najít stacionární body polynomu $p(x) = -5x^2 + 18x - 19$ z intervalu $[0,3]$. Rovnici $p'(x) = 0$, tj. $-10x + 18 = 0$, pak vyhovuje $x = 9/5$. To znamená, že v posledním případě jsme (kromě již zahrnutých krajních bodů) získali ještě jeden bod $[9/5, 6/5]$, ve kterém může být globální extrém. Celkem máme tyto „podezřelé“ body

$$[1,1], \quad [0,0], \quad [0,3], \quad [3,0], \quad \left[\tfrac{9}{5}, \tfrac{6}{5}\right]$$

po řadě s funkčními hodnotami

$$-4, \quad -1, \quad -19, \quad -10, \quad -\tfrac{14}{5}.$$

Vidíme, že největší hodnoty $-1$ nabývá funkce $f$ v bodě $[0,0]$ a nejmenší hodnoty $-19$ pak v bodě $[0,3]$. □

**8.50.** Rozhodněte, zda funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x,y,z) = y^2 z$ nabývá extrémů na úsečce dané rovnicemi $2x + y + z = 1$, $x - y + 2z = 0$ a omezením $x \in [-1,2]$. Pokud ano, tak tyto extrémy nalezněte a určete, o jaké extrémy se jedná. Všechna svoje rozhodnutí zdůvodněte.

**Řešení.** Hledáme extrémy spojité funkce na kompaktní množině, funkce tedy bude nabývat na dané množině jak svého minima tak maxima a to buď v bodech, kde je gradient zkoumané funkce lineární kombinací gradientů funkcí zadávající vazební podmínky, nebo v krajních bodech úsečky. Najděme body splňující podmínku s gradienty:

$$\begin{aligned} 0 &= 2k + l, \\ 2yz &= k - l, \\ y^2 &= k + 2l, \\ 2x + y + z &= 1, \\ x - y + 2z &= 0, \end{aligned}$$

která má řešení $[x,y,z] = [\frac{2}{3}, 0, -\frac{1}{3}]$ a $[x,y,z] = [\frac{4}{9}, \frac{2}{9}, -\frac{1}{9}]$ (proměnné $k$ a $l$ můžeme samozřejmě dopočítat také, ale nezajímají



Důkaz. V odstavci 8.5 a při důkazu Taylorovy věty jsme odvodili, jak se chová diferencování složených zobrazení vzniklých z funkcí a křivek. Tím jsme dokázali speciální případy této věty s $n = r = 1$. Obecný případ se odvodí prakticky stejným postupem, jen budeme pracovat více s vektory.

Zvolme libovolný pevný přírůstek $v$ a počítejme směrovou derivaci pro kompozici $G \circ F$ v bodě $x \in E_n$. Ve skutečnosti to znamená spočíst postupně diferenciály pro jednotlivé souřadné funkce zobrazení $G$ složené s $F$. Pišme tedy rovnou jednodušeji $g \circ F$ pro kteroukoliv z nich.

$$d_v(g \circ F)(x) = \lim_{t \to 0} \frac{1}{t}\big(g(F(x+tv)) - g(F(x))\big).$$

Výraz v závorce můžeme ovšem z definice diferenciálu $g$ vyjádřit jako

$$\begin{aligned} g(F(x+tv)) - g(F(x) = dg(F(x))(F(x+tv) - F(x)) \\ + \alpha(F(x+tv) - F(x)), \end{aligned}$$

kde $\alpha$ je funkce definovaná na okolí bodu $F(x)$, která je spojitá a splňuje $\lim_{v \to 0} \frac{1}{\|v\|}\alpha(v) = 0$. Dosazením do rovnosti pro směrovou derivaci dostáváme

$$\begin{aligned} d_v(g \circ F)(x) &= \lim_{t \to 0} \frac{1}{t}\big(dg(F(x))(F(x+tv) - F(x)) \\ &\qquad + \alpha(F(x+tv) - F(x))\big) \\ &= dg(F(x))\left(\lim_{t \to 0} \frac{1}{t}\Big(F(x+tv) - F(x)\Big)\right) \\ &\qquad + \lim_{t \to 0} \frac{1}{t}\Big(\alpha(F(x+tv) - F(x))\Big) \\ &= dg(F(x)) \circ D^1F(x)(v) + 0, \end{aligned}$$

kde jsme využili vlastnosti funkce $\alpha$ a skutečnosti, že lineární zobrazení mezi konečněrozměrnými prostory jsou vždy spojitá.

Dokázali jsme tedy tvrzení pro jednotlivé funkce $g_1, \ldots, g_r$ zobrazení $G$. Celá věta nyní vyplývá z toho, jak se násobí matice. □



Ilustrujme teď využití konceptu transformace a věty o derivaci složených zobrazení na jednoduchém příkladě. Viděli jsme, že polární souřadnice vzniknou z kartézských transformací $F : \mathbb{R}^2 \to \mathbb{R}^2$, kterou v souřadnicích $(x,y)$ a $(r,\varphi)$ zapíšeme takto (např. na definičním oboru všech bodů v prvním kvadrantu roviny mimo body s $x = 0$)

$$r = \sqrt{x^2 + y^2}, \ \varphi = \arctan\frac{y}{x}.$$

Uvažme funkci $g_t : E_2 \to \mathbb{R}$, která má v polárních souřadnicích vyjádření

$$g(r,\varphi,t) = \sin(r - t).$$

Taková funkce nám snad dobře přibližuje vlnění povrchu hladiny po bodovém vzruchu v počátku v čase $t$, viz obrázek s hodnotou $t = -\pi/2$. Zatímco v polárních souřadnicích bylo snadné ji zadat, v kartézských bychom asi tápali.

nás). Krajní body dané úsečky jsou $[-1, \frac{5}{3}, \frac{4}{3}]$ a $[2, -\frac{4}{3}, -\frac{5}{3}]$. Z těchto čtyř bodů nabývá funkce největší hodnoty v prvním z krajních bodů ($f(x, y, z) = \frac{100}{27}$), tam tedy nabývá maxima na dané úsečce a nejmenší hodnoty v druhém z krajních bodů ($f(x, y, z) = -\frac{80}{27}$), tam tedy nabývá svého minima na dané úsečce. □

**8.51.** Najděte maximální a minimální hodnotu polynomu

$$p(x, y) = 4x^3 - 3x - 4y^3 + 9y$$

na množině

$$M = \left\{[x, y] \in \mathbb{R}^2;\ x^2 + y^2 \leq 1\right\}.$$

**Řešení.** Také v tomto příkladu máme zadán polynom na kompaktní množině, a proto se omezíme na hledání stacionárních bodů uvnitř či na hranici $M$ a „krajních" bodů na hranici $M$. Jako řešení rovnic

$$p_x(x, y) = 12x^2 - 3 = 0, \quad p_y(x, y) = -12y^2 + 9 = 0$$

však dostáváme pouze body

$$\left[\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}\right], \quad \left[\tfrac{1}{2}, -\tfrac{\sqrt{3}}{2}\right], \quad \left[-\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}\right], \quad \left[-\tfrac{1}{2}, -\tfrac{\sqrt{3}}{2}\right],$$

které se nacházejí na hranici $M$. To znamená, že $p$ nemá uvnitř $M$ žádný extrém. Stačí tak najít maximum a minimum $p$ na jednotkové kružnici $k : x^2 + y^2 = 1$. Kružnici $k$ vyjádříme parametricky jako

$$x = \cos t, \quad y = \sin t, \qquad t \in [-\pi, \pi].$$

Od hledání extrémů $p$ na $M$ tak přecházíme k hledání extrémů funkce

$$f(t) := p(\cos t, \sin t) = 4\cos^3 t - 3\cos t - 4\sin^3 t + 9\sin t$$

na intervalu $[-\pi, \pi]$. Pro $t \in [-\pi, \pi]$ platí

$$f'(t) = -12\cos^2 t \sin t + 3\sin t - 12\sin^2 t \cos t + 9\cos t,$$

Abychom mohli určit stacionární body, musíme funkci $f'$ vyjádřit ve tvaru, ze kterého bude možné vypočítat, kde její graf protíná osu $x$. Použijeme k tomu identitu

$$\tfrac{1}{\cos^2 t} = 1 + \operatorname{tg}^2 t,$$

která platí všude, kde mají obě strany smysl. S její pomocí dostáváme

$$f'(t) = \cos^3 t \left[-12\operatorname{tg} t + 3\left(\operatorname{tg} t + \operatorname{tg}^3 t\right) - 12\operatorname{tg}^2 t + 9\left(1 + \operatorname{tg}^2 t\right)\right]$$

pro $t \in [-\pi, \pi]$ taková, že je $\cos t \neq 0$. Toto omezení ovšem nevyloučí žádné stacionární body, protože $\sin t \neq 0$, je-li $\cos t = 0$. Stacionárními body $f$ jsou tak body $t \in [-\pi, \pi]$, pro které je

$$-4\operatorname{tg} t + \operatorname{tg} t + \operatorname{tg}^3 t - 4\operatorname{tg}^2 t + 3 + 3\operatorname{tg}^2 t = 0.$$

Substitucí $s = \operatorname{tg} t$ obdržíme

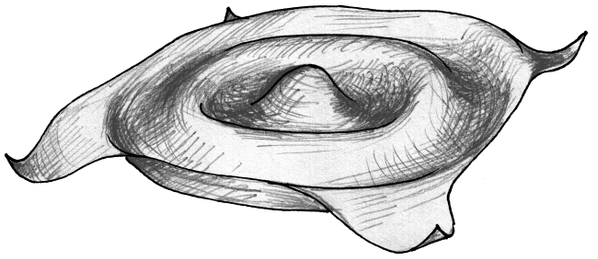
$$s^3 - s^2 - 3s + 3 = 0, \quad \text{tj.} \quad (s - 1)\left(s - \sqrt{3}\right)\left(s + \sqrt{3}\right) = 0.$$

Hodnotám

$$s = 1, \quad s = \sqrt{3}, \quad s = -\sqrt{3}$$

odpovídá postupně

$$t \in \{-\tfrac{3}{4}\pi, \tfrac{1}{4}\pi\}, \quad t \in \{-\tfrac{2}{3}\pi, \tfrac{1}{3}\pi\}, \quad t \in \{-\tfrac{1}{3}\pi, \tfrac{2}{3}\pi\}.$$



Spočtěme nyní derivaci této funkce v kartézských souřadnicích. Použitím naší věty dostaneme

$$\begin{aligned}\frac{\partial g}{\partial x}(x, y, t) &= \frac{\partial g}{\partial r}(r, \varphi)\frac{\partial r}{\partial x}(x, y) + \frac{\partial g}{\partial \varphi}(r, \varphi)\frac{\partial \varphi}{\partial x}(x, y)\\ &= \cos(\sqrt{x^2 + y^2} - t)\frac{x}{\sqrt{x^2 + y^2}} + 0\end{aligned}$$

a podobně

$$\begin{aligned}\frac{\partial g}{\partial y}(x, y, t) &= \frac{\partial g}{\partial r}(r, \varphi)\frac{\partial r}{\partial y}(x, y) + \frac{\partial g}{\partial \varphi}(r, \varphi)\frac{\partial \varphi}{\partial y}(x, y)\\ &= \cos(\sqrt{x^2 + y^2} - t)\frac{y}{\sqrt{x^2 + y^2}}.\end{aligned}$$

**8.17. Věta o inverzním zobrazení.** U funkcí jedné proměnné rozhodovala nenulovost první derivace o tom, je-li funkce rostoucí či klesající. Pak takovou musela být i na nějakém okolí zvoleného bodu, a tudíž tam existovala i inverzní funkce. Její derivace pak byla převrácenou hodnotou derivace funkce původní.



Když tuto situaci interpretujeme z pohledu zobrazení $E_1 \to E_1$ a lineárních zobrazení $\mathbb{R} \to \mathbb{R}$ coby jejich diferenciálů, je nenulovost nutnou a dostatečnou podmínkou k invertibilitě příslušného diferenciálu. Takto obdržíme tvrzení platné pro konečněrozměrné prostory obecně:

VĚTA O INVERZNÍM ZOBRAZENÍ

**Věta.** *Nechť $F : E_n \to E_n$ je diferencovatelné zobrazení na nějakém okolí bodu $x_0 \in E_n$ a nechť je Jacobiho matice $D^1 f(x_0)$ invertibilní. Pak na nějakém okolí bodu $x_0$ existuje inverzní zobrazení $F^{-1}$ a jeho diferenciál v bodě $F(x_0)$ je inverzním zobrazením k diferenciálu $D^1 F(x_0)$, tzn. je zadán inverzní maticí k Jacobiho matici zobrazení $F$ v bodě $x_0$.*

DŮKAZ. Nejdříve si zkusme ověřit, že tvrzení je rozumné a očekávatelné. Pokud bychom předpokládali, že inverzní zobrazení existuje a je diferencovatelné v bodě $F(x_0)$, věta o derivování složených funkcí si vynucuje vztah

$$\mathrm{id}_{\mathbb{R}^n} = D^1(F^{-1} \circ F)(x_0) = D^1(F^{-1}) \circ D^1 F(x_0),$$

což ověřuje vztah v závěru věty. Víme proto od začátku, jaký diferenciál pro $F^{-1}$ hledat.

V dalším kroku předpokládejme, že inverzní zobrazení $F^{-1}$ na okolí bodu $F(x_0)$ existuje a je spojité. Budeme v této situaci ověřovat existenci diferenciálu. Z diferencovatelnosti $F$ na okolí $x_0$ vyplývá, že



$$F(x) - F(x_0) - D^1 F(x_0)(x - x_0) = \alpha(x - x_0)$$

Nyní vyčíslíme funkci $f$ ve všech těchto bodech a také v krajních bodech $t = -\pi, t = \pi$. Při seřazení podle velikosti je

$$f\left(-\tfrac{1}{3}\pi\right) = -1 - 3\sqrt{3} < f\left(-\tfrac{3}{4}\pi\right) = -3\sqrt{2} < f\left(-\tfrac{2}{3}\pi\right) = 1 - 3\sqrt{3} < -1,$$

$$f(-\pi) = f(\pi) = -1 < 0,$$

$$f\left(\tfrac{2}{3}\pi\right) = 1 + 3\sqrt{3} > f\left(\tfrac{1}{4}\pi\right) = 3\sqrt{2} > f\left(\tfrac{1}{3}\pi\right) = -1 + 3\sqrt{3} > 0.$$

Globální minimum má funkce $f$ tedy v bodě $t = -\pi/3$ a maximum v bodě $t = 2\pi/3$.

Nyní se vraťme k původní funkci $p$. Ze znalosti hodnot $\cos\left(-\frac{1}{3}\pi\right) = \frac{1}{2}$, $\sin\left(-\frac{1}{3}\pi\right) = -\frac{\sqrt{3}}{2}$, $\cos\left(\frac{2}{3}\pi\right) = -\frac{1}{2}$, $\sin\left(\frac{2}{3}\pi\right) = \frac{\sqrt{3}}{2}$, nabývá polynom $p$ minimální hodnoty $-1 - 3\sqrt{3}$ (pochopitelně stejné jako $f$) v bodě $[1/2, -\sqrt{3}/2]$ a maximální hodnoty $1 + 3\sqrt{3}$ v bodě $[-1/2, \sqrt{3}/2]$. □

**8.52.** V jakých bodech nabývá funkce

$$f(x, y) = x^2 - 4x + y^2$$

globálních extrémů na množině $M : |x| + |y| \leq 1$?

**Řešení.** Pokud vyjádříme $f$ ve tvaru

$$f(x, y) = (x - 2)^2 - 4 + y^2,$$

je vidět, že tato funkce má globální maximum a minimum ve stejných bodech jako funkce

$$g(x, y) := \sqrt{(x - 2)^2 + y^2}, \quad [x, y] \in M.$$

Posunutí funkce ani aplikace rostoucí funkce $v = \sqrt{u}$ pro $u \geq 0$ totiž nemění body, kde nastávají extrémy (pouze změní hodnotu extrémů). O funkci $g$ však víme, že udává vzdálenost bodu $[x, y]$ od bodu $[2, 0]$. Neboť množina $M$ je zřejmě čtvercem s vrcholy $[1, 0]$, $[0, 1]$, $[-1, 0]$, $[0, -1]$, nejblíže z bodů $M$ k bodu $[2, 0]$ je vrchol $[1, 0]$ a nejvzdálenější je vrchol $[-1, 0]$. Máme výsledek – minimální hodnotu má $f$ v bodě $[1, 0]$ a maximální v bodě $[-1, 0]$. □

**8.53.** Spočítejte lokální extrémy funkce $y = f(x)$ určené implicitně rovnicí

$$3x^2 + 2xy + x = y^2 + 3y + \tfrac{5}{4}, \quad [x, y] \in \mathbb{R}^2 \setminus \left\{\left[x, x - \tfrac{3}{2}\right];\ x \in \mathbb{R}\right\}.$$

**Řešení.** V souladu s teoretickou částí (viz 8.18) označme

$$F(x, y) = 3x^2 + 2xy + x - y^2 - 3y - \tfrac{5}{4},$$
$$[x, y] \in \mathbb{R}^2 \setminus \left\{\left[x, x - \tfrac{3}{2}\right];\ x \in \mathbb{R}\right\}$$

a vypočtěme derivaci

$$y' = f'(x) = -\frac{F_x(x,y)}{F_y(x,y)} = -\frac{6x+2y+1}{2x-2y-3}.$$

Vidíme, že tato derivace existuje spojitě na celé zadané množině. Zvláště je na této množině implicitně určena funkce $f$ (jmenovatel je nenulový).

se zobrazením $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ splňující $\lim_{v\to 0} \frac{1}{\|v\|}\alpha(v) = 0$. Pro ověření aproximační vlastnosti lineárního zobrazení $(D^1F(x_0))^{-1}$ je třeba pouze spočíst následující limitu pro $y = F(x)$ jdoucí k $y_0 = F(x_0)$

$$\lim_{y\to y_0} \frac{1}{\|y - y_0\|}\left(F^{-1}(y) - F^{-1}(y_0) - (D^1F(x_0))^{-1}(y - y_0)\right).$$

Dosazením z předchozí rovnosti dostáváme

$$\lim_{y\to y_0} \frac{1}{\|y - y_0\|}\Big(x - x_0 - (D^1F(x_0))^{-1}(D^1F(x_0)(x - x_0) + \alpha(x - x_0))\Big)$$
$$= \lim_{y\to y_0} \frac{-1}{\|y - y_0\|}(D^1F(x_0))^{-1}(\alpha(x - x_0))$$
$$= (D^1F(x_0))^{-1} \lim_{y\to y_0} \frac{-1}{\|y - y_0\|}(\alpha(x - x_0)),$$

kde poslední rovnost vyplývá ze skutečnosti, že lineární zobrazení mezi konečněrozměrnými prostory jsou vždy spojitá a díky invertibilitě diferenciálu jeho předřazení limitnímu procesu neovlivní ani existenci limity. Chceme dokázat, že tato limita bude nulová.

Všimněme si, že jsme zdánlivě s důkazem skoro hotoví. Limita na konci našeho výrazu je v důsledku vlastností funkce $\alpha$ nulová, pokud jsou velikosti $\|F(x) - F(x_0)\|$ větší než $C\|x - x_0\|$ pro nějakou konstantu $C$. To je o trochu silnější vlastnost, než že je $F^{-1}$ spojité, v literatuře se této vlastnosti říká, že je funkce *lipschitzovsky spojitá*[3]. Zbývá nám tedy už „jenom“ dokázat existenci Lipschitzovsky spojitého inverzního zobrazení k zobrazení $F$.



Pro další úvahy si zjednodušíme práci převedením obecného případu na o něco jednodušší tvrzení. Zejména bez újmy na obecnosti lze vhodnou volbou kartézských souřadnic dosáhnout $x_0 = 0 \in R^n$, $y_0 = F(x_0) = 0 \in \mathbb{R}^n$.

Složením zobrazení $F$ s jakýmkoliv lineárním zobrazením $G$ dostaneme opět diferencovatelné zobrazení a víme také, jak se změní diferenciál. Volbou $G(x) = (D^1F(0))^{-1}(x)$ dostáváme $D^1(G \circ F)(0) = \mathrm{id}_{\mathbb{R}^n}$. Můžeme tedy zrovna předpokládat

$$D^1F(0) = \mathrm{id}_{\mathbb{R}^n}.$$

Uvažme za těchto předpokladů zobrazení $K(x) = F(x) - x$. Toto zobrazení je opět diferencovatelné a jeho diferenciál v bodě 0 je zjevně nulový.

Pro libovolné spojitě diferencovatelné zobrazení $K$ v okolí počátku $\mathbb{R}^n$ platí díky Taylorovu rozvoji prvního řádu se zbytkem jednotlivých souřadných funkcí $K_i$ a díky definici euklidovské vzdálenosti odhad

$$\|K(x) - K(y)\| \leq C\sqrt{n}\|x - y\|,$$

kde $C$ je ohraničeno maximem všech absolutních hodnot parciálních derivací v Jacobiho matici zobrazení $K$ na sledovaném okolí.[4]

Protože v našem případě je diferenciál zobrazení $K$ v bodě $x_0 = 0$ nulový, můžeme volbou dostatečně malého okolí $U$

[3] Tento mimořádně užitečný technický pojem budeme potkávat často. Není přitom složité najít spojité funkce, které lipschityovsky spojité nebudou, např. $f(x) = \sqrt{|x|}$ je spojitá funkce, která ale má v nule nevlastní derivaci a tedy nemůže být lipschitzovská

[4] Z této úvahy okamžitě plyne, že funkce, která má spojité parciální derivace na kompaktní množině, je na ní i Lipschitzovsky spojitá.

Lokální extrém může nastat pouze pro $x$, $y$, pro která je $y' = 0$, tj. $6x+2y+1 = 0$. Dosadíme-li $y = -3x-1/2$ do rovnice $F(x, y) = 0$, obdržíme po úpravě $-12x^2 + 6x = 0$ a následně

$$[x, y] = \left[0, -\tfrac{1}{2}\right], \quad [x, y] = \left[\tfrac{1}{2}, -2\right].$$

Snadno také spočítáme

$$y'' = \left(y'\right)' = -\tfrac{(6+2y')(2x-2y-3)-(6x+2y+1)(2-2y')}{(2x-2y-3)^2}.$$

Dosazením $x = 0$, $y = -1/2$, $y' = 0$ a $x = 1/2$, $y = -2$, $y' = 0$ dostaneme

$$y'' = -\tfrac{6(-2)-0}{4} > 0 \quad \text{pro } [x, y] = \left[0, -\tfrac{1}{2}\right]$$

a

$$y'' = -\tfrac{6(+2)-0}{4} < 0 \quad \text{pro } [x, y] = \left[\tfrac{1}{2}, -2\right].$$

Dokázali jsme tak, že implicitně zadaná funkce má v bodě $x = 0$ ostré lokální minimum a v bodě $x = 1/2$ ostré lokální maximum. □

**8.54.** Najděte lokální extrémy funkce $z = f(x, y)$ zadané na maximální množině implicitně rovnicí

$$x^2 + y^2 + z^2 - xz - yz + 2x + 2y + 2z - 2 = 0. \tag{8.2}$$

**Řešení.** Derivování (‖8.2‖) podle $x$ a $y$ dává

$$2x + 2zz_x - z - xz_x - yz_x + 2 + 2z_x = 0,$$
$$2y + 2zz_y - xz_y - z - yz_y + 2 + 2z_y = 0.$$

Odtud vyplývají rovnosti

$$z_x = f_x(x, y) = \frac{z - 2x - 2}{2z - x - y + 2},$$
$$z_y = f_y(x, y) = \frac{z - 2y - 2}{2z - x - y + 2}. \tag{8.3}$$

Všimněme si, že parciální derivace jsou spojité všude, kde je definována funkce $f$. To implikuje, že lokální extrémy mohou být pouze ve stacionárních bodech. Ve těchto bodech pak platí

$$z_x = 0, \quad \text{tj.} \quad z - 2x - 2 = 0,$$
$$z_y = 0, \quad \text{tj.} \quad z - 2y - 2 = 0.$$

Máme dvě rovnice, které umožňují vyjádřit $x$ a $y$ v závislosti na $z$. Dosazením do (‖8.2‖) potom již získáme body

$$[x, y, z] = \left[-3 + \sqrt{6}, -3 + \sqrt{6}, -4 + 2\sqrt{6}\right],$$
$$[x, y, z] = \left[-3 - \sqrt{6}, -3 - \sqrt{6}, -4 - 2\sqrt{6}\right].$$

Nyní potřebujeme druhé derivace k tomu, abychom mohli říci, zda jde v příslušných bodech o lokální extrémy. Derivováním $z_x$ v (‖8.3‖) dostáváme

$$z_{xx} = f_{xx}(x, y) = \tfrac{(z_x-2)(2z-x-y+2)-(z-2x-2)(2z_x-1)}{(2z-x-y+2)^2},$$

derivujeme-li podle $x$, a

$$z_{xy} = f_{xy}(x, y) = \tfrac{z_y(2z-x-y+2)-(z-2x-2)(2z_y-1)}{(2z-x-y+2)^2},$$

počátku dosáhnout platnosti ohraničení

$$\|K(x) - K(y)\| \le \frac{1}{2}\|x - y\|.$$

Dále dosazením za definici $K(x) = F(x) - x$ a použitím trojúhelníkové nerovnosti $\|(u - v) + v\| \le \|u - v\| + \|v\|$, tj. také $\|u\| - \|v\| \le \|u - v\|$, dostáváme

$$\|y - x\| - \|F(x) - F(y)\| \le \|F(x) - F(y) + y - x\| \le \frac{1}{2}\|y - x\|.$$

Odtud konečně

$$\frac{1}{2}\|x - y\| \le \|F(x) - F(y)\|.$$

Tímto odhadem jsme dosáhli opravdu pěkného pokroku: jsou-li na našem malém okolí $U$ počátku $x \neq y$, pak nutně musí být také $F(x) \neq F(y)$. Je tedy naše zobrazení vzájemně jednoznačné. Pišme $F^{-1}$ pro jeho inverzi definovanou na obrazu $U$. Pro ni náš odhad říká

$$\|F^{-1}(x) - F^{-1}(y)\| \le 2\|x - y\|,$$

je tedy toto zobrazení určitě nejen spojité ale dokonce Lipschitzovsky spojité, tak jak jsme v předchozí části důkazu potřebovali.



Zdánlivě jsme tedy již úplně hotoví (s důkazem), to ale není pravda. Abychom skutečně dokončili důkaz, musíme ukázat, že je zobrazení $F$ zúžené na dostatečně malé okolí nejen vzájemně jednoznačné, ale že také zobrazuje otevřené okolí nuly na otevřené okolí nuly.[5]

Zvolme si $\delta$ tak malé, aby okolí $V = \mathcal{O}_\delta(0)$ leželo v $U$ včetně své hranice a zároveň aby Jacobiho matice zobrazení $F$ byla na celém $V$ invertibilní. To je jistě možné, protože determinant je spojité zobrazení. Označme $B$ hranici množiny $V$ (tj. příslušnou sféru). Protože je $B$ kompaktní a $F$ spojité, má funkce

$$\rho(x) = \|F(x)\|$$

na $B$ maximum i minimum. Označme $a = \frac{1}{2}\min_{x\in B}\rho(x)$ a uvažujme libovolné $y \in \mathcal{O}_a(0)$. Samozřejmě je $a > 0$. Chceme ukázat, že existuje alespoň jedno $x \in V$ takové, že $y = F(x)$, čímž bude celá věta o inverzní funkci dokázána.

Za tímto účelem uvažme funkci ($y$ je náš pevně zvolený bod)

$$h(x) = \|F(x) - y\|^2.$$

Opět obraz $h(V) \cup h(B)$ musí mít minimum. Ukážeme nejprve, že toto minimum nemůže nastat pro $x \in B$. Platí totiž $F(0) = 0$, a proto $h(0) = \|y\| < a$. Zároveň podle naší definice $a$ je pro $y \in \mathcal{O}_a(0)$ vzdálenost $y$ od $F(x)$ pro $x \in B$ alespoň $a$ (protože $a$ jsme volili jako polovinu minima z velikosti $F(x)$ na hranici). Minimum tedy nastává uvnitř $V$ a musí být ve stacionárním bodě $z$ funkce $h$. To ale znamená že pro všechna $j = 1, \ldots, n$ platí

$$\frac{\partial h}{\partial x^j}(z) = \sum_{i=1}^{n} 2(f_i(z) - y_i)\frac{\partial f_i}{\partial x_j}(z) = 0.$$

Na tento systém rovnic se můžeme dívat jako na systém lineárních rovnic s proměnnými $\xi_i = f_i(z) - y_i$ a koeficienty zadanými dvojnásobkem Jacobiho matice $D^1F(z)$. Pro každé $z \in V$ má takový systém ovšem pouze jedno řešení a to je nulové, protože Jacobiho matice je podle našeho předpokladu invertibilní.

[5] V literatuře lze snadno dohledat příklady zobrazení, která třeba spojitě a bijektivně zobrazí úsečku na čtverec apod.

když derivujeme podle $y$. Důvodem, proč jsme neurčili také $z_{yy}$, je záměnné postavení $x$ a $y$ v (‖8.2‖) (pokud zaměníme $x$ za $y$, rovnice se nezmění). Navíc také $x$-ové a $y$-ové souřadnice uvažovaných bodů jsou stejné, a proto je v těchto bodech $z_{xx} = z_{yy}$. Snadno již ve stacionárních bodech vyčíslíme

$$f_{xx}\left(-3+\sqrt{6},-3+\sqrt{6}\right) = f_{yy}\left(-3+\sqrt{6},-3+\sqrt{6}\right) = -\tfrac{1}{\sqrt{6}},$$
$$f_{xy}\left(-3+\sqrt{6},-3+\sqrt{6}\right) = f_{yx}\left(-3+\sqrt{6},-3+\sqrt{6}\right) = 0,$$
$$f_{xx}\left(-3-\sqrt{6},-3-\sqrt{6}\right) = f_{yy}\left(-3-\sqrt{6},-3-\sqrt{6}\right) = \tfrac{1}{\sqrt{6}},$$
$$f_{xy}\left(-3-\sqrt{6},-3-\sqrt{6}\right) = f_{yx}\left(-3-\sqrt{6},-3-\sqrt{6}\right) = 0.$$

Při zápisu do Hessiánu je

$$Hf\left(-3+\sqrt{6},-3+\sqrt{6}\right) = \begin{pmatrix} -\frac{1}{\sqrt{6}} & 0 \\ 0 & -\frac{1}{\sqrt{6}} \end{pmatrix},$$
$$Hf\left(-3-\sqrt{6},-3-\sqrt{6}\right) = \begin{pmatrix} \frac{1}{\sqrt{6}} & 0 \\ 0 & \frac{1}{\sqrt{6}} \end{pmatrix}.$$

Očividně první Hessián je negativně a druhý pozitivně definitní, což znamená, že v bodě $\left[-3+\sqrt{6},-3+\sqrt{6}\right]$ je ostré lokální maximum, zatímco v bodě $\left[-3-\sqrt{6},-3-\sqrt{6}\right]$ je ostré lokální minimum funkce $f$. □

**8.55.** Stanovte ostré lokální extrémy funkce

$$f(x,y) = \tfrac{1}{x} + \tfrac{1}{y}, \quad x \neq 0,\ y \neq 0$$

na množině bodů, které vyhovují rovnici $\frac{1}{x^2} + \frac{1}{y^2} = 4$.

**Řešení.** Neboť funkce $f$ i funkce zadaná implicitně rovnicí $\frac{1}{x^2} + \frac{1}{y^2} - 4 = 0$ mají zřejmě spojité parciální derivace všech řádů na množině $\mathbb{R}^2 \setminus \{[0,0]\}$, hledejme stacionární body, tj. hledejme řešení rovnic $L_x = 0$, $L_y = 0$ pro

$$L(x,y,\lambda) = \tfrac{1}{x} + \tfrac{1}{y} - \lambda\left(\tfrac{1}{x^2} + \tfrac{1}{y^2} - 4\right), \quad x \neq 0,\ y \neq 0.$$

Takto dostáváme rovnice

$$-\tfrac{1}{x^2} + \tfrac{2\lambda}{x^3} = 0, \quad -\tfrac{1}{y^2} + \tfrac{2\lambda}{y^3} = 0,$$

které vedou na $x = 2\lambda$, $y = 2\lambda$. Vzhledem k uvažované množině bodů podmínka $x = y$ dává stacionární body

$$\left[\frac{\sqrt{2}}{2},\frac{\sqrt{2}}{2}\right], \quad \left[-\frac{\sqrt{2}}{2},-\frac{\sqrt{2}}{2}\right]. \tag{8.4}$$

Zkoumejme dále druhý diferenciál funkce $L$. Snadno lze určit

$$L_{xx} = \tfrac{2}{x^3} - \tfrac{6\lambda}{x^4}, \quad L_{xy} = 0, \quad L_{yy} = \tfrac{2}{y^3} - \tfrac{6\lambda}{y^4}, \quad x \neq 0,\ y \neq 0,$$

odkud plyne

$$d^2L(x,y) = \left(\tfrac{2}{x^3} - \tfrac{6\lambda}{x^4}\right)dx^2 + \left(\tfrac{2}{y^3} - \tfrac{6\lambda}{y^4}\right)dy^2.$$

Diferencováním vazebné podmínky $\frac{1}{x^2} + \frac{1}{y^2} = 4$ pak dostáváme

$$-\tfrac{2}{x^3}\,dx - \tfrac{2}{y^3}\,dy = 0, \quad \text{tj.} \quad dy^2 = \tfrac{y^6}{x^6}\,dx^2.$$

Tím jsme našli hledaný bod $x = z \in V$ splňující pro všechna $i = 1,\dots,n$ rovnost $f_i(z) = y_i$, tj. $F(z) = y$. □

**8.18. Věta o implicitní funkci.** Naším dalším cílem je využít větu o inverzním zobrazení pro práci s implicitně definovanými funkcemi. Pro začátek uvažujme diferencovatelnou funkci $F(x,y)$ definovanou v rovině $E_2$ a hledejme body $(x,y)$, ve kterých platí $F(x,y) = 0$.



Příkladem může být třeba obvyklá (implicitní) definice přímek a kružnic:

$$F(x,y) = ax + by + c = 0,$$
$$F(x,y) = (x-s)^2 + (y-t)^2 - r^2 = 0,\ r > 0.$$

Zatímco v prvém případě je (při $b \neq 0$) předpisem zadaná funkce

$$y = f(x) = -\frac{a}{b}x - \frac{c}{b}$$

pro všechna $x$, ve druhém případě můžeme pro libovolný bod $(x_0,y_0)$ splňující rovnici kružnice a takový, že $y_0 \neq t$ (to jsou totiž krajní body kružnice ve směru souřadnice $x$), najít okolí bodu $x_0$, na kterém bude buď

$$y = f(x) = t + \sqrt{(x-s)^2 - r}$$

nebo

$$y = f(x) = t - \sqrt{(x-s)^2 - r},$$

podle toho na kterou půlkružnici patří bod $(x_0,y_0)$. Při načrtnutí obrázku je důvod zřejmý – nemůžeme chtít pomocí funkce $y = f(x)$ postihnout horní i dolní půlkružnici zároveň. Zajímavější jsou krajní body intervalu $[s-r, s+r]$. Ty také vyhovují rovnici kružnice, platí v nich ale $F_y(s \pm r, t) = 0$, což vystihuje polohu tečny ke kružnici v těchto bodech rovnoběžnou s osou $y$. V těchto bodech skutečně neumíme najít okolí, na němž by kružnice byla popsána jako funkce $y = f(x)$.

Navíc umíme i derivaci naší funkce $y = f(x) = t + \sqrt{(x-s)^2 - r^2}$, tam kde je definována, vyjádřit pomocí parciálních derivací funkce $F$:

$$f'(x) = \frac{1}{2}\frac{2(x-s)}{\sqrt{(x-s)^2 - r^2}} = \frac{x-s}{y-t} = -\frac{F_x}{F_y}.$$

Když prohodíme roli proměnných $x$ a $y$ a budeme chtít najít závislost $x = f(y)$ takovou, aby $F(f(y),y) = 0$, pak v okolí bodů $(s \pm r, t)$ bez problémů uspějeme. Všimněme si, že v těchto bodech je parciální derivace $F_x$ nenulová.

Naše pozorování tedy (pro pouhé dva příklady) říká: pro funkci $F(x,y)$ a bod $(a,b) \in E_2$ takový, že $F(a,b) = 0$, umíme jednoznačně najít funkci $y = f(x)$ splňující $F(x,f(x)) = 0$, pokud je $F_y(a,b) \neq 0$. V takovém případě umíme i vypočíst $f'(a) = -F_x(a,b)/F_y(a,b)$. Dokážeme, že ve skutečnosti toto tvrzení platí vždy. Poslední tvrzení o derivaci přitom je dobře zapamatovatelné (a při pečlivém vnímání věcí i pochopitelné) z výrazu pro diferenciál funkce $g(x) = F(x,y(x))$ a diferenciál $dy = f'(x)dx$, neboť

$$0 = dg = F_x dx + F_y dy = (F_x + F_y f'(x))dx.$$

Obdobně bychom mohli pracovat s implicitními výrazy $F(x,y,z) = 0$, přičemž můžeme hledat funkci $g(x,y)$ takovou, že $F(x,y,g(x,y)) = 0$. Jako příklad uvažme třeba funkci $f(x,y) = x^2 + y^2$, jejímž grafem je rotační paraboloid s počátkem v bodě $(0,0)$. Ten můžeme implicitně zadat také rovnicí

$$0 = F(x,y,z) = z - x^2 - y^2.$$

Proto je

$$d^2L(x,y) = \left[\tfrac{2}{x^3} - \tfrac{6\lambda}{x^4} + \left(\tfrac{2}{y^3} - \tfrac{6\lambda}{y^4}\right)\tfrac{y^6}{x^6}\right]dx^2.$$

Uvažujeme vlastně jednorozměrnou kvadratickou formu, jejíž pozitivní (negativní) definitnost ve stacionárním bodě znamená, že v tomto bodě je minimum (maximum). Uvědomíme-li si, že pro stacionární body bylo $x = 2\lambda$, $y = 2\lambda$, pouhým dosazením získáváme

$$d^2L\left(\tfrac{\sqrt2}{2},\tfrac{\sqrt2}{2}\right) = -4\sqrt2\,dx^2, \quad d^2L\left(-\tfrac{\sqrt2}{2},-\tfrac{\sqrt2}{2}\right) = 4\sqrt2\,dx^2,$$

což znamená, že v bodě $\left[\sqrt2/2, \sqrt2/2\right]$ má funkce $f$ ostré lokální maximum a v bodě $\left[-\sqrt2/2, -\sqrt2/2\right]$ potom ostré lokální minimum. Ještě doplňme hodnoty

$$f\left(\frac{\sqrt2}{2},\frac{\sqrt2}{2}\right) = 2\sqrt2, \quad f\left(-\frac{\sqrt2}{2},-\frac{\sqrt2}{2}\right) = -2\sqrt2. \tag{8.5}$$

Nyní si ukážeme rychlejší způsob, jak jsme mohli dospět k výsledku. Známe (příp. snadno určíme) druhé parciální derivace funkce $L$, tj. její Hessián vzhledem k proměnným $x$ a $y$:

$$HL(x,y) = \begin{pmatrix} \frac{2}{x^3} - \frac{6\lambda}{x^4} & 0 \\ 0 & \frac{2}{y^3} - \frac{6\lambda}{y^4} \end{pmatrix}.$$

Vyčíslením

$$HL\left(\frac{\sqrt2}{2},\frac{\sqrt2}{2}\right) = \begin{pmatrix} -2\sqrt2 & 0 \\ 0 & -2\sqrt2 \end{pmatrix},$$

$$HL\left(-\frac{\sqrt2}{2},-\frac{\sqrt2}{2}\right) = \begin{pmatrix} 2\sqrt2 & 0 \\ 0 & 2\sqrt2 \end{pmatrix}$$

pak zjistíme, že tato kvadratická forma je pro první stacionární bod negativně definitní (jedná se o ostré lokální maximum) a pozitivně definitní pro druhý stacionární bod (ostré lokální minimum).

Upozorněme na nebezpečí tohoto „rychlejšího“ přístupu, kdybychom obdrželi indefinitní formu (matici). V takovém případě bychom nemohli tvrdit, že v daném bodě extrém nenastává. Při nezačlenění vazebné podmínky (což jsme během výpočtu $d^2L$ provedli) totiž uvažujeme obecnější situaci. Grafem funkce $f$ na zadané množině je křivka, kterou lze zadat jako funkci jedné proměnné. Tomu musí odpovídat jednodimenzionální kvadratická forma. □

**8.56.** Nalezněte globální extrémy funkce

$$f(x,y) = \tfrac{1}{x} + \tfrac{1}{y}, \quad x \neq 0,\ y \neq 0$$

na množině bodů, které vyhovují rovnici $\frac{1}{x^2} + \frac{1}{y^2} = 4$.

**Řešení.** Na tomto příkladu si ukážeme, že hledání globálních extrémů může být výrazně snazší než hledání extrémů lokálních (viz předešlý příklad) také tehdy, když jsou uvažovány hodnoty funkce na neohraničené množině. Stejným způsobem jako v minulém příkladu

Než zformulujeme výsledek rovnou pro obecnou situaci, všimněme si ještě, jaké dimenze se mohou/mají v problému vyskytovat. Pokud bychom pro tuto funkci $F$ chtěli najít křivku $c(x) = (c_1(x), c_2(x))$ v rovině takovou, že

$$F(x, c(x)) = F(x, c_1(x), c_2(x)) = 0,$$

pak to jistě budeme umět (dokonce pro všechny počáteční podmínky $x = a$) také, ale výsledek nebude jednoznačný pro danou počáteční podmínku. Stačí totiž uvážit libovolnou křivku na rotačním paraboloidu, jejíž průmět do první souřadnice má nenulovou derivaci. Pak považujeme $x$ za parametr křivky a za $c(x)$ zvolíme její průmět do roviny $yz$.



Očekáváme tedy, že jedna funkce $m+1$ proměnných zadává implicitně nadplochu v $\mathbb{R}^{m+1}$, kterou chceme vyjádřit alespoň lokálně jako graf jedné funkce v $m$ proměnných. Lze očekávat, že $n$ funkcí v $m+n$ proměnných bude zadávat průnik $n$ nadploch v $\mathbb{R}^{m+n}$, což je ve „většině“ případů $m$–rozměrný objekt.

Uvažujme proto diferencovatelné zobrazení

$$F = (f_1, \dots, f_n) : \mathbb{R}^{m+n} \to \mathbb{R}^n.$$

Jacobiho matice tohoto zobrazení bude mít $n$ řádků a $m+n$ sloupců a můžeme si ji symbolicky zapsat jako

$$D^1F = (D^1_xF, D^1_yF) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \dots & \frac{\partial f_1}{\partial x_m} & \frac{\partial f_1}{\partial x_{m+1}} & \dots & \frac{\partial f_1}{\partial x_{m+n}} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \dots & \frac{\partial f_n}{\partial x_m} & \frac{\partial f_n}{\partial x_{m+1}} & \dots & \frac{\partial f_n}{\partial x_{m+n}} \end{pmatrix},$$

kde $(x_1, \dots, x_{m+n}) \in \mathbb{R}^{m+n}$ zapisujeme jako $(x,y) \in \mathbb{R}^m \times \mathbb{R}^n$, $D^1_xF$ je matice s $n$ řádky a prvními $m$ sloupci v Jacobiho matici, zatímco $D^1_yF$ je čtvercová matice řádu $n$ se zbylými sloupci. Vícerozměrnou analogií k předchozí úvaze s nenulovou parciální derivací podle $y$ je požadavek, aby matice $D^1_yF$ byla invertibilní.

### Věta o implicitním zobrazení

**Věta.** *Nechť $F : \mathbb{R}^{m+n} \to \mathbb{R}^n$ je zobrazení třídy $C^1$ na otevřeném okolí bodu $(a,b) \in \mathbb{R}^m \times \mathbb{R}^n = \mathbb{R}^{m+n}$, ve kterém je $F(a,b) = 0$ a $\det D^1_yF \neq 0$. Potom existuje diferencovatelné zobrazení $G : \mathbb{R}^m \to \mathbb{R}^n$ definované na nějakém okolí $U$ bodu $a \in \mathbb{R}^m$ s obrazem $G(U)$, který obsahuje bod $b$, a takové, že $F(x, G(x)) = 0$ pro všechny $x \in U$.*

*Navíc je Jacobiho matice $D^1G$ zobrazení $G$ na okolí bodu $a$ zadána součinem matic*

$$D^1G(x) = -(D^1_yF)^{-1}(x, G(x)) \cdot D^1_xF(x, G(x)).$$



Důkaz. Pro zvýšení srozumitelnosti uvedeme napřed kompletní důkaz pro nejjednodušší případ rovnice $F(x,y) = 0$ s funkcí $F$ dvou proměnných. Bude zdánlivě složitý, protože jej schválně vedeme tak, jak jej bude možné použít i pro obecné dimenze z věty. Rozšíříme funkci $F$ na

$$\tilde F : \mathbb{R}^2 \to \mathbb{R}^2, \quad (x,y) \mapsto (x, F(x,y)).$$

bychom ovšem nejprve stanovili stacionární body (‖8.4‖) a hodnoty (‖8.5‖). Raději zdůrazněme, že v tomto příkladu hledáme extrémy funkce na nekompaktní množině, a tak se nemůžeme spokojit s pouhým vyčíslením funkčních hodnot ve stacionárních bodech. Důvodem je, že funkce $f$ na uvažované množině vůbec nemusí maximální ani minimální hodnoty nabývat – její obor hodnot zde může být otevřeným intervalem. Ukažme si, že tomu tak ale není.

Uvažujme proto $|x| \geq 10$ a uvědomme si, že rovnici $\frac{1}{x^2} + \frac{1}{y^2} = 4$ mohou splňovat pouze hodnoty $y$, pro které je $|y| \geq 1/2$. Máme tak odhady

$$-2\sqrt{2} < -\tfrac{1}{10} - 2 \leq f(x,y) \leq \tfrac{1}{10} + 2 < 2\sqrt{2}, \quad \text{je-li} \quad |x| \geq 10.$$

Současně je (záměnou $x$ za $y$ dostaneme stejnou úlohu)

$$-2\sqrt{2} < -\tfrac{1}{10} - 2 \leq f(x,y) \leq \tfrac{1}{10} + 2 < 2\sqrt{2}, \quad \text{je-li} \quad |y| \geq 10.$$

Odtud vidíme, že globálních extrémů na uvedené množině musí funkce $f$ nabývat, a to uvnitř čtverce $ABCD$ s vrcholy v bodech $A = [-10,-10], B = [10,-10], C = [10,10], D = [-10,10]$. Jako průnik „stokrát zmenšeného“ čtverce s vrcholy $\tilde{A} = [-1/10,-1/10]$, $\tilde{B} = [1/10,-1/10], \tilde{C} = [1/10,1/10], \tilde{D} = [-1/10,1/10]$ a zadané množiny potom očividně dostaneme prázdnou množinu. Globální extrémy jsou tedy v bodech ve vnitřku kompaktní množiny ohraničené těmito dvěma čtverci. Neboť je na této množině $f$ spojitě diferencovatelná, globální extrémy mohou být jedině ve stacionárních bodech. Nutně je

$$f_{\max} = f\left(\tfrac{\sqrt{2}}{2}, \tfrac{\sqrt{2}}{2}\right) = 2\sqrt{2}, \quad f_{\min} = f\left(-\tfrac{\sqrt{2}}{2}, -\tfrac{\sqrt{2}}{2}\right) = -2\sqrt{2}.$$

□

**8.57.** Určete maximální a minimální hodnotu, kterých nabývá funkce $f(x,y,z) = xyz$ na množině $M$ vymezené podmínkami

$$x^2 + y^2 + z^2 = 1, \quad x + y + z = 0.$$

**Řešení.** Není obtížné si uvědomit, že $M$ je kružnice. V rámci řešení úlohy však postačuje vědět, že je $M$ kompaktní, tj. ohraničená (první podmínka je rovnice jednotkové sféry – kulové plochy) a uzavřená (množina, která je řešením uvedených rovnic, je uzavřená, neboť z platnosti těchto rovnic pro všechny členy jisté konvergentní posloupnosti vyplývá jejich platnost pro limitu této posloupnosti). Funkce $f$ i vazebné funkce $F(x,y,z) = x^2 + y^2 + z^2 - 1$, $G(x,y,z) = x + y + z$ mají spojité parciální derivace všech řádů (jsou to polynomy). Jacobiho matice vazeb pak je

$$\begin{pmatrix} F_x(x,y,z) & F_y(x,y,z) & F_z(x,y,z) \\ G_x(x,y,z) & G_y(x,y,z) & G_z(x,y,z) \end{pmatrix} = \begin{pmatrix} 2x & 2y & 2z \\ 1 & 1 & 1 \end{pmatrix}.$$

Jacobiho matice zobrazení $\tilde{F}$ je

$$D^1\tilde{F}(x,y) = \begin{pmatrix} 1 & 0 \\ F_x(x,y) & F_y(x,y) \end{pmatrix}.$$

Z předpokladu $F_y(a,b) \neq 0$ vyplývá, že totéž platí i na nějakém okolí bodu $(a,b)$ a tedy je na tomto okolí funkce $\tilde{F}$ invertibilní podle věty o inverzním zobrazení. Uvažme tedy jednoznačně definované a diferencovatelné inverzní zobrazení $\tilde{F}^{-1}$ na nějakém okolí bodu $(a,0)$.

Nyní označme $\pi : \mathbb{R}^2 \to \mathbb{R}$ projekci na druhou souřadnici a uvažujme funkci $f(x) = \pi \circ \tilde{F}^{-1}(x,0)$. To je dobře definovaná a diferencovatelná funkce. Máme ověřit, že následující výraz

$$F(x, f(x)) = F(x, \pi(\tilde{F}^{-1}(x,0)))$$

bude na okolí bodu $x = a$ nulový. Přitom z definice $\tilde{F}(x,y) = (x, F(x,y))$ vyplývá, že i její inverze musí mít tvar $\tilde{F}^{-1}(x,y) = (x, \pi\tilde{F}^{-1}(x,y))$. Můžeme proto pokračovat v předchozím výpočtu:

$$F(x, f(x)) = \pi(\tilde{F}(x, \pi(\tilde{F}^{-1}(x,0)))) = \\ = \pi(\tilde{F}(\tilde{F}^{-1}(x,0))) = \pi(x,0) = 0.$$

Tím máme dokázánu první část věty a zbývá spočíst derivaci funkce $f(x)$. Tuto derivaci můžeme odečíst opět z věty o inverzním zobrazení pomocí matice $(D^1\tilde{F})^{-1}$.

Následující výsledek je snadné ověřit roznásobením matic. (Spočíst lze také přímo explicitní formulí pro inverzní matici s pomocí determinantu a algebraicky adjungované matice, viz odstavec 2.23)

$$\begin{pmatrix} 1 & 0 \\ F_x(x,y) & F_y(x,y) \end{pmatrix}^{-1} = (F_y(x,y))^{-1} \begin{pmatrix} F_y(x,y) & 0 \\ -F_x(x,y) & 1 \end{pmatrix}.$$

Dle definice $f(x) = \pi\tilde{F}^{-1}(x,0)$ nás z této matice zajímá první položka na druhém řádku, která je právě Jacobiho maticí $D^1 f$. V našem jednoduchém případě je to právě požadovaný skalár $-F_x(x, f(x))/F_y(x, f(x))$.



Obecný důkaz je bezezbytku stejný, není v něm potřeba změnit žádný z uvedených vztahů (všechny položky v nich jen dostanou vektorový smysl), kromě posledního výpočtu derivace funkce $f$, kde místo jednotlivých parciálních derivací budou vystupovat příslušné části Jacobiho matice $D^1_x F$ a $D^1_y F$. Samozřejmě je přitom třeba místo se skaláry pracovat s vektory a maticemi.

Pro výpočet Jacobiho matice zobrazení $G$ opět použijeme výpočtu inverzní matice, není ale až tak vhodné přímo využít postupu z odstavce 2.23. Snadnější je nechat se přímo inspirovat případem v dimenzi $m + n = 2$, označit si matici

$$(D^1\tilde{F}^{-1}) = \begin{pmatrix} E_m & 0 \\ D^1_x F(x,y) & D^1_y F(x,y) \end{pmatrix}^{-1} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

s bloky danými dělením na $m$ a $n$ řádků i sloupců (tj. např. $A$ má rozměr $m \times m$, zatímco $C$ je rozměru $n \times m$) a přímo spočíst matice $A, B, C, D$ z definiční rovnosti pro inverzi:

$$\begin{pmatrix} E_m & 0 \\ D^1_x F(x,y) & D^1_y F(x,y) \end{pmatrix} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} E_m & 0 \\ 0 & E_n \end{pmatrix}.$$

Její hodnost je snížena (menší než 2), právě když je vektor $(2x, 2y, 2z)$ násobkem vektoru $(1, 1, 1)$, což dává $x = y = z$ a podle druhé ze zadaných podmínek dále $x = y = z = 0$. Ovšem množina $M$ počátek neobsahuje. Nic nám tedy nebrání hledat stacionární body použitím metody Lagrangeových multiplikátorů. Pro

$$L(x, y, z, \lambda_1, \lambda_2) = xyz - \lambda_1 \left(x^2 + y^2 + z^2 - 1\right) - \lambda_2 (x + y + z)$$

rovnice $L_x = 0, L_y = 0, L_z = 0$ po řadě dávají

$$yz - 2\lambda_1 x - \lambda_2 = 0,$$

$$xz - 2\lambda_1 y - \lambda_2 = 0,$$

$$xy - 2\lambda_1 z - \lambda_2 = 0.$$

Odečtením první rovnice od druhé a od třetí dostaneme

$$xz - yz - 2\lambda_1 y + 2\lambda_1 x = 0,$$

$$xy - yz - 2\lambda_1 z + 2\lambda_1 x = 0,$$

tj. po úpravě

$$(x - y)\,(z + 2\lambda_1) = 0,$$

$$(x - z)\,(y + 2\lambda_1) = 0.$$

Poslední rovnice jsou splněny v těchto čtyřech případech

$$x = y, x = z; \quad x = y, y = -2\lambda_1;$$

$$z = -2\lambda_1, x = z; \quad z = -2\lambda_1, y = -2\lambda_1,$$

tedy (zahrnutím podmínky $G = 0$)

$$x = y = z = 0; \quad x = y = -2\lambda_1, z = 4\lambda_1;$$

$$x = z = -2\lambda_1, y = 4\lambda_1; \quad x = 4\lambda_1, y = z = -2\lambda_1.$$

S výjimkou prvního případu (který zřejmě nemůže být splněn) začleněním podmínky $F = 0$ obdržíme

$$(4\lambda_1)^2 + (-2\lambda_1)^2 + (-2\lambda_1)^2 = 1, \quad \text{tj.} \quad \lambda_1 = \pm\tfrac{1}{2\sqrt{6}}.$$

Celkem tak získáváme body

$$\left[-\tfrac{1}{\sqrt{6}}, -\tfrac{1}{\sqrt{6}}, \tfrac{2}{\sqrt{6}}\right], \quad \left[-\tfrac{1}{\sqrt{6}}, \tfrac{2}{\sqrt{6}}, -\tfrac{1}{\sqrt{6}}\right], \quad \left[\tfrac{2}{\sqrt{6}}, -\tfrac{1}{\sqrt{6}}, -\tfrac{1}{\sqrt{6}}\right],$$

$$\left[\tfrac{1}{\sqrt{6}}, \tfrac{1}{\sqrt{6}}, -\tfrac{2}{\sqrt{6}}\right], \quad \left[\tfrac{1}{\sqrt{6}}, -\tfrac{2}{\sqrt{6}}, \tfrac{1}{\sqrt{6}}\right], \quad \left[-\tfrac{2}{\sqrt{6}}, \tfrac{1}{\sqrt{6}}, \tfrac{1}{\sqrt{6}}\right].$$

Nebudeme ověřovat, zda se jedná o stacionární body. Důležité je, že v této šestici jsou zahrnuty všechny stacionární body.

Hledáme globální maximum a minimum spojité funkce $f$ na kompaktní množině $M$. Globální extrémy (o kterých víme, že existují) však mohou být pouze v bodech lokálních extrémů vzhledem k $M$. Tyto lokální extrémy pak musí být v některém z uvedených bodů. Proto pouze

Zjevně odtud plyne $A = E_m$, $B = 0$, $D = (D_y^1 F)^{-1}$ a konečně $D_x^1 F + D_y^1 F \cdot C = 0$. Z poslední rovnosti pak dostáváme požadovaný vztah

$$D^1 G = C = -(D_y^1 F)^{-1} \cdot D_x^1 F.$$

Tím je věta dokázána. □

**8.19. Gradient funkce.** Jak jsme viděli v minulém odstavci, je-



li $F$ spojitě diferencovatelná funkce $n$ proměnných, zadává předpis $F(x_1, \ldots, x_n) = b$ s nějakou pevnou hodnotou $b \in \mathbb{R}$ podmnožinu $M \subset \mathbb{R}^n$, která mívá vlastnosti $(n-1)$–rozměrné nadplochy. Přesněji řečeno, pokud je vektor parciálních derivací

$$D^1 F = \left(\frac{\partial F}{\partial x_1}, \ldots, \frac{\partial F}{\partial x_n}\right)$$

nenulový, můžeme lokálně množinu $M$ popsat jako graf spojitě diferencovatelné funkce v $n-1$ proměnných. Hovoříme v této souvislosti také o *úrovňových množinách* $M_b$. Vektor $D^1 F \in \mathbb{R}^n$ se nazývá *gradient funkce* $F$. V technické a fyzikální literatuře se často zapisuje také jako grad $F$, případně také $\nabla F$.

Protože je $M_b$ zadáno pomocí konstantní hodnoty funkce $F$, budou derivace křivek ležících v $M$ mít jistě tu vlastnost, že na nich bude diferenciál $dF$ vždy vyčíslen nulově – skutečně, pro každou takovou křivku bude $F(c(t)) = b$ a tedy i

$$\frac{d}{dt} F(c(t)) = dF(c'(t)) = 0.$$

Naopak uvažme obecný vektor $v = (v_1, \ldots, v_n) \in \mathbb{R}^n$ a velikost příslušné směrové derivace

$$|d_v F| = \left|\frac{\partial f}{\partial x_1} v_1 + \cdots + \frac{\partial f}{\partial x_n} v_n\right| = \cos\varphi \, \|D^1 F\| \|v\|$$

kde $\varphi$ je odchylka vektoru $v$ od gradientu $F$, viz pojednání o odchylkách vektorů a přímek ve čtvrté kapitole (definice 4.18).

Odtud ovšem vyplývá, že nulové jsou právě ty směrové derivace, které jsou kolmé na gradient, zatímco směr zadaný gradientem je právě ten směr, ve kterém funkce $F$ nejrychleji roste.

Protože je tečná rovina k neprázdné úrovňové množině $M_b$ v okolí jejího bodu dána derivacemi křivek v ní ležících, budenenulový gradientem $D^1 F$ tzv. *normálovým vektorem* nadplochy $M_b$. Zaměření tečné roviny je tedy ortogonálním doplňkem gradientu.

Např. pro sféru v $\mathbb{R}^3$ o poloměru $r > 0$ a středu $(a, b, c)$ zadanou rovnicí

$$F(x, y, z) = (x - a)^2 + (y - b)^2 + (z - c)^2 = r^2$$

dostáváme normálové vektory v bodě $P = (x_0, y_0, z_0)$ jako nenulový násobek gradientu, tj. násobek průvodiče

$$D^1 F = (2(x_0 - a), 2(y_0 - b), 2(z_0 - c)),$$

a tečné vektory budou právě všechny vektory kolmé na gradient. Implicitně proto jde vždy tečnou rovinu ke sféře v bodě $P$ popsat s pomocí gradientu rovnicí

$$0 = (x_0 - a)(x - x_0) + (y_0 - b)(y - y_0) + (z_0 - c)(z - z_0).$$

To je speciální případ obecné formule:

vyčíslíme funkci $f$ v těchto bodech. Tím zjistíme, že hledané maximum je

$$f\left(-\frac{1}{\sqrt{6}},-\frac{1}{\sqrt{6}},\frac{2}{\sqrt{6}}\right)=f\left(-\frac{1}{\sqrt{6}},\frac{2}{\sqrt{6}},-\frac{1}{\sqrt{6}}\right)=$$
$$=f\left(\frac{2}{\sqrt{6}},-\frac{1}{\sqrt{6}},-\frac{1}{\sqrt{6}}\right)=\frac{1}{3\sqrt{6}}$$

a minimum potom

$$f\left(\frac{1}{\sqrt{6}},\frac{1}{\sqrt{6}},-\frac{2}{\sqrt{6}}\right)=f\left(\frac{1}{\sqrt{6}},-\frac{2}{\sqrt{6}},\frac{1}{\sqrt{6}}\right)=$$
$$=f\left(-\frac{2}{\sqrt{6}},\frac{1}{\sqrt{6}},\frac{1}{\sqrt{6}}\right)=-\frac{1}{3\sqrt{6}}.$$

□

**8.58.** Určete, ve kterých bodech nastávají extrémy funkce $f:\mathbb{R}^3\to\mathbb{R}$, $f(x,y,z)=x^2+y^2+z^2$, na rovině $x+y-z=1$ a určete, o jaké extrémy se jedná.

**Řešení.** Snadno sestavíme rovnice rovnice popisující lineární závislost normály k vazební ploše a gradientu zkoumané funkce:

$$x=k,\ \ y=k\ z=-k,\quad k\in\mathbb{R},$$

jejichž jediným řešením je bod $[\frac{1}{3},\frac{1}{3},-\frac{1}{3}]$. Navíc si všimneme, že funkce roste ve směru (1,-1,0) a tento směr náleží do vazební roviny. V získaném bodě tedy musí nastávat minimum zkoumané funkce.

**Jiné řešení.** Úlohu převedeme na vyšetření extrému funkce dvou reálných proměnných na $\mathbb{R}^2$. Vazební podmínka je totiž lineární a snadno z ní vyjádříme $z=x+y-1$. Dosazením do zadané funkce pak získáme reálnou funkci dvou proměnných: $f(x,y)=x^2+y^2+(x+y-1)^2=2x^2+2xy+y^2-2x-2y+1$. Položením obou parciálních derivací rovno nule, dostáváme lineární soustavu

$$4x+2y-2=0,\quad 4y+2x-2=0,$$

jejímž jediným řešením je bod $[\frac{1}{3},\frac{1}{3}]$. Protože se jedná o kvadratickou funkci s kladnými koeficienty u neznámých, je tato na $\mathbb{R}^2$ neomezená a tudíž v získaném bodě nastává (globální) minimum. Z úvodního lineárního vyjádření proměnné $z$ pak získáme odpovídající bod ve vazební rovině: $[\frac{1}{3},\frac{1}{3},-\frac{1}{3}]$. □

**8.59.** Určete body, ve kterých nastávají extrémy funkce $x+y:\mathbb{R}^3\to\mathbb{R}$ na kružnici dané rovnicemi $x+y+z=1$ a $x^2+y^2+z^2=4$.

**Řešení.** „Podezřelé“ body jsou body, pro které platí

$$(1,1,0)=k\cdot(1,1,1)+l\cdot(x,y,z),\quad k,l\in\mathbb{R}.$$

### Tečná nadrovina implicitně zadané nadplochy

**Věta.** *Pro reálnou funkci $F(x_1,\dots,x_n)$ v $n$ proměnných a bod $P=(a_1,\dots,a_n)$ v úrovňové množině $M_b=\{x\in\mathbb{R}^n;\ F(x)=b\}$ funkce $F$, v jehož okolí je $M_b$ grafem funkce $(n-1)$ proměnných, je implicitní rovnice pro tečnou nadrovinu k $M_b$ dána vztahem*

$$0=\frac{\partial F}{\partial x_1}(P)\cdot(x_1-a_1)+\cdots+\frac{\partial F}{\partial x_n}(P)\cdot(x_n-a_n).$$

Důkaz. Tvrzení je zřejmé z předchozího výkladu. Tečná nadrovina totiž musí být $(n-1)$–rozměrná, její zaměření je proto zadané jako jádro lineární formy dané gradientem (nulové hodnoty příslušného lineárního zobrazení $\mathbb{R}^n\to\mathbb{R}$ zadaného násobení sloupce souřadnic řádkovým vektorem grad $F$). Zvolený bod $P$ přitom naší rovnici zjevně vyhovuje. □

**8.20. Model osvětlení 3D objektů.** Uvažujme osvětlení 3D objektu, kde známe směr $v$ dopadu světla na 2D povrch tohoto objektu, tj. množinu $M$ zadanou implicitně nějakou rovnicí $F(x,y,z)=0$. Intenzitu osvětlení bodu $P\in M$ definujme jako $I\cos\varphi$, kde $\varphi$ je úhel mezi normálou k $M$ a vektorem opačným ke směru toku světla.. Jak jsme viděli, normála je určena gradientem funkce $F$. Znaménko našeho výrazu pak bude označovat, kterou stranu plochy osvětlujeme.

Uvažujme např. osvětlení o intenzitě $I_0$ ve směru vektoru $v=(1,1,-1)$ (tj. „šikmo dolů“) a za objekt zvolme kouli zadanou rovnicí $F(x,y,z)=x^2+y^2+z^2-1\le 0$. Pro povrchový bod $P=(x,y,z)\in M$ proto dostaneme intenzitu

$$I(P)=\frac{\operatorname{grad}F\cdot v}{\|\operatorname{grad}F\|\|v\|}I_0=\frac{-2x-2y+2z}{2\sqrt{3}}I_0.$$

Všimněme si, že dle očekávání je maximální (plnou) intenzitou $I_0$ osvětlen bod $P=\frac{1}{\sqrt{3}}(-1,-1,1)$ na povrchu koule.

**8.21. Tečné a normálové prostory.** Přejděme nyní s našimi úvahami o tečnách a normálách k obecným dimenzím.



Máme-li zobrazení $F:\mathbb{R}^{m+n}\to\mathbb{R}^n$, se souřadnými funkcemi $f_i$, můžeme opět uvažovat $n$ rovnic pro $n+m$ proměnných

$$f_i(x_1,\dots,x_{m+n})=b_i,\quad i=1,\dots,n,$$

vyjadřujících rovnost $F(x)=b$ pro vektor $b\in\mathbb{R}^n$.

Pak, za podmínek věty o implicitní funkci, je množina všech řešení $(x_1,\dots,x_{m+n})\in\mathbb{R}^{m+n}$ alespoň lokálně grafem zobrazení $G:\mathbb{R}^m\to\mathbb{R}^n$.

Pro pevnou volbu $b=(b_1,\dots,b_n)$ je samozřejmě množinou všech řešení průnik nadploch $M(b_i,f_i)$ příslušejících jednotlivým funkcím $f_i$. Totéž musí platit pro tečné směry, zatímco normálové směry jsou generovány jednotlivými gradienty. Proto je-li $D^1F$ Jacobiho matice zobrazení implicitně zadávajícího množinu $M$ s bodem $P=(a_1,\dots,a_{m+n})\in M$, v jehož okolí je $M$ grafem zobrazení,

$$D^1F=\begin{pmatrix}\frac{\partial f_1}{\partial x_1}&\cdots&\frac{\partial f_1}{\partial x_{m+n}}\\ \vdots&\ddots&\vdots\\ \frac{\partial f_n}{\partial x_1}&\cdots&\frac{\partial f_n}{\partial x_{m+n}}\end{pmatrix},$$

Zřejmě $x = y(= 1/l)$. Dosazením do rovnic kružnice pak získáme dvojici řešení

$$\left[\frac{1}{3} \pm \frac{\sqrt{22}}{6}, \frac{1}{3} \pm \frac{\sqrt{22}}{6}, \frac{1}{3} \mp \frac{\sqrt{22}}{3}\right].$$

Vzhledem ke kompaktnosti kružnice stačí prověřit funkční hodnoty v těchto dvou bodech. Zjišťujeme, že v prvním bodě nastává maximum a v druhém minimum dané funkce na kružnici. □

*8.60.* Určete, ve kterých bodech nastávají extrémy funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x, y, z) = x^2 + y^2 + z^2$, na rovině $2x + y - z = 1$ a určete, o jaké extrémy se jedná. ○

*8.61.* Určete maximum funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = xy$ na kružnici o poloměru 1 se středem v bodě $[x_0, y_0] = [0, 1]$. ○

*8.62.* Určete, ve kterých bodech nastává minimum funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f = xy$ na kružnici o poloměru 1 se středem v bodě $[x_0, y_0] = [2, 0]$. ○

*8.63.* Určete, ve kterých bodech nastává minimum funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f = xy$ na kružnici o poloměru 1 se středem v bodě $[x_0, y_0] = [2, 0]$. ○

*8.64.* Určete, ve kterých bodech nastává minimum funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f = xy$ na elipse $x^2 + 3y^2 = 1$. ○

*8.65.* Určete, ve kterých bodech nastává minimum funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f = x^2 y$ na kružnici o poloměru jedna se středem v bodě $[x_0, y_0] = [0, 0]$. ○

*8.66.* Určete maximum funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^3 y$ na kružnici $x^2 + y^2 = 1$. ○

*8.67.* Určete maximum funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = xy$ na elipse $2x^2 + 3y^2 = 1$. ○

*8.68.* Určete maximum funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = xy$ na elipse $x^2 + 2y^2 = 1$. ○

### H. Objemy, povrchy, těžiště těles

**8.69.** Určete objem tělesa ležícího v polorovině $z \geq 0$, ve válci $x^2 + y^2 \leq 1$ a v polorovině

a) $z \leq x$,

b) $x + y + z \leq 0$.

potom bude afinní podprostor v $\mathbb{R}^{m+n}$ obsahující právě všechny tečny procházející bodem $P$ dán implicitně rovnicemi:

$$0 = \frac{\partial f_1}{\partial x_1}(P) \cdot (x_1 - a_1) + \cdots + \frac{\partial f_1}{\partial x_n}(P) \cdot (x_{m+n} - a_{m+n})$$

$$\vdots$$

$$0 = \frac{\partial f_n}{\partial x_1}(P) \cdot (x_1 - a_1) + \cdots + \frac{\partial f_n}{\partial x_n}(P) \cdot (x_{m+n} - a_{m+n}).$$

Tento podprostor se nazývá *tečný prostor* k (implicitně zadané) $m$–rozměrné ploše $M$ v bodě $P$.

*Normálový prostor* v bodě $P$ je afinní podprostor generovaný bodem $P$ a gradienty všech funkcí $f_1, \ldots, f_n$ v bodě $P$, tj. řádky Jacobiho matice $D^1 F$.

Jako jednoduchý příklad si spočtěme tečnu a normálový prostor ke kuželosečce v $\mathbb{R}^3$. Uvažujme rovnici kuželu s vrcholem v počátku

$$0 = f(x, y, z) = z - \sqrt{x^2 + y^2}$$

a rovinu zadanou

$$0 = g(x, y, z) = z - 2x + y + 1.$$

Bod $P = (1, 0, 1)$ patří jak kuželu tak rovině a průnik $M$ těchto dvou ploch je křivka (namalujte si obrázek). Její tečnou v bodě $P$ bude přímka zadaná rovnicemi

$$\begin{aligned} 0 &= -\frac{1}{2\sqrt{x^2 + y^2}} 2x \Big|_{x=1, y=0} \cdot (x - 1) \\ &\quad - \frac{1}{2\sqrt{x^2 + y^2}} 2y \Big|_{x=1, y=0} \cdot y + 1 \cdot (z - 1) \\ &= -x + z \\ 0 &= -2(x - 1) + y + (z - 1) = -2x + y + z + 1, \end{aligned}$$

zatímco rovina kolmá k naší křivce bodem $P$ bude parametricky dána výrazem

$$(1, 0, 1) + \tau(-1, 0, 1) + \sigma(-2, 1, 1)$$

s parametry $\tau$ a $\sigma$.

**8.22. Vázané extrémy.** Nyní se dostáváme k první opravdu vážné aplikaci diferenciálního počtu více proměnných. Typickou úlohou optimalizace nebo řízení je najít extrémy hodnot závisejících na několika (ale konečně mnoha) parametrech, ovšem za nějakých dalších podmínek na vzájemné vztahy parametrů.

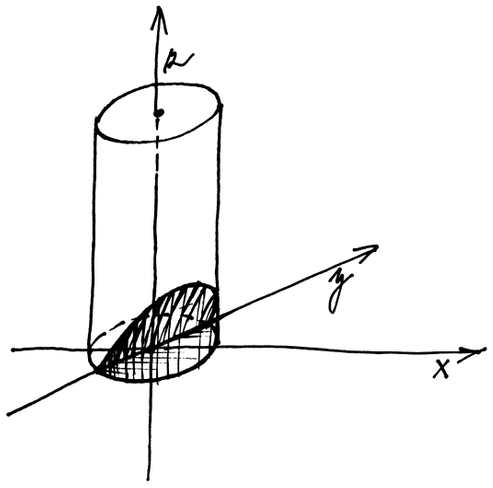


Velice často má řešená úloha $m + n$ parametrů, které jsou vázány $n$ podmínkami. V našem jazyce diferenciálního počtu tedy hledáme extrémy diferencovatelné funkce $h$ na množině bodů $M$ zadaných implicitně rovnicí $F(x_1, \ldots, x_{m+n}) = 0$. K tomu již máme připraveny účinné postupy.

Pro každou křivku $c(t) \subset M$ procházející přes $P = c(0)$ musí být $h(c(t))$ extrémem pro tuto funkci jedné proměnné. Proto také musí být derivace

$$\frac{d}{dt} h(c(t))_{|t=0} = d_{c'(0)} h(P) = dh(P)(c'(0)) = 0.$$

To ale znamená, že diferenciál funkce $h$ se v bodě $P$ nuluje na všech tečných přírůstcích k $M$ v bodě $P$. Tato vlastnost je ekvivalentní tvrzení, že gradient $h$ leží v normálovém podprostoru




**Řešení.** a) Objem spočítáme pohodlně s využitím válcových souřadnic. V nich je válec určen nerovnicí $r \le 1$, polorovinu $z \le x$ pak zapíšeme jako $z \le r\cos\varphi$. Celkem dostáváme

$$V = \int_0^1 \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \int_0^{r\cos\varphi} r \,\mathrm{d}z\,\mathrm{d}\varphi\,\mathrm{d}r = \frac{2}{3}.$$

b) Tuto úlohu převedeme na úlohu zcela analogickou části a) pomocí rotace kolem osy $z$ o úhel $\pi/4$ (ať už v kladném či záporném smyslu). Aplikací matice rotace $\begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/2 & 0 \\ \sqrt{2}/2 & \sqrt{2}/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ dostáváme v nových souřadnicích $(x', y', z')$ z nerovnice $x + y + z \le 0$ nerovnici $\sqrt{2}x' + z' \le 0$. Nyní již snadno zapíšeme integrál udávající objem zkoumaného tělesa:

$V = \int_0^1 \int_{\frac{\pi}{2}}^{\frac{3\pi}{2}} \int_{-\sqrt{2}r\cos\varphi}^0 r \,\mathrm{d}z\,\mathrm{d}\varphi\,\mathrm{d}r = \frac{2\sqrt{2}}{3}$. Výsledek jsme mohli z části (a) odvodit bez výpočtu, pokud bychom si všimli, že tělesa se jsou po rotaci stejná až na stejnolehlost s koeficientem $\sqrt{2}$ ve směru osy $y$. Viz též poznámka ‖8.79‖. □

**8.70.** Určete objem tělesa v $\mathbb{R}^3$, které je dáno nerovnostmi $x^2 + y^2 + z^2 \le 1$, $3x^2 + 3y^2 \ge z^2$, $x \ge 0$.

**Řešení.**

(přesněji v jeho zaměření). Takové body $P \in M$ budeme nazývat *stacionární body* funkce $H$ vzhledem k vazbám $F$.

Jak jsme viděli v minulém odstavci, normálový prostor k naší množině $M$ je generován řádky Jacobiho matice zobrazení $F$ a stacionární body jsou proto ekvivalentně určeny následujícím tvrzením (užíváme zde popis souřadnic $(x, y) = (x_1, \dots, x_m, y_1, \dots, y_n) \in \mathbb{R}^{m+n}$):

METODA LAGRANGEOVÝCH MULTIPLIKÁTORŮ

**Věta.** *Nechť $F = (f_1, \dots, f_n) : \mathbb{R}^{m+n} \to \mathbb{R}^n$ je diferencovatelná v okolí bodu $P$, $F(P) = 0$. Dále nechť $M$ je zadána implicitně rovnicí $F(x, y) = 0$ a hodnost matice $D^1F$ v bodě $P$ je $n$. Pak $P$ je stacionárním bodem spojitě diferencovatelné funkce $h : \mathbb{R}^{m+n} \to \mathbb{R}$ vzhledem k podmínkám $F$, právě když existují reálné parametry $\lambda_1, \dots, \lambda_n$ takové, že*

$$\operatorname{grad} h = \lambda_1 \operatorname{grad} f_1 + \cdots + \lambda_n \operatorname{grad} f_n.$$



Všimněme si, že *metoda Lagrangeových multiplikátorů* je algoritmická. Podívejme se nejprve na počty neznámých a rovnic: gradienty jsou vektory o $m+n$ souřadnicích, tedy požadavek z věty dává $m + n$ rovnic. Jako proměnné máme jednak souřadnice $x_1, \dots, x_{m+n}$ hledaných stacionárních bodů $P$ vzhledem k vazbám, ale navíc také $n$ parametrů $\lambda_i$ v hledané lineární kombinaci. Zbývá však požadavek, že hledaný bod $P$ patří implicitně zadané množině $M$, což představuje dalších $n$ rovnic. Celkem tedy máme $2n + m$ rovnic pro $2n + m$ proměnných, a proto lze očekávat, že řešením bude diskrétní množina bodů $P$ (tj. každý z nich bude izolovaným bodem).

**8.23. Nerovnost mezi aritmetickým a geometrickým průměrem.** Jako příklad praktického použití metody Lagrangeových multiplikátorů dokážeme nerovnost

$$\frac{1}{n}(x_1 + \cdots + x_n) \ge \sqrt[n]{x_1 \cdots x_n}$$

pro jakýchkoliv $n$ kladných reálných čísel $x_1, \dots, x_n$, přičemž rovnost nastane, právě když jsou si všechna $x_i$ rovna.

Uvažme tedy součet $x_1 + \cdots + x_n = c$ jako vazebnou podmínku pro nějakou blíže neurčenou nezápornou konstantu $c$. Budeme hledat maxima a minima funkce

$$f(x_1, \dots, x_n) = \sqrt[n]{x_1 \cdots x_n}$$

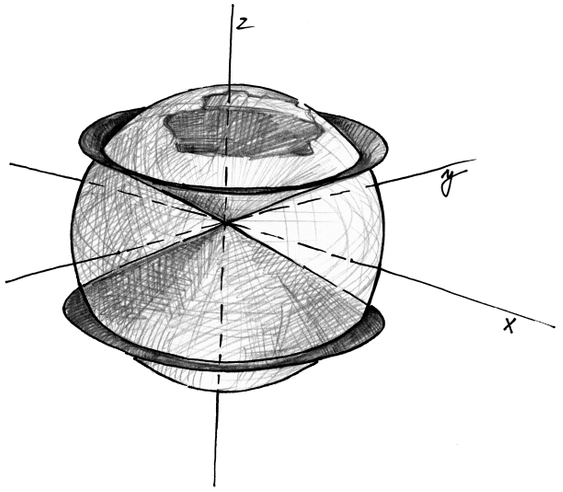
za naší vazební podmínky a předpokladu $x_1 > 0, \dots, x_n > 0$.

Normálový vektor k nadrovině definované podmínkou je $(1, \dots, 1)$. Extrém funkce $f$ tedy může nastat pouze v bodech, kdy je její gradient násobkem tohoto normálového vektoru. Pro hledané body tedy dostáváme soustavu rovnic

$$\frac{1}{n}\frac{1}{x_i}\sqrt[n]{x_1 \cdots x_n} = \lambda,$$

pro $i = 1, \dots, n$ a $\lambda \in \mathbb{R}$.

Tato soustava má zjevně na zkoumané množině jediné řešení $x_1 = \cdots = x_n$. Pokud bychom uvažovali i nulové hodnoty $x_i$, byla by naše množina $M$ zadaná omezením kompaktní, a proto by na ní musela mít funkce $f$ jak maximum, tak minimum. Minimum však zjevně dosahuje, právě když je některá z hodnot $x_i$ nulová, v našem bodě s $x_i = \frac{c}{n}$, $i = 1, \dots, n$, nabývá tedy nutně ostrého maxima.




Nejprve si uvědomme, o jaké těleso se jedná. Jde o část zadané koule, která leží vně daného kužele (viz obr.).

Objem spočítáme asi nejlépe jako rozdíl objemu poloviny koule a poloviny kulové výseče dané zadaným kuželem (všimněme si, že objem tělesa se nezmění, nahradíme-li podmínku $x \geq 0$ podmínkou $z \geq 0$ – výseč řežeme buď „vodorovně“ nebo „svisle“, ale vždy napůl) Budeme počítat ve sférických souřadnicích.

$$\begin{aligned} x &= r\cos(\varphi)\sin(\psi), \\ y &= r\sin(\varphi)\sin(\psi), \\ z &= r\cos(\psi), \end{aligned}$$

$\varphi \in [0, 2\pi)$, $\psi \in [0, \pi)$, $r \in (0, \infty)$.

Tato transformace $\mathbb{R}^3 \to \mathbb{R}^3$ má jakobián $r^2 \sin(\psi)$.

Určeme nejprve objem koule. Integrační meze: je vhodné si vyjádřit podmínky, kterými je těleso omezeno v souřadnicích, ve kterých budeme počítat. Ve sférických souřadnicích je koule dána nerovnicí

$$x^2 + y^2 + z^2 = r^2 \leq 1.$$

Hledejme integrační meze nejprve například pro proměnnou $\varphi$. Označíme-li $\pi_\varphi$ projekci na souřadnici $\varphi$ ve sférických souřadnicích ($\pi_\varphi(\varphi, \theta, r) = \varphi$), pak obraz projekce $\pi_\varphi$ uvažovaného tělesa nám udává integrační meze proměnné $\varphi$. Víme, že $\pi_\varphi(koule) = [0, 2\pi)$ (to víme buď díky naší prostorové představivosti, nebo z rovnice koule $r^2 \leq 1$, ve které proměnná $\varphi$ nevystupuje a nejsou na ni tedy kladena žádná omezení, nabývá tudíž všech možných hodnot).

Máme-li již meze jedné z proměnných určeny, můžeme určit meze další z proměnných. Tyto již mohou záviset na proměnných, jejichž meze jsme již určili (v tomto případě tomu tak nebude). Volíme tedy libovolně $\varphi_0 \in [0, 2\pi)$ a pro toto $\varphi_0$ (dále již pevně zvolené) určíme průnik tělesa (koule) s plochou $\varphi = \varphi_0$ a jeho projekci $\pi_\psi$ na proměnnou $\psi$. Opět jako při určování mezí pro $\varphi$ není proměnná $\psi$

Ve všech ostatních bodech s daným součtem souřadnic $c$ je pak hodnota jejich geometrického průměru menší a nerovnost je dokázána.

### 2. Integrování podruhé

Nyní se vrátíme k procesu integrování, který jsme částečně popsali v druhé části šesté kapitoly. Nepůjdeme do detailů a budeme se soustředit na rozšíření tohoto procesu pro veličiny závislé na více proměnných, případně závislé na parametrech.

**8.24. Integrály závislé na parametrech.** Jestliže integrujeme  (třeba ve smyslu Riemannova integrálu) podle jedné proměnné $x$ funkci $n + 1$ proměnných $f(x, y_1, \ldots, y_n)$, potom bude výsledek funkcí $F(y_1, \ldots, y_n)$ ve zbývajících proměnných.

Často se v praktických úlohách setkáváme s úkolem vyšetřovat právě takovou funkci $F$. Např. můžeme hledat objem, povrch nebo obsah tělesa závisejícího na parametrech a určit třeba minimální a maximální hodnoty (i s dodatečnými vazbami). Z první části této kapitoly víme, že pro takové účely máme nástroje opírající se o parciální derivace funkcí. Ideální by proto jistě bylo, kdybychom mohli operace derivování a integrování prohodit a za chvíli si to skutečně dokážeme. Začneme se studiem spojité závislosti na parametrech.

**Věta.** *Pro spojitou funkci $f(x, y_1, \ldots, y_n)$ definovanou pro všechna $x$ z konečného intervalu $[a, b]$ a všechna $(y_1, \ldots, y_n)$ z nějakého okolí $U$ bodu $c = (c_1, \ldots, c_n) \in \mathbb{R}^n$ uvažujme integrál*

$$F(y_1, \ldots, y_n) = \int_a^b f(x, y_1, \ldots, y_n)\, dx.$$

*Potom je i funkce $F(y_1 \ldots, y_n)$ spojitá na okolí $U$ bodu $c$.*

Důkaz. Pro ověření prvního tvrzení ve větě stačí vzpome-  nout definici Riemannova integrálu a již dříve ověřenou skutečnost, že spojitá funkce je na kompaktním množině ve skutečnosti stejnoměrně spojitá.

Zvolme si tedy okolí $W$ pevně zvoleného bodu $y$, tak aby pro všechny $\bar{y} \in W$ a všechna $x \in [a, b]$ platilo

$$|f(x, \bar{y}) - f(x, y)| < \varepsilon$$

pro zvolené malé kladné $\varepsilon$. Riemannův integrál je pro libovolnou spojitou funkci vyčíslen pomocí aproximací konečnými součty (ekvivalentně horními, dolními nebo Riemannovými součty s libovolnými reprezentanty $\xi_i$, viz odstavec 6.25 v šesté kapitole). Každý takový součet se ale pro zvolené parametry $\bar{y}$ a $y$ můžeme snadno odhadnout (nejprve použijeme trojúhelníkovou nerovnost při přechodu absolutní hodnoty do sumy a pak se opíráme o naši volbu okolí $W$)

$$\begin{aligned} \left| \sum_{i=0}^{k-1} f(\xi_i, \bar{y})(x_{i+1} - x_i) - \sum_{i=0}^{k-1} f(\xi_i, y)(x_{i+1} - x_i) \right| \\ \leq \sum_{i=0}^{k-1} \left| f(\xi_i, \bar{y}) - f(\xi_i, y) \right| (x_{i+1} - x_i) \\ < \varepsilon(b - a). \end{aligned}$$

Odtud však plyne, že i limitní hodnoty $F(y)$ a $F(\bar{y})$ se nemohou lišit o více než $\varepsilon(b - a)$, a jde proto o spojitou funkci. □

nijak omezena (ani nerovnicí $r^2 \leq 1$, ani rovnicí $\varphi = \varphi_0$] může tak nabývat všech svých hodnot, $\psi \in [0, \pi)$.

Konečně hledáme pro libovolně (dále ale pevně) zvolené $\varphi = \varphi_0$ a $\psi = \psi_0$ průmět $\pi_r(U)$ objektu (úsečky) $U$ dané omezeními $r^2 \leq 1$, $\varphi = \varphi_0$, $\psi = \psi_0$ na proměnnou $r$. Jediným omezením na $r$ je podmínka $r^2 \leq 1$, tedy $r \in (0, 1]$.

Všimněme si, že integrační meze proměnných jsou na sobě nezávislé, můžeme tedy integrovat v libovolném pořadí. Je tedy

$$V_{\text{koule}} = \int_0^1 \int_0^{2\pi} \int_0^{\pi} r^2 \sin(\psi)\, \mathrm{d}\psi\, \mathrm{d}\varphi\, \mathrm{d}r = \frac{4}{3}\pi.$$

Vypočtěme objem kulové výseče dané podmínkami $x^2 + y^2 + z^2 \leq 1$ a $3x^2 + 3y^2 \geq z^2$. Opět vyjádřeme podmínky ve sférických souřadnicích: $r^2 \leq 1, 3\sin^2(\psi) \geq \cos^2(\psi)$, neboli $\tan(\psi) \geq \frac{1}{\sqrt{3}}$. Opět jako v případě koule vidíme, že v podmínkách se vyskytují proměnné nezávisle, integrační meze jednotlivých proměnných tedy budou na sobě nezávislé. Z podmínky $r^2 \leq 1$ máme $r \in (0, 1]$, z podmínky $\tan(\psi) \geq \frac{1}{\sqrt{3}}$ vyplývá $\psi \in [0, \frac{\pi}{6}]$. Na proměnnou $\varphi$ žádné podmínky neklademe, je tedy $\varphi \in [0, 2\pi]$.

$$V_{\text{výseč}} = \int_0^{2\pi} \int_0^1 \int_0^{\frac{\pi}{6}} r^2 \sin\psi\, \mathrm{d}\psi\, \mathrm{d}r\, \mathrm{d}\varphi = \frac{2-\sqrt{3}}{3}\pi,$$

celkem

$$V = V_{\text{koule}} - V_{\text{výseč}} = \frac{2}{3}\pi - \frac{2-\sqrt{3}}{3}\pi = \frac{\pi}{\sqrt{3}}.$$

Mohli bychom též počítat objem přímo:

$$V = \int_0^{\pi} \int_0^1 \int_{\frac{\pi}{6}}^{\frac{5\pi}{6}} r^2 \sin\psi\, \mathrm{d}\psi\, \mathrm{d}r\, \mathrm{d}\varphi = \frac{\pi}{\sqrt{3}}.$$

Ve válcových souřadnicích

$$\begin{aligned} x &= r\cos(\varphi), \\ y &= r\sin(\varphi), \\ z &= z \end{aligned}$$

s jakobiánem této transformace $r$, vypadá výpočet objemu jako rozdílu objemu koule a kulové výseče následovně:

$$V = \frac{2}{3}\pi - \int_0^{2\pi} \int_0^{\frac{1}{2}} \int_0^1 r\, \mathrm{d}z\, \mathrm{d}r\, \mathrm{d}\varphi = \frac{\pi}{\sqrt{3}}.$$

Všimněme si, že ve válcových souřadnicích nemůžeme spočítat objem tělesa přímo, musíme ho rozdělit na dvě tělesa daná navíc omezením

**8.25. Integrace funkcí více proměnných.** U funkcí jedné proměnné jsme motivovali integrování představou o výpočtu plochy pod grafem funkce jedné proměnné. Teď budeme místo toho uvažovat objem části trojrozměrného prostoru pod grafem funkce $z = f(x, y)$ dvou proměnných, resp. vícerozměrné obdoby. Tehdy jsme vybírali malé intervaly $[x_i, x_{i+1}]$ o délce $\Delta x_i$ dělících celý interval, přes který integrujeme, vybrali jsme jejich reprezentanty $\xi_i$ a přiblížili příslušnou část plochy ploškou obdélníku s výškou danou hodnotou funkce $f(\xi_i)$ v tomto reprezentantu. tj. výrazem $f(\xi)\Delta x_i$.

V případě dvou proměnných nyní budeme pracovat s děleními v obou a hodnotami reprezentujícími výšku grafu nad jednotlivými obdélníčky v rovině.

Prvně se ale musíme vypořádat s oborem integrace, tj. oblastí v rovině proměnných, nad kterou chceme naši funkci $f$ integrovat. Příkladem může sloužit funkce $z = f(x, y) = \sqrt{1 - x^2 - y^2}$, která pro $(x, y)$ uvnitř jednotkového kruhu má za svůj graf povrch jednotkové sféry. Integrováním této funkce na jednotkovém kruhu tedy dostaneme objem poloviny jednotkové koule.

Nejjednodušším přístupem je uvažovat pouze obory integrace $M$, které jsou dány jako součiny intervalů, tj. jsou zadány rozsahem $x \in [a, b]$ a $y \in [c, d]$. Hovoříme v této souvislosti o *vícerozměrném intervalu*. Pokud je $M$ jiná ohraničená množina v $\mathbb{R}^2$, pracujeme místo ní s dostatečně velikou oblastí $[a, b] \times [c, d]$, ale upravíme naši funkci tak, že $f(x, y) = 0$ pro všechny body mimo $M$. Pro naši kouli bychom tedy integrovali na množině $M = [-1, 1] \times [-1, 1]$ funkci

$$f(x, y) = \begin{cases} \sqrt{1 - x^2 - y^2} & \text{pro } x^2 + y^2 \leq 1 \\ 0 & \text{jinak.} \end{cases}$$

Definice Riemannova integrálu pak zcela věrně sleduje náš postup z odstavce 6.24. Můžeme tak přitom činit pro libovolný konečný počet proměnných.

RIEMANNŮV INTEGRÁL

Riemannův integrál reálné funkce $f$ definované na vícerozměrném intervalu $I = [a_1, b_1] \times [a_2, b_2] \times \ldots \times [a_n, b_n]$ existuje, jestliže pro každou volbu posloupnosti dělení $\Xi$ (dělíme vícerozměrný interval ve všech proměnných zároveň) a reprezentantů jednotlivých krychliček $\xi_{i_1 \ldots i_n}$, s maximální velikostí mezi všemi použitými intervaly jdoucí k nule, budou integrální součty

$$S_{\Xi,\xi} = \sum_{i_1 \ldots i_n} f(\xi_{i_1 \ldots i_n}) \Delta x_{i_1 \ldots i_n}$$

(píšeme zde $\Delta x_{i_1 \ldots i_n}$ pro součin všech velikostí jednotlivých intervalů z dělení definujících kostičku s příslušnými indexy) vždy konvergovat k hodnotě

$$S = \int_I f(x_1, \ldots, x_n)\, dx_1 \ldots dx_n$$

nezávislé na zvolené posloupnosti dělení a reprezentantů. O funkci $f$ pak říkáme, že je riemannovsky integrovatelná na intervalu $I$.

$r \le \frac{1}{2}$, resp. $r \ge \frac{1}{2}$.

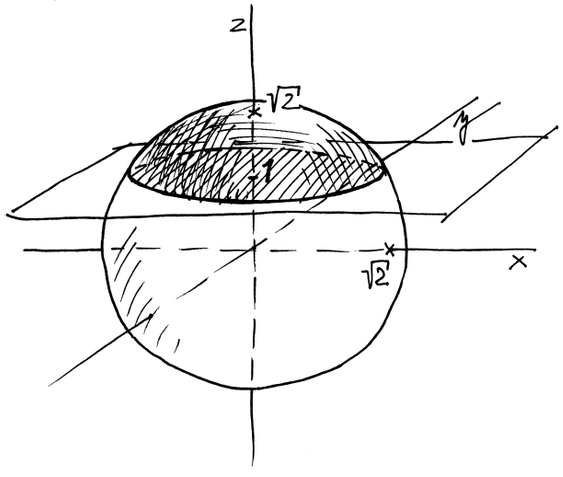
$$\begin{aligned} V &= V_1 + V_2 \\ &= \int_0^{2\pi}\int_0^{\frac{1}{2}}\int_0^{\sqrt{3}r} r\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi + \int_0^{2\pi}\int_{\frac{1}{2}}^{1}\int_0^{\sqrt{1-r^2}} r\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi \\ &= \frac{\pi}{\sqrt{3}}. \end{aligned}$$

□

Další alternativou by byl výpočet objemu jako objemu rotačního tělesa, opět bychom těleso rozdělili na stejné dvě části jako v předchozím případě a to na část „pod kuželem“ a část „pod sférou“. Tyto části však nejsou přímo rotačními tělesy, které dostaneme rotací podle některé z os. Objem první z nich spočítáme jako rozdíl objemu válce $x^2 + y^2 \le \frac{1}{4}, 0 \le z \le \frac{\sqrt{3}}{2}$ a části kužele $3x^2 + 3y^2 \le z^2, 0 \le z \le \frac{\sqrt{3}}{2}$, objem druhé pak jako rozdíl objemu rotačního tělesa vzniklého rotací části oblouku $y = \sqrt{(1-x^2)}$, $\frac{1}{2} \le x \le 1$ kolem osy $z$ a válce $x^2 + y^2 \le \frac{1}{4}, 0 \le z \le \frac{\sqrt{3}}{2}$.

$$\begin{aligned} V &= V_1 + V_2 \\ &= \left(\frac{\pi\sqrt{3}}{8} - \frac{\pi\sqrt{3}}{24}\right) + \left(\pi\int_0^{\frac{\sqrt{3}}{2}}(1-r^2)\,\mathrm{d}r - \frac{\pi\sqrt{3}}{8}\right) \\ &= \frac{\pi\sqrt{3}}{4} + \frac{\pi}{4\sqrt{3}} = \frac{\pi}{\sqrt{3}}. \end{aligned}$$

**8.71.** Vypočtěte objem kulové úseče, kterou odřezává rovina $z = 1$ z koule $x^2 + y^2 + z^2 = 2$.




**Řešení.** Spočítáme integrál v kulových souřadnicích. Vrchlík si můžeme představit jako kulovou výseč bez kužele (s vrcholem v bodě $[0,0,0]$ a kruhovou podstavou $z = 1, x^2 + y^2 = 1$). Výseč je v těchto souřadnicích součinem intervalů $[0,\sqrt{2}] \times [0, 2\pi) \times [0, \pi/4]$. Integrujeme tedy v daných mezích a to v libovolném pořadí.

$$\int_0^{2\pi}\int_0^{\sqrt{2}}\int_0^{\frac{\pi}{4}} r^2 \sin(\theta)\,\mathrm{d}\theta\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{4}{3}(\sqrt{2}-1)\pi.$$



Jako docela jednoduché cvičení si podrobně dokažte, že každá funkce riemannovsky integrovatelná na intervalu $I$ musí být na tomto intervalu omezená. Je tomu tak podobně jako v případě jedné proměnné proto, že kontrolujeme normy v definici použitých dělení jen velmi hrubě.

Ještě hůře dopadneme, když se pokusíme integrovat tímto způsobem přes neomezené intervaly, protože na rozdíl od integrálů v jedné proměnné neumíme snadno nahradit hledaný výsledek jednoznačně limitou integrálů přes ohraničené oblasti, viz poznámky v odstavci 8.28 níže. Budeme proto nyní pro jednoduchost hovořit o integraci funkcí přes $\mathbb{R}^n$ pouze pro funkce s kompaktním nosičem, tj. takové, které jsou identicky nulové vně nějakého uzavřeného a ohraničeného intervalu $I$.

Omezenou množinu $M \subset \mathbb{R}^n$ označujeme za *riemannovsky měřitelnou*, jestliže je její charakteristická funkce, definovaná

$$\chi_M(x_1,\ldots,x_n) = \begin{cases} 1 & \text{pro } (x_1,\ldots,x_n) \in S \\ 0 & \text{pro všechny ostatní body v } \mathbb{R}^n, \end{cases}$$

riemannovsky integrovatelná na $\mathbb{R}^n$.

Pro jakoukoliv riemannovsky měřitelnou množinu $M$ a funkci $f$ definovanou ve všech bodech $M$ můžeme uvažovat funkci $\tilde{f} = \chi_M \cdot f$ jako funkci definovanou na celém $\mathbb{R}^n$ a tato funkce $\tilde{f}$ zjevně má kompaktní nosič. Riemannův integrál funkce $f$ na množině $M$ definujeme jako

$$\int_M f\,dx_1\ldots dx_n = \int_{\mathbb{R}^n} \tilde{f}\,dx_1\ldots dx_n,$$

pokud integrál napravo (ve výše uvedeném smyslu) existuje.

Tato definice Riemannova integrálu nedává přímo rozumný návod, jak hodnoty integrálů skutečně vypočíst. Sama ale okamžitě vede k základním vlastnostem Riemannova integrálu (srovnejte s Větou 6.24):

**8.26. Věta.** *Množina riemannovsky integrovatelných reálných funkcí na intervalu $I \subset \mathbb{R}^n$ je vektorovým prostorem nad reálnými skaláry a Riemannův integrál je na něm lineární formou.*

*Pokud je obor integrace $S$ zadán jako disjunktní sjednocení konečně mnoha Riemannovsky měřitelných oborů $S_i$, je integrál funkce $f$ přes $S$ dán součtem integrálů přes obory $S_i$.*

Důkaz. Všechny vlastnosti plynou přímo z definice Riemannova integrálu a vlastností konvergentních posloupností reálných čísel, zcela stejně jako v případě jedné proměnné. Doporučujeme promyslet samostatně podrobnosti. □

Přepišme si větu do obvyklých rovností:

Konečná aditivita a linearita

První část říká, že lineární kombinace (nad skaláry v $\mathbb{R}$) riemannovsky integrovatelných funkcí $f_i : I \to \mathbb{R}, i = 1,\ldots,k$, na intervalu $I$ je vždy opět riemannovsky integrovatelná a spočte se takto:

$$\begin{aligned} &\int_I \Big(a_1 f_1(x_1,\ldots,x_n) + \cdots + a_k f_k(x_1,\ldots,x_n)\Big)\,dx_1\ldots dx_n = \\ &= a_1\int_I f_1(x_1,\ldots,x_n)\,dx_1\ldots dx_n + \ldots \\ &\quad \cdots + a_k\int_I f_k(x_1,\ldots,x_n)\,dx_1\ldots dx_n. \end{aligned}$$

Musíme ještě odečíst objem kužele. Ten je roven $\frac{1}{3}\pi R^2 V$ (kde $R$ je poloměr podstavy kužele a $V$ jeho výška, v našem případě jsou obě hodnoty rovny jedné) tedy celkový objem je

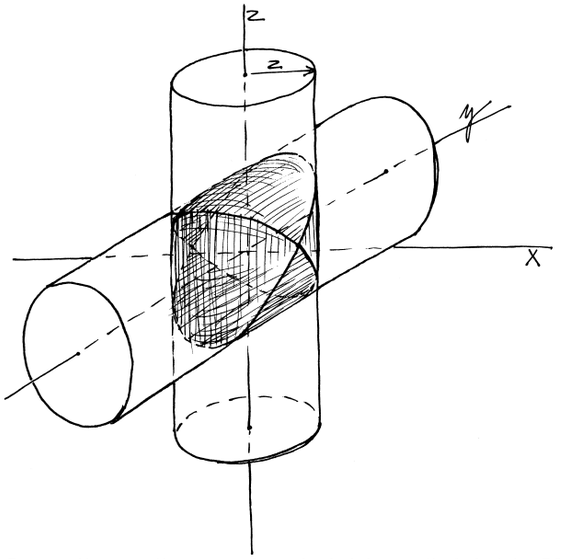
$$V_{\text{výseč}} - V_{\text{kužel}} = \frac{4}{3}(\sqrt{2}-1) - \frac{1}{3}\pi = \frac{1}{3}\pi(4\sqrt{2}-5).$$

Stejným způsobem bychom mohli obecně spočítat objem kulové úseče o výšce $v$ v kouli o poloměru $R$:

$$\begin{aligned} V &= V_{\text{výseč}} - V_{\text{kužel}} \\ &= \int_0^{2\pi} \int_0^{\arccos\left(\frac{R-v}{R}\right)} \int_0^R r^2 \sin(\theta)\,\mathrm{d}r\,\mathrm{d}\theta\,\mathrm{d}\varphi \\ &\quad -\frac{1}{3}\pi(2Rv - v^2)(R-v) \\ &= \frac{1}{3}\pi v^2(3R - v). \end{aligned}$$

□

**8.72.** Určete objem části válce $x^2 + z^2 = 16$, který leží uvnitř válce $x^2 + y^2 = 16$.




**Řešení.** Integrál vypočteme v kartézských souřadnicích. Vzhledem k symetrii tělesa stačí integrovat přes první oktant (zaměníme-li $x$ za $-x$, či $y$ za $-y$, či $z$ za $-z$ tak se rovnice tělesa nezmění). Část tělesa ležící v prvním oktantu je dána částí prostoru ležícího pod grafem funkce $z(x,y) = \sqrt{16-x^2}$ a nad čtvrtkruhem $x^2 + y^2 \le 16$, $x \ge 0$, $y \ge 0$. Objem celého tělesa je tak roven

$$V = 8\int_0^4 \int_0^{\sqrt{16-x^2}} \frac{4}{\sqrt{16-x^2}}\,\mathrm{d}y\,\mathrm{d}x = 128.$$ □

**Poznámka.** Všimněme si, že průmět daného tělesa je jak do roviny $y = 0$, tak do roviny $z = 0$ kružnice o poloměru 4, a přesto se nejedná o kouli.

Druhá část pak říká že pro disjunktní riemannovsky měřitelné množiny $M_1$ a $M_2$ a pro funkci $f : \mathbb{R}^n \to \mathbb{R}$ riemannovsky integrovatelnou na obou těchto množinách platí

$$\begin{aligned} &\int_{M_1 \cup M_2} f(x_1,\dots,x_n)\,dx_1\dots dx_n \\ &\qquad = \int_{M_1} f(x_1,\dots,x_n)\,dx_1\dots dx_n + \\ &\qquad\quad + \int_{M_2} f(x_1,\dots,x_n)\,dx_1\dots dx_n. \end{aligned}$$

**8.27. Násobné integrály.** Vzápětí uvidíme, že riemannovsky měřitelné množiny zejména zahrnují případy, kdy lze obor integrace $M$ definovat pomocí spojité funkční závislosti souřadnic hraničních bodů tak, že pro danou první souřadnici $x$ umíme zadat dvěma funkcemi rozsah další souřadnice $y \in [\varphi(x), \psi(x)]$, poté rozsah další souřadnice $z \in [\eta(x,y), \zeta(x,y)]$ apod. pro všechny další souřadnice.

V případě naší koule z úvodního příkladu to skutečně umíme: pro $x \in [-1,1]$ definujeme pro $y$ rozsah $y \in [-\sqrt{1-x^2}, \sqrt{1-x^2}]$. Objem koule pak můžeme buď spočítat integrováním výše uvedené funkce $f$ nebo můžeme integrovat charakteristickou funkci koule, tj. funkci identicky rovnou jedné na oblasti $S \subset \mathbb{R}^3$, která je definována ještě dalším určením $z \in [-\sqrt{1-x^2-y^2}, \sqrt{1-x^2-y^2}]$.

Podstatná je přitom následující věta, která převádí výpočet Riemannova integrálu na postupný výpočet několika integrálů v jedné proměnné (a ostatní proměnné jsou přitom považovány za parametry, které se mohou proto objevovat i v mezích pro integraci)

### Násobné integrály

**Věta.** *Nechť $M \subset \mathbb{R}^n$ je ohraničená množina zadaná jako výše pomocí spojitých funkcí $\psi_i$, $\eta_i$ (kde vždy $\psi_i \le \eta_i$)*

$$\begin{aligned} M = \{(x_1,\dots,x_n);\ x_1 \in [a,b],\, x_2 \in [\psi_2(x_1), \eta_2(x_1)],\dots, \\ x_n \in [\psi_n(x_1,\dots,x_{n-1}), \eta_n(x_1,\dots,x_{n-1})]\}, \end{aligned}$$

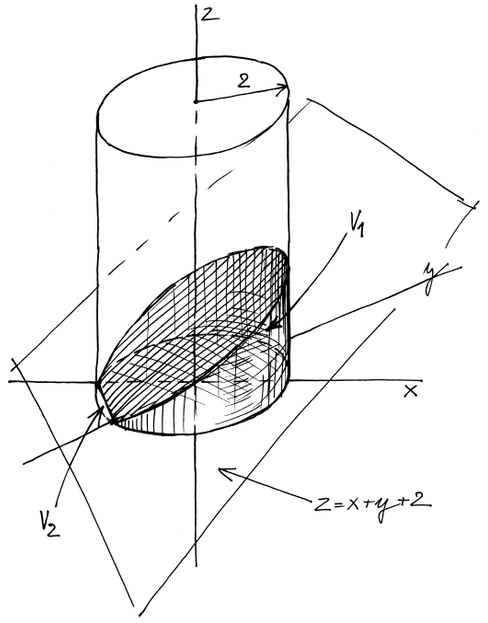
*a $f$ je funkce spojitá na $M$. Pak Riemannův integrál funkce $f$ přes množinu $M$ existuje a je vyčíslen vztahem*

$$\begin{aligned} \int_M f(x_1,x_2,\dots,x_n)\,dx_1\dots dx_n = \int_a^b \Bigg( \int_{\psi_2(x_1)}^{\eta_2(x_1)} \dots \\ \dots \Bigg( \int_{\psi_n(x_1,\dots,x_{n-1})}^{\eta_n(x_1,\dots,x_{n-1})} f(x_1,x_2,\dots,x_n)\,dx_n \Bigg) \dots dx_2 \Bigg) dx_1 \end{aligned}$$

Důkaz. Důkaz si nejprve provedeme pro dvě proměnné a pak uvidíme, že pro obecný případ vlastně už nic nového vymýšlet nebudeme.

Uvažme interval $I = [a,b] \times [c,d]$ obsahující naši množinu $M = \{(x,y); x \in [a,b], y \in [\psi(x), \eta(y)]\}$ a dělení $\Xi$ intervalu $I$ s reprezentanty $\xi_{ij}$.

**8.73.** Určete objem části prostoru ležící uvnitř válce $x^2 + y^2 = 4$ a ohraničené rovinami $z = 0$ a $z = x + y + 2$.




**Řešení.** V příkladu budeme používat válcových souřadnic daných rovnicemi $x = r\cos(\varphi)$, $y = r\sin(\varphi)$, $z = z$ s jakobiánem této transformace $J = r$. Těleso rozdělíme na dvě části ležící nad, respektive pod rovinou $z = 0$, jejich objemy označíme $V_1$, resp. $V_2$. Dále si všimněme, že částí tělesa o objemu $V_1$ je i jehlan s vrcholy $[0, 0, 0]$, $[0, 0, 2]$, $[-2, 0, 0]$, $[0, -2, 0]$. Část tělesa ležící nad rovinou $z = 0$ tedy rozdělíme ještě na dvě části, jejichž objem spočítáme zvlášť.

$$\begin{aligned} V_1 - V_{\text{jehlan}} &= \int_{-\pi/2}^{\pi} \left( \int_0^2 [r\sin\varphi + r\cos\varphi + 2] r \,\mathrm{d}r \right) \mathrm{d}\varphi, \\ &= 6\pi + \frac{16}{3}, \\ V_{\text{jehlan}} &= \frac{4}{3} \end{aligned}$$

Dále

$$V_1 - V_2 = \int_{-\pi}^{\pi} \int_0^2 r^2 (\sin(\varphi) + \cos(\varphi)) + 2r \,\mathrm{d}r \,\mathrm{d}\varphi = 8\pi,$$

tedy $V_1 + V_2 = 4\pi + \frac{40}{3}$. □

**Poznámka.** Ve výpočtu jsme využili toho, že integrováním funkce dvou proměnných přes nějakou oblast v $\mathbb{R}^2$, získáme rozdíl objemů oblastí v $\mathbb{R}^3$ ohraničených grafem integrované funkce a ležících nad, resp. pod, danou oblastí v rovině $z = 0$.

**8.74.** Určete objem tělesa v $\mathbb{R}^3$, které je dáno průnikem koule $x^2 + y^2 + z^2 = 4$ s válcem $x^2 + y^2 = 1$.

Příslušná integrální suma je

$$\begin{aligned} S_{\Xi,\xi} &= \sum_{i,j} f(\xi_{ij}) \Delta x_{ij} \\ &= \sum_i \left( \sum_j f(\xi_{ij}) \Delta y_j \right) \Delta x_i, \end{aligned}$$

kde píšeme $\Delta x_{ij}$ pro součin velikostí $\Delta x_i$ a $\Delta x_j$ intervalů, které odpovídají výběru reprezentanta $\xi_{ij}$.

Předpokládejme nyní chvíli, že pracujeme pouze s výběry reprezentantů takovými, že všechny $\xi_{ij}$ mají stejnou první souřadnici $x_i$. Jestliže pak ponecháme dělení intervalu $[a, b]$ a budeme zjemňovat dále pouze dělení $[c, d]$, budou se hodnoty vnitřní sumy v našem výrazu blížit k hodnotě integrálu

$$S_i = \int_{\varphi(x_i)}^{\eta(x_i)} f(x_i, y)\, dy,$$

který jistě existuje, protože je funkce $f(x_i, y)$ po částech spojitá. Navíc ale tímto způsobem získáme spojitou funkci ve volném parametru $x_i$, viz 8.24. Proto další zjemňování dělení intervalu $[a, b]$ povede limitně právě na požadovaný vztah

$$\left( \sum_i S_i \Delta x_i \right) \to S = \int_a^b \left( \int_{\psi(x)}^{\eta(y)} f(x, y)\, dy \right) dx.$$

Zbývá nám ještě se vypořádat s obecnými výběry reprezentantů obecných dělení $\Xi$.

Protože ale pracujeme s (po částech) spojitou funkcí $f$ na kompaktní množině, je tam ve skutečnosti stejnoměrně souvislá. Jestliže tedy vybereme předem malé $\varepsilon > 0$, můžeme vždy najít pro normu dělení ohraničení $\delta > 0$ tak, že odchylka hodnot funkce $f$ pro obecné volby $x_{ij}$ od výše použitých voleb nebude převyšovat $\varepsilon$. Proto dopadnou limitní procesy i pro obecné Riemannovy sumy $S_{\Xi,\xi}$ stejně jako jsme viděli výše.

Obecný případ nyní můžeme dokázat snadno indukcí.



V případě $n = 1$ je výsledek triviální a výše uvedená argumentace může být snadno převedena v obecný indukční krok, jestliže místo $y$ píšeme $(x_2, \ldots, x_n)$, místo $x$ máme $x_1$ a jednotlivé krychličky v dělení vnímáme jako $(n-1)$-rozměrné krychličky kartézsky vynásobené posledním intervalem.

V předposledním kroku argumentace pak místo prosté jednorozměrné integrace použijeme indukční předpoklad. Závěrečný argument o stejnoměrné spojitosti zůstává stejný.

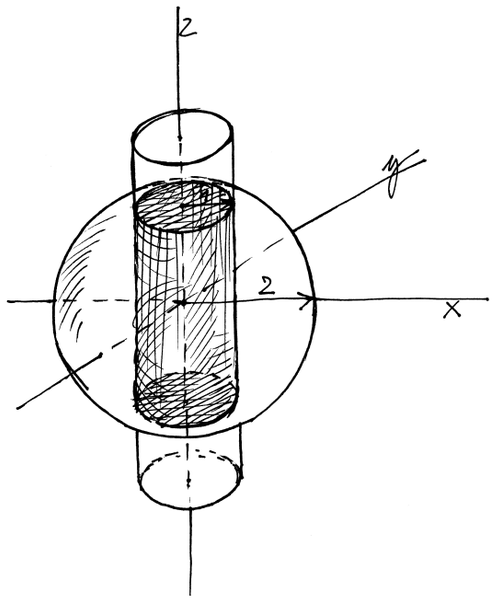
Doporučujeme projít podrobně jako cvičení. □



V právě dokázané větě je v případě vícerozměrného intervalu $I$ kterékoliv pořadí integrace vyjádřením oblasti $I$ v požadovaném tvaru. Na výsledku integrálu tak pořadí integrace nemůže mít vliv. Platí proto následující slavná věta:

FUBINIHO VĚTA

**8.28. Důsledek.** *Pro vícerozměrný interval* $M = [a_1, b_1] \times [a_2, b_2] \times \ldots \times [a_n, b_n]$ *a spojitou funkci* $f(x_1, \ldots, x_n)$ *na* $M$ *je násobný Riemannův integrál*

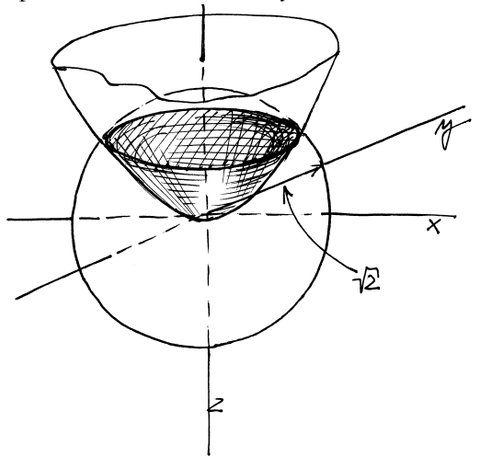



**Řešení.** Vzhledem k symetrii tělesa spočítáme pouze objem části tělesa ležící v prvním oktantu. Integrujeme ve válcových souřadnicích daných rovnicemi $x = r\cos(\varphi)$, $y = r\sin(\varphi)$, $z = z$, s jakobiánem dané transformace $J = r$, a to část prostoru mezi rovinou $z = 0$ a grafem funkce $z = \sqrt{4 - x^2 - y^2} = \sqrt{4 - r^2}$. Můžeme tedy rovnou psát dvojný integrál

$$V = 8\int_0^{\pi/2}\int_0^1 r\sqrt{4 - r^2}\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{4}{3}(8 - 3\sqrt{3})\pi.$$

□

**8.75.** Určete objem tělesa v $\mathbb{R}^3$, které je dáno průnikem koule $x^2 + y^2 + z^2 = 2$ s paraboloidem $z = x^2 + y^2$.




**Řešení.** Použijeme opět válcových souřadnic.

$$V = \int_0^{2\pi}\int_0^1\int_{r^2}^{\sqrt{2-r^2}} r\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{4\sqrt{2}\pi}{3} - \frac{7\pi}{6}.$$

□

$$\int_M f(x_1,\ldots,x_n)\,dx_1\ldots dx_n = \int_{a_1}^{b_1}\int_{a_2}^{b_2}\ldots\int_{a_n}^{b_n} f(x_1,\ldots,x_n)\,dx_1\ldots dx_n$$

*nezávislý na pořadí, ve kterém postupně integraci provádíme.*

Možnost zaměňovat pořadí integrace v násobných integrálech je nesmírně užitečná. I my jsme tento výsledek už dříve využili při studiu vztahu Fourierových transformací a konvolucí, viz odstavec 7.9.

Naše odvození Fubiniho věty je opřené o jednoduché vlastnosti Riemannovy integrace a spojitost integrované funkce. Ve skutečnosti ale Fubini svůj výsledek odvodil v daleko obecnějším kontextu integrace, zatímco námi uvedenou větu běžně používali matematici jako Cauchy nejméně 100 let před Fubinim.

Všimněme si také, že u Riemannova integrálu pro funkce více proměnných jsme nezavedli žádný pojem nevlastního integrálu pro neomezené funkce. Ověřte si, že to ani nemůže moc rozumně jít na následujícím příkladu dvou násobných integrálů:

$$\int_0^1\left(\int_0^1 \frac{x-y}{(x+y)^3}\,dy\right)dx = \frac{1}{2},$$
$$\int_0^1\left(\int_0^1 \frac{x-y}{(x+y)^3}\,dx\right)dy = -\frac{1}{2}.$$

Zdůvodnění lze vytušit už z vlastností neabsolutně konvergentních řad, kdy přerovnáním pořadí sčítanců lze dosáhnout jakéhokoliv výsledku.

O něco lepší je situace, když počítáme Riemannův integrál omezené riemannovsky integrovatelné funkce $f(x)$, která nemá kompaktní nosič, přes celé $\mathbb{R}^n$. Za předpokladu, že existuje univerzální odhad

$$\left|\int_I f(x)\,dx\right| \le C$$

s konstantou $C$ nezávislou na volbě $n$–rozměrného intervalu $I$, pak je možné definovat

$$\int_{\mathbb{R}^n} f(x)\,dx = \lim_{r\to\infty}\int_{I_r} f(x)\,dx,$$

kde $I_r = \{(x_1,\ldots,x_n);\ |x_j| < r,\ j = 1,\ldots,n\}$ a výsledek je samozřejmě ohraničený stejnou konstantou $C$. V tomto případě platí i Fubiniho věta ve tvaru

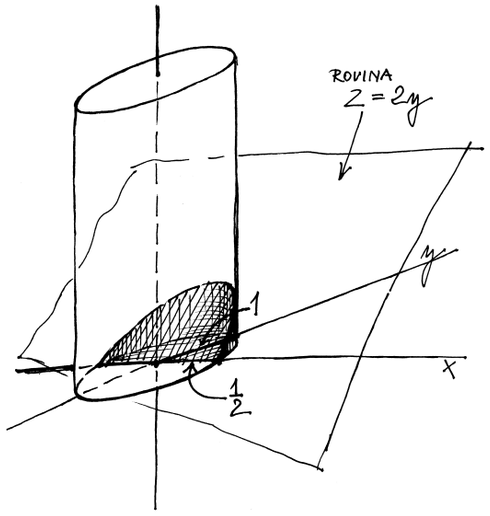
$$\int_{\mathbb{R}^n} f(x)\,dx = \int_{-\infty}^{\infty}\ldots\left(\int_{-\infty}^{\infty} f(x)\,dx_1\right)\ldots dx_n.$$

**8.29. Poznámky o integraci.** Riemannův integrál se u funkcí více proměnných chová ještě hůře, než jsme viděli u funkcí jedné proměnné v kapitole šesté. Proto byli vyvinuty sofistikovanější přístupy k integraci, které jsou odvozeny od zavedení míry množin. Podívejme se aspoň velice přibližně na tento problém.



Říkáme, že je omezená množina $M \subset \mathbb{R}^n$ *riemannovsky měřitelná*, jestliže je její charakteristická funkce $\chi_M$ riemannovsky integrovatelná na $\mathbb{R}^n$. Můžeme také uvažovat striktní analogii dolních a horních Riemannových integrálů z funkcí jedné proměnné. To znamená, že budeme v Riemannových součtech místo hodnot funkce v reprezentantech vždy brát infimum, resp. supremum,

**8.76.** Určete objem tělesa v $\mathbb{R}^3$, které je ohraničeno eliptickým válcem $4x^2 + y^2 = 1$, rovinami $z = 2y$ a $z = 0$, ležící nad rovinou $z = 0$.

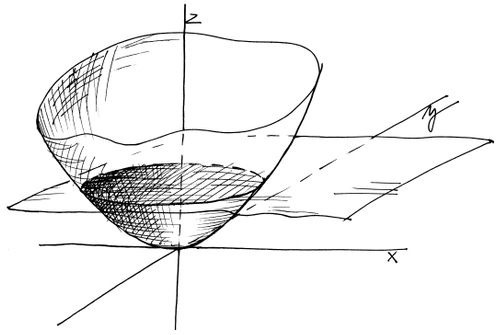



**Řešení.** Vzhledem k symetrii úlohy bude výhodné zavést souřadnice $x = \frac{1}{2}r\cos(\varphi)$, $y = r\sin(\varphi)$, $z = z$, s jakobiánem příslušné transformace $J = \frac{1}{2}r$. Eliptický válec má v těchto souřadnicích rovnici $r^2 = 1$. Hledaný objem je pak

$$\begin{aligned} V &= \int_0^{\pi}\int_0^1 2r\sin(\varphi)\frac{1}{2}r\,\mathrm{d}r\,\mathrm{d}\varphi \\ &= \int_0^{\pi}\int_0^1 r^2\sin(\varphi)\,\mathrm{d}r\,\mathrm{d}\varphi = \int_0^{\pi}\frac{1}{3}\sin(\varphi)\,\mathrm{d}\varphi = \frac{2}{3}. \end{aligned}$$

□

**8.77.** Určete objem tělesa v $\mathbb{R}^3$, které je ohraničeno paraboloidem $2x^2 + y^2 = z$ a rovinou $z = 2$.




**Řešení.** Obdobně jako v předchozí úloze volíme „speciální“ souřadnice respektující symetrii úlohy: $x = \frac{1}{\sqrt{2}}r\cos(\varphi)$, $y = r\sin(\varphi)$, $z = z$ s jakobiánem $J = \frac{1}{\sqrt{2}}r$. Rovnice paraboloidu je v těchto souřadnicích

hodnot přes dotčený mnohoměrný interval. Pro omezené funkce tak vždy dostaneme dobře definované hodnoty a jestliže takto budeme postupovat pro charakteristickou funkcí $\chi_M$ pevně zvolené množiny $M$, dostaneme tzv. vnitřní a vnější Riemannovu míru množiny $M$. Zjevně je vnitřní míra limitou ploch daných součtem objemů všech intervalů z našich dělení zcela uvnitř $M$. Naopak, vnější míra je dána limitou součtů objemů všech intervalů protínajících $M$. Z definice pak přímo vyplývá, že $M$ je riemannovsky měřitelná, právě když její horní a dolní míry splývají.[6]

Všechny množiny, které mají vnější míru nulovou jsou samozřejmě riemannovsky měřitelné. Říkáme jim množiny míry nula. Lze ukázat, že riemannovsky integrovatelné jsou právě ty omezené funkce s kompaktním nosičem, jejichž množina všech bodů nespojitosti má Riemannovu míru nula. Jistě bude takto definovaná míra konečně aditivní, tj. disjunktní sjednocení konečně mnoha měřitelných je měřitelná množina a její míra je dána příslušným konečným součtem. Tak jako u jedné proměnné ale neplatí, že by spočetné disjunktní sjednocení měřitelných bylo opět měřitelné, takže musíme opět očekávat problémy s limitními přechody, tak jak jsme je viděli v případě jedné proměnné.

Jestliže se omezíme na vektorový prostor $\mathcal{S}_c(\mathbb{R}^n)$ všech spojitých funkcí s kompaktním nosičem, můžeme postupovat zcela stejně jako v kapitole sedmé a definovat pro funkce $f \in \mathcal{S}_c(\mathbb{R}^n)$ jejich normy

$$\|f\|_p = \left(\int_{\mathbb{R}^n} |f(x_1,\ldots,x_n)|^p\,dx_1\ldots dx_n\right)^{1/p}$$

pro všechny hodnoty $1 \le p < \infty$. Ověření vlastností normy s využitím Hölderovy a Minkowského nerovnosti přitom bude díky definici Riemannova integrálu pomocí rozdělení opět zcela stejné jako u funkcí jedné proměnné.

Dostáváme tak metrické prostory $\mathcal{L}^p$. Jak víme z obecné teorie, jejich zúplnění existuje (a přitom jednoznačně, až na izometrie) a lze ukázat, že půjde opět o prostory funkcí. Navíc lze vybudovat obecnější teorii integrování tak, aby byly normy na těchto zúplněných prostorech dány stejnými vztahy jako výše. Do těchto oblastí matematické analýzy se již zde nebudeme pouštět.

**8.30. Derivace podle parametrů.** Konečně se teď můžeme snadno vypořádat se slíbenou závislostí integrálů na parametrech. Následující výsledek má četná využití. Např. jej můžeme ocenit při zkoumání integrálních transformací, kterým jsme se věnovali v druhé části předchozí kapitoly sedmé.



Také naše předchozí výsledky o extrémech funkcí více proměnných nyní mají přímé použití např. pro minimalizaci ploch nebo objemů objektů zadanými funkcemi v závislosti na parametrech.

### Derivace podle parametru

**Věta.** *Pro spojitou funkci $f(x, y_1, \ldots, y_n)$ definovanou pro všechna $x$ z konečného intervalu $[a, b]$ a pro všechna $(y_1, \ldots, y_n)$ z nějakého okolí $U$ bodu $c = (c_1, \ldots, c_n) \in \mathbb{R}^n$ uvažujme integrál*

$$F(y_1,\ldots,y_n) = \int_a^b f(x, y_1, \ldots, y_n)\,dx.$$

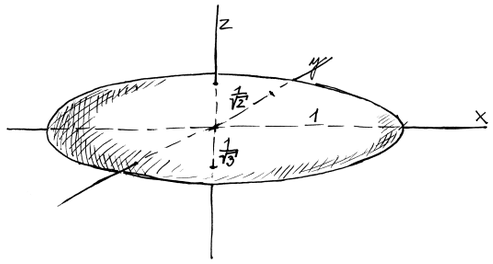
[6] Uveden0 konstrukci konečně aditivní míry na $\mathbb{R}^n$ se také říká *Jordanova míra*.

$z = r^2$ a pro objem tělesa můžeme psát

$$\begin{aligned} V &= 4\int_0^{\pi/2}\int_0^{\sqrt{2}}\int_{r^2}^{2}\frac{1}{\sqrt{2}}r\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi \\ &= 2\sqrt{2}\int_0^{\pi/2}\int_0^{\sqrt{2}}2r - r^3\,\mathrm{d}r\,\mathrm{d}\varphi = 2\sqrt{2}\int_0^{\pi/2}\mathrm{d}\varphi \\ &= \sqrt{2}2\pi. \end{aligned}$$

□

**8.78.** Vypočtěte objem elipsoidu $x^2 + 2y^2 + 3z^2 = 1$.




**Řešení.** Uvážíme souřadnice

$$\begin{aligned} x &= r\cos(\varphi)\sin(\theta), \\ y &= \tfrac{1}{\sqrt{2}}r\sin(\varphi)\sin(\theta), \\ z &= \tfrac{1}{\sqrt{3}}r\cos(\theta). \end{aligned}$$

Odpovídající jakobián je pak $\frac{1}{\sqrt{6}}r^2\sin(\theta)$, objem je tedy

$$V = \int_0^{2\pi}\int_0^{\pi}\int_0^{1}\frac{1}{\sqrt{6}}r^2\sin(\theta)\,\mathrm{d}r\,\mathrm{d}\theta\,\mathrm{d}\varphi = \frac{4}{3\sqrt{6}}\pi.$$

□

**8.79. Poznámka.** Poznamenejme, že při lineárních (a afinních) změnách souřadnic „deformujeme“ prostor „rovnoměrně“, tj. stejně ve všech jeho částech. Objem libovolného tělesa se tedy mění o konstantní násobek odpovídající změně objemu infinitesimálního objemového elementu, což je jakobián. Jestliže tedy už považujeme za známý objem koule daného poloměru $r$, v tomto případě $r = 1$, můžeme rovnou psát pro objem elipsoidu $V = \frac{1}{\sqrt{6}}\cdot\frac{4}{3}\pi = \frac{4}{3\sqrt{6}}\pi$.

**8.80.** Vypočtěte objem tělesa omezeného paraboloidem $2x^2 + 5y^2 = z$ a rovinou $z = 1$.

**Řešení.** Volíme souřadnice

$$\begin{aligned} x &= \tfrac{1}{\sqrt{2}}r\cos(\varphi), \\ y &= \tfrac{1}{\sqrt{5}}r\sin(\varphi), \\ z &= z. \end{aligned}$$

Determinant jakobiánu je $\frac{r}{\sqrt{10}}$, objem je tedy

$$V = \int_0^{2\pi}\int_0^{1}\int_{r^2}^{1}\frac{r}{\sqrt{10}}\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{\pi}{2\sqrt{10}}.$$

□

*Jestliže existuje spojitá parciální derivace $\frac{\partial f}{\partial y_j}$ na okolí bodu $c$, potom existuje i $\frac{\partial F}{\partial y_j}(c)$ a platí*

$$\frac{\partial F}{\partial y_j}(c) = \int_a^b \frac{\partial f}{\partial y_j}(x, c_1, \ldots, c_n)\,dx.$$

Důkaz. Díky uvažované spojitosti všech funkcí můžeme



snadno využít naše znalosti o primitivních funkcích z integrace v jedné proměnné a výsledek bude jednoduchým důsledkem Fubiniho věty. Protože všechny ostatní parametry $y_j$ hrají v našich úvahách jen pasivní roli konstantního parametru, můžeme rovnou bez újmy na obecnosti předpokládat, že v našem tvrzení vystupuje jediný parametr $y$.

Označme si

$$G(y) = \int_a^b \frac{\partial f}{\partial y}(x, y)\,dx, \qquad F(y) = \int_a^b f(x, y)\,dx$$

a spočtěme s pomocí Fubiniho věty primitivní funkci

$$\begin{aligned} H(y) &= \int_{y_0}^{y} G(s)\,ds = \int_{y_0}^{y}\left(\int_a^b \frac{\partial f}{\partial s}(x, s)\,dx\right)ds = \\ &= \int_a^b\left(\int_{y_0}^{y}\frac{\partial f}{\partial s}(x, s)\,ds\right)dx = F(y) - F(y_0). \end{aligned}$$

Konečně, derivací podle $y$ dostáváme

$$G(y) = \frac{\partial H}{\partial y}(y) = \frac{\partial F}{\partial y}(y),$$

což jsme chtěli dokázat. □

**8.31. Změna souřadnic při integraci.** Při výpočtu integrálů



funkcí jedné proměnné jsme používali transformace souřadnic jako mimořádně silný nástroj. V případě integrálů funkcí více proměnných je to velice podobné.

Připomeňme nejdříve (s vhodnou interpretací pro následné zobecnění), jak je to s transformacemi pro jednu proměnnou. Integrovaný výraz $f(x)\,dx$ vyjadřuje plochu obdélníčku určeného (linearizovaným) přírůstkem proměnné $x$ a hodnotou $f(x)$. Pokud proměnnou transformujeme vztahem $x = u(t)$, vyjadřuje se i linearizovaný přírůstek jako

$$dx = \frac{du}{dt}\,dt,$$

a proto i příslušný příspěvek pro integrál je vyjádřen jako

$$f(u(t))\frac{du}{dt}\,dt,$$

přičemž buď předpokládáme, že znaménko derivace $u'(t)$ je kladné, nebo dojde k obrácení mezí integrálu, takže ve výsledku se znaménko neprojeví.

Intuitivně je postup v $n$ proměnných docela podobný, pouze musíme použít znalostí z lineární algebry o objemu rovnoběžnostěnů.

V Riemannových součtech používáme pro Riemannovy integrály přiblížení, které vezme objem (plochu) malého vícerozměrného intervalu a vynásobí ji hodnotou funkce v reprezentujícím bodě. Pokud použijeme transformaci souřadnic, dostaneme nejen hodnotu funkce v reprezentujícím bodě v novém souřadném

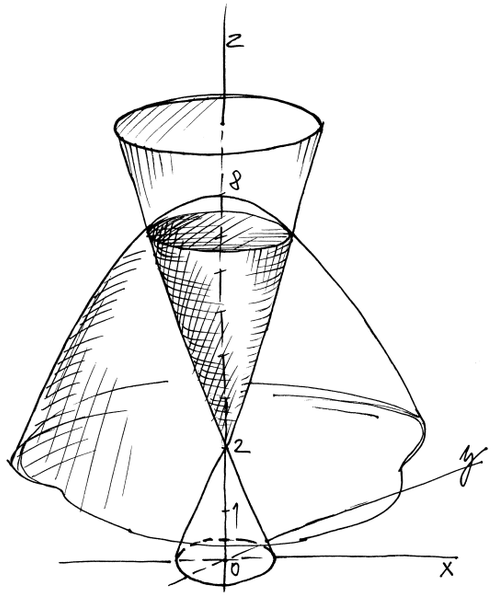
**8.81.** Určete objem tělesa ležícího v prvním oktantu a ohraničeném plochami $y^2 + z^2 = 9$ a $y^2 = 3x$.

**Řešení.** Ve válcových souřadnicích

$$V = \int_0^{\pi/2} \int_0^3 \int_0^{\frac{r^2}{3}\cos^2(\varphi)} r \,\mathrm{d}x\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{27}{16}\pi.$$

□

**8.82.** Určete objem tělesa v $\mathbb{R}^3$, které je ohraničeno částí kužele $2x^2 + y^2 = (z-2)^2$, $z \geq 2$ a paraboloidem $2x^2 + y^2 = 8 - z$.




**Řešení.** Zjistíme nejprve průnik zadaných ploch:

$$(z-2)^2 = -z + 8,\ z \geq 2,$$

tedy $z = 4$ a dostáváme rovnici průniku daných ploch $2x^2 + y = 4$. Substitucí $x = \frac{1}{\sqrt{2}} r\cos(\varphi)$, $y = r\sin(\varphi)$, $z = z$ převedeme dané plochy na tvar $r^2 = (z-2)^2$, $z \geq 2$ a $r^2 = 8 - z$, tedy $z = r + 2$ pro první plochu a $z = 8 - r^2$ pro druhou plochu. Celkem je průmět daného tělesa do souřadnice $\varphi$ roven intervalu $[0, 2\pi]$, pro dané $\varphi_0 \in [0, 2\pi]$ je potom průmět průniku tělesa s rovinou $\varphi = \varphi_0$ do souřadnice $r$ roven (pro libovolné $\varphi_0$) intervalu $[0, 2]$. Pro dané $r_0$ a $\varphi_0$ je pak průmět průniku tělesa s přímkou $r = r_0$, $\varphi = \varphi_0$ na souřadnici $z$ roven intervalu $[r_0 + 2, 8 - r_0^2]$. jakobián uvažované transformace je $J = \frac{1}{\sqrt{2}} r$, celkem tedy můžeme psát

$$V = \int_0^{2\pi} \int_0^2 \int_{r+2}^{8-r^2} \frac{r}{\sqrt{2}} \,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{16\sqrt{2}}{3}\pi.$$

□

**8.83.** Určete objem tělesa ležícího uvnitř válce $y^2 + z^2 = 4$, dále v polorovině $x \geq 0$ a konečně ohraničeného plochou $y^2 + z^2 + 2x = 16$.

vyjádření, ale musíme také vést v patrnosti změnu plochy nebo objemu příslušného malého vícerozměrného intervalu. Opět tu půjde o lineární přiblížení změny a tu máme dobře zvládnutou — jde přeci o působení lineárního přiblížení použité transformace, tj. akci Jacobiho matice, viz 8.14. Změna objemu je přitom dána (v absolutní hodnotě) pomocí determinantu z této matice (viz naše úvahy na toto téma v lineární algebře, zejména 4.22).

### Transformace souřadnic

**Věta.** *Nechť* $G(t_1, \ldots, t_n) : \mathbb{R}^n \to \mathbb{R}^n$, $(x_1, \ldots, x_n) = G(t_1, \ldots, t_n)$, *je spojitě diferencovatelné invertibilní zobrazení,* $N = G(M)$ *a* $M$ *jsou riemannovsky měřitelné množiny a* $f : M \to \mathbb{R}$ *je spojitá funkce. Potom platí*

$$\int_M f(x_1, \ldots, x_n)\,dx_1 \ldots dx_n = \int_N f(G(t_1, \ldots, t_n))\left|\det(D^1 G(t_1, \ldots, t_n))\right| dt_1 \ldots dt_n.$$

Důkaz. Protože pracujeme se spojitou funkcí $f$ a diferencovatelnou změnou souřadnic, zjevně existují integrály na obou stranách dokazované rovnosti. Potřebujeme tedy pouze dokázat, že se jejich hodnoty budou skutečně rovnat.



Označme si naši složenou funkci

$$g(t_1, \ldots, t_n) = f(G(t_1, \ldots, t_n)),$$

zvolme si dostatečně velký $n$–rozměrný interval $I$ obsahující $N$ a jeho dělení $\Xi$. Celý důkaz je jen přesnějším zápisem výše uvedené úvahy.

Nejprve si všimněme dvou věcí: jednak jsou obrazem hranic našich intervalů $I_{i_1 \ldots i_n}$ diferencovatelné objekty (stěny, hrany apod.), proto budou obrazy $J_{i_1 \ldots i_n} = G(I_{i_1 \ldots i_n})$ těchto intervalů opět riemannovsky měřitelné množiny. Pro každý jednotlivý dílek $I_{i_1 \ldots i_n}$ našeho dělení $\Xi$ proto existuje integrál jakékoliv spojité funkce přes množiny $J_{i_1 \ldots i_n}$.

Dále nás bude zajímat „linearizovaný“ obraz intervalu $I_{i_1 \ldots i_n}$ v zobrazení $G$. Ten dostaneme tak, že si zvolíme pevně střed $t_{i_1 \ldots i_n}$ intervalu $I_{i_1 \ldots i_n}$, tento střed zobrazíme na střed $G(t_{i_1 \ldots i_n})$ uvažovaného obrazu a k samotnému zobrazení použijeme linearizaci $D^1 G$ (tj. Jacobiho matici) zobrazení $G$ ve středu $t_{i_1 \ldots i_n}$. Jde tedy o obraz $R_{i_1 \ldots i_n}$ intervalu $I_{i_1 \ldots i_n}$ zadaný afinním zobrazením takto:

$$R_{i_1 \ldots i_n} = G(t_{i_1 \ldots i_n}) + D^1 G(t_{i_1 \ldots i_n})(I_{i_1 \ldots i_n} - t_{i_1 \ldots i_n}).$$

Všimněme si, že odečtením středu $t_{i_1 \ldots i_n}$ od intervalu $I_{i_1 \ldots i_n}$ dostáváme interval se středem v počátku souřadnic, jeho obrazem v lineárním zobrazení bude $n$–rozměrný rovnoběžnostěn opět se středem v počátku a ten konečně posouváme do vybraného středu, viz obrázek.

Objem tohoto rovnoběžnostěnu nezávisí na volbě jeho středu a je roven

$$\operatorname{vol} R_{i_1 \ldots i_n} = |\det G(t_{i_1 \ldots i_n})| \operatorname{vol} I_{i_1 \ldots i_n},$$

viz odstavec 4.22 na straně 206

Jestliže bude naše dělení hodně jemné, bude se tento objem hodně málo lišit od objemu obrazu $J_{i_1, \ldots i_n}$. Přesněji řečeno, díky stejnoměrné spojitosti zobrazení $G$, můžeme pro každé malé $\varepsilon > 0$

**Řešení.** Ve válcových souřadnicích

$$V = \int_0^{2\pi} \int_0^2 \int_0^{8-\frac{r^2}{2}} r \,\mathrm{d}x \,\mathrm{d}r \,\mathrm{d}\varphi = 28\pi.$$

□

**8.84. Těžiště tělesa.** Souřadnice $(x_t, y_t, z_t)$ těžiště (homogenního) tělesa $T$ o objemu $V$ v $\mathbb{R}^3$ je dáno po souřadnicích následujícími integrály:

$$x_t = \iiint_T x \,\mathrm{d}x \,\mathrm{d}y \,\mathrm{d}z,$$
$$y_t = \iiint_T y \,\mathrm{d}x \,\mathrm{d}y \,\mathrm{d}z,$$
$$z_t = \iiint_T z \,\mathrm{d}x \,\mathrm{d}y \,\mathrm{d}z.$$

Analogicky spočteme těžiště tělesa v $\mathbb{R}^2$ či v jiných dimenzích.

**8.85.** Určete těžiště části elipsy $3x^2 + 2y^2 = 1$ ležící v prvním kvadrantu roviny $\mathbb{R}^2$.

**Řešení.** Spočítejme nejprve obsah dané elipsy. Transformací souřadnic $x = \frac{1}{\sqrt{3}}x'$, $y = \frac{1}{\sqrt{2}}y'$ s jakobiánem $\frac{1}{\sqrt{6}}$ dostaneme

$$S = \int_0^{\frac{1}{\sqrt{3}}} \int_0^{\sqrt{\frac{1-3x^2}{2}}} \mathrm{d}y \,\mathrm{d}x = \frac{1}{\sqrt{6}} \int_0^1 \int_0^{\sqrt{1-x^2}} \mathrm{d}y' \,\mathrm{d}x' = \frac{\pi}{4\sqrt{6}}.$$

Další potřebné integrály můžeme spočítat přímo v kartézských souřadnicích $x$ a $y$:

$$\begin{aligned} T_x &= \int_0^{\frac{1}{\sqrt{3}}} \int_0^{\sqrt{\frac{1-3x^2}{2}}} x \,\mathrm{d}y \,\mathrm{d}x = \int_0^{\frac{1}{\sqrt{3}}} x\sqrt{\frac{1-3x^2}{2}} \,\mathrm{d}x = \\ &= \frac{1}{2}\int_0^{\frac{1}{3}} \sqrt{\frac{1-3t}{2}} \,\mathrm{d}t = \frac{\sqrt{2}}{18}, \end{aligned}$$

$$\begin{aligned} T_y &= \int_0^{\frac{1}{\sqrt{3}}} \int_0^{\sqrt{\frac{1-3x^2}{2}}} y \,\mathrm{d}y \,\mathrm{d}x = \frac{1}{2}\int_0^{\frac{1}{\sqrt{3}}} \frac{1-3x^2}{2} \,\mathrm{d}x = \\ &= \frac{1}{4}\int_0^{\frac{1}{\sqrt{3}}} (1-3x^2) \,\mathrm{d}x = \frac{\sqrt{3}}{18}. \end{aligned}$$

Souřadnice těžiště jsou potom $[\frac{4\sqrt{3}}{9\pi}, \frac{2\sqrt{2}}{\pi}]$. □

**8.86.** Určete objem a souřadnice těžiště homogenního rotačního kužele o kruhové podstavě s poloměrem $r$ a výšce $h$.

**Řešení.** Otočíme-li kužel vrcholem dolů a ten umístíme do počátku souřadnic, pak ve válcových souřadnicích:

$$V = 4\int_0^{\pi/2} \int_0^r \int_{\frac{h}{r}\rho}^h \rho \,\mathrm{d}z \,\mathrm{d}\rho \,\mathrm{d}\varphi = \frac{1}{3}\pi h r^2.$$

najít normu $\delta$ dělení takovou, že pro všechna jemnější dělení již bude platit

$$G(t_{i_1\dots i_n}) + (1+\varepsilon)D^1G(t_{1\dots t_n})(I_{i_1\dots i_n}) \supset J_{i_1\dots i_k}.$$

Pak ovšem jistě bude také pro $n$–rozměrné objemy platit (připomeňme, že vynásobením všech stran rovnoběžnostěnu stejným koeficientem $1+\varepsilon$ vynásobíme jeho objem $n$–tou mocninou téhož koeficientu)

$$\begin{aligned} \mathrm{vol}(J_{i_1\dots i_n}) &\le (1+\varepsilon)^n \,\mathrm{vol}(R_{i_1\dots i_n}) \\ &= (1+\varepsilon)^n \left|\det G(t_{i_1\dots i_k})\right| \,\mathrm{vol}_n(I_{i_1\dots i_n}). \end{aligned}$$

Nyní již umíme celý integrál odhadnout shora

$$\begin{aligned} &\int_M f(x_1,\dots,x_n)\,dx_1\cdots dx_n = \\ &= \sum_{i_1\dots i_n} \int_{J_{i_1\dots in}} f(x_1,\dots,x_n)\,dx_1\dots dx_n \\ &\le \sum_{i_1\dots i_n} \Big(\sup_{(t_1,\dots,t_n)\in I_{i_1\dots in}} g\Big) \,\mathrm{vol}_n(J_{i_1\dots i_n}) \\ &\le (1+\varepsilon)^n \sum_{i_1\dots i_n} \Big(\sup_{(t_1,\dots,t_n)\in I_{i_1\dots in}} g\Big) \left|\det G(t_{i_1\dots i_k})\right| \,\mathrm{vol}_n(I_{i_1\dots i_n}). \end{aligned}$$

Při limitním procesu pro zmenšující se normy dělení zůstává hodnota nalevo stále stejná, zatímco napravo jistě dostaneme Riemannův integrál funkce $g(t_1,\dots,t_n)|\det(D^1G(t_1,\dots,t_n))|$.

Místo dokazované rovnosti ve větě tak dostáváme nerovnost:

$$\begin{aligned} &\int_M f(x_1,\dots,x_n)\,dx_1\dots dx_n \\ &\le \int_N f(G(t_1,\dots,t_n))\left|\det(D^1G(t_1,\dots,t_n))\right| dt_1\dots dt_n. \end{aligned}$$

Nyní však můžeme zopakovat stejnou argumentaci tak, že zaměníme $G$ s $G^{-1}$, obory integrace $M$ a $N$ a funkce $f$ a $g(t_1,\dots,t_n)|\det(D^1G(t_1,\dots,t_n))|$. Okamžitě tak dostaneme nerovnost opačnou:

$$\begin{aligned} &\int_N g(t_1,\dots,t_n)\left|\det(D^1G(t_1,\dots,t_n))\right| dt_1\dots dt_n \\ &\le \int_M f(x_1,\dots,x_n)\left|\det(D^1G(G^{-1}(x_1,\dots,x_n)))\right| \\ &\qquad \left|\det(D^1G^{-1}(x_1,\dots,x_n))\right| dx_1\dots dx_n \\ &= \int_M f(x_1,\dots,x_n)\,dx_1\dots dx_n \end{aligned}$$

a tím je důkaz ukončen. □

**8.32. Příklad v dimenzi dvě.** Docela přehledné jsou transformace proměnných pro integrál spojité funkce $f(x,y)$ ve dvou proměnných. Uvažme diferencovatelnou transformaci



$$G(s,t) = (x(s,t), y(s,t)).$$

Označíme si $g(s,t) = f(x(s,t), y(s,t))$ a dostáváme

$$\int_{G(N)} f(x,y)\,dxdy = \int_N g(s,t) \left|\frac{\partial x}{\partial s}\frac{\partial y}{\partial t} - \frac{\partial x}{\partial t}\frac{\partial y}{\partial s}\right| dsdt.$$

Jako úplně jednoduchý příklad spočteme integrál z charakteristické funkce kružnice o poloměru $R$ (tj. plochu této kružnice) a integrál z funkce $f(t,\theta) = \cos(t)$ zadané v polárních souřadnicích uvnitř kružnice o poloměru $\frac{1}{2}\pi$ (tj. objem schovaný pod takovou „čepičkou jarmulkou posazenou nad počátek“, viz obrázek).

Těžiště zjevně leží na ose $z$. Pro $z$-tovou souřadnici pak máme

$$z = \frac{1}{V}\int_{\text{kužel}} z\,dV = \frac{4}{V}\int_0^{\pi/2}\int_0^r\int_{\frac{h}{r}\rho}^h z\rho\,\mathrm{d}z\,\mathrm{d}\rho\,\mathrm{d}\varphi = \frac{3}{4}h.$$

Těžiště tedy leží ve výšce $\frac{1}{4}h$ nad středem podstavy kužele. □

**8.87.** Určete těžiště tělesa ohraničeného paraboloidem $2x^2 + 2y^2 = z$, válcem $(x+1)^2 + y^2 = 0$ a rovinou $z = 0$.

**Řešení.** Nejprve určeme objem daného tělesa. Zkusme použít válcových souřadnic ($x = r\cdot\cos\varphi$, $y = r\cdot\sin\varphi$, $z = z$): v nich je rovnice paraboloidu $z = 2r^2$, rovnice válce pak zní $r = -2\cos(\varphi)$. Všimneme-li si navíc, že rovina $x = 0$ je tečná k danému válci, snadno již určíme meze příslušného integrálu udávajícího objem zadaného tělesa:

$$\begin{aligned} V &= \int_{\frac{\pi}{2}}^{\frac{3\pi}{2}}\int_0^{-2\cos\varphi}\int_0^{2r^2} r\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi \\ &= \int_{\frac{\pi}{2}}^{\frac{3\pi}{2}}\int_0^{-2\cos\varphi} 2r^3\,\mathrm{d}r\,\mathrm{d}\varphi \\ &= \int_{\frac{\pi}{2}}^{\frac{3\pi}{2}} 8\cos^4\pi\varphi = 3\pi, \end{aligned}$$

kde pro výpočet posledního integrálu můžeme využít rekurentní metodu z 6.22.

Nyní přistupme k výpočtu těžiště tělesa. Z toho, že je těleso symetrické podle roviny $y = 0$ vyplývá, že $y$-ová souřadnice tělesa bude nulová. Zbylé dvě souřadnice $x_T$ a $y_T$ hledaného těžiště spočítáme pomocí následujících integrálů:

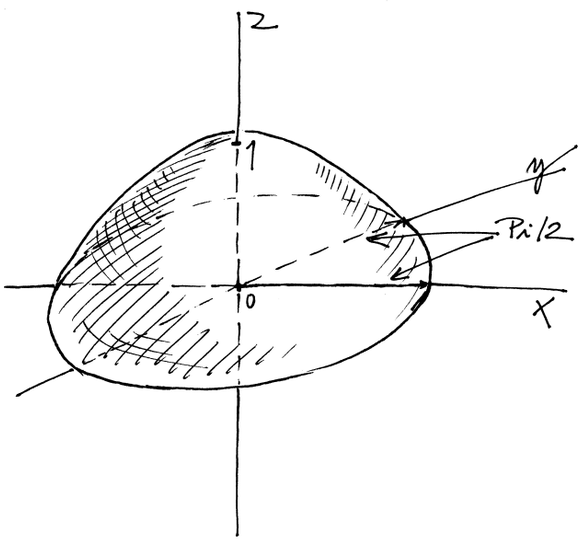
$$\begin{aligned} x_T &= \frac{1}{V}\int\int\int_{\mathrm{B}} x\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z \\ &= \frac{1}{V}\int_0^{2r^2}\int_{\frac{\pi}{2}}^{\frac{3\pi}{2}}\int_0^{-2\cos\varphi} r^2\cos\varphi\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi \\ &= \frac{1}{V}\int_{\frac{\pi}{2}}^{\frac{3\pi}{2}}\int_0^{-2\cos\varphi} 2r^4\cos\varphi\,\mathrm{d}r\,\mathrm{d}ph \\ &= \frac{1}{V}\int_{\frac{\pi}{2}}^{\frac{3\pi}{2}} -\frac{64}{5}\cos^6\varphi\,\mathrm{d}\varphi = -\frac{4}{3}, \end{aligned}$$

kde jsme pro výpočet posledního integrálu opět použili 6.22.

Analogicky pak spočítáme i $z$-tovou souřadnici těžiště:

$$z_T = \frac{1}{V}\int_0^{2r^2}\int_{\frac{\pi}{2}}^{\frac{3\pi}{2}}\int_0^{-2\cos\varphi} zr\cos\varphi\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{20}{9}.$$

Hledané souřadnice těžiště jsou tedy $[-\frac{4}{3}, 0, \frac{20}{9}]$. □




Nejprve spočítáme Jacobiho matici transformace $x = r\cos\theta$, $y = r\sin\theta$

$$D^1G = \begin{pmatrix} \cos\theta & -r\sin\theta \\ \sin\theta & r\cos\theta \end{pmatrix}.$$

Proto je determinant z této matice roven

$$\det D^1G(r,\theta) = r(\sin^2\theta + \cos^2\theta) = r.$$

Můžeme tedy přímo počítat pro kružnici $S$, která je obrazem obdélníku $(r,\theta) \in [0,R]\times[0,2\pi] = T$. Dostaneme tedy plochu kružnice:

$$\int_S dxdy = \int_0^{2\pi}\int_0^R rdr\,d\theta = \int_0^R 2\pi rdr = \pi R^2.$$

Integrace funkce $f$ proběhne s využitím násobného integrování a integrace per partés obdobně:

$$\int_S f\,dxdy = \int_0^{2\pi}\int_0^{\pi/2} r\cos r dr\,d\theta = \pi^2 - 2\pi.$$

**8.33. Křivkové integrály.** Často nám nestačí umět integrovat přes otevřené podmnožiny v $\mathbb{R}^n$, protože naše veličiny jsou dány pouze na objektech podobných křivkám nebo plochám v $\mathbb{R}^3$. Předchozí úvahy o změnách souřadnic při výpočtu integrálů nám přiblížily i intuitivní představu, že je náš proces integrace součtem objemů malých linearizovaných rovnoběžnostěnů vynásobených hodnotou integrované funkce. Rozvinutím této myšlenky bychom mohli zavést integraci na takových vícerozměrných plochách v $\mathbb{R}^n$ přímo. My si ale problém integrace nejprve zbavíme závislosti na souřadnicích a pak jej lehce převedeme na již dobře zvládnutou integraci na $\mathbb{R}^n$.



Připomeňme si výpočet délky křivky pomocí integrálu v jedné proměnné, který jsme diskutovali již v odstavci 6.7. Křivku jsme parametrizovali jako zobrazení $c(t) : \mathbb{R} \to \mathbb{R}^n$ a v euklidovském vektorovém prostoru $\mathbb{R}^n$ jsme vyjádřili velikost $\|c'(t)\|$ tečného vektoru. Tento postup přitom byl dán univerzálním vztahem pro libovolný tečný vektor, tj. našli jsme ve skutečnosti zobrazení $\rho : \mathbb{R}^n \to \mathbb{R}$, které vyčíslením na $c'(t)$ dalo skutečnou velikost. Toto zobrazení splňovalo $\rho(a\,v) = |a|\rho(v)$, protože jsme ignorovali orientaci křivky danou naší parametrizací. Pokud bychom chtěli délku se znaménkem respektujícím orientaci, pak by naše

**8.88.** Určete těžiště homogenního tělesa v $\mathbb{R}^3$, které leží nad rovinou $z = 0$, pod rovinou $z = 2$ a je dále ohraničeno kužely $x^2 + y^2 = z^2$ a $x^2 + y^2 = 2z^2$.

**Řešení.** Úlohu lze řešit standardně, jak jsme činili v předchozích příkladech. Výpočet by bylo například výhodné provádět ve válcových souřadnicích.

My si však všimneme toho, že těleso je jakési „mezikuželí“: vznikne vyříznutím rotačního kužele $K_1$ s podstavou o poloměru 4 z rotačního kužele $K_2$ o poloměru podstavy 8 a společné výšce délky 2.

Těžiště zkoumaného tělesa pak určíme „pravidlem páky“: souřadnice těžiště soustavy dvou těles je dáno váženým průměrem souřadnic těžišť jednotlivých těles, kde váhy jsou dány hmotnostmi těles. (v příkladu ‖8.86‖ jsme vypočítali, že těžiště homogenního rotačního kužele leží ve čtvrtině výšky). Větší a menší kužel tak mají společné těžiště a tudíž tento bod bude těžištěm i zkoumaného tělesa vzniklého vyříznutím menšího kužele z většího. Souřadnice daného tělesa jsou tedy $[0, 0, \frac{3}{2}]$. □

**8.89.** Určete objem tělesa v $\mathbb{R}^3$, které je ohraničeno částí kužele $x^2 + y^2 = (z-2)^2$ a paraboloidem $x^2 + y^2 = 4 - z$.

**Řešení.** Ve válcových souřadnicích sestavíme integrál, který i snadno vypočítáme:

$$V = \int_0^{2\pi} \int_0^1 \int_{r+2}^{4-r^2} r \,\mathrm{d}z \;\mathrm{d}r \,\mathrm{d}\varphi = \frac{5}{6}\pi.$$

□

**8.90.** Určete objem tělesa v $\mathbb{R}^3$, které leží pod kuželem $x^2 + y^2 = (z-2)^2$, $z \le 2$ a nad paraboloidem $x^2 + y^2 = z$.

**Řešení.**

$$V = \int_0^{2\pi} \int_0^1 \int_{r^2}^{2-r} r \,\mathrm{d}z \;\mathrm{d}r \,\mathrm{d}\varphi = \frac{5}{6}\pi.$$

Všimněme si, že uvažované těleso je středově souměrné podle středu $[0, 0, 2]$ s tělesem z předchozího příkladu ‖8.89‖ a má tak nutně stejný objem. □

*8.91.* Určete těžiště plochy omezené parabolou $y = 4 - x^2$ a přímkou $y = 0$. ○

*8.92.* Určete těžiště kruhové výseče z kruhu o poloměru 1 příslušné úhlu 60°. ○

*8.93.* Určete těžiště půlkruhu $x^2 + y^2 = 1$, $y \ge 0$. ○

*8.94.* Určete těžiště kruhové výseče z kruhu o poloměru 1 příslušné úhlu 120°. ○

*8.95.* Určete objem tělesa v $\mathbb{R}^3$ daného nerovnostmi $z \ge 0$, $z - x \le 0$ a $(x-1)^2 + y^2 \le 1$. ○

zobrazení $\rho$ bylo lineární na každém jednorozměrném podprostoru $L \subset \mathbb{R}^n$.

Budeme teď postupovat velice podobně. Uvažme nějakou diferencovatelnou křivku $c(t)$ v $\mathbb{R}^n$, $t \in [a, b]$, a předpokládejme, že je na nějakém okolí jejích hodnot definovaná diferencovatelná funkce $f$. Diferenciál této funkce nám pro každý tečný vektor dává přírůstek této funkce v daném směru. Děje se tak pomocí diferenciálu složeného zobrazení $f \circ c$ vztahem

$$d(f \circ c)(t) = \frac{\partial f}{\partial x_1}(c(t))c_1'(t) + \cdots + \frac{\partial f}{\partial x_n}(c(t))c_n'(t).$$

Můžeme tedy zkusit zadefinovat hodnotu integrálu $\int_M f\,d\,\mathrm{vol}\,M$ funkce $f$ přes neparametrizovanou křivku $M \subset \mathbb{R}^n$ (píšeme zatím symbolicky $\mathrm{vol}\,M$ pro zdáraznění, že se opíráme o pojem objemu, podobně jako jsme u integrálů v jedné proměnné psali $dx$) pomocí nějaké její parametrizace:

$$\int_M f\,\mathrm{vol}_M = \int_a^b \Big( \frac{\partial f}{\partial x_1}(c(t))c_1'(t) + \cdots + \frac{\partial f}{\partial x_n}(c(t))c_n'(t) \Big) dt.$$

Okamžitě ověříme, že změna parametrizace křivky nemá žádný vliv na hodnotu. Skutečně, pokud napíšeme $c(t) = c(\psi(s))$, $a = \psi(\tilde{a})$, $b = \psi(\tilde{b})$, dostaneme naším postupem

$$\int_{\tilde{a}}^{\tilde{b}} \Big( \frac{\partial f}{\partial x_1}(c(\psi(s)))c_1'(\psi(s)) + \ldots + \frac{\partial f}{\partial x_n}(c(\psi(s)))c_n'(\psi(s)) \Big) \frac{d\psi}{ds}\, ds$$

a věta o transformaci souřadnic pro integrál jedné proměnné dává právě stejnou hodnotu, pokud je $\frac{d\psi}{ds} > 0$, tj. pokud zachováváme orientaci křivky, a totéž až na znaménko, pokud je derivace transformace záporná.

Přesněji řešeno, naučili jsme se integrovat diferenciál funkce $df$ přes křivky. Není teď ovšem asi přímo vidět souvislost s integrací funkcí. Evidentně nedostaneme délku křivky, když za $f$ zvolíme konstantní funkci s hodnotou jedna. Ke zdůvodnění potřebujeme geometrický pohled na věc. Velikost vektoru je totiž dána pomocí kvadratické formy, nikoliv lineární. Jestliže ale vezmeme odmocninu z hodnot (pozitivně definitní) kvadratické formy, dostaneme formu lineární, až na znaménka, viz výše. Ještě se k těmto souvislostem vrátíme.

**8.34. Vektorová pole a lineární formy.** Parametrizaci křivky jsme využili v předchozím odstavci k tomu, že jsme ke každému bodu v obrazu $M$ křivky dostali *tečný vektor* $c'(t) \in \mathbb{R}^n$. Máme tak dáno zobrazení $X : M \to M \times \mathbb{R}^n$, $c(t) \mapsto (c(t), c'(t))$. Hovoříme o *vektorovém poli $X$ podél křivky $M$*.

Obecně definujeme *vektorové pole* $X$ na otevřené množině $U \subset \mathbb{R}^n$ jako přiřazení vektoru $X(x) \in \mathbb{R}^n$ v zaměření euklidovského prostoru $\mathbb{R}^n$ ke každému jeho bodu $x$ v uvažovaném definičním oboru.

Jestliže máme dáno vektorové pole $X$ na otevřené množině $U \subset \mathbb{R}^n$, pak můžeme pro každou diferencovatelnou funkci $f$ na $U$ definovat její derivaci ve směru vektorového pole $X$ pomocí směrové derivace předpisem

$$X(f) : U \to \mathbb{R}, \qquad X(f)(x) = d_{X(x)} f.$$

Je-li tedy v souřadnicích $X(x) = (X_1(x), \ldots X_n(x))$, pak

$$X(f)(x) = X_1(x)\frac{\partial f}{\partial x_1}(x) + \cdots + X_n(x)\frac{\partial f}{\partial x_n}(x).$$

*8.96.* Určete objem $\mathbb{R}^3$ daného nerovnostmi $z \geq 0, z - y \leq 0$ ○

*8.97.* Určete objem tělesa ohraničeného plochou

$$3x^2 + 2y^2 + 3z^2 + 2xy - 2yz - 4xz = 1.$$

○

*8.98.* Určete objem části prostoru $\mathbb{R}^3$ uvnitř elipsoidu $2x^2+y^2+z^2 = 6$ a v poloprostoru $x \geq 1$. ○

**8.99. Povrch grafu reálné funkce $f(x, y)$ dvou proměnných $x$ a $y$.** Povrch grafu funkce dvou proměnných nad plochou $S$ v rovině $xy$ je dán integrálem

$$P = \int_S \sqrt{1 + f_x^2 + f_y^2}\,\mathrm{d}x\,\mathrm{d}y.$$

Určete obsah části pláště kužele $x^2 + y^2 = z^2$, která leží nad rovinnou $z = 0$ a uvnitř válce $x^2 + y^2 = y$.

**Řešení.** Hledaný povrch vypočítáme jako povrch grafu funkce $z = \sqrt{x^2 + y^2}$ nad kruhem $K$: $x^2 - (y - \frac{1}{2})^2$. Snadno nahlédneme, že

$$f_x = \frac{x}{x^2 + y^2},\ f_y = \frac{y}{x^2 + y^2}$$

a povrch můžeme vyjádřit integrálem

$$\begin{aligned}\iint_K \sqrt{1 + f_x^2 + f_y^2}\,\mathrm{d}x\,\mathrm{d}y &= \iint_K \sqrt{2}\,\mathrm{d}x\,\mathrm{d}y = \\ = \sqrt{2}\int_0^{\pi}\int_0^{\sin\pi} r\,\mathrm{d}r\,\mathrm{d}\varphi &= \frac{\sqrt{2}}{2}\int_0^{\pi}\sin^2\varphi \\ = \frac{\sqrt{2}\pi}{4}.&\end{aligned}$$

□

*8.100.* Určete povrch plochy paraboloidu $z = x^2 + y^2$ nad kruhem $x^2 + y^2 \leq 4$. ○

*8.101.* Určete povrch části roviny $x+2y+z = 10$ nad útvarem daným nerovnostmi $(x - 1)^2 + y^2 \leq 1$ a $y \geq x$. ○

Ukažme si příklad, kde také využijeme získaných znalostí z teorie Fourierových transformací z minulé kapitoly.

**8.102. Fourierova transformace a difrakce.** Intenzita světla je fyzikální veličina kvantitativně vyjadřující přenos energie vlněním. Intenzita obecné světelné vlny je definována jako časová střední hodnota velikosti Poyntingova vektoru, který je vektorovým součinem navzájem kolmých vektorů elektrického a magnetického pole. Pro monochromatickou rovinnou vlnu šířící se ve směru osy $y$ platí

$$I = c\varepsilon_0\frac{1}{\tau}\int_0^{\tau} E_y^2\,\mathrm{d}t,$$

kde $c$ je rychlost světla a $\varepsilon_0$ je permitivita vakua. Monochromatická vlna je popsána harmonickou funkcí $E_y = \psi(x, t) = A\cos(\omega t -$

Nejjednodušší vektorová pole budou mít v souřadnicích všechny souřadné funkce rovny nule, kromě jedné funkce $X_i$, která bude konstantně jednička. Takové pole pak odpovídá příslušné parciální derivaci podle proměnné $x_i$. Tomu odpovídá také obvyklý zápis

$$X(x) = X_1(x)\frac{\partial}{\partial x_1} + \cdots + X_n(x)\frac{\partial}{\partial x_n}.$$

Množina všech možných tečných vektorů v bodech otevřené podmnožiny $U \in \mathbb{R}^n$ se nazývá *tečný prostor* $TU$. Vektorový prostor všech vektorů v bodě $x$ zapisujeme jako $T_xU$. Pro množinu všech hladkých vektorových polí na $U$ používáme značení $\mathcal{X}(U)$. Vektorová pole $\frac{\partial}{\partial x_i}$ můžeme chápat jako generátory $\mathcal{X}(U)$, jako koeficienty v lineárních kombinacích ovšem připouštíme hladké funkce.

Při studiu vektorových prostorů jsme již ve druhé kapitole narazili na potřebnost tzv. lineárních forem. Definovali jsme je v odstavci 2.39 na straně 95. Lineární forma na zaměření $\mathbb{R}^n$ našeho euklidovského prostoru $\mathbb{R}^n$ přiřazená k bodu $x \in \mathbb{R}^n$ je lineárním zobrazením definovaným na tečném prostoru $T_xU$. Jestliže máme dáno zobrazení $\eta : U \subset \mathbb{R}^n \to \mathbb{R}^{n*}$ na otevřené podmnožině $U$, hovoříme o *lineární formě* $\eta$ *na* $U$.

Každá diferencovatelná funkce $f$ na otevřené podmnožině $U \subset \mathbb{R}^n$ definuje lineární formu $df$ na $U$. Pro množinu všech hladkých lineárních forem na $U$ používáme značení $\Omega^1(U)$.

Je zřejmé, že v souřadnicích $(x_1, \ldots, x_n)$ můžeme využít diferenciálů jednotlivých souřadných funkcí a každou lineární formu $\eta$ vyjádřit

$$\eta(x) = \eta_1(x)dx_1 + \cdots + \eta_n(x)dx_n,$$

kde $\eta_i(x)$ jsou jednoznačně určené funkce. Taková forma $\eta$ se vyčíslí na vektorovém poli $X(x) = X_1(x)\frac{\partial}{\partial x_1} + \cdots + X_n(x)\frac{\partial}{\partial x_n}$ jako

$$\eta(X(x)) = \eta_1(x)X_1(x) + \cdots + \eta_n(x)X_n(x).$$

V případě, že je forma $\eta$ diferenciálem funkce $f$, dostáváme právě výše použité vyjádření $X(f)(x) = df(X(x))$.

Všimněme si, že jsme v předchozím odstavci vlastně zavedli integrál libovolné lineární formy přes (neparametrizované) křivky $M$ pomocí jakékoliv parametrizace $c(t)$

$$\int_M \eta = \int_a^b \eta(c(t))(c'(t))\,dt,$$

protože jsme tehdy sice pracovali s diferenciálem funkce, ale ve skutečnosti jsme ověřili nezávislost hodnoty integrálu na volbě parametrizace pro jakoukoliv lineární formu.

Všimněme si také, že není třeba psát nějaký symbol, označující vzhledem k jakému konceptu objemu integrujeme, je to dáno definicí lineární formy.

**8.35. $k$–rozměrné plochy a $k$–formy.** Místo parametrizovaných



křivek teď budeme pracovat s diferencovatelnými zobrazeními $\varphi : V \subset \mathbb{R}^k \to \mathbb{R}^n$, $k \leq n$, s injektivním diferenciálem $d\varphi(u)$ v každém bodě svého otevřeného definičního oboru $V$. Takovým zobrazením říkáme *imerze*.

Podmnožinu $M \subset \mathbb{R}^n$ nazýváme varietou dimenze $r$, jestliže má každý bod $x \in M$ okolí $U$, které je obrazem takové imerze $\varphi : V \subset \mathbb{R}^k \to M \subset \mathbb{R}^n$, že ji lze rozšířit na zobrazení $\tilde{\varphi} : V \times \tilde{V} \to \mathbb{R}^n$, které je difeomorfismem a $\tilde{\varphi}^{-1}(M) = V \times \{0\}$. Tuto jen zdánlivě složitou definici si můžeme snadno představit pro variety dimenze dvě v $\mathbb{R}^3$ — lokálně je varieta vložená do trojrozměrného

$k\ x$). Číslo $A$ je maximální amplituda vlny, $\omega$ je úhlová frekvence a pro libovolné pevné $t$ je nejmenší periodou tzv. vlnová délka $\lambda$. Přitom $k$ představuje rychlost šíření vlny $k = \frac{2\pi}{\lambda}$. Platí

$$\begin{aligned} I &= c\varepsilon_0 \frac{1}{\tau}\int_0^\tau E_y^2 \,\mathrm{d}t = c\varepsilon_0 \frac{1}{\tau}\int_0^\tau A^2\cos^2(\omega t - k\,x)\,\mathrm{d}t = \\ &= c\varepsilon_0 A^2 \frac{1}{\tau}\int_0^\tau \frac{1+\cos(2(\omega t - k\,x))}{2}\,\mathrm{d}t = \\ &= \frac{1}{2}c\varepsilon_0 A^2 \frac{1}{\tau}\big[t + \frac{\sin(2(\omega t - k\,x))}{2\omega}\big]_0^\tau = \\ &= \frac{1}{2}c\varepsilon_0 A^2 \frac{1}{\tau}\big(\tau + \frac{\sin(2(\omega\tau - k\,x)) - \sin(2(-k\,x))}{2\omega}\big) = \\ &= \frac{1}{2}c\varepsilon_0 A^2\big(1 + \frac{\sin(2(\omega\tau - k\,x)) - \sin(2(-k\,x))}{2\omega\tau}\big) \doteq \frac{1}{2}c\varepsilon_0 A^2 \end{aligned}$$

Druhý člen v závorce můžeme zanedbat, protože je vždy menší než $\frac{2}{2\omega\tau} = \frac{T}{2\pi\tau} < 10^{-6}$ pro reálné detektory světla, je tedy nepatrný oproti 1. Intenzita světla je přímo úměrná druhé mocnině amplitudy.

Difrakcí rozumíme takovou odchylku od přímočarého šíření světla, která nemůže být vysvětlena jako důsledek odrazu či lomu (či změnou směru paprsku v prostředí se spojitě se měnícím indexem lomu). S difrakcí se setkáváme při šíření prostorově ohraničeného svazku světla. Difrakční jevy jsou nejvýrazněji a snadno pozorovatelné tehdy, když světlo prochází otvory či překážkami, jejichž velikost je řádově srovnatelná s vlnovou délkou světla. Při Fraunhoferově difrakci v následujícím příkladu prochází rovinná monochromatická vlna velmi úzkou obdélníkovou štěrbinou a promítá se na vzdálenou plochu, například posvítíme-li laserovým ukazovátkem drobnou štěrbinou na stěnu. Obraz, který dostaneme je Fourierovou transformací funkce propustnosti stínítka - štěrbiny.

Zvolme rovinu difrakčního stínítka za souřadnicovou rovinu $z = 0$. Nechť kolmo na tuto rovinu dopadá rovinná vlna $A\exp(ikz)$ (nezávisí na místě dopadu $(x, y)$ na stínítku). Označme $s(x, y)$ funkci propustnosti stínítka, pak lze výsledné vlnění dopadající na projekční plochu v místě $(\xi, \eta)$ popsat jako integrální součet všech vln (Huygensův-Fresnelův princip), které prošly stínítkem a šíří se dále prostředím ze všech bodů $(x, y, 0)$ (jako kulová vlna) do bodu $(\xi, \eta, z)$:

$$\psi(\xi,\eta) = A\iint_{\mathbb{R}^2} s(x,y)e^{-ik(\xi x+\eta y)}\,\mathrm{d}x\,\mathrm{d}y$$

.

$$\psi(\xi,\eta) = A\int_{-p/2}^{p/2}\int_{-q/2}^{q/2} e^{-ik(\xi x+\eta y)}\,\mathrm{d}y\,\mathrm{d}x$$

$$\psi(\xi,\eta) = A\int_{-p/2}^{p/2} e^{-ik\xi x}\,\mathrm{d}x\int_{-q/2}^{q/2} e^{-ik\eta y}\,\mathrm{d}y =$$

prostoru jako jedna vrstva v cibuli a příslušné křivočaré souřadnice $(x, y, z)$ z definice tuto vrstvu zadávají pomocí konstatní hodnoty $z = 0$. Typicky můžeme proto zadat variety pomocí implicitních zobrazení, viz odstavec 8.18 a diskuse v 8.19.[7]

Zobrazení $\varphi$ z definice nazýváme *lokální parametrizací variety* $M$. Tečný prostor $TM$ k varietě $M$ je soubor vektorových podprostorů $T_xM \subset T_x\mathbb{R}^n$, které obsahují všechny vektory tečné ke křivkám v $M$. Evidentně každá parametrizace $\varphi$ zadává difeomorfismus

$$\varphi_* : TV \to T\varphi(V) \subset TM, \varphi_*(c'(t)) = \frac{d}{dt}\varphi(c(t)).$$

Tato definice nezávisí na volbě křivky reprezentující vektor $c'(t)$, protože při výpočtu derivace na pravé straně potřebujeme znát jen první derivace.

Naše definice jsou přímočarým zobecněním pojmu křivka a plocha v rovině či prostoru a jejich tečen či tečných rovin. Vyloučili jsme přitom křivky a plochy, které se samy protínají, a dokonce i ty, které se samy k sobě jen přibližují. Např. si jistě umíme představit křivku znázorňující číslovku 8 parametrizovanou zobrazením $\varphi$ s všude injektivním diferenciálem. Nebudeme ale umět splnit druhou vlastnost v okolí bodu, kde se nám dvě větve křivky potkávají.

Abychom mohli v lineárním přiblížení hovořit o objemu na $k$–rozměrných varietách, podobně jako jsme to již dělali s křivkami, potřebujeme objekty, které budou v každém bodě lineární v $k$ různých vektorových argumentech a budou jim přiřazovat číslo. Navíc budeme kvůli souladu s orientacemi požadovat, aby při prohození pořadí kterýchkoliv dvou argumentů hodnota změnila znaménko. S takovými objekty jsme se již setkali v odstavci 2.44 na straně 99 a hlavně při počítání objemů rovnoběžnostěnů pomocí determinantu v odstavci 4.22 na straně 206.

### Vnější diferenciální formy

**Definice.** Vektorový prostor všech $k$–lineárních antisymetrických forem na tečném prostoru $T_xU$ na otevřené podmnožině $U \subset \mathbb{R}^n$ budeme značit $\Lambda^k(T_x\mathbb{R}^n)^*$. Stručně hovoříme o vnější $k$–formě v bodě $x$.

Přiřazení $k$–formy $\eta(x)$ každému bodu $x \in U$ z otevřené podmnožiny v $\mathbb{R}^n$ zadává *vnější diferenciální k–formu* na $U$. Množinu hladkých vnějších $k$–forem na $U$ značíme $\Omega^k(U)$. Pro $k = 0$ jde o prostor hladkých funkcí $\Omega^0(U)$ na množině $U$.

Uvažme nyní nějakou hladkou parametrizaci $\varphi : V \to M$ variety $M$, nějaké $\eta(\varphi(u)) \in \Lambda^k(T_{\varphi(u)}\mathbb{R}^n)$ a zvolme libovolně $k$ vektorů $X_1(u), \ldots, X_k(u)$ v tečném prostoru $T_uV$. Podobně jako u lineárních forem nyní můžeme vyčíslit formu $\eta$ na obrazech vektorů $X_i$ pomocí parametrizace $\varphi$. Říkáme této operaci *stažení formy* $\eta$ *pomocí* $\varphi$.

$$\begin{aligned} &\varphi^*(\eta(\varphi(u)))(X_1(u),\ldots,X_k(u)) \\ &\qquad = \eta(\varphi(u))(\varphi_*(X_1(u)),\ldots,\varphi_*(X_1(u))). \end{aligned}$$

Přímo z definice např. spočteme

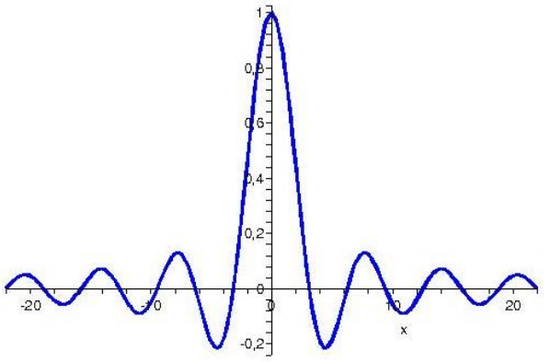
$$\varphi^*(dx_i)\big(\frac{\partial}{\partial u_k}\big) = dx_i\big(\varphi_*\big(\frac{\partial}{\partial u_k}\big)\big) = \frac{\partial\varphi_i}{\partial u_k},$$

[7] Pokud má čtenář v tomto místě požtíže s pochopením pojmu varieta, může se v dalším textu omezit jen na křivky nebo plochy v euklidovských prostorech, resp. podmnožiny zadané lokálně jako grafy hladkých zobrazení.

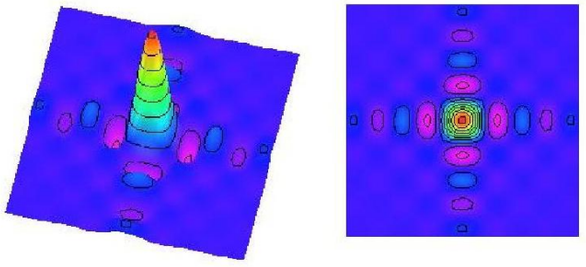
$$= A\left[\frac{e^{-ik\xi x}}{-ik\xi}\right]_{-p/2}^{p/2}\left[\frac{e^{-ik\eta y}}{-ik\eta}\right]_{-q/2}^{q/2} =$$

$$= A\,\frac{2\sin(k\,\xi p/2)}{k\xi}\,\frac{2\sin(k\,\eta q/2)}{k\eta} = Apq\,\frac{\sin(k\,\xi p/2)}{k\xi p/2}\,\frac{\sin(k\,\eta q/2)}{k\eta q/2}$$

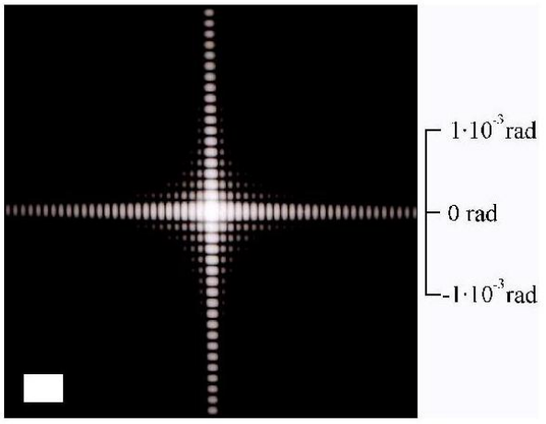
Graf funkce $f(x) = \frac{\sin x}{x}$ vypadá následovně:




Graf funkce $\psi(\xi,\eta) = \frac{\sin\xi}{\xi}\frac{\sin\eta}{\eta}$ pak takto:



Popisovaná difrakce pak takto:




Protože $\lim_{x\to 0}\frac{\sin x}{x} = 1$, je intenzita ve středu obrazu přímo úměrná $I_0 = A^2p^2q^2$. Fourierovu transformaci si můžete prohlédnout jednoduše, když posvítíte laserovým ukazovátkem skrz drobnou škvírku mezi palcem a ukazováčkem, bude to obraz funkce

a tedy

$$\varphi^*(dx_i) = \frac{\partial\varphi_i}{\partial u_1}du_1 + \cdots + \frac{\partial\varphi_i}{\partial u_n}du_n. \tag{8.1}$$

Stejně tak je okamžitým důsledkem definice vztah pro stažení libovolné $k$–formy pomocí složení dvou difeomorfismů. Ověřte si samostatně následující rovnost:

$$(\varphi\circ\psi)^*\alpha = \psi^*\left(\varphi^*\alpha\right). \tag{8.2}$$

Hladká $k$–forma $\eta$ na $k$–rozměrné podvarietě je takové zobrazení $M \to \Lambda^k(T_xM)^*$, že stažením této formy jakoukoliv parametrizací dostaneme hladkou vnější $k$–formu na $V$. Pro množinu všech hladkých vnějších $k$–forem na $M$ budeme používat značení $\Omega^k(M)$.

**8.36. Vnější součin vnějších forem.** Máme-li dány $k$–formu $\alpha \in \Lambda^k\mathbb{R}^{n*}$ a $\ell$–formu $\beta \in \Lambda^k\mathbb{R}^{n*}$, můžeme pomocí všech možných permutací $\sigma$ argumentů snadno vytvořit $(k+\ell)$–formu $\alpha\wedge\beta$.



Musíme prostě prostřídat argumenty ve všech pořadích a opatřit vždy správným znaménkem:

$$(\alpha\wedge\beta)(X_1,\ldots,X_{k+\ell}) = \frac{1}{k!\ell!}\sum_{\sigma\in\Sigma_{k+\ell}}\operatorname{sign}(\sigma)\alpha(X_{\sigma(1)},X_{\sigma(k)})\beta(X_{\sigma(k+1)},X_{\sigma(k+\ell)}).$$

Z definice je zřejmé, že $\alpha\wedge\beta$ je skutečně $(k+\ell)$–forma. V nejjednodušším případě 1–forem definice říká

$$(\alpha\wedge\beta)(X,Y) = \alpha(X)\beta(Y) - \alpha(Y)\beta(X)$$

a v případě 1–formy $\alpha$ a $k$–formy $\beta$ dostáváme

$$(\alpha\wedge\beta)(X_0,X_1,\ldots,X_k) = \sum_{j=0}^{k}(-1)^j\alpha(X_j)\beta(X_0,\ldots,\hat{X}_j,\ldots,X_k),$$

kde stříška značí vynechání příslušného argumentu. Zcela obdobně definujeme vnější součin konečně mnoha forem (buď přímo podobnou formulí nebo si všimneme, že je vnější součin dvou forem asociativní operací – promyslete si samostatně!).

Stejné značení budeme používat pro formy v $\Omega^k(M)$. Tak jako jsme měli generátory $\frac{\partial}{\partial x_i}$ všech vektorových polí v $\mathcal{X}(\mathbb{R}^n)$, stejně jsou všechny lineární formy v $\Omega^1(\mathbb{R}^n)$ generovány formami $dx_i$. Jejich vnější součiny

$$\varepsilon_{i_1\ldots i_k} = dx_{i_1}\wedge\cdots\wedge dx_{i_k}$$

s $k$-ticemi indexů $i_1 < i_2 < \cdots < i_k$ generují celý prostor $\Omega^k(\mathbb{R}^n)$. Skutečně, prohozením dvou sousedních forem v součinu jen měníme znaménko a zejména tedy je celý výraz identicky nulový, jestliže se dva indexy opakují. Každá $k$–forma $\alpha$ je proto dána jednoznačně pomocí funkcí $\alpha_{i_1\ldots i_k}(x)$

$$\alpha(x) = \sum_{i_1<\cdots<i_k}\alpha_{i_1\ldots i_k}(x)dx_{i_1}\wedge\cdots\wedge dx_{i_k}.$$

Všimněme si ještě, že vnější součin funkce, tj. 0–formy, $f$ s $k$–formou $\alpha$ je prostě násobek formy $\alpha$ funkcí $f$.

Ověřte si samostatně, že pro stažení vnějšího součinu pomocí difeomorfismu $\varphi: V\to U$ platí

$$\varphi^*(\alpha\wedge\beta) = \varphi^*\alpha\wedge\varphi^*\beta.$$

její propustnosti. Obraz na posledním obrázku je dobře vidět, pokud si vytvoříte kvalitní obdélníkovou štěrbinu např. slepením dobře ohraněných samolepek.

### I. Aplikace Stokesovy věty – Greenova věta

**8.103.** Vypočtěte

$$\int_c (x-y)dx + x\ \mathrm{d}y,$$

kde $c$ je kladně orientovaná křivka, kterou představuje obvod čtverce $ABCD$ určeného vrcholy $A = [2,2]$; $B = [-2,2]$; $C = [-2,-2]$; $D = [2,-2]$.

**Řešení.** Pomocí Greenovy věty (viz 8.44) převedeme daný křivkový integrál na integrál plošný. Integrál je tvaru $\int_c f(x,y)\,\mathrm{d}x + g(x,y)\,\mathrm{d}y$, kde $f(x,y) = x-y$ a $g(x,y) = x$. Potřebné parciální derivace funkcí $f(x,y)$ a $g(x,y)$ tedy jsou $f_y(x,y) = -1$ a $g_x(x,y) = 1$. Funkce $f(x,y)$ a $g(x,y)$ i $f_y(x,y)$ a $g_x(x,y)$ jsou spojité na $\mathbb{R}^2$. a můžeme tak Greenovy věty použít:

$$\begin{aligned}\int_c (x-y)\ \mathrm{d}x + x\ \mathrm{d}y &= \iint_D (1+1)\ \mathrm{d}x\ \mathrm{d}y == 2\iint_D \mathrm{d}x\ \mathrm{d}y = \\ &= 2\int_{-2}^{2}\int_{-2}^{2} \mathrm{d}x\ \mathrm{d}y = 2\big[x\big]_{-2}^{2}\cdot\big[y\big]_{-2}^{2} = 32.\end{aligned}$$

□

**8.104.** Vypočtěte

$$\int_c x^4\ \mathrm{d}x + xy\ \mathrm{d}y,$$

kde $c$ je kladně orientovaná křivka procházející vrcholy, $A = [0,0]$; $B = [1,0]$; $C = [0,1]$.

**Řešení.** Křivka $c$ je hranicí trojúhelníka $ABC$. Integrované funkce jsou spojitě diferencovatelné dokonce na celém $\mathbb{R}^2$ a můžeme použít Greenovu větu:

$$\begin{aligned}\int_c x^4\ \mathrm{d}x + xy\ \mathrm{d}y &= \iint_D y\ \mathrm{d}x\ \mathrm{d}y = \int_0^1\int_0^{-x+1} y\ \mathrm{d}x\ \mathrm{d}y = \\ &= \int_0^1 \left[\frac{y^2}{2}\right]_0^{-x+1} \mathrm{d}x = \int_0^1 \left[\frac{x^2-2x+1}{2}\right] \mathrm{d}x = \\ &= \frac{1}{2}\left[\frac{x^3}{3} - \frac{2x^2}{2} + x\right]_0^1 = \frac{1}{6}.\end{aligned}$$

□

**8.37. Integrace vnějších forem na $\mathbb{R}^n$.** Úplně jedinečné chování mají vnější $n$–formy na $\mathbb{R}^n$. Máme totiž k dispozici jedinou posloupnost neklesajících $n$ indexů $i_k = k$. Proto je celý prostor $\Omega^n(\mathbb{R}^n)$ generován jedinou formou $\varepsilon_{12\dots n}$ a je možné jej identifikovat s prostorem funkcí $f(x)$. Každá taková funkce nám v každém bodě $x \in \mathbb{R}^n$ definuje infinitesimální výpočet objemu prostředním $n$–formy

$$\omega(x) = f(x)dx_1 \wedge \cdots \wedge dx_n, \tag{8.3}$$

tj. $f$ nám v každém bodě zadává měřítko, s jakým bereme standardní objem. Můžeme tedy nově interpretovat naši dřívější proceduru integrace funkcí $f$ na riemannovsky měřitelných otevřených podmnožinách $U \subset \mathbb{R}^n$.

Nejprve definujeme formu $\omega_{\mathbb{R}^n}$ zadávající standardní $n$–rozměrný objem rovnoběžníků, tj. ve standardních souřadnicích bude

$$\omega_{\mathbb{R}^n} = dx_1 \wedge \cdots \wedge dx_n.$$

Chceme–li „postaru“ integrovat funkci $f(x)$, uvážíme místo ní formu $\omega = f\omega_{\mathbb{R}^n}$, tj. ve standardních souřadnicích bude mít $\omega$ tvar (8.3). Definujeme

$$\int_U \omega = \int_U f(x)dx_1 \wedge \cdots \wedge dx_n = \int_U f(x)\,dx_1 \dots dx_n,$$

kde na pravé straně stojí Riemannův integrál funkce. Všimněme si, že nalevo stojí $n$-forma zcela nezávisle na volbě souřadnic.

Jestliže budeme chtít formu $\omega$ vyjádřit v jiných souřadnicích prostřednictvím difeomorfismu $\varphi : V \to U$, znamená to, že budeme vyčíslovat $\omega$ v bodě $\varphi(u) = x$ na hodnotách vektorů $\varphi_*(X_1), \dots, \varphi_*(X_n)$. To ale znamená, že budeme v souřadnicích $(u_1, \dots, u_n)$ integrovat formu $\varphi^*\omega$, a snadno spočteme (podívejte se na vztah (8.1) v odstavci 8.35)

$$\begin{aligned}(\varphi^*\omega)(u) = f(\varphi(u))\big(&\frac{\partial\varphi_1}{\partial u_1}du_1 + \cdots + \frac{\partial\varphi_1}{\partial u_n}du_n\big) \wedge \dots \\ &\wedge \big(\frac{\partial\varphi_n}{\partial u_1}du_1 + \cdots + \frac{\partial\varphi_n}{\partial u_n}du_n\big) \\ &= f(\varphi(u))\det(D^1\varphi(u))du_1 \wedge \cdots \wedge du_n.\end{aligned}$$

Dosazením do naší interpretace integrálu dostáváme

$$\int \varphi^*(f\omega) = \int_V f(u)\det(D^1\varphi(u))du_1 \cdots du_n,$$

což je podle věty o transformaci proměnných z odstavce 8.31 tatáž hodnota, pokud je determinant Jacobiho matice stále kladný, a stejná hodnota až na znaménko, pokud je záporný.

Naše nová interpretace tedy dává geometrický smysl pro integrál $n$–formy na $\mathbb{R}^n$, pokud příslušný Riemannův integrál v nějakých (a pak už jakýchkoliv) souřadnicích existuje. Tato integrace přitom bere v úvahu orientaci oblasti, přes kterou integrujeme.

**8.38. Integrace vnějších forem na varietách.** Teď už máme skoro všechno připravené pro definici integrálu $k$–formy na $k$–rozměrné orientované varietě. Budeme se pro jednoduchost zabývat hladkými formami $\omega$ s kompaktním nosičem.



**8.105.** Vyčíslete

$$\int_c (xy + x + y)\ \mathrm{d}x + (xy + x - y)\ \mathrm{d}y,$$

kde $c$ je kružnice o poloměru 1 se středem v počátku.

**Řešení.** Opět jsou splněny předpoklady pro užití Greenovy věty a postupně dostáváme

$$\begin{aligned}
&\int_c (xy + x + y)\ \mathrm{d}x + (xy + x - y)\ \mathrm{d}y \\
&= \iint_D y + 1 - x - 1\ \mathrm{d}x\ \mathrm{d}y \\
&= \int_0^1 \int_0^{2\pi} r^2 (\sin\varphi - \cos\varphi)\ \mathrm{d}r\ \mathrm{d}\varphi = \\
&= \int_0^1 r^2\ \mathrm{d}r \int_0^{2\pi} \sin\varphi - \cos\varphi d\varphi = \frac{1}{3}\big[ - \cos\varphi - \sin\varphi\big]_0^{2\pi} = 0.
\end{aligned}$$

□

**8.106.** Vypočtěte $\int_c (2e^{2x}\sin y - 3y^3)dx + (e^{2x}\cos y + \frac{4}{3}x^3)dy$, kde $c$ je kladně orientovaná elipsa $4x^2 + 9y^2 = 36$.

**Řešení.** : Použijeme Greenovu větu, volíme lineární deformaci polárních souřadnic $x = 3r\cos\varphi$, $\varphi \in [0, 2\pi]$,
$y = 2r\sin\varphi$ $r \in [0, 1]$
a dostáváme (jakobián transformace souřadnic je $6r$):

$$\begin{aligned}
&\int_c (2e^{2x}\sin y - 3y^3)dx + (e^{2x}\cos y + \frac{4}{3}x^3)\,\mathrm{d}y = \\
&= \iint_D 2e^{2x}\cos y + 4x^2 - (2e^{2x}\cos y - 9y^2)\ \mathrm{d}x\ \mathrm{d}y = \\
&= \int_0^1 \int_0^{2\pi} 6r\left[4(3r\cos\varphi)^2 + 9(2r\sin\varphi)^2\right] = \\
&= 216\int_0^1 r^3\ \mathrm{d}r \int_0^{2\pi} \mathrm{d}\varphi = 216\cdot\big[\frac{r^4}{4}\big]_0^1 \cdot 2\pi = 108\pi.
\end{aligned}$$

□

**8.107.** Vypočtěte

$$\int_c (e^x \ln y - y^2 x)dx + \left(\frac{e^x}{y} - \frac{1}{2}x^2 y\right)\mathrm{d}y,$$

kde $c$ je kladně orientovaná kružnice $(x-2)^2 + (y-2)^2 = 1$.

Předpokládejme nejprve, že máme danou $k$–rozměrnou varietu $M \subset \mathbb{R}^n$, nějakou její lokální parametrizaci $\varphi : V \subset \mathbb{R}^k \to U \subset M \subset \mathbb{R}^n$. Volbou parametrizace $\varphi$ jsme si zároveň zvolili *orientaci variety* $U \subset M$. Tato orientace bude stejná pro takové volby parametrizací, které se liší o difeomorfismy s kladnými determinanty jejich Jacobiho matic. Orientace bude opačná pro parametrizace lišící se o difeomorfismy se zápornými determinanty Jacobiho matic. Zjevně tedy na každé souvislé varietě $M$ máme právě dvě orientace. Pokud jednu z nich zvolíme, omezujeme tím zároveň množinu parametrizací kompatibilních s touto orientací. Takto budeme dále vždy postupovat a budeme hovořit o *orientovaných varietách*.

Zvolme nyní formu $\omega$ s kompaktním nosičem uvnitř obrazu parametrizace $U \subset M$ orientované variety $M$. Forma $\varphi^*(\omega)$ je hladkou $k$–formou na $V \subset \mathbb{R}^k$ s kompaktním nosičem. *Integrál formy $\omega$ na $M$* definujeme pomocí zvolené parametrizace kompatibilní s orientací takto:

$$\int_M \omega = \int_{\mathbb{R}^k} \varphi^*(\omega).$$

Pokud zvolíme jinou kompatibilní parametrizaci $\tilde\varphi = \varphi \circ \psi$, kde $\psi$ je difeomorfismus $\psi : W \to V \subset \mathbb{R}^k$, snadno můžeme počítat podle stejné definice. Označme si přitom

$$\varphi^*(\omega)(u) = f(u)du_1 \wedge \cdots \wedge du_k.$$

S využitím vztahu (8.2) pro stažení formy pomocí složeného zobrazení spočteme

$$\begin{aligned}
\int_M \omega &= \int_{\mathbb{R}^k} \tilde\varphi^*(\omega) = \int_{\mathbb{R}^k} \psi^*(\varphi^*\omega) \\
&= \int_{\mathbb{R}^k} \psi^*\left(f\ du_1 \wedge \cdots \wedge du_k\right) \\
&= \int_{\mathbb{R}^k} f(\psi(v))\det(D^1\psi)(v)dv_1\cdots dv_k.
\end{aligned}$$

Je to tedy opět stejná hodnota jako $\int_{\mathbb{R}^k}\varphi^*\omega$.

Tím jsme dokázali korektnost naší definice integrálu $\int_M \omega$ za předpokladu, že integrovaná $k$–forma má kompaktní nosič ležící v obrazu jediné parametrizace.

Typické variety $M$ jsou ale dány implicitními rovnicemi, např. $x^2+y^2+z^2 = 1$ zadává povrch jednotkové koule, tj. sféru $S^2 \subset R^3$. Budeme-li chtít integrovat nějakou vnější 2–formu na $S^2$, budeme muset použít několik parametrizací. Naštěstí je zjevně naše definice integrálu aditivní ve vztahu k disjunktním sjednocením oborů integrace. Jestliže tedy umíme napsat

$$M = U_1 \cup U_2 \cup \cdots \cup U_m \cup B,$$

kde $U_i$ jsou po dvou disjunktní obrazy parametrizací $\varphi_i$ a $B$ je množina, jejíž vzor v kterékoliv parametrizaci je riemannovsky měřitelná množina míry nula, spočteme

$$\int_M \omega = \int_{U_1} \omega + \cdots + \int_{U_m} \omega$$

a snadno ověříme, že tato hodnota nezávisí na volbě množin $U_i$ a parametrizací (zejména nás netrápí množina $B$, protože na ní bude výsledek jakékoliv integrace nulový). Představte si třeba rozložení sféry na horní a dolní hemisféru, přičemž rovník $B$ nám zůstane nepokrytý.

Při praktickém počítání si pak zpravidla rozdělíme celou varietu na několik disjunktních oblastí a integrujeme na každém zvlášť. Uvedeme si ale globální definici, která je technicky výhodnější.

**Řešení.**

$$\int_c (e^x \ln y - y^2 x)dx + (\frac{e^x}{y} - \frac{1}{2}x^2 y)dy =$$
$$= \iint_D \frac{e^x}{y} - xy - \frac{e^x}{y} + 2xy \ \mathrm{d}x \ \mathrm{d}y =$$
$$= \int_0^1 \int_0^{2\pi} r(r\cos\varphi + 2)\cdot(r\sin\varphi + 2) \ \mathrm{d}r \ \mathrm{d}\varphi =$$
$$= \int_0^1 \int_0^{2\pi} r^3 \sin\varphi\cos\varphi + 2r^2(\sin\varphi + \cos\varphi) + 4r \ \mathrm{d}r \ \mathrm{d}\varphi =$$
$$= \frac{1}{4}\int_0^{2\pi} \sin\varphi\cos\varphi \ \mathrm{d}\varphi + \frac{2}{3}\int_0^{2\pi} \sin\varphi + \cos\varphi \ \mathrm{d}\varphi + 4\pi =$$
$$= \frac{1}{3}\Big[\frac{\sin^2\varphi}{2}\Big]_0^{2\pi} + \Big[-\cos\varphi + \sin\varphi\Big]_0^{2\pi} + 4\pi = 4\pi.$$

□

*8.108.* Vypočtěte integrál

$$\int_c (e^x \sin y - xy^2)dx + \left(e^x \cos y - \frac{1}{2}x^2 y\right) \mathrm{d}y,$$

kde $c$ je kladně orientovaná kružnice $x^2 + y^2 + 4x + 4y + 7 = 0$. ◯

*8.109.* Vypočtěte

$$\int_c (3y - e^{\sin x}) \ \mathrm{d}x + (7x + \sqrt{y^4 + 1}) \ \mathrm{d}y,$$

kde $c$ je kladně orientovaná kružnice $x^2 + y^2 = 9$. ◯

*8.110.* Vypočtěte integrál

$$\int_c (\frac{1}{x} + 2xy - \frac{y^3}{3})\,dx + (\frac{1}{y} + x^2 + \frac{x^3}{3}) \ \mathrm{d}y,$$

kde $c$ je kladně orientovaná hranice množiny $D = \{(x, y) \in \mathbb{R}^2 : 4 \leq x^2 + y^2 \leq 9, \frac{x}{\sqrt{3}} \leq y \leq \sqrt{3}x\}$. ◯

**8.111. Poznámka.** Důsledkem *Greenovy věty* je vztah pro výpočet obsahu oblasti $D$, která je ohraničená křivkou $c$.

$$m(D) = \frac{1}{2}\int_c -y \ \mathrm{d}x + x \ \mathrm{d}y.$$

**8.39. Rozklad jednotky.** Uvažme nějakou varietu $M \subset \mathbb{R}^n$ a její pokrytí otevřenými obrazy $U_i$ parametrizací $\varphi_i$. Jistě budeme umět najít spočetné pokrytí každé variety $M$ (stačí si uvědomit, že si jistě vystačíme s parametrizacemi, které počátek zobrazí na body s racionálními souřadnicemi v $\mathbb{R}^n$). Navíc můžeme jistě předpokládat, že libovolný bod $x \in M$ patří do nejvýše konečně mnoha množin $U_i$. Takovému pokrytí říkáme *lokálně konečné pokrytí parametrizacemi* $\varphi_i$.



Nyní si vzpomeňme na hladké varianty charakteristických funkcí z odstavce 6.7. Zkonstruovali jsme tam pro každá kladná čísla $0 < \varepsilon < r$ funkci $f_{\varepsilon,r}(t)$ takovou, že $f_{\varepsilon,r}(t) = 1$ pro $|t| < r - \varepsilon$, zatímco $f_{\varepsilon,r}(t) = 0$ pro $|t| > r + \varepsilon$, a $0 \leq f_{\varepsilon,r}(t) \leq 1$ všude. Přitom zároveň platilo $f(t) \neq 0$, právě když $|t| \leq r + \varepsilon$ (na obrázku v 6.6 připomíná graf této funkce charakteristickou funkci).

Jestliže nyní definujeme

$$\chi_{r,\varepsilon,x_0}(x) = f_{\varepsilon,r}(|x - x_0|),$$

dostáváme hladkou funkci identicky jedničkovou uvnitř koule $B_{r-\varepsilon}(x_0)$ s nosičem právě $B_{r+\varepsilon}(x_0)$ a s hodnotami mezi nulou a jedničkou všude.

**Lemma** (Whitneyho věta)**.** *Každá uzavřená množina $K \subset \mathbb{R}^n$ je množinou všech nulových bodů nějaké hladké reálné nezáporné funkce.*

Důkaz. Idea důkazu je prostá. Je-li $K = \mathbb{R}^n$, vyhovuje identicky nulová funkce, předpokládejme $K \neq \mathbb{R}^n$.

Otevřenou množinu $U = \mathbb{R}^n \setminus K$ vyjádříme jako sjednocení nejvýše spočetně mnoha otevřenými koulemi $B_{r_i}(x_i)$ a pro každou z nich zvolíme hladkou nezápornou funkci $f_i$ na $\mathbb{R}^n$, jejíž nosič je právě $B_{r_i}(x_i)$, viz funkce $\chi_{r,\varepsilon,x_0}$ výše. Nyní sečteme všechny tyto funkce do nekonečné řady

$$f(x) = \sum_{k=1}^{\infty} a_k f_k(x),$$

přičemž koeficienty $a_k$ zvolíme tak malé, aby tato řada konvergovala k hladké funkci $f(x)$.

K tomu stačí např. zvolit $a_k$ tak, aby všechny parciální derivace všech funkcí $a_k f_k(x)$ až do řádu $k$ včetně byly shora odhadnuty číslem $2^{-k}$. Pak totiž nejen samotná řada $\sum_k a_k f_k$ je shora odhadnuta součtem řady $\sum_k 2^{-k}$ a tedy podle Weierstrassova kriteria konverguje stejnoměrně na celém $\mathbb{R}^n$, ale totéž dostaneme pro všechny řady parciálních derivací, protože je můžeme vždy napsat jako

$$\sum_{k=0}^{r-1} a_k \frac{\partial^r f_k}{\partial x_{i_1}\cdots\partial x_{i_r}} + \sum_{k=r}^{\infty} a_k \frac{\partial^r f_k}{\partial x_{i_1}\cdots\partial x_{i_r}},$$

přičemž první část je hladká funkce, protože jde o konečný součet hladkých funkcí, a druhou část máme opět odhadnutou shora absolutně konvergující řadou čísel a bude tedy opět tento výraz stejnoměrně konvergovat k $\frac{\partial^r f}{\partial x_{i_1}\cdots\partial x_{ir}}$.

Z definice je zřejmé, že funkce $f(x)$ splňuje požadavky v lemmatu. □

**8.112.** Vypočtěte obsah plochy dané elipsou $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$.

**Řešení.** Použitím vztahu ‖8.111‖ a pomocí transformace souřadnic $x = a\cos t$, $y = b\sin t$, pro $t \in [0, 2\pi]$ dostáváme

$$\begin{aligned} m(D) &= \frac{1}{2}\int_c -y\,\mathrm{d}x + x\,\mathrm{d}y = \\ &= \frac{1}{2}\int_0^{2\pi} a\cos t \cdot b\cos t dt - \frac{1}{2}\int_0^{2\pi} b\sin t \cdot (-a\sin t) dt = \\ &= \frac{1}{2}ab\int_0^{2\pi} \cos^2 t dt + \frac{1}{2}ab\int_0^{2\pi} \sin^2 t dt = \\ &= \frac{1}{2}ab\int_0^{2\pi} \cos^2 t + \sin^2 t dt = \frac{1}{2}ab2\pi = \pi ab, \end{aligned}$$

což je vskutku známý vzorec pro výpočet elipsy s poloosami $a$ a $b$. □

**8.113.** Vypočtěte obsah plochy ohraničené cykloidou danou parametricky $\psi(t) = [a(t - \sin t); a(1 - \cos t)]$, pro $a \geq 0$, $t \in (0, 2\pi)$ a osou $x$.

**Řešení.** Plocha je dána křivkami $c_1$ a $c_2$. Takže pro obsah dostáváme

$$m(D) = \tfrac{1}{2}\textstyle\int_{c_1} -y\,\mathrm{d}x + x\,\mathrm{d}y + \tfrac{1}{2}\int_{c_2} -y\,\mathrm{d}x + x\,\mathrm{d}y.$$

Každý z uvedených integrálů spočítáme zvlášť: parametrické vyjádření křivky $c_1$ (úseku osy $x$) je $(t; 0)$; $t \in [0; 2a\pi]$ a pro první integrál můžeme psát

$$\frac{1}{2}\int_{C_1} -y\,\mathrm{d}x + x\,\mathrm{d}y = \frac{1}{2}\int_0^{2a\pi} 0 \cdot 1\,\mathrm{d}t + \int_0^{2a\pi} t \cdot 0 dt = 0.$$

Parametrické vyjádření křivky $c_2$ je $\psi(t) \in (a(t - \sin t), a(1 - \cos t))$; $t \in [2\pi; 0]$.

Vzorec pro obsah předpokládá kladně orientovanou křivku, což pro uvažované parametrické vyjádření cykloidy znamená, že se pohybujeme proti směru parametrizace, tedy od větší meze k menší.

### Rozklad jednotky na varietě

**Věta.** *Uvažme varietu $M \subset \mathbb{R}^n$ a její lokálně konečné pokrytí otevřenými obrazy $U_i$ parametrizací $\varphi_i$. Pak na množinách $U_i$ existuje soustava hladkých reálných nezáporných funkcí $f_i$ takových, že pro každý bod $x \in M$ platí $\sum_i f_i(x) = 1$ a zároveň $f_i(x) \neq 0$, právě když $x \in U_i$.*

Soustavě funkcí $f_i$ z věty říkáme *rozklad jednotky podřízený lokálně konečnému pokrytí* variety parametrizacemi.

Důkaz. Nejprve si rozšíříme množiny $U_i$ na otevřené množiny $\tilde{U}_i$ pomocí rozšířených parametrizací $\tilde{\varphi}$ z definice pojmu variety a jejích lokálních parametrizací. Jistě tak můžeme učinit tak, aby i nadále byly množiny $\tilde{U}_i$ lokálně konečným pokrytím otevřeného okolí $\tilde{U} = \cup_i \tilde{U}_i \subset \mathbb{R}^n$ variety $M$.

Pro každou otevřenou množinu $\tilde{U}_i$ nyní zvolme funkci $g_i(x)$ na celém $\mathbb{R}^n$, tak aby $g_i(x) \neq 0$ právě pro $x \in \tilde{U}_i$. To umíme podle právě dokázané Whitneyho věty. Nyní je funkce $g(x) = \sum_i g_i(x)$ dobře definovaná pro všechna $x \in \mathbb{R}^n$ a hladká, díky lokální konečnosti pokrytí (pro každý pevný bod $x$ jde o konečnou sumu nenulových funkcí na nějakém jeho okolí). Funkce $g(x)$ je přitom nenulová pro všechna $x \in M$, můžeme proto na místo funkcí $g_i(x)$ zúžených na $M$ uvažovat funkce $f_i(x) = g_i(x)/g(x)$, které již splňují obě požadované vlastnosti ve větě. □

**8.40. Integrace $k$–forem na varietách.** Teď již máme vše připraveno k definici integrálu $k$–forem na $k$–rozměrných varietách. Uvažme tedy nějakou takovou varietu $M \subset \mathbb{R}^n$ a nějakou formu $\omega \in \Omega^k(M)$ s kompaktním nosičem.



Zvolme si nějaké lokálně konečné pokrytí variety $M$ parametrizacemi $\varphi_i : V_i \to U_i$ takovými, že uzávěry všech obrazů $\varphi_i(V_i)$ jsou kompaktní a k tomuto pokrytí podřízený rozklad jednotky $f_i$. Integrál definujeme vztahem

$$\int_M \omega = \int_M \sum_i f_i\omega = \sum_i \int_{U_i} f_i\omega,$$

kde integrály v sumě napravo jsme již definovali, protože formy $f_i\omega$ mají nosič uvnitř obrazu v parametrizaci $\varphi_i$. Ve skutečnosti můžeme předpokládat, že bude naše suma konečná, protože nám stačí uvažovat parametrizace pokrývající kompaktní nosič formy $\omega$. Jde tedy o dobře definované číslo, nicméně je třeba ověřit, že výsledná hodnota skutečně nezávisí na našich volbách.

Zvolme si tedy nějakou novou parametrizaci $\varphi : V \to U$ kousku variety $U \subset M$ a podívejme se, čím integrál přes $U$ přispěje k naší integraci. Dostáváme

$$\int_U \omega = \sum_i \int_{V_i \cap V} (f_i \circ \varphi)(\varphi^*\omega) = \int_V \varphi^*\omega.$$

Na levé straně přitom máme standardní integrál přes otevřenou množinu $\mathbb{R}^k$ a napravo tentýž integrál v jiné parametrizaci.

Pokud tedy zvolíme jiné pokrytí a jiný rozklad jednotky, můžeme výše uvedenou úvahu provést pro společné zjemnění těchto pokrytí a ověříme, že ve skutečnosti je námi definovaný výraz na všech volbách nezávislý (promyslete si podrobněji!).

Pro obsah cykloidy tak dostáváme

$$\frac{1}{2}\int_{c_2} -y\ \mathrm{d}x + x\ \mathrm{d}y = \frac{1}{2}\int_{2\pi}^{0} a(t-\sin t)\cdot a(\sin t)\ \mathrm{d}t -$$

$$-\frac{1}{2}\int_{2\pi}^{0} a(1-\cos t)\cdot a(1-\cos t)\ \mathrm{d}t =$$

$$=\frac{1}{2}a^2\int_{0}^{2\pi} t\sin t - \sin^2 t - 1 + 2\cos t - \cos^2 t\ \mathrm{d}t =$$

$$=\frac{1}{2}a^2\int_{2\pi}^{0} t\sin t + 2\cos t - 2\ \mathrm{d}t =$$

$$=\frac{1}{2}a^2[-t\cos t - \sin t + 2\cos t - 2]_{2\pi}^{0} = 3\pi a^2.$$

□

### J. Aplikace Stokesovy věty – Gaussova-Ostrogradského věta

**8.114.** Vypočtěte $I = \iint_S x^3\ \mathrm{d}y\ \mathrm{d}z + y^3\ \mathrm{d}x\ \mathrm{d}z + z^3\ \mathrm{d}x\ \mathrm{d}y$, kde $S$ je dáno koulí $x^2+y^2+z^2=1$.

**Řešení.** V průběhu výpočtu bude výhodné použít sférických souřadnic

$$\begin{aligned} x &= \rho\sin\varphi\cos\psi & \rho &= [0,1],\\ y &= \rho\sin\varphi\sin\psi & \varphi &= [0,\pi],\\ z &= \rho\cos\varphi & \psi &= [0,2\pi]. \end{aligned}$$

Jakobián této transformace je $-\rho^2\sin\varphi$.

Zadaný integrál je pak roven

$$I = \iint_S x^3\ \mathrm{d}y\ \mathrm{d}z + y^3\ \mathrm{d}x\ \mathrm{d}z + z^3\ \mathrm{d}x\ \mathrm{d}y =$$

$$= \iiint_V 3x^2 + 3y^2 + 3z^2\ \mathrm{d}x\ \mathrm{d}y\ \mathrm{d}z =$$

$$= 3\int_0^1\int_0^{2\pi}\int_0^{\pi} \rho^2\sin\varphi\left(\rho^2\sin^2\varphi\cos^2\psi + \rho^2\sin^2\varphi\sin^2\psi + \right.$$

$$\left. +\rho^2\cos^2\varphi\right)\ \mathrm{d}\rho\ \mathrm{d}\varphi\ \mathrm{d}\psi =$$

$$= 3\int_0^1\int_0^{2\pi}\int_0^{\pi} \rho^4\sin\varphi\left(\sin^2\varphi\left(\cos^2\psi+\sin^2\psi\right) + \right.$$

$$\left. +\cos^2\varphi\right)\ \mathrm{d}\rho\ \mathrm{d}\varphi\ \mathrm{d}\psi =$$

$$= 3\int_0^1\int_0^{2\pi}\int_0^{\pi} \rho^4\sin\varphi\ \mathrm{d}\rho\ \mathrm{d}\varphi\ \mathrm{d}\psi = 3\cdot\left[\frac{\rho^5}{5}\right]_0^1 [\psi]_0^{2\pi}[\cos\varphi]_0^{\pi} =$$

**8.41. Vnější diferenciál vnějších forem.** Jak jsme viděli, diferenciál funkce lze chápat jako zobrazení

$$d : \Omega^0(\mathbb{R}^n) \to \Omega^1(\mathbb{R}^n).$$

Prostřednictvím parametrizací lze tuto definici rozšířit na funkce na varietách $M$ a jejich diferenciálem jsou lineární formy na $M$. Následující věta tento diferenciál rozšiřuje na libovolné vnější formy na varietách $M \subset \mathbb{R}^n$.

VNĚJŠÍ DIFERENCIÁL

**Věta.** *Existuje jediné zobrazení $d : \Omega^k(M) \to \Omega^{k+1}M$, pro všechny variety $M \subset \mathbb{R}^n$ a $k = 0, \dots, n$, takové že*

- *$d$ je lineární vzhledem k násobení reálnými čísly,*
- *pro $k = 0$ jde o diferenciál funkcí,*
- *$d(\alpha\wedge\beta) = (d\alpha)\wedge\beta + (-1)^r\alpha\wedge(d\beta)$, kde $\alpha \in \Omega^r(M)$,*
- *pro každou funkci $f$ na $M$ platí $d(df) = 0$.*

Zobrazení $d$ říkáme *vnější diferenciál*.

DŮKAZ. Pišme lokálně $k$–formu ve tvaru

$$\alpha = \sum_{i_1<\cdots<i_k} a_{i_1\cdots i_k} dx_{i_1}\wedge\cdots\wedge dx_{i_k}.$$

Jestliže diferenciál $d$ existuje, pak podle požadovaných vlastností musí být roven

$$d\alpha = \sum_{i_1<\cdots<i_k} da_{i_1\cdots i_k} dx_{i_1}\wedge\cdots\wedge dx_{i_k}$$

$$= \sum_{i_1<\cdots<i_k} \frac{\partial a_{i_1\cdots i_k}}{\partial x_i} dx_i\wedge dx_{i_1}\wedge\cdots\wedge dx_{i_k}.$$

Skutečně, bázové lineární formy $dx_i$ jsou ve skutečnosti diferenciály souřadných funkcí, a proto dalším diferencování již podle poslední vlastnosti musíme dostat nulu, zatímco diferenciál funkcí známe. Přitom dále je $d(f\beta) = df\wedge\beta + f\,d\beta$. (Promyslete si podrobnosti!).

Naopak, když takto v souřadnicích diferenciál $d$ definujeme, snadno ověříme všechny požadované vlastnosti. (Dokončete samostatně!) □

**8.42. Variety s hranicí.** V praktických úlohách často pracujeme



s varietami $M$ jako je např. otevřená koule v trojrozměrném prostoru, zároveň nás ale zajímá i hranice těchto variet $\partial M$, což je v případě koule sféra.

Nejjednodušší je situace se souvislými křivkami. Buď jde o uzavřenou křivku, jako je např. kružnice v rovině, a pak je její hranice prázdná, nebo je hranice tvořena dvěma hraničními body. Tyto body budeme brát včetně orientace zděděné z křivky, tj. počáteční bod budeme brát se znaménkem mínus, koncový se znaménkem plus.

Všimněme si, že jestliže integrujeme po křivce $M$, která je obrazem parametrizace $\varphi : [a,b]$, diferenciál funkce $df$, pak přímo z definice dostáváme

$$\int_M df = \int_a^b d(f\circ\varphi)(t)\,dt = f(\varphi(b)) - f(\varphi(a)).$$

Výsledek tedy nezáleží nejen na zvolené parametrizaci, nýbrž ani na skutečné křivce. Záleží jen na počátečním a koncovém bodu.

$$= 3 \cdot \frac{1}{5} \cdot 2\pi \cdot [-1-1] = -\frac{12}{5}\pi.$$

□

**8.115. Vektorový tvar Gaussovy-Ostrogradského věty.** Pro vektorové pole $F(x,y,z) = f(x,y,z)\frac{\partial}{\partial x} + g(x,y,z)\frac{\partial}{\partial y} + h(x,y,z)\frac{\partial}{\partial z}$ definujeme jeho divergenci $\operatorname{div} X := f_x + g_y + h_z$. Gaussovu-Ostrogradského větu pak můžeme formulovat takto:

$$\iiint_V \operatorname{div}\vec{F}(x,y,z)\ \mathrm{d}x\ \mathrm{d}y\ \mathrm{d}z = \iint_S \vec{F}(x,y,z)\cdot\vec{n}(x,y,z)\ \mathrm{d}S,$$

kde $\vec{n}(x,y,z)$ je jednotková vnější normála k ploše $S$ v bodě $[x,y,z] \in S$ ($S$ je hranicí normálního oboru V).

**8.116.** Vypočtěte tok vektorového pole daného funkcí $F = (xy^2, yz, x^2z)$, přes válec $x^2+y^2 = 4, z = 1, z = 3$.

**Řešení.** Nejprve spočtěme divergenci daného vektorového pole:

$$\operatorname{div} F = \nabla\cdot F = \left(\frac{\partial(xy^2)}{\partial x} + \frac{\partial(yz)}{\partial y} + \frac{\partial(x^2z)}{\partial z}\right) = y^2 + z + x^2.$$

Tedy tok $T$ vektorového pole je rovem

$$\iiint_V y^2+z+x^2\ \mathrm{d}x\ \mathrm{d}y\ \mathrm{d}z =$$

$$= \int_0^2\int_0^{2\pi}\int_1^3 \rho\cdot(\rho^2\sin^2\varphi + z + \rho^2\cos^2\varphi)\ \mathrm{d}\rho\ \mathrm{d}\varphi\ \mathrm{d}z =$$

$$= \int_0^2\int_0^{2\pi}\int_1^3 \rho\cdot(\rho^2(\sin^2\varphi+\cos^2\varphi) + z)\ \mathrm{d}\rho\ \mathrm{d}\varphi\ \mathrm{d}z =$$

$$= \int_0^2\int_0^{2\pi}\int_1^3 \rho\cdot(\rho^2(\sin^2\varphi+\cos^2\varphi) + z)\ \mathrm{d}\rho\ \mathrm{d}\varphi\ \mathrm{d}z =$$

$$= \int_0^2\int_0^{2\pi}\int_1^3 \rho^3 + \rho z\ \mathrm{d}\rho\ \mathrm{d}\varphi\ \mathrm{d}z =$$

$$= 2\pi\int_0^2\int_1^3 \rho^3+\rho z\ \mathrm{d}\rho\ \mathrm{d}z = 2\pi\int_1^3 [\frac{\rho^4}{4}+\frac{\rho^2}{2}z]_0^2\ \mathrm{d}z =$$

$$= 2\pi\int_1^3 4+2z\ \mathrm{d}z = 2\pi[4z+z^2]_1^3 = 2\pi[12+9-4-1] = 32\pi.$$

□

Když si křivku rozdělíme na několik na sebe navazujících disjunktních intervalů, integrál se rozpadne na součet rozdílů hodnot v koncových bodech, ty se však všechny vykrátí a zůstane nám opět totéž.

Tento jev nyní budeme diskutovat v obecných dimenzích. K tomu potřebujeme formalizovat pojem hranice variety a její orientace. Nejjednodušším příkladem je poloprostor $\bar{M} = \mathbb{R}_- \times \mathbb{R}^{n-1}$, kde $\mathbb{R}_- = \{(x_1,\dots,x_n)\in\mathbb{R}^n;\ x_1 \le 0\}$. Jeho hranicí je $\partial M = \{(x_1,x_2,\dots,x_n)\in\mathbb{R}^n;\ x_1 = 0\}$. Orientací na tomto poloprostoru zděděnou ze standardní orientace rozumíme tu určenou formou $dx_2\wedge\cdots\wedge dx_n$.

### Orientovaná hranice variety

Uvažme uzavřenou podmnožinu $\bar{M}\subset\mathbb{R}^n$ takovou, že její vnitřek $M\subset\bar{M}$ je orientovanou $k$–rozměrnou varietou s pokrytím kompatibilními parametrizacemi $\varphi_i$. Dále předpokládejme, že pro každý hraniční bod $x\in\partial M = \bar{M}\setminus M$ má okolí v $\bar{M}$ s parametrizací $\varphi: V\subset\mathbb{R}_-\times\mathbb{R}^{k-1}\to M$ takovou, že body $x\in\partial M\cap\varphi(V)$ jsou právě obrazem hranice poloprostoru $\mathbb{R}_-\times\mathbb{R}^{k-1}$. Podmnožinu $\bar{M}$ s těmito vlastnostmi nazýváme *orientovaná varieta s hranicí*.

Zúžení parametrizací zahrnujících hranici na tuto hranici $\partial M$ zadává na $\partial M$ strukturu $k-1$–rozměrné orientované variety.

**8.43. Stokesova věta.** Nyní se dostáváme k velice důležitému a užitečnému výsledku. Hlavní větu o vícerozměrné analogii křivkových a plošných integrálů formulujeme pro hladké formy a hladké variety. Zběžná analýza důkazu ale ukazuje, že ve skutečnosti potřebujeme jen jednou spojitě diferencovatelnou vnější formu, kterou integrujeme, a dvakrát spojitě integrovatelné parametrizace variety. V praxi navíc často máme hranici oblasti podobnou jako třeba u jednotkové krychle v $\mathbb{R}^3$. Tj. máme v hranici nespojitosti derivací na riemannovsky měřitelné množině míry nula. V takovém případě si integraci rozdělíme na hladké části a výsledky sečteme. Všimněme si, že přitom sice vzniknou nové kusy hranic, ty však sousedí a jsou v sousedících oblastech s opačnými orientacemi, takže se jejich přínos integraci vzájemně vyruší (podobně jako tomu výše bylo u hraničních bodů po částech diferencovatelné křivky).

### Stokesova věta

**Věta.** *Uvažme hladkou vnější $(k-1)$–formu $\omega$ s kompaktním nosičem na orientované varietě $\bar{M}$ s hranicí $\partial M$ se zděděnou orientací. Pak platí*

$$\int_M d\omega = \int_{\partial M}\omega.$$

Důkaz. S využitím vhodného lokálně konečného pokrytí variety $\bar{M}$ a jemu podřízeného rozkladu jednotky vyjádříme integrály na obou stranách jako součet (dokonce konečný, protože je nosič uvažované formy $\omega$ kompaktní) integrálů forem na $\mathbb{R}^k$ nebo poloprostoru $\mathbb{R}_-\times\mathbb{R}^{k-1}$.

Rozklad jednotky se nám tu hodí jako topologický nástroj umožňující lokalizovat řešený problém a dokazovat větu zvlášť pro dva případy, $M=\mathbb{R}^k$ a $M=\mathbb{R}_-\times\mathbb{R}^{k-1}$. Začneme s obtížnějším případem poloprostoru $M$. Uvažme tedy formu $\omega$ je forma s kompaktním nosičem na uzávěru $\bar{M}$. Pak bude $\omega$ jistě součtem forem

**8.117.** Vypočtěte tok vektorového pole daného funkcí $F = (y, x, z^2)$, přes kouli $x^2 + y^2 + z^2 = 4$.

**Řešení.** Divergence daného vektorového pole je:

$$\operatorname{div} F = \nabla \cdot F = \left(\frac{\partial y}{\partial x} + \frac{\partial x}{\partial y} + \frac{\partial z^2}{\partial z}\right) = 2z.$$

Hledaný tok je pak roven

$$\begin{aligned}
&\iiint_V 2z \,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z = \int_0^2 \int_0^{\pi} \int_0^{2\pi} \rho^2 \sin\varphi \cdot 2\rho\cos\varphi \,\mathrm{d}\rho\,\mathrm{d}\varphi\,\mathrm{d}\psi = \\
&= 2\int_0^2 \rho^3 \,\mathrm{d}\rho \int_0^{2\pi} \mathrm{d}\psi \int_0^{\pi} \sin\varphi\cos\varphi \,\mathrm{d}\varphi = \\
&= 2[\frac{\rho^4}{4}]_0^2 \cdot [\psi]_0^{2\pi} \cdot [\frac{\sin^2\varphi}{2}]_0^{\pi} = \\
&= 2 \cdot \frac{16}{4} \cdot 2\pi \cdot 0 = 0.
\end{aligned}$$

□

### K. Diferenciální rovnice 1.řádu

**8.118.** Určete všechna řešení diferenciální rovnice

$$y' = \frac{\sqrt{1-y^2}}{\cos^2 x}\left(1 + \cos^2 x\right).$$

**Řešení.** Máme zadánu obyčejnou diferenciální rovnici prvního řádu ve tvaru $y' = f(x, y)$, čemuž říkáme, že je rozřešená vzhledem k derivaci. Navíc ji můžeme uvést do tvaru $y' = f_1(x) \cdot f_2(y)$ pro spojité funkce $f_1$ a $f_2$ jedné proměnné (na jistých otevřených intervalech), tj. jedná se o diferenciální rovnici se separovanými proměnnými.

Při výpočtu nejprve nahradíme $y' = dy/dx$ a upravíme diferenciální rovnici do tvaru

$$\frac{1}{\sqrt{1-y^2}}\,dy = \frac{1+\cos^2 x}{\cos^2 x}\,dx.$$

Neboť

$$\int \frac{1+\cos^2 x}{\cos^2 x}\,dx = \int \frac{1}{\cos^2 x} + 1\,dx,$$

můžeme integrováním podle základních vzorců získat

$$\arcsin y = \operatorname{tg} x + x + C, \quad C \in \mathbb{R}. \tag{8.6}$$

Uvědomme si však, že při dělení výrazem $\sqrt{1-y^2}$ jsme mlčky předpokládali jeho nenulovost, tj. výpočet je platný pro $y \neq \pm 1$. Dosadíme-li konstantní funkce $y \equiv 1$, $y \equiv -1$ do dané diferenciální rovnice, ihned vidíme, že diferenciální rovnici vyhovují. Máme tedy další dvě řešení, o kterých mluvíme jako o singulárních. Situaci, kdy je $\cos x = 0$, neřešíme. V tomto případě totiž pouze ztrácíme body definičních oborů (nikoli samotná řešení).

tvaru

$$\omega = \eta_j(x) dx_1 \wedge \cdots \wedge \hat{dx_j} \wedge \cdots \wedge dx_k,$$

kde stříška značí vynechání příslušné lineární formy a $\omega_j(x)$ je hladká funkce s kompaktním nosičem. Její vnější diferenciál je

$$d\omega = (-1)^j \frac{\partial \eta_j}{\partial x_j} dx_1 \wedge \cdots \wedge dx_k.$$

Pokud je $j > 1$, je vyčíslení formy $\omega$ podél hranice $\partial M = \{x \in \mathbb{R}^k;\ x_1 = 0\}$ identicky nulové. Zároveň s využitím základní věty o primitivní funkci pro funkce jedné proměnné dostáváme

$$\begin{aligned}
\int_M d\omega &= (-1)^j \int_{\mathbb{R}^{k-1}} \left(\int_{-\infty}^{\infty} \frac{\partial \eta_j}{\partial x_j}\,dx_j\right) dx_1 \cdots \hat{dx_j} \cdots dx_k \\
&= (-1)^j \int_{\mathbb{R}^{k-1}} \left[\eta_j\right]_{-\infty}^{\infty} dx_1 \cdots \hat{dx_j} \cdots dx_k = 0,
\end{aligned}$$

protože má funkce $\omega_j$ kompaktní nosič. Věta tedy v tomto případě platí. Pokud je ale $j = 1$, pak dostáváme

$$\begin{aligned}
\int_M d\omega &= \int_{\mathbb{R}^{k-1}} \left(\int_{-\infty}^{0} \frac{\partial \eta_1}{\partial x_1}\,dx_1\right) dx_2 \cdot \cdots \cdot dx_k \\
&= \int_{\mathbb{R}^{k-1}} \eta_1(0, x_2, \ldots, x_k) dx_2 \cdots dx_k = \int_{\partial M} \omega.
\end{aligned}$$

Tím je důkaz Stokesovy věty ukončen. □

**8.44. Poznámky o využití Stokesovy věty.** Dokázali jsme mimořádně důležitý výsledek, který pokrývá několik klasických integrálních vztahů z klasické vektorové analýzy. Např. si všimněme, že podle Stokesovy věty je integrace vnějšího diferenciálu $d\omega$ jakékoliv $(k-1)$–formy přes kompaktní varietu bez hranice vždy nulová (např. když integrujeme 2–formu $d\omega$ přes sféru $S^2 \subset \mathbb{R}^3$).



Podívejme se postupně na případy Stokesovy věty v nízkých dimenzích.

**Případ** $n = 2, k = 1$**.** Zkoumáme tedy plochu $M$ v rovině ohraničenou křivkou $C = \partial M$. Je-li forma $\omega(x, y) = f(x, y)dx + g(x, y)dy$, je $d\omega = \left(-\frac{\partial f}{\partial y} + \frac{\partial g}{\partial x}\right)dx \wedge dy$. Stokesova věta tedy dává vztah

$$\int_C f(x, y)dx + g(x, y)dy = \int_M \left(-\frac{\partial f}{\partial y} + \frac{\partial g}{\partial x}\right)dx \wedge dy,$$

což je jeden z klasických tvarů tzv. *Greenovy věty*.

Jestliže využijeme standardní skalární součin na $\mathbb{R}^2$, můžeme vektorové pole $X$ ztotožnit s lineární formou $\omega_X$ takovou, že $\omega_X(Y) = \langle Y, X\rangle$. Ve standardních souřadnicích $(x, y)$ to prostě znamená, že pole $X = f(x, y)\frac{\partial}{\partial x} + g(x, y)\frac{\partial}{\partial y}$ zadá právě formu $\omega$ zadanou výše. Integrál z $\omega_X$ podél křivky $C$ má ve fyzice význam práce vykonané pohybem po této křivce v silovém poli $X$. Greenova věta pak mimo jiné říká, že pokud je $\omega_X = dF$ pro nějakou funkci $F$, pak je vykonaná práce po uzavřené křivce vždy nulová. Takovým polím se říká potenciálové a funkce $F$ je potenciál pole $X$.

Také jsme Greenovou větou znovu ověřili, že integrace diferenciálu funkce po křivce závisí jen na počátečním a koncovém bodu křivky.

**Případ** $n = 3, k = 2$**.** Zkoumáme oblast v $\mathbb{R}^3$ ohraničenou plochou $S$. Je-li $\omega = f(x, y, z)dy \wedge dz + g(x, y, z)dz \wedge dx +$

Nyní si několik částí výpočtu okomentujme. Vyjádření $y' = dy/dx$ umožňuje mnoho symbolických úprav. Kupříkladu je

$$\frac{dz}{dy}\cdot\frac{dy}{dx}=\frac{dz}{dx},\quad \frac{1}{\frac{dy}{dx}}=\frac{dx}{dy}.$$

Platnost těchto dvou „samozřejmých“ vztahů je ve skutečnosti zaručena po řadě větou o derivaci složené funkce a větou o derivaci inverzní funkce. Právě výhodnost jasných úprav byla motivací pro G. W. Leibnize při zavádění dodnes používaného značení. Dále si všimněme, že jsme obecné řešení (‖8.6‖) neupravili do nabízejícího se tvaru

$$y=\sin(\operatorname{tg}x+x+C),\quad C\in\mathbb{R}. \tag{8.7}$$

Přestože, jak je koneckonců obvyklé, nebudeme při počítání diferenciálních rovnic uvádět definiční obory (pro která $x$ mají výrazy smysl), nebudeme je ani měnit „nadbytečnými“ úpravami. Je totiž zřejmé, že funkce $y$ uvedená v (‖8.7‖) je definována pro všechna $x\in(0,\pi)\setminus\{\pi/2\}$, avšak pro hodnoty $x$ blízké $\pi/2$ (při daném $C$) neexistuje $y$ takové, aby bylo splněno (‖8.6‖). Řešeními diferenciálních rovnic jsou obecně křivky, které není vždy možné vyjádřit jako grafy elementárních funkcí (na celých intervalech, kde je uvažujeme). Proto se o to občas nebudeme ani pokoušet. □

**8.119.** Uveďte obecné řešení rovnice $y' = (2-y)\operatorname{tg}x$.

**Řešení.** Opět máme diferenciální rovnici se separovanými proměnnými. Postupně dostáváme

$$\begin{aligned}\frac{dy}{dx}&=(2-y)\operatorname{tg}x,\\ -\frac{dy}{y-2}&=\frac{\sin x}{\cos x}\,dx,\\ -\ln|y-2|&=-\ln|\cos x|-\ln|C|,\quad C\neq 0.\end{aligned}$$

Posunutí dané integrováním jsme zde vyjádřili pomocí $\ln|C|$, což je vhodné (vzhledem k následujícím úpravám) zvláště tehdy, když na obou stranách rovnice obdržíme logaritmus. Dále je

$$\begin{aligned}\ln|y-2|&=\ln|C\cos x|,\quad C\neq 0,\\ |y-2|&=|C\cos x|,\quad C\neq 0,\\ y-2&=C\cos x,\quad C\neq 0,\end{aligned}$$

kde bychom měli psát $\pm C$ (po odstranění absolutní hodnoty). Tím, že však uvažujeme všechna nenulová $C$, nezáleží na tom, zda píšeme $+C$, nebo $-C$. Všimněme si, že jsme dělili výrazem $y-2$. Proto je třeba případ $y\equiv 2$ vyšetřovat zvlášť. Derivace konstantní funkce je nulová, a tudíž jsme nalezli ještě jedno řešení $y\equiv 2$. To však není singulární: volbou $C=0$ jej můžeme zahrnout do dříve určeného obecného řešení.

$h(x,y,z)dx\wedge dy$, dostaneme $d\omega=\left(\frac{\partial f}{\partial x}+\frac{\partial g}{\partial y}+\frac{\partial h}{\partial z}\right)dx\wedge dy\wedge dz$ a Stokesova věta říká

$$\begin{aligned}\int_S f(x,y,z)dy\wedge dz+g(x,y,z)dz\wedge dx+h(x,y,z)dx\wedge dy\\ =\int_M\left(\frac{\partial f}{\partial x}+\frac{\partial g}{\partial y}+\frac{\partial h}{\partial z}\right)dx\wedge dy\wedge dz.\end{aligned}$$

To je tvrzení tzv. *Gaussovy–Ostrogradského věty*.

I tato věta má velmi názornou fyzikální interpretaci. Každé vektorové pole $X=f(x,y,z)\frac{\partial}{\partial x}+g(x,y,z)\frac{\partial}{\partial y}+h(x,y,z)\frac{\partial}{\partial z}$ zadá dosazením za první argument ve standardní formě objemu vnější 2–formu $\omega^X(x,y,z)=f(x,y,z)dy\wedge dz+g(x,y,z)dz\wedge dx+h(x,y,z)dx\wedge dy$. Integrál této formy přes plochu můžeme vnímat tak, že integrovaná 2–forma v každém bodě infinitesimálně přidá k integrálu přírůstek rovný objemu rovnoběžnostěnu zadaného polem $X$ a malým kouskem plochy. Vnímáme-li vektorové pole jako rychlost pohybu jednotlivých bodů prostoru, půjde o „průtok“ danou plochou. Na pravé straně integrálu pak je výraz, který můžeme definovat jako $d(\omega^X)=(\operatorname{div}X)dx\wedge dy\wedge dz$. Gaussova–Ostrogradského věta říká, že když je $\operatorname{div}X$ identicky nulové, pak celkový průtok hraniční plochou oblasti je nulový. Proto se polím s $\operatorname{div}X=0$ říká bezzřídlová pole.

**Případ $n=3,k=1$.** V tomto případě máme v $\mathbb{R}^3$ plochu $M$ ohraničenou křivkou $C$. V případě, že lineární forma $\omega$ je diferenciálem nějaké funkce, zjišťujeme, že integrál po ploše závisí jen na hraniční křivce. Jde o *klasickou Stokesovu větu*. Pokud stejně jako v rovině použijeme standardní skalární součin k identifikaci vektorového pole $X=f\frac{\partial}{\partial x}+g\frac{\partial}{\partial y}+h\frac{\partial}{\partial z}$ s formou $\omega=f dx+g dx+h dz$, dostaneme

$$\int_C f dx+g dx+h dz=\int_M d\omega,$$

kde $d\omega=\left(\frac{\partial h}{\partial y}-\frac{\partial g}{\partial z}\right)dy\wedge dz+\left(\frac{\partial f}{\partial z}-\frac{\partial g}{\partial x}\right)dz\wedge dx+\left(\frac{\partial g}{\partial x}-\frac{\partial f}{\partial y}\right)dx\wedge dy$. Tuto 2–formu můžeme opět identifikovat s jediným vektorovým polem $\operatorname{rot}X$, které dá $d\omega$ dosazením do standardní formy objemu. Tomu poli se říká *rotace vektorového pole* $X$. Vidíme, že v třírozměrném prostoru jsou vektorová pole $X$ s vlastností $\omega_X=dF$ pro nějakou funkci $F$ zadána podmínkou $\operatorname{rot}X=0$. Opět jim říkáme potenciálová pole.

### 3. Diferenciální rovnice

V této části se vrátíme k (vektorovým) funkcím jedné proměnné, které ale budeme zadávat a zkoumat pomocí jejich okamžitých změn. V závěru se pak také zastavíme u případu rovnic obsahujících parciální derivace.

**8.45. Lineární a nelineární diferenční modely.** Pojem derivace



jsme zavedli, abychom mohli pracovat s okamžitými změnami studovaných veličin. Ze stejných důvodů jsme kdysi v úvodní kapitole zaváděli diference a právě vztahy mezi hodnotami veličin a změnami těch samých nebo jiných veličin vedly k tzv. diferenčním rovnicím. Jako motivační úvod k rovnicím obsahujícím derivace neznámých funkcí se k diferenčním rovnicím na chvilku vraťme.

Nejjednodušším modelem bylo úročení vkladů nebo půjček (a totéž pro tzv. Malthusiánský model populace). Přírůstek byl úměrný hodnotě, viz 1.10. V rámci spojitého modelování stejný požadavek povede na rovnici vztahující derivaci funkce $y'(t)$ s její

Správný výsledek tak je

$$y = 2 + C\cos x, \quad C \in \mathbb{R}. \qquad \square$$

**8.120.** Nalezněte řešení diferenciální rovnice

$$(1 + \mathrm{e}^x)\, yy' = \mathrm{e}^x$$

splňující počáteční podmínku $y(0) = 1$.

**Řešení.** Jsou-li funkce $f : (a, b) \to \mathbb{R}$ a $g : (c, d) \to \mathbb{R}$ spojité a je-li $g(y) \neq 0$, $y \in (c, d)$, má počáteční úloha

$$y' = f(x)g(y), \quad y(x_0) = y_0$$

právě jedno řešení pro libovolné $x_0 \in (a, b)$, $y_0 \in (c, d)$. Toto řešení je implicitně určeno jako

$$\int_{y_0}^{y(x)} \frac{dt}{g(t)} = \int_{x_0}^{x} f(t)\, dt.$$

V konkrétních příkladech si počínáme tak, že najdeme všechna řešení a pak vybereme to, které vyhovuje počáteční podmínce.

Počítejme

$$\begin{aligned}
\left(1 + \mathrm{e}^x\right) y\, dy/dx &= \mathrm{e}^x, \\
y\, dy &= \frac{\mathrm{e}^x}{1 + \mathrm{e}^x}\, dx, \\
\frac{y^2}{2} &= \ln\left(1 + \mathrm{e}^x\right) + \ln|C|, \quad C \neq 0, \\
\frac{y^2}{2} &= \ln\left(C\left[1 + \mathrm{e}^x\right]\right), \quad C > 0.
\end{aligned}$$

Dosazení $y = 1, x = 0$ poté dává

$$\tfrac{1}{2} = \ln(C \cdot 2), \quad \text{tj.} \quad C = \tfrac{\sqrt{\mathrm{e}}}{2}.$$

Nalezli jsme tak řešení

$$\tfrac{y^2}{2} = \ln\left(\tfrac{\sqrt{\mathrm{e}}}{2}\left[1 + \mathrm{e}^x\right]\right),$$

tj.

$$y = \sqrt{2\ln\left(\tfrac{\sqrt{\mathrm{e}}}{2}\left[1 + \mathrm{e}^x\right]\right)}$$

v okolí bodu $[0, 1]$, kde je $y > 0$. $\square$

**8.121.** Určete řešení diferenciální rovnice

$$y' = \tfrac{y^2+1}{x+1},$$

pro které je $y(0) = 1$.

**Řešení.** Podobně jako v předchozím příkladu dostáváme

$$\begin{aligned}
\frac{dy}{y^2 + 1} &= \frac{dx}{x + 1}, \\
\operatorname{arctg} y &= \ln|x + 1| + C, \quad C \in \mathbb{R}.
\end{aligned}$$

Počáteční podmínka (tedy dosazení $x = 0$ a $y = 1$) dává

$$\operatorname{arctg} 1 = \ln|1| + C, \quad \text{tj.} \quad C = \tfrac{\pi}{4}.$$

Proto řešením zadaného počátečního problému je funkce

$$y(x) = \operatorname{tg}\left(\ln|x + 1| + \tfrac{\pi}{4}\right)$$

hodnotou (tradičně se u takových rovnic explicitně nevypisuje argument neznámé funkce, který je buď znám z kontextu nebo na jeho označení nezáleží)

$$y' = r \cdot y \tag{8.4}$$

s konstantou úměrnosti $r$.

Je snadné uhodnout *řešení* této rovnosti, tj. funkci $y(t)$ po jejímž dosazení bude rovnost identicky splněna,

$$y(t) = C\,\mathrm{e}^{rt}$$

s libovolnou konstantou $C$. Tuto konstantu určíme jednoznačně volbou tzv. *počáteční hodnoty* $y_0 = y(t_0)$ v nějakém bodě $t_0$. Pokud by část růstu v našem modelu byla dána konstantním působením nezávislým na hodnotě $y$ nebo $t$ (jako jsou např. paušální poplatky za vedení účtu nebo přirozený úbytek populace třeba v důsledku porážek na jatkách), mohli bychom použít rovnici s konstantou $s$ na pravé straně

$$y' = r \cdot y + s. \tag{8.5}$$

Zjevně bude řešením této rovnice funkce

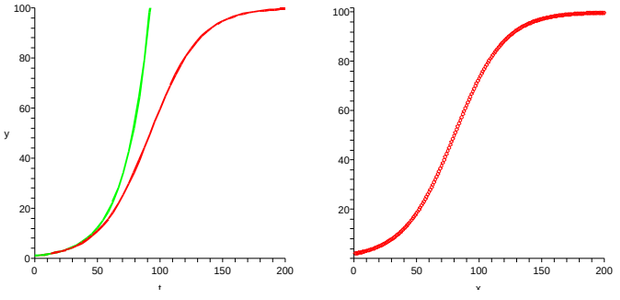
$$y(t) = C\,\mathrm{e}^{rt} - \frac{s}{r}.$$

K tomuto závěru je velice lehké dojít, pokud si uvědomíme, že množinou všech řešení rovnice (8.4) je jednorozměrný vektorový prostor, zatímco řešení rovnice (8.5) se obdrží přičtením kteréhokoliv jednoho jejího řešení ke všem řešením předchozí rovnice. Lze pak snadno najít konstantní řešení $y(t) = k$ pro $k = -\frac{s}{r}$.

Podobně se nám v odstavci 1.13 podařilo vytvořit tzv. logistický model populačního růstu založený na předpokladu, že poměr změny velikosti populace $p(n + 1) - p(n)$ a její velikosti $p(n)$ je v afinní závislosti na samotné velikosti populace. Přitom jsme chtěli, aby se model choval podobně jako Malthusiánský při malých hodnotách populace a vůbec nerostl při dosažení limitní hodnoty $K$. Nyní můžeme tentýž vztah pro spojitý model formulovat pro populaci $p(t)$ závislou na čase $t$ pomocí rovnosti

$$p' = p\left(-\frac{r}{K}p + r\right), \tag{8.6}$$

tj. při hodnotě $p(t) = K$ pro velkou konstantu $K$ je skutečně okamžitý přírůstek funkce $p$ nulový, zatímco pro $p(t)$ blízké nule je poměr rychlosti růstu populace k její velikosti blízký $r$, což bývá malé číslo v řádu setin vyjadřující rychlost růstu populace za dobrých podmínek.




Není jistě snadné vyřešit bez znalostí teorie takovou rovnici (i když právě tento typ rovnic zanedlouho zvládneme), nicméně jako cvičení na derivování lze snadno ověřit, že následující funkce je řešením pro každou konstantu $C$:

$$p(t) = \frac{K}{1 + CK\,\mathrm{e}^{-rt}}.$$

v okolí bodu $[0, 1]$. □

**8.122.** Vyřešte

$$y' = \frac{x + y + 1}{2x + 2y - 1}. \tag{8.8}$$

**Řešení.** Nechť má funkce $f : (a, b) \times (c, d) \to \mathbb{R}$ spojité parciální derivace druhého řádu a $f(x, y) \neq 0$, $x \in (a, b)$, $y \in (c, d)$. Pak lze diferenciální rovnici $y' = f(x, y)$ převést na rovnici se separovanými proměnnými právě tehdy, když

$$\begin{vmatrix} f(x, y) & f'_y(x, y) \\ f'_x(x, y) & f''_{xy}(x, y) \end{vmatrix} = 0, \quad x \in (a, b),\ y \in (c, d).$$

S trochou námahy tak lze dokázat, že diferenciální rovnici ve tvaru $y' = f(ax + by + c)$ můžeme převést na rovnici se separovanými proměnnými, a to pomocí substituce $z = ax + by + c$. Podotkněme, že proměnná $z$ zde nahrazuje $y$.

Položíme tedy $z = x + y$, což dává $z' = 1 + y'$. Dosazením do (‖8.8‖) získáváme

$$\begin{aligned} z' - 1 &= \frac{z + 1}{2z - 1}, \\ \frac{dz}{dx} &= \frac{z + 1}{2z - 1} + 1, \\ \frac{dz}{dx} &= \frac{3z}{2z - 1}, \\ \left(\frac{2}{3} - \frac{1}{3z}\right) dz &= 1\, dx, \\ \frac{2}{3} z - \frac{1}{3} \ln|z| &= x + C, \quad C \in \mathbb{R}, \end{aligned}$$

resp.

$$\tfrac{2}{3} z - \tfrac{1}{3} \ln|Cz| = x, \quad C \neq 0.$$

Ještě se musíme vrátit k původní proměnné $y$ v jednom z těchto tvarů. Obecné řešení lze proto zapsat např. jako

$$\tfrac{2}{3} x + \tfrac{2}{3} y - \tfrac{1}{3} \ln|x + y| = x + C, \quad C \in \mathbb{R},$$

tj.

$$x - 2y + \ln|x + y| = C, \quad C \in \mathbb{R}.$$

Zároveň existuje singulární řešení $y = -x$, které vyplývá z omezení $z \neq 0$ výše provedených úprav (kdy jsme dělili hodnotou $3z$). □

**8.123.** Vyřešte diferenciální rovnici

$$xy' + y \ln x = y \ln y.$$

**Řešení.** Pomocí substituce $u = y/x$ lze každou homogenní diferenciální rovnici $y' = f(y/x)$ převést na rovnici (se separovanými proměnnými)

$$u' = \tfrac{1}{x} (f(u) - u), \quad \text{tj.} \quad u'x + u = f(u).$$

Srovnáním grafu této funkce s volbou $K = 100$, $r = 0,05$ a $C = 1$ na levém obrázku (první dvě jsme takto použili v 1.13, poslední odpovídá přibližně počáteční hodnotě $p(0) = 1$) s pravým obrázkem (řešení diferenční rovnice z 1.13 s týmiž hodnotami parametrů) vidíme, že skutečně oba přístupy k modelování populací dávají docela podobné výsledky. Pro srovnání výstupu je také do levého obrázku vkreslen graf řešení rovnice (8.4) s touž konstantou $r$ a počáteční podmínkou.

**8.46. Diferenciální rovnice prvního řádu.** Obecně rozumíme



(obyčejnou) diferenciální rovnicí prvního řádu vztah mezi derivací funkce $y'(t)$ v proměnné $t$, její hodnotou $y(t)$ a samotnou proměnnou, který lze zapsat s pomocí nějaké reálné funkce $F : \mathbb{R}^3 \to \mathbb{R}$ jako rovnost

$$F(y', y, t) = 0.$$

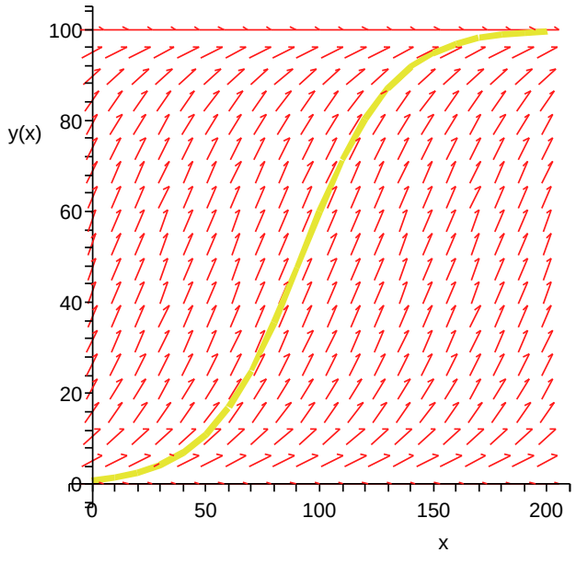
Zápis připomíná implicitně zadané funkce $y(t)$, nicméně navíc je tu závislost na derivaci hledané funkce $y(t)$. Znovu si povšimněme konvence, že při výskytu $t$ považujeme tuto proměnnou za nezávislou proměnnou hledané funkce $y(t)$ a nikoliv volný parametr problému.

Pokud je rovnice alespoň explicitně vyřešena vzhledem k derivaci, tj.

$$y' = f(t, y)$$

pro nějakou funkci $f : \mathbb{R}^2 \to \mathbb{R}$, můžeme si dobře graficky představit, co taková rovnice zadává. Pro každou hodnotu $(t, y)$ v rovině si totiž můžeme představit šipku udávající vektor $(1, f(t, y))$, tj. rychlost se kterou se nám bod grafu řešení bude pohybovat rovinou v závislosti na volném parametru $t$.

Např. pro rovnici (8.6) dostaneme takovýto obrázek (i s vyneseným řešením pro počáteční hodnotu jako výše).




Intuitivně lze na základě takových obrázků očekávat, že pro každou počáteční podmínku bude existovat právě jedno řešení naší rovnice. Jak ale uvidíme, takové tvrzení platí jen pro dostatečně hladké funkce $f$.

Název této diferenciální rovnice je založen na následující definici. Funkce dvou proměnných $f$ se nazývá homogenní $k$-tého stupně, jestliže je $f(tx, ty) = t^k f(x, y)$. Diferenciální rovnice ve tvaru

$$P(x, y)\,dx + Q(x, y)\,dy = 0$$

je totiž homogenní diferenciální rovnicí, právě když jsou funkce $P$ a $Q$ homogenní stejného stupně $k$.

Např. takto můžeme odhalit, že zadaná rovnice

$$x\,dy + (y \ln x - y \ln y)\,dx = 0$$

je homogenní. Samozřejmě není obtížné ji hned rozřešit vzhledem k derivaci a zapsat ve tvaru

$$y' = \tfrac{y}{x} \ln \tfrac{y}{x}.$$

Substitucí $u = y/x$ počítáme

$$\begin{aligned} u'x + u &= u \ln u, \\ \frac{du}{dx}\,x &= u\,(\ln u - 1), \\ \frac{du}{u\,(\ln u - 1)} &= \frac{dx}{x}, \end{aligned}$$

přičemž $u\,(\ln u - 1) \neq 0$. Pomůžeme-li si další substitucí $t = \ln u - 1$, snadno integrujeme

$$\begin{aligned} \int \frac{du}{u\,(\ln u - 1)} &= \int \frac{dx}{x}, \\ \int \frac{dt}{t} &= \int \frac{dx}{x}, \\ \ln|t| &= \ln|x| + \ln|C|, \quad C \neq 0, \\ \ln|\ln u - 1| &= \ln|Cx|, \quad C \neq 0, \\ \ln u - 1 &= Cx, \quad C \neq 0, \\ \ln \frac{y}{x} &= Cx + 1, \quad C \neq 0, \\ y &= x\mathrm{e}^{Cx+1}, \quad C \neq 0. \end{aligned}$$

Vyloučené případy $u = 0$ a $\ln u = 1$ nevedou na dvě řešení, neboť $u = 0$ implikuje $y = 0$, což nelze do původní rovnice vůbec dosadit. Zato $\ln u = 1$ dává $y/x = \mathrm{e}$ a funkce $y = \mathrm{e}x$ zřejmě řešením je. Proto obecným řešením je

$$y = x\mathrm{e}^{Cx+1}, \quad C \in \mathbb{R}.$$

□

**8.124.** Vypočtěte

$$y' = -\tfrac{4x+3y+1}{3x+2y+1}.$$

**Řešení.** Obecně platí, že jsme schopni vyřešit každou rovnici typu

$$y' = f\left(\frac{ax + by + c}{Ax + By + C}\right). \tag{8.9}$$

**8.47. Integrace diferenciálních rovnic.** Ještě než se pustíme do zkoumání existence řešení diferenciálních rovnic, ukážeme si aspoň jednu úplně elementární metodu řešení. Převádí řešení na obyčejné integrování a zpravidla pak pro řešení obdržíme implicitní popis.



ROVNICE SE SEPAROVANÝMI PROMĚNNÝMI

Uvažujme diferenciální rovnici ve tvaru

$$y' = f(t) \cdot g(y) \tag{8.7}$$

pro dvě spojité funkce jedné reálné proměnné $f$ a $g$, $g(y) \neq 0$.

Řešení této rovnice lze získat integrací, tj. nalezením primitivních funkcí

$$G(y) = \int \frac{dy}{g(y)}, \quad F(t) = \int f(t)\,dt.$$

Postup spolehlivě najde řešení splňující $g(y(t)) \neq 0$.

Pak totiž spočtením funkce $y(x)$ z implicitně zadaného vztahu $F(t) + C = G(y)$ s libovolnou konstantou $C$ vede k řešení, protože derivováním této rovnosti s použitím pravidla pro derivování složené funkce $G(y(t))$ dostaneme skutečně $\frac{1}{g(y)} \cdot y'(t) = f(t)$.

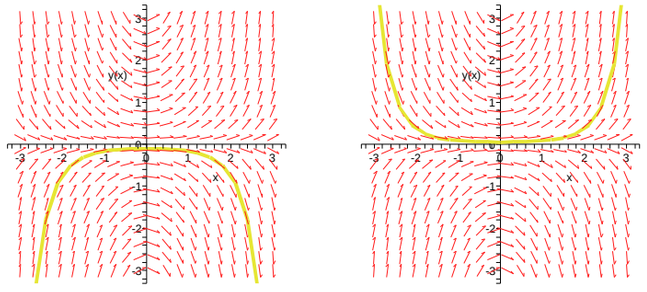
Jako příklad najděme řešení rovnice

$$y' = x \cdot y.$$

Přímým výpočtem dostaneme $\ln|y(x)| = \frac{1}{2}x^2 + C$. Odtud to vypadá (alespoň pro kladná $y$) na

$$y(x) = \mathrm{e}^{\frac{1}{2}x^2+C} = D \cdot \mathrm{e}^{\frac{1}{2}x^2},$$

kde $D$ je nyní libovolná kladná konstanta. Zastavme se ale pozorněji u výsledné formule a znamének. Konstantní řešení $y(x) = 0$ vyhovuje naší rovnici také a pro záporná $y$ můžeme použít stejné řešení s zápornými konstantami $D$. Ve skutečnosti může být konstanta $D$ jakákoliv a našli jsme řešení vyhovující jakékoliv počáteční hodnotě.




Na obrázku jsou vynesena dvě řešení, která ukazují na nestabilitu rovnice vůči počátečním podmínkám: Jestliže pro libovolné $x_0$ změníme malinké $y_0$ z negativní na pozitivní hodnotu, pak se nám dramaticky mění chování výsledného řešení. Navíc si povšimněme konstantního řešení $y(x) = 0$, které odpovídá počáteční podmínce $y(x_0) = 0$.

Pomocí separací proměnných umíme snadno vyřešit nelineární rovnici z předchozího odstavce, která popisovala logistický model populace. Zkuste si jako cvičení.

Pokud má soustava lineárních rovnic

$$ax + by + c = 0, \quad Ax + By + C = 0 \tag{8.10}$$

právě jedno řešení $x_0, y_0$, pak pomocí substitucí $u = x - x_0$, $v = y - y_0$ převedeme rovnici (‖8.9‖) na homogenní rovnici

$$\frac{dv}{du} = f\left(\frac{au+bv}{Au+Bv}\right).$$

Pokud soustava (‖8.10‖) nemá řešení, příp. jich má nekonečně mnoho, lze rovnici (‖8.9‖) převést substitucí $z = ax + by$ na rovnici se separovanými proměnnými (často se v těchto případech již jedná o rovnici se separovanými proměnnými).

V tomto příkladu má příslušná soustava rovnic

$$4x + 3y + 1 = 0, \quad 3x + 2y + 1 = 0$$

právě jedno řešení $x_0 = -1$, $y_0 = 1$. Substitucí $u = x + 1$, $v = y - 1$ obdržíme homogenní rovnici

$$\frac{dv}{du} = -\frac{4u+3v}{3u+2v},$$

kterou řešíme další substitucí $z = v/u$. Získáváme

$$\begin{aligned} z'u + z &= -\frac{4+3z}{3+2z}, \\ \frac{dz}{du}\,u &= -\frac{2z^2+6z+4}{3+2z}, \\ \frac{2z+3}{2z^2+6z+4}\,dz &= -\frac{du}{u} \end{aligned}$$

za předpokladu, že $z^2 + 3z + 2 \neq 0$. Integrováním přecházíme ke

$$\begin{aligned} \frac{1}{2}\ln\left|z^2+3z+2\right| &= -\ln|u| + \ln|C|, \quad C \neq 0, \\ \frac{1}{2}\ln\left|\left(z^2+3z+2\right)u^2\right| &= \ln|C|, \quad C \neq 0, \\ \ln\left|\left(z^2+3z+2\right)u^2\right| &= \ln C^2, \quad C \neq 0, \\ \left(z^2+3z+2\right)u^2 &= \pm C^2, \quad C \neq 0. \end{aligned}$$

Při přeznačení tak máme

$$\left(z^2+3z+2\right)u^2 = D, \quad D \neq 0$$

a přechodem k původním proměnným dále

$$\begin{aligned} \left(\frac{v^2}{u^2} + 3\frac{v}{u} + 2\right)u^2 &= D, \quad D \neq 0, \\ v^2 + 3vu + 2u^2 &= D, \quad D \neq 0, \\ (y-1)^2 + 3(y-1)(x+1) + 2(x+1)^2 &= D, \quad D \neq 0. \end{aligned}$$

Jednoduchými úpravami vyjádříme obecné řešení jako

$$(x + y)\,(2x + y + 1) = D, \quad D \neq 0.$$

Vraťme se k podmínce $z^2 + 3z + 2 \neq 0$. Z $z^2 + 3z + 2 = 0$ plyne $z = -1$ nebo $z = -2$, tj. $v = -u$ nebo $v = -2u$. Pro $v = -u$ je $x = u - 1$ a $y = v + 1 = -u + 1$, což znamená, že $y = -x$. Podobně pro $v = -2u$ je $y = -2u + 1$, a tedy $y = -2x - 1$. Obě funkce



V první kapitole jsme se obzvlášť pečlivě věnovali tzv. lineárním diferenčním rovnicím a jejich docela ošklivě vypadající obecné řešení jsme spočetli v odstavci 1.10 na straně 15. Přestože tedy bylo předem jasné, že půjde o jednorozměrný afinní prostor vyhovujících posloupností, šlo zdánlivě o velmi nepřehlednou sumu, protože bylo třeba zohlednit všechny měnící se koeficienty.

Lze snad tedy odtud čerpat inspiraci k následující konstrukci řešení obecné lineární rovnice prvního řádu

$$y' = a(t)y + b(t) \tag{8.8}$$

se spojitými koeficienty $a(t)$ a $b(t)$.

Nejprve najděme řešení homogenizované rovnice $y'(t) = a(t)y(t)$. To snadno spočteme pomocí separace proměnných a dostáváme

$$y(t) = y_0 F(t, t_0), \quad F(t, s) = \mathrm{e}^{\int_s^t a(x)\,dx}.$$

V případě diferenčních rovnic jsme „uhádli“ řešení a pak jsme indukcí dokázali, že je správně. Tady to je ještě jednodušší, stačí správné řešení zderivovat a tvrzení bude ověřeno.

Řešení lineární rovnice prvního řádu

Řešení rovnice (8.8) s počátečními podmínkami $y(t_0) = y_0$ je na intervalech spojitosti koeficientů $a(t)$, $b(t)$ dáno vztahem

$$y(t) = y_0 F(t, t_0) + \int_{t_0}^{t} F(t, s)b(s)\,ds,$$

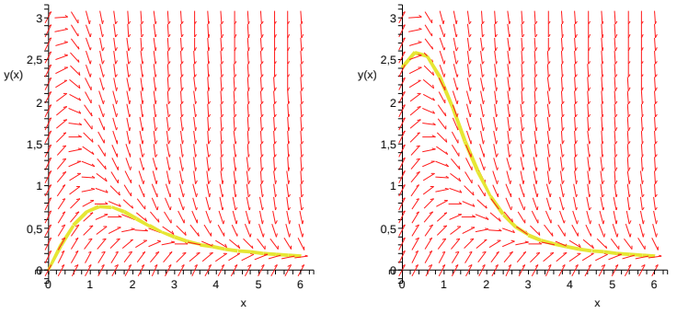
kde $F(t, s) = \mathrm{e}^{\int_s^t a(x)\,dx}$.

Ověřte si správnost řešení sami (pozor na derivaci integrálu, kde je $t$ jak v horní mezi, tak jako volný parametr v integrandu).

Například tedy nyní umíme přímo řešit rovnici

$$y' = 1 - x \cdot y$$

a narazíme tentokrát na stabilní chování viditelné na následujícím obrázku.






**8.48. Transformace souřadnic.** Sledování našich obrázků snad naznačuje, že diferenciální rovnici je možné vnímat jako geometrický objekt (zobrazené „směrové pole šipek“) a řešení bychom měli umět hledat pomocí vhodně zvolených souřadnic. Vrátíme se k tomuto pohledu později, teď si jen ukážeme tři jednoduché typické triky, jak se jeví z pohledu explicitního zápisu rovnic v souřadnicích.

Začněme tzv. *homogenními rovnicemi* tvaru

$$y' = f\left(\frac{y}{t}\right).$$

$y = -x$, $y = -2x - 1$ však vyhovují původní diferenciální rovnici a lze je navíc zahrnout do obecného řešení volbou $D = 0$. Všechna řešení proto známe z implicitního tvaru

$$(x + y)\,(2x + y + 1) = D, \quad D \in \mathbb{R}.$$

□

**8.125.** Stanovte obecné řešení diferenciální rovnice

$$\left(x^2 + y^2\right) dx - 2xy\, dy = 0.$$

**Řešení.** Pro $y \neq 0$ jednoduchými úpravami dostáváme

$$y' = \frac{x^2+y^2}{2xy} = \frac{1+\left(\frac{y}{x}\right)^2}{2\frac{y}{x}},$$

a tak použitím substituce $u = y/x$ přejdeme k rovnici

$$u'x + u = \frac{1+u^2}{2u}.$$

Pro $u \neq \pm 1$ a $D = -1/C$ máme

$$\begin{aligned}
\frac{du}{dx}\,x &= \frac{1 + u^2 - 2u^2}{2u}, \\
\frac{2u}{1-u^2}\,du &= \frac{dx}{x}, \\
-\ln\left|1-u^2\right| &= \ln|x| + \ln|C|, \quad C \neq 0, \\
\ln\frac{1}{\left|1-u^2\right|} &= \ln|Cx|, \quad C \neq 0, \\
\frac{1}{1-u^2} &= Cx, \quad C \neq 0, \\
1 &= Cx\left(1 - \frac{y^2}{x^2}\right), \quad C \neq 0, \\
-\frac{D}{x} &= 1 - \frac{y^2}{x^2}, \quad D \neq 0, \\
-Dx &= x^2 - y^2, \quad D \neq 0.
\end{aligned}$$

Podmínka $u = \pm 1$ odpovídá $y = \pm x$. Zatímco $y \equiv 0$ řešením není, obě funkce $y = x$, $y = -x$ řešeními jsou a získáváme je volbou $D = 0$. Obecné řešení tedy je

$$y^2 = x^2 + Dx, \quad D \in \mathbb{R}.$$

□

**8.126.** Vyřešte

$$y' = x - \frac{2y}{x^2-1}.$$

**Řešení.** Rovnice v zadání má tvar $y' = a(x)y + b(x)$, tj. jedná se o lineární diferenciální rovnici, která je nehomogenní (funkce $b$ není identicky nulová). Obecné řešení takové rovnice lze získat metodou integračního faktoru (kdy nehomogenní rovnici vynásobíme výrazem $\mathrm{e}^{-\int a(x)\,dx}$) nebo metodou separace proměnných (kdy integrační konstantu získanou při řešení přidružené homogenní rovnice považujeme za funkci v proměnné $x$). Obě tyto metody si objasníme na uvedeném příkladu.

Jestliže uvážíme transformaci $z = \frac{y}{t}$ za předpokladu $t \neq 0$, pak s využitím pravidla pro derivování složené funkce dostáváme

$$z' = \frac{1}{t^2}\left(t\,y' - y\right) = \frac{1}{t}\left(f(z) - z\right),$$

což je rovnice se separovanými proměnnými.

Druhým příkladem budou rovnice tzv. *Bernoulliho typu*, které jsou tvaru

$$y' = f(t)y + g(t)y^r,$$

kde $r \in \mathbb{R}$, $r \neq 0, 1$. Volba transformace $z = y^{1-r}$ vede na rovnici

$$\begin{aligned}
z' &= (1-r)y^{-r}\left(f(t)y + g(t)y^r\right) \\
&= (1-r)f(t)z + (1-r)g(t),
\end{aligned}$$

což je lineární rovnice, kterou už také umíme integrovat.

Nakonec se podívejme na mimořádně významnou nelineární rovnici tzv *Riccatiho typu*. Jde o rozšíření Bernoulliho rovnice s $n = 2$ o absolutní člen

$$y' = f(t)y + g(t)y^2 + h(t).$$

Tuto rovnici umíme také převést na lineární rovnici za předpokladu, že umíme uhodnout jedno partikulární řešení $x(t)$. Pak totiž můžeme použít transformaci

$$z = \frac{1}{y - x}.$$

Pověřte se samostatně, že tato transformace vede na rovnici

$$z' = -\big(f(t) + 2xg(t)\big)z - g(t).$$

Stejně jako jsme viděli u integrace funkcí (což je vlastně nejjednodušší typ rovnic se separovanými proměnnými), zpravidla pro rovnice neexistuje řešení vyjádřitelné explicitně pomocí elementárních funkcí.

Podobně jako u klasických inženýrských tabulek hodnot speciálních funkcí byly také sestaveny knihy přehledů řešených základních rovnic. Dnes je v podstatě všechna v nich ukrytá moudrost převedena do softwarových systémů jako Maple či Mathematica. Tam tedy sice můžeme zadat jakoukoliv úlohu na řešení obyčejných diferenciálních rovnic, v překvapivě velkém množství případů dostaneme výsledky, pro většinu zadání to ale nakonec nebude možné.

Východiskem jsou numerické metody hledající řešení pouze přibližně. Zejména pro ně potřebujeme ale dobrá teoretická východiska ohledně existence, jednoznačnosti a stability řešení.



Začneme tzv. Picardovou–Lindelöfovou větou:

EXISTENCE A JEDNOZNAČNOST ŘEŠENÍ ODR

**8.49. Věta.** *Nechť má funkce $f(t, y) : \mathbb{R}^2 \to \mathbb{R}$ spojité parciální derivace na nějaké otevřené množině $U$. Pak pro každý bod $(t_0, y_0) \in U \supset \mathbb{R}^2$ existuje maximální interval $I = [t_0 - a, t_0 + b]$ s kladnými $a, b \in \mathbb{R}$, a právě jedna funkce $y(t) : I \to \mathbb{R}$, která na intervalu $I$ vyhovuje rovnici*

$$y' = f(t, y).$$

V rámci metody integračního faktoru násobíme původní rovnici výrazem

$$\mathrm{e}^{\int \frac{2}{x^2-1}\,\mathrm{d}x} = \mathrm{e}^{\ln\left|\frac{x-1}{x+1}\right|} = \frac{x-1}{x+1},$$

kde příslušným integrálem rozumíme libovolně zvolenou primitivní funkci a kde lze uvažovat libovolný nenulový násobek získané funkce (a proto jsme také mohli odstranit absolutní hodnotu). Uvažujeme tedy rovnici

$$y'\,\tfrac{x-1}{x+1} + \tfrac{2y}{(x+1)^2} = \tfrac{x(x-1)}{x+1}.$$

Podstatou metody integračního faktoru je, že na levé straně je derivace výrazu $y\frac{x-1}{x+1}$. Integrováním snadno obdržíme

$$y\tfrac{x-1}{x+1} = \int \tfrac{x(x-1)}{x+1}\,dx = \tfrac{x^2}{2} - 2x + 2\ln|x+1| + C, \quad C \in \mathbb{R}.$$

Řešeními jsou tak funkce

$$y = \tfrac{x+1}{x-1}\left(\tfrac{x^2}{2} - 2x + 2\ln|x+1| + C\right), \quad C \in \mathbb{R}.$$

Při metodě variace konstant nejprve vyřešíme přidruženou homogenní rovnici

$$y' = -\tfrac{2y}{x^2-1},$$

což je rovnice se separovanými proměnnými. Platí

$$\begin{aligned}
\frac{dy}{dx} &= -\frac{2y}{x^2-1},\\
\frac{dy}{y} &= -\frac{2}{x^2-1}\,dx,\\
\ln|y| &= -\ln|x-1| + \ln|x+1| + \ln|C|, \quad C \neq 0,\\
\ln|y| &= \ln\left|C\,\frac{x+1}{x-1}\right|, \quad C \neq 0,\\
y &= C\,\frac{x+1}{x-1}, \quad C \neq 0,
\end{aligned}$$

kde jsme museli vyloučit případ $y = 0$. Funkce $y \equiv 0$ je však řešením homogenní lineární diferenciální rovnici vždy a můžeme ji zahrnout do obecného řešení. Obecným řešením přidružené homogenní rovnice tudíž je

$$y = \tfrac{C(x+1)}{x-1}, \quad C \in \mathbb{R}.$$

Na konstantu $C$ nahlížejme dále jako na funkci $C(x)$. Derivujme

$$y' = \tfrac{C'(x)\,(x+1)(x-1)+C(x)\,(x-1)-C(x)\,(x+1)}{(x-1)^2}$$

a následně dosaďme do původní rovnice

$$\tfrac{C'(x)\,(x+1)(x-1)+C(x)\,(x-1)-C(x)\,(x+1)}{(x-1)^2} = x - \tfrac{2\,C(x)\,(x+1)}{(x-1)(x^2-1)}.$$

Po úpravě dostáváme

$$C'(x) = \tfrac{x(x-1)}{x+1},$$

Důkaz. Všimněme si, že jestliže je funkce $y(t)$ řešením naší rovnice splňující počáteční podmínku $y(t_0) = t_0$, pak také splňuje rovnost

$$y(t) = y_0 + \int_{t_0}^{t} y'(s)\,ds = y_0 + \int_{t_0}^{t} f(s, y(s))\,ds.$$

Pravá strana tohoto výrazu je ovšem, až na konstantu, integrální operátor

$$L(y)(t) = y_0 + \int_{t_0}^{t} f(s, y(s))\,ds.$$

Při řešení naší diferenciální rovnice prvního řádu tedy vlastně hledáme pevný bod pro tento operátor $L$, tj. chceme najít funkci $y = y(t)$ s $L(y) = y$.

Naopak, jestliže je riemannovsky integrovatelná funkce $y(t)$ pevným bodem operátoru $L(y)$, pak z věty o primitivní funkci okamžitě vidíme, že skutečně $y(t)$ vyhovuje zadané diferenciální rovnici, včetně počátečních podmínek.



Pro operátor $L$ můžeme docela lehce odhadnout, jak se liší jeho hodnoty $L(y)$ a $L(z)$ pro různé argumenty $y(t)$ a $z(t)$. Skutečně, díky spojitosti parciálních derivací funkce $f$ víme, že je $f$ lokálně lipschitzovská. To znamená, že máme k dispozici odhad

$$|f(t, y) - f(t, z)| \leq C|y - z|,$$

s konstantou $C$, jestliže omezíme hodnoty $(t, y)$ na okolí bodu $(t_0, y_0)$ s kompaktním uzávěrem. Zvolíme $\varepsilon > 0$ a omezíme se na $t$ v nějakém intervalu $J = [t_0 - a_0, t_0 + b_0]$ tak, aby $J \times [y_0 - \varepsilon, y_0 + \varepsilon] \subset U$, a omezíme se na funkce $y(t)$ a $z(t)$, které budou pro $t \in J$ splňovat

$$\max_{t\in J} |y(t) - y_0| < \varepsilon, \ \max_{t\in J} |z(t) - y_0| < \varepsilon.$$

Nyní dostáváme odhad

$$\begin{aligned}
|(L(y) - L(z))(t)| &= \left|\int_{t_0}^{t} f(s, y(s)) - f(s, z(s))\,ds\right|\\
&\leq \int_{t_0}^{t} |f(s, y(s)) - f(s, z(s))|\,ds\\
&\leq C\int_{t_0}^{t} |y(s) - z(s)|\,ds\\
&\leq D|t - t_0|
\end{aligned}$$

pro vhodné konstanty $C$ a $D$. Pro $\delta > 0$ dostatečně malé proto bude platit

$$\max_{|t-t_0|<\delta} |L(y)(t) - L(z)(t)| \leq \max_{|t-t_0|<\delta} c\,|y(t) - z(t)|$$

s nějakou konstantou $0 < c < 1$. Takovýmto operátorům jsme v odstavci 7.19 na str. 417 říkali *kontrakce*. V předpokladech Banachovy věty o kontrakci zajišťující jednoznačně určený pevný bod ale potřebujeme ještě úplnost prostoru $X$ funkcí, na nichž operátor $L$ operuje.



V našem případě si můžeme povšimnout, že již ze spojitosti zobrazení $f(t, y)$ vyplývá stejnoměrný odhad pro všechny výše uvažované funkce $y(t)$ a hodnoty $t > s$ v jejich definičním oboru:

$$|L(y)(t) - L(y)(s)| \leq \int_{s}^{t} |f(r, y(r)|dr \leq D\,|t - s|$$

tj.

$$C(x) = \int \frac{x(x-1)}{x+1}\,dx,$$

$$C(x) = \frac{x^2}{2} - 2x + 2\ln|x+1| + C, \quad C \in \mathbb{R}.$$

Nyní již stačí dosadit

$$y = C(x)\,\tfrac{x+1}{x-1} = \tfrac{x+1}{x-1}\left(\tfrac{x^2}{2} - 2x + 2\ln|x+1| + C\right), \quad C \in \mathbb{R}.$$

Vidíme, že jsme obdrželi výsledek ve stejném tvaru jako v prvním případě. To by nemělo být překvapivé už z toho důvodu, že rozdíly mezi těmito metodami jsou nevýznamné a že se při nich počítají totožné integrály.

Na závěr si všimněme, že řešení $y$ rovnice $y' = a(x)y$ lze stejným způsobem určit pro libovolnou spojitou funkci $a$. Vždy tedy je

$$y = C\mathrm{e}^{\int a(x)\,dx}, \quad C \in \mathbb{R}.$$

Podobně řešení rovnice $y' = a(x)y + b(x)$ doplněné počáteční podmínkou $y(x_0) = y_0$ lze při spojitosti koeficientů (funkcí $a, b$) explicitně určit jako

$$y = \mathrm{e}^{\int_{x_0}^{x} a(t)\,dt}\left(y_0 + \int_{x_0}^{x} b(t)\,\mathrm{e}^{-\int_{x_0}^{t} a(s)\,ds}\,\mathrm{d}t\right).$$

Ještě dodejme, že lineární rovnice nemá žádná singulární řešení a v obecném řešení vystupuje $C \in \mathbb{R}$. □

**8.127.** Vypočtěte lineární rovnici

$$\left(y' + 2xy\right)\mathrm{e}^{x^2} = \cos x.$$

**Řešení.** Kdybychom postupovali podle metody integračního faktoru, pouze bychom triviálně přepisovali zadání. Uvedený tvar diferenciální rovnice má totiž požadovanou vlastnost – na levé straně je derivace výrazu $y\,\mathrm{e}^{x^2}$. Můžeme proto ihned spočítat

$$\left(y\,\mathrm{e}^{x^2}\right)' = \cos x,$$

$$y\,\mathrm{e}^{x^2} = \int \cos x\,dx,$$

$$y\,\mathrm{e}^{x^2} = \sin x + C, \quad C \in \mathbb{R},$$

$$y = \mathrm{e}^{-x^2}(\sin x + C), \quad C \in \mathbb{R}.$$

□

**8.128.** Stanovte všechna nenulová řešení Bernoulliho rovnice

$$y' - \tfrac{y}{x} = 3xy^2.$$

**Řešení.** Bernoulliho rovnice

$$y' = a(x)y + b(x)y^r, \quad r \neq 0,\ r \neq 1,\ r \in \mathbb{R}$$

se řeší po vydělení členem $y^r$ substitucí $u = y^{1-r}$, která vede na lineární diferenciální rovnici

$$u' = (1-r)\left[a(x)u + b(x)\right].$$

s univerzální konstantou $D > 0$. Můžeme se tedy kromě výše uvedených podmínek ještě omezit na podmnožinu všech stejnoměrně spojitých funkcí. Ta je ale již kompaktní a tedy úplnou množinou spojitých funkcí na našem intervalu, viz Arzelova–Ascoliho věta 7.23, a proto existuje jednoznačně daný pevný bod $y(t)$ této kontrakce $L$, který je řešením naší rovnice.

Zbývá ukázat existenci maximálního intervalu $I = [t_0 - a, t_0 + b]$. Předpokládejme, že máme nalezeno řešení $y(t)$ na intervalu $(t_0, t_1)$ a zároveň existuje konečná limita

$$y_1 = \lim_{t \to t_1} y(t).$$

Pak ale podle výše dokázaného musí existovat řešení s počáteční podmínkou $(t_1, y_1)$, na nějakém okolí bodu $t_1$ a přitom nalevo od něj musí splývat s řešením $y(t)$. Jistě tedy jde řešení $y(t)$ prodloužit napravo od $t_1$. Existují tedy pouze dvě možnosti, kdy řešení napravo od $t_1$ neexistuje: buď neexistuje konečná limita $y(t)$ v bodě $t_1$ zleva nebo sice limita $y_1$ existuje, ale bod $(t_1, y_1)$ je na hranici definičního oboru $U$ funkce $f$. V obou případech jde skutečně o maximální prodloužení řešení napravo od $t_0$.

Obdobně argumentujeme pro maximální řešení nalevo od $t_0$. □

**8.50. Iterativní aproximace řešení.** Postup v důkazu předchozí



věty lze přeformulovat do iterativní procedury, která poskytuje přibližná řešení pomocí postupné integrace. Pomocí konkrétního odhadu pro konstantu $c$ z důkazu můžeme dostat i přímé odhady chyb. Zkuste si sami promyslet jako cvičení (viz postup v důkazu Banachovy věty o pevném bodu v odstavci 7.19). Lze pak i vcelku snadno přímo ukázat, že jde o stejnoměrně konvergentní posloupnost spojitých funkcí a tedy bude i limitou spojitá funkce (aniž bychom se dovolávali na složité věty ze sedmé kapitoly).

PICARDOVY APROXIMACE

Jednoznačné řešení rovnice

$$y' = f(t, y),$$

jejíž pravá strana $f$ má spojité parciální derivace, můžeme na dostatečně malém intervalu vyjádřit jako limitu postupných iterací začínajících konstantní funkcí (tzv. *Picardova aproximace*):

$$y_0(t) = y_0, \quad y_{n+1}(t) = L(y_n),\ n \in \mathbb{N}.$$

Jde o stejnoměrně konvergující posloupnost spojitých funkcí se spojitou limitou $y(t)$.

Všimněme si, že jsme ve skutečnosti potřebovali jen lipschitzovskost parciálních derivací funkce $f$, věta tedy platí i s tímto slabším předpokladem. Ukážeme v dalším odstavci, že pouhá spojitost funkce $f$ již zajišťuje existenci řešení také, na jednoznačnost však nestačí.

**8.51. Nejednoznačnost řešení.** Začněme úplně jednoduchým příkladem. Uvažme rovnici

$$y' = \sqrt{|y|}.$$

Snadno lze najít řešení pomocí separace proměnných

$$y(t) = \frac{1}{4}(t + C)^2,$$

pro kladná $y$, s libovolnou konstantou $C$ a $t + C > 0$. Pro počáteční hodnoty $(t_0, y_0)$ s $y_0 \neq 0$ jde přitom o zadání vyhovující předchozí

V tomto konkrétním příkladu substituce $u = y^{1-2} = 1/y$ dává

$$u' + \tfrac{u}{x} = -3x.$$

Stejně jako v minulém příkladu počítáme

$$u = \mathrm{e}^{-\ln|x|}\left[\int -3x\,\mathrm{e}^{\ln|x|}\,dx\right],$$

kde $\ln|x|$ jsme obdrželi jako (libovolně zvolenou) primitivní funkci k $1/x$. Dále je

$$u = \mathrm{e}^{\ln\frac{1}{|x|}}\left[\int -3x\,\mathrm{e}^{\ln|x|}\,dx\right],$$

$$u = \frac{1}{|x|}\left[\int -3x\,|x|\,dx\right].$$

Absolutní hodnotu lze nahradit za znaménko, které lze vytknout a pokrátit, tj. stačí uvažovat

$$u = \tfrac{1}{x}\left[\int -3x^2\,dx\right] = \tfrac{1}{x}\left[-x^3 + C\right], \quad C \in \mathbb{R}.$$

Návratem k původní proměnné dostaneme

$$y = \tfrac{1}{u} = \tfrac{x}{C-x^3}, \quad C \in \mathbb{R}.$$

Úpravami vyloučený případ $y \equiv 0$ je singulárním řešením (což samozřejmě platí pro každou Bernoulliho rovnici s kladným $r$). □

**8.129.** Záměnou proměnných řešte rovnici

$$y\,dx - \left(x + y^2 \sin y\right)\,dy = 0.$$

**Řešení.** Je-li proměnná $x$ ve vyjádření diferenciální rovnice prvního řádu pouze v první mocnině a $y$ se vyskytuje v argumentu elementárních funkcí, je možné aplikovat tzv. metodu záměny proměnných, kdy hledáme řešení jako funkci $x$ nezávislé proměnné $y$.

Nejprve rozřešíme diferenciální rovnici vzhledem k derivaci, tj. vyjádříme

$$y' = \tfrac{y}{x+y^2\sin y}.$$

Tato rovnice není žádného z předchozích typů, a proto využijeme úpravy

$$\frac{dy}{dx} = \frac{y}{x + y^2\sin y},$$

$$\frac{dx}{dy} = \left(\frac{y}{x + y^2\sin y}\right)^{-1} = \frac{x}{y} + y\sin y,$$

$$x' = \frac{1}{y}\,x + y\sin y.$$

Tím jsme přešli k lineární diferenciální rovnici. Snadno pak dopočítáme její obecné řešení

$$x = -y\cos y + Cy, \quad C \in \mathbb{R}.$$

□

větě, a proto bude lokálně existovat řešení právě jedno. Zjevně musí být řešení stále neklesající, proto pro záporné hodnoty $y_0$ dostaneme stejné řešení, jen s opačným znaménkem a $t + C < 0$.

Pro počáteční podmínku $(t_0, y_0) = (t_0, 0)$ ovšem máme kromě na sebe navazující řešení nalevo a napravo od $t_0$, které jsme už našli, ještě identicky nulové řešení $y(t) = 0$. Můžeme tedy tyto dvě větve nalevo a napravo navazovat libovolně, viz obrázek. Nicméně existenci nějakého řešení garantuje následující věta, které se říkává Peanova věta o existenci řešení:

**Věta.** *Uvažme funkci $f : \mathbb{R}^2 \to \mathbb{R}$ spojitou na nějaké otevřené množině $U$. Pak pro každý bod $(t_0, y_0) \in U \subset \mathbb{R}^2$ existuje spojité řešení rovnice*

$$y' = f(t, y)$$

*lokálně na nějakém okolí bodu $t_0$.*

Důkaz. Důkaz uvedeme jen stručně a necháváme na čtenáři doplnění řady detailů. Místo Picardových aproximací budeme postupovat zdánlivě zcela naivně.



Budeme konstruovat řešení napravo od počátečního bodu $t_0$. Zvolíme si za tím účelem malý krok $h > 0$ a označíme si body

$$t_k = t_0 + kh, \quad k = 1, 2, \ldots.$$

V počátečním bodě $(t_0, y_0)$ máme definovánu hodnotu derivace $f(t_0, y_0)$ příslušné křivky řešení $(t, y(t))$, můžeme tedy přibližně nahradit parametrizovanou přímkou s touže derivací:

$$y^{(0)}(t) = y_0 + f(t_0, y_0)(t - t_0)$$

a označíme si $y_1 = y^{(0)}(t_1)$. Induktivně takto sestrojíme funkce a body

$$y^{(k)}(t) = y_k + f(x_k, y_k)(t - t_k), \quad y_{k+1} = y^{(k)}(t_{k+1}).$$

Nyní si definujeme $y_h(t)$ pomocí slepení jednotlivých lineárních částí, tj.

$$y_h(t) = y^{(k)}(t) \quad \text{pro všechna } t \in [kh, (k+1)h].$$

To je evidentně spojitá funkce, které říkáme *Eulerova aproximace* řešení.

Nyní zbývá již „jen“ dokázat, že existuje limita funkcí $y_h$ pro $h$ jdoucí k nule a že je řešením.



K tomu je třeba si povšimnout (jak jsme již učinili v důkazu věty o jednoznačnosti a existenci řešení), že díky stejnoměrné spojitosti $f(t, y)$ na okolí $U$, na kterém hledáme řešení, máme k dispozici pro každé předem zvolené $\varepsilon > 0$ takové $\delta$, že

$$|f(t, y) - f(s, z)| < \varepsilon,$$

kdykoliv bude $\|(t - s, y - z)\| < \delta$.

Zejména tedy budou všechny naše funkce $y_h$ v množině stejnoměrně spojitých funkcí na našem dotčeném intervalu. Proto podle Arzelovy–Ascoliho věty (viz odstavec 7.23 na straně 419) bude existovat posloupnost hodnot $h_n \to 0$ taková, že příslušná posloupnost funkcí $y_{h_n}$ bude stejnoměrně konvergovat ke spojité funkci $y$. Pišme dále jednodušeji $y_n(t) = y_{h_n}(t) \to y(t)$.

Pro každou ze spojitých funkcí $y_h$ ovšem máme jen konečně mnoho bodů v intervalu $[t_0, t]$, kde není diferencovatelná a

Další příklady na diferenciálních rovnic 1. řádu najdete na straně 513.

### L. Slovní úlohy vedoucí na diferenciální rovnice

**8.130.** Rychlost, kterou se rozpadá daný izotop daného prvku, je přímo úměrná množství daného izotopu. Poločas rozpadu izotopu Plutonia, $^{239}$Pu, je 24 100 let. Za jak dlouho ubude setina z nukleární pumy, jejíž aktivní složkou je zmiňovaný izotop?

**Řešení.** Označíme-li množství Plutonia jako $m$, tak pro rychlost rozkladu můžeme napsat diferenciální rovnici

$$\frac{dm}{dt} = -k \cdot m,$$

kde $k$ je nějaká neznámá konstanta. Řešením je tedy funkce $m(t) = m_0 e^{-kt}$. Dosazením do rovnice pro poločas rozpadu ($e^{-kt} = \frac{1}{2}$) získáme konstantu $k \doteq -2,88 \cdot 10^5$. Hledaný čas je přibližně 349 let. □

**8.131.** Čistička vody o objemu 2000 m$^3$ byla znečištěna olovem, které se nachází ve vodě v ní v množství 10 g/m$^3$. Do čističky přitéká čistá voda rychlostí 2 m$^3$/s a stejnou rychlostí i vytéká. Za jak dlouho poklesne obsah olova ve vodě v čističce pod 10 $\mu$g/m$^3$ (což je hygienická norma pro obsah olova v pitné vodě podle směrnice Evropského společenství), předpokládáme-li, že voda je neustále rovnoměrně promíchávána?

**Řešení.** Označme objem vody v nádrži jako $V$ (m$^3$), rychlost vytékání vody jako $v$ (m$^3$/s), konečně nechť $m$ je hmotnost vody v nádrži v gramech. Za infinitesimální (nekonečně malou) časovou jednotku d$t$ vyteče z nádrže $\frac{m}{V} \cdot v\,\mathrm{d}t$ gramů olova, pro změnu hmotnosti množství olova v čističce tedy můžeme sestavit diferenciální rovnici

$$\mathrm{d}m = -\frac{m}{V} \cdot v\,\mathrm{d}t.$$

Separací proměnných dostáváme rovnici

$$\frac{\mathrm{d}m}{m} = -\frac{v}{V}\,\mathrm{d}t,$$

integrací obou stran rovnice a odlogaritmováním dostaneme řešení ve tvaru $m(t) = m_0 e^{-\frac{v}{V}t}$, kde $m_0$ je množství olova v nádrži v čase $t = 0$. Po dosazení číselných hodnot zjistíme, že $t \doteq 6\,\mathrm{h}\ 35\,\mathrm{min}$. □

**8.132.** Rychlost šíření zprávy v populaci o $P$ lidech je přímo úměrná počtu lidí, kteří zprávu ještě neslyšeli. Určete funkci $f$ popisující počet lidí v čase, kteří již zprávu slyšeli. Je vhodné tento model šíření zprávy používat pro malá nebo velká $P$?

můžeme tedy psát

$$y_n(t) = y_0 + \int_{t_0}^{t} y_n'(s)\,ds.$$

Ale derivace na jednotlivých intervalech jsou konstantní takže můžeme psát (zde $k$ je největší splňující $t_0 + kh_n \le t$, zatímco $y_j$ a $t_j$ jsou body z definice funkce $y_{h_n}$)

$$y_n(t) = y_0 + \sum_{j=0}^{k-1} \int_{t_j}^{t_{j+1}} f(t_j, y_j)ds \quad + \int_{t_k}^{t} f(t_k, y_k).$$

Rádi bychom místo toho viděli

$$y_n(t) = y_0 + \int_{t_0}^{t} f(s, y_n(s))\,ds,$$

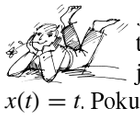
ale rozdíl tohoto integrálu a posledních dvou členů v předchozím výrazu je odhadnut možnými rozdíly hodnot funkce $f(t, y)$ a délkami intervalů. Díky našemu univerzálnímu odhadu pro $f(t, y)$ výše můžeme tedy v limitním procesu $\lim_{n\to\infty} y_n(t)$ místo skutečných hodnot použít právě poslední integrál a dostáváme

$$\begin{aligned} y(t) &= \lim_{n\to\infty} \Big(y_0 + \int_{t_0}^{t} f(s, y_n(s))\,ds\Big) \\ &= y_0 + \int_{t_0}^{t} \big(\lim f(s, y_n(s))\big)\,ds \\ &= y_0 + \int_{t_0}^{t} f(s, y(s))\,ds, \end{aligned}$$

kde jsme pro limitní přechod u integrace využili stejnoměrné konvergence $y_n(t) \to y(t)$.

Tím je věta dokázána. □

**8.52. Systémy rovnic prvního řádu.** Na řešení rovnice $y' = f(x, y)$ lze také pohlížet jako na hledání (parametrizované) křivky $(x(t), y(t))$ v rovině, kde jsme již předem pevně zvolili parametrizaci proměnné $x(t) = t$. Pokud ale akceptujeme tento pohled, pak můžeme jednak zapomenout na tuto pevnou volbu pro jednu proměnnou a hlavně přibrat libovolný počet proměnných.



Například v rovině můžeme psát takový systém ve tvaru

$$x' = f(t, x, y), \quad y' = g(t, x, y)$$

se dvěma funkcemi $f, g : \mathbb{R}^3 \to \mathbb{R}$. Obdobně pro více proměnných.

Jednoduchým příkladem v rovině může sloužit systém rovnic

$$x' = -y, \quad y' = x.$$

Snadno lze uhádnout (nebo aspoň ověřit), že řešením takového systému je např.

$$x(t) = R\cos t, \quad y(t) = R\sin t$$

s libovolnou nezápornou konstantou $R$ a křivky řešení budou právě parametrizované kružnice o poloměru $R$.

V obecném případě budeme pracovat s vektorovým zápisem systému ve tvaru

$$x' = f(t, x)$$

pro vektorovou funkci $x : \mathbb{R} \to \mathbb{R}^n$ a zobrazení $f : \mathbb{R}^{n+1} \to \mathbb{R}^n$. Na takové systémy umíme přímo rozšířit platnost věty o jednoznačnosti a řešení:

**Řešení.** Sestavíme diferenciální rovnici pro $f$. Rychlost šíření zprávy $\frac{df}{dt} = f'(t)$ má být přímo úměrná počtu lidí, kteří o ní ještě neslyšeli, tedy hodnotě $P - f(t)$. Celkem

$$\frac{df}{dt} = k(P - f(t)).$$

Separací proměnných a zavedením konstanty $K$ (počet lidí, kteří znají zprávu v čase $t = 0$ musí být $P - K$) dostáváme řešení

$$f(t) = P - Ke^{-kt},$$

kde $k$ je kladná reálná konstanta.

Tento model má zřejmě smysl jen pro velká $P$. □

**8.133.** Rychlost, kterou se šíří epidemie v dané uzavřené populaci o $P$ lidech, je přímo úměrná součinu počtu lidí, kteří jsou nakaženi, a počtu lidí, kteří jsou ještě nenakaženi. Určete funkci $f(t)$ popisující počet nakažených v čase.

**Řešení.** Jako v předchozím příkladě sestavíme diferenciální rovnici

$$\frac{df}{dt} = k \cdot f(t)\,(P - f(t))\,.$$

Separací proměnných dostáváme

$$f(t) = \frac{K}{1 + Le^{-Kkt}},$$

kde $K$ a $L$ jsou integrační konstanty. □

**8.134.** Změna rychlosti předmětu padajícího v konstantním gravitačním poli v prostředí s jistým odporem je dána vztahem:

$$\frac{dv}{dt} = g - kv,$$

kde $k$ je konstanta udávající odpor prostředí. Byl vypuštěn předmět pohybující se počáteční rychlostí $5\,\mathrm{ms}^{-1}$ v gravitačním poli $g = 10\mathrm{ms}^{-2}$, konstanta odporu prostředí je $k = 0.5\,\mathrm{s}^{-1}$. Jaká bude rychlost předmětu za 3 vteřiny?

**Řešení.**

$$v = \frac{g}{k} - \left(\frac{g}{k} - v_0\right) e^{-kt},$$

po dosazení $v(3) = 20 - 15e^{-\frac{3}{2}}\,\mathrm{ms}^{-1}$. □

**8.135.** Rychlost nárůstu populace odmocninového brouka je nepřímo úměrná její velikosti. V čase $t = 0$ čítala populace 100 brouků. Za měsíc se populace zdvojnásobila. Jak bude populace velká za dva měsíce?

**Řešení.** Uvažujme spojitou aproximaci počtu brouků a označme jejich počet $P$. Pak můžeme sestavit následující rovnici:

$$\frac{dP}{dt} = \frac{k}{P},$$

### Existence a jednoznačnost pro systémy ODR

**Věta.** *Uvažme funkce $f_i : \mathbb{R}^{n+1} \to \mathbb{R}$, $i = 1, \ldots, n$, se spojitými parciálními derivacemi. Pak pro každý bod $(t_0, x_1^0, \ldots, x_n^0) \in \mathbb{R}^{n+1}$ existuje maximální interval $[t_0 - a, t_0 + b]$, s $a, b \in \mathbb{R}$ kladnými, a právě jedna funkce $x(t) = (x_1(t), \ldots, x_n(t)) : \mathbb{R} \to \mathbb{R}^n$, která je řešením systému rovnic*

$$\begin{aligned} x_1' &= f_1(t, x_1, \ldots, x_n) \\ &\vdots \\ x_n' &= f_n(t, x_1, \ldots, x_n) \end{aligned}$$

*s počáteční podmínkou*

$$x_1(t_0) = x_1^0, \ldots, x_n(t_0) = x_n^0.$$

Důkaz. Důkaz je skoro identický s důkazem existence a jednoznačnosti pro jednu rovnici s jednou neznámou funkcí, jak jsme ukázali ve větě 8.49. Neznámá funkce $x(t) = (x_1(t), \ldots, x_n(t))$ je křivkou v $\mathbb{R}^n$ vyhovující zadané rovnici, a proto jsou její komponenty $x_i(t)$ opět vyjádřitelné pomocí integrálů



$$x_i(t) = x_i(t_0) + \int_{t_0}^{t} x_i'(s)\,ds = x_i + \int_{t_0}^{t} f_i(t, x(s))\,ds.$$

Opět tedy pracujeme s integrálním operátorem $y \mapsto L(y)$, tentokrát zobrazujícím křivky v $\mathbb{R}^n$ na křivky $\mathbb{R}^n$ a hledáme jeho pevný bod. Protože je euklidovská vzdálenost dvou bodů v $\mathbb{R}^n$ vždy shora odhadnuta součtem velikostí rozdílů jednotlivých komponent, postupuje se zcela stejně jako v případě 8.49. Je pouze zapotřebí si povšimnout, že velikost vektoru

$$\|f(t, z_1, \ldots, z_n) - f(t, y_1, \ldots, y_n)\|$$

je odhadnuta shora součtem

$$\begin{aligned} &\|f(t, z_1, \ldots, z_n) - f(t, y_1, z_2 \ldots, z_n)\| + \ldots \\ &\qquad + \|f(t, y_1, \ldots, y_{n-1}, z_n) - f(t, y_1, \ldots, y_n)\|. \end{aligned}$$

Doporučujeme podrobně projít a promyslet důkaz Věty 8.49 z tohoto pohledu samostatně. □

Při zavádění a studiu modelů nějakého reálného systému je podstatné tzv. kvalitativní chování řešení v závislosti na počátečních podmínkách a na volných parametrech systému (tj. ať už konstant nebo funkcí).

Jako takový docela jednoduchý příklad systému rovnic prvního řádu zmiňme klasický populační model „dravec – kořist“, který zavedli ve dvacátých létech minulého století Lotka a Volterra.

Označme $x(t)$ vývoj počtu jedinců v populaci kořisti a $y(t)$ totéž pro dravce. Předpokládáme, že přírůstek kořisti by se řídil Malthusiánským modelem (tj. exponenciální růst s koeficientem $\alpha$), kdyby nebyli loveni. U dravce naopak očekáváme, že by bez kořisti pouze přirozeně vymíral (tj. exponenciální pokles stavů s koeficientem $\gamma$). Přitom dále uvazujeme interakci dravce s kořistí, kterou očekáváme přímo úměrnou počtu obou s jistým koeficientem $\beta$, u dravce navíc ještě opatřený multiplikativním koeficientem vyjadřujícím jeho efektivitu při lovu kořisti. Dostáváme systém dvou rovnic:

$P = \sqrt{Kt + c}$. Dopočtením ze zadaných hodnot $P(2) = \sqrt{7} \cdot 100$, což je odhad skutečného množství brouků. □

*8.136.* Najděte rovnici křivky ležící v 1. kvadrantu a procházející bodem $\left[1, 3/4\right]$, jejíž tečna v libovolném bodě vytíná na kladné poloose $y$ úsek velikostí odpovídající průvodiči bodu dotyku (tj. vzdálenosti bodu dotyku od počátku). ○

*8.137.* Zkoumejte množství chemické sloučeniny $S$ (izolované od okolí) v kontejneru, která je nestálá a postupem času se rozpadá, přičemž střední doba života jedné její molekuly je $q$ (jednotek času). Pokud bylo na počátku (tj. v čase $t = 0$) v kontejneru $M$ molů sloučeniny $S$, kolik molů této sloučeniny by mělo být v kontejneru v čase $t \geq 0$? ○

*8.138.* Těleso o hmotnosti 100 g při zavěšení protáhne pružinu o 5 cm. Má-li toto těleso při průchodu rovnovážným bodem rychlost 10 cm/s, vyjádřete jeho polohu v závislosti na čase $t$. ○

Další slovní úlohy vedoucí na diferenciální rovnice naleznete na straně 513.

### M. Diferenciální rovnice vyšších řádů

**8.139. Tlumený oscilátor.** Zkusme si popsat jednoduchý model pro pohyb nějakého tělesa upnutého k jednomu bodu silnou pružinou. Je-li $y(t)$ výchylka našeho tělesa od bodu $y_0 = y(0) = 0$, pak lze uvažovat, že zrychlení $y''(t)$ v čase $t$ bude úměrné velikosti výchylky, avšak s opačným znaménkem. Konstanta úměrnosti $k$ je nazývána pružinovou konstantou. Uvažujeme-li $k = 1$, dostáváme tedy tzv. rovnici oscilátoru

$$y''(t) = -y(t).$$

Tato rovnice odpovídá systému rovnic

$$x'(t) = -y(t), \quad y'(t) = x(t)$$

z 8.7. Řešením takového systému je

$$x(t) = R\cos(t - \tau), \quad y(t) = R\sin(t - \tau)$$

s libovolnou nezápornou konstantou $R$, která určuje maximální amplitudu, a konstantou $\tau$, která určuje fázový posun.

Pro určení jednoznačného řešení potřebujeme proto znát nejen počáteční polohu $y_0$, nýbrž také rychlost pohybu v tomto okamžiku. Těmito dvěma údaji bude určena jak amplituda tak fázový posun jednoznačně.

Představme si navíc, že vlivem vlastností materiálu pružiny bude ještě dodatečně působit síla, která bude úměrná okamžité rychlosti pohybu našeho objektu, opět se znaménkem opačným než je amplituda. To vyjádříme dodatečným členem s první derivací a naše rovnice je

**Model Lotky a Volterry**

$$x' = \alpha x - \beta yx$$
$$y' = -\gamma y + \delta\beta xy.$$

Zajímavé je, že stejný model docela dobře vystihuje i vývoj nezaměstnanosti v systému omezeném na zaměstnavatele a jejich zaměstnance a to tak, že zaměstnanci hrají roli dravců, zatímco zaměstnavatelé jsou lovenou kořistí.

O tomto a podobných modelech lze nalézt nepřeberné množství literatury.

**8.53. Stabilita systémů rovnic.** My se nyní omezíme jen na jednu základní větu o stabilitě systémů. Všimněme si, že nám za předpokladu spojitosti parciálních derivací funkcí zadávajících systémy (ve skutečnosti jejich lipschitzovskosti) zajišťuje spojitost chování řešení a to jak v závislosti na počátečních podmínkách tak na samotných rovnicích.



S rostoucí vzdáleností $t$ od počáteční hodnoty $t_0$ ovšem odhady rostou exponenciálně! Tento výsledek tedy má pouze lokální charakter a není v rozporu s příkladem nestabilně se chovající rovnice $y' = ty$ ilustrované v odstavci 8.47.

Uvažujme dva systémy rovnic zapsané ve vektorovém tvaru

$$x' = f(t, x), \quad y' = g(t, y),$$

a předpokládejme, že zobrazení $f, g : U \subset \mathbb{R}^{n+1} \to \mathbb{R}^n$ mají spojité parciální derivace na otevřené množině $U$ s kompaktním uzávěrem. Takové funkce budou jistě stejnoměrné spojité a stejnoměrně lipschitzovské na $U$, můžeme si tedy označit konečné hodnoty

$$C = \sup_{x \neq y;\ (t,x),\,(t,y) \in U} \frac{|f(t,x) - f(t,y)|}{|x - y|}$$
$$B = \sup_{(t,x) \in U} |f(t,x) - g(t,x)|$$

S tímto značením nyní můžeme zformulovat naši základní větu:

**Věta.** *Nechť $x(t)$ a $y(t)$ jsou dvě pevně zvolená řešení systémů*

$$x' = f(t, x), \quad y' = g(t, y),$$

*zadaná počátečními podmínkami $x(t_0) = x_0$ a $y(t_0) = y_0$. Potom*

$$|x(t) - y(t)| \leq |x_0 - y_0|\,\mathrm{e}^{C|t-t_0|} + \tfrac{B}{C}\left(\mathrm{e}^{C|t-t_0|} - 1\right).$$

Důkaz. Bez újmy na obecnosti můžeme předpokládat $t_0 = 0$. Z vyjádření řešení $x(t)$ a $y(t)$ jako pevných bodů příslušných integrálních operátorů okamžitě vyplývá odhad



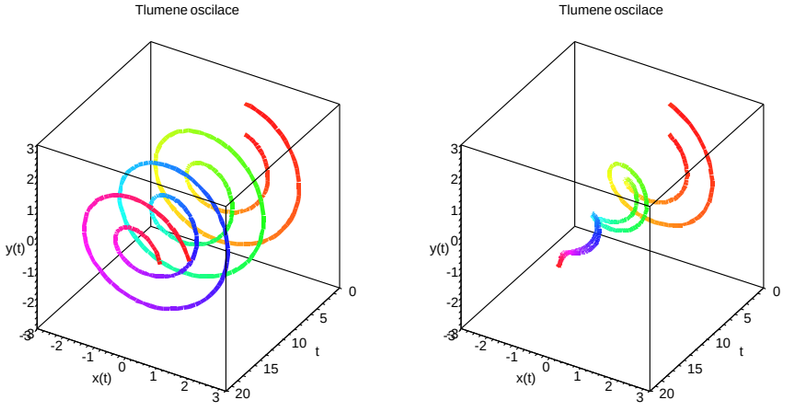
$$|x(t) - y(t)| \leq |x_0 - y_0| + \int_0^t |f(s, x(s)) - g(s, y(s))|\,ds.$$

Integrand přitom můžeme dále odhadnout

$$\begin{aligned} &|f(s, x(s)) - g(s, y(s))| \\ &\quad \leq |f(s, x(s)) - f(s, y(s))| + |f(s, y(s)) - g(s, y(s))| \\ &\quad \leq C\,|x(s) - y(s)| + B. \end{aligned}$$

$$y''(t) = -y(t) - \alpha y'(t),$$

kde $\alpha$ je konstanta, která vyjadřuje velikost tlumení. Na následujícím obrázku jsou vyneseny tzv. fázové diagramy pro řešení s dvěma různými počátečními podmínkami a to nalevo při nulovém tlumení, zatímco napravo je použit koeficient $\alpha = 0.3$




Samotné oscilace jsou vyjádřeny hodnotami na ose $y$, hodnoty $x$ zobrazují rychlost pohybu.

**8.140. Netlumené kmitání.** Nalezněte funkci $y(t)$ vyhovující diferenciální rovnici a počátečním podmínkám:

$$y''(t) + 4y(t) = f(t), \;\; y(0) = 0, \;\; y'(0) = -1,$$

kde funkce $f(t)$ je po částech spojitá:

$$f(t) = \begin{cases} \cos(2t) & \text{pro } 0 \le t < \pi, \\ 0 & \text{pro } t \ge \pi. \end{cases}$$

**Řešení.** Úloha je modelem netlumeného kmitání pružiny (bez zahrnutí tření a jiných vlivů, například nelinearit v tuhosti pružiny apod.), které je buzené vnější silou jen během počáteční doby a poté ustane.

Funkci $f(t)$ lze zapsat jako lineární kombinaci Heavisideovy funkce $u(t)$ a jejího posunutí, tj.

$$f(t) = \cos(2t)(u(t) - u_\pi(t))$$

Protože

$$\mathcal{L}(y'')(s) = s^2\mathcal{L}(y) - sy(0) - y'(0) = s^2\mathcal{L}(y) + 1,$$

dostáváme s využitím předchozích příkladů 7. a 8. k výpočtu Laplaceovy transformace pravé strany

$$\begin{aligned} s^2\mathcal{L}(y) + 1 + 4\mathcal{L}(y) &= \mathcal{L}(\cos(2t)(u(t) - u_\pi(t))) = \\ &= \mathcal{L}(\cos(2t)\cdot u(t)) - \mathcal{L}(\cos(2t)\cdot u_\pi(t)) = \\ &= \mathcal{L}(\cos(2t)) - e^{-\pi s}\mathcal{L}(\cos(2(t+\pi))) = \\ &= (1 - e^{-\pi s})\frac{s}{s^2+4}. \end{aligned}$$

Jestliže si označíme $F(t) = |x(t) - y(t)|$, $\alpha = |x_0 - y_0|$, přepíšeme náš odhad jako

$$F(t) \le \alpha + \int_0^t (C\,F(s) + B)\,ds. \tag{8.9}$$

Takový odhad můžeme docela snadno využít díky následujícímu obecnému výsledku, kterému se říkává *Gronwallova nerovnost*. Všimněte si podobnosti s obecným řešením lineárních rovnic.

**Lemma.** *Nechť reálná funkce $F(t)$ splňuje na intervalu $t \in [0, t_{max}]$ nerovnost*

$$F(t) \le \alpha(t) + \int_0^t \beta(s)F(s)\,ds$$

*pro nějaké reálné funkce $\alpha(t)$, $\beta(t)$, kde $\beta(t) \ge 0$. Potom také*

$$F(t) \le \alpha(t) + \int_0^t \alpha(s)\beta(s)\,\mathrm{e}^{\int_s^t \beta(r)\,dr}\,ds$$

*pro všechna $t \in [0, t_{max}]$. Jestliže je navíc $\alpha(t)$ neklesající, pak*

$$F(t) \le \alpha(t)\,\mathrm{e}^{\int_0^t \beta(s)\,ds}.$$

Důkaz lemmatu. Pišme pro přehlednost

$$G(t) = \mathrm{e}^{-\int_0^t \beta(s)\,ds}.$$

Přímým výpočtem s využitím prvního předpokladu věty dostáváme

$$\begin{aligned} \frac{d}{dt}\left(G(t)\int_0^t \beta(s)F(s)\,ds\right) &= \\ &= \beta(t)G(t)\left(F(t) - \int_0^t \beta(s)F(s)\,ds\right) \\ &\le \alpha(t)\beta(t)G(t) \end{aligned}$$

Nyní integrací podle $t$ a vydělením nenulovou funkcí $G(t)$

$$\int_0^t \beta(s)F(s)\,ds \le \int_0^t \alpha(s)\beta(s)\frac{G(s)}{G(t)}\,ds,$$

což po přičtení $\alpha(t)$ k oběma stranám již dává první tvrzení lemmatu.

Za dodatečného předpokladu neklesající $\alpha(t)$ můžeme pokračovat

$$F(t) \le \alpha(t)\Big(1 + \int_0^t \beta(s)\,\mathrm{e}^{\int_s^t \beta(r)\,dr}\,ds\Big).$$

Nyní si stačí povšimnout, že integrand je vlastně derivací

$$-\beta(s)\,\mathrm{e}^{\int_s^t \beta(r)\,dr} = \frac{d}{ds}\left(\mathrm{e}^{\int_s^t \beta(r)\,dr}\right),$$

a proto konečně dostáváme

$$\begin{aligned} F(t) &\le \alpha(t)\Big(1 - \int_0^t \frac{d}{ds}\,\mathrm{e}^{\int_s^t \beta(r)\,dr}\,ds\Big) \\ &= \alpha(t)\Big(1 + \mathrm{e}^{\int_s^t \beta(r)\,dr} - 1\Big) \end{aligned}$$

a druhé tvrzení lemmatu je dokázáno také. □

A teď už můžeme důkaz věty o spojité závislosti na parametrech rychle dokončit. Již jsme získali odhad (8.9) a použitím trochu modifikované funkce $\tilde{F}(t) = F(t) + \frac{B}{C}$ z něj dostaneme

$$\tilde{F}(t) \le \tfrac{D}{C} + \alpha + \int_0^t C\tilde{F}(s)\,ds.$$

Odtud

$$\mathcal{L}(y) = -\frac{1}{s^2+4} + (1-e^{-\pi s})\frac{s}{(s^2+4)^2}.$$

Inverzní transformací dostáváme řešení ve tvaru

$$y(t) = -\tfrac{1}{2}\sin(2t) + \tfrac{1}{4}t\sin(2t) + \mathcal{L}^{-1}\left(e^{-\pi s}\frac{s}{(s^2+4)^2}\right).$$

Podle vztahu (‖7.35‖), ale

$$\begin{aligned}\mathcal{L}^{-1}\left(e^{-\pi s}\frac{s}{(s^2+4)^2}\right) &= \tfrac{1}{4}\mathcal{L}^{-1}(e^{-\pi s}\,\mathcal{L}(t\sin(2t)))\\ &= (t-\pi)\sin(2(t-\pi))\cdot H_\pi(t).\end{aligned}$$

Protože je Heavisideova funkce pro $t < \pi$ nulová a pro $t > \pi$ rovna 1, dostáváme řešení ve tvaru

$$y(t) = \begin{cases} -\frac{1}{2}\sin(2t) + \frac{1}{4}t\sin(2t) & \text{pro } 0 \le t < \pi \\ \frac{\pi-2}{4}\sin(2t) & \text{pro } t \ge \pi \end{cases}$$

□

**8.141.** Určete obecné řešení rovnice

$$y''' - 5y'' - 8y' + 48y = 0.$$

**Řešení.** Jde o lineární diferenciální rovnici (3. řádu) s konstantními koeficienty, neboť má tvar

$$y^{(n)} + a_1 y^{(n-1)} + a_2 y^{(n-2)} + \cdots + a_{n-1}y' + a_n y = f(x)$$

pro jisté konstanty $a_1, \ldots, a_n \in \mathbb{R}$. Navíc je $f(x) \equiv 0$, tj. rovnice je homogenní.

Nejprve nalezneme kořeny tzv. charakteristického polynomu

$$\lambda^n + a_1\lambda^{n-1} + a_2\lambda^{n-2} + \cdots + a_{n-1}\lambda + a_n.$$

Každému $k$-násobnému reálnému kořenu $\lambda$ totiž odpovídá $k$ řešení

$$\mathrm{e}^{\lambda x}, x\,\mathrm{e}^{\lambda x}, \ldots, x^{k-1}\,\mathrm{e}^{\lambda x}$$

a každé $k$-násobné dvojici komplexních kořenů $\lambda = \alpha \pm \mathrm{i}\beta$ odpovídá $k$ dvojic řešení

$$\begin{aligned}&\mathrm{e}^{\alpha x}\cos(\beta x),\ x\,\mathrm{e}^{\alpha x}\cos(\beta x),\ \ldots,\ x^{k-1}\,\mathrm{e}^{\alpha x}\cos(\beta x),\\ &\mathrm{e}^{\alpha x}\sin(\beta x),\ x\,\mathrm{e}^{\alpha x}\sin(\beta x),\ \ldots,\ x^{k-1}\,\mathrm{e}^{\alpha x}\sin(\beta x).\end{aligned}$$

Obecné řešení potom odpovídá všem lineárním kombinacím výše uvedených řešení.

Uvažujme proto polynom

$$\lambda^3 - 5\lambda^2 - 8\lambda + 48$$

s kořeny $\lambda_1 = \lambda_2 = 4$, $\lambda_3 = -3$. Znalost kořenů však znamená, že známe také obecné řešení

$$y = C_1\mathrm{e}^{4x} + C_2 x\,\mathrm{e}^{4x} + C_3\mathrm{e}^{-3x}, \quad C_1, C_2, C_3 \in \mathbb{R}.$$ □

To už je předpoklad Gronwallovy nerovnosti s dokonce konstantními parametry, dostáváme tedy podle druhého tvrzení lemmatu

$$F(t) + \tfrac{B}{C} \le (\alpha + \tfrac{B}{C})\,\mathrm{e}^{\int_0^t C\,ds},$$

neboli právě námi dokazované tvrzení

$$F(t) \le \alpha\,\mathrm{e}^{Ct} + \tfrac{B}{C}(\mathrm{e}^{Ct} - 1).$$ □

Z tvrzení věty okamžitě vyplývá spojitá závislost jak na počátečních podmínkách, tak na případných dalších parametrech, v nichž by funkce $f$ byla lokálně Lipschitzovsky spojitá. Úplně jednoduchá rovnice v jedné proměnné $x' = x$ s exponenciálním řešením ukazuje, že nelze doufat v obecné lepší výsledky.

**8.54. Diferencovatelnost řešení.** V praktických problémech nás zajímá diferencovatelnost získaných řešení a to také ve vztahu k počátečním podmínkám, resp. dalším parametrům systému.



Všimněme si, že v obecném vektorovém popisu systému obyčejných rovnic

$$x' = f(t, x)$$

můžeme vždy předpokládat, že vektorová funkce nezávisí implicitně na $t$. Skutečně, pokud totiž na $t$ explicitně závisí, můžeme přidat jednu proměnnou $x_0$ a zapsat stejný systém rovnic pro křivku $\tilde{x}'(t) = (x_0(t), x_1(t), \ldots, x_n(t))$ jako

$$\begin{aligned} x_0' &= 1,\\ x_1' &= f_1(x_0, x_1, \ldots, x_n),\\ &\vdots\\ x_n' &= f_n(x_0, x_1, \ldots, x_n),\end{aligned}$$

s počátečními podmínkami

$$x_0(t_0) = t_0,\ x_(t_0) = x_1, \ldots, x_n(t_0) = x_n.$$

Takovýmto systémům nezávislým explicitně na čase říkáme *autonomní systémy obyčejných diferenciálních rovnic*.

Pro zjednodušení postupu se tedy budeme zabývat autonomními systémy závislými na parametrech $\lambda$ a s počátečními podmínkami

$$y' = f(y, \lambda),\ y(t_0) = x. \tag{8.10}$$

Bez újmy na obecnosti budeme u autonomních systémů vždy uvažovat počáteční hodnotu $t_0 = 0$ a v případě potřeby budeme řešení s $y(0) = x$ psát ve formě $y(t, x, \lambda)$, abychom zdůraznili závislost na parametrech.

Pro pevné hodnoty počátečních podmínek (a případných parametrů) bude samotné řešení vždy o jeden řád vícekrát diferencovatelné než je řád diferencovatelnosti funkce $f$. Snadno to odvodíme induktivně pomocí pravidla o derivování složených zobrazení. Je-li $f$ spojitě diferencovatelná,

$$y''(t) = D^1 f(y(t))\cdot y'(t) = D^1 f(y(t))\cdot f(y(t))$$

existuje a je spojitá. Má-li $f$ spojité všechny parciální derivace druhého řádu, dostaneme výraz pro třetí derivaci:

$$\begin{aligned} y^{(3)}(t) = {} & D^2 f(y(t))\big(f(y(t)), f(y(t))\big)\\ & + \big(D^1 f(y(t))\big)^2 \cdot f(y(t)).\end{aligned}$$

Promyslete si podrobně argumentaci pro vyšší řády.

**8.142.** Vypočtěte

$$y''' + y'' + 9y' + 9y = \mathrm{e}^x + 10\cos(3x)\,.$$

**Řešení.** Nejprve vyřešíme přidruženou homogenní rovnici. Příslušný charakteristický polynom je v tomto případě

$$\lambda^3 + \lambda^2 + 9\lambda + 9$$

a má kořeny $\lambda_1 = -1$, $\lambda_2 = 3\mathrm{i}$, $\lambda_3 = -3\mathrm{i}$. Obecné řešení přidružené homogenní rovnice je tedy

$$y = C_1\mathrm{e}^{-x} + C_2\cos(3x) + C_3\sin(3x)\,, \quad C_1, C_2, C_3 \in \mathbb{R}.$$

Řešení nehomogenní rovnice uvedeme ve tvaru

$$y = C_1\mathrm{e}^{-x} + C_2\cos(3x) + C_3\sin(3x) + y_p, \quad C_1, C_2, C_3 \in \mathbb{R}$$

pro jisté partikulární řešení $y_p$ nehomogenní rovnice.

Pravá strana zadané rovnice je ve speciálním tvaru. Obecně platí, že pokud je nehomogenní část dána funkcí

$$P_n(x)\,\mathrm{e}^{\alpha x},$$

přičemž $P_n$ je polynom $n$-tého řádu, existuje partikulární řešení

$$y_p = x^k\, R_n(x)\,\mathrm{e}^{\alpha x},$$

kde $k$ je násobnost čísla $\alpha$ jako kořene charakteristického polynomu a $R_n$ je polynom stupně nejvýše $n$. Ještě obecněji, pro nehomogenní část

$$\mathrm{e}^{\alpha x}\,[P_m(x)\cos(\beta x) + S_n(x)\sin(\beta x)]\,,$$

přičemž $P_m$ je polynom stupně $m$ a $S_n$ polynom stupně $n$, existuje partikulární řešení ve tvaru

$$y_p = x^k\,\mathrm{e}^{\alpha x}\,[R_l(x)\cos(\beta x) + T_l(x)\sin(\beta x)]\,,$$

kde $k$ je násobnost čísla $\alpha + \mathrm{i}\beta$ jako kořene charakteristického polynomu a $R_l$, $T_l$ jsou polynomy stupně nejvýše $l = \max\{m, n\}$.

V tomto příkladu je nehomogenní část součtem dvou funkcí ve speciálním tvaru (viz výše). Najdeme proto příslušná dvě partikulární řešení pomocí metody neurčitých koeficientů a ta pak sečteme. Tím získáme partikulární řešení a posléze i obecné řešení zadané diferenciální rovnice. Začněme s funkcí $y = \mathrm{e}^x$, které odpovídá partikulární řešení $y_{p_1}(x) = A\mathrm{e}^x$ pro jisté $A \in \mathbb{R}$. Protože

$$y_{p_1}(x) = y'_{p_1}(x) = y''_{p_1}(x) = y'''_{p_1}(x) = A\mathrm{e}^x,$$

dosazením do původní rovnice s pravou stranou, kde je pouze funkce $y = \mathrm{e}^x$, získáváme

$$20A\mathrm{e}^x = \mathrm{e}^x, \quad \text{tj.} \quad A = \tfrac{1}{20}.$$

Pro pravou stranu tvořenou funkcí $y = 10\cos(3x)$ hledáme partikulární řešení ve tvaru

$$y_{p_2}(x) = x\,[B\cos(3x) + C\sin(3x)]\,.$$

Předpokládejme na chvíli, že řešení $y(t, x)$ našeho systému (8.10) je spojitě diferencovatelné i v parametrech $x \in \mathbb{R}^n$. Pak můžeme derivaci

$$\Phi(t, x) = D^1_x(y(t, x)),$$

tj. Jacobiho matici všech parciálních derivací podle souřadnic $x_i$, závisející jednak na čase $t$, ale také na počáteční podmínce $x$, určit pomocí pravidla pro derivování kompozice zobrazení:

$$\begin{aligned} D^1_x\big(y'(t, x)\big) &= \frac{d}{dt}\big(D^1_x y(t, x)\big) \\ &= D^1 f(y(t, x)) \cdot D^1_x y(t, x). \end{aligned}$$

Derivace podle počátečních podmínek podél řešení $y(t, x)$ systému (8.10) jsou tedy dány jako řešení systému $n^2$ rovnic prvního řádu s počáteční podmínkou

$$\Phi'(t, x) = F(t, x) \cdot \Phi(t, x),\ \Phi(0, x) = E, \tag{8.11}$$

kde $F(t, x) = D^1 f(y(t, x))$ a počáteční podmínka vychází z identity $y(0, x) = x$. Jednoznačnou existenci řešení tohoto (maticového) systému a jeho spojitou závislost na parametrech jsme již dokázali.

Následující věta říká, že ve skutečnosti pro systémy se spojitě diferencovatelnými pravými stranami $f$ skutečně takto derivace podle parametrů vždy dostaneme.

### Diferencovatelnost řešení

**Věta.** *Uvažme otevřenou podmnožinu $U \subset \mathbb{R}^{n+k}$ a zobrazení $f : U \to \mathbb{R}^n$ se spojitými prvními derivacemi. Pak systém diferenciálních rovnic závislý na parametru $\lambda \in \mathbb{R}^k$ s počáteční podmínkou v bodě $x \in U$*

$$y'(t) = f(y(t), \lambda), \quad y(0) = x$$

*má jednoznačně určené řešení $y(t, x, \lambda)$, které je zobrazením se spojitými prvními parciálními derivacemi ve všech proměnných.*



Důkaz. Nejprve si všimněme, že můžeme uvažovat systém závisející na parametrech jako obyčejný autonomní systém bez parametrů, když i parametry považujeme za prostorové proměnné a dodáme (vektorové) podmínky $\lambda'(t) = 0$ a $\lambda(0) = \lambda$. Bez újmy na obecnosti proto stačí dokazovat větu pro autonomní systémy bez dodatečných parametrů a soustředit se na závislost na počátečních podmínkách.

Stejně jako v základní větě o existenci vyjdeme z Picardových aproximací řešení pomocí integrálního operátoru

$$y_0(t, x) = x,\ y_{k+1}(t, x) = x + \int_0^t f(y_k(s, x))\,ds.$$

Drobným upřesněním důkazu této věty 8.49 ověříme stejnoměrnou konvergenci aproximací $y_k(t, x)$ k řešení $y(t, x)$ a to včetně proměnné $x$.

Zvolme si nyní pro počáteční podmínku pevně bod $x_0$, zvolme jeho malé okolí $V$, které budeme případně zmenšovat během následujících odhadů, a pišme $C$ pro konstantu, která díky Lipschitzovskosti funkce $f$ dává na tomto okolí odhad

$$|f(y) - f(z)| \le C\,|y - z\,|.$$

Již víme, že pokud bude derivace

$$\Phi(t, x) = D^1_x y(t, x)$$

Připomeňme, že číslo $\lambda = 3\mathrm{i}$ jsme obdrželi jako kořen charakteristického polynomu. Snadno spočítáme derivace

$$\begin{aligned} y'_{p_2}(x) &= [B\cos(3x) + C\sin(3x)] \\ &\quad + x\,[-3B\sin(3x) + 3C\cos(3x)]\,, \\ y''_{p_2}(x) &= 2\,[-3B\sin(3x) + 3C\cos(3x)] \\ &\quad + x\,[-9B\cos(3x) - 9C\sin(3x)]\,, \\ y'''_{p_2}(x) &= 3\,[-9B\cos(3x) - 9C\sin(3x)] \\ &\quad + x\,[27B\sin(3x) - 27C\cos(3x)]\,, \end{aligned}$$

jejichž dosazením do rovnice s pravou stranou tvořenou funkcí $y = 10\cos(3x)$ po úpravě dostaneme

$$-18B\cos(3x) - 18C\sin(3x) - 6B\sin(3x) + 6C\cos(3x) = 10\cos(3x)\,.$$

Porovnání koeficientů vede na systém lineárních rovnic

$$-18B + 6C = 10, \quad -18C - 6B = 0$$

s jediným řešením $B = -1/2$ a $C = 1/6$, tj.

$$y_{p_2}(x) = x\left[-\tfrac{1}{2}\cos(3x) + \tfrac{1}{6}\sin(3x)\right].$$

Celkem je tudíž obecným řešením

$$y = C_1\mathrm{e}^{-x} + C_2\cos(3x) + C_3\sin(3x) + \frac{1}{20}\mathrm{e}^{x} - \frac{1}{2}x\cos(3x) + \frac{1}{6}x\sin(3x)\,, \quad C_1, C_2, C_3 \in \mathbb{R}.$$

□

**8.143.** Určete obecné řešení rovnice

$$y'' + 3y' + 2y = e^{-2x}.$$

**Řešení.** Daná rovnice je lineární (všechny derivace se v rovnici vyskytují v první mocnině) diferenciální rovnice s konstantními koeficienty druhého řádu (nejvyšší derivace hledané funkce, která se v rovnici vyskytuje je druhá). Nejprve vyřešíme zhomogenizovanou rovnici

$$y'' + 3y' + 2y = 0.$$

Její charakteristický polynom je

$$x^2 + 3x + 2 = (x+1)(x+2),$$

s kořeny $x_1 = -1$ a $x_2 = -2$. Obecné řešení zhomogenizované rovnice je tedy

$$c_1e^{-x} + c_2e^{-2x},$$

kde $c_1, c_2$ jsou libovolné reálné konstanty.

Nyní metodou neurčitých koeficientů nalezneme (nějaké) partikulární řešení původní nehomogenní rovnice. Podle tvaru nehomogenity řešení $y(t,x)$ existovat, bude dána rovnicí (8.11) s počáteční podmínkou. Definujme tedy $\Phi(t,x)$ touto rovnicí a zkoumejme výraz

$$G(t,h) = |y(t,x_0+h) - y(t,x_0) - h\Phi(t,x_0)|$$

s malými přírůstky $h \in \mathbb{R}^n$. Abychom dokázali, že spojitá derivace existuje, musíme dokázat, že

$$\lim_{h\to 0}\frac{1}{h}G(t,h) = 0.$$

Budeme k tomu potřebovat několik odhadů. Předně z poslední věty o spojité závislosti na počátečních podmínkách přímo vidíme odhad:

$$|y(t,x_0+h) - y(t,x_0)| \le |h|\,\mathrm{e}^{C|t|}\,.$$

V dalším kroku použijeme Taylorův rozvoj se zbytkem pro zobrazení $f$

$$f(y) - f(z) = D^1 f(z)\cdot(y-z) + R(y,z),$$

kde $R(y,z)$ splňuje $|R(y,z)|/|y-z| \to 0$ při $|y-z| \to 0$. Dostáváme první odhad, při kterém využíváme definice zobrazení $\Phi(t,x_0)$ pomocí jeho derivace. Píšeme opět $F(t,x) = D^1 f(y(t,x)))$

$$\begin{aligned} G(t,h) &\le \int_0^t |f(y(s,x_0+h)) - f(y(s,x_0)) \\ &\qquad - h\,F(s,x_0)\Phi(s,x_0)|\,ds \\ &\le \int_0^t \|F(s,x_0)\|\,|y(s,x_0+h) - y(s,x_0) - h\,\Phi(s,x_0)|\,ds \\ &\quad + \int_0^t |R(y(s,x_0+h), y(s,x_0))|\,ds, \end{aligned}$$

kde pracujeme s normou na maticích danou jako maximum absolutních hodnot jejich komponent.

Podle předpokladu je $F(t,x)$ spojité, proto na našem okolí $V$ a pro $|t| < T$ s dostatečně malým $T$, abychom zůstávali v okolí $V$, můžeme ohraničit normu

$$\|F(t,x_0)\| \le B$$

a zároveň pro libovolně zvolenou konstantu $\varepsilon > 0$ umíme najít ohraničení $|h| < \delta$, při kterém bude zbytek $R$ splňovat

$$\begin{aligned} |R(y(t,x_0+h), y(t,x_0))| &\le \varepsilon|y(t,x_0+h) - y(t,x_0)| \\ &\le |h|\varepsilon\,\mathrm{e}^{CT}\,. \end{aligned}$$

Můžeme proto náš odhad dále vylepšit takto

$$G(t,h) \le B\int_0^t G(s,h)\,ds + \varepsilon|h|T\,\mathrm{e}^{CT}\,.$$

Gronwallovo lemma (viz 8.53) nám již dává

$$G(t,h) \le \varepsilon|h|T\,\mathrm{e}^{(C+B)T}\,.$$

Odtud ale už přímo vyplývá že výraz $\frac{1}{h}G(t,h)$ konverguje k nule a důkaz je dokončen. □

Velmi podobně se dokáže, že spojitá diferencovatelnost pravé strany až do řádu $k$ včetně zajišťuje stejný řád diferencovatelnosti řešení ve všech vstupních parametrech.

Dokonce platí, že je-li pravá strana $f$ analytická (tj. funkce daná svojí konvergentní Taylorovou řadou obdobně k úvahám v kapitole šesté) ve všech parametrech, pak je analytická i závislost řešení na všech parametrech.

a protože $-2$ je kořenem charakteristického polynomu dané rovnice hledáme řešení ve tvaru $y_0 = axe^{-2x}$, kde $a \in \mathbb{R}$.

Dosazením do původní rovnice obdržíme

$$a[-4e^{-2x} + 4xe^{-2x} + 3(e^{-2x} - 2xe^{-2x}) + 2xe^{-2x}] = e^{-2x},$$

odkud $a = -1$. Partikulárním řešením dané rovnice je tedy funkce $-xe^{-2x}$, obecným řešením potom prostor funkcí $c_1e^{-x} + c_2e^{-2x} - xe^{-2x}$, $c_1, c_2 \in \mathbb{R}$. □

**8.144.** Určete obecné řešení rovnice

$$y'' + y' = 1.$$

**Řešení.** Charakteristický polynom dané rovnice je $x^2 + x$ s kořeny 0 a $-1$, obecné řešení zhomogenizované rovnice je tedy $c_1 + c_2e^{-x}$, kde $c_1, c_2 \in \mathbb{R}$.

Partikulární řešení hledáme ve tvaru $ax$, $a \in \mathbb{R}$ (nula je kořenem charakteristického polynomu). Po dosazení do původní rovnice dostáváme $a = 1$. Obecné řešení dané nehomogenní rovnice je $c_1 + c_2e^{-x} + x$, $c_1, c_2 \in \mathbb{R}$. □

**8.145.** Určete obecné řešení rovnice

$$y'' + 5y' + 6y = e^{-2x}.$$

**Řešení.** Charakteristický polynom rovnice je $x^2 + 5x + 6 = (x + 2)(x + 3)$, jeho kořeny jsou $-2$ a $-3$, obecné řešení zhomogenizované rovnice je tedy $c_1e^{-2x} + c_2e^{-3x}$, $c_1, c_2 \in \mathbb{R}$. Partikulární řešení hledáme metodou neurčitých koeficientů ve tvaru $axe^{-2x}$, $a \in \mathbb{R}$ ($-2$ je kořenem charakteristického polynomu). Dosazením do původní rovnice získáme $a = 1$. Obecné řešení dané rovnice je tedy

$$c_1e^{-2x} + c_2e^{-3x} + xe^{-2x}.$$

□

**8.146.** Určete obecné řešení rovnice

$$y'' - y' = 5.$$

**Řešení.** Charakteristický polynom je $x^2 - x$ s kořeny 1, 0, obecné řešení zhomogenizované rovnice je tedy $c_1 + c_2e^x$, kde $c_1, c_2 \in \mathbb{R}$. Partikulární řešení hledáme metodou neurčitých koeficientů ve tvaru $ax$, $a \in \mathbb{R}$, dostáváme $a = -5$. Obecné řešení dané rovnice je tvaru

$$c_1 + c_2e^x - 5x.$$

□

**8.55. Toky vektorových polí.** Ještě než se přesuneme k rovnicím vyšších řádů, podíváme se chvíli na systémy rovnic prvního řádu geometrickým pohledem. Nyní můžeme geometricky formalizovat pravou stranu autonomního systému jako přiřazení vektoru $f(x) \in \mathbb{R}^n$ v zaměření euklidovského prostoru $\mathbb{R}^n$ ke každému jeho bodu $x$ v uvažovaném definičním oboru. Hovoříme o *vektorovém poli* $X(x) = f(x)$.



Jestliže máme dáno vektorové pole $X$ na otevřené množině $U \subset \mathbb{R}^n$, pak můžeme pro každou diferencovatelnou funkci $f$ na $U$ definovat její derivaci ve směru vektorového pole $X$ předpisem

$$X(f) : U \to \mathbb{R}, \qquad X(f)(x) = d_{X(x)}f.$$

Je-li tedy v souřadnicích $X(x) = (X_1(x), \dots X_n(x))$, pak

$$X(f)(x) = X_1(x)\frac{\partial f}{\partial x_1}(x) + \cdots + X_n(x)\frac{\partial f}{\partial x_n}(x).$$

Nejjednodušší vektorová pole budou mít v souřadnicích všechny souřadné funkce rovny nule, kromě jedné funkce $X_i$, která bude konstantně jednička. Takové pole pak odpovídá příslušné parciální derivaci podle proměnné $x_i$. Tomu odpovídá také obvyklý zápis

$$X(x) = X_1(x)\frac{\partial}{\partial x_1} + \cdots + X_n(x)\frac{\partial}{\partial x_n}.$$

Nyní můžeme řešení našeho systému rovnic ekvivalentně popsat jako hledání křivky $x(t)$, která pro každé $t$ ze svého definičního oboru splňuje

$$x'(t) = X(x(t)),$$

tečný vektor hledané křivky je v každém jejím bodě zadán vektorovým polem $X$. Každou takovou křivku nazýváme *integrální křivkou* vektorového pole $X$ a zobrazení

$$\mathrm{Fl}_t^X : \mathbb{R}^n \to \mathbb{R}^n,$$

definované v bodě $x_0$ jako hodnota integrální křivky $x(t)$, splňující $x(0) = x_0$ nazýváme *tokem vektorového pole* $X$. Věta o jednoznačnosti a existenci řešení systémů rovnic říká, že pro každé spojitě diferencovatelné vektorové pole $X$ existuje jeho tok v každém bodě $x_0$ definičního oboru pro dostatečně malá $t$. Jednoznačnost řešení navíc přímo zajišťuje, že

$$\mathrm{Fl}_{t+s}^X(x) = \mathrm{Fl}_t^X \circ \mathrm{Fl}_s^X(x),$$

kdykoliv obě strany existují. Navíc je zobrazení $\mathrm{Fl}_{t_0}^X(x)$ s pevným parametrem $t$ diferencovatelné ve všech bodech $x$, kde je definované.

Pokud je vektorové pole $X$ definované na celém $\mathbb{R}^n$ a má kompaktní nosič, pak zjevně existuje jeho tok ve všech bodech a pro všechna $t$. Takovým vektorovým polím říkáme *úplná*. Tok úplného vektorového pole je tedy složen z difeomorfismů $\mathrm{Fl}_t^X\ \mathbb{R}^n \to \mathbb{R}^n$ s inverzními difeomorfismy $\mathrm{Fl}_{-t}^X$.

Jednoduchým příkladem úplného vektorového pole je pole $X(x) = \frac{\partial}{\partial x_1}$. Jeho tok je dán

$$\mathrm{Fl}_t^X(x_1, \dots, x_n) = (x_1 + t, x_2, \dots, x_n).$$

Naopak, vektorové pole $X(t) = t^2\frac{d}{dt}$ na jednorozměrném prostoru $\mathbb{R}$ není úplné, protože jeho řešení jsou tvaru

$$t \mapsto \frac{1}{C - t}$$

pro počáteční podmínky s $t_0 \neq 0$ a „utečou" tedy do nekonečných hodnot v konečném čase.

**8.147.** Vyřešte rovnici

$$y'' - 2y' + y = \frac{\mathrm{e}^x}{x^2+1}.$$

**Řešení.** Řešení této nehomogenní rovnice určíme metodou variace konstant, kdy řešení obdržíme ve tvaru

$$y = C_1(x)\, y_1(x) + C_2(x)\, y_2(x) + \cdots + C_n(x)\, y_n(x),$$

přičemž $y_1, \ldots, y_n$ zadávají obecné řešení přidružené homogenní rovnice a funkce $C_1(x), \ldots, C_n(x)$ získáme ze soustavy

$$\begin{aligned}
C_1'(x)\, y_1(x) + \cdots + C_n'(x)\, y_n(x) &= 0,\\
C_1'(x)\, y_1'(x) + \cdots + C_n'(x)\, y_n'(x) &= 0,\\
&\vdots\\
C_1'(x)\, y_1^{(n-2)}(x) + \cdots + C_n'(x)\, y_n^{(n-2)}(x) &= 0,\\
C_1'(x)\, y_1^{(n-1)}(x) + \cdots + C_n'(x)\, y_n^{(n-1)}(x) &= f(x).
\end{aligned}$$

Charakteristický polynom $\lambda^2 - 2\lambda + 1$ má kořeny $\lambda_1 = \lambda_2 = 1$. Řešení rovnice tak hledáme ve tvaru

$$C_1(x)\,\mathrm{e}^x + C_2(x)\, x\,\mathrm{e}^x$$

a uvažujeme soustavu

$$\begin{aligned}
C_1'(x)\,\mathrm{e}^x + C_2'(x)\, x\,\mathrm{e}^x &= 0,\\
C_1'(x)\,\mathrm{e}^x + C_2'(x)\left[\mathrm{e}^x + x\,\mathrm{e}^x\right] &= \frac{\mathrm{e}^x}{x^2+1}.
\end{aligned}$$

Neznámé $C_1'(x)$ a $C_2'(x)$ vypočítáme pomocí Cramerova pravidla. Z

$$\begin{vmatrix} \mathrm{e}^x & x\,\mathrm{e}^x \\ \mathrm{e}^x & \mathrm{e}^x + x\,\mathrm{e}^x \end{vmatrix} = \mathrm{e}^{2x},$$

$$\begin{vmatrix} 0 & x\,\mathrm{e}^x \\ \frac{\mathrm{e}^x}{x^2+1} & \mathrm{e}^x + x\,\mathrm{e}^x \end{vmatrix} = -x\,\frac{\mathrm{e}^{2x}}{x^2+1},$$

$$\begin{vmatrix} \mathrm{e}^x & 0 \\ \mathrm{e}^x & \frac{\mathrm{e}^x}{x^2+1} \end{vmatrix} = \frac{\mathrm{e}^{2x}}{x^2+1}$$

plyne

$$\begin{aligned}
C_1(x) &= -\int \frac{x}{x^2+1}\,dx = -\frac{1}{2}\ln\left(x^2+1\right) + C_1, \quad C_1 \in \mathbb{R},\\
C_2(x) &= \int \frac{dx}{x^2+1} = \operatorname{arctg} x + C_2, \quad C_2 \in \mathbb{R}.
\end{aligned}$$

Obecné řešení proto je

$$y = C_1\mathrm{e}^x + C_2 x\,\mathrm{e}^x - \tfrac{1}{2}\,\mathrm{e}^x \ln\left(x^2+1\right) + x\,\mathrm{e}^x \operatorname{arctg} x, \quad C_1, C_2 \in \mathbb{R}.$$

□

Popis vektorového pole jakožto přiřazení tečného vektoru v zaměření ke každému bodu euklidovského prostoru je nezávislé na souřadnicích. Následující věta nám tedy dává geometrický lokální kvalitativní popis všech řešení systémů obyčejných diferenciálních rovnic v okolí každého bodu $x$ ve kterém je dané vektorové pole $X$ nenulové.

**Věta.** *Je-li $X$ vektorové pole definované na okolí bodu $x_0 \in \mathbb{R}^n$ a platí $X(x_0) \neq 0$, pak existuje transformace souřadnic $F$ taková, že v nových souřadnicích $y = F(x)$ je vektorové pole $X$ dáno jako pole $\frac{\partial}{\partial y_1}$.*



Důkaz. Budeme konstruovat difeomorfismus $F = (f_1, \ldots, f_n)$ postupně. Geometricky lze podstatu důkazu shrnout tak, že si vybereme nadplochu komplementární k směrům $X(x)$, procházející bodem $x_0$, na ní zvolíme souřadnice a ty pak rozneseme na nějaké okolí bodu $x_0$ pomocí toku pole $X$.

Nejdříve použijeme posunutí $x_0$ do počátku souřadnic a lineární transformaci na $\mathbb{R}^n$ tak, abychom dosáhli $X(0) = \frac{\partial}{\partial x_1}(0)$. Nyní si zapišme v těchto souřadnicích $(x_1, \ldots, x_n)$ tok pole $X$ procházející v čase $t = 0$ bodem $(x_1, \ldots, x_n)$ jako $x_i(t) = \varphi_i(t, x_1, \ldots, x_n)$. Definujeme

$$f_i(x_1, \ldots, x_n) = \varphi_i(x_1, 0, x_2, \ldots, x_n).$$

Protože tok pole $X$ splňuje (nalevo je vektor s uvedenými souřadnicemi $\varphi_i$)

$$(\varphi_i(0, 0, x_2, \ldots, x_n)) = (0, x_2, \ldots, x_n),$$

neboť jde o tok v čase nula, dostáváme

$$\frac{\partial F}{\partial x_i}(0) = (0, \ldots, 1, \ldots, 0), \quad i = 2, \ldots, n,$$

a stejný vztah platí i pro $i = 1$, protože je $X = \frac{\partial}{\partial x_1}$. Je tedy Jacobiho matice zobrazení $F$ v počátku jednotkovou maticí $E$, a proto jde skutečně o transformaci souřadnic na nějakém okolí (viz věta o inverzním zobrazení v odstavci 8.17).

Nyní přímo z definice zobrazení $F$ pomocí toku vektorového pole $X$ bude v nových souřadnicích $(y_1, \ldots, y_n)$ tok pole vyjádřen jako

$$\mathrm{Fl}_t^X(y_1, \ldots, y_n) = (y_1 + t, y_2, \ldots, y_n),$$

ověřte si samostatně podrobně! □

**8.56. Rovnice vyšších řádů.** Obyčejnou diferenciální rovnicí řádu $k$ (vyřešenou vzhledem k nejvyšší derivaci) rozumíme rovnici



$$y^{(k)}(t) = f(t, y(t), y'(t), \ldots, y^{(k-1)}(t)),$$

kde $f$ je známá funkce v $k+1$ proměnných, $x$ je nezávisle proměnná a $y(t)$ je neznámá funkce v jedné proměnné. Ukážeme, že taková rovnice je vždy ekvivalentní systému $k$ rovnic prvního řádu.

Zavedeme nové neznámé funkce v proměnné $t$ takto: $y_0(t) = y(t)$, $y_1(t) = y_0'(t), \ldots, y_{k-1}(t) = y_{k-2}'(t)$. Nyní je funkce $y(t)$

**8.148.** Určete jedinou funkci $y$ vyhovující lineární diferenciální rovnici

$$y^{(3)} - 3y' - 2y = 2e^x,$$

s počátečními podmínkami $y(0) = 0$, $y'(0) = 0$, $y''(0) = 0$.

**Řešení.** Charakteristický polynom je $x^3 - 3x - 2$ s kořeny 2 a dvojnásobným kořenem $-1$, partikulární řešení hledáme ve tvaru $ae^x, a \in \mathbb{R}$, snadno zjistíme že je jím funkce $-\frac{1}{2}e^x$, obecné řešení dané rovnice je tedy

$$c_1e^{2x} + c_2e^{-x} + c_3xe^{-x} - \frac{1}{2}e^x.$$

Dosazením do počátečních podmínek získáme jedninou funkci vyhovující zadání

$$\frac{2}{9}e^{2x} + \frac{5}{18}e^{-x} + \frac{1}{3}xe^{-x} - \frac{1}{2}e^x.$$

□

Další příklady na diferenciální rovnice vyššího řádu naleznete na straně 517

### N. Aplikace Laplaceovy transformace

Diferenciální rovnice s konstantními koeficienty můžeme také řešit pomocí Laplaceovy transformace.

**8.149.** Označme $\mathcal{L}(y)(s)$ Laplaceovu transformaci funkce $y(t)$. Metodou per partes dokažte, že platí

**Řešení.**

$$\mathcal{L}(y')(s) = s\mathcal{L}(y)(s) - y(0) \tag{8.11}$$

$$\mathcal{L}(y'')(s) = s^2\mathcal{L}(y) - sy(0) - y'(0)$$

a indukcí:

$$\mathcal{L}(y^{(n)})(s) = s^n\mathcal{L}(y)(s) - \textstyle\sum_{i=1}^{n} s^{n-i}\, y^{(i-1)}(0)\,. \qquad \square$$

**8.150.** Najděte funkci $y(t)$ vyhovující diferenciální rovnici

$$y''(t) + 4y(t) = \sin 2t$$

a počátečním podmínkám $y(0) = 0$ a $y'(0) = 0$.

**Řešení.** Z předchozího příkladu ‖8.149‖:

$$s^2\mathcal{L}(y)(s) + 4\mathcal{L}(y)(s) = \mathcal{L}(\sin 2t)(s)$$

Přitom

$$\mathcal{L}(\sin 2t)(s) = \frac{2}{s^2+4},$$

tj.

$$\mathcal{L}(y)(s) = \frac{2}{(s^2+4)^2}.$$

Zpětnou transformací dostáváme

$$y(t) = \tfrac{1}{8}\sin 2t - \tfrac{1}{4}t\cos 2t\,. \qquad \square$$

řešením naší původní rovnice tehdy a jen tehdy, když je první komponentou řešení systému rovnic

$$\begin{aligned} y_0' &= y_1 \\ y_1' &= y_2 \\ &\vdots \\ y_{n-2}' &= y_{n-1} \\ y_{n-1}' &= f(t, y_0, y_1, \ldots, y_{n-1}). \end{aligned}$$

Přímým důsledkem vět z 8.52–8.54 je proto následující

#### O řešení ODR vyšších řádů

**Věta.** *Nechť funkce $f(t, y_0, \ldots, y_{k-1}) : U \subset \mathbb{R}^{k+1} \to \mathbb{R}$, má spojité parciální derivace na otevřené množině $U$. Pak pro každý bod $(t_0, z_0, \ldots, z_{k-1}) \in U$ existuje maximální interval $I_{max} = [x_0 - a, x_0 + b]$, s kladnými $a, b \in \mathbb{R}$, a právě jedna funkce $y(t) : I_{max} \to \mathbb{R}$, která je řešením rovnice $k$-tého řádu*

$$y^{(k)}(t) = f(t, y(t), y'(t), \ldots, y^{(k-1)}(t))$$

*s počáteční podmínkou*

$$y(t_0) = z_0, y'(t_0) = z_1, \ldots, y^{(k-1)}(t_0) = z_{k-1}.$$

*Toto řešení navíc závisí diferencovatelně na počáteční podmínce a případných dalších parametrech vstupujících diferencovatelně do funkce $f$.*

Vidíme tedy, že pro jednoznačné zadání řešení obyčejné diferenciální rovnice $k$–tého řádu musíme zadat v jednom bodě hodnotu a prvních $k-1$ derivací výsledné funkce.

Pokud bychom pracovali se systémem $\ell$ rovnic řádu $k$, pak stejný postup převede tento systém také na systém $k\ell$ rovnic prvního řádu. Opět tedy bude plati obdobná věta o existenci jednoznačnosti, spojitosti a diferencovatelnosti.

Na všechny takové systémy se samozřejmě také přenáší silnější vlastnosti v případech, kdy je pravá strana rovnice $f$ diferencovatelná do řádu $k$ včetně nebo analytická, včetně parametrů, kteréžto vlastnosti se přenáší i na řešení.

**8.57. Lineární diferenciální rovnice.** Již jsme přemýšleli o operaci derivování jako o lineárním zobrazení z (dostatečně) hladkých funkcí do funkcí. Pokud derivace $(\frac{d}{dx})^j$ jednotlivých řádů $j$ vynásobíme pevnými funkcemi $a_j(t)$ a výrazy sečteme, dostaneme tzv. *lineární diferenciální operátor*:

$$y(t) \mapsto D(y)(t) = a_k(t)y^{(k)}(t) + \cdots + a_1(t)y'(t) + a_0y(t).$$

Řešit příslušnou *homogenní lineární diferenciální rovnici* pak znamená najít funkci $y$ splňující $D(y) = 0$, tj. obrazem je identicky nulová funkce.

Ze samotné definice je zřejmé, že součet dvou řešení bude opět řešením, protože pro libovolné funkce $y_1$ a $y_2$ platí

$$D(y_1 + y_2)(t) = D(y_1)(t) + D(y_2)(t).$$

Obdobně je také konstantní násobek řešení opět řešením. Celá množina všech řešení lineární diferenciální rovnice $k$-tého řádu je tedy vektorovým prostorem. Přímou aplikací předchozí věty o jednoznačnosti a existenci řešení rovnic dostáváme:

**8.151.** Najděte funkci $y(t)$ vyhovující diferenciální rovnici

$$y''(t) + 6y'(t) + 9y(t) = 50\sin t$$

a počátečním podmínkám $y(0) = 1$ a $y'(0) = 4$.

**Řešení.** Laplaceovou transformací dostáváme

$$s^2\mathcal{L}(y)(s) - s - 4 + 6(s\mathcal{L}(y)(s) - 1) + 9\mathcal{L}(y)(s) = 50\mathcal{L}(\sin t)(s),$$

tj.

$$(s^2 + 6s + 9)\mathcal{L}(y)(s) = \frac{50}{s^2+1} + s + 10,$$

$$\mathcal{L}(y)(s) = \frac{50}{(s^2+1)(s+3)^2} + \frac{s+10}{(s+3)^2}.$$

Rozkladem na parciální zlomky prvního členu dostaneme

$$\frac{50}{(s^2+1)(s+3)^2} = \frac{As+B}{s^2+1} + \frac{C}{s+3} + \frac{D}{(s+3)^2},$$

tedy

$$50 = (As+B)(s+3)^2 + C(s^2+1)(s+3) + D(s^2+1).$$

Dosazením $s = -3$ dostáváme

$$50 = 10D \quad \text{tedy} \quad D = 5$$

a porovnáním koeficientů u $s^3$

$$0 = A + C, \quad \text{tedy} \quad A = -C.$$

Porovnáním koeficientů u $s$ pak

$$0 = 9A + 6B + C = 8A + 6B, \quad \text{tedy} \quad B = \frac{4}{3}C.$$

Porovnáním absolutních členů dostaneme

$$50 = 9B + 3C + D = 12C + 3C + 5$$

$$\text{tedy} \quad C = 3,\ B = 4,\ A = -3.$$

Protože

$$\frac{s+10}{(s+3)^2} = \frac{s+3+7}{(s+3)^2} = \frac{1}{s+3} + \frac{7}{(s+3)^2},$$

platí

$$\begin{aligned}\mathcal{L}(y)(s) &= \tfrac{-3s+4}{s^2+1} + \tfrac{3}{s+3} + \tfrac{5}{(s+3)^2} + \tfrac{1}{s+3} + \tfrac{7}{(s+3)^2} \\ &= \tfrac{-3s}{s^2+1} + \tfrac{4}{s^2+1} + \tfrac{4}{s+3} + \tfrac{12}{(s+3)^2}.\end{aligned}$$

Odtud inverzní Laplaceovou transformací dostáváme řešení ve tvaru

$$y(t) = -3\cos t + 4\sin t + 4e^{-3t} + 12te^{-3t}\,. \qquad \square$$

PROSTOR ŘEŠENÍ LINEÁRNÍCH ROVNIC

**Věta.** *Množina všech řešení homogenní lineární diferenciální rovnice $k$–tého řádu je vždy vektorový prostor dimenze $k$. Proto můžeme vždy řešení zadat jako lineární kombinaci libovolné množiny $k$ lineárně nezávislých řešení. Taková řešení jsou zadána jednoznačně lineárně nezávislými počátečními podmínkami na hodnotu funkce $y(t)$ a jejích prvních $k-1$ derivací v jednom pevném bodě $t_0$.*

DŮKAZ. Jestliže zvolíme $k$ lineárně nezávislých počátečních podmínek v jednom pevném bodě, pak dostaneme pro každou z nich jednoznačně určené řešení naší rovnice. Lineární kombinace těchto počátečních podmínek přitom vede na tutéž lineární kombinaci příslušných řešení. Všechny možné počáteční podmínky tak vyčerpáme, proto takto dostaneme i celý prostor řešení naší rovnice. $\square$

**8.58. Lineární diferenciální rovnice s konstantními koeficienty.** Předchozí diskuse nám jistě připomněla situaci s homogenními lineárními diferenčními rovnicemi, se kterými jsme se potýkali v odstavci 3.9 třetí kapitoly. Analogie jde i dále v okamžiku, kdy jsou všechny koeficienty $a_j$ diferenciálního operátoru $D$ konstantní. Už jsme viděli u takové rovnice prvního řádu (8.8), že řešením je exponenciála s vhodnou konstantou u argumentu. Stejně jako u diferenčních rovnic se podbízí vyzkoušet, zda takový tvar řešení $y(t) = \mathrm{e}^{\lambda t}$ s neznámým parametrem $\lambda$ může splnit rovnici $k$–tého řádu. Dosazením dostaneme

$$D(\mathrm{e}^{\lambda t}) = \left(a_k\lambda^k + a_{k-1}\lambda^{k-1} + \cdots + a_1\lambda + a_0(x)\right)\mathrm{e}^{\lambda t}\,.$$

Parametr $\lambda$ tedy vede na řešení lineární diferenciální rovnice s konstantními koeficienty tehdy a jen tehdy, když je $\lambda$ kořenem tzv. *charakteristického polynomu* $a_k\lambda^k + \cdots + a_1\lambda + a_0$.

Pokud má tento polynom $k$ různých kořenů, dostáváme bázi celého vektorového prostoru řešení. Pokud je $\lambda$ násobný kořen, přímým výpočtem s využitím toho, že je pak také kořenem derivace charakteristického polynomu, dostaneme, že je řešením i funkce $y(t) = t\,\mathrm{e}^{\lambda t}$. Podobně pak pro vyšší násobnost $\ell$ dostáváme $\ell$ různých řešení $\mathrm{e}^{\lambda t}, t\,\mathrm{e}^{\lambda t}, \ldots, t^\ell\,\mathrm{e}^{\lambda t}$.

U obecné lineární diferenciální rovnice předepisujeme nenulovou hodnotu diferenciálního operátoru $D$. Opět úplně analogicky k úvahám o systémech lineárních rovnic nebo u lineárních diferenčních rovnic přímo vidíme, že obecné řešení takovéto (nehomogenní) rovnice

$$D(y)(t) = b(t)$$

pro nějakou pevně zadanou funkci $b(t)$ je součtem jednoho jakéhokoliv řešení této rovnice a množiny všech možných řešení příslušné homogenní rovnice $D(y)(t) = 0$. Celý prostor řešení je tedy opět pěkný konečněrozměrný afinní prostor, byť ukrytý v obrovském prostoru funkcí.

Metody pro nalezení jednoho partikulárního řešení jsou předvedeny v konkrétních příkladech ve vedlejším sloupci. V principu jsou, podobně jako u diferenčních rovnic, založeny na hledání řešení v podobném tvaru v jakém je pravá strana.

**8.59. Maticové systémy s konstantními koeficienty.** Ještě se podívejme na velmi speciální případ systému prvního řádu, jehož pravá strana je zadána násobením matice a $n^2$-rozměrné neznámé vektorové funkce $Y(t)$.



**8.152.** Najděte funkci $y(t)$ vyhovující diferenciální rovnici

$$y''(t) = \cos(\pi t) - y(t), \quad t \in (0, +\infty)$$

a počátečním podmínkám $y(0) = c_1$, $y'(0) = c_2$.

**Řešení.** Nejdříve podotkněme, že z teorie obyčejných diferenciálních rovnic vyplývá, že úloha má právě jedno řešení. Dále připomeňme

$$\mathcal{L}\left(f''\right)(s) = s^2\mathcal{L}(f)(s) - s\lim_{t\to 0+} f(t) - \lim_{t\to 0+} f'(t)$$

a

$$\mathcal{L}(\cos(bt))(s) = \tfrac{s}{s^2+b^2}, \quad b \in \mathbb{R}.$$

Aplikování Laplaceovy transformace na zadanou diferenciální rovnici proto dává

$$s^2\mathcal{L}(y)(s) - sc_1 - c_2 = \tfrac{s}{s^2+\pi^2} - \mathcal{L}(y)(s),$$

tj.

$$\mathcal{L}(y)(s) = \frac{s}{\left(s^2+1\right)\left(s^2+\pi^2\right)} + \frac{c_1 s}{s^2+1} + \frac{c_2}{s^2+1}. \tag{8.12}$$

Stačí tudíž najít funkci $y$ splňující (‖8.12‖). Rozkladem na parciální zlomky získáváme

$$\tfrac{s}{(s^2+1)(s^2+\pi^2)} = \tfrac{1}{\pi^2-1}\left(\tfrac{s}{s^2+1} - \tfrac{s}{s^2+\pi^2}\right).$$

Z výše uvedeného vyjádření $\mathcal{L}(\cos(bt))(s)$ a dříve dokázaného

$$\mathcal{L}(\sin t)(s) = \tfrac{1}{s^2+1}$$

tak již dostáváme hledané řešení

$$y(t) = \tfrac{1}{\pi^2-1}(\cos t - \cos(\pi t)) + c_1\cos t + c_2\sin t\,. \qquad \square$$

**8.153.** Vyřešte soustavu diferenciálních rovnic

$$x''(t)+x'(t) = y(t)-y''(t)+\mathrm{e}^t, \quad x'(t)+2x(t) = -y(t)+y'(t)+\mathrm{e}^{-t}$$

při počátečních podmínkách $x(0) = 0$, $y(0) = 0$, $x'(0) = 1$, $y'(0) = 0$.

**Řešení.** Opět aplikujeme Laplaceovu transformaci. Tím s využitím

$$\mathcal{L}\left(\mathrm{e}^{\pm t}\right)(s) = \tfrac{1}{s\mp 1}$$

převedeme první rovnici na

$$s^2\mathcal{L}(x)(s) - s\lim_{t\to 0+} x(t) - \lim_{t\to 0+} x'(t) + s\mathcal{L}(x)(s) - \lim_{t\to 0+} x(t) =$$
$$= \mathcal{L}(y)(s) - \left(s^2\mathcal{L}(y)(s) - s\lim_{t\to 0+} y(t) - \lim_{t\to 0+} y'(t)\right) + \tfrac{1}{s-1}$$

a druhou potom na

$$s\mathcal{L}(x)(s) - \lim_{t\to 0+} x(t) + 2\mathcal{L}(x)(s) =$$
$$= -\mathcal{L}(y)(s) + s\mathcal{L}(y)(s) - \lim_{t\to 0+} y(t) + \tfrac{1}{s+1}.$$

Vyčíslíme-li limity (dle počátečních podmínek), obdržíme lineární rovnice

$$s^2\mathcal{L}(x)(s) - 1 + s\mathcal{L}(x)(s) = \mathcal{L}(y)(s) - s^2\mathcal{L}(y)(s) + \tfrac{1}{s-1}$$

a

$$s\mathcal{L}(x)(s) + 2\mathcal{L}(x)(s) = -\mathcal{L}(y)(s) + s\mathcal{L}(y)(s) + \tfrac{1}{s+1}$$

$$Y'(t) = A\cdot Y(t) \tag{8.12}$$

s konstantní maticí $A \in \mathrm{Mat}_n(\mathbb{R})$. Kombinací našich znalostí z lineární algebry a z analýzy funkcí jedné proměnné můžeme přímo uhádnout řešení, jestliže definujeme tzv. *exponentu matice* předpisem

$$B(t) = \mathrm{e}^{tA} = \sum_{k=0}^{\infty} \frac{t^k}{k!}A^k.$$

Na výraz napravo přitom můžeme formálně nahlížet jako na matici, jejímiž komponentami $b_{ij}$ jsou nekonečné řady vzniklé z uvedených součinů. Jestliže odhadneme všechny komponenty v $A$ maximem jejich absolutních hodnot $\|A\| = C$, pak pro $k$-tý sčítanec v $b_{ij}(t)$ dostaneme v absolutní hodnotě odhad $\frac{t^k}{k!}n^kC^k$. Nutně tedy je každá řada $b_{ij}(t)$ absolutně a stejnoměrně konvergentní a je shora ohraničena hodnotou $\mathrm{e}^{mC}$. Když zkusíme derivovat členy naší řady člen po členu, dostaneme stejnoměrně konvergentní řadu s limitou $A\,\mathrm{e}^{tA}$. Bude proto, podle obecných vlastností stejnoměrně konvergentních řad, tomuto výrazu rovna i derivace

$$\frac{d}{dt}\left(\mathrm{e}^{tA}\right) = A\,\mathrm{e}^{tA}\,.$$

Tím jsme získali obecné řešení našeho systému (8.12) ve tvaru

$$Y(t) = \mathrm{e}^{tA}\cdot Z\,,$$

kde $Z \in \mathrm{Mat}_n(\mathbb{R})$ je libovolná konstantní matice. Skutečně, exponenta $\mathrm{e}^{tA}$ je invertibilní maticí pro všechna $t$, a proto jsme tak dostali vektorový prostor správné dimenze a tudíž všechna obecná řešení.

Pozoruhodné je, že pokud řešíme jen vektorovou rovnici s konstantní maticí $A \in \mathrm{Mat}_n(\mathbb{R})$, $y'(t) = A\cdot y(t)$, pro neznámou funkci $y : \mathbb{R} \to \mathbb{R}^n$, pak exponenta $\mathrm{e}^{tA}$ zadá $n$ lineárně nezávislých řešení pomocí svých $n$ sloupců. Obecné řešení pak opět obdržíme jako jejich libovolnou lineární kombinaci.



Závěrem si připomeňme, že jsme maticový systém prvního řádu potkali v odstavci 8.54, když jsme přemýšleli o derivací řešení vektorové rovnice podle počátečních podmínek. Uvažme nyní diferencovatelné vektorové pole $X(x)$ definované na okolí bodu $x_0 \in \mathbb{R}^n$ takové, že $X(x_0) = 0$. Potom je bod $x_0$ pevným bodem jeho toku $\mathrm{Fl}_t^X(x)$.

Pro diferenciál $\Phi(t) = D_x\,\mathrm{Fl}_t^X(x_0)$ platí (viz (e8.42b) na straně 501)

$$\Phi'(t) = D^1X(x_0)\cdot\Phi(t), \quad \Phi(0) = E.$$

Známe tedy explicitně evoluci diferenciálu toku vektorového pole v jeho singulárním bodě $x_0$, která je dána exponentou

$$\Phi(t) = \mathrm{e}^{tA}, \quad A = D^1X(x_0).$$

To je užitečný krok k úvahám o kvalitativním chování v okolí stacionáního bodu $x_0$.

**8.60. Poznámka o Markovových řetězcích.** Ve třetí kapitole



jsme se zabývali iterativními procesy a významnou roli tam hrály tzv. stochastické matice a jimi zadané Markovovy procesy. Připomeňme, že matice $A$ je stochastická, jestliže součet každého jejího sloupce dá jedničku. Jinými slovy, platí

$$(1\ \ldots\ 1)\cdot A = (1\ \ldots\ 1).$$

s právě jedním řešením

$$\mathcal{L}(x)(s) = \tfrac{2s-1}{2(s-1)(s+1)^2}, \quad \mathcal{L}(y)(s) = \tfrac{3s}{2(s^2-1)^2}.$$

Opět si pomůžeme rozkladem na parciální zlomky se ziskem

$$\mathcal{L}(x)(s) = \tfrac{1}{8}\tfrac{1}{s-1} + \tfrac{3}{4}\tfrac{1}{(s+1)^2} - \tfrac{1}{8}\tfrac{1}{s+1} = \tfrac{3}{4}\tfrac{1}{(s+1)^2} + \tfrac{1}{4}\tfrac{1}{s^2-1}.$$

Neboť již dříve jsme vypočítali

$$\mathcal{L}\left(t\,\mathrm{e}^{-t}\right)(s) = \tfrac{1}{(s+1)^2}, \quad \mathcal{L}(\sinh t)(s) = \tfrac{1}{s^2-1},$$
$$\mathcal{L}(t\sinh t)(s) = \tfrac{2s}{(s^2-1)^2},$$

dostáváme

$$x(t) = \tfrac{3}{4}\,t\,\mathrm{e}^{-t} + \tfrac{1}{4}\sinh t, \quad y(t) = \tfrac{3}{4}\,t\sinh t.$$

Čtenář může sám ověřit, že tyto funkce $x$ a $y$ jsou skutečně hledaným řešením. Ověření však důrazně doporučujeme provést (např. z toho důvodu, že Laplaceovy transformace funkcí $y = \mathrm{e}^t$, $y = \sinh t$ a $y = t\sinh t$ jsme získali pouze pro $s > 1$). □

**8.154.** Najděte řešení soustavy diferenciálních rovnic:

$$x'(t) = -2x(t) + 3y(t) + 3t^2,$$
$$y'(t) = -4x(t) + 5y(t) + e^t, \quad x(0) = 1,\ y(0) = -1$$

**Řešení.**

$$\mathcal{L}(x')(s) = \mathcal{L}(-2x + 3y + 3t^2)(s),$$
$$\mathcal{L}(y')(s) = \mathcal{L}(-4x + 5y + e^t)(s).$$

Přitom levé strany lze zapsat pomocí (‖8.11‖) a pravé lze rozepsat vzhledem k linearitě operátoru $\mathcal{L}$. Protože $\mathcal{L}(3t^2)(s) = \frac{6}{s^3}$ a $\mathcal{L}(e^t)(s) = \frac{1}{s-1}$ dostáváme systém lineárních rovnic

$$s\mathcal{L}(x)(s) - 1 = -2\mathcal{L}(x)(s) + 3\mathcal{L}(y)(s) + \tfrac{6}{s^3},$$
$$s\mathcal{L}(y)(s) + 1 = -4\mathcal{L}(x)(s) + 5\mathcal{L}(y)(s) + \tfrac{1}{s-1}.$$

Po úpravě dostaneme maticově $\mathbf{A}(s)\hat{\mathbf{x}}(s) = \mathbf{b}(s)$, kde jsme označili $\mathbf{A}(s) = \begin{pmatrix} s+2 & -3 \\ 4 & s-5 \end{pmatrix}$, $\hat{\mathbf{x}}(s) = \begin{pmatrix} \mathcal{L}(x)(s) \\ \mathcal{L}(y)(s) \end{pmatrix}$ a $\mathbf{b}(s) = \begin{pmatrix} 1 + \frac{6}{s^3} \\ -1 + \frac{1}{s-1} \end{pmatrix}$. Cramerovo pravidlo říká, že

$$\mathcal{L}(x)(s) = \tfrac{|\mathbf{A}_1|}{|\mathbf{A}|}, \quad \mathcal{L}(y)(s) = \tfrac{|\mathbf{A}_2|}{|\mathbf{A}|}, \text{ kde}$$

$$|\mathbf{A}| = \begin{vmatrix} s+2 & -3 \\ 4 & s-5 \end{vmatrix} = s^2 - 3s + 2,$$
$$|\mathbf{A}_1| = \begin{vmatrix} 1+\frac{6}{s^3} & -3 \\ -1+\frac{1}{s-1} & s-5 \end{vmatrix} = (s-5)(1+\tfrac{6}{s^3}) + 3(-1+\tfrac{1}{s-1})$$
$$|\mathbf{A}_2| = \begin{vmatrix} s+2 & 1+\frac{6}{s^3} \\ 4 & -1+\frac{1}{s-1} \end{vmatrix} = (s+2)(-1+\tfrac{1}{s-1}) - 4 - \tfrac{24}{s^3}.$$

Odtud

$$\mathcal{L}(x)(s) = \frac{1}{(s-1)(s-2)}\left(\frac{(s-5)(s^3+6)}{s^3} - 3\frac{s-2}{s-1}\right),$$

Jestliže vezmeme exponentu $\mathrm{e}^{tA}$, dostaneme

$$(1\ \ldots 1)\cdot \mathrm{e}^{tA} = \sum_{k=0}^{\infty} \frac{t^k}{k!}(1\ \ldots 1)\cdot A^k = \mathrm{e}^t(1\ \ldots 1).$$

Je tedy pro každé $t$ invertibilní matice $B(t) = \mathrm{e}^{-t}\,\mathrm{e}^{tA}$ stochastická. Dostaneme tak spojitou verzi Markovova procesu (infinitesimálně) generovaného stochastickou maticí $A$.

Skutečně, derivací podle $t$ dostaneme

$$\frac{d}{dt}B(t) = -\mathrm{e}^{-t}\,\mathrm{e}^{tA} + \mathrm{e}^{-t}\,A\,\mathrm{e}^{tA} = (-E + A)B(t),$$

je tedy matice $B(t)$ řešením maticového systému rovnic s konstantními koeficienty

$$Y'(t) = (A - E)\cdot Y(t)$$

se stochastickou matici $A$. To má vcelku zřejmé intuitivní vysvětlení. Když je $A$ stochastická, pak okamžitý přírůstek vektoru $y(t)$ ve vektorovém systému s maticí $A$, $y'(t) = A\cdot y(t)$, je opět stochastický vektor. My ale pro Markovův proces chceme, aby vektor $y(t)$ zůstával stochastický pro všechna $t$. Součet přírůstků jednotlivých komponent vektoru $y(t)$ tedy musí být nulový a to zajišťuje odečtení jednotkové matice.

Jak jsme již viděli výše, maticové řešení $Y'(t)$ má ve svých sloupcích bázi všech řešení $y'(t)$ vektorového sytému.

Předpokládejme nyní navíc, že je matice $A$ primitivní, tj. nějaká její mocnina má samé positivní komponenty, viz 3.19 na straně 139. Pak víme, že její mocniny konvergují k matici $A_\infty$, která má ve všech svých sloupcích vlastní vektor k vlastnímu číslu 1. Jistě proto existuje univerzální konstantní odhad pro všechny mocniny $\|A^k - A_\infty\| \le C$ a pro každé malé kladné $\varepsilon$ existuje $N \in \mathbb{N}$ tak, že pro všechna $k \ge N$ máme již $\|A^k - A_\infty\| \le \varepsilon$. Můžeme nyní odhadnou rozdíl mezi řešením $Y'(t)$ pro velká $t$ a konstantní maticí $A_\infty$

$$\left\|\mathrm{e}^{-t}\sum_{k=0}^{\infty}\frac{t^k}{k!}A^k - \mathrm{e}^{-t}\sum_{k=0}^{\infty}\frac{t^k}{k!}A_\infty\right\| \le \mathrm{e}^{-t}\sum_{k<N}\frac{t^k}{k!}C\|A_\infty\| + \mathrm{e}^{-t}\,\varepsilon\|A_\infty\|.$$

Limitu výrazu $f(t) = \mathrm{e}^{-t}\sum_{k<N}\frac{t^k}{k!}$ lze snadno spočíst iterovaným použitím L'Hospitalova pravidla. Skutečně, derivací sumy dostaneme totéž, ale s $N$ o jedničku menším, derivace ve jmenovateli se nemění, je tedy limita nulová. Proto k našemu zvolenému $\varepsilon$ jistě najdeme i $T$ tak, aby $f(t)$ bylo pro $t \ge T$ již menší než $\varepsilon$. Celý výraz jsme tedy odhadli (pro $n \ge N$ a $t \ge T > 0$) číslem $\varepsilon(C+1)\|A_\infty\|$.

Dokázali jsem tak velmi zajímavé tvrzení, které hodně připomíná diskrétní variantu Markovových procesů:

### Spojité procesy se stochastickou maticí

**Věta.** *Každá primitivní stochastická matice $A$ zadává vektorový systém rovnic*

$$y'(t) = (A - E)\cdot y(t)$$

*s následujícími vlastnostmi*

*(1) báze vektorového prostoru všech řešení je dána sloupci ve stochastické matici*

$$Y(t) = \mathrm{e}^{-t}\,e^{tA},$$

$$\mathcal{L}(y)(s) = \frac{1}{(s-1)(s-2)}\left(\frac{(s+2)(2-s)}{s-1} - \frac{4s^3+24}{s^3}\right).$$

Rozkladem na parciální zlomky vyjádříme Laplaceovy obrazy řešení

$$\mathcal{L}(x)(s) = -\tfrac{39}{2s^2} - \tfrac{3}{(s-1)^2} + \tfrac{28}{s-1} - \tfrac{21}{4(s-2)} - \tfrac{15}{s^3} - \tfrac{87}{4s},$$

$$\mathcal{L}(x)(s) = -\tfrac{18}{s^2} - \tfrac{3}{(s-1)^2} + \tfrac{27}{s-1} - \tfrac{7}{s-2} - \tfrac{12}{s^3} - \tfrac{21}{s}$$

a zpětnou transformací dostáváme řešení Cauchyovy úlohy:

$$x(t) = -\tfrac{39}{2}t - 3te^t + 28e^t - \tfrac{21}{4}e^{2t} - \tfrac{15}{2}t^2 - \tfrac{87}{4},$$
$$y(t) = -18t - 3te^t + 27e^t - 7e^{2t} - 6t^2 - 21\,. \qquad \square$$

## O. Rovnice vedení tepla

**8.155.** Nalezněte řešení tzv. rovnice vedení tepla (rovnice difuze)

$$u_t(x,t) = a^2\, u_{xx}(x,t), \quad x \in \mathbb{R},\ t > 0$$

splňující počáteční podmínku $\lim\limits_{t\to 0+} u\,(x,t) = f(x)$.

Poznámky: Symbolem $u_t = \frac{\partial u}{\partial t}$ zde rozumíme parciální derivaci funkce $u$ podle $t$ (tj. derivujeme podle $t$, přičemž $x$ považujeme za konstantní) a podobně $u_{xx} = \frac{\partial^2 u}{\partial x^2}$ označuje druhou parciální derivaci podle $x$ (kdy dvakrát derivujeme podle $x$ a na $t$ nahlížíme při derivování jako na konstantu). Fyzikální interpretací úlohy je, že se snažíme určit teplotu $u(x,t)$ v tepelně izolované a homogenní tyči nekonečné délky (rozsah proměnné $x$), je-li dána počáteční teplota tyče funkcí $f$. Tyč má konstantní průřez a teplo se v ní může šířit pouze vedením. Koeficient $a^2$ je pak roven podílu $\frac{\alpha}{c\varrho}$, kde $\alpha$ je koeficient tepelné vodivosti, $c$ je specifické teplo a $\varrho$ je hustota. Zvláště se tedy předpokládá, že $a^2 > 0$.

**Řešení.** Na rovnici vedení tepla aplikujeme Fourierovu transformaci vzhledem k proměnné $x$. Platí ovšem

$$\mathcal{F}\,(u_t)\,(\omega,t) = \tfrac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{\infty} u_t(x,t)\,\mathrm{e}^{-i\omega x}\,dx =$$
$$= \left(\tfrac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{\infty} u\,(x,t)\,\mathrm{e}^{-i\omega x}\,dx\right)',$$

kde je derivováno podle $t$, tj. je

$$\mathcal{F}\,(u_t)\,(\omega,t) = (\mathcal{F}\,(u)\,(\omega,t))' = (\mathcal{F}\,(u))_t\,(\omega,t).$$

Současně víme, že

$$\mathcal{F}\left(a^2\,u_{xx}\right)(\omega,t) = a^2\,\mathcal{F}\,(u_{xx})\,(\omega,t) = -a^2\omega^2\,\mathcal{F}\,(u)\,(\omega,t).$$

Při označení $y(\omega,t) = \mathcal{F}\,(u)\,(\omega,t)$ tak přecházíme k rovnici

$$y_t = -a^2\omega^2\,y.$$

Podobnou diferenciální rovnici jsme již při počítání Fourierových transformací řešili, a tudíž pro nás není obtížné stanovit všechna její řešení

$$y(\omega,t) = K\,(\omega)\,\mathrm{e}^{-a^2\omega^2 t}, \quad K\,(\omega) \in \mathbb{R}.$$

Zbývá určit $K(\omega)$. Transformace počáteční podmínky dává

*(2) je-li počáteční podmínka $y_0 = y(t_0)$ stochastický vektor, pak i řešení $y(t)$ je stochastický vektor pro všechna $t$,*

*(3) každé stochastické řešení konverguje pro $t \to \infty$ k vlastnímu vektoru $y_\infty$ matice $A$ příslušnému vlastnímu číslu 1 matice $A$.*

**8.61. Poznámky o parciálních diferenciálních rovnicích.**



V praktických úlohách se velice často potkáváme s rovnicemi, které dávají do vztahů neznámé funkce více proměnných a jejich derivací. Jestliže jme tedy u obyčejných rovnic pracovali v nejobecnější poloze s vektorovou rovnicí

$$F(x, \dot{x}, \ddot{x}, \dddot{x}, \dots) = 0,$$

kde tečky nad vektorem proměnných $x \in \mathbb{R}^n$ označují (násobné) derivace podle dodatečné proměnné $t$, a cílem bylo najít křivku $x(t)$ vyhovující po dosazení rovnici. Proměnná $t$ v $F$ nevystupuje pouze proto, že ji vždy umíme schovat do vektorové proměnné $x$ jako souřadnici $x_0 = t$ (s přidanou rovnicí $\dot{x}_0 = 1$).

Nyní místo jedné proměnné $t$ bychom tedy chtěli umět pracovat podobně s rovnicemi

$$F((u, u_x, u_y, u_{xx}, u_{xy}, u_{yy}, \dots) = 0,$$

kde $u$ je neznámá funkce dvou proměnných $x$ a $y$ a indexy naznačují parciální derivace. Už v tomto nejjednodušším případě ale nejsou k dispozici obecné věty o jednoznačnosti a existenci řešení v obdobě k obyčejným diferenciálním rovnicím.

Stejně jako u obyčejných rovnic přitom můžeme také uvažovat vektorové formulace (jak pro $F$ tak pro $u$). Hovoříme pak také o systémech parciálních diferenciálních rovnic.

V praktickém užití se nejvíce objevují rovnice prvního a druhého řádu, tj. případy, kdy v definiční rovnici nevystupují parciální derivace řádů vyšších. Jde o velice složitou tématiku, která vyžaduje silné matematické nástroje a my se zde omezíme jen na několik jednoduchých poznámek a pozorování.

Začněme s tou nejjednodušší zajímavou možností jedinou rovnicí pro skalární funkci $f(x,y)$ ve tvaru

$$a(u,x,y)u_x + b(u,x,y) = 0,$$

kde $a$ a $b$ jsou známé funkce tří proměnných, $u$ je hledané řešení. Zpravidla takový problém řešíme na nějaké oblasti $D \subset \mathbb{R}^2$ s hranicí $\partial D$ (která bude v tomto případě křivkou).

Vcelku přirozený nápad je snažit se najít nějaké řešení podél jednotlivých křivek z vhodné soustavy, které nám vyplní celou oblast $D$. Díky nulovosti pravé strany se přímo podbízí hledat křivky, na nichž bude řešení $u$ konstantní. Pokud zároveň nebudou tyto křivky tečné k hranici $\partial D$, budeme umět minimálně na nějakém okolí rozšířit hraniční hodnotu $u_0$ konstantně podél takové křivky.

Derivací $u(c(t))$ podle $t$ dostaneme

$$0 = \frac{d}{dt}u(c(t)) = u_x(c(t))\dot{x}(t) + u_y(c(t))\dot{y}(t),$$

což nám dává systém rovnic pro hledané křivky

$$\dot{x} = a(u, x(t), y(t)), \quad \dot{y} = b(u, x(t), y(t)).$$

Ten má pro dostatečně diferencovatelné funkce $a$, $b$ a každou počáteční podmínku $x(0)$, $y(0)$ právě jedno řešení. Zkonstruovaným křivkám se říká *charakteristiky* parciální diferenciální rovnice prvního řádu, příslušné soustavě obyčejných diferenciálních rovnic pak *charakteristické rovnice*.

$$\mathcal{F}(f)(\omega) = \lim_{t\to 0+} \mathcal{F}(u)(\omega,t) = \lim_{t\to 0+} y(\omega,t) = K(\omega)\,\mathrm{e}^0 = K(\omega),$$

a proto je

$$y(\omega,t) = \mathcal{F}(f)(\omega)\,\mathrm{e}^{-a^2\omega^2 t}, \quad K(\omega)\in\mathbb{R}.$$

Nyní se pomocí inverzní Fourierovy transformace vraťme k původní diferenciální rovnici s řešením

$$u(x,t) = \tfrac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} y(\omega,t)\,\mathrm{e}^{i\omega x}\,d\omega =$$

$$= \tfrac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} \mathcal{F}(f)(\omega)\,\mathrm{e}^{-a^2\omega^2 t}\,\mathrm{e}^{i\omega x}\,d\omega =$$

$$= \tfrac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\left(\tfrac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(s)\,\mathrm{e}^{-i\omega s}\,ds\right)\mathrm{e}^{-a^2\omega^2 t}\,\mathrm{e}^{i\omega x}\,d\omega =$$

$$= \tfrac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(s)\left(\tfrac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\mathrm{e}^{-a^2\omega^2 t}\,\mathrm{e}^{-i\omega(s-x)}\,d\omega\right)ds.$$

Vypočítáním Fourierovy transformace $\mathcal{F}(f)$ funkce $f(t) = \mathrm{e}^{-at^2}$ pro $a > 0$ jsme při přeznačení proměnných obdrželi

$$\tfrac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\mathrm{e}^{-cp^2}\,\mathrm{e}^{-irp}\,dp = \tfrac{1}{\sqrt{2c}}\,\mathrm{e}^{-\frac{r^2}{4c}}, \quad c>0.$$

Dle tohoto vztahu (uvažte $c = a^2t > 0$, $p = \omega$, $r = s - x$) platí

$$\tfrac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\mathrm{e}^{-a^2\omega^2 t}\,\mathrm{e}^{-i\omega(s-x)}\,d\omega = \tfrac{1}{\sqrt{2a^2t}}\,\mathrm{e}^{-\frac{(s-x)^2}{4a^2t}},$$

a tedy

$$u(x,t) = \tfrac{1}{2a\sqrt{\pi t}}\int_{-\infty}^{\infty} f(s)\,\mathrm{e}^{-\frac{(x-s)^2}{4a^2t}}\,ds.$$

□

### P. Numerické řešení diferenciálních rovnic

Nyní uvádíme dva jednoduché příklady na využití Eulerovy metody při řešení diferenciálních rovnic.

**8.156.** Pomocí Eulerovy metody řešte rovnici $y' = -y^2$ s počáteční podmínkou $y(1) = 1$. Přibližné řešení určete na intervalu $[1,3]$. Pokuste se odhadnout, s pro jakou hodnotu kroku $h$ bude chyba menší než 0,1.

**Řešení.** Eulerova metoda pro uvedenou rovnici je dána vztahem

$$y_{k+1} = y_k - h\cdot y_k^2$$

pro

$$x_0 = 1, \quad y_0 = 1, \quad x_k = x_0 + k\cdot h, \quad y_k = y(x_k).$$

Začneme výpočet s krokem $h = 1$ a v každé iteraci tuto hodnotu vydělíme dvěma. Odhad „dostatečnosti“ $h$ uděláme poněkud nepřesně tak, že porovnáme dvě po sobě jdoucí přibližné hodnoty funkce $y$ ve společných bodech a výpočet zakončíme, pokud maximum absolutní hodnoty rozdílu těchto hodnot nebude větší než požadovaná přesnost 0,1.

Tím jsme v tomto případě problém vyřešili, protože když už jednou máme řešení charakteristických rovnic, nutně musí být řešení podél nich konstantní a řešení tak skutečně (lokálně) obdržíme. V okamžiku, kdy přidáme pravou stranu rovnice funkci $f(x,y)$ a píšeme $z = u(x,y)$, dává stejný postup dodatečnou podmínku

$$\dot x = a(u,x(t),y(t)),\ \dot y = b(u,x(t),y(t)),\ \dot z = f(x(t),y(t))$$

opět řešení $z(t) = u(x(t),y(t))$ podél každé charakteristiky $c(t) = (x(t),y(t))$. Skutečně, z naší konstrukce je zaručeno jak $\dot z = f$, tak $\dot z = u_x\dot x + u_y\dot y$, a proto je naše rovnice podél charakteristik splněna. To ale obecně neznamená, že takto zkonstruované $u$ je skutečně řešením původního problému. To musíme ověřit zkouškou.

Zkusme si úplně jednoduchý příklad s rovnicí

$$yu_x - xu_y = 0$$

a s počáteční podmínkou $u(x,0) = x$. Příslušné charakteristické rovnice jsme už viděli:

$$\dot x = y, \qquad \dot y = -x.$$

Řešení s počáteční podmínkou $x(0) = R$, $y(0) = 0$ je tvaru

$$x(t) = R\sin t,\ y(t) = R\cos t, u(t) = R.$$

Takto je dobře definovaná funkce $u(x,y)$ (v polárních souřadnicích) jen lokálně. Jednak to zjevně není diferencovatelná funkce v počátku souřadnic, také ale podél charakteristiky dojdeme z $(R,0)$ do bodu $(-R,0)$ a naše $u$ již nebude splňovat počáteční podmínky.

Stejné postupy můžeme (se stejnými potížemi) použít při vyšším počtu proměnných a také s vektorovými hodnotami. Jestliže budeme psát $\nabla u$ pro gradient vektorové funkce $u:\mathbb{R}^n\to\mathbb{R}^k$ a zvolíme libovolnou matici $A$ funkcí $a_{ij}(u,x)$ s $n$ sloupci a $\ell$ řádky, pak můžeme uvažovat homogenní rovnici

$$A(u,x)\cdot\nabla u = F(u,x).$$

Pro případ matice $A$ s jediným řádkem dostáváme obecnou obdobu předchozího příkladu. Nejblíže chování obyčejných diferenciálních rovnic budeme v případě, kdy je matice $A$ invertibilní. Pak ji můžeme převést na pravou stranu a dostaneme systém rovnic tvaru

$$\nabla u = G(u,x).$$

V souřadnicích můžeme totéž psát jako

$$u^p_i = \frac{\partial u^p}{\partial x_i}(u,x) = F^p_i(u,x).$$

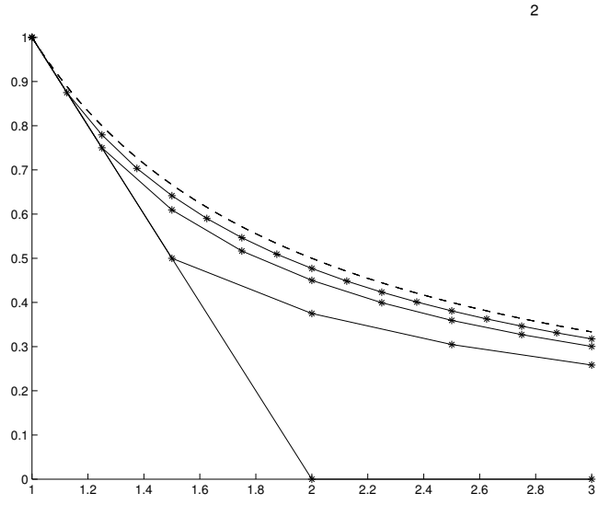
S počtením počtu podmínek a neznámých zjistíme, že pokud řešení existuje, bude lokálně zadáno počáteční podmínkou v jednom bodě (tj. velmi podobné chování jako v případě obyčejných diferenciálních rovnic). Vcelku přímočará geometrická analýza tohoto problému (tzv. Frobeniova věta) ukazuje, že evidentní nutná podmínka kompatibility

$$\frac{\partial^2 u^p}{\partial x_i\partial x_j} = \frac{\partial F^p_i}{\partial x_j} = \frac{\partial F^p_j}{\partial x_i}$$

je zároveň podmínkou dostatečnou.

| Výsledky |
|---|
| $h_0 = 1$ |
| $y^{(0)} = (1\ 0\ 0)$ |
| $h_1 = 0,5$ |
| $y^{(1)} = (1 \quad 0,5 \quad 0,375 \quad 0,3047 \quad 0,2583)$ |
| Maximální rozdíl: 0, 375. |
| $h_2 = 0,25$ |
| $y^{(2)} = (1.0000 \quad 0.7500 \quad 0.6094 \quad 0.5165 \quad 0.4498 \quad 0.3992$ $0.3594 \quad 0.3271 \quad 0.3004)$ |
| Maximální rozdíl: 0, 1094. |
| $h_3 = 0,125$ |
| $y^{(3)} = (1,0000 \quad 0,8750 \quad 0,7793 \quad 0,7034 \quad 0,6415 \quad 0,5901$ $0,5466 \quad 0,5092 \quad 0,4768 \quad 0,4484 \quad 0,4233 \quad 0,4009$ $0,3808 \quad 0,3627 \quad 0,3462 \quad 0,3312 \quad 0,3175)$ |
| Maximální rozdíl: 0.0322. |

Za použití vhodného programového vybavení lze získat následující grafickou prezentaci výsledků, kde čárkovaně je přesné řešení, jímž je funkce $y = 1/x$.




□

**8.157.** Pomocí Eulerovy metody řešte rovnici $y' = -2y$ s počáteční podmínkou $y(0) = 1$ s krokem $h = 1$. Vysvětlete jev, který nastane a navrhněte jiný postup.

**Řešení.** Eulerova metoda je v tomto případě dána vztahem

$$y_{k+1} = y_k - h \cdot 2y_k = -y_k.$$

Pro počáteční podmínku $y_0 = 1$ tak dostaneme jako výsledek střídání hodnot $\pm 1$. To je typický projev nestability metody při velké hodnotě kroku $h$. Pokud z nějakých důvodů nelze krok zmenšit (např při zpracování digitálních dat, kde krok je pevně určen), je možné dosáhnout lepších výsledků pomocí tzv. *implicitní Eulerovy metody*, Ta je obecně

**8.62. Poznámky o numerických metodách.** Kromě tak jednoduchých rovnic, jako jsou ty lineární s konstantními koeficienty se v praxi málo setkáváme s analyticky řešitelnými rovnicemi. Většinou proto potřebujeme postupy, jak přibližně spočíst řešení těch rovnic, se kterými pracujeme.

Už jsme podobné úvahy dělali všude tam, kde jsme se zabývali aproximacemi (tj. zejména lze doporučit porovnání s dřívějšími odstavci o splajnech, Taylorových polynomech a Fourierových řadách). S trochou odvahy můžeme také považovat diferenční a diferenciální rovnice za vzájemné aproximace. V jednom směru nahrazujeme diference diferenciály (např. u ekonomických nebo populačních modelů), ve druhém pak naopak.

Zastavíme se na chvilku u nahrazování derivací diferencemi. Nejdříve si však zavedeme obvyklé značení pro zápis odhadů chyb.

Připomeňme, že pro funkci $f(x)$ v proměnné $x$ říkáme, že je v okolí hromadného bodu $x_0$ svého definičního oboru *řádu velikosti* $O(\varphi(x))$ pro nějakou funkci $\varphi(x)$, jestliže existuje okolí $U$ bodu $x_0$ a konstanta $C$ taková, že

$$|f(x)| \leq C \cdot |\varphi(x)|$$

pro všechny $x \in U$. Limitní bod $x_0$ bývá často i nevlastní hodnota $\pm\infty$.

Nejobvyklejší příklady jsou $O(x^p)$ pro *polynomiální řád velikosti* a to v nule nebo v nekonečnu, $O(\ln x)$ pro *logaritmický řád velikosti* v nekonečnu atd. Všimněme si, že logaritmický řád velikosti nezávisí na volbě základu.

Dobrým příkladem je aproximace funkce jejím Taylorovým polynomem řádu $k$ v bodě $x_0$. Taylorova věta pro funkce jedné proměnné říká, že chyba této aproximace je $O(h^{k+1})$, kde $h$ je přírůstek argumentu $x - x_0 = h$.

Podobné úvahy jsme dělali i u Fourierových řad.

**8.63. Eulerova metoda.** V případě obyčejných diferenciálních rovnic je nejjednodušším schématem aproximace tzv. Eulerovými polygony. Budeme ji prezentovat pro jednu obyčejnou rovnici s jednou nezávislou a jednou závislou veličinou. Úplně stejně ale funguje pro systémy rovnic, když skalární veličiny a jejich derivace v čase $t$ nahradíme vektory závislé na času a jejich derivacemi.

Uvažujme tedy opět rovnici (pro jednoduchost a bez újmy na obecnosti prvního řádu)

$$y'(t) = f(t, y(t)).$$

Označme si diskrétní přírůstek času $h$, tj. $t_n = t_0 + nh$, a $y_n = y(t_n)$. Z Taylorovy věty (se zbytkem druhého řádu) a naší rovnice vyplývá, že

$$y_{n+1} = y_n + y'(t_n)h + O(h^2) = y_n + f(t_n, y_n)h + O(h^2).$$

Jestliže tedy od $t_0$ do $t_n$ uděláme $n$ takových kroků o přírůstek $h$, bude očekávaný odhad celkové chyby vyplývající z lokálních nepřesností naší lineární aproximace nejvýše $hO(h^2)$, tj. chyba bude v řádu velikosti $O(h)$. Ve skutečnosti vstupují při výpočtu do hry ještě zaokrouhlovací chyby.

Při numerickém řešení Eulerovou metodou postupujeme tak, že za přibližné řešení považujeme po částech lineární polygon definovaný výše.

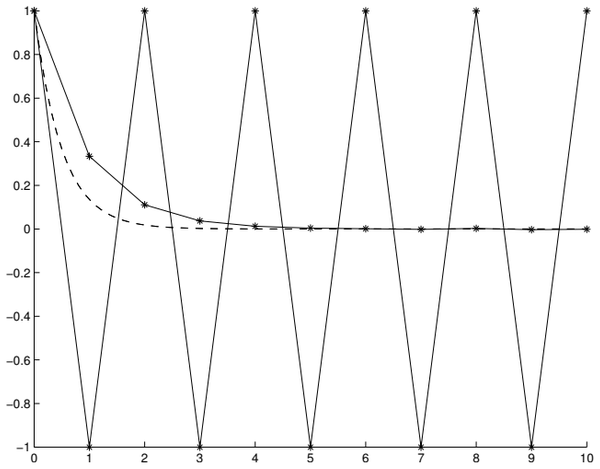
pro rovnici $y' = f(x, y)$ dána vztahem

$$y_{k+1} = y_k + h \cdot f(x_{k+1}, y_{k+1}),$$

v každém kroku tedy je v obecném případě potřeba řešit nelineární rovnici. Pro náš příklad ale dostáváme

$$y_{k+1} = y_k - 2h \cdot y_{k+1},$$

takže pro $h = 1$ máme $y_{k+1} = \frac{1}{3} y_k$. Získané výsledky je opět možné prezentovat graficky včetně přesného řešení rovnice.




□

Ve skutečnosti jsou při praktických úlohách skoro výlučně používány numerické metody řešení diferenciálních rovnic, obyčejných i parciálních. Jde o mimořádně širokou a teoreticky i prakticky zajímavou oblast výzkumu i použití matematických metod. Bohužel zde nemáme prostor pro podrobnější výklad.

## Q. Doplňující příklady k celé kapitole

*8.158.* Nádrž na 300 hl obsahuje 100 hl slané vody, v níž je rozpuštěno 50 kg soli. Do nádrže začne vtékat stálou rychlostí 6 hl/min slaná voda obsahující 2 kg soli na jeden hl. Směs, která je promícháváním neustále udržována homogenní, vytéká z nádrže neměnnou rychlostí 4 hl/min. Vyjádřete množství (v kg) soli v nádrži po uplynutí $t$ minut jako funkci proměnné $t \in [0, 100]$. ○

*8.159.* V rámci řízeného experimentu došlo k vyhasnutí malé experimentální tavící pece při konstantní okolní teplotě 300 K. Experiment začal ve 12.00. Ve 13.00 byla měřením odhadnuta teplota v peci na 1300 K a v 15.00 na 550 K. Za předpokladu, že tyto odhady teplot jsou přesné, vypočtěte teplotu v peci ve 14.00. ○

*8.160.* Poločas rozpadu radioaktivního izotopu síry $^{35}S$ je 87,5 dní. Po nějaké době zbylo z 1 kg tohoto izotopu pouze 90 dkg. Po jaké? (ve výsledku můžete používat funkce ln) ○

*8.161.* Poločas rozpadu radioaktivního prvku $A$ je pět let, prvku $B$ jeden rok. Máme-li 5 kg prvku $B$ a 1 kg prvku $A$, za jak dlouho budeme mít stejné množství obou? (ve výsledku můžete používat funkce ln) ○

*8.162.* Poločas rozpadu radioaktivního prvku $A$ je osm let, prvku $B$ dva roky. Máme-li 3 kg prvku $B$ a 1 kg prvku $A$, za jak dlouho budeme mít stejné množství obou? (ve výsledku můžete používat funkce ln) ○

*8.163.* Poločas rozpadu radioaktivního izotopu kobaltu $^{60}Co$ je 5,27 let. Za jak dlouho ubude kilogram ze čtyř kilogramů tohoto izotopu kobaltu? (ve výsledku můžete používat funkce ln) ○

*8.164.* Vyřešte diferenciální rovnici pro funkci $y = y(x)$:

$$y' = \frac{1 + y^2}{1 + x^2}.$$

○

*8.165.* Určete všechna řešení rovnice se separovanými proměnnými

$$y - y^2 + xy' = 0.$$

○

*8.166.* Vyřešte rovnici

$$1 + \tfrac{dy}{dx} = \mathrm{e}^y.$$

○

*8.167.* Vypočtěte rovnici $2y = x^3 y'$. ○

*8.168.* Stanovte všechna řešení rovnice

$$\sqrt{4 - y^2}\, dx + y\, dy = 0.$$

○

*8.169.* Řešte

$$y' \operatorname{tg} x = y^2 + 1 - 2y.$$

○

*8.170.* Stanovte obecné řešení diferenciální rovnice

$$\tfrac{x^2+1}{x} = \tfrac{y}{1-y^2}\, y'.$$

○

*8.171.* Napište obecné řešení diferenciální rovnice

$$(x+1)\,\mathrm{d}y + xy\,\mathrm{d}x = 0.$$

○

*8.172.* Najděte řešení diferenciální rovnice

$$\sin y \cos x\, dy = \cos y \sin x\, dx$$

splňující $4y(0) = \pi$. ○

*8.173.* Vyřešte počáteční úlohu

$$\left(x^2+1\right)\left(y^2-1\right) + xyy' = 0, \quad y(1) = \sqrt{2}.$$

○

*8.174.* Určete partikulární řešení rovnice

$$y' \sin x = y \ln y$$

procházející bodem $[\pi/2, \mathrm{e}]$. ○

*8.175.* Nalezněte všechna řešení diferenciální rovnice

$$2\,(1+\mathrm{e}^x)\, yy' = \mathrm{e}^x,$$

která splňují podmínku $y(0) = 0$. ○

*8.176.* Vyřešte homogenní rovnici

$$\left(xy' - y\right)\cos\tfrac{y}{x} = x.$$

○

*8.177.* Určete obecné řešení homogenní diferenciální rovnice $y^3 = x^3\, y'$. ○

*8.178.* Nalezněte všechna řešení rovnice

$$xy' = \sqrt{x^2 - y^2} + y.$$

○

*8.179.* Určete obecné řešení, je-li zadáno

$$xy' = y\cos\left(\ln\tfrac{y}{x}\right).$$

*8.180.* Jako homogenní řešte rovnici $(x + y)\,dx - (x - y)\,dy = 0$.

*8.181.* Vypočítejte $y' = (x + y)^2$.

*8.182.* Uveďte obecné řešení pro

$$y' = \tfrac{x-y+3}{x+y-5}.$$

*8.183.* Spočtěte

$$y' = \tfrac{x-y+1}{x-y}.$$

*8.184.* Určete všechna řešení diferenciální rovnice

$$y' = \tfrac{5y-5x-1}{2y-2x-1}.$$

*8.185.* Najděte obecné řešení následující rovnice

$$y' = \tfrac{x-y-1}{x+y+3}.$$

*8.186.* Stanovte obecné řešení pro rovnici

$$y' = \tfrac{2x-y-5}{x-3y-5}.$$

*8.187.* Jako explicitně dané funkce vyjádřete řešení rovnice

$$y' = \tfrac{x+2y-7}{x-3}.$$

*8.188.* Metodou variace konstant vypočtěte $y' + 2y = x$.

*8.189.* Určete obecné řešení rovnice $y' = 6x + 2y + 3$.

*8.190.* Vyřešte lineární rovnici

$$y' = 4xy + (2x + 1)\mathrm{e}^{2x^2}.$$

*8.191.* Řešte rovnici $y'x + y = x \ln x$.

*8.192.* Vypočtěte lineární diferenciální rovnici

$$y'x = y + x^2 \ln x.$$

○

*8.193.* Stanovte všechna řešení rovnice

$$y' \cos x = (y + 2\cos x) \sin x.$$

○

*8.194.* Najděte řešení rovnice $y' = 6x - 2y$, které vyhovuje počáteční podmínce $y(0) = 0$. ○

*8.195.* Vypočtěte počáteční problém

$$y' + y \sin x = \sin x, \quad y\left(\tfrac{\pi}{2}\right) = 2.$$

○

*8.196.* Uveďte řešení rovnice $y' = 4y + \cos x$, které prochází bodem $[0, 1]$. ○

*8.197.* Pro libovolné $a, b \in \mathbb{R}$ řešte

$$xy' + y = \mathrm{e}^x, \quad y(a) = b.$$

○

*8.198.* Stanovte obecné řešení rovnice

$$3x^2 y' + xy = \tfrac{1}{y^2}.$$

○

*8.199.* Řešte Bernoulliho rovnici

$$y' = xy - y^3 \mathrm{e}^{-x^2}.$$

○

*8.200.* Vypočtěte Bernoulliho rovnici

$$y' - \tfrac{y}{x} = y^2 \sin x.$$

○

*8.201.* Najděte všechna řešení rovnice

$$y' = \tfrac{4y}{x} + x\sqrt{y}.$$

○

*8.202.* Řešte rovnici

$$xy' + 2y + x^5 y^3 \mathrm{e}^x = 0.$$

○

*8.203.* Pro $a, b > 0$ stanovte obecné řešení

$$y\,dy = \left(a\,\tfrac{y^2}{x^2} + b\,\tfrac{1}{x^2}\right) dx.$$

○

*8.204.* Záměnou proměnných řešte

$$2y + \left(y^2 - 6x\right) y' = 0.$$

○

*8.205.* Vyřešte rovnici

$$y' = \tfrac{y}{2y \ln y + y - x}.$$

○

*8.206.* Spočítejte obecné řešení následující rovnice

$$x\,dx = \left(\tfrac{x^2}{y} - y^3\right) dy.$$

○

*8.207.* Záměnou proměnných vypočtěte

$$(x + y)\,dy = y\,dx + y \ln y\,dy.$$

○

*8.208.* Řešte

$$y' \left(\mathrm{e}^{-y} - x\right) = 1.$$

○

*8.209.* Spočítejte

$$y' = \tfrac{1}{2x - y^2}.$$

○

*8.210.* Vyřešte rovnici

$$2y\,dx + x\,dy = 2y^3\,dy.$$

○

*8.211.* Spočtěte

$$y'' + 3y' + 2y = (20x + 29)\,\mathrm{e}^{3x}.$$

○

*8.212.* Uveďte libovolné řešení nehomogenní lineární rovnice

$$y'' + y' + \tfrac{5}{2}\,y = 25 \cos(2x)\,.$$

○

*8.213.* Určete řešení rovnice

$$y'' + 2y' + 2y = 3\mathrm{e}^{-x}\cos x.$$

○

*8.214.* Nalezněte obecné řešení rovnice

$$y'' = 2y' + y + 1,$$

splňující $y(0) = 0$ a $y'(0) = 1$. ○

*8.215.* Nalezněte obecné řešení rovnice

$$y'' = 4y - 3y' + 1,$$

splňující $y(0) = 0$ a $y'(0) = 2$. ○

*8.216.* Stanovte obecné řešení lineární rovnice

$$y'' - 2y' + 5y = 5\mathrm{e}^{2x}\sin x.$$

○

*8.217.* Využitím speciálního tvaru pravé strany určete všechna řešení rovnice

$$y'' + y' = x^2 - x + 6\mathrm{e}^{2x}.$$

○

*8.218.* Vyřešte

$$y^{(4)} - 2y'' + y = 8\left(\mathrm{e}^{x} + \mathrm{e}^{-x}\right) + 4\left(\sin x + \cos x\right).$$

○

*8.219.* Metodou variace konstant vypočtěte

$$y'' - 2y' + y = \tfrac{\mathrm{e}^{x}}{x}.$$

○

*8.220.* Řešte

$$y'' + 4y' + 4y = \mathrm{e}^{-2x}\ln x.$$

○

*8.221.* Pomocí metody variace konstant najděte obecné řešení pro rovnici

$$y'' + 4y = \tfrac{1}{\sin(2x)}.$$

○

*8.222.* Vyřešte rovnici $y'' + y = \operatorname{tg}^2 x$. ○

*8.223.* Nalezněte řešení diferenciální rovnice

$$y^{(3)} = -2y'' - 2y' - y + \sin(x),$$

splňující $y(0) = -\frac{1}{2}$, $y'(0) = \frac{\sqrt{3}}{2}$ a $y''(0) = -1 - \frac{\sqrt{3}}{2}$. ○

*8.224.* Vypočtěte rovnici $y''' - 2y'' - y' + 2y = 0$. ○

*8.225.* Uveďte obecné řešení pro rovnici

$$y^{(4)} + 2y'' + y = 0.$$

○

*8.226.* Vyřešte

$$y^{(6)} + 2y^{(5)} + 4y^{(4)} + 4y''' + 5y'' + 2y' + 2y = 0.$$

○

*8.227.* Najděte obecné řešení lineární rovnice

$$y^{(5)} - 3y^{(4)} + 2y''' = 8x - 12.$$

○

### Řešení cvičení

*8.21.* Jak čtenář snadno nahlédne, Taylorův polynom daného stupně funkce dané mnohočlenem více neznámých, je mnohočlen sám, případně ořezaný o vyšší mocniny. Tedy v tomto případě $T(x, y, z) = xz^2 + xy + 1$.

*8.22.* $T(x, y) = y^2$. Rovnice tečná roviny je dána lineární částí Taylorova polynomu, tj. $z = 0$, zadaný bod v ní neleží.

*8.23.* $T^2_{\ln(xy+1)}(1, 1) = \ln(2) + \frac{1}{4}(x^2 + y^2 + xy - x - y - 1)$.

*8.24.* y+xy.

*8.32.* Stacionární body $(\pm\frac{1}{2}, \mp 1, \pm\frac{1}{8})$. Hessiány jsou v obou indefinitní, extrém nenastává.

*8.33.* Stac. body $[\mp 2, \pm 1, \pm 2]$, Hessián je v obou indefinitní, extrémy v těchto bodech nejsou.

*8.34.* Stac. body $[\pm\frac{1}{8}, \pm 1, \mp\frac{1}{2}]$, Hessiány jsou v těchto bodech indefinitní, extrémy nenastávají.

*8.35.* Stac. body $[\pm 2, \mp 2, \pm 1]$, extrémy v nich nenastávají.

*8.36.* Stacionární body: $(0, -1/4)$, $(\pm\sqrt{3}, -1)$, minimum v bodě $(0, -1/4)$.

*8.37.* Stacionární body: $(0, -1/2)$, Hessián v tomto bodě indefinitní, nemá extrém.

*8.38.* Globální minimum je v bodě $(1/7, -2/7)$.

*8.39.* Stacionární bod $(-1/9, 2/9)$, Hessián v něm indefinitní, extrém nenastává.

*8.60.* V bodě $[\frac{1}{3}, \frac{1}{6}, -\frac{1}{6}]$, minimum.

*8.61.* V bodě $[-\frac{\sqrt{3}}{2}, \frac{3}{2}]$.

*8.62.* $[\frac{3}{2} + \frac{\sqrt{3}}{2}, -\frac{\sqrt[4]{3}}{\sqrt{2}}]$.

*8.63.* $[\frac{3}{2} + \frac{\sqrt{3}}{2}, -\frac{\sqrt[4]{3}}{\sqrt{2}}]$.

*8.64.* V bodech $[\pm\frac{1}{\sqrt{2}}, \mp\frac{1}{\sqrt{6}}]$.

*8.65.* V bodech $[\pm\frac{\sqrt{6}}{3}, -\frac{\sqrt{3}}{3}]$.

*8.66.* $3\sqrt{3}/16$.

*8.67.* $1/(2\sqrt{6})$.

*8.68.* $(1/\sqrt{2}, 1/2)$, $(-1/\sqrt{2}, -1/2)$.

*8.91.* $[0, \frac{8}{5}]$.

*8.92.* $[\frac{\sqrt{3}}{\pi}, \frac{1}{\pi}]$.

*8.93.* $[0, \frac{4}{3\pi}]$.

*8.94.* $[\frac{\sqrt{3}}{2\pi}, \frac{3}{2\pi}]$.

*8.95.* $V = \pi$.

*8.96.* $8\pi$.

*8.97.* $\frac{\sqrt{2}\pi}{3}$.

*8.98.* $4\sqrt{3}\pi - \frac{16}{3}\pi$.

*8.100.* $\frac{\pi}{6}(17\sqrt{17} - 1)$.

*8.101.* $\sqrt{6}(\pi/4 - 1/2)$.

*8.108.* $4\pi$.

*8.109.* $36\pi$.

*8.110.* $\frac{65\pi}{24}$.

*8.136.* $y = 1 - \frac{x^2}{4}$, $x \in (0, 2)$.

*8.137.* $Me^{-t/q}$.

*8.138.* $\frac{\sqrt{2}}{2}\sin(2t)$.

*8.158.* $2\,(100+2t)\,-\frac{15\cdot 10^5}{(100+2t)^2}$.

*8.159.* 800 K.

*8.160.* $-87{,}5\frac{\ln(0{,}9)}{\ln(2)} \doteq 13{,}3$ dne.

*8.161.* $\frac{5\ln(5)}{4\ln(2)}$.

*8.162.* $\frac{8\ln(3)}{3\ln(2)}$.

*8.163.* $5{,}27\frac{\ln(\frac{4}{3})}{\ln(2)}$.

*8.164.* $y=\frac{x+C}{1-Cx}$. (použijte součtového vzorce pro tangens).

*8.165.* $y\equiv 0$, $y=(1-Cx)^{-1}$, $C\in\mathbb{R}$.

*8.166.* $y=-\ln(1-Ce^{x})$, $C\in\mathbb{R}$.

*8.167.* $y=Ce^{-1/x^2}$, $C\in\mathbb{R}$.

*8.168.* $y\equiv 2$, $y\equiv -2$, $(x-C)^2+y^2=2^2$, $C\in\mathbb{R}$.

*8.169.* $y\equiv 1$, $y=1-\frac{1}{\ln|\sin x|+C}$, $C\in\mathbb{R}$.

*8.170.* $x^2+2\ln|x|+\ln\left|y^2-1\right|=C$, $C\in\mathbb{R}$.

*8.171.* $y=C\,(x+1)\,e^{-x}$, $C\in\mathbb{R}$.

*8.172.* $\sqrt{2}\cos y=\cos x$.

*8.173.* $y=\sqrt{\frac{e^{1-x^2}}{x^2}+1}$.

*8.174.* $y=e^{\operatorname{tg}(x/2)}$.

*8.175.* $y=\pm\sqrt{\ln(e^{x}+1)-\ln 2}$.

*8.176.* $x=Ce^{\sin\frac{y}{x}}$, $C\in\mathbb{R}$.

*8.177.* $y^2=x^2+Cx^2y^2$, $C\in\mathbb{R}$.

*8.178.* $y=x$, $y=-x$, $y=x\sin(\ln|Cx|)$, $C\in\mathbb{R}\setminus\{0\}$.

*8.179.* $\operatorname{cotg}\left(\frac{1}{2}\ln\frac{y}{x}\right)=\ln|Cx|$, $C\in\mathbb{R}\setminus\{0\}$.

*8.180.* $\operatorname{arctg}\frac{y}{x}=\ln\left(x^2+y^2\right)+C$, $C\in\mathbb{R}$.

*8.181.* $y=\operatorname{tg}(x+C)\,-x$, $C\in\mathbb{R}$.

*8.182.* $C=(x-1)^2-2(y-4)(x-1)-(y-4)^2$, $C\in\mathbb{R}\setminus\{0\}$.

*8.183.* $(x-y)^2+2x+C=0$, $C\in\mathbb{R}$.

*8.184.* $y=x$, $C=5x-2y+\ln|y-x|$, $C\in\mathbb{R}$.

*8.185.* $(x+1)^2-2(x+1)(y+2)-(y+2)^2=C$, $C\in\mathbb{R}\setminus\{0\}$.

*8.186.* $3(y+1)^2-2(y+1)(x-2)+2(x-2)^2=C$, $C\in\mathbb{R}\setminus\{0\}$.

*8.187.* $y=5-x+C(x-3)^2$, $C\in\mathbb{R}$.

*8.188.* $y=Ce^{-3x}+\frac{1}{3}x-\frac{1}{9}$, $C\in\mathbb{R}$.

*8.189.* $y=Ce^{2x}-3(x+1)$, $C\in\mathbb{R}$.

*8.190.* $y=\left(x^2+x+C\right)e^{2x^2}$, $C\in\mathbb{R}$.

*8.191.* $y=\frac{C}{x}+\frac{x\ln x}{2}-\frac{x}{4}$, $C\in\mathbb{R}$.

*8.192.* $y=Cx+x^2\ln x-x^2$, $C\in\mathbb{R}$.

*8.193.* $y=\frac{\sin^2 x+C}{\cos x}$, $C\in\mathbb{R}$.

*8.194.* $y=3x+\frac{3}{2}e^{-2x}-\frac{3}{2}$, $C\in\mathbb{R}$.

*8.195.* $y=e^{\cos x}+1$.

*8.196.* $y=\frac{1}{17}\sin x-\frac{4}{17}\cos x+\frac{21}{17}e^{4x}$.

*8.197.* $y = \frac{e^x+ab-e^a}{x}$.

*8.198.* $y^3 = \frac{\ln|x|+C}{x}$, $C \in \mathbb{R}$.

*8.199.* $y \equiv 0$, $y^2 = \frac{e^{x^2}}{2x+C}$, $C \in \mathbb{R}$.

*8.200.* $y \equiv 0$, $\frac{1}{y} = \frac{C}{x} + \cos x - \frac{\sin x}{x}$, $C \in \mathbb{R}$.

*8.201.* $y \equiv 0$, $y = x^4 \left(\frac{1}{2}\ln|x| + C\right)^2$, $C \in \mathbb{R}$.

*8.202.* $y \equiv 0$, $y^{-2} = x^4\,(2e^x + C)$, $C \in \mathbb{R}$.

*8.203.* $y^2 + \frac{b}{a} = Ce^{-\frac{2a}{x}}$, $C \in \mathbb{R}$.

*8.204.* $x = \frac{y^2}{2} + Cy^3$, $C \in \mathbb{R}$.

*8.205.* $x = y\ln y + \frac{C}{y}$, $C \in \mathbb{R}$.

*8.206.* $x^2 + y^2\left(y^2 - C\right) = 0$, $C \in \mathbb{R}$.

*8.207.* $x = y\ln y - \frac{y\ln^2 y}{2} + Cy$, $C \in \mathbb{R}$.

*8.208.* $x = (C + y)\,e^{-y}$, $C \in \mathbb{R}$.

*8.209.* $x = \frac{y^2}{2} + \frac{y}{2} + \frac{1}{4} + Ce^{2y}$, $C \in \mathbb{R}$.

*8.210.* $x = \frac{2}{7}y^3 + \frac{C}{\sqrt{y}}$, $C \in \mathbb{R}$.

*8.211.* $y = C_1e^{-2x} + C_2e^{-x} + (x+1)e^{3x}$, $C_1, C_2 \in \mathbb{R}$.

*8.212.* Např. $y = 8\sin(2x) - 6\cos(2x)$.

*8.213.* $y = e^{-x}\,(C_1\cos x + C_2\sin x) + \frac{3x}{2}\,e^{-x}\sin x$, $C_1, C_2 \in \mathbb{R}$.

*8.214.*

$$y = \frac{1}{2}e^{(1+\sqrt{2})x} + \frac{1}{2}e^{(1-\sqrt{2}x)x} - 1.$$

*8.215.* $y = \frac{3}{5}e^x - \frac{7}{20}e^{-4x} - \frac{1}{4}$.

*8.216.* $y = C_1e^x\cos(2x) + C_2e^x\sin(2x) + e^{2x}\left(\sin x - \frac{1}{2}\cos x\right)$, přičemž $C_1, C_2 \in \mathbb{R}$.

*8.217.* $y = C_1 + C_2e^{-x} + \frac{1}{3}x^3 - \frac{3}{2}x^2 + 3x + e^{2x}$, $C_1, C_2 \in \mathbb{R}$.

*8.218.* $y = (C_1 + C_2x)\,e^x + (C_3 + C_4x)\,e^{-x} + x^2\left(e^x + e^{-x}\right) + \cos x + \sin x$, $C_1, C_2, C_3, C_4 \in \mathbb{R}$.

*8.219.* $y = C_1e^x + C_2x\,e^x + x\,e^x\,(\ln|x| - 1)$, $C_1, C_2 \in \mathbb{R}$.

*8.220.* $y = C_1e^{-2x} + C_2x\,e^{-2x} + \frac{x^2}{2}\,e^{-2x}\ln x - \frac{3x^2}{4}\,e^{-2x}$, $C_1, C_2 \in \mathbb{R}$.

*8.221.* Pro $C_1, C_2 \in \mathbb{R}$ je $y = -\frac{x}{2}\cos(2x) + \frac{1}{4}\sin(2x)\ln|\sin(2x)| + C_1\cos(2x) + C_2\sin(2x)$.

*8.222.* $y = C_1\cos x + C_2\sin x - 2 + \frac{1}{2}\sin x\ln\left|\frac{1+\sin x}{1-\sin x}\right|$, $C_1, C_2 \in \mathbb{R}$.

*8.223.* $y(x) = -e^{-x} + e^{-\frac{1}{2}x}\sin(\frac{\sqrt{3}}{2}x) + e^{-\frac{1}{2}x}\cos(\frac{\sqrt{3}}{2}x) - \frac{1}{2}\sin(x) - \frac{1}{2}\cos(x)$.

*8.224.* $y = C_1e^x + C_2e^{-x} + C_3e^{2x}$, $C_1, C_2, C_3 \in \mathbb{R}$.

*8.225.* $y = C_1\cos x + C_2\sin x + C_3x\cos x + C_4x\sin x$, přičemž konstanty $C_1, C_2, C_3, C_4 \in \mathbb{R}$.

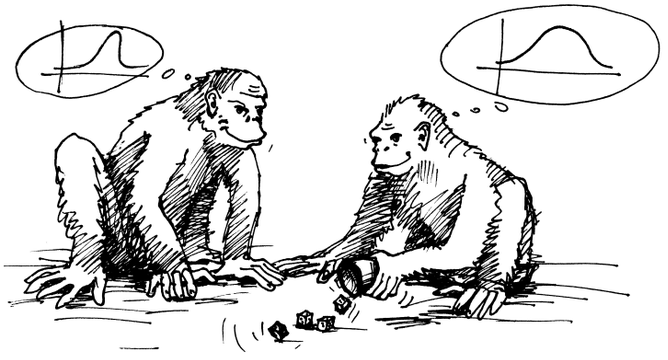
*8.226.* $y = \left(C_1 + C_3x + C_5e^{-x}\right)\cos x + \left(C_2 + C_4x + C_6e^{-x}\right)\sin x$, $C_1, C_2, C_3, C_4, C_5, C_6 \in \mathbb{R}$.

*8.227.* $y = C_1 + C_2x + C_3x^2 + C_4e^{2x} + C_5e^x + \frac{x^4}{6}$, přičemž konstanty $C_1, C_2, C_3, C_4, C_5 \in \mathbb{R}$.

KAPITOLA 9

# Statistické a pravděpodobnostní metody

*Je statistika částí matematiky?*
*– když ano, pak matematiky potřebuje moc…!*



## A. Tečky, čáry, obdélníčky

Získaná data z praxe můžeme zachytit různými způsoby. Uveďme několik základních.

**9.1. Zobrazování získaných dat.** U 20 matematiků bylo zjištěn počet členů domácnosti, ve které žijí. V tabulce je uvedena četnost, se kterou se dané počty členů domácnosti vyskytly.

| Počet členů | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Počet domácností | 5 | 5 | 1 | 6 | 2 | 1 |

Vytvořte tabulku rozložení četnost. Určete průměr, medián a modus počtu osob v domácnosti. Sestavte sloupcový diagram dat.

**Řešení.** Do tabulky rozložení četností zapíšeme nejen vlastní četnosti, ale i kumulativní četnosti a pravděpodobnosti, že s jakou má náhodně vybraná domácnost daný počet členů (tzv. relativní četnost). Možný počet členů domácnosti označíme $x_i$, odpovídající četnost pak $n_i$, relativní četnost $p_i$ $(= n_i / \sum_{j=1}^{6} n_j = n_i/20)$, kumulativní četnost $N_i$ $(= \sum_{j=1}^{i} x_j)$ a relativní kumulativní četnost

Statistika je, v širším slova smyslu, jakékoliv zpracování číselných nebo jiných dat o nějakém souboru objektů a jejich více či méně přehledná prezentace. V tomto smyslu hovoříme o *popisné statistice*. Jejím předmětem je tedy zpracování a zpřehledňování dat o objektech daného souboru, např. roční příjmy všech občanů zpracovávané z kompletních dat finančních úřadů.

Matematická statistika spočívá ve využití matematických metod pro odvozování závěrů platných pro celý (potenciálně nekonečný) soubor objektů na základě nějakého „malého“ vzorku. Např. zjišťujeme zatížení populace chorobami pomocí dat získaných u několika nahodile vybraných osob, chceme ale interpretovat výsledky ve vztahu k celé populaci.

Podstatou popisné statistiky je odvození jednoduchých (zpravidla) číselných charakteristik o velkých souborech dat, resp. jejich vhodná vizualizace. Podstatou matematické statistiky je pro prezentovaná data zjišťovat, jaké vlastnosti skutečně mají objekty, které jsou daty popisovány, a zároveň, jak věrohodné jsou odvozené výsledky. Zpravidla přitom jde o sběr a zpracování dat o nějakém souboru objektů, jejich následnou analýzu a, konečně, o vyslovení důsledků pozorování pro rozsáhlejší soubor objektů než jsou ty, jejichž data jsme zpracovávali. Ještě jinak řečeno, výsledkem použití matematické statistiky je sdělení o velkém souboru objektů na základě studia malé (zpravidla náhodně vybrané) části z nich, společně s kvalitativním odhadem věrohodnosti výsledného sdělení.

Matematická statistika je opřena hlavně o nástroje teorie pravděpodobnosti, které jsou velice užitečné (a zajímavé) i samy o sobě. Nejvíce úsilí budeme v dalším textu věnovat právě jim.

Celá tato kapitola poskytuje elementární úvod do metod pravděpodobnosti a statistiky, který by měl být dostatečný pro správné chápání běžných statistických informací všude kolem nás. Pro seriozní porozumění práci matematického statistika bude třeba sáhnout po dalších zdrojích.

### 1. Popisná statistika

Popisná statistika není sama o sobě matematická disciplína, byť používá četné manipulace s čísly a občas i velmi sofistikované metody. Je přitom ale dobrou příležitostí k ilustraci matematického přístupu k budování obecně užitečných nástrojů.

Zároveň by nám měla posloužit jako motivace pro řadu úvah v pravděpodobnosti, protože už budeme tušit, k čemu je později v matematické statice budeme potřebovat.

$F_i (= N_i/20 = \sum_{j=1}^{i} p_j)$:

| $x_i$ | $n_i$ | $p_i$ | $N_i$ | $F_i$ |
|---|---|---|---|---|
| 1 | 5 | 1/4 | 5 | 1/4 |
| 2 | 5 | 1/4 | 10 | 1/2 |
| 3 | 1 | 1/20 | 11 | 11/20 |
| 4 | 6 | 3/10 | 17 | 17/20 |
| 5 | 2 | 1/10 | 19 | 19/20 |
| 6 | 1 | 1/20 | 20 | 1 |

Snadno již také sestavíme požadované (sloupcové) grafy (relativních, kumulativních) četností:

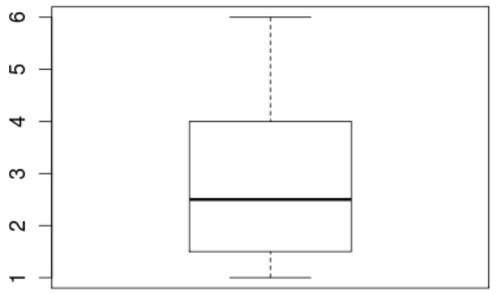
Snadno spočítáme průměr počtu osob v domácnosti:

$$\bar{x} = \frac{5 \cdot 1 + 5 \cdot 2 + 3 \cdot 1 + 6 \cdot 4 + 2 \cdot 5 + 1 \cdot 6}{20} = 2{,}9.$$

Medián je pak průměr desáté a jedenácté hodnoty (seřazených podle velikosti), tedy průměr z čísla 2 a 3, $\tilde{x} = 2, 5$.

Modus je nejčastěji se vyskytující hodnota, tedy $\hat{x} = 4$.

Uvedená data také můžeme zobrazit pomocí *krabicového diagramu*:




Horní a dolní strana „krabice“ odpovídá prvnímu (též dolnímu), resp. třetímu (též hornímu) kvartilu, její výška je tedy rovna kvartilovému rozpětí. Tlustá vodorovná čára mediánu je vedena ve výšce mediánu, dolní a horní vodorovná čára v diagramu odpovídá minimálnímu a maximálnímu prvku výběru, případně hodnotě, která je o 1,5 násobku kvartilového rozpětí nižší (resp. vyšší) než dolní (resp. horní) strana krabice. Případná data mimo toto rozpětí značíme v diagramu kolečky.

Není též problém sestavit histogram daných dat:

**9.1. Pravděpodobnost nebo statistika?** Ne náhodou se vracíme



k části našich motivačních náznaků z první kapitoly, jak jen se nám podařilo shromáždit dostatek matematických nástrojů jak diskrétní, tak spojité povahy.

Statistikami je totiž dnes zaplaveno kdejaké sdělení, ať už v médiích, politické nebo odborné. Nicméně porozumět obsahu takového sdělení a pochopit možnosti či oprávněnost využití jednotlivých statistických metod a pojmů si vyžaduje mnoho znalostí z různých oblastí matematiky, kterými jsme dosud procházeli. V tomto odstavci ještě nezačneme s matematickou teorií — ve volném sledu poznámek se jen zamyslíme nad dalšími kroky a cíli.

Vezměme si jako příklad souboru objektů všechny studenty konkrétního základního kurzu. Jako číselné údaje pak můžeme např. zkoumat

- „průměrný počet bodů“ dosažený při hodnocení tohoto předmětu v minulém semestru a „rozptyl“ dosažených hodnot,
- „průměrné známky“ dosažené u zkoušky z tohoto a z jiných pevně vybraných předmětů a „korelace“ (tj. vzájemnou souvislost) mezi výsledky,
- „korelace“ dat vypovídajících o historii dřívějšího studia u konkrétních studentů,
- „korelace“ neúspěchů ve studiu a počtu pracovních hodin týdně odpracovaných studentem či studentkou mimo fakultu,
- ...

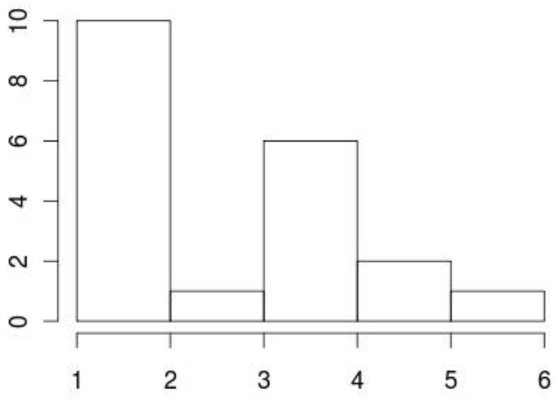
Zastavme se u prvního údaje. Samotný aritmetický průměr bodů nám mnoho neřekne ani o kvalitě přednášky ani o kvalitě přednášejícího ani o samotném hodnocení konkrétních studentů. Možná nás bude více zajímat hodnota, která bude „uprostřed souboru“, tj. počet bodů, pro které je stejně studentů pod ní a nad ní (nebo obdobně první a poslední čtvrtina, desetina apod.). Všem takovým údajům říkáme *statistiky* posuzované veličiny. Takové statistiky budou jistě zajímavé pro samotné studenty a je docela jednoduché je zavést, spočíst i sdělit.

Z obecné zkušenosti nebo jako výsledek teoretických úvah mimo samotnou matematiku víme, že rozumné hodnocení by mělo mít tzv. „normální“ rozdělení. Tento pojem patří do teorie pravděpodobnosti a k jeho zavedení potřebujeme poměrně dost matematiky. Porovnáním výsledku třeba i docela malého náhodného výběru studentů s teoretickým předpokladem můžeme zjistit odhad parametrů takového rozdělení, ale také činit závěry, zda je celé hodnocení postaveno rozumně.

Zároveň lze z číselných hodnot našich statistik pro konkrétní výběr kvalitativně popsat věrohodnost našich závěrů. Stejně tak budeme umět spočíst statistiky, které nebudou odrážet polohy hodnot uvnitř daného statistického souboru ale variabilitu sledovaných hodnot. Tak například když výsledky hodnocení nebudou vykazovat dostatečnou variabilitu, přičemž studenti jistě různé výkony prokazují, jde opět o náznak, že je s předmětem něco v nepořádku. Když působí zjištěná data zcela chaotickým dojmem, pak asi také.

V předchozím odstavci jsme mlčky předpokládali, že považujeme zpracovávaná data za věrohodná. To však v praktickém využití tak nebývá. Naopak samotná data jsou zatížena chybami, zpravidla vznikajícími v důsledku konstrukce experimentu a samotného sběru dat.

V mnoha případech také není známo mnoho o charakteru rozdělení dat. V takových případech je obvyklé používat metody




Všimněme si, že četnosti výskytů jedno a dvoučlenných domácností byly sloučeny do jednoho obdélníčku. Tento postup se používá pro „zpřehlednění dat" – existují (různá a nejednoznačná) pravidla, jak při slučování postupovat. Proto pouze na tento fakt upozorňujeme, aniž bychom uvedli přesný postup (v podstatě je to, jak se to komu líbí). □

**9.2.** Pro soubor znaků $x = (x_1, x_2, \ldots, x_n)$ vypočtěte průměr a rozptyl centrovaných hodnot $x_i - \bar{x}$ a standardizovaných hodnot $\frac{x_i - \bar{x}}{s_x}$.

**Řešení.** Průměr centrovaných hodnot zjistíme přímým výpočtem za použití definice aritmetického průměru

$$\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x}) = \frac{1}{n}\sum_{i=1}^{n} x_i - \frac{\bar{x}}{n}\sum_{i=1}^{n} 1 = \bar{x} - \bar{x} = 0.$$

Rozptyl centrovaných hodnot je zřejmě shodný s rozptylem původních hodnot $s_x$. Pro standardizované hodnoty je průměr zjevně opět roven nule a rozptyl je roven

$$\tfrac{1}{n}\sum_{i=1}^{n}\left(\tfrac{x_i-\bar{x}}{s_x}\right)^2 = \tfrac{1}{s_x^2}\cdot\tfrac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})^2 = 1. \qquad \square$$

**9.3.** Dokažte, že pro rozptyl platí vztah $s_x^2 = \frac{1}{n}\sum_{i=1}^{n} x_i^2 - \bar{x}^2$.

**Řešení.** Z definice rozptylu a aritmetického průměru

$$s_x^2 = \frac{1}{n}\sum_{i=1}^{n}\left(x_i^2 - 2x_i\bar{x} + \bar{x}^2\right) = \frac{1}{n}\sum_{i=1}^{n} x_i^2 - \frac{2\bar{x}}{n}\sum_{i=1}^{n} x_i + \bar{x}^2 =$$

$$= \frac{1}{n}\sum_{i=1}^{n} x_i^2 - \bar{x}^2.$$

□

**9.4.** Byly naměřeny následující hodnoty nějakého znaku

10; 7; 7; 8; 8; 9; 10; 9; 4; 9; 10; 9; 11; 9; 7; 8; 3; 9; 8; 7.

Určete aritmetický průměr, medián, kvartily, rozptyl a příslušný krabicový diagram.

neparametrické statistiky (kterých se jen letmo dotkneme na konci kapitoly).

Velmi zajímavé vývody můžeme formulovat, když porovnáním statistik pro různé veličiny uvedené výše budeme moci dovozovat informace o souvislostech. Pokud např. neexistuje žádná doložitelná souvislost mezi historií předchozího studia a výsledky v dané přednášce, je jedním z možných vysvětlení závěr, že je přednáška prostě špatně vedená.

Shrňme si tedy tyto úvahy takto:

- V popisné statistice máme k dispozici nástroje, které umožňují dobře porozumět struktuře a povaze i velmi rozsáhlých dat;
- v matematice pracujeme s abstraktním matematickým popisem pravděpodobnosti, který je použitelný pro analýzu daných dat, zejména když máme k dispozici teoretický model, kterému mají odpovídat;
- závěry statických šetření na vzorcích konkrétních souborů dat může dát matematická statistika;
- i to, do jaké míry je takový popis adekvátní pro konkrétní výběr dat, je možné vyjádřit pomocí metod matematické statistiky.

Než se do takového složitého programu pustíme, zastavme se u prvního bodu.

**9.2. Terminologie.** Statistikové zavedli veliké množství názvů a budeme si je muset osvojit. Základním východiskem je *statistický soubor*, což je přesně definovaná množina základních *statistických jednotek*. Ty mohou být dány buď výčtem nebo nějakými pravidly v rámci většího souboru.



Na každé statistické jednotce měříme jeden nebo více *statistických znaků*, přitom ovšem chápeme „měření" velice široce.

Např. souborem mohou být všichni studenti dané univerzity, každý zvlášť je pak *statistickou jednotkou*. O těchto jednotkách pak můžeme schraňovat mnoho znaků – např. všechny číselné hodnoty zjistitelné z informačního systému, jakou mají jednotliví studenti nejraději barvu, co snědli večer před poslední písemkou, atd.

Základním objektem pro zkoumání jednotlivých znaků je pak *soubor hodnot*. Zpravidla jej máme ve formě uspořádaných hodnot. Uspořádání je buď dáno přirozeně (když jsou hodnotami např. reálná čísla) nebo je můžeme zavést pro určitost (třeba když budeme sledovat barvy, tak je můžeme vyjadřovat v RGB standardu a řadit podle tohoto příznaku). Můžeme pracovat i s hodnotami neuspořádanými.

Protože smyslem statistického popisu je srozumitelně a přehledně sdělit něco o celém souboru, budeme jistě chtít umět jednotlivé hodnoty nějak porovnávat a poměřovat. Je tedy podstatné mít k tomu dispozici nějaké *měřítko*. Nejčastěji máme znaky vyjádřeny číselnou hodnotou. Ovšem věcný význam dat může být kvantifikován v různé míře a podle toho rozeznáváme různé *typy měřítek* znaků.

### Typy měřítek znaků

Podle toho jakého charakteru jsou hodnoty, hovoříme o typu:

- *nominálním*, kdy mezi hodnotami není žádný vztah, jde pouze o označení jednotlivých kvalitativních jmen, tj. možných hodnot (např. politické strany v ČR nebo přednášející na univerzitě při zkoumání jejich obliby);

**Řešení.** Označíme-li různé hodnoty znaku $a_i$ a jejich četnosti $n_i$, pak můžeme soubor dat ze zadání uspořádat do následující tabulky.

| $a_i$ | 3 | 4 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|
| $n_i$ | 1 | 1 | 4 | 4 | 6 | 3 | 1 |

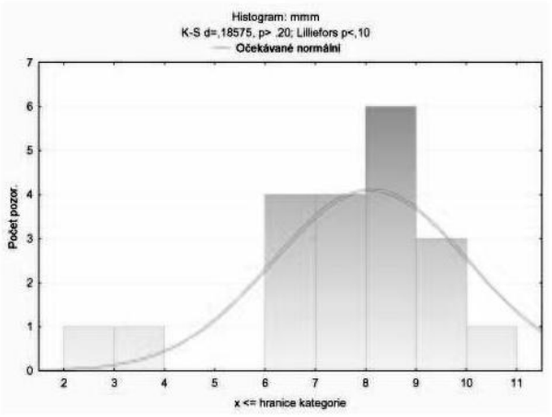
Z definice aritmetického průměru pak máme

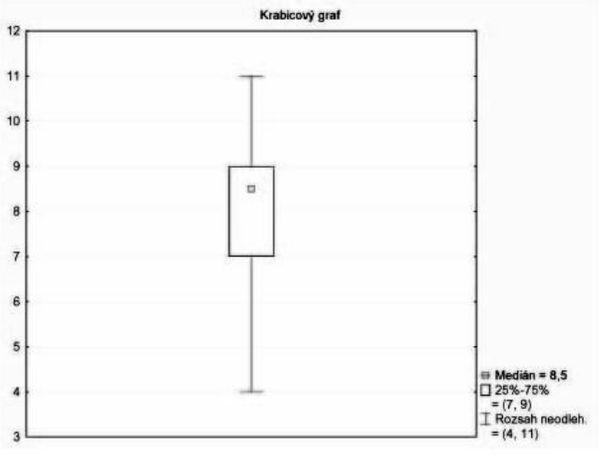
$$\bar{x} = \frac{3+4+4\cdot 7+4\cdot 8+6\cdot 9+3\cdot 10+11}{1+1+4+4+6+3+1} = \frac{162}{20} = 8{,}1.$$

Protože desátý člen v posloupnosti uspořádaných hodnot znaku je $x_{(10)} = 8$ a jedenáctý $x_{(11)} = 9$, je medián roven $\tilde{x} = \frac{8+9}{2} = 8{,}5$. Dolní kvartil je $x_{0,25} = \frac{x_{(5)}+x_{(6)}}{2} = 7$ a horní $x_{0,75} = \frac{x_{(15)}+x_{(16)}}{2} = 9$. Z definice rozptylu spočítáme

$$s_x^2 = \frac{5{,}1^2+4{,}1^2+4\cdot 1{,}1^2+4\cdot 0{,}1^2+6\cdot 0{,}9^2+3\cdot 1{,}9^2+2{,}9^2}{1+1+4+4+6+3+1} = \\ = 3{,}59.$$

Na následujících obrázcích je zobrazen příslušný histogram a krabicový diagram.




- *ordinálním*, kdy platí totéž jako předchozí, ale s přidaným uspořádáním (např. počet hvězdiček u hotelů v turistických průvodcích);
- *intervalovém*, kdy jde o číselné hodnoty, ale jde o porovnání velikostí, nikoliv absolutní hodnotu (např. u měření teplot je poloha nuly zpravidla dohodnuta, ale není podstatná);
- *poměrovém*, kdy máme pevně stanovené měřítko a nulu (např. většina fyzikálních nebo ekonomických veličin).

U nominálních typů znaků jsme schopni věcně interpretovat pouze rovnost $x_1 = x_2$, u ordinálních i nerovnost $x_1 < x_2$, případně $x_1 > x_2$, u intervalových navíc umíme posoudit rozdíl $x_1 - x_2$. U poměrových typů měřítek máme k dispozici rovnost, nerovnost, rozdíl i podíl $x_1/x_2$.

**9.3. Třídění hodnot.** V dalším budeme pracovat se *souborem hodnot* $x_1, x_2, \ldots, x_n$, které lze uspořádat (nejedná se tedy o hodnoty typy znaků nominálních) a které vznikly měřením na $n$ statistických jednotkách, a uspořádáme je do *uspořádaného souboru hodnot*

$$x_{(1)}, x_{(2)}, \ldots, x_{(n)}. \tag{9.1}$$

Číslo $n$ nazýváme *rozsah souboru*.

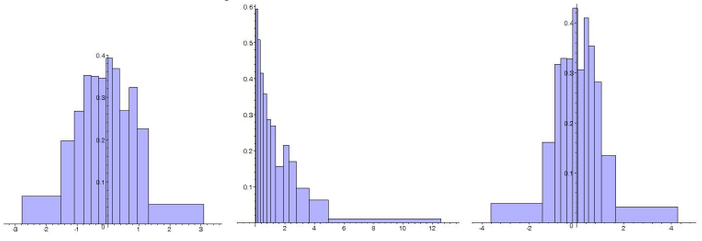
Pokud pracujeme s rozsáhlými soubory znaků, které ale připouští jen málo hodnot, je nejjednodušší uvádět pouze četnosti výskytu. Např. při průzkumu preferencí politických stran nebo u prezentace kvality hotelové sítě uvádíme u každé možné hodnoty počet jejích výskytů.

Pokud je možných hodnot mnoho (nebo dokonce připouštíme spojitě rozprostřené reálné hodnoty), dělíme často možný rozsah hodnot na vhodný počet intervalů a o statistickém znaku uvádíme četnost hodnot v daných intervalech. Intervalům se často říká *třídy* a počtu znaků ve třídě pak *třídní četnosti*. Používáme také *kumulativní četnosti* a *kumulativní třídní četnosti*, které pro danou třídu vznikají prostým součtem třídních četností s hodnotami nejvýše jako má ta daná.

Nejčastěji pak uvažujeme střed $a_i$ dané třídy za hodnotu, která ji reprezentuje a hodnota $a_i n_i$, kde $n_i$ je četnost výskytu této třídy představuje celkový příspěvek této třídy. Velmi často také místo četností zobrazujeme relativní četnosti $a_i/n$, resp. relativní kumulativní četnosti.

Graf, který na jedné ose vynáší intervaly jednotlivých tříd a nad nimi obdélníky s výškou rovnou četnosti se nazývá *histogram*. Obdobně se znázorňuje kumulativní četnost.

Na obrázku jsou histogramy souborů o rozsahu $n = 500$, které vznikly náhodným generováním dat s různými standardními rozděleními (časem jim budeme říkat normální, $\chi^2$ a studentovo)



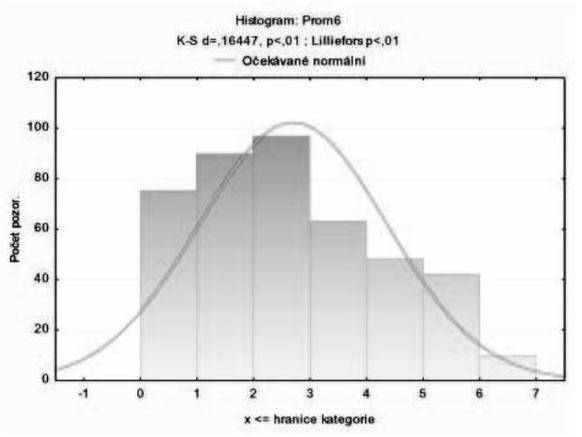
□

**9.5.** V daném rybníku se vylovilo 425 kaprů a u všech byly zjištěny jejich hmotnosti. Pak se vhodně zvolily hmotnostní intervaly a sestavila se následující tabulka četností:

| Hmotnost (kg) | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 |
|---|---|---|---|---|---|---|---|
| Střed třídy | 0,5 | 1,5 | 2,5 | 3,5 | 4,5 | 5,5 | 6,5 |
| Četnost | 75 | 90 | 97 | 63 | 48 | 42 | 10 |

Načrtněte histogram, určete aritmetický, geometrický a harmonický průměr hmotnosti kaprů, dále určete medián, horní a dolní kvartil, modus, rozptyl, směrodatnou odchylku, variační koeficient a načrtněte příslušný krabicový diagram.

**Řešení.** Histogram má tvar




Z definic příslušných pojmů v části 9.4 přímo spočítáme aritmetický průměr $\bar{x} = 2{,}7\text{kg}$, geometrický průměr $\bar{x}^G = 2{,}1\text{kg}$, harmonický průměr $\bar{x}^H = 1{,}5\text{kg}$. Z definic v 9.5 je medián roven $\tilde{x} = x_{0,5} = 2{,}5\text{kg}$, dolní a horní kvartil $x_{0,25} = 1{,}5\text{kg}$ resp. $x_{0,75} = 3{,}5\text{kg}$ a pro modus platí $\hat{x} = 2{,}5\text{kg}$. Z definic v části 9.6 spočítáme rozptyl hmotnosti kaprů $s_x^2 = 2{,}7\text{kg}^2$, tj. směrodatná odchylka je $s_x = 1{,}7\text{kg}$, a variační koeficient $V_x = 0{,}6$. □

**9.6.** Dokažte, že entropie nabývá svého maxima, jsou-li hodnoty nominálního znaku rovnoměrně rozloženy, tj. četnost každé třídy je $n_i = 1$.

**Řešení.** Podle definice entropie 9.9 hledáme maximum funkce $H_X = -\sum_{i=1}^{n} p_i \ln p_i$ vzhledem k neznámým relativním četnostem $p_i = \frac{n_i}{n}$, které navíc splňují $\sum_{i=1}^{n} p_i = 1$. Jedná se tedy o klasickou úlohu hledání vázaného extrému, kterou můžeme vyřešit například pomocí Lagrangeových multiplikátorů. Příslušná Lagrangeova funkce je

$$L(p_1, \ldots, p_n, \lambda) = -\sum_{i=1}^{n} p_i \ln p_i + \lambda \left( \sum_{i=1}^{n} p_i - 1 \right).$$

**9.4. Míry polohy statistických znaků.** Chceme-li vyjádřit velikost hodnot, kolem kterých se jednotlivá pozorování znaků shromažďují používáme většinou pojmy z následující definice. Budeme teď pracovat se znaky poměrových (nebo případně intervalových) typů měřítek.

Uvažme (netříděný) soubor $(x_1, \ldots, x_n)$ hodnot měřeného znaku pro všechny zpracovávané statistické jednotky a nechť $n_1, \ldots, n_m$ jsou třídní četnosti $m$ různých hodnot $a_1, \ldots, a_n$, nabývaných tímto souborem.

### Průměry

**Definice.** *Aritmetický průměr* (často také jen *průměr*) je dán

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i = \frac{1}{n} \sum_{j=1}^{m} n_j a_j.$$

*Geometrický průměr* je dán

$$\bar{x}^G = \sqrt[n]{x_1 x_2 \cdots x_n}$$

a má smysl pouze u kladných hodnot znaků. Harmonický průměr je dán

$$\bar{x}^H = \left( \frac{1}{n} \sum_{i=1}^{n} \frac{1}{x_i} \right)^{-1}$$

a je také definován jen pro kladné hodnoty znaků.

Aritmetický průměr je jediný z těchto průměrů, který je invariantní vůči afinním transformacím, tj. pro libovolné skaláry $a$, $b$ platí

$$\overline{(a + b \cdot x)} = \frac{1}{n} \sum_{i=1}^{n} (a + b x_i) = a + b \sum_{i=1}^{n} x_i = a + b \cdot \bar{x}.$$

Aritmetický průměr je proto obzvlášť vhodný pro intervalové typy měřítek.

Logaritmus geometrického průměru je aritmetický průměr logaritmů znaků. Je obzvlášť vhodný pro znaky, které se kumulují multiplikativně, např. úrokové míry. Je-li totiž úroková míra v jednotlivých časových jednotkách $x_i\%$, bude za celé období výsledek takový, jakoby byla po celou dobu konstantní úroková míra $\bar{x}^G\%$.

Jako ilustraci tehdy rozvíjených metod jsme dokázali v odstavci 8.23 na straně 464, že je geometrický průměr vždy nejvýše tak velký jako aritmetický. Obdobně je tomu pro harmonický průměr a platí

$$\bar{x}^H \leq \bar{x}^G \leq \bar{x}.$$

**9.5. Medián, kvartil, decil, percentil, ...** Jiný způsob vyjádření míry, jakou hodnotu nabývají znaky, je najít pro číslo $\alpha$ mezi nulou a jedničkou takovou hodnotu $x_\alpha$, aby $100\,\alpha\%$ hodnot znaku bylo nejvýše $x_\alpha$ a zbylé byly větší než $x_\alpha$. Pokud takový znak není určen jednoznačně, volíme zpravidla průměr mezi dvěma extrémními možnými hodnotami.

Číslu $x_\alpha$ říkáme *$\alpha$–kvantil*. Dosáhl-li tedy nějaký účastník soutěže výsledku, který jej řadí do $x_{1,00}$, neznamená to, že byl jistě lepší než všichni ostatní. Jen nebyl nikdo jiný ještě lepší než on.

Nejobvyklejší hodnoty $x_\alpha$ jsou:

- *medián* (často také výběrový medián) definovaný vztahem

$$\tilde{x} = x_{0,50} = \begin{cases} x_{((n+1)/2)} & \text{pro liché } n \\ \frac{1}{2}\left(x_{(n/2)} + x_{(n/2+1)}\right) & \text{pro sudé } n \end{cases},$$

Pro její parciální derivace platí $\frac{\partial L}{\partial p_i} = -\ln p_i - 1 + \lambda$, a proto je její stacionární bod určen rovnicemi $p_i = e^{\lambda-1}$ pro všechna $i = 1, \ldots, n$. Navíc víme, že součet relativních četností $p_i$ je roven jedné. To znamená $ne^{\lambda-1} = 1$ a odtud $\lambda = 1 - \ln n$. Dosazením zřejmě $p_i = \frac{1}{n}$. □

**9.7.** Následující grafy udávají četnosti možných bodových zisků studentů předmětu MB104 na Fakultě informaticky Masarykovy univerzity v roce 2012. Kumulativní graf je uváděn s „prohozenými“ osami oproti předchozímu příkladu.

Četnosti jednotlivých bodových zisků jsou uvedeny v následující tabulce:

| Body | Počet studentů |
|---|---|
| 20.5 | 1 |
| 20 | 1 |
| 19 | 2 |
| 18.5 | 1 |
| 18 | 2 |
| 17.5 | 3 |
| 17 | 2 |
| 16.5 | 4 |
| 16 | 3 |
| 15.5 | 5 |
| 15 | 7 |
| 14.5 | 6 |
| 14 | 14 |
| 13.5 | 21 |
| 13 | 21 |
| 12.5 | 19 |
| 12 | 17 |
| 11.5 | 18 |
| 11 | 31 |
| 10.5 | 22 |
| 10 | 53 |

| Body | Počet studentů |
|---|---|
| 9.5 | 9 |
| 9 | 9 |
| 8.5 | 13 |
| 8 | 8 |
| 7.5 | 13 |
| 7 | 4 |
| 6.5 | 7 |
| 6 | 4 |
| 5.5 | 8 |
| 5 | 7 |
| 4.5 | 9 |
| 4 | 5 |
| 3.5 | 7 |
| 3 | 8 |
| 2.5 | 8 |
| 2 | 14 |
| 1.5 | 8 |
| 1 | 2 |
| 0.5 | 6 |
| 0 | 9 |

Tomu potom odpovídá následující histogram:

kde $x_{(k)}$ představuje hodnotu v uspořádaném souboru hodnot (9.1)

- *dolní a horní kvartil* $Q_1 = x_{0,25}$ a $Q_3 = x_{0,75}$;
- *p-tý kvantil* (též *výběrový kvantil* nebo *percentil*) $x_p$, kde $0 < p < 1$ (zpravidla zadaný na dvě desetinná místa).

Lze se setkat také s hodnotou *modus*, která udává hodnotu $\hat{x}$ znaku s největší četností v souboru $x$.

Aritmetický průměr, medián a modus představují jakési očekávatelné hodnoty znaků. Průměr u znaku podílového typu, medián u poměrového a modus u ordinálního nebo nominálního.

Všimněme si, že všechny $\alpha$–kvantily hodnot v intervalových měřítcích jsou invariantní vzhledem k afinním transformacím hodnot (promyslete si podrobně!).

**9.6. Míry variability statistických znaků.** Rozumným požadavkem na jakoukoliv míru variability souboru hodnot znaků $x \in \mathbb{R}^n$ je její invariance vůči konstantním posunutím. V euklidovském prostoru $\mathbb{R}^n$ má tuto vlastnost standardní vzdálenost bodů a nezávislý na posunutí o konstantní hodnotu je i výběrový průměr. Proto volíme následující



ROZPTYL A SMĚRODATNÁ ODCHYLKA

**Definice.** *Rozptyl* souboru znaků $x$ je definován vztahem

$$s_x^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x}_i)^2.$$

*Směrodatná odchylka* $s_x$ je dána jako odmocnina z výběrového rozptylu.

Často se v literatuře také pro rozptyl používá název *střední kvadratická odchylka*.

Variabilita statistických znaků by neměla záviset na konstantním posunutí všech hodnot. Při naší definici jsme proto vyšli z toho, že jak standardní vzdálenost bodů v $\mathbb{R}^n$ tak výběrový průměr jsou vůči posunutím o konstantní hodnotu invariantní, bude proto skutečně i pro neuspořádaný soubor znaků

$$y = (x_1 + c, x_2 + c, \ldots, x_n + c)$$

vždy platit také $s_y = s_x$.

Někdy se místo naší hodnoty $s_x$ používá tzv. *výběrový rozptyl*, který se odlišuje jen tím, že se ve jmenovateli zlomku používá $(n - 1)$, důvod uvidíme později.

V případě třídních četností $n_j$ hodnot $a_j$ pro $m$ tříd dává stejný výraz hodnotu rozptylu

$$s_x^2 = \frac{1}{n}\sum_{j=1}^{m} n_j(a_j - \bar{x})^2,$$

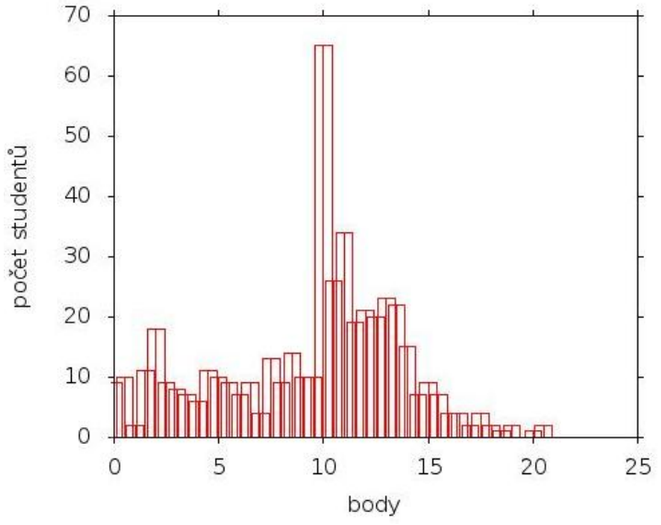
ale v praxi se doporučuje používat tzv. Shepardovu korekci, která $S_x^2$ zmenší o $h^2/12$, kde $h$ je šířka stejných intervalů definujících třídy hodnot.

Dále se ještě můžeme potkat s tzv. *rozpětím výběru*

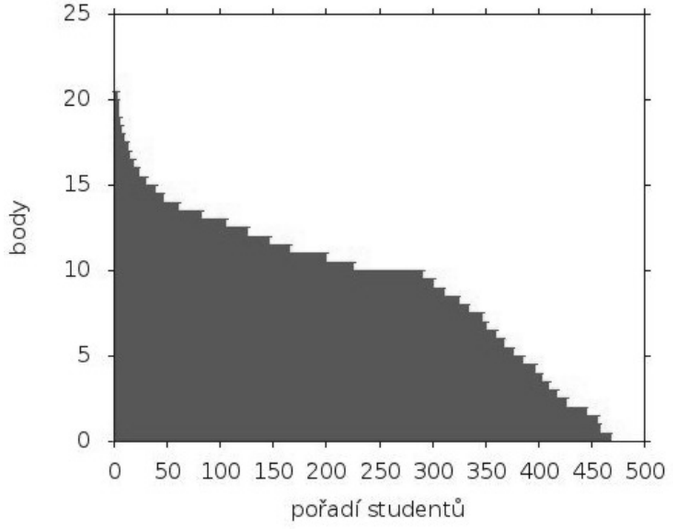
$$R = x_{(n)} - x_{(1)}$$

a *kvartilovým rozpětím výběru*

$$Q = Q_3 - Q_1.$$




Histogram jsme obdrželi z informačního systému Masarykovy univerzity. Vidíme, že je zvolen poněkud netradiční způsob zobrazování, kdy danému bodovému zisku odpovídá „dvojitý obdélníček“. Je na vkusu každého čtenáře, jaký způsob výpisu dat zvolí (je možno některé hodnoty počítat do jedné, čímž snížíme počet obdélníčků, nebo používat tenčí obdélníčky).




Snadno si všimneme, že modusem bodových hodnot je číslo 10, což byla shodou okolností bodová hranice zaručující absolvování předmětu. Průměr získaných bodů je 9,48.

**9.8.** Uveďme ještě sloupcové diagramy bodových zisků studentů předmětu MB101 v podzimním semestru 2010 (první semestr studia) a to jednak všech účastníků předmětu a poté studentů, kteří úspěšně ukončili bakalářské studium.

Používá se také tzv. *průměrná odchylka*, která je dána průměrnou vzdáleností hodnot od mediánu

$$D_x = \frac{1}{n}\sum_{i=1}^{n}|x_i - \tilde{x}|.$$

Následující věta podává zdůvodnění, proč tyto míry variability volíme:

**Věta.** *Funkce* $S(t) = (1/n)\sum_{i=1}^{n}(x_i - t)^2$ *nabývá svého minima pro* $t = \bar{x}$*, tj. pro výběrový průměr.*

*Funkce* $D(t) = (1/n)\sum_{i=1}^{n}|x_i - t|$ *nabývá svého minima pro* $t = \tilde{x}$*, tj. pro medián.*

Důkaz. Protože je součet vzdáleností všech hodnot od výběrového průměru nulový, dostáváme přímým výpočtem

$$\begin{aligned}\sum_{i=1}^{n}(x_i - t)^2 &= \sum_{i=1}^{n}\big((x_i - \bar{x})^2 + (\bar{x} - t)^2 - 2(x_i - \bar{x})(\bar{x} - t)\big)\\ &= n(\bar{x} - t)^2 + \sum_{i=1}^{n}(x_i - \bar{x})^2,\end{aligned}$$

což ověřuje první tvrzení.

U druhého si musíme dát pozor na definici mediánu. Součet si za tím účelem přeskládáme tak, abychom vždy postupně sčítali první s posledním sčítancem, pak druhý s předposledním atd. V prvním případě tedy jde o výraz $|x_{(1)} - t| + |x_{(n)} - t|$, a ten bude roven vzdálenosti $x_{(n)} - x_{(1)}$, pokud bude $t$ uvnitř rozsahu hodnost, a bude ještě vetší jinak. Další dvojice v součtu nám stejně dá $x_{(n-1)} - x_{(2)}$, pokud bude $x_{(2)} \le t \le x_{(n-1)}$ a bude větší jinak. Postupně tedy požadavek na minimalizaci součtu povede právě na $t = \tilde{x}$. □

V praxi potřebujeme poměřovat variabilitu různých souborů hodnot znaků různých statistických jednotek. Pro tento účel je vhodné relativizovat měřítko a používáme proto tzv. *variační koeficient* daného souboru $x$

$$V_X = \frac{\sqrt{s_x^2}}{|\bar{x}|}.$$

Tuto relativní míru variability lze také chápat v procentech směrodatné odchylky ve vztahu k výběrovému průměru $\bar{x}$.

**9.7. Šikmost rozložení hodnot znaků.** Pokud jsou rozloženy znaky našeho souboru naprosto symetricky kolem výběrového průměru, bude zejména platit

$$\bar{x} = \tilde{x}$$

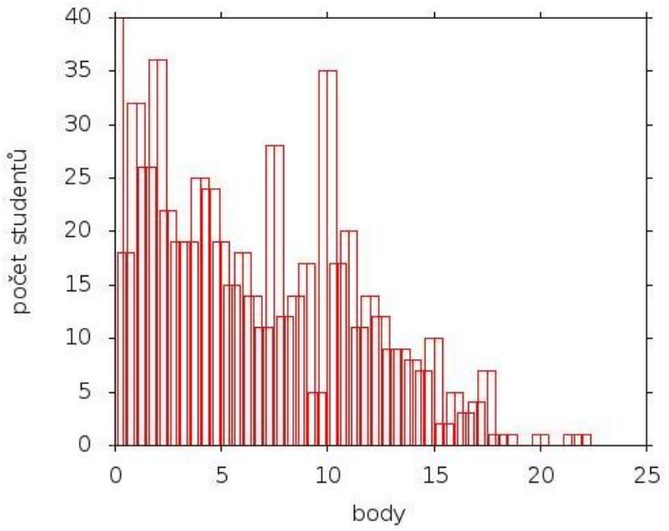
Často ale potkáváme rozložení hodnot splňujících

$$\bar{x} > \tilde{x},$$

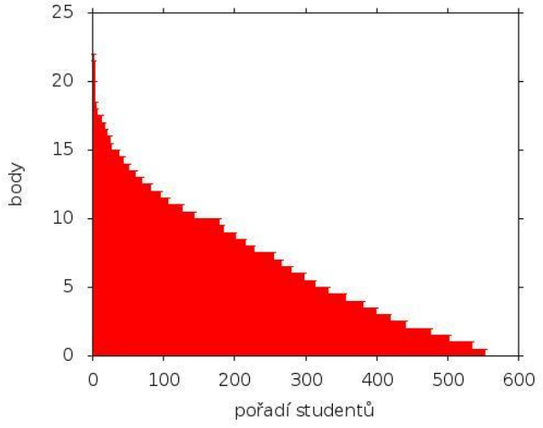
např. to je běžné u rozložení mezd v populaci. Docela užitečnou charakteristikou v tomto směru je tzv. Pearsonův koeficient, který je dán vztahem

$$\beta = 3\frac{\bar{x} - \tilde{x}}{S_x}$$

a můžeme si z něho udělat představu o relativní míře (absolutní hodnota $\beta$) i charakteru zešikmení (znaménko). Zejména si všimněme, že směrodatná odchylka je vždy kladná, takže již znaménko nám ukazuje, kterým směrem k zešikmení dochází.




Výsledky opět můžeme zachytit i alternativně:




A nyní grafy bodových zisků účastníků, kteří dále úspěšně pokračovali ve studiu.

### Kvantilové koeficienty šikmosti

Podrobnější informaci v tomto směru dávají tzv. *kvantilové koeficienty šikmosti*

$$\beta_p = \frac{x_{1-p} + x_p}{x_{1-p} - x_p},$$

pro každé $0 < p < 1$. Jejich význam je zřejmý, když čitatel zlomku vyjádříme jako $(x_{1-p} - \tilde{x}) - (\tilde{x} - x_p)$.

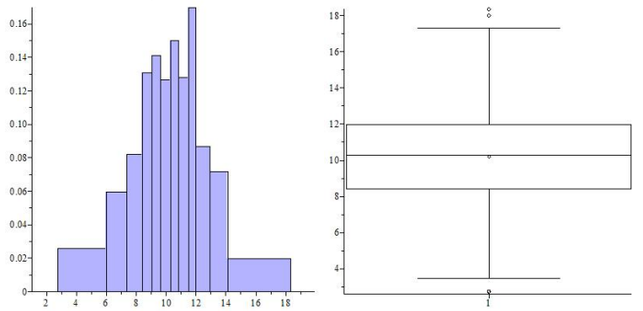
Speciálně dostáváme tzv. *kvartilový koeficient šikmosti* při volbě $p = 0{,}25$.

**9.8. Diagramy.** Pro rychlé vstřebávání složitěji strukturovaných informací je člověk skvěle vybaven zrakově. Proto se pro zobrazení statistiky jednotlivých znaků nebo jejich korelací používá mnoho standardizovaných nástrojů. Jedním z nich jsou tzv. *krabicové diagramy*.



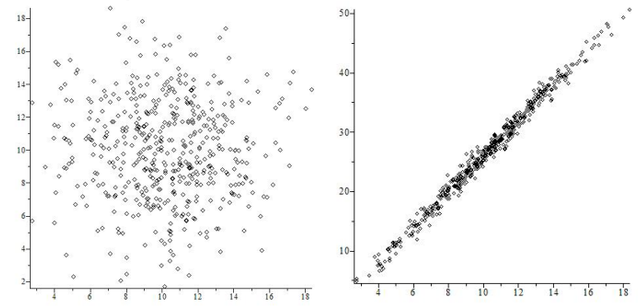
### Krabicový diagram

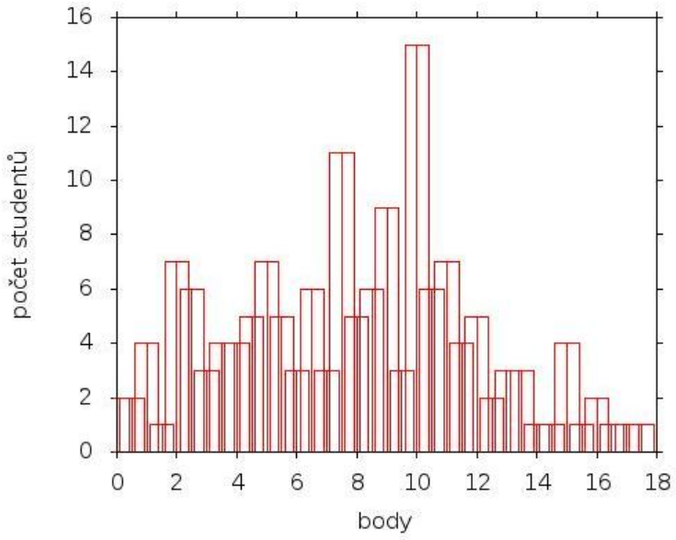
Na obrázku je zobrazen histogram a krabicový diagram stejného souboru hodnot (normální rozdělení s průměrem 10 a rozptylem 3, $n = 500$).

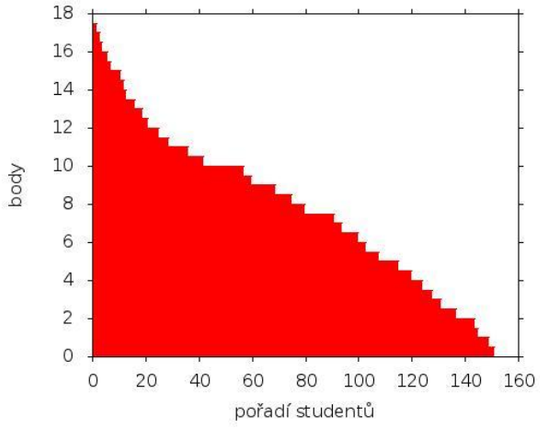


Střední linka je medián, kraje boxu jsou kvartily, „packy“ ukazují 1,5 kvartilového rozsahu, ne však víc než kraje rozsahu výběru, případné hodnoty mimo jsou přímo naznačeny body.

Běžné zobrazovací nástroje nám umožňují dobře vidět případné závislosti dvou výběrů zjištěných znaků. Např. na levém obrázku níže jsou za souřadnice voleny hodnoty ze dvou nezávislých normálních rozdělení s průměrem 10 a rozptylem 3. Na pravém obrázku je první souřadnice ze stejných dat, druhá je z první dána vztahem $y = 3x + 4$, ale je navíc zatížená malou náhodnou chybou.






Vidíme, že modus zisku bodů v prvním případě je 0, ve druhém případě je to opět deset. Rozložení bodových zisků se blíží rozložení bodových zisků z předmětu MB104, který je zařazen ve čtvrtém semestru studia.

**9.9.** Auto jelo z Brna do Prahy rychlostí 160 km/h, z Prahy do Brna rychlostí 120 km/h. Jaké průměrné rychlosti na trase dosáhlo?

**Řešení.** Toto je základní příklad, kde je použití aritmetického průměru nevhodné. Na průměrnou rychlost totiž klademe požadavek, aby auto jedoucí touto rychlostí strávilo na trase stejnou dobu. Označíme-li $d$ vzdálenost obou měst v kilometrech, $v_p$ průměrnou rychlost tak

$$\frac{d}{160}+\frac{d}{120}=\frac{2d}{v_p},$$

odkud

$$v_p=\frac{2}{\frac{1}{160}+\frac{1}{120}}\doteq 137{,}14.$$

**9.9. Entropie.** Variabilitu potřebujeme vyjadřovat i u nominálních typů znaků, např. ve statistické fyzice nebo teorii informace. K dispozici máme jen třídní četnosti a můžeme tedy použít princip klasické pravděpodobnosti (viz čtvrtá část první kapitoly), kdy relativní četnost $i$-té třídy, $p_i=\frac{n_i}{n}$, vnímáme jako pravděpodobnost, že náhodně vybraný prvek bude v této třídě.

Rozptyl poměrových hodnot znaku, u kterého máme vyjádřeny třídní četnosti $n_j$, byl v odstavci 9.6 vyjádřen vztahem

$$s_x^2=\sum_{j=1}^{m}\frac{n_j}{n}(a_j-\bar{x})^2=\sum_{j=1}^{m}p_j(a_j-\bar{x})^2,$$

kde $p_j$ označuje (klasickou) pravděpodobnost, že hodnota znaku bude v $j$-té třídě. Jde tedy o vážený průměr přepočtených hodnot znaků, kde je hodnota $F(a_j)=(a_j-\bar{x})^2$ vstupuje s vahou $p_j$.

Variabilitu hodnot znaků nominálního typu budeme vyjadřovat podobným výrazem, označíme ho $H_X$. Nemáme sice k dispozici žádné číselné hodnoty $a_j$ pro pořadové indexy $j$, můžeme se ale zajímat o funkce $F$ závisející na relativních četnostech $p_j$, tj. zkusíme pro datový soubor $x$ definovat

$$H_X=\sum_{i=1}^{n}p_iF(p_i),$$

kde $F$ je zatím neznámá funkce.

Pokud znak nabývá právě jedné hodnoty, tj. pokud $p_k=1$ pro nějaké $k$ a všechna ostatní $p_j=0$, pak budeme jistě říkat, že variabilita je nulová. Je tedy v každém případě $F(1)=0$.

Dále budeme požadovat, aby $H_X$ měla následující vlastnost. Pokud je zkoumaný soubor znaků $Z$ tvořen dvojicemi znaků ze souborů $X$ a $Y$ (např. můžeme na statistických jednotkách-osobách sledovat barvu očí a barvu vlasů), je rozumné, aby variabilita znaků $z$ byla součtem variabilit jednotlivých znaků, tj. požadujeme v takovém případě $H_Z=H_X+H_Y$.

Známe relativní třídní četnosti $p_i$ pro znaky v souboru $X$ a $q_j$ pro znaky souboru $Y$. Relativní třídní četnosti pro $Z$ jsou

$$r_{ij}=\frac{n_im_j}{nm}=p_iq_j$$

a požadujeme tedy rovnost (rozsahy součtů jsou zřejmé z kontextu)

$$\sum_{i,j}p_iq_jF(p_iq_j)=\sum_i p_iF(p_i)+\sum_j q_jF(q_j).$$

Díky tomu, že $p_i$ a $q_j$ jsou relativní četnosti a tedy dávají v součtu 1, můžeme pravou stranu rovnosti přepsat jako

$$\Big(\sum_j q_j\Big)\Big(\sum_i p_iF(p_i)\Big)+\Big(\sum_i p_i\Big)\Big(\sum_j q_jF(q_j)\Big)$$

a dostáváme vztah

$$\sum_{i,j}p_iq_jF(p_iq_j)=\sum_{i,j}p_iq_j\big(F(p_i)+F(q_j)\big).$$

Je zřejmé, že tomuto požadavku vyhovuje jakýkoliv konstantní násobek logaritmu při kterémkoliv pevně zvoleném základu $a>1$ (a lze ukázat, že jiná spojitá řešení $F$ neexistují).

Poněvadž je $p_i\le 1$, je jistě $\ln p_i\le 0$. My však chceme variabilitu nezápornou, zvolíme proto za funkci $F$ logaritmickou funkci s násobkem $-1$. Taková volba také automaticky splňuje náš požadavek $F(1)=0$.

Průměrná rychlost je tedy dána harmonickým průměrem (viz 9.3 průměrovaných rychlostí

□

### B. Vizualizace vícerozměrných dat.

V předchozích příkladech jsme se věnovali zobrazování jednoho znaku měřeného u více objektů (získané body studentů). Grafická vizualizace dat pomáhá k lepší představě o datech. Jak ale postupovat, pokud u některých, řekněme $n$ objektů, měříme nějakých $p$ znaků, $p \geq 3$. Tato měření není možné znázornit způsoby, které jsme se již naučili. Jednou z možných metod, je tzv. *metoda hlavních komponent*. V této metodě využijeme pojmu vlastního vektoru a vlastních čísel (viz 2.46) výběrové varianční matice (viz 9.38). Zaveďme následující označení:

- náhodné vektory měření $\mathbf{x}_i = (x_{i1}, x_{i2}, \ldots, x_{in})^T$, $i = 1, \ldots, n$,
- průměr $j$-tého znaku $m_j = \frac{1}{n}\sum_{i=1}^{n} x_{ij}$, $j = 1, \ldots, p$,
- rozptyl $j$-tého znaku $s_j = \frac{1}{n-1}\sum_{i=1}^{n}(x_{ij} - m_j)^2$, $j = 1, \ldots, p$,
- vektor průměrů $\mathbf{m} = (m_1, \ldots, m_p)$,
- výběrová varianční matice $\frac{1}{n-1}\sum_{i=1}^{n}(\mathbf{x}_i - \mathbf{m})(\mathbf{x}_i - \mathbf{m})^T$ (všimněme si, že každý sčítanec v předchozí sumě je maticí rozměrů $p \times p$).

Varianční matice je symetrická, tudíž má všechna vlastní čísla reálná a její vlastní vektory jsou navzájem kolmé. Volíme-li navíc vlastní vektory jednotkové, pak z toho vyplývá, že vlastní hodnota příslušná nějakému vlastnímu vektoru varianční matice dává rozptyl (velikosti) průmětu daných dat do tohoto směru (promítáme v $p$-rozměrném prostoru). Cílem této metody je nalézt směr (v $p$-rozměrném prostoru znaků), pro který je rozptyl průmětů daných dat do něj největší. Tento směr tedy odpovídá tomu vlastnímu vektoru varianční matice, který odpovídá největší vlastní hodnotě. Lineární kombinace daná složkami tohoto vektoru se nazývá 1. hlavní komponenta. Velikost průmětu daných dat do tohoto směru relativně dobře odhaduje data (hlavní komponentu lze chápat jako jeden znak, který nahrazuje $p$ znaků, jde tedy o náhodný vektor o $n$ položkách). Pokud od dat odečteme tento průmět a opět uvážíme směr největší variability takto pozměněných dat, dostáváme 2. hlavní komponentu a opakováním tohoto postupu dostáváme další hlavní komponenty. Směr největší variability je ovšem vlastní vektor varianční matice odpovídající největšímu vlastnímu číslu (čtenář si laskavě rozmyslí). Směry dalších hlavních

#### Entropie

Míru variability znaků v nominálním měřítku vyjadřujeme pomocí *entropie*. Je dána vztahem

$$H_X = -\sum_{i=1}^{k} \frac{n_i}{n} \ln\left(\frac{n_i}{n}\right),$$

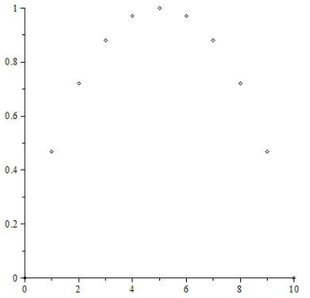
kde $k$ je počet tříd ve výběru. Kromě přirozeného logaritmu se často také setkáváme (např. teorii informace) se stejným vztahem ale s logaritmem při základu 2.

Často se také místo $H_X$ pracuje s veličinou

$$e^{H_X} = \prod_i p_i^{-p_i},$$

případně totéž s jiným zvoleným základem pro logaritmus.

V tomto tvaru se pěkně spočítá, že pro výběr $X$ s $k$ stejně velkými třídními četnostmi je $e^{H_X} = \left((\frac{1}{k})^{-\frac{1}{k}}\right)^k = k$, nezávisle na velikosti výběru. Na obrázku jsou vyneseny entropie $y$ při základu 2 pro výskyt písmen $a$ a $b$ v desetipísmenných slovech s písmeny $a$ a $b$, kde $x$ je počet výskytů písmene $b$.




Všimněme si, že pro shodný výskyt, tj. pro pět písmen $b$, vyjde maximální entropie 1 a skutečně je $2^1 = 2$.

### 2. Pravděpodobnost

Před dalším čtením lze čtenářům vřele doporučit zopakování obsahu čtvrté části první kapitoly (tj. odstavce začínající na straně 17). Tehdy jsme pracovali převážně s tzv. klasickou konečnou pravděpodobností a zavedli jsme základy formalismu, který nyní rozšíříme. Hlavní změnou bude, že náš základní prostor $\Omega$ už nebude obecně obsahovat jen konečně mnoho prvků (ve skutečnosti nemusí být ani spočetný). Připomeňme, že v našich úvahách o tzv. geometrické pravděpodobnosti na konci čtvrté části první kapitoly jsme potřebovali jako základní prostor pro popis jevu vhodnou část euklidovského prostoru a jevy pak byly vhodně vybrané podmnožiny. Tedy samozřejmě samé nespočetné množiny.

Začneme jednoduchým, stále ještě diskrétním, ale nekonečným příkladem, ke kterému se ve výkladu budeme občas vracet.

**9.10. Proč nekonečné množiny jevů?** Představme si experiment, ve kterém opakovaně házíme mincí dokud nepadne líc. Ptáme se, jaká je pravděpodobnost, že budeme házet alespoň 3–krát nebo právě 35–krát nebo nejvýš 10–krát apod.



komponent pak odpovídají dalším vlastním vektorům varianční matice (seřazenými podle velikosti vlastních hodnot, které jim přísluší).

**9.10.** Určete 1. hlavní komponentu následujících jednoduchých dat a vektor, který jejím použitím nahrazuje naměřená data. U pěti osob byla změřena výška, délka malíčku a délka ukazováčku s výsledky zaznamenanými v tabulce (výsledky jsou v centimetrech).

**Řešení.**

| | Martin | Michal | Matěj | Honza | Markéta |
|---|---|---|---|---|---|
| ukazováček | 9 | 11 | 8 | 8 | 8 |
| malíček | 7,5 | 8 | 6,3, | 6 | 6,5 |
| výška | 186 | 187 | 173 | 174 | 167 |

.

Vektory pozorovaných hodnot jsou: $\mathbf{x}_1 = (9; 7{,}5; 186)$, $\mathbf{x}_2 = (11; 8; 187)$, $\mathbf{x}_3 = (8; 6; 173)$, $\mathbf{x}_4 = (8; 6; 174)$, $\mathbf{x}_5 = (8; 6{,}5, 167)$. Varianční matice těchto vektorů jsou postupně

$$\begin{pmatrix} 0{,}04 & 0{,}14 & 1{,}72 \\ 0{,}14 & 0{,}49 & 6{,}02 \\ 1{,}72 & 6{,}02 & 73{,}96 \end{pmatrix}, \quad \begin{pmatrix} 4{,}840 & 2{,}64 & 21{,}12 \\ 2{,}64 & 1{,}44 & 11{,}52 \\ 21{,}12 & 11{,}52 & 92{,}16 \end{pmatrix},$$

$$\begin{pmatrix} 0{,}641 & 0{,}640 & 3{,}521 \\ 0{,}640 & 0{,}640 & 3{,}52 \\ 3{,}521 & 3{,}52 & 19{,}36 \end{pmatrix}, \quad \begin{pmatrix} 0{,}641 & 0{,}640 & 2{,}721 \\ 0{,}640 & 0{,}640 & 2{,}72 \\ 2{,}721 & 2{,}72 & 11{,}56 \end{pmatrix},$$

$$\begin{pmatrix} 0{,}641 & 0{,}240 & 8{,}321 \\ 0{,}240 & 0{,}09 & 3{,}12 \\ 8{,}32 & 3{,}12 & 108{,}16 \end{pmatrix}.$$

Výběrovou varianční matice je pak čtvrtina ze součtu těchto matic, tedy

$$S = \begin{pmatrix} 1{,}70 & 1{,}075 & 9{,}35 \\ 1{,}075 & 0{,}825 & 6{,}725 \\ 9{,}35 & 6{,}725 & 76{,}30 \end{pmatrix}$$

Vlastní hodnoty matice $S$ jsou přibližně 2,7, 312,2 a 0,38. Jednotkový vlastní vektor odpovídající největší z nich pak cirka (0,122; 0,09; 0,989). První hlavní komponenta je tedy (185 5; 186,8; 172,4; 173,4; 166,5), tedy se příliš neliší od výšky zkoumaných osob. □

**9.11.** Žáci jedné třídy dosáhli následujících známek v různých předmětech:

Elementární jevy bychom tedy mohli uvažovat ve tvaru $\omega_k \in \mathbb{N}_{\geq 1} \cup \{\infty\}$, které slovně vyjadřujeme „líc padne poprvé právě v $k$–tém hodu“. Všimněme si, že jsme přidali $k = \infty$, protože formálně nemůžeme vyloučit, že budou vždycky padat pouze ruby mince.

Zjevně můžeme takový problém dobře zvládat, když vyjdeme z klasické pravděpodobnosti 0,5 pro obě možné strany mince při jednom hodu, nemůžeme ale v abstraktním modelu omezit celkový počet hodů nějakým pevným přirozeným číslem $N$. Na druhé straně, očekávaná pravděpodobnost, že padne ve všech prvních $(k-1)$ pokusech vždy rub v $n \geq k$ pokusech celkem, je dána zlomkem

$$\frac{2^{n-k}}{2^n} = 2^{-k},$$

kde v čitateli je počet možností příznivých z $n$ nezávislých hodů (tj. možností jak rozestavit libovolně dvě hodnoty do $n-k$ zbývajících pozic) a ve jmenovateli je počet všech možností výsledků. Podle očekávání tato pravděpodobnost nezávisí na zvoleném $n$ a platí $\sum_{k=1}^{\infty} 2^{-k} = 1$. Musí být proto pravděpodobnost neustálého opakování rubu nulová.

Můžeme tedy nyní zavést skutečně pravděpodobnost na základní prostoru $\Omega$ s elementárními jevy $\omega_k$, kterým přiřazujeme pravděpodobnost $2^{-k}$. Dostaneme tak pravděpodobnostní prostor ve smyslu následujících definic.

K tomuto jednoduchému ilustračnímu příkladu se ještě budeme vracet.

**9.11. Jevová pole.** Budeme pracovat s neprázdnou pevně zvolenou množinou $\Omega$ ve které se budou odehrávat všechny výsledky a kterou nazýváme *základní prostor*. Prvky $\omega \in \Omega$ představují jednotlivé *možné výsledky*. V pravděpodobnostních modelech ale nemusíme připouštět všechny možné podmnožiny coby uvažované jevy. Zejména jednotlivé prvky $\omega$ nemusí být mezi jevy. Požadujeme ale, aby uvažované podmnožiny splňovaly axiomy tzv. *$\sigma$–algeber*.



Níže uvedené axiomy jsou vybrány z větší sady přirozených požadavků v minimální podobě. První vychází z představy, že určitě budeme chtít připustit jev jistý. Druhý je vynucen požadavkem, že chceme vždy mít možnost negovat výskyt jevu, třetí potřebou zkoumat výskyt alespoň jednoho z dané spočetné množiny jevů (např. v případech podobných tomu v předcházejícím odstavci, kdy sice víme, že nikdo nehodí mincí nekonečně krát, nicméně nemůžeme předem omezit počet hodů).

### $\sigma$–ALGEBRY PODMNOŽIN

Systém podmnožin $\mathcal{A}$ základního prostoru se nazývá *jevové pole* a jeho prvky se nazývají *jevy*, jestliže platí

- $\Omega \in \mathcal{A}$, tj. základní prostor, je jevem,
- je-li $A, B \in \mathcal{A}$, pak $A \setminus B \in \mathcal{A}$, tj. pro každé dva jevy je jevem i jejich množinový rozdíl,
- je-li $A_i \in \mathcal{A}$, $i \in I$, nejvýše spočetný systém jevů, pak také jejich sjednocení je jevem, tj. $\cup_{i \in I} A_i \in \mathcal{A}$.

Jako obvykle, ze základních axiomů hned vyplývají jednoduché důsledky, které popisují další (intuitivně požadované) vlastnosti ve formě matematických vět. Čtenář by si měl promyslet, že obě vlastnosti skutečně platí.

| Žák číslo | Matika | Fyzika | Dějepis | ČJ | Tělocvik |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 2 | 2 | 1 |
| 2 | 1 | 3 | 1 | 1 | 1 |
| 3 | 2 | 1 | 1 | 1 | 1 |
| 4 | 2 | 2 | 2 | 2 | 1 |
| 5 | 1 | 1 | 3 | 2 | 1 |
| 6 | 2 | 1 | 2 | 1 | 2 |
| 7 | 3 | 3 | 2 | 2 | 1 |
| 8 | 3 | 2 | 1 | 1 | 1 |
| 9 | 4 | 3 | 2 | 3 | 1 |
| 10 | 2 | 3 | 1 | 2 | 1 |

Určete první hlavní komponentu těchto dat a vektor dat, který jejím použitím nahrazuje původní data.

**Řešení.** Vektory pozorování jsou $\mathbf{x}_1 = (1,1,2,2,1), \ldots, \mathbf{x}_{10} = (2,3,1,2,1)$, jim odpovídající varianční matice pak

$$\begin{pmatrix} 1{,}21 & 1{,}10 & -0{,}330 & -0{,}330 & 0{,}110 \\ 1{,}10 & 1, & -0{,}300 & -0{,}300 & 0{,}100 \\ -0{,}330 & -0{,}300 & 0{,}0900 & 0{,}0900 & -0{,}0300 \\ -0{,}330 & -0{,}300 & 0{,}0900 & 0{,}0900 & -0{,}0300 \\ 0{,}110 & 0{,}100 & -0{,}0300 & -0{,}0300 & 0{,}0100 \end{pmatrix}, \ldots,$$

$$\begin{pmatrix} 0{,}0100 & -0{,}100 & 0{,}0701 & -0{,}0300 & 0{,}0100 \\ -0{,}100 & 1, & -0{,}700 & 0{,}300 & -0{,}100 \\ 0{,}0701 & -0{,}700 & 0{,}490 & -0{,}210 & 0{,}0701 \\ -0{,}0300 & 0{,}300 & -0{,}210 & 0{,}0900 & -0{,}0300 \\ 0{,}0100 & -0{,}100 & 0{,}0701 & -0{,}0300 & 0{,}0100 \end{pmatrix}$$

Výběrová varianční matice je pak

$$\begin{pmatrix} 0{,}99 & 0{,}44 & -0{,}078 & 0{,}26 & -0{,}01 \\ 0{,}44 & 0{,}89 & -0{,}22 & 0{,}22 & -0{,}11 \\ -0{,}078 & -0{,}22 & 0{,}45 & 0{,}23 & 0{,}03 \\ 0{,}26 & 0{,}22 & 0{,}23 & 0{,}45 & -0{,}078 \\ -0{,}01 & -0{,}11 & 0{,}033 & -0{,}0778 & 0{,}100 \end{pmatrix},$$

její dominantní vlastní hodnota je pak cca 13,68 a jí příslušný jednotkový vlastní vektor je přibližně (0,70; 0,65; −0,13; 0,28; −0,07). Hlavní komponenta je tedy (1,58; 2,73; 2,13; 2,93; 1,45; 1,93; 4,28; 3,48; 5,26; 3,71) □

Další možnou metodou vizualizace vícerozměrných dat je tzv. shluková analýza, tou se ale zabývat nebudeme.

### C. Klasická a podmíněná pravděpodobnost

V první kapitole jsme se již seznámili s klasickou pravděpodobností, viz 1.13. Pro připomenutí si uveďme některé komplikovanější příklady.

**9.12.** Alešovi zbylo 2500 Kč z pořádání tábora. Aleš není žádný ňouma: 50 Kč přidal z kasičky a rozhodl se jít hrát ruletu na automaty. Aleš sází pouze na barvu. Pravděpodobnost výhry při sázce na barvu

Komplementy a průniky

Budeme využívat následující důsledky a terminologii:

- Komplement $A^c = \Omega \setminus A$ jevu $A$ je jevem, který nazýváme *opačný jev* k jevu $A$.
- Průnik dvou jevů opět jevem, protože pro každé dvě podmnožiny $A, B \subset \Omega$ platí

$$A \setminus (\Omega \setminus B) = A \cap B.$$

Hovoříme přitom o *současném nastoupení jevů* $A$ a $B$

Jevové pole je tedy systém podmnožin základního prostoru uzavřený na konečné průniky, spočetná sjednocení a množinové rozdíly.

Jednotlivé množiny $A \in \mathcal{A}$ nazýváme *náhodné jevy* (vzhledem k $\mathcal{A}$).

**9.12. Pravděpodobnostní prostor.** Teď popíšeme, co bude v našem matematickém modelu pravděpodobnost. Nejdříve ale ještě připomeneme názvosloví užívané už v první kapitole.

Terminologie

Používáme následující názvy týkající se jevů:

- celý základní prostor $\Omega$ se nazývá *jistý jev*, prázdná podmnožina $\emptyset \in \mathcal{A}$ se nazývá *nemožný jev*;
- jednoprvkové podmnožiny $\{\omega\} \in \Omega$ se nazývají *elementární jevy*;
- průnik jevů $\cap_{i\in I} A_i$ odpovídá *společnému nastoupení jevů* $A_i$, $i \in I$;
- sjednocení jevů $\cup_{i\in I} A_i$ odpovídá *nastoupení alespoň jednoho z jevů* $A_i$, $i \in I$;
- je-li $A \cap B = \emptyset$, pak se jevy $A, B \in \mathcal{A}$ nazývají *neslučitelné*,
- je-li $A \subset B$, pak říkáme, že jev $A$ má za *důsledek* jev $B$;
- je-li $A \in \mathcal{A}$, pak se jev $B = \Omega \setminus A$ nazývá *opačný jev k jevu* $A$, píšeme $B = A^c$.

Hned v prvním odstavci této části jsme viděli příklad pravděpodobnosti definované na nekonečné množině elementárních jevů. Obecně budeme pravděpodobnost chápat takto:

Pravděpodobnost

**Definice.** *Pravděpodobnostní prostor* je jevové pole $\mathcal{A}$ podmnožin základního prostoru $\Omega$, na kterém je definována skalární funkce $P : \mathcal{A} \to \mathbb{R}$ s následujícími vlastnosti:

- $P$ je nezáporná, tj. $P(A) \geq 0$ pro všechny jevy $A$,
- $P$ je spočetně aditivní, tj. $P(\cup_{i\in I} A_i) = \sum_{i\in I} P(A_i)$, pro každý nejvýše spočetný systém po dvou neslučitelných jevů,
- pravděpodobnost jistého jevu je 1.

Funkci $P$ říkáme *pravděpodobnost* na jevovém poli $(\Omega, \mathcal{A})$.

Z definice okamžitě vidíme, že pro opačné jevy platí

$$P(A^c) = 1 - P(A).$$

Podobně zůstávají v platnosti důkazy, které jsme o sčítání pravděpodobností odvodili pro konečné systémy (protože vztahy stejně vždy obsahovaly pouze konečně mnoho množin – promyslete si podrobněji!) Zejména tedy platí pro libovolnou množinu $k$

je 18/37. Začíná sázet na 10 Kč a pokud prohraje, v další sázce vsadí dvojnásobek toho, co v předchozí (pokud na to ještě má, pokud ne, tak končí s hrou – byť by měl ještě peníze na nějakou menší sázku). Pokud nějakou sázku vyhraje, v následující sázce hraje opět o 10 Kč. Jaká je pravděpodobnost, že při tomto postupu vyhraje dalších 2550 Kč? (jakmile bude 2550 Kč v plusu, tak končí)

**Řešení.** Nejprve spočítejme, kolikrát po sobě může Aleš prohrát. Začíná-li s 10 Kč, tak na $n$ vsazení potřebuje

$$10+20+\cdots+10\cdot 2^{n-1} = 10\cdot\left(\sum_{i=0}^{n-1} 2^i\right) = 10\cdot\left(\frac{2^n-1}{2-1}\right) = 10\cdot(2^n-1).$$

Jak snadno nahlédneme, číslo 2550 je tvaru $10(2^n-1)$ a to pro $n=8$. Aleš tedy může sázet osmkrát po sobě bez ohledu na výsledek sázky, na devět sázek by potřeboval již $10(2^9-1) = 5110$ Kč a to v průběhu hry nikdy mít nebude (jakmile bude mít 5100 Kč, tak končí). Aby tedy jeho hra skončila neúspěchem, musel by prohrát osmkrát v řadě. Pravděpodobnost prohry při jedné sázce je 19/37, pravděpodobnost prohry v osmi po sobě následujících (nezávislých) sázkách je tedy $(19/37)^8$. Pravděpodobnost, že v těchto osmi hrách vyhraje 10 Kč (při daném postupu) je tedy $1-(19/37)^8$. Na to, aby vyhrál 2550 Kč, potřebuje 255 krát vyhrát po desetikoruně. Tedy opět podle pravidla součinu je pravděpodobnost výhry

$$\left(1-\left(\frac{19}{37}\right)^8\right)^{255} \doteq 0,29.$$

Tedy pravděpodobnost výhry je nižší, než kdyby vsadil rovnou vše na jednu barvu. □

**9.13.** Samostatně si můžete vyzkoušet spočítat předchozí příklad za předpokladu, že Aleš sází stejnou metodou jako v předchozím příkladě, končí však až v okamžiku, kdy nemá žádné peníze (pokud nemá na vsazení dvojnásobku částky prohrané v předchozí sázce, ale má ještě nějaké peníze, začíná sázet znovu od 10 Kč).

S podmíněnou pravděpodobností jsme se setkali již v první kapitole, viz 1.20.

**9.14.** Z definičního vztahu podmíněné pravděpodobnosti (viz 9.14) odvoďte pro jev $A$ a jev $B$, který je disjunktním sjednocením jevů $B_1, B_2, \ldots, B_n$ vztah

$$P(A|B) = \sum_{i=1}^{n} P(A|B_i)P(B_i|B) \tag{9.1}$$

jevů $A_i$ vztah

$$\begin{aligned} P(\cup_{i=1}^k A_i) = &\sum_{i=1}^{k} P(A_i) - \sum_{i=1}^{k-1}\sum_{j=i+1}^{k} P(A_i\cap A_j) + \\ &+ \sum_{i=1}^{k-2}\sum_{j=i+1}^{k-1}\sum_{\ell=j+1}^{k} P(A_i\cap A_j\cap A_\ell) - \\ &- \cdots + \\ &+ (-1)^{k-1} P(A_1\cap A_2\cap\cdots\cap A_k). \end{aligned}$$

Stejně zůstává beze změny definice *stochasticky nezávislých jevů*, která vystihuje představu, že u nezávisle probíhajících jevů se jejich pravděpodobnosti mají násobit.

STOCHASTICKÁ NEZÁVISLOST

Jevy $A$ a $B$ jsou stochasticky nezávislé, jestliže platí

$$P(A\cap B) = P(A)P(B).$$

Je samozřejmé, že jev jistý a jev nemožný jsou stochasticky nezávislé na jakémkoliv jiném jevu.

Připomeňme, že výměnou jednoho z jevů $A_i$ v systému po dvou stochasticky nezávislých jevů $A_1, A_2, \ldots$, za jev opačný $A_i^c$ dostaneme opět systém stochasticky nezávislých jevů, a platí vztah (1.12) ze strany 23

$$\begin{aligned} P(A_1\cup\cdots\cup A_k) &= 1 - P(A_1^c\cap\cdots\cap A_k^c) = \\ &= 1-(1-P(A_1))\ldots(1-P(A_k)). \end{aligned}$$

Základním příkladem pro nás i nadále zůstává tzv. klasická konečná pravděpodobnost, kterou jsme se při tvorbě matematického modelu inspirovali. Připomeňme, že v tomto případě je $\Omega$ konečná množina, jevovým polem $\mathcal{A}$ je systém všech podmnožin v $\Omega$ a *klasická pravděpodobnost* je pravděpodobnostní prostor $(\Omega, \mathcal{A}, P)$ s pravděpodobnostní funkcí $P:\mathcal{A}\to\mathbb{R}$,

$$P(A) = \frac{|A|}{|\Omega|}.$$

To odpovídá představě o relativní četnosti $p_A$ jevu $A$ při náhodném výběru prvků z množinu $\Omega$.

Naše definice pravděpodobnosti zajišťuje rozumné chování na rostoucích či klesajících spočetných řetězcích jevů:

**9.13. Věta.** *Uvažme pravděpodobnostní prostor $(\Omega, \mathcal{A}, P)$ a neklesající řetězec jevů $A_1\subset A_2\subset\ldots$. Pak platí*

$$P\left(\bigcup_{i=1}^{\infty} A_i\right) = \lim_{i\to\infty} P(A_i).$$

*Pokud je naopak $A_1\supset A_2\supset A_3\supset\ldots$, potom platí*

$$P\left(\bigcap_{i=1}^{\infty} A_i\right) = \lim_{i\to\infty} P(A_i).$$

DŮKAZ. Přepíšeme uvažované sjednocení jevů $A=\cup_{i=1}^{\infty}A_i$ pomocí neslučitelných jevů

$$\tilde{A}_i = A_i \setminus A_{i-1},$$

definovaných pro všechna $i=2,3,\ldots$, a klademe $\tilde{A}_1 = A_1$. Potom

$$P(A) = P\left(\bigcup_{i=1}^{\infty}\tilde{A}_i\right) = \sum_{i=1}^{\infty} P(\tilde{A}_i) = \lim_{k\to\infty}\sum_{i=1}^{k} P(\tilde{A}_i).$$

**Řešení.** Všimněme si nejprve, že jevy $A \cap B_1$, $A \cap B_2$,…, $A \cap B_n$ jsou rovněž disjunktní. Můžeme tedy psát

$$\begin{aligned} P(A|B_1 \cup \cdots \cup B_n) &= \frac{P\left(A \cap (B_1 \cup \cdots \cup B_n)\right)}{P(B_1 \cup \cdots \cup B_n)} = \\ &= \frac{P\left((A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)\right)}{P(B)} = \\ &= \frac{\sum_{i=1}^{n} P(A \cap B_i)}{P(B_i)} \cdot \frac{P(B_i)}{P(B)} = \\ &= \sum_{i=1}^{n} P(A|B_i) P(B_i|B). \end{aligned}$$

□

**9.15.** Máme čtyři sáčky a v nich následující počty koulí: v prvním čtyři bílé, ve druhém tři bílé a jednu černou, ve třetím dvě bílé a dvě černé a ve čtvrtém čtyři černé. Náhodně vybereme sáček a z něj začneme bez vracení vytahovat koule. Určete pravděpodobnost, že

a) první dvě vytažené koule budou různých barev
b) a že druhá vytažená koule bude bílá, jestliže první vytažená koule byla bílá.

**Řešení.** Protože ve všech sáčcích je stejný počet koulí, je pravděpodobnost vytažení libovolné z koulí, potažmo libovolné dvojice koulí, stejná. Budeme tedy příklad řešit pomocí klasické pravděpodobnosti

a) Celkem můžeme vytáhnout 24 různých dvojic koulí, z toho je sedm dvojic složených z různobarevných koulí, hledaná pravděpodobnost je tedy 7/24.
b) Označme $A$ jev, že první vytažená koule byla bílá, $B$ jev, že druhá vytažená koule bude bílá. Potom $P(B \cap A)$ je pravděpodobnost, že první dvě vytažené koule budou bílé a ta je podobně jako v předchozím případě $10/24 = 5/12$. A opět klasickou pravděpodobností můžeme spočítat i $P(A)$, všech koulí je 16, z toho 9 bílých. Celkem

$$P(B|A) = \frac{P(B \cap A)}{P(A)} = \frac{\frac{5}{12}}{\frac{9}{16}} = \frac{20}{27}.$$

**Jiné řešení**. Jev $A$ můžeme uvážit jako sjednocení tří disjunktních jevů $A_1$, $A_2$, resp. $A_3$ a to, že jsme zvolili první sáček a z něj vytáhli bílou kouli, že jsme zvolili druhý sáček a z něj vytáhli bílou kouli a konečně že jsme zvolili třetí sáček a z něj vytáhli bílou kouli. Protože v každém sáčku je stejný počet koulí, je pravděpodobnost vytažení libovolné (bílé) koule shodná a tudíž $P(A) = \frac{9}{16}$ a

Přitom ale pro konečné součty máme

$$\sum_{i=1}^{\infty} P(\tilde{A}_i) = P(A_1) + \sum_{i=2}^{k} \big(P(A_i) - P(A_{i-1})\big) = P(A_n)$$

díky předpokládaným vztahům $A_{i-1} \subset A_i$. Tím jsme dokázali první tvrzení věty.

Ve druhém tvrzení můžeme přejít od jevů $A_i$ k jejich komplementům $B_i = A_i^c$. Ty pak splňují předpoklady první části věty. Komplement k uvažovanému průniku je

$$B = A^c = \left(\bigcap_{i=1}^{\infty} A_i\right)^c = \bigcup_{i=1}^{\infty} B_i.$$

Druhé tvrzení nyní plyne ze vztahu

$$P(A) = 1 - P(B) = \lim_{i \to \infty} \big(1 - P(B_i)\big) = 1 - \lim_{i \to \infty} P(B_i)$$

a důkaz je ukončen. □

**9.14. Podmíněná pravděpodobnost.** Popřemýšlejme nad následujícím úkolem. V předmětu $X$ obvykle uspěje u zkoušky 40% studentů, v předmětu $Y$ obvykle uspěje 80% studentů. Zaslechneme-li na chodbě jednoho ze studentů obou předmětů říkat, že u zkoušky uspěl, s jakou pravděpodobností šlo o předmět $X$?



Jak jsme stručně zmínili už v odstavci 1.20 na straně 23, umíme takové úlohy formalizovat následovně.

**Definice.** Nechť $H$ je jev s nenulovou pravděpodobností v jevovém poli $\mathcal{A}$ v pravděpodobnostním prostoru $(\Omega, \mathcal{A}, P)$. *Podmíněná pravděpodobnost* $P(A|H)$ jevu $A \in \mathcal{A}$ vzhledem k hypotéze $H$ je definována vztahem

$$P(A|H) = \frac{P(A \cap H)}{P(H)}.$$

Definice odpovídá představě z klasické pravděpodobnosti, že jevy $A$ a $H$ nastanou zároveň, za předpokladu, že jev $H$ nastal, s pravděpodobností $P(A \cap H)/P(H)$.

Je také vidět přímo z definice, hypotéza $H$ a jev $A$ jsou nezávislé tehdy a jen tehdy, je-li $P(A) = P(A|H)$.

Na první pohled se může zdát, že zavedením podmíněné pravděpodobnosti jsme nic nového nepřinesli. Ve skutečnosti jde o velice důležitý přístup, ke kterému se budeme vracet i ve statistice. Hypotéza totiž může mít charakter tzv. apriorní (tj. předem předpokládané) pravděpodobnosti a výsledné pravděpodobnosti pak říkáme aposteriorní (tj. bereme ji jako důsledek našeho předpokladu).

Přímo z definice vyplývá následující výsledek.

**Lemma.** *Nechť jev $B$ je disjunktním sjednocením jevů $B_1$, $B_2$,…, $B_n$. Potom*

$$P(A|B) = \sum_{i=1}^{n} P(A|B_i) P(B_i|B) \tag{9.2}$$

$P(A_1|A) = \frac{\frac{4}{16}}{\frac{9}{16}} = \frac{4}{9}$, $P(A_2|A) = \frac{3}{9} = \frac{1}{3}$, $P(A_3|A) = \frac{2}{9}$. Použitím vztahu (9.2) pak dostáváme

$$\begin{aligned}
&P(B|A) = \\
&= P(B|A_1)P(A_1|A) + P(B|A_2)P(A_2|A) + P(B|A_3)P(A_3|A) = \\
&= P(B|A_1) \cdot \frac{P(A_1)}{P(A)} + P(B|A_2) \cdot \frac{P(A_2)}{P(A)} + P(B|A_3) \cdot \frac{P(A_3)}{P(P(A)} = \\
&= 1 \cdot \frac{4}{9} + \frac{2}{3} \cdot \frac{3}{9} + \frac{1}{3}\frac{2}{9} = \frac{20}{27}.
\end{aligned}$$

□

**9.16.** Mirek má čtyři sáčky, v každém jsou bílé a černé kuličky a to v těchto počtech: čtyři bílé; tři bílé a jedna černá; dvě bílé a dvě černé; jedna bílá a tři černé. Mirek náhodně jeden sáček vybral a náhodně z něj vytáhl jednu kouli. Byla černá. Mirek tento sáček zahodil a náhodně vybral jeden ze zbylých tří sáčků a z něj náhodně jednu kouli. Jaká je pravděpodobnost, že bude bílá?

**Řešení.** Podobně jako v předchozím příkladě, označíme jako $A$ jev, že Mirek náhodně vybral sáček a z něj náhodně černou kouli. Tento jev disjunktním sjednocením jevů $A_i$, $i = 2, 3, 4$, kde $A_i$ je jev, že Mirek vybral $i$-tý sáček a z něj potom černou kouli. Opět je pravděpodobnost vytažení libovolné (černé) koule stejná a tedy $P(A_2|A) = \frac{1}{6}$, $P(A_3|A) = \frac{2}{6} = \frac{1}{3}$ a $P(A_4|A) = \frac{3}{6} = \frac{1}{2}$. Nechť $B$ je jev, že Mirek po zahození jednoho ze sáčků vybral ze zbylých bílou kouli. Pokud vyhodil druhý sáček, tak ve zbylých sáčcích je dohromady 7 bílých koulí a pravděpodobnost, že vytáhne jednu z nich je $P(B|A_2) = \frac{7}{12}$ (opět můžeme použít klasickou pravděpodobnost, protože v každém sáčku je stejný počet koulí a tedy má každá stejnou pravděpodobnost, že bude vytažena). Obdobně $P(B|A_3) = \frac{8}{12}$ a $P(B|A_4) = \frac{9}{12}$. Pak podle (5) je hledaná pravděpodobnost

$$\begin{aligned}
&P(B|A) = \\
&= P(B|A_2)P(A_2|A) + P(B|A_3)P(A_3|A) + P(B|A_4)P(A_4|A) = \\
&= \tfrac{7}{12} \cdot \tfrac{1}{6} + \tfrac{8}{12} \cdot \tfrac{1}{3} + \tfrac{9}{12} \cdot \tfrac{1}{2} = \tfrac{25}{36}.
\end{aligned}$$

□

**9.17.** Mirek má čtyři sáčky, v každém jsou bílé a černé kuličky a to v těchto počtech: jedna bílá a jedna černá; tři bílé a jedna černá; jedna bílá a dvě černé; jedna bílá a tři černé. Mirek náhodně jeden sáček vybral a náhodně z něj vytáhl jednu kouli. Byla bílá. Mirek tento sáček zahodil a náhodně vybral jeden ze zbylých tří sáčků a z něj náhodně jednu kouli. Jaká je pravděpodobnost, že bude bílá?

**Řešení.** Podobně jako v předchozím příkladě uvážíme jev $A$, totiž že Mirek vybral náhodně sáček a z něj náhodně bílou kouli jako sjednocení čtyř disjunktních jevů $A_1$, $A_2$, $A_3$ a $A_4$: Mirek vytáhl bílou kouli a před tím zahodil první, resp. druhý, resp. třetí, resp. čtvrtý sáček.

Důkaz. Všimněme si nejprve, že jevy $A \cap B_1, A \cap B_2, \ldots, A \cap B_n$ jsou rovněž disjunktní. Můžeme tedy psát

$$\begin{aligned}
P(A|B_1 \cup \cdots \cup B_n) &= \frac{P\left(A \cap (B_1 \cup \cdots \cup B_n)\right)}{P(B_1 \cup \cdots \cup B_n)} = \\
&= \frac{P\left((A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)\right)}{P(B)} = \\
&= \frac{\sum_{i=1}^{n} P(A \cap B_i)}{P(B_i)} \cdot \frac{P(B_i)}{P(B)} = \\
&= \sum_{i=1}^{n} P(A|B_i)P(B_i|B).
\end{aligned}$$

□

Uvažujme zvláštní případ $B = \Omega$. Pak jevy $B_i$ můžeme interpretovat jako „možné stavy světa“, $P(A|B_i)$ vyjadřuje pravděpodobnost jevu $A$, pokud je svět v $i$–tém stavu, $P(B_i|\Omega) = P(B_i)$ je pravděpodobnost toho, že svět se v $i$–tém stavu nachází. Podle předchozího lemmatu platí

$$P(A) = P(A|\Omega) = \sum_{i=1}^{n} P(A|B_i)P(B_i).$$

Tento vztah se nazývá vzorec pro celkovou pravděpodobnost (nebo věta o úplné pravděpodobnosti).

**9.15. Bayesova věta.** Jednoduchým přepsáním vzorce pro podmíněnou pravděpodobnost dostáváme

$$P(A \cap B) = P(B \cap A) = P(A)P(B|A) = P(B)P(A|B).$$

Odtud okamžitě plyne velice důležitý důsledek:

Bayesův vzorec

**Věta.** *Pro pravděpodobnost jevů A a B platí*

$$P(A|B) = \frac{P(A)P(B|A)}{P(B)} \tag{9.3}$$

$$P(A|B) = \frac{P(A)P(B|A)}{P(A)P(B|A) + P(A^c)P(B|A^c)}. \tag{9.4}$$

Prvnímu tvrzení se také říká vzorec pro *inverzní pravděpodobnosti*, zatímco druhé tvrzení je označováno jako 1. *Bayesův vzorec*.

Důkaz. První tvrzení je jen přepsáním výpočtu před větou. Abychom dostali druhé tvrzení všimněme si, že

$$P(B) = P(B \cap A) + P(B \cap A^c),$$

proto můžeme podle vzorce pro celkovou pravděpodobnost dosadit $P(B) = P(A)P(B|A) + P(A^c)P(B|A^c)$ do vzorce pro inverzní pravděpodobnost a dostáváme právě druhé tvrzení věty. □

Bayesův vzorec bývá často formulován v lehce obecnějším tvaru, který se dokáže stejným způsobem jako (9.4):

Nechť je základní prostor $\Omega$ sjednocením disjunktních jevů $A_1, \ldots A_n$. Pak pro libovolné $i \in \{1, \ldots, n\}$ platí

$$P(A_i|B) = \frac{P(B|A_i)P(A_i)}{\sum_{i=1}^{n} P(B|A_i)P(A_i)}. \tag{9.5}$$

Pravděpodobnost vytažení bílé koule z prvního sáčku je $P(A_1) = \frac{1}{4}\cdot\frac{1}{2}$ (jev $A_1$ je dán tím, že současně nastaly dva nezávislé jevy a to, že vytáhl první sáček a že z prvního sáčku vytáhl bílou kouli), podobně $P(A_2) = \frac{1}{4}\cdot\frac{3}{4}$, $P(A_3) = \frac{1}{4}\cdot\frac{1}{3}$, $P(A_4) = \frac{1}{4}\cdot\frac{1}{4}$. $P(A) = P(A_1)+P(A_2)+P(A_3)+$ $+P(A_4) = \frac{11}{24}$. Všimněme si, že pravděpodobnost $P(A)$ nemůžeme počítat klasickou pravděpodobností, tedy prostým podělením počtu bílých koulí ku počtu všech koulí, protože například pravděpodobnost vytažení dané koule v prvním sáčku je dvojnásobná oproti vytažení dané koule ze čtvrtého sáčku. Pro podmíněné pravděpodobnosti pak platí $P(A_1|A) = P(A_1)/P(A) = \frac{3}{11}$, $P(A_2|A) = \frac{9}{22}$, $P(A_3|A) = \frac{2}{11}$, $P(A_4|A) = \frac{3}{22}$. Označíme ještě písmenem $B$ jev, že Mirek po zahození jednoho ze sáčků vytáhne bílou kouli a znovu budeme chtít použít vztah (5). Zbývá ještě dopočítat $P(B|A_i)$, $i = 1, \ldots 4$. Jev $P(B|A_1)$ rozdělíme na tři disjunktní jevy $B_2$, $B_3$, $B_4$, totiž že druhá vytažená koule byla z druhého, resp. třetího, resp. čtvrtého sáčku. Celkem

$$P(B|A_1) = P(B_2|A_1) + P(B_3|A_1) + P(B_4|A_1) = \\ = \frac{1}{3}\cdot\frac{3}{4} + \frac{1}{3}\cdot\frac{1}{3} + \frac{1}{3}\cdot\frac{1}{4} = \frac{4}{9}.$$

Obdobně

$$P(B|A_2) = \frac{1}{3}\cdot\frac{1}{2} + \frac{1}{3}\cdot\frac{1}{3} + \frac{1}{3}\cdot\frac{1}{4} = \frac{13}{36},$$
$$P(B|A_3) = \frac{1}{3}\cdot\frac{1}{2} + \frac{1}{3}\cdot\frac{3}{4} + \frac{1}{3}\cdot\frac{1}{4} = \frac{1}{2},$$
$$P(B|A_4) = \frac{1}{3}\cdot\frac{1}{2} + \frac{1}{3}\cdot\frac{3}{4} + \frac{1}{3}\cdot\frac{1}{3} = \frac{19}{36}.$$

Celkem pak

$$P(B|A) = P(B|A_1)P(A_1|A) + P(B|A_2)P(A_2|A) + \\ + P(B|A_3)P(A_3|A) + P(B|A_4)P(A_4|A) = \\ = \frac{4}{9}\cdot\frac{3}{11} + \frac{13}{36}\cdot\frac{9}{22} + \frac{1}{2}\cdot\frac{2}{11} + \frac{19}{36}\cdot\frac{3}{22} = \frac{19}{44}.$$

□

**9.18.** Dva střelci vystřelí každý dvě rány na terč. První má pravděpodobnost zásahu 80%, druhý 60%. V terči se našly dvě rány. Jaká je pravděpodobnost, že obě patří prvnímu střelci?

**Řešení.** Pravděpodobnost zásahu prvního střelce jsou tedy 4/5, druhého 3/5. Uvažme dva jevy:

$A$ ... v terči se našly dva zásahy patřící prvnímu střelci,

$B$ ... v terči se našly dva zásahy.

Dle zadání úlohy máme zjistit $P(A|B)$. Rozdělme jev $B$ na šest disjunktních jevů podle toho, který střelec a který svůj výstřel do terče umístil. Jevy uvedeme v tabulce a u každého navíc spočítáme pravděpodobnost toho, že nastane. Uvědomíme si při tom, že každá

**9.16. Poznámky.** Nyní se můžeme snadno vypořádat s úvodní



otázkou z minulého odstavce. Dotaz si nejprve malinko upřesníme. Uvažujeme jev $A$ představující „student u zkoušky uspěl“ a jev $B$, který říká „student byl zkoušen z předmětu $X$“. Předpokládáme přitom, že pravděpodobnosti zkoušení z obou předmětů jsou stejné, tj. $P(B) = P(B^c) = 0{,}5$. Zatímco hledaná pravděpodobnost $P(B|A)$ je zatím spíše nejasná, pravděpodobnost $P(A|B) = 0{,}4$ je dána přímo v zadání.

To je typický případ použití Bayesových vzorců. Když přitom použijeme druhý z nich, vůbec nemusíme počítat $P(A)$:

$$P(B|A) = \frac{P(B)P(A|B)}{P(B)P(A|B) + P(B^c)P(A|B^c)} = \\ = \frac{0{,}5\cdot 0{,}4}{0{,}5\cdot 0{,}4 + 0{,}5\cdot 0{,}8} = \frac{1}{3}.$$

Abychom si přiblížili roli apriorní pravděpodobnosti hypotézy, podívejme se ještě na jeden příklad.

Řekněme, že testy připravenosti a znalostí, na základě kterých jsou studenti přijímáni na univerzitu, mají následující spolehlivost v testování inteligence osob: 99% inteligentních osob má pozitivní výsledek testu, zatímco u neinteligentních uchazečů má 0,5% z nich pozitivní výsledek testu. Chceme zjistit, s jakou pravděpodobností je náhodně vybraný student na univerzitě inteligentní.

Máme tedy jev $A$ „náhodně zvolená osoba je inteligentní“ a jev $B$ „osoba prošla testem s pozitivním výsledkem“. Dle Bayesova vzorce můžeme opět rovnou spočíst pravděpodobnost, že nastal jev $A$ za předpokladu, že nastal jev $B$. Musíme jen dodat všeobecnou pravděpodobnost $p = p(A)$, že náhodně zvolený uchazeč o studium je inteligentní.

$$P(A|B) = \frac{p\cdot 0{,}99}{p\cdot 0{,}99 + (1-p)\cdot 0{,}005}.$$

V následující tabulce je spočten pro různé hodnoty $p$ vyjádřené v jednotkách promile. V prvním sloupci tedy je výsledek za předpokladu, že je mezi uchazeči o studium každý druhý inteligentní atd.

| $p$ | 500 | 100 | 50 | 10 | 1 | 0,1 |
|---|---|---|---|---|---|---|
| $P(A\|B)$ | 0,99 | 0,96 | 0,91 | 0,67 | 0,17 | 0,02 |

Pokud tedy je každý druhý uchazeč inteligentní, máme na univerzitě používající náš test 99% inteligentních studentů. Pokud ale naší představě o inteligenci odpovídá jen 1% populace a uchazeči jsou dobrým náhodným vzorkem, pak už máme na univerzitě jen zhruba dvě třetiny inteligentních studentů ...

Představme si ale, že obdobné testování provedeme při plošném testování výskytu nějaké nemoci, třeba HIV. Dejme tomu, že máme stejně citlivý test jako výše a prověříme jím o přestávce mezi přednáškami všechny přítomné studenty. V tomto případě bychom měli předpokládat, že parametr $p$ bude obdobný jako u celé populace, tj. řekněme jeden nakažený z 10000 obyvatel, což odpovídá poslednímu sloupci v tabulce. Pak ovšem je výsledek testu katastroficky nespolehlivý. Jen asi u 2 procent pozitivně otestovaných se jedná o skutečně nemocné studenty!

Všimněme si, že problém je zapříčiněn jakýmkoliv malým výskytem pozitivních výsledků u zdravých osob. I kdybychom zlepšili test tak, že bude na 100% účinný při testu pozitivní osoby, neovlivníme skoro vůbec výsledné pravděpodobnosti v tabulce.

Při lékařské diagnostice vzácných chorob je při pozitivním výsledku testu nutné provést další test. Přitom výsledek prvního testu

uvažovaná střelba se skládá ze čtyř nezávislých jevů: výsledek střelby hráče $A$ či $B$ v prvním či druhém výstřelu. V tabulce značíme zásah jedničkou, minutí terče nulou.

| | 1. střelec | | 2.střelec | | pst nastoupení jevu |
|---|---|---|---|---|---|
| $B_1$ | 0 | 1 | 0 | 1 | $\frac{1}{5}\cdot\frac{4}{5}\cdot\frac{2}{5}\cdot\frac{3}{5}$ |
| $B_2$ | 0 | 1 | 1 | 0 | $\frac{24}{25^2}$ |
| $B_3$ | 1 | 0 | 1 | 0 | $\frac{24}{25^2}$ |
| $B_4$ | 1 | 0 | 0 | 1 | $\frac{24}{25^2}$ |
| $B_5$ | 1 | 1 | 0 | 0 | $\frac{64}{25^2}$ |
| $B_6$ | 0 | 0 | 1 | 1 | $\frac{9}{25^2}$ |

Sečtením pravděpodobnosti těchto disjunktních jevů dostáváme:

$$P(B)=\sum_{i=1}^{6}P(B_i)=169/625.$$

Nyní můžeme přistoupit k výpočtu podmíněné pravděpodobnosti podle vztahu z odstavce 9.14:

$$P(A|B)=\frac{P(A\cap B)}{P(B)}=\frac{P(B_5)}{P(B)}=\frac{\frac{64}{625}}{\frac{169}{625}}=\frac{64}{169}\doteq 0{,}38.$$

□

**9.19.** Hodíme mincí. Pokud padne líc, dáme do krabice bílou kulečníkovou kouli, pokud padne rub, dáme tam kouli černou. To opakujeme $n$-krát. Potom poslepu vybereme z krabice jednu kouli a nevrátíme ji zpět. Tato vybraná koule je bílá. Určete pravděpodobnost, že další poslepu vybraná koule je černá.

**Řešení.** V zadání není řečeno, o jakou minci jde. Aby úloha vůbec měla nějaký rozumný smysl,budeme předpokládat, že výsledky hodů touto mincí jsou nezávislé a že existuje pravděpodobnost padnutí lícové strany. Tuto pravděpodobnost označíme $p$. Ze zadaného faktu, že první vytažená koule je bílá, usoudíme, že $p>0$. Poznámku o tom, že koule jsou kulečníkové, budeme chápat tak, že jednotlivé koule jsou hmatem nerozlišitelné a tedy vyjádření „vybereme poslepu“ označuje totéž, co „vybereme náhodně“. Jev „koule v krabici je bílá“ odpovídá jevu „v příslušném hodu mincí padl líc“. To znamená, že pravděpodobnostní prostor „náhodné vytažení koule z krabice“ je izomorfní pravděpodobnostnímu prostoru „hod mincí“. Z předpokládané nezávislosti výsledků jednotlivých hodů mincí plyne nezávislost barev tažených koulí. Touto úvahou dostáváme, že hledaná pravděpodobnost je rovna $1-p$.

Je provedená úvaha přesvědčivá? Očekáváme přece, že v plné krabici je $np$ bílých a $n(1-p)$ černých koulí (přesněji řečeno, celé části těchto hodnot). Jednu bílou kouli jsme odstranili, takže relativní $P(A|B)$ má roli apriorní pravděpodobnosti $P(A)$ při druhém testu. Tento postup umožňuje „kumulovat zkušenost“.

V obou případech tedy musíme při přípravě testu dbát na to, abychom si zajistili přiměřeně vysoké $p$. U procesu přijímání studentů na univerzitu to asi bude dobrý marketing univerzity, který zajistí, aby se neinteligentní osoby hlásily v daleko menší míře, než je jejich výskyt v populaci. U testování chorob nejspíš půjde o souběh dalších skutečností a činností (např. testování HIV pozitivitu pouze u rizikových skupin obyvatelstva a podobně).

**9.17. Borelovské množiny.** Vraťme se k jednoduchému a názornému příkladu statistik kolem výsledků studentů v daném předmětu. Ten je a není podobný klasické pravděpodobnosti a s ní související statistice při házení kostkou.



Na jedné straně máme pouze konečný počet studentů a připustili jsme pouze konečný počet možných bodových hodnocení práce studenta za semestr (např. celá čísla od 0 do 20). Zároveň ale není patrně vhodné představovat si výsledky jednotlivých studentů jako analogii nezávislého házení pravidelnou kostkou. Jednak neexistuje pravidelný 21–stěn, ale hlavně by to byla skutečně divně vedená přednáška.

Na základním (konečném) prostoru $\Omega$ všech studentů máme prostě definovánu funkci bodového ohodnocení $X:\Omega\to\mathbb{R}$, která má tu vlastnost, že můžeme modelovat pravděpodobnosti příslušnosti její hodnoty do předem zvoleného intervalu při náhodném výběru studenta. Např. můžeme chtít modelovat pravděpodobnost, že student uspěl s hodnocením A nebo B. Pokud známe výsledky všech studentů, snadno dostaneme statistiky celého souboru, např. výběrový průměr $\bar{X}$ a směrodatnou odchylku $S_x$.

Patrně bychom od rozumně vedené přednášky a dobrých studentů očekávali, že nejvyšší pravděpodobnost výsledku bude ležet někde uprostřed škály v „úspěšném intervalu“, zatímco ideální výsledek plného bodového zisku příliš pravděpodobný nebude. Stejně tak bude příliš mnoho hodnot $X$ v intervalu neúspěšných hodnot na většině univerzit bráno jako výrazný neúspěch přednášejícího.

Často ale v podobných situacích máme k dispozici jen náhodně vybraných několik studentů a známe příslušné statistiky jen pro tento vybraný vzorek. Pak se můžeme dívat na příslušné hodnoty jako na vektor $(X_1,\dots,X_k)$ a bude nás opět zajímat jakákoliv funkce na tomto vektoru (např. některá z výše zmíněných statistik).

Je to typický příklad tzv. náhodných veličin a náhodných vektorů, jak je budeme definovat v dalším odstavci. Budeme chtít umět diskutovat pravděpodobnost, že hodnota $X$ padne do kteréhokoliv intervalu $(a,b)\subset\mathbb{R}$ s reálnými čísly $a,b$ a uzavřenými nebo otevřenými konci intervalu. Případně budeme potřebovat totéž pro vícerozměrné intervaly v $\mathbb{R}^k$ a vektory $(X_1,\dots,X_k)$.

Zkusme tedy uvažovat číselné veličiny $X$ na nějakém základním prostoru, tj. obyčejné funkce $X:\Omega\to\mathbb{R}$. Chceme pracovat s pravděpodobnostmi příslušnosti hodnoty $X$ do předem zadaného intervalu. Musíme proto uvést do souladu požadavky na pravděpodobnostní prostor všech jevových polí s vlastnostmi takových funkcí:



### Borelovské množiny v $\mathbb{R}^k$

Na prostoru $\mathbb{R}^k$ uvažujme nejmenší jevové pole $\mathcal{B}$ obsahující všechny $k$–rozměrné intervaly. Množinám v $\mathcal{B}$ říkáme *Borelovské množiny* na $\mathbb{R}^k$. Speciálně pro $k=1$ půjde o všechny množiny,

četnost černých koulí o něco vzroste a proto i pravděpodobnost vytažení černé koule bude větší než $1-p$. Než budete číst dále, pokuste se uhodnout, zda pravděpodobnost vytažení černé koule bude $1-p$ nebo větší, případně jak tuto pravděpodobnost ovlivní hodnota $n$ (počet koulí v krabici před vytahováním).

Úlohu budeme nyní řešit poněkud sofistikovaněji. Označme $B_i$ jev „v plné krabici je $i$ bílých koulí“ (zřejmě $i \in \{0, 1, 2, \ldots, n\}$), $A$ jev „první vytažená koule je bílá“ a $C$ jev „druhá vytažená koule je černá“. Jev $B_i$ je vlastně jevem, že v sérii $n$ hodů mincí padl líc $i$-krát, tedy

$$P(B_i) = \binom{n}{i} p^i (1-p)^{n-i}.$$

Podmíněná pravděpodobnost vytažení bílé koule za podmínky, že v krabici je právě $i$ bílých koulí, je rovna

$$P(A|B_i) = \frac{i}{n}.$$

Zajímá nás pravděpodobnost jevu $C$ když víme, že nastal jev $A$, tedy $P(C|A)$. Poněvadž jevy $B_i$ jsou neslučitelné, jsou neslučitelné i jevy $C \cap B_i$. Současně platí $C = \bigcup_{i=0}^{n} (C \cap B_i)$ a toto sjednocení je disjunktní. Proto můžeme psát

$$\begin{aligned} P(C|A) &= P\left(\bigcup_{i=0}^{n} (C \cap B_i)|A\right) = \sum_{i=0}^{n} \frac{P\big((C \cap B_i) \cap A\big)}{P(A)} = \\ &= \frac{1}{P(A)} \sum_{i=0}^{n} P\big(C \cap (A \cap B_i)\big) = \\ &= \frac{1}{P(A)} \sum_{i=0}^{n} P(A \cap B_i) P(C|A \cap B_i) = \\ &= \frac{1}{P(A)} \sum_{i=0}^{n} P(B_i) P(A|B_i) P(C|A \cap B_i). \end{aligned}$$

Za pravděpodobnost $P(A)$ můžeme ještě dosadit ze vzorce pro celkovou pravděpodobnost a dostaneme

$$\begin{aligned} P(C|A) &= \frac{\sum_{i=0}^{n} P(B_i) P(A|B_i) P(C|A \cap B_i)}{P(A)} = \\ &= \frac{\sum_{i=0}^{n} P(B_i) P(A|B_i) P(C|A \cap B_i)}{\sum_{i=0}^{n} P(B_i) P(A|B_i)}. \end{aligned} \tag{9.2}$$

Tato formulka bývá někdy nazývána 2. *Bayesův vzorec*; obecně platí za předpokladu, že prostor $\Omega$ je disjunktním sjednocením jevů $B_i$.

které ze všech intervalů obdržíme konečnými průniky a nejvýše spočetnými sjednoceními.[1]

**9.18. Náhodné veličiny.** Nyní už máme všechno připraveno pro definici náhodných veličin a náhodných vektorů. Poznamenejme již předem, že pro klasickou konečnou pravděpodobnost je náhodnou veličinou každá reálná funkce $X : \Omega \to \mathbb{R}$. Skutečně, na konečné množině $\Omega$ nabývá $X$ jen konečně mnoho hodnot a každá podmnožina v $\Omega$ je jevem.



NÁHODNÉ VELIČINY A VEKTORY

**Definice.** *Náhodná veličina* $X$ na pravděpodobnostním prostoru $(\Omega, \mathcal{A}, P)$ je taková funkce $X : \Omega \to \mathbb{R}$, že vzor $X^{-1}(B)$ patří do $\mathcal{A}$ pro každou Borelovskou množinu $B \in \mathcal{B}$ na $\mathbb{R}$. Reálná funkce $P_X(B) = P(X^{-1}(B))$ definovaná na všech intervalech $B \subset \mathbb{R}$ se nazývá *rozdělení (pravděpodobnosti) náhodné veličiny* $X$.

*Náhodný vektor* $X = (X_1, \ldots, X_k)$ na $(\Omega, \mathcal{A}, P)$ je $k$–tice náhodných veličin $X_i : \Omega \to \mathbb{R}$ definovaných na stejném základním pravděpodobnostním prostoru $(\Omega, \mathcal{A}, P)$.

Jestliže vybereme intervaly $I_1, \ldots, I_k$ v $\mathbb{R}$ a definujeme množinu $B = I_1 \times \cdots \times I_k$, pak jistě existuje pravděpodobnost současného výskytu všech $k$ jevů $X_i \in I_i$. Díky aditivitě funkce $P$ tedy bude, obdobně jako ve skalárním případě, existovat reálná funkce $P_X(B) = P(X^{-1}(B))$ definovaná na všech $k$–rozměrných intervalech $B \subset \mathbb{R}^k$. Nazýváme ji *rozdělení (pravděpodobnosti) náhodného vektoru* $X$.

**9.19. Distribuční funkce.** Rozdělení náhodných veličin zadáváme nejčastěji pomocí pravidla, jak roste pravděpodobnost s přírůstkem intervalu $B$.

Definice náhodné veličiny zajišťuje, že pro všechny intervaly $I$ s krajními body $a, b$, $-\infty \le a \le b \le \infty$, existuje pravděpodobnost jevu $P(I)$. Budeme ji zapisovat stručně $P(a < X < b)$, resp. $P(X < b)$ pokud je $a = -\infty$, pro otevřený interval $I$ a obdobně pro intervaly uzavřené nebo z jedné strany uzavřené. Ve speciálním případě jediné hodnoty píšeme $P(X = a)$.

Podobně u náhodného vektoru $X = (X_1, \ldots, X_k)$ píšeme stručně $P(a_1 < X_1 < b_1, \ldots, a_k < X_k < b_k)$, pro současné nastoupení jevů, kdy hodnoty $X_i$ padnou do uvedených intervalů (které mohou být také uzavřené neohraničené apod.).

DISTRIBUČNÍ FUNKCE

**Definice.** *Distribuční funkcí* náhodné veličiny $X$ je funkce $F_X$ $\mathbb{R} \to [0, 1]$ definovaná pro všechny $x \in \mathbb{R}$ vztahem[2]

$$F_X(x) = P(X < x).$$

*Distribuční funkcí* náhodného vektoru $(X_1, \ldots, X_k)$ je funkce $F_X : \mathbb{R}^k \to \mathbb{R}$ definovaná pro všechny $x = (x_1, \ldots, x_k) \in \mathbb{R}^k$ vztahem

$$F_X(x) = P(X_1 < x_1, \ldots, X_k < x_k).$$

[1] V této souvislosti se často také hovoří o tzv. *$\sigma$–algebře Borelovsky měřitelných množin na $\mathbb{R}^k$* a následující definici lze formulovat tak, že náhodné veličiny jsou Borelovsky měřitelné funkce.

[2] V literatuře se stejně často potkáváme také s definicí s neostrou nerovností, tj. pravděpodobnost $P(X = x)$ je ještě započtena také. V takovém případě platí obdobné vlastnosti jako ve větě 9.20, jen je distribuční funkce zprava spojitá apod.

Ještě si uvědomíme, že podle zadání úlohy jsme alespoň jednou hodili mincí a tedy $n \geq 1$. Nyní můžeme vypočítat

$$\begin{aligned}\sum_{i=0}^{n} P(B_i)P(A|B_i) &= \sum_{i=0}^{n} \binom{n}{i} p^i(1-p)^{n-i} \cdot \frac{i}{n} = \\ &= \sum_{i=1}^{n} \frac{(n-1)!}{(i-1)!(n-i)!} p^i(1-p)^{n-i} = \\ &= \sum_{i=0}^{n-1} \frac{(n-1)!}{i!(n-i-1)!} p^{i+1}(1-p)^{n-i-1} = \\ &= p\sum_{i=0}^{n-1} \binom{n-1}{i} p^i(1-p)^{n-1-i} = \\ &= p\big(p+(1-p)\big)^{n-1} = p,\end{aligned}$$

$$\begin{aligned}&\sum_{i=0}^{n} P(B_i)P(A|B_i)P(C|A\cap B_i) = \\ &= \sum_{i=0}^{n} \binom{n}{i} p^i(1-p)^{n-i} \cdot \frac{i}{n} \cdot \frac{n-i}{n-1} = \\ &= \sum_{i=1}^{n-1} \frac{(n-2)!}{(i-1)!(n-i-1)!} p^i(1-p)^{n-i} = \\ &= \sum_{i=0}^{n-2} \frac{(n-2)!}{i!(n-2-i)!} p^{i+1}(1-p)^{n-i-1} = \\ &= p(1-p)\sum_{i=0}^{n-2} \binom{n-2}{i} p^i(1-p)^{n-2-i} = \\ &= \begin{cases} p(1-p), & n > 1 \\ 0, & n = 1, \end{cases}\end{aligned}$$

takže po dosazení do druhého Bayesova vzorce dostaneme hledanou pravděpodobnost

$$P(C|A) = \begin{cases} 0, & n = 1, \\ 1-p, & n > 1. \end{cases}$$

Jednoduchá úvaha o izomorfii pravděpodobnostních prostorů tedy dala správný výsledek; výpočet pouze upozornil na triviální případ $n = 1$. □

**9.20.** V jedné vědomostní soutěži bylo hlavní výhrou Ferrari 599 GTB Fiorano. Soutěžící, který se dostal do posledního kola, byl přiveden před tři stejná vrata. Podmínkou získání výhry bylo správně uhodnout, za kterými vraty se automobil nachází. Soutěžící jedna vrata označil a poté asistent otevřel ta z neoznačených vrat, za nimiž byla koza. Poslední soutěžní otázkou bylo, zda soutěžící chce svůj tip měnit.

Je-li z kontextu zřejmé, které veličiny se distribuční funkce týká, její označení vypouštíme, tj. píšeme $F(x)$.

Další věta nás ujistí, že pro každou náhodnou veličinu umíme výhradně z distribuční funkce počítat pravděpodobnosti, že hodnoty $X$ padnou do jakéhokoliv intervalu, tj. ve skutečnosti do jakékoliv Borelovské množiny $B$.

**9.20. Věta.** *Pro každou náhodnou veličinu $X$ má její distribuční funkce $F : \mathbb{R} \to [0,1]$ následující vlastnosti*

*(1) $F$ je neklesající funkce;*
*(2) $F$ má v každém bodě $x \in \mathbb{R}$ limitu zleva i limitu zprava;*
*(3) $F$ je zleva spojitá;*
*(4) v nevlastních bodech má $F$ limity*

$$\lim_{x\to\infty} F(x) = 1, \qquad \lim_{x\to-\infty} F(x) = 0; \tag{9.6}$$

*(5) pravděpodobnost, že $X$ nabývá právě hodnotu $x$ je dána*

$$P(X = x) = \lim_{y\to x_+} F(y) - F(x). \tag{9.7}$$

*(6) Distribuční funkce náhodné veličiny má vždy nejvýše spočetně mnoho bodů nespojitosti.*

Důkaz. Důkaz spočívá ve vcelku jednoduchým přímých výpočtech. Zejména si uvědomme, že jevy $a \leq X < b$ a $X < a$ jsou disjunktní a proto platí

$$P(a \leq X < b) = P(X < b) - P(X < a) = F(b) - F(a).$$

Odtud již okamžitě z definice pravděpodobnosti plyne první dokazovaná vlastnost.

Další dvě tvrzení odvodíme z vlastností pravděpodobnosti na rostoucích či klesajících řetězcích jevů, které jsme odvodili ve větě 9.13. Zvolme nerostoucí posloupnost čísel $r_n > 0$ konvergující k 0 a uvažujme jevy $A_n$ zadané požadavkem $X < x - r_n$. Sjednocení všech těchto jevů je právě jev $A$ zadaný nerovností $X < x$. Jev $A$ přitom pochopitelně nezávisí na volbě posloupnosti $r_n$. Podle prvního tvrzení věty 9.13 tedy bude

$$P(A) = \lim_{n\to\infty} P(A_n).$$

To však podle testu konvergence funkcí pomocí posloupností (viz str. 256) znamená, že limita zleva funkce $F_X$ v bodě $x$ existuje a je rovna $P(A)$. To dokazuje polovinu tvrzení (2) a zároveň tvrzení (3).

Zcela obdobně můžeme pomocí zvolené posloupnosti čísel $r_n$ definovat jevy $A_n$ odpovídající hodnotám $X_n < x + r_n$. tentokrát máme nerostoucí řetězec $A_1 \supset A_2 \supset \ldots$ a jejich průnikem bude jev $X \leq x$. Pro pravděpodobnost jevu $A$ platí, podle druhé vlastnosti z věty 9.13,

$$P(A) = \lim_{n\to\infty} P(A_n) = P(X \leq x),$$

což ověřuje že limita zprava funkce $F$ v bodě $x$ existuje. Zároveň jsme přitom ověřili i vlastnost (5).

Limitní hodnoty z vlastnosti (4) věty se odvodí zcela obdobně s použitím věty 9.13, jak jsme výše spočetli limity zleva a zprava výše. V prvém případě půjde o jevy $A_n$ zadané pomocí $X < r_n$, pro jakoukoliv rostoucí posloupnost $r_n \to \infty$. Jejich sjednocením bude jev jistý $\Omega$. Ve druhém případě půjde o jevy $A_n$ zadané pomocí $X < r_n$ pro jakoukoliv klesající posloupnost $r_n \to -\infty$ a jejich průnikem bude jev nemožný.

**Řešení.** Nevyslovený předpoklad úlohy je ten, že soutěžící zmíněný automobil chce získat. Nejdříve zkuste ověřit, jak spolehlivou intuici pro náhodné jevy již máte. Můžete uvažovat například takto: „Za jedněmi ze zbývajících dvou vrat je Ferrari, za každými z nich se stejnou pravděpodobností. Proto je jedno, která vrata jsou označená a nemá smysl svůj tip měnit.“ Nebo: „Pravděpodobnost, že jsem si hned na začátku tipnul správně je $\frac{1}{3}$. Na této pravděpodobnosti ta ukázaná koza nic nezmění, takže pravděpodobnost, že jsem tipoval špatně je $\frac{2}{3}$. Proto když tip změním, tak s pravděpodobností $\frac{2}{3}$ vyhraji.“

Změnit tip je rozumné pouze v případě, že pravděpodobnost automobilu za neoznačenými a neotevřenými vraty je větší, než jeho pravděpodobnost za vraty označenými. Pro výpočet si označíme jevy $H$ „původní tip je správný“, $A$ „tip byl změněn“ a $C$ „soutěžící vyhrál“. Zajímají nás tedy pravděpodobnosti $P(C|A)$ a $P(C|A^c)$.

Soutěžící nejprve označil jedna vrata ze tří, Ferrari je jen za jedněmi z nich. Tedy

$$P(H) = \frac{1}{3}, \quad P(H^c) = 1 - \frac{1}{3} = \frac{2}{3}.$$

Změnu tipu považujeme za jev nezávislý na tipu původním, tedy

$$P(A|H) = P(A|H^c) = P(A), \quad P(A^c|H) = P(A^c|H^c) = P(A^c).$$

Pokud původní tip byl správný a soutěžící rozhodnutí změnil, pak nemohl vyhrát; naopak, pokud původní tip byl špatný a soutěžící rozhodnutí změnil, vyhrál jistě, tedy

$$P(C|A \cap H) = 0 = P(C|A^c \cap H^c),$$
$$P(C|A^c \cap H) = 1 = P(C|A \cap H^c).$$

Ze druhého Bayesova vzorce (‖9.2‖) nyní dostaneme

$$P(C|A) = \frac{P(H)P(A|H)P(C|A \cap H) + P(H^c)P(A|H^c)P(C|A \cap H^c)}{P(A)} = P(H^c) = \frac{2}{3}$$

a analogicky

$$P(C|A^c) = \frac{P(H)P(A^c|H)P(C|A^c \cap H) + P(H^c)P(A^c|H^c)P(C|A^c \cap H^c)}{P(A^c)} = P(H) = \frac{1}{3}.$$

Dostali jsme, že $P(C|A) > P(C|A^c)$, a proto je výhodné změnit tip. □

*9.21.* Máme dva sáčky. V jednom jsou dvě bílé a dvě černé v druhém jedna bílá a dvě černé. Náhodně vybereme sáček a z něj postupně (bez

Zbývá dokázat poslední tvrzení. Podle již dokázaných vlastností jsou body nespojitosti distribuční funkce právě ty hodnoty $x$, ve kterých má náhodná veličina tuto hodnotu s nenulovou pravděpodobností, tj. $P(X = x) \neq 0$. Označme nyní $M_n$ množinu těch bodů $x$, pro které je $P(X = x) > \frac{1}{n}$. Evidentně je množina $M$ všech bodů nespojitosti dána jako sjednocení $M = \cup_{n=2}^{\infty}$. Protože je ale součet pravděpodobností disjunktních jevů vždy nejvýše jedna, nemůže obsahovat $M_n$ více než $n - 1$ prvků. Je tedy $M$ spočetným sjednocením konečných množin a je tedy sama spočetná. □

Nyní je zřejmé, že můžeme z distribuční funkce snadno spočíst pravděpodobnost, že hodnota náhodné veličiny padne do jakéhokoliv daného intervalu. Zadává tedy skutečně distribuční funkce $F_X$ celé rozložení pravděpodobnostní náhodné veličiny $X$.

**9.21. Diskrétní a spojité náhodné veličiny.** Náhodné veličiny se



chovají zásadně odlišně podle toho, jestli je veškerá nenulová pravděpodobnost „soustředěna do několika konečných hodnot“ nebo je naopak „spojitě rozprostřena“ po (části) reálné osy.

### Diskrétní náhodné veličiny

Jestliže náhodná veličina $X$ na pravděpodobnostním prostoru $(\Omega, \mathcal{A}, P)$ nabývá jen konečně mnoha různých hodnot $x_1, x_2, \ldots, x_n \in \mathbb{R}$ nebo případně spočetně mnoha reálných hodnot $x_1, x_2, \ldots$, říkáme, že jde o *diskrétní náhodnou veličinu*.

Definujeme pak *pravděpodobnostní funkci* $f(x)$ vztahem

$$f(x) = \begin{cases} P(X = x_i) & x = x_i \\ 0 & \text{jinak.} \end{cases}$$

Protože je pravděpodobnost spočetně aditivní a jednotlivé jevy $X = x_i$ jsou disjunktní, je součet všech hodnot $f(x_i)$ dán buď konečným součtem nebo absolutně konvergentní řadou

$$\sum_i f(x_i) = 1.$$

Pro rozdělení pravděpodobnosti veličiny $X$ platí

$$P(X^{-1}(B)) = \sum_{x_i \in B} f(x_i)$$

a tedy zejména je distribuční funkce tvaru

$$F_X(t) = \sum_{x_i < t} f(x_i).$$

Všimněme si, že distribuční funkce $F(x)$ diskrétní náhodné veličiny je po částech konstantní a $F(x) = 1$ pro $x$ větší než všechna $x_i$.

Každá náhodná veličina definovaná na klasickém konečném pravděpodobnostním prostoru je diskrétní.

I když hodnoty náhodné veličiny $X$ nejsou diskrétní, můžeme postupovat podobně. Intuitivně lze při infinitesimální změně hodnoty $x$ o přírůstek $dx$ uvažovat takto: hustotu $f(x)$ pravděpodobnosti pro náhodnou veličinu $X$ si představíme jako

$$P(x \leq X < x + dx) = f(x)dx.$$

To znamená, že chceme pro $-\infty \leq a \leq b \leq \infty$

$$P(a \leq X < b) = \int_a^b f(x)dx.$$

vracení) dvě koule. Jaká je pravděpodobnost, že druhá vytažená bude černá, jestliže první vytažená koule byla bílá. ○

### D. Co je pravděpodobnost?

Nejprve si připomeňme geometrickou pravděpodobnost, jak jsme se s ní setkali v 1.21.

**9.22. Buffonova jehla.** Jehlu o délce $l$ házíme na síť rovnoběžek tvořících pásy o šířce $l$. Jaká je pravděpodobnost, že jehla po dopadu zůstane v pozici protínající některou rovnoběžku?

**Řešení.** Pozice jehly po dopadu je dána dvěma nezávislými parametry, totiž vzdáleností $d$ jejího středu od nejbližší rovnoběžky, ($d \in [0, l/2]$) a úhlem $\alpha$ ($\alpha \in [0, \pi/2]$), který jehla svírá s rovnoběžkami. Podmínka, že jehla protne některou z rovnoběžek je ekvivalentní nerovnosti $l/2 \sin\alpha > d$. Oblast možných jevů, možných dvojic $(\alpha, d)$, je obdélník $\pi/2 \times l/2$. Příznivé jevy, tedy ty dvojice $(\alpha, d)$, pro které $l/2 \sin\alpha > d$, odpovídají bodům v obdélníku ležícím pod křivkou $l/2 \sin\alpha$ (přičemž za proměnnou považujeme $\alpha$, kterou vynášíme na osu $x$). Obsah útvaru je podle 6.35

$$\int_0^{\frac{\pi}{2}} \frac{l}{2} \sin\alpha \, \mathrm{d}\alpha = \frac{l}{2}.$$

Hledanou pravděpodobnost tak určíme (viz 1.21) jako

$$\frac{\frac{l}{2}}{\frac{\pi}{2} \cdot \frac{l}{2}} = \frac{2}{\pi}.$$

□

Následující (známý) příklad, ve kterém rovněž využijeme geometrickou pravděpodobnost, ilustruje, že si musíme dávat velký pozor na to, co považujeme za „zřejmé“

**9.23. Bertrandův paradox.** Určete pravděpodobnost toho, že náhodně vybraná tětiva v dané kružnici bude mít délku větší, než je strana rovnostranného trojúhelníka vepsaného do této kružnice.

**Řešení.** Ukážeme tři různé způsoby, jak „tuto“ pravděpodobnost odvodit.

1) Každá tětiva je jednoznačně dána svým středem. Její náhodný výběr je tedy dán náhodným výběrem jejího středu. Tětiva je delší než strana vepsaného rovnostranného trojúhelníka, leží-li její střed uvnitř soustředné kružnice o poloviční poloměru. Střed vybíráme „náhodně“ z celé kružnice, je tedy pravděpodobnost, že padne do vnitřního kruhu dána poměrem obsahů těchto kruhů, tedy je to $\frac{1}{4}$.

2) Oproti předcházejícímu odvození provedeme úvahu, že hledaná pravděpodobnost by měla být stejná, omezíme-li se pouze na tětivy

#### Spojité náhodné veličiny

Náhodná veličina $X$, pro kterou existuje její *hustota pravděpodobnosti* $f$ splňující

$$F_X(b) = \int_{-\infty}^{b} f(x)dx,$$

se nazývá *spojitá náhodná veličina*.

Všimněme si, že distribuční funkce $F(x)$ spojité náhodné veličiny $X$ je vždy diferencovatelná a její derivace se rovná hustotě pravděpodobnosti $X$, tj. platí $F'(x) = f(x)$.



Samozřejmě se také můžeme setkat se smíšeným chováním u veličin, které mají část pravděpodobnosti rozprostřenu spojitě, některých hodnot ale nabývají s nenulovou pravděpodobností. Představme si třeba chaotického přednášejícího, který s pravděpodobností $p$ zůstává stát na místě za řečnickým pultíkem, jakmile se však odtud pohne, je jeho pozice v kterémkoliv jiném místě na stupínku stejně pravděpodobná.

Bude tedy příslušná náhodná veličina udávající jeho polohu mít distribuční funkci (zavádíme si souřadnice tak, že pultík je v pozici 0 a posluchárna je ohraničena hodnotami $\pm 1$)

$$F(t) = \begin{cases} 0 & \text{je-li } t \le -1 \\ \frac{1-p}{2}(t+1) & \text{je-li } t \in (-1, 0) \\ p + \frac{1-p}{2}(t+1) & \text{je-li } t \in [0, 1) \\ 1 & \text{je-li } t \ge 1. \end{cases}$$

Distribuční funkce takovýchto veličin můžeme často přímo vyjadřovat pomocí Riemannova-Stieltjesova integrálu $F(t) = \int_{-\infty}^{t} f(x)d(g(x))$, který jsme zavedli v odstavci 6.48 na straně 369. V předchozím příkladu bychom zvolili třeba $f(x) = 1$ a

$$g(x) = \begin{cases} -1 & \text{pro } x \le -1 \\ \frac{1-p}{2}x & \text{pro } -1 < x < 0 \\ \frac{1-p}{2}x + p & \text{pro } 0 \le x < 1 \\ \frac{1+p}{2} & \text{pro } x \ge 1. \end{cases}$$

Připomeňme, že distribuční funkce nemůže mít více než spočetně mnoho bodů nespojitosti.

**9.22. Několik diskrétních rozdělení.** Požadavky na vlastnosti rozdělení náhodných veličin zpravidla vychází z modelovaných situací a ve skutečnosti pak ani nemáme moc možností, jak rozdělení pravděpodobnosti může vypadat.



Uvedeme přehled nejjednodušších diskrétních rozdělení.

#### Degenerované rozdělení

Rozdělení odpovídající konstantní náhodné veličině $X = \mu$ se nazývá *degenerované rozdělení* $\mathrm{Dg}(\mu)$.

Jeho distribuční funkce $F_X$ a pravděpodobnostní funkce $f_X$ jsou dány

$$F_X(t) = \begin{cases} 0 & t \le \mu \\ 1 & t > \mu \end{cases} \qquad f_X(t) = \begin{cases} 1 & t = \mu \\ 0 & \text{jinak} \end{cases}.$$

Nyní popišme pokus s pouze dvěma možnými výsledky, kterým budeme říkat zdar a nezdar. Pokud má zdar pravděpodobnost $p$, pak nezdar musí mít pravděpodobnost $1 - p$.

daného směru. Středy tětiv jednoho směru leží v dané kružnici na jediném jejím průměru daného směru. Středy vyhovujících tětiv pak jsou ty z tohoto průměru, které leží uvnitř vnitřní kružnice (viz předchozí bod), tedy na jejím průměru daného směru. Poměry průměrů kružnic jsou $1:2$, hledaná pravděpodobnost je tedy $\frac{1}{2}$.

3) Tětiva kružnice je též určena svými krajními body (ležícími na kružnici). Pokud jeden z krajních bodů tětivy, řekněme $A$, fixujeme (opět vzhledem k symetrii by to nemělo ovlivnit výslednou pravděpodobnost), tak druhý, aby tětiva vyhověla požadavku, musí ležet na kratším oblouku $BC$, kde $ABC$ je rovnostranný trojúhelník vepsaný do dané kružnice. Délka tohoto oblouku činí jednu třetinu z obvodu kružnice. Hledaná pravděpodobnost je tedy $\frac{1}{3}$.

Jak je možné, že nám vyšla pokaždé jiná pravděpodobnost? Zadání úlohy je totiž nejednoznačné. Je nutné specifikovat, co to znamená „náhodný“ výběr tětivy. Každý ze tří pravděpodobností popisuje hledanou pravděpodobnost při vybírání tětivy popsaným způsobem. Tyto způsoby nejsou ekvivalentní, což kromě spočtené pravděpodobnosti potvrzuje i rozložení středů takto vybíraných tětiv: v prvním případě jsou středy rovnoměrně rozmístěny uvnitř celé kružnice. Ve druhém a ve třetím případě je větší koncentrace středů u středu dané kružnice.

□

**9.24. Dvě obálky.** V každé ze dvou obálek je umístěna určitá suma peněz. Víme, že v jedné obálce je dvojnásobek toho, co v druhé. Můžeme si zvolit jednu z obálek (a vzít si obnos v ní). Po volbě jsme dotázáni, jestli nechceme výběr změnit (a vzít si sumu z druhé obálky). Je výhodné svoje rozhodnutí změnit?

**Řešení.** Na první pohled musí být úplně jedno, kterou obálku zvolíme. Pravděpodobnost, že si vybereme tu s větším obnosem je $1/2$, nemá tedy smysl rozhodnutí měnit.

Proveďme však následující úvahu: v prvně zvolené obálce je suma $a$. Ve druhé je tedy obnos $a/2$, či $2a$, a to každý s poloviční pravděpodobností. Pokud tedy změníme své rozhodnutí, tak s pravděpodobností $1/2$ získáme obnos $a/2$, s pravděpodobností $1/2$ obnos $2a$, tedy průměrně

$$\frac{1}{2}\frac{a}{2}+\frac{1}{2}2a=\frac{5}{4}a.$$

Bylo by tedy výhodné volbu změnit. Co je špatného na této úvaze?

Je to několik věcí. Je to průměrování fiktivních výher $a/2$ a $2a$. Situace je totiž dána dvěma obálkami s výhrami $a$ a $2a$. Při změně obálky budou naše výhry opět buď $a$ (pokud jsme si na počátku vybrali obálku se sumou $2a$), nebo $2a$ (pokud jsme si na poprvé vybrali

### Alternativní rozdělení

Rozdělení náhodné veličiny $X$ s dvěma hodnotami 0 pro nezdar a 1 pro zdar, přičemž zdar nastává s pravděpodobností $p$, říkáme *alternativní rozdělení* $\mathrm{A}(p)$. Jeho distribuční a pravděpodobnostní funkce jsou tvaru:

$$F_X(t)=\begin{cases}0 & t\le 0\\ 1-p & 0<t\le 1\\ 1 & t>1\end{cases}\qquad f_X(t)=\begin{cases}p & t=1\\ 1-p & t=0\\ 0 & \text{jinak.}\end{cases}$$

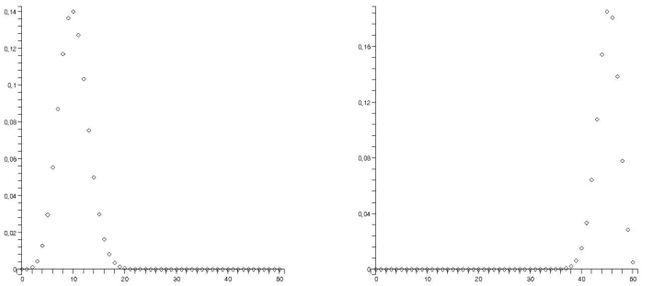
Uvažme dále rozdělení veličiny $X$ odpovídající $n$–krát nezávisle opakovanému pokusu popsanému alternativním rozdělením, přičemž naše náhodná veličina měří počet zdarů. Je tedy zjevné, že pravděpodobnostní funkce bude mít nenulové hodnoty právě v celých číslech $0,\dots,n$ odpovídajícím celkovému počtu úspěchů v pokusech (a nezáleží nám na pořadí).

### Binomické rozdělení

*Binomické rozdělení* $\mathrm{Bi}(n,p)$ má pravděpodobnostní funkci

$$f_X(t)=\begin{cases}\binom{n}{t}p^t(1-p)^{n-t} & t\in\{0,1,\dots,n\}\\ 0 & \text{jinak}\end{cases}.$$

Na obrázku jsou pravděpodobnostní funkce pro $\mathrm{Bi}(50,0{,}2)$, a $\mathrm{Bi}(50,0{,}9)$. Rozdělení pravděpodobnosti odpovídá intuici, že nejvíce výsledků bude blízko u hodnoty $np$:



Uvažujme nezávisle prováděné pokusy s alternativním rozdělením pravděpodobnosti $\mathrm{A}(p)$ jako u binomického rozdělení a zvolme si kladné přirozené číslo $r$. Budeme pokračovat v pokusech tak dlouho, dokud nenastane právě $r$ zdarů.

Náhodná veličina $X$ bude dána počtem nezdarů předcházejících $r$-tému zdaru. V případě $r=1$ tedy jsme zpět u našeho příkladu z 9.10. Náhodný jev $X=k$ nastane, právě když v prvních $k+r-1$ pokusech nastane právě $r-1$ zdarů a přitom zároveň v $(k+r)$-tém pokusu nastane zdar.

### Geometrické rozdělení

Náhodná veličina $X$, která je dána počtem nezdarů před dosažením právě $r$-tého zdaru, má rozdělení pravděpodobnosti

$$P(X=k)=\binom{k+r-1}{r-1}p^r(1-p)^k,\quad k=0,1,2,\dots$$

Tomuto rozdělení že také říká *negativně binomické rozdělení*, v případě $r=1$ pak *geometrické rozdělení*.

obálku se sumou $a$). Tedy celková průměrná výhra je (jako na začátku)

$$\frac{1}{2}a + \frac{1}{2}2a = \frac{3}{2}a. \qquad \square$$

### E. Náhodné veličina, hustota, distribuční funkce

**9.25.** Při jednom hodu kostkou je zřejmě množina elementárních jevů $\Omega = \{\omega_1, \ldots, \omega_6\}$, kde $\omega_i$ znamená, že na kostce padne číslo $i$. Jevovým polem nechť je

$$\mathcal{A} = \{\emptyset, \{\omega_1, \omega_2\}, \{\omega_3, \omega_4, \omega_5, \omega_6\}, \Omega\}.$$

Zjistěte, jestli zobrazení $X : \Omega \to \mathbb{R}$ dané předpisem

i) $X(\omega_i) = i$ pro každé $i \in \{1, 2, 3, 4, 5, 6\}$,

ii) $X(\omega_1) = X(\omega_2) = -2, X(\omega_3) = X(\omega_4) = X(\omega_5) = X(\omega_6) = 3$

je náhodnou veličinou vzhledem k $\mathcal{A}$.

**Řešení.** Nejprve je dobré se přesvědčit, že množina $\mathcal{A}$ opravdu splňuje všechny axiomy v 9.11 a je tedy dobře definovaným jevovým polem. Pak podle definice 9.18 je náhodná veličina taková funkce $X : \Omega \to \mathbb{R}$, že vzor každé Borelovské množiny $B \subset \mathbb{R}$ leží v $\mathcal{A}$. Pokud v případě i) uvážíme například uzavřený interval $[2, 3]$, je jasné, že $X^{-1}([2, 3]) = \{\omega_2, \omega_3\} \notin \mathcal{A}$. Funkce $X$ tedy v tomto případě není náhodná veličina.

V případě ii) se naopak lze lehce přesvědčit, že $X$ je náhodná veličina. Vezmeme-li totiž libovolný interval v $\mathbb{R}$, tak mohou nastat právě čtyři možnosti. Buď neobsahuje číslo -2 ani 3, pak je vzorem $X$ prázdná množina, pokud obsahuje jen -2, je vzorem $\{\omega_1, \omega_2\}$, pokud obsahuje jen 3, je vzorem $\{\omega_3, \omega_4, \omega_5, \omega_6\}$ a pokud interval obsahuje obě čísla, pak je vzorem celá množina $\Omega$. Ve všech případech vzor leží v jevovém poli $\mathcal{A}$. $\square$

**9.26.** Je dáno jevové pole $(\Omega, \mathcal{A})$, kde $\Omega = \{\omega_1, \omega_2, \omega_3, \omega_4, \omega_5\}$ a

$$\mathcal{A} = \{\emptyset, \{\omega_1, \omega_2\}, \{\omega_3\}, \{\omega_4, \omega_5\}, \{\omega_1, \omega_2, \omega_3\}, \{\omega_1, \omega_2, \omega_4, \omega_5\}, \{\omega_3, \omega_4, \omega_5\}, \Omega\}.$$

Najděte co nejobecnější zobrazení $X : \Omega \to \mathbb{R}$, které bude náhodnou veličinou vzhledem k $\mathcal{A}$.

**Řešení.** Protože se jevy $\omega_1, \omega_2$ nevyskytují samostatně v $\mathcal{A}$, je zřejmé, že náhodná veličina $X$ je musí zobrazit na stejné číslo, tj. $X(\omega_1) = X(\omega_2) = a$, pro nějaké $a \in \mathbb{R}$. Ze stejného důvodu musí být $X(\omega_4) = X(\omega_5) = b$, pro nějaké $b \in \mathbb{R}$. Obsahuje-li interval obě číslo $a$ i $b$, pak je jeho vzorem $\{\omega_1, \omega_2, \omega_4, \omega_5\} \in \mathcal{A}$, což je v pořádku. Zbývá jev $\omega_3$, který se může zobrazit na libovolné $c \in \mathbb{R}$. Jednoduše se potom přesvědčíme o tom, že vzory všech intervalů

Geometrické rozdělení se ve fyzice objevuje u tzv. Einsteinovy–Boseovy statistiky.

**9.23. Poissonovo rozdělení.** V praktických úlohách často úvaha o binomickém rozdělení vede k dalším modelovým případům.



Uvažme situaci, kdy do $n$ přihrádek rozdělujeme $r$ vzájemně nerozlišitelných předmětů. Umístění kteréhokoliv předmětu do pevně zvolené přihrádky má pravděpodobnost $1/n$ (každá z nich je stejně pravděpodobná).

Náhodnou veličinu, která popisuje počet $X$ předmětů v jedné pevně zvolené přihrádce můžeme popsat následovně. Máme možnosti hodnot $X = k$, kde $k = 0, \ldots, r$ a pravděpodobnost jednotlivých hodnot je

$$P(X = k) = \binom{r}{k}\left(\frac{1}{n}\right)^k\left(1 - \frac{1}{n}\right)^{r-k} = \binom{r}{k}\frac{(n-1)^{r-k}}{n^r}.$$

Jde proto o rozložení $X$ typu $\mathrm{Bi}(r, 1/n)$.

S takovouto veličinou se můžeme potkat např. u popisu fyzikální soustavy s velikým počtem molekul plynu. Přihrádky představují malé objemy prostoru a sledujeme rozložení molekul. Zajímá nás pak, co se bude dít s veličinami $X_n$, když bude vzrůstat počet přihrádek $n$ společně s počtem předmětů $r_n$ tak, že v průměru nám na každou přihrádku bude připadat (přibližně) stejný počet prvků $\lambda$.

Zajímá nás tedy chování našeho rozdělení veličin $X_n$ při limitním přechodu $n \to \infty$. Standardní úpravy (můžeme je brát i jako výzvu k opakování postupů z analýzy funkcí jedné proměnné!) vedou při $\lim_{n\to\infty} r_n/n = \lambda$ k výsledku:

$$\begin{aligned}
\lim_{n\to\infty} P(X_n = k) &= \lim_{n\to\infty}\binom{r_n}{k}\frac{(n-1)^{r_n-k}}{n^{r_n}} = \\
&= \lim_{n\to\infty}\frac{r_n(r_n-1)\ldots(r_n-k+1)}{(n-1)^k}\frac{1}{k!}\left(1-\frac{1}{n}\right)^{r_n} = \\
&= \frac{\lambda^k}{k!}\lim_{n\to\infty}\left(1+\frac{-\frac{r_n}{n}}{r_n}\right)^{r_n} = \\
&= \frac{\lambda^k}{k!}\,\mathrm{e}^{-\lambda},
\end{aligned}$$

protože obecně funkce $(1+x/n)^n$ konvergují stejnoměrně k funkci $\mathrm{e}^x$ na každém omezeném intervalu v $\mathbb{R}$.

Poissonovo rozdělení

*Poissonovo rozdělení* $\mathrm{Po}(\lambda)$ popisuje náhodné veličiny s pravděpodobnostní funkcí

$$f_X(t) = \begin{cases} \frac{\lambda^k}{k!}\,\mathrm{e}^{-\lambda} & t \in \mathbb{N} \\ 0 & \text{jinak.} \end{cases}$$

Samozřejmě platí

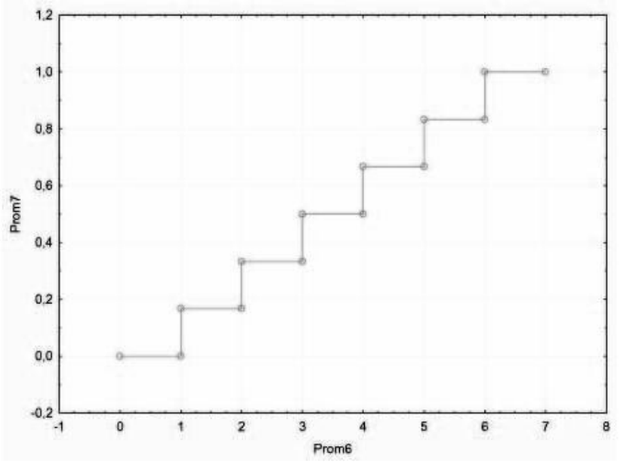
$$\sum_{k=0}^{\infty} f_X(k) = \sum_k \frac{\lambda^k}{k!}\,\mathrm{e}^{-\lambda} = \mathrm{e}^{-\lambda}\sum_k \frac{\lambda^k}{k!} = \mathrm{e}^{-\lambda+\lambda} = 1.$$

Jak jsme odvodili výše, toto diskrétní rozdělení $\mathrm{Po}(\lambda)$ s libovolným $\lambda > 0$ (rozložené do nekonečně mnoha bodů) dobře aproximuje binomická rozložení $\mathrm{Bi}(n, p_n)$, kde $np_n = \lambda$, pro veliká $n$.

pro takto definované $X$ jsou množiny v $\mathcal{A}$, tj. $X$ je náhodná veličina vzhledem k $\mathcal{A}$. □

**9.27.** Náhodná veličina $X$ nabývá hodnoty $i$ s pravděpodobností $P(X = i) = \frac{1}{6}$ pro $i = 1, \ldots, 6$. Zapište distribuční funkci $F_X(x)$ a načrtněte její graf.

**Řešení.** Z definice 9.19 je distribuční funkce rovna $F_X(x) = P(X < x)$. To znamená, že $F_X(x) = 0$ pro $x < 1$, $F_X(x) = \frac{[x]}{6}$ pro $1 \leq x < 6$, kde $[x]$ značí celou část čísla $x$, a $F_X(x) = 1$ pro $x \geq 6$. Graficky znázorněno




□

**9.28.** Střelec střílí do terče, dokud ho netrefí. Má v zásobě 4 náboje. Pravděpodobnost zásahu je přitom při každém výstřelu rovna 0,6. Nechť náhodná veličina $X$ udává počet nespotřebovaných nábojů. Určete pravděpodobnostní a distribuční funkci $X$ a nakreslete jejich grafy.

**Řešení.** Pravděpodobnost, že střelec $k$–krát terč netrefí a pak ho trefí je zřejmě rovna $0{,}4^k \cdot 0{,}6$. Proto $f_X(x) = P(X = x) = 0{,}4^{3-x} \cdot 0{,}6$ pro $x \in \{1, 2, 3\}$. Pokud střelec netrefí terč na tři pokusy, už mu každopádně nezbude žádný náboj, ať už ho v posledním pokusu trefí nebo ne. Proto $f_X(0) = P(X = 0) = 0{,}4^3$.

Z definice distribuční funkce 9.19 je

$$F_X(x) = P(X < x) = \begin{cases} 0 & \text{pro } x \leq 0, \\ 0{,}4^3 = 0{,}064 & \text{pro } x \in (0, 1], \\ 0{,}4^3 + 0{,}4^2 \cdot 0{,}6 = 0{,}16 & \text{pro } x \in (1, 2], \\ 0{,}4^3 + 0{,}4^2 \cdot 0{,}6 + 0{,}4 \cdot 0{,}6 = 0{,}4 & \text{pro } x \in (2, 3], \\ 1 & \text{pro } x > 3. \end{cases}$$

Grafy pravděpodobnostní a distribuční funkce vypadají následovně.

**9.24. Dva příklady Poissonova rozdělení.** Kromě výše



zmíněného fyzikálního modelu lze takové chování při sledování výskytu jevů v prostoru s konstantní očekávanou hustotou na jednotku objemu (např. při sledování výskytu bakterií na sklíčku pod mikroskopem, které se stejně pravděpodobně vyskytují v kterékoliv jeho části). Je-li „průměrná hustota výskytu“ v jednotkové ploše $\lambda$, pak při rozdělení celé oblasti na $n$ stejných částí bude výskyt $k$ jevů v jedné vybrané části modelován náhodnou veličinou $X$ s Poissonovým rozdělením. Takovéto pozorování při praktické diagnostice v biochemické laboratoři umožní výpočet docela přesného celkového počtu bakterií ve vzorku ze skutečného počtu odečteného jen v několika náhodně vybraných malých částech vzorku.



Zkusme nyní popsat události, které se vyskytují náhodně v čase $t \geq 0$ a přitom pravděpodobnost výskytu v následujícím malinkém časovém intervalu o délce $h$ nezávisí na předchozí historii a je rovna stále stejné hodnotě $h\lambda$ pro pevné $\lambda > 0$. Přitom pravděpodobnost, že nastane jev v daném malinkém intervalu více než jedenkrát bude velmi malá.

Označme si náhodnou veličinu $X_t$ vyčíslující počet výskytu sledovaného jevu v intervalu $[0, t)$ a zkusme vyjádřit naše požadavky infinitesimálně. Chceme, aby

- pravděpodobnost právě jedné události v každém časovém úseku o délce $h$ byla rovna $h\lambda + \alpha(h)$, kde funkce $\alpha(h)$ splňuje $\lim_{h \to 0_+} \frac{\alpha(h)}{h} = 0$;
- pravděpodobnost $\beta(h)$, že nastane více než jedna událost v časovém úseku délky $h$, splňuje $\lim_{h \to 0_+} \frac{\beta(h)}{h} = 0$;
- jevy $X_t = j$ a $X_{t+h} - X_t = k$ jsou nezávislé pro všechny $j, k \in \mathbb{N}$ a $t, h > 0$.

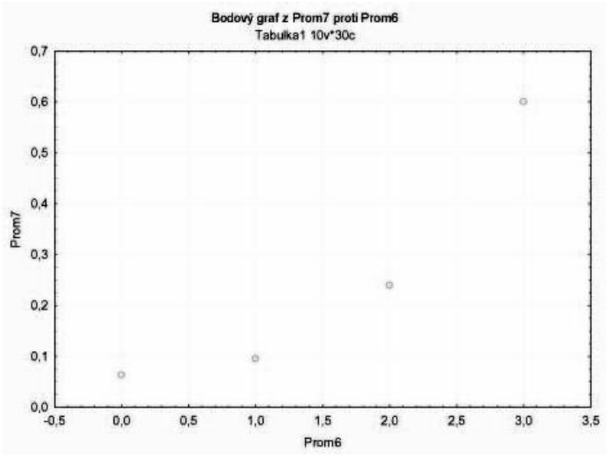
Označíme si funkce $p_k(t) = P(X_t = k)$, $k \in \mathbb{N}$, a položíme samozřejmé okrajové podmínky $p_0(0) = 1$ a $p_k(0) = 0$ pro $k > 0$. Nyní přímo spočteme

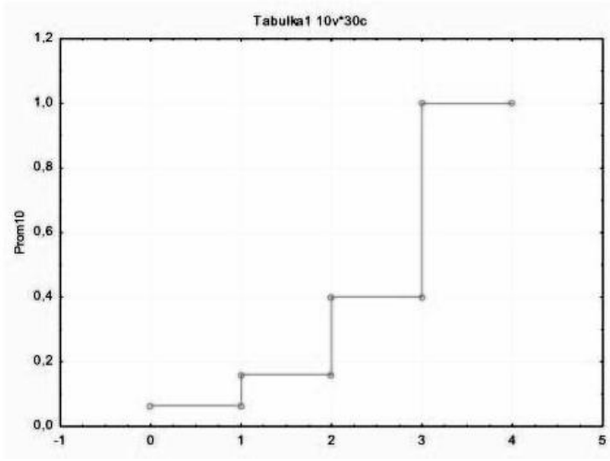
$$\begin{aligned} p_0(t + h) &= p_0(t) P(X_{t+h} - X_t = 0) = \\ &= p_0(t)(1 - h\lambda - \alpha(h) - \beta(h)) \end{aligned}$$

a podobně

$$\begin{aligned} p_k(t + h) &= P(X_t = k, X_{t+h} - X_t = 0) + \\ &\quad + P(X_t = k - 1, X_{t+h} - X_t = 1) + \\ &\quad + P(X_t \leq k - 2, X_{t+h} = k) = \\ &= p_k(t) P(X_{t+h} - X_t = 0) + p_{k-1} P(X_{t+h} - X_t = 1) + \\ &\quad + \sum_{i=0}^{k-2} P(X_t = i, X_{t+h} - X_t = k - i) = \\ &= p_k(t)(1 - h\lambda - \alpha(h) - \beta(h)) + p_{k-1}(t)(h\lambda + \alpha(h)) + \\ &\quad + \sum_{i=0}^{k-2} p_i(t) P(X_{t+h} - X_t = k - i). \end{aligned}$$

Odtud ale vidíme (píšeme stejně jako v 6.17 na straně 340 symbol $o(h)$ pro výrazy, které podělené $h$ dávají limitu pro $h \to 0_+$




□

**9.29.** Náhodná veličina má distribuční funkci

$$F_X(x) = \begin{cases} 0 & \text{pro } x \le 3 \\ \frac{1}{3}x - 1 & \text{pro } 3 < x \le 6 \\ 1 & \text{pro } 6 < x. \end{cases}$$

i) Zdůvodněte, že jde skutečně o distribuční funkci.

ii) Určete hustotu pravděpodobnosti náhodné veličiny $X$.

iii) Vypočtěte $P(2 < X < 4)$.

**Řešení.** a) Jde zřejmě o spojitou neklesající funkci, která navíc vyhovuje $\lim_{x\to-\infty} F(x) = 0$ a $\lim_{x\to\infty} F(x) = 1$.

b) Podle 9.21 je hustota pravděpodobnosti spojité náhodné veličiny dána derivací distribuční funkce. Na intervalu $(3, 6)$ je tedy hustota $f(x) = \frac{1}{3}$. Na intervalech $(-\infty, 3)$ a $(6, \infty)$ je evidentně derivace nulová. Jde tedy o rovnoměrné rozdělení, viz 9.25.

c) Z definice distribuční funkce $P(2 < X < 4) = F_X(4) - F_X(2) = \frac{4}{3} - 1 = \frac{1}{3}$. □

nulovou)

$$\frac{p_0(t+h) - p_0(t)}{h} = -\lambda p_0(t) + \frac{1}{h}\,\mathrm{o}(h)$$
$$\frac{p_k(t+h) - p_k(t)}{h} = -\lambda p_k(t) + \lambda p_{k-1}(t) + \frac{1}{h}\,\mathrm{o}(h)$$

a limitním přechodem pro $h \to 0_+$ tak dostáváme (nekonečný!) systém obyčejných diferenciálních rovnic:

$$p_0'(t) = -\lambda p_0(t),\ p_0(0) = 1$$
$$p_k'(t) = -\lambda p_k(t) + \lambda p_{k-1}(t),\ p_k(0) = 0$$

pro všechny $t > 0$ a $k \in \mathbb{N}$, s počáteční podmínkou.

Nemusíme se ale děsit, protože první z nich má jediné řešení

$$p_0(t) = \mathrm{e}^{-\lambda t},$$

které okamžitě můžeme dosadit a vyřešit druhou rovnici. Obdržíme

$$p_1(t) = \lambda t\,\mathrm{e}^{-\lambda t}.$$

Matematickou indukcí teď už snadno dovodíme, že ve skutečnosti má celý systém jediné řešení a to

$$p_k(t) = \frac{(\lambda t)^k}{k!}\,\mathrm{e}^{-\lambda t},\ t > 0,\ k \in \mathbb{N}.$$

Ověřili jsme tedy, že pro každý proces splňující tři výše uvedené vlastnosti má náhodná veličina $X_t$ udávají počet výskytů v časovém intervalu $[0, t)$ rozdělení $\mathrm{Po}(\lambda t)$.

V praxi jsou takové procesy spojeny např. s poruchovostí strojů a zařízení.

**9.25. Spojitá rozdělení.** Nejjednodušším příkladem spojitého



rozdělení je rovnoměrné rozprostření veškeré pravděpodobnosti na nějakém intervalu. Na něm lze dobře ilustrovat, že při jednoduše formulovaném požadavku na chování rozdělení nám nezbude moc prostoru pro jeho definici. Nyní chceme, aby pravděpodobnost hodnoty veličiny $X$ v každém intervalu stejné délky obsaženém v daném intervalu $(a, b) \subset \mathbb{R}$ byla stejná, tj. hustota $f_X$ našeho rozdělení náhodné veličiny $X$ má být konstantní.

ROVNOMĚRNÉ ROZDĚLENÍ

Pro libovolná reálná čísla $-\infty < a < b < \infty$ definujeme hustotu a distribuční funkci takto:

$$f_X(t) = \begin{cases} 0 & t \le a \\ \frac{1}{b-a} & t \in (a, b) \\ 0 & t \ge b, \end{cases} \qquad F_X(t) = \begin{cases} 0 & t \le a \\ \frac{t-a}{b-a} & t \in (a, b) \\ 1 & t \ge b. \end{cases}$$

Říkáme, že veličina $X$ má *rovnoměrné rozdělení*.

Další rozdělení budeme podobné diskrétnímu Poissonovu. Předpokládejme, že sledujeme výskyt náhodného jevu takového, že jeho výskyty v nepřekrývajících se intervalech jsou nezávislé. Je-li tedy $p(t)$ pravděpodobnost, že jev nenastane během intervalu délky $t$, pak nutně $p(t + s) = p(t)p(s)$ pro všechna $t, s > 0$. Předpokládejme navíc diferencovatelnost funkce $p$ a $p(0) = 1$.

Pak jistě $\ln p(t+s) = \ln p(t) + \ln p(s)$, takže limitním přechodem (s využitím L'Hospitalova pravidla)

$$\big(\ln(p)\big)'(t) = \lim_{s\to 0_+} \frac{\ln p(t+s) - \ln p(t)}{s} = \frac{p'(0)}{p(0)} = p'(0).$$

**9.30.** Hustota pravděpodobnosti náhodné veličiny $X$ má tvar $f(x) = \frac{a}{1+x^2}$ pro $x \in \mathbb{R}$. Určete

i) koeficient $a$,

ii) distribuční funkci,

iii) $P(-1 < X < 1)$.

**Řešení.** a) Aby funkce $f(x)$ byla hustotou pravděpodobnosti, musí být její integrál přes celé $\mathbb{R}$ roven jedné. Dostáváme tedy podmínku

$$1 = \int_{-\infty}^{\infty} \frac{a}{1+x^2} dx = a[\operatorname{arctg} x]_{-\infty}^{\infty} = a\pi.$$

Odtud $a = \frac{1}{\pi}$.

b) Distribuční funkce je podle 9.21 dána integrálem

$$F_X(x) = \int_{-\infty}^{x} f(t)dt = \frac{1}{\pi}\int_{-\infty}^{x} \frac{dt}{1+t^2} = \frac{1}{\pi}\operatorname{arctg} x + \frac{1}{2}.$$

c) Z definice distribuční funkce a podle b) je

$$P(-1 < X < 1) = F_X(1) - F_X(-1) = \frac{1}{\pi}\cdot\frac{\pi}{4} - \frac{1}{\pi}\cdot\left(-\frac{\pi}{4}\right) = \frac{1}{2}.$$

□

**9.31.** Diskrétní náhodný vektor má sdruženou pravděpodobnostní funkci danou tabulkou

| X \ Y | 2 | 5 | 6 |
|---|---|---|---|
| 1 | $\frac{1}{5}$ | $\frac{1}{10}$ | $\frac{1}{20}$ |
| 2 | $\frac{1}{10}$ | $\frac{1}{20}$ | 0 |
| 3 | $\frac{3}{10}$ | $\frac{1}{20}$ | $\frac{3}{20}$ |

Určete

i) marginální distribuční a pravděpodobnostní funkce;

ii) sdruženou distribuční funkci a vhodným způsobem ji znázorněte;

iii) $P(Y > 3X)$.

**Řešení.** a) Marginální rozdělení náhodné veličiny $X$ resp. $Y$ dostaneme podle 9.27 sečtením sdružené pravděpodobnostní funkce přes všechny možné hodnoty veličiny $Y$ (odpovídá sečtení hodnot v každém řádku) resp. $X$ (odpovídá sečtení hodnot v každém sloupci). Pomocí tabulky proto dostáváme

| X | 1 | 2 | 3 |
|---|---|---|---|
| $f_X$ | $\frac{7}{20}$ | $\frac{3}{20}$ | $\frac{1}{2}$ |

a

| Y | 2 | 5 | 6 |
|---|---|---|---|
| $f_Y$ | $\frac{3}{5}$ | $\frac{1}{5}$ | $\frac{1}{5}$ |

b) Sdružená distribuční funkce v bodě $(a, b)$ je podle definice rovna součtu všech hodnot sdružené pravděpodobnostní funkce $f_{(X,Y)}$ takových, že $X \le a$ a $Y \le b$. To v tabulce zhruba řečeno odpovídá součtu všech hodnot ležících v podtabulce, jejíž pravý spodní roh je $(a, b)$. Přesněji máme pro sdruženou distribuční funkci $F_{(X,Y)}$ následující tabulku

Označme si proto spočtenou derivaci $p'(0) = -\lambda \in \mathbb{R}$, přičemž volíme záporné znaménko, protože víme, že $p'(0)$ nemůže být kladné, když je $p(0) = 1$.

Pak tedy pro $p(t)$ platí $\ln p(t) = -\lambda t + C$ a počáteční podmínka dává jediné řešení

$$p(t) = \mathrm{e}^{-\lambda t}.$$

Všimněme si, že z definice našich objektů vyplývá, že $\lambda > 0$.

Nyní uvažme náhodnou veličinu $X$ udávající (náhodný) okamžik, kdy náš jev poprvé nastane. Zřejmě tedy je distribuční funkce rozdělení pro $X$ dána

$$F_X(t) = 1 - p(t) = \begin{cases} 1 - \mathrm{e}^{-\lambda t} & t > 0 \\ 0 & t \le 0. \end{cases}$$

Je vidět, že skutečně jde o rostoucí funkci s hodnotami mezi nulou a jedničkou a správnými limitami v $\pm\infty$. Hustotu tohoto rozdělení dostaneme derivováním distribuční funkce.

EXPONENCIÁLNÍ ROZDĚLENÍ

Spojité rozdělení náhodné veličiny $X$ s hustotou

$$f_X(t) = \begin{cases} \lambda\,\mathrm{e}^{-\lambda t} & t > 0 \\ 0 & t \le 0. \end{cases}$$

se nazývá *exponenciální rozdělení* $\mathrm{ex}(\lambda)$.

Budeme také potkávat rozdělení, které je podobné jako exponenciální, ale s hustotou tvaru

$$cx^{a-1}\,\mathrm{e}^{-bx}$$

pro $x > 0$, s danými konstantami $a > 0, b > 0$, zatímco konstantu $c$ je třeba dopočítat. Potřebujeme

$$1 = \int_0^{\infty} cx^{a-1}\,\mathrm{e}^{-bx}\,dx = \int_0^{\infty} c\left(\frac{t}{b}\right)^{a-1}\mathrm{e}^{-t}\,\frac{1}{b}\,dt = \frac{c}{b^a}\Gamma(a).$$

GAMA ROZDĚLENÍ

Rozdělení, jehož hustota je nulová pro $x \le 0$, zatímco pro $x > 0$ je dána předpisem

$$f(X) = \frac{b^a}{\Gamma(a)}x^{a-1}\,\mathrm{e}^{-bx},$$

se nazývá *gama rozdělení* $\Gamma(a, b)$ s parametry $a > 0, b > 0$.

Exponenciální rozdělení je tedy speciálním případem tohoto rozdělení s parametrem $a = 1$.

**9.26. Normální rozdělení.** Jestliže v binomiálním rozdělení zachováme konstantní úspěšnost $p$, ale budeme přidávat počet pokusů $n$, bude pravděpodobnostní funkce kupodivu pořád mít podobný tvar (i když jiné rozměry).



Na obrázku při rostoucím $n$ se budou vynesené bodové hodnoty slévat do křivky, která by nám měla dát hustotu spojitého rozdělení aproximujícího dobře Bi(n, p) pro veliká $n$.

Naznačíme dopředu, kde hledat. Vzpomeňme na hladkou funkci $y = f(x) = \mathrm{e}^{-x^2/2}$, kterou jsme v odstavci 6.6 na straně 329 zmiňovali jako vhodný nástroj pro konstrukce funkcí hladkých, ale nikoliv analytických. Na obrázku je srovnání této křivky (vpravo) s vynesenými hodnotami Bi(5000, 0,5).

| $F_{(X,Y)}$ | [2,5) | [5,6) | [6,∞) |
|---|---|---|---|
| [1,2) | $\frac{1}{5}$ | $\frac{3}{10}$ | $\frac{7}{20}$ |
| [2,3) | $\frac{3}{10}$ | $\frac{9}{20}$ | $\frac{1}{2}$ |
| [3,∞) | $\frac{3}{5}$ | $\frac{4}{5}$ | 1 |

a na intervalech $(-\infty, 1) \times \mathbb{R}$ a $\mathbb{R} \times (-\infty, 2)$ je $F_{(X,Y)}$ zřejmě nulová.
c) Očividně $P(Y > 3X) = P(X = 1, Y = 5) + P(X = 1, Y = 6) = \frac{1}{10} + \frac{1}{20} = \frac{3}{20}$ □

**9.32.** Určete pravděpodobnost $P(2X > Y)$, je-li hustota náhodného vektoru $(X, Y)$

$$f_{(X,Y)}(x, y) = \begin{cases} \frac{1}{6}(4x - y) & \text{pro } 1 \le x \le 2,\ 2 \le y \le 4, \\ 0 & \text{jinak.} \end{cases}$$

**Řešení.** Z definice

$$\begin{aligned} P(2X > Y) &= \int_{-\infty}^{\infty} \int_{-\infty}^{2x} f_{(X,Y)}(x, y)\,dy\,dx = \\ &= \int_1^2 \int_2^{2x} \frac{1}{6}(4x - y)\,dy\,dx = \\ &= \int_1^2 \left[\frac{2}{3}xy - \frac{1}{12}y^2\right]_2^{2x} dx = \\ &= \int_1^2 \left(x^2 - \frac{4}{3}x + \frac{1}{3}\right) dx = \\ &= \left[\frac{1}{3}x^3 - \frac{2}{3}x^2 + \frac{1}{3}x\right]_1^2 = \frac{2}{3}. \end{aligned}$$

□

**9.33.** Určete marginální distribuční funkce, sdruženou a marginální hustotu náhodného vektoru $(X, Y)$, je-li

$$F_{(X,Y)}(x, y) = \begin{cases} 0 & \text{pro } x < 0,\ y < 0 \\ \frac{1}{4}x^2 y^2 & \text{pro } 0 \le x \le 1,\ 0 \le y \le 2 \\ 1 & \text{pro } x > 1,\ y > 2 \end{cases}$$

**Řešení.** Hustotu náhodného vektoru $(X, Y)$ dostaneme derivováním distribuční funkce podle $x$ a $y$. Tedy pro $0 \le x \le 1, 0 \le y \le 2$ je $f_{(X,Y)}(x, y) = xy$, jinde je hustota nulová. Marginální hustota náhodné veličiny $X$ je pak

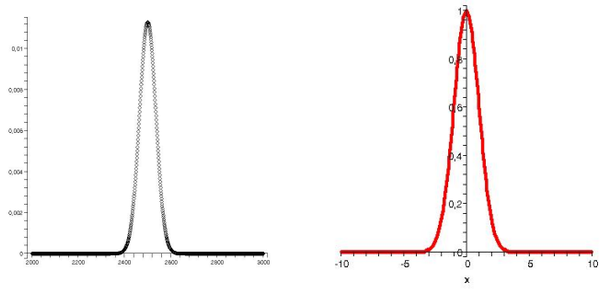
$$f_X(x) = \int_{-\infty}^{\infty} f_{(X,Y)}(x, y)\,dy = \int_0^2 xy\,dy = [\frac{1}{2}xy^2]_0^2 = 2x.$$

Podobně pro $Y$ dostaneme $f_Y(y) = \frac{1}{2}y$. Marginální distribuční funkce jsou

$$F_X(x) = \int_{-\infty}^{x} f_X(t)dt = \int_0^x 2t\,dt = x^2$$

a

$$F_Y(y) = \int_{-\infty}^{y} f_Y(t)dt = \int_0^y \frac{1}{2}t\,dt = \frac{1}{4}y^2.$$ □



Podbízí se proto hledat vhodné spojité rozdělení, které by mělo hustotu danou pomocí vhodně upravené takové funkce.

Funkce $e^{-x^2/2}$ je vždy kladná funkce, stačí nám spočíst $\int_{-\infty}^{\infty} e^{-x^2/2}\,dx$ a pokud to bude konečné číslo, prostě tuto funkci vynásobíme jeho převrácenou hodnotou. Spočítat tento integrál sice není možné pomocí elementárních funkcí, můžeme si ale pomoci vícerozměrnou integrací a Fubiniho větou. Snadno totiž pomocí transformace do polárních souřadnic spočteme, že

$$\begin{aligned} 2\pi &= \int_{\mathbb{R}^2} e^{-(x^2+y^2)/2}\,dx\,dy \\ &= \left(\int_{-\infty}^{\infty} e^{-x^2/2}\,dx\right)\left(\int_{-\infty}^{\infty} e^{-y^2/2}\,dy\right) \end{aligned}$$

(srovnejte s poznámkami na konci odstavce 8.28, ověřte, že integrovaná funkce skutečně vyhovuje tam uvedeným podmínkám, a spočtěte si podrobně!). Odtud ale již vidíme, že hledaný integrál má hodnotu $\sqrt{2\pi}$ a bude proto funkce $f(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$ dobře definovanou hustotou náhodné veličiny.

### Normální rozdělení

Spojité rozdělení náhodné veličiny $Z$ s hustotou

$$\varphi(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$$

se nazývá (standardizované) *normální rozdělení* N(0, 1). Příslušnou distribuční funkci

$$\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-x^2/2}\,dx$$

nelze vyjádřit pomocí elementárních funkcí, přesto se s ní numericky běžně počítá (pomocí tabulek nebo softwarových aplikací).

Grafu hustoty $\varphi(x)$ se také často říká *Gaussova křivka*.

Tím jsme ještě evidentně nenašli tu pravou hustotu aproximující binomiální rozdělení. Obrázek, srovnávající pravděpodobnostní funkci binomického rozdělení s Gaussovou křivkou, ukazuje, že budeme chtít jednak posouvat hodnotu, kde dochází k maximální hodnotě a také zužovat či rozšiřovat oblast s výrazněji kladnými hodnotami. Toho můžeme snadno docílit vnesením dvou reálných parametrů $\mu$ a $\sigma > 0$ takto:

$$g_{\mu,\sigma}(x) = e^{-(x-\mu)^2/(2\sigma^2)}.$$

Nyní snadno spočteme pomocí jednoduché substituce proměnné

$$\int_{-\infty}^{\infty} e^{-(x-\mu)^2/(2\sigma^2)}\,dx = \sqrt{2\pi}\sigma.$$

Dostáváme tedy celou dvouparametrickou třídu hustot

$$\varphi_{\mu,\sigma} = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

**9.34.** V urně je 14 kuliček – 4 červené, 5 bílých a 5 modrých. Náhodně bez vracení vybereme 6 kuliček. Určete rozložení náhodného vektoru $(X, Y)$, označuje-li $X$ počet tažených červených kuliček a $Y$ počet tažených bílých kuliček. Určete rovněž marginální rozložení veličin $X$ a $Y$. Dále vypočtěte $P(X \leq 3)$, $P(1 \leq Y \leq 4)$.

**Řešení.** Z definice pravděpodobnostní funkce je její hodnota v bodě $(x, y)$ určena pravděpodobností $P(X = x, Y = y)$, tedy pravděpodobností, že vytáhneme $x$ červených a $y$ bílých kuliček. Počet možností vytažení $x$ Červených kuliček je $\binom{4}{x}$, podobně počet vytažení $y$ bílých je $\binom{5}{y}$. Zbylých $6 - x - y$ modrých kuliček pak můžeme vytáhnout $\binom{5}{6-x-y}$ způsoby. Dohromady tedy máme $\binom{4}{x}\binom{5}{y}\binom{5}{6-x-y}$ možností. Hodnoty tohoto výrazu pro všechny možné hodnoty $x$, $y$ jsou v následující tabulce.

| x\ y | 0 | 1 | 2 | 3 | 4 | 5 | $\sum_X$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 5 | 50 | 100 | 50 | 5 | 210 |
| 1 | 4 | 100 | 400 | 400 | 100 | 4 | 1008 |
| 2 | 30 | 300 | 600 | 300 | 30 | 0 | 1260 |
| 3 | 40 | 200 | 200 | 40 | 0 | 0 | 480 |
| 4 | 10 | 25 | 10 | 0 | 0 | 0 | 45 |
| $\sum_Y$ | 84 | 630 | 1260 | 840 | 180 | 9 | 3003 |

Hodnoty nejvíce napravo a dole jsou součty možností přes všechny hodnoty $y$ resp. $x$. Hodnoty pravděpodobnostní funkce jsou pak zřejmě dány vydělením příslušných hodnot v tabulce počtem všech výběrů šesti kuliček, tj. vydělením číslem $\binom{14}{6} = 3003$. Marginální rozložení $X$ resp. $Y$ je přitom dáno hodnotami nejvíce napravo resp. dole v tabulce.

Pravděpodobnost $P(X \leq 3)$ jednoduše spočítáme pomocí marginálního rozložení $X$

$$P(X \leq 3) = F_X(3) = \frac{1}{3003}(210 + 1008 + 1260 + 480) = 0{,}985.$$

Podobně pro pravděpodobnost $P(1 \leq Y \leq 4)$ máme

$$P(1 \leq Y \leq 4) = F_Y(4) - F_Y(1) = \\ = \frac{1}{3003}(630 + 1260 + 840 + 180) = 0{,}969.$$

□

**9.35.** Hustota náhodného vektoru $(X, Y, Z)$ je

$$f(x, y, z) = \begin{cases} c(x + y + z) & \text{pro } 0 \leq x \leq 1, 0 \leq y \leq 1, 0 \leq z \leq 1 \\ 0 & \text{jinak.} \end{cases}$$

Určete konstantu $c$, distribuční funkci a vypočtěte

$$P(0 \leq X \leq \tfrac{1}{2}, 0 \leq Y \leq \tfrac{1}{2}, 0 \leq Z \leq \tfrac{1}{2}).$$

náhodných veličin. Příslušná rozdělení budeme značit $\mathrm{N}(\mu, \sigma)$.

K asymptotické blízkosti normálního a binomického rozdělení pro $n \to \infty$ se ještě vrátíme, jenom co si k tomu vytvoříme patřičné nástroje.

**9.27. Rozdělení náhodných vektorů.** Obdobně jako u skalárních veličin definujeme distribuční funkce a hustotu nebo pravděpodobnostní funkci pro spojité a diskrétní náhodné vektory. Hovoříme také o simultánních (sdružených) pravděpodobnostních funkcích a hustotách.



Pro dvě diskrétní náhodné veličiny, tj. diskrétní vektor $(X, Y)$ náhodných veličin, definujeme *(sdruženou) pravděpodobnostní funkci*

$$f(x, y) = \begin{cases} P(X = x_i \wedge Y = y_j) & x = x_i,\ y = y_j \\ 0 & \text{jinak.} \end{cases}$$

Pro spojité veličiny pak definujeme pro všechny $a, b \in \mathbb{R}$

$$F(a, b) = P(X < a, Y < b) = \\ = \int_{-\infty}^{b} \int_{-\infty}^{a} f(x, y) dx dy$$

a funkci $f(x, y)$ nazýváme *(sdruženou) hustotou* náhodného vektoru $(X, Y)$.

Pro obecný náhodný vektor $X = (X_1, \ldots, X_n)$ obdobně při spojitých náhodných veličinách $X_i$ definujeme

$$F(a_1, \ldots, a_n) = P(X_1 < a_1, \ldots, X_n < a_n) = \\ = \int_{-\infty}^{a_n} \cdots \int_{-\infty}^{a_1} f(x, y)\, dx_1 \cdots dx_n$$

a obdobně pro diskrétní náhodné veličiny.

*Marginální rozložení* pro jednu z proměnných obdržíme tak, že přes ostatní posčítáme nebo zintegrujeme.

Např. u diskrétních vektorových veličin $(X, Y)$ tvoří jevy $(X = x_i, Y = y_j)$ pro všechny možné hodnoty $x_i$ a $y_j$ s nenulovými pravděpodobnostmi pro $X$ a $Y$ úplný systém jevů pro vektor $(X, Y)$ a dostáváme vztah:

$$P(X = x_i) = \sum_{j=1}^{\infty} P(X = x_i, Y = y_j)$$

mezi *marginálním rozdělením pravděpodobnosti* náhodné veličiny $X$ a sdruženým rozdělením pravděpodobnosti náhodného vektoru $(X, Y)$. Zcela obdobně postupujeme u spojitých náhodných vektorů s pomocí integrálů.

**9.28. Nezávislost náhodných veličin.** Víme už, co to je (ne)závislost náhodných jevů, kterou jsme diskutovali v odstavci 9.12. O náhodných veličinách $X_1, \cdots, X_n$ řekneme, že jsou *(stochasticky) nezávislé*, jestliže jsou pro libovolná čísla $a_i \in \mathbb{R}$ nezávislé jevy $X_1 < a_1, \ldots, X_n < a_n$.



To již díky axiomům pravděpodobnosti zaručuje, že budou nezávislé i všechny jevy zadané příslušností hodnot veličin $X_k \in I_k$ do libovolných intervalů $I_k$. Přímo z definičních vlastností pak také odvodíme, že jsou náhodné veličiny $X_i$ nezávislé, právě když jejich sdružená distribuční funkce $F$ splňuje

$$F(x_1, \ldots, x_n) = F_1(x_1) \cdots F_n(x_n),$$

kde $F_i$ jsou distribuční funkce veličin $X_i$.

**Řešení.** Integrál hustoty pravděpodobnosti přes celý prostor musí být roven jedné, a proto

$$1 = \int_0^1 \int_0^1 \int_0^1 c(x+y+z)dzdydx = c\int_0^1 \int_0^1 (x+y+\tfrac{1}{2})dydx = \\ = c\int_0^1 (x+1)dx = \tfrac{3}{2}c.$$

Odtud $c = \frac{2}{3}$. Distribuční funkce je z definice rovna

$$F_X(x,y,z) = \tfrac{2}{3}\int_0^x \int_0^y \int_0^z (r+s+t)dtdsdr = \\ = \tfrac{2}{3}\int_0^x \int_0^y (rz+sz+\tfrac{1}{2}z^2)dsdr = \tfrac{2}{3}\int_0^x (rzy+\tfrac{1}{2}y^2z+\tfrac{1}{2}z^2y)dr = \\ = \tfrac{2}{3}(\tfrac{1}{2}x^2zy+\tfrac{1}{2}y^2zx+\tfrac{1}{2}z^2yx) = \tfrac{1}{3}(x^2zy+y^2zx+z^2yx),$$

a proto je hledaná pravděpodobnost

$$P(0 \le X \le \tfrac{1}{2}, 0 \le Y \le \tfrac{1}{2}, 0 \le Z \le \tfrac{1}{2}) = F(\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2}) = \tfrac{1}{16}. \qquad \square$$

**9.36.** Určete konstantu $a$ tak aby funkce

$$f(x) = \begin{cases} 0 & \text{pro } x \le 1 \\ a\ln(x) & \text{pro } 1 < x < 2 \\ 0 & \text{pro } 2 \le x \end{cases}$$

zadávala hustotu pravděpodobnosti nějaké náhodné veličiny.

**Řešení.** Podmínka na to, aby zadaná funkce zadávala hustotu pravděpodobnosti je

$$\int_{-\infty}^{\infty} f(x) = 1$$

Bude potřeba spočítat $\int \ln(x)\,\mathrm{d}x$:

$$\int \ln(x)\,\mathrm{d}x = x\ln(x) - \int 1\,\mathrm{d}x = x\ln(x) - x = x(\ln(x)-1).$$

Celkem

$$\int_{-\infty}^{\infty} f(x) = \int_1^2 a\ln(x) = a[x(\ln(x)-1)]_1^2 = a(2\ln(2)-1),$$

tedy $a = \frac{1}{2\ln(2)-1}$. $\square$

**9.37.** V lese, jehož hranice tvoří na mapě pravidelný šestiúhelník se ztratilo dítě. Předpokládejme, že pravděpodobnost toho, že dítě je v určité části lesa, je úměrná pouze velikosti této části, nikoliv jejímu umístění.

- Jaké je rozdělení pravděpodobnosti vzdálenosti dítěte od zvolené strany (přímky) lesa
- Jaké je rozdělení pravděpodobnosti vzdálenosti dítěte od nejbližší strany lesa.

**Řešení.**

- Nechť $a$ je strana šestiúhelníka. Pak rozdělení pravděpodobnosti je

$$f(x) = \begin{cases} 0 & \text{pro } x \le 0 \\ \frac{4}{9a^2}x + \frac{2}{3\sqrt{3}a} & \text{pro } 0 < x \le \frac{1}{2}\sqrt{3}a \\ -\frac{4}{9a^2}x + \frac{2}{\sqrt{3}a} & \text{pro } \frac{1}{2}\sqrt{3}a \le x \le \sqrt{3}a \\ 0 & \text{pro } x > \sqrt{3}a \end{cases},$$

pro první část.

Pro diskrétní nezávislé veličiny z definice okamžitě vyplývá, že sdružená pravděpodobnostní funkce nezávislých veličin je dána součiny jednotlivých hodnot

$$f_{X,Y}(x,y) = \sum_{x_i}\sum_{y_j} x_i y_j.$$

Derivací sdružené distribuční funkce spojitých proměnných dostáváme obdobný vztah mezi jejich hustotami:

$$f_{X,Y}(x,y) = \frac{\partial^2}{\partial x \partial y} F_{X,Y}(x,y) = \\ = \frac{\partial^2}{\partial x \partial y} F_X(x) F_Y(y) = \\ = f_X(x) f_Y(y).$$

Jde tedy o prostý součin hustot jednotlivých veličin.

Hustoty náhodných vektorů vyšších dimenzí s nezávislými spojitými komponentami se chovají zcela obdobně a jejich sdružené hustoty jsou součinem hustot jednotlivých veličin, tj.

$$f_{X_1,\ldots,X_n}(x_1,\ldots,x_n) = f_{X_1}(x_1)\cdots f_{X_n}(x_n).$$

Podívejme se na jednoduchý příklad, který ukazuje, že není dobré zjednodušeně vidět náhodný vektor, coby stochastický objekt, jen jako dvojici náhodných veličin. Uvažme náhodný vektor $(X,Y)$, který má rovnoměrné spojité rozdělení na jednotkovém kruhu v rovině $\mathbb{R}^2$ se středem v počátku. Bude tedy jeho (sdružená) hustota

$$f(x,y) = \begin{cases} \frac{1}{\pi} & x^2+y^2 \le 1 \\ 0 & \text{jinak.} \end{cases}$$

Je vidět, že veličiny $X$ a $Y$ z tohoto náhodného vektoru nemohou být nezávislé. Např. si všimněme, že pravděpodobnost, že $(X,Y)$ padne do doplňku jednotkového kruhu ve čtverci s vrcholy o souřadnicích $\pm 1$ je nulová, zatímco marginální distribuční funkce jsou pro hodnoty $|x| \le 1$ a $|y| \le 1$ nenulové.

Když ovšem vyjádříme tentýž náhodný vektor v polárních souřadnicích $(R,\Phi)$, dostáváme

$$P(R < r_0, \Phi < \varphi_0) = \int_0^{r_0}\int_0^{\varphi_0} \frac{1}{\pi} r\,d\varphi dr = \frac{1}{2}\varphi_0 r_0^2.$$

Sdružená hustota vektoru $(R,\Phi)$ je tedy $f(r,\varphi) = \frac{r}{\pi}$ při $0 < r \le 1, 0 < \varphi \le 2\pi$ a jinak je nulová. Marginální hustoty jsou

$$f_R(r) = \int_0^{2\pi} \frac{r}{\pi}\,d\varphi = 2r, \quad \text{je-li } 0 < r \le 1,$$

$$f_\Phi(\varphi) = \int_0^1 \frac{r}{\pi}\,dr = \frac{1}{2\pi}, \quad \text{je-li } 0 < \varphi \le 2\pi,$$

a nula jinak. Náhodné veličiny $R$ a $\Phi$ jsou tedy nezávislé.

**9.29. Funkce náhodných veličin.** 
Náhodné vektory potkáváme v praktických modelech ve dvou velmi odlišných rolích. Můžeme sledovat skutečně několik různých náhodných veličin popisujících více či méně související jevy. Jako příklad nám mohou sloužit různorodé číselné parametry svázané s jednotlivými studenty (prospěch v různých předmětech, váha, výška, stáří, roční příjem, atd.). V tomto případě budeme potřebovat nástroje, které nám umožní sledovat rozdíly či závislosti mezi takovými veličinami.

Můžeme ale také sledovat jen jeden parametr na velkém souboru objektů a vybíráme přitom jen menší počet $n$ z nich. Takový

- Spočtěme nejprve distribuční funkci $F$ hledaného rozložení náhodné veličiny $X$ udávající vzdálenost dítěte od nejbližší strany lesa. Vzdálenost se může pohybovat v intervalu $I = \langle 0, \frac{\sqrt{3}}{2}a\rangle$. Pro $y \in I$ potom máme

$$F(y) = P[X < y] = \frac{\frac{\sqrt{3}}{4}a^2 - \frac{(\frac{\sqrt{3}}{2}a-y)^2}{\frac{3}{4}a^2}\frac{\sqrt{3}}{4}a^2}{\frac{\sqrt{3}}{4}a^2} = 1 - \frac{4(\frac{\sqrt{3}}{2}a-y)^2}{3a^2}$$

Celkem tedy

$$F(y) = \begin{cases} 0 & \text{pro } y \le 0 \\ 1 - \frac{4(\frac{\sqrt{3}}{2}a-y)^2}{3a^2} & \text{pro } y \in \langle 0, \frac{\sqrt{3}}{2}a\rangle \\ 1 & \text{pro } y \ge \frac{\sqrt{3}}{2}a \end{cases}$$

Pro hustotu pravděpodobnosti, která je derivací distribuční funkce dostáváme:

$$f(x) = \begin{cases} 0 & \text{pro } x \le 0 \\ \frac{8(\frac{\sqrt{3}}{2}a-y)}{3a^2} & \text{pro } y \in \langle 0, \frac{\sqrt{3}}{2}a\rangle \\ 0 & \text{pro } y \ge \frac{\sqrt{3}}{2}a \end{cases}$$

□

**9.38.** Nechť veličina náhodná veličina $X$ má rovnoměrné rozdělení na intervalu $\langle 0, r\rangle$. Určete distribuční funkci a hustotu pravděpodobnosti rozdělení objemu koule o poloměru $X$.

**Řešení.** Určeme nejprve distribuční funkci $F$ (pro $0 < d < \frac{4}{3}\pi r^3$)

$$F(d) = P\left[\frac{4}{3}\pi X^3 \le d\right] = P\left[X \le \sqrt[3]{\frac{3d}{4\pi}}\right] = \frac{\sqrt[3]{\frac{3d}{4\pi}}}{r},$$

celkem

$$F(x) = \begin{cases} 0 & \text{pro} \quad x \le 0 \\ \sqrt[3]{\frac{3}{4\pi r^3}}\, x^{\frac{1}{3}} & \text{pro} \quad 0 < x < \frac{4}{3}\pi r^3 \\ 1 & \text{pro} \quad x \ge \frac{4}{3}\pi r^3 \end{cases}$$

Derivováním pak obdržíme hustotu pravděpodobnosti:

$$f(x) = \begin{cases} 0 & \text{pro} \quad x \le 0 \\ \sqrt[3]{\frac{1}{36\pi r^3}}\, x^{-\frac{2}{3}} & \text{pro} \quad 0 < x < \frac{4}{3}\pi r^3 \\ 0 & \text{pro} \quad x \ge \frac{4}{3}\pi r^3 \end{cases}$$

□

**9.39.** Stanovte hodnotu parametru $a \in \mathbb{R}$ tak, aby funkce

$$f(x) = \begin{cases} 0 & \text{pro} \quad x \le 0 \\ ax^2 & \text{pro} \quad 0 < x < 3 \\ 0 & \text{pro} \quad x \ge 3 \end{cases}$$

zadávala hustotu pravděpodobnosti náhodné veličiny $X$. Určete distribuční funkci, hustotu pravděpodobnosti a střední hodnotu rozdělení objemu krychle, jejíž délka hrany je náhodná veličina s hustotou pravděpodobnosti danou funkcí $f$.

postup popisujeme pomocí $n$–rozměrného vektoru $(X_1, \ldots, X_n)$, kde všechny náhodné veličiny $X_k$ mají stejné rozdělení pravděpodobnosti. Tady nás budou velice zajímat veličiny, které budou odpovídat statistickým číselným charakteristikám, které jsme již potkali v předchozí části této kapitoly.

Budeme umět oba případy zvládat jedním jednoduchým konceptem. Místo dané náhodné veličiny nebo náhodného vektoru budeme uvažovat funkci z těchto veličin.

I u jediné veličiny jde o velice užitečný nástroj. Místo náhodné veličiny $X$, např. „roční plat zaměstnance“, budeme vyčíslovat jinou závislou hodnotu $\psi(X)$, např. „roční čistý příjem zaměstnance po zdanění a včetně sociálních dávek“. V systému s tzv. sociální solidaritou je první veličina hodně variabilní, zatímco druhá může být skoro konstantní. Statisticky se proto budou značně odlišovat.

### Funkce náhodných veličin a vektorů

Pro danou spojitou funkci $\psi : \mathbb{R} \to \mathbb{R}$ a náhodnou veličinu $X$ máme dánu také náhodnou veličinu $Y = \psi(X)$. Nazýváme ji *funkcí náhodné veličiny* $X$.

V případě náhodného vektoru $(X_1, \ldots, X_n)$ a funkce $\psi : \mathbb{R}^n \to \mathbb{R}$ hovoříme o funkci $Y = \psi(X_1, \ldots, X_n)$ náhodného vektoru.

Všimněme si, že požadavek spojitosti $\psi$ zaručuje, že je $Y$ opět náhodnou veličinou podle naší definice, protože vzor borelovské množiny ve spojitém zobrazení je opět borelovská množina. Obecněji můžeme právě tento požadavek na $\psi$ vztáhnout pro každý speciální případ veličiny či vektoru a definovat tak pojem funkce z náhodné veličiny či vektoru obecněji.

Nejjednodušší funkcí po konstantách je afinní závislost

$$\psi(X) = a + bX$$

s konstantami $a, b \in \mathbb{R}$, $b \neq 0$.

Je-li $f_X(x)$ pravděpodobnostní funkce náhodné veličiny s diskrétním rozdělením, snadno se vypočte

$$f_{\psi(X)}(y) = P(\psi(X) = y) = \sum_{\psi(x_i)=y} f(x_i).$$

V případě afinní závislosti $Y = a+bX$ je proto pravděpodobnostní funkce nenulová právě v bodech $y_i = ax_i + b$.

Jako příklad na funkci náhodného vektoru si rozmyslete součet $n$ nezávislých náhodných veličin s alternativním rozdělením $\mathrm{A}(p)$. Samozřejmě dostáváme právě binomiální rozdělení $\mathrm{Bi}(n, p)$.

Podobně můžeme přepočíst distribuční funkci rozdělení funkce ze spojité náhodné veličiny, či vektoru. Ukážeme na příkladu.

V předposledním odstavci jsme zavedli veličinu $Z$ s normálním rozdělením $\mathrm{N}(0, 1)$. Snadno spočteme, že veličiny $Y = \mu + \sigma Z$ budou mít normální rozdělení $\mathrm{N}(\mu, \sigma)$ diskutované tamtéž. Skutečně,

$$\begin{aligned} F_Y(y) &= P(Y < y) = P(\mu + \sigma Z < y) = \\ &= \Phi\big(\frac{1}{\sigma}(y-\mu)\big) = \tfrac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{y-\mu}{\sigma}} \mathrm{e}^{-z^2/2}\, dz = \\ &= \int_{-\infty}^{y} \frac{1}{\sqrt{2\pi}\sigma}\, \mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}}\, dx, \end{aligned}$$

kde jsme v posledním kroku použili substituci $x = \mu + \sigma z$. To je právě požadovaný výraz.

**Řešení.** Jednoduše $a = \frac{1}{9}$. Distribuční funkce náhodné veličiny $X$ je tedy $F_X(t) = \frac{1}{27}t^3$ pro $t \in (0, 3)$, pro menší $t$ je tato funkce nulová, pro větší rovna 1. Označme $Z = X^3$ náhodnou veličinu označující objem krychle. Ten je v intervalu $(0, 27)$, pro $t \in (0, 27)$ a distribuční funkci $F_Z$ náhodné veličiny $Z$ tedy můžeme psát $F_Z(t) = P[Z < t] = P[X^3 < t] = P[X < \sqrt[3]{t}] = F_X(\sqrt[3]{t}) = \frac{1}{27}t$, hustota pravděpodobnosti je pak $f_Z(t) = \frac{1}{27}$ na intervalu $(0, 27)$, jinak nula, jedná se tedy o rovnoměrné rozdělení pravděpodobnosti na daném intervalu, střední hodnota je tudíž 13, 5. □

**9.40.** Stanovte hodnotu parametru $a \in \mathbb{R}$ tak, aby funkce

$$f(x) = \begin{cases} 0 & \text{pro } x \le 0 \\ ax & \text{pro } 0 < x < 3 \\ 0 & \text{pro } x \ge 3 \end{cases}$$

zadávala hustotu pravděpodobnosti náhodné veličiny $X$. Určete distribuční funkci, hustotu pravděpodobnosti a střední hodnotu rozdělení obsahu čtverce, jehož délka hrany je náhodná veličina s hustotou pravděpodobnosti danou funkcí $f$.

**Řešení.** Budeme postupovat jako v předchozím příkladě. Opět snadno zjistíme $a = \frac{2}{9}$. Distribuční funkce náhodné veličiny $X$ je tedy $F_X(t) = \frac{1}{9}t^2$ pro $t \in (0, 3)$, pro menší $t$ je tato funkce nulová, pro větší rovna 1. Označme $Z = X^2$ náhodnou veličinu označující obsah čtverce. Ten je v intervalu $(0, 9)$, pro $t \in (0, 9)$ a distribuční funkci $F_Z$ náhodné veličiny $Z$ tedy můžeme psát $F_Z(t) = P[Z < t] = P[X^2 < t] = P[X < \sqrt{t}] = F_X(\sqrt{t}) = \frac{1}{9}t$, hustota pravděpodobnosti je pak $f_Z(t) = \frac{1}{9}$ na intervalu $(0, 9)$, jinak nula, jedná se tedy o rovnoměrné rozdělení pravděpodobnosti na daném intervalu, střední hodnota je tudíž 4, 5. □

*9.41.* Stanovte hodnotu parametru $a \in \mathbb{R}$ tak, aby funkce

$$f(x) = \begin{cases} 0 & \text{pro } x \le 0 \\ ax^2 & \text{pro } 0 < x < 2 \\ 0 & \text{pro } x \ge 2 \end{cases}$$

zadávala hustotu pravděpodobnosti náhodné veličiny $X$. Určete distribuční funkci, hustotu pravděpodobnosti a střední hodnotu rozdělení objemu krychle, jejíž délka hrany je náhodná veličina s hustotou pravděpodobnosti danou funkcí $f$. ○

**9.42.** Náhodně rozřízneme úsečku délky $l$ na dvě části. Určete distribuční funkci a hustotu pravděpodobnosti rozdělení obsahu obdélníka, jehož délky stran jsou rovny délkám takto vzniklých úseček.

**Řešení.** Spočítejme hledanou distr. funkci. Označme ještě $X$ náhodnou veličinu s rovnoměrným rozložením na intervalu $\langle 0, l \rangle$ udávající délku jedné ze stran (délka druhé je pak $l - X$). Obsah obdélníka



Se součty nezávislých náhodných veličin je to malinko složitější. Uvažme dvě takové spojité veličiny $X$ a $Y$ s hustotami $f_X$ a $f_Y$. Přímým výpočtem spočteme distribuční funkci náhodné proměnné $V = X + Y$.

$$F_V(u) = \int_{x+y<u} f_X(x) f_Y(y)\, dxdy = \\ = \int_{-\infty}^{u} \left( \int_{-\infty}^{\infty} f_X(x) f_Y(v - x)\, dx \right) dv.$$

Je tedy sdruženou hustotou součtu dvou nezávislých veličin právě konvoluce jejich hustot

$$f_V = f_X * f_Y,$$

se kterou jsme se setkali již v odstavci 7.28 na straně 425. Úplně stejně dostaneme diskrétní konvoluci pravděpodobnostních funkcí v případě diskrétních náhodných veličin.

Konvoluci jsme si v 7. kapitole představovali jako jisté „rozmlžení" hodnot jedné z funkcí pomocí jádra vyjádřeného druhou. Promyslete si, že to je ta správná intuice i pro hustotu součtu nezávislých náhodných veličin. Je proto také samozřejmé, že má být konvoluce symetrická vůči oběma argumentům.

**9.30. Číselné charakteristiky náhodných veličin.** Viděli jsme, že při statistickém zkoumání hodnot (např. zpracování výsledků nějakého měření) hledáme výpovědi pomocí číselných charakteristik, jako jsou aritmetický průměr a směrodatná odchylka. Nyní zavedeme obdobné charakteristiky pro náhodné veličiny a náhodné vektory. První z nich je obdobou aritmetického průměru.



STŘEDNÍ HODNOTA

Pro libovolnou náhodnou veličinu $X$ definujeme její *střední hodnotu* $\mathrm{E}\,X$ vztahem

$$\mathrm{E}\,X = \begin{cases} \sum_i x_i f_X(x_i) & \text{pro diskrétní veličinu} \\ \int_{-\infty}^{\infty} x f_X(x) dx & \text{pro spojitou veličinu,} \end{cases}$$

pokud uvedené sumy či integrály absolutně konvergují. Když absolutně nekonvergují, říkáme, že náhodná veličina $X$ střední hodnotu nemá.

*Střední hodnotou náhodného vektoru* rozumíme vektor středních hodnot jeho jednotlivých komponent.

Střední hodnotu můžeme přímo vyjádřit také pro funkce $Y = \psi(X)$ náhodné veličiny či vektoru $X$. Připomeňme, že uvažujeme pouze takové funkce $\psi$, kdy je $Y$ opět náhodnou veličinou.

V diskrétním případě můžeme přímo spočíst

$$\mathrm{E}\,Y = \sum_j y_j P(Y = y_j) = \\ = \sum_j y_j \sum_{\psi(x_i)=y_j} P(X = x_j) = \\ = \sum_i \psi(x_i) P(X = x_i),$$

pokud suma absolutně konverguje. Samozřejmě, není zaručeno, že funkce z náhodné veličiny, které má střední hodnotu, bude mít střední hodnotu také.

$S$, tedy součin $x(l-x)$ pro $x \in \langle 0, l\rangle$ může zřejmě nabývat hodnot $\langle 0, l^2/4\rangle$. Volíme-li $d \in \langle 0, l^2/4\rangle$, můžeme psát

$$F(d) = P[S \le d] = P[X(l-X) \le d]$$

Hledáme tedy ty hodnoty $x$, pro které je $x(l-x) \le d$. Řešíme kvadr. nerovnici, kořeny odpovídající kvadratické rovnice jsou $\frac{l-\sqrt{l^2-4d}}{2}$ a $\frac{l+\sqrt{l^2-4d}}{2}$, hodnoty $x$ uvnitř tohoto intervalu nerovnici nesplňují, hodnoty vně potom ano. Je tedy

$$P[X(l-X) \le d] = P[X \in \langle 0, l\rangle \setminus (\frac{l-\sqrt{l^2-4d}}{2}, \frac{l+\sqrt{l^2-4d}}{2})]$$
$$= \frac{l-\sqrt{l^2-4d}}{l} = 1 - \frac{\sqrt{l^2-4d}}{l}$$

Celkem

$$F(x) = \begin{cases} 0 & \text{pro} \quad x \le 0 \\ 1 - \frac{\sqrt{l^2-4x}}{l} & \text{pro} \quad 0 \le x \le \frac{l^2}{4} \\ 1 & \text{pro} \quad x > \frac{l^2}{4} \end{cases}$$

Hustotu pravděpodobnosti pak dostaneme derivací:

$$f(x) = \begin{cases} 0 & \text{pro} \quad x \le 0 \\ \frac{2}{l\sqrt{l^2-4x}} & \text{pro} \quad 0 \le x \le \frac{l^2}{4} \\ 0 & \text{pro} \quad x > \frac{l^2}{4} \end{cases}$$

□

**9.43.** Nezávislé náhodné veličiny $X$ a $Y$ mají následující hustoty pravděpodobnosti:

$$f_X(t) = \begin{cases} 0 & \text{pro } t \le 0, \\ 1 & \text{pro } 0 < t < 1, \\ 0 & \text{pro } 1 \le t, \end{cases} \quad f_Y(t) = \begin{cases} 0 & \text{pro } t \le 0, \\ 2t & \text{pro } 0 < t < 1, \\ 0 & \text{pro } 1 \le t. \end{cases}$$

Určete distribuční funkci náhodné veličiny udávající obsah obdélníka o stranách $X$ a $Y$.

**Řešení.**

$$F_Y(t) = \begin{cases} 0 & \text{pro} \quad t \le 0 \\ 2t - t^2 & \text{pro} \quad 0 < t < 1 \\ 1 & \text{pro} \quad 1 \le t \end{cases}$$

□

**9.44.** Nechť $X$, $Y$ jsou nezávislé náhodné veličiny, přičemž $X$ má rovnoměrné rozdělení pravděpodobnosti na intervalu $(0, 2)$, $Y$ je pak dána následující hustotou pravděpodobnosti:

$$f(x) = \begin{cases} 0 & \text{pro} \quad x \le 0 \\ 2x & \text{pro} \quad 0 < x < 1 \\ 0 & \text{pro} \quad x \ge 1. \end{cases}$$

Určete pravděpodobnost, že $Y$ je menší než $X^2$.

Podobně vyjádříme střední hodnotu funkce ze spojité náhodné veličiny:

$$\mathrm{E}\,\psi(X) = \int_{-\infty}^{\infty} \psi(x) f_X(x) dx,$$

pokud tento integrál absolutně konverguje.

Všimněme si náhodná veličina $Y = \psi(X)$ nemusí být pro funkci spojité náhodné veličiny opět spojitá. Nicméně v případě spojité monotónní funkce $\psi$ a spojité veličiny $X$ tomu tak bude a mělo by být vcelku jednoduchým cvičením ověřit, že námi definovaná $\mathrm{E}\,\psi(X)$ skutečně splývá s $\mathrm{E}\,Y$.

Střední hodnotu náhodné veličiny můžeme nahlížet jako „očekávanou hodnotu“. Ve statistice zanedlouho uvidíme, že má skutečně přímý vztah k aritmetickému průměru vektoru hodnot.

**9.31. Petrohradský paradox.** Vraťme se k příkladu, kterým jsme motivovali potřebu diskrétních náhodných veličin v odstavci 9.10. Přeformulujeme tentýž model jako potenciální pravidla herny a dostaneme pěkný příklad situace, ve které střední hodnota zkoumané veličiny nebude podle naší definice vůbec existovat.



Návštěvník zaplatí vklad $C$ a poté hází mincí. Je-li $T$ počet hodů potřebných k první hlavě, pak obdrží výhru $2^T$. Ptáme se, jaká je „rozumná hodnota“ pro vklad $C$? Je-li $X$ náhodná veličina popisující výhru, jistě se nám zdá, že správnou odpovědí je „cokoliv menší než střední hodnota $\mathrm{E}\,X$“.

Jak jsme odvodili v 9.10, je (za předpokladu férové mince) $P(T = k) = 2^{-k}$. Sečteme-li všechny pravděpodobnosti výsledků vynásobené výhrami $2^k$, dostaneme $\sum_1^\infty 1 = \infty$. Střední hodnota tedy neexistuje. Zdá se proto, že se hráči vyplatí vložit i velký vklad...

Ve skutečnosti simulací hry zjistíme, že nezávisle na počtu pokusů se prakticky všechny výhry budou pohybovat v rozmezí cca do $2^4$. Důvodem je, že nikdo nemůže hrát neomezeně dlouho a vysoké výhry jsou proto velice nepravděpodobné a proto je při reálných úvahách nelze brát vážně. V teorii rozhodování se takovým případům, kdy očekávaná hodnota nemá přímý vztah k vyčíslenému užitku říká *Petrohradský paradox* a k této tématice lze najít rozsáhlou literaturu.[3]

**9.32. Vlastnosti střední hodnoty.** U jednoduchých rozdělení můžeme snadno spočíst jejich střední hodnotu přímo z definice. Např. pro náhodnou veličinu s alternativním rozdělením $\mathrm{A}(p)$ spočteme okamžitě



$$\mathrm{E}\,X = (1-p)\cdot 0 + p \cdot 1 = p.$$

Stejně tak bychom mohli spočíst střední hodnotu $np$ binomického rozdělení $\mathrm{Bi}(n, p)$, to už ale dá trochu přemýšlení. Nicméně výsledek je okamžitým důsledkem následující obecné věty, protože $\mathrm{Bi}(n, p)$ je součtem $n$ náhodných veličin s alternativním rozděleními $\mathrm{A}(p)$.

Uvažme nějaké náhodné veličiny $X$, $Y$, reálné konstanty $a$, $b$ a podívejme se na střední hodnoty funkcí veličin $X + Y$ a $a + bX$, za předpokladu, že střední hodnoty $\mathrm{E}\,X$ a $\mathrm{E}\,Y$ existují.

Přímo z definice je samozřejmé, že konstantní náhodná veličina $a$ má za střední hodnotu opět $a$. Dále,

$$\mathrm{E}(bX) = b\,\mathrm{E}\,X,$$

protože konstanta $b$ se vytkne jak ze sum, tak z integrálů.

[3] Bernoulli, 1738, viz Wiki – hodnota není dána cenou ale užitkem

**Řešení.** Protože $X$ a $Y$ jsou nezávislé náhodné veličiny, je sdružená hustota pravděpodobnosti $f_{(X,Y)} : \mathbb{R}^2 \to \mathbb{R}^2$ veličiny $(X, Y)$ dána součinem hustot pravděpodobnosti $f_X$ veličiny $X$ a $f_Y$ veličiny $Y$, tedy

$$f_{(X,Y)}(u, v) = \\ = \begin{cases} f_X(u) \cdot f_Y(v) = \frac{1}{2} \cdot 2v = v & \text{pro } (u, v) \in (0, 2) \times (0, 1), \\ 0 & \text{jinak.} \end{cases}$$

Hledaná pravděpodobnost $P$ je pak dána integrálem hustoty pravděpodobnosti $f_{(X,Y)}$ přes tu část roviny $O$, kde je $Y < X^2$:

$$P = \iint_O f_{(X,Y)} \,\mathrm{d}x\,\mathrm{d}y = 1 - \iint_{\mathbb{R}^2 \setminus O} f_{(X,Y)} \,\mathrm{d}x\,\mathrm{d}y = \\ = 1 - \int_0^1 \int_{x^2}^1 y \,\mathrm{d}y\,\mathrm{d}x = \frac{3}{5}.$$

□

*9.45.* Nechť $X, Y$ jsou nezávislé náhodné veličiny, přičemž $X$ je dána následující hustotou pravděpodobnosti:

$$f_1(x) = \begin{cases} 0 & \text{pro } x \le 0 \\ 2x & \text{pro } 0 < x < 1 \\ 0 & \text{pro } x \ge 1, \end{cases}$$

veličina $Y$ pak touto hustotou pravděpodobnosti:

$$f_2(x) = \begin{cases} 0 & \text{pro } x \le 0 \\ \frac{x}{2} & \text{pro } 0 < x < 2 \\ 0 & \text{pro } x \ge 2. \end{cases}$$

Určete pravděpodobnost, že $Y$ je větší než $X^2$. ○

**Řešení.** $f_{(X,Y)}(u, v) = uv$, pro $(u, v) \in (0, 1) \times (0, 2)$, $f_{(X,Y)}(u, v) = 0$ jinak. Pro hledanou pravděpodobnost $P$ pak máme

$$P = \int_0^1 \int_{x^2}^2 xy \,\mathrm{d}y\,\mathrm{d}x = \frac{11}{12}.$$ □

*9.46.* Nechť $X, Y$ jsou nezávislé náhodné veličiny, přičemž $X$ je dána následující hustotou pravděpodobnosti:

$$f(x) = \begin{cases} 0 & \text{pro } x \le 0 \\ \frac{2x}{9} & \text{pro } 0 < x < 3 \\ 0 & \text{pro } x \ge 1, \end{cases}$$

veličina $Y$ pak touto hustotou pravděpodobnosti:

$$f(x) = \begin{cases} 0 & \text{pro } x \le 0 \\ \frac{x}{2} & \text{pro } 0 < x < 2 \\ 0 & \text{pro } x \ge 2. \end{cases}$$

Určete pravděpodobnost, že $Y$ je větší než $X^3$.

○

**Řešení.**

$$P = \int_0^{\sqrt[3]{2}} \int_{x^3}^2 xy \,\mathrm{d}y\,\mathrm{d}x = \frac{\sqrt[3]{4}}{12}.$$ □

Obecněji, střední hodnotu součinu dvou nezávislých náhodných veličin $X$ a $Y$ spočteme následovně. Předpokládejme, že vektor $(X, Y)$ má diskrétní nezávislé komponenty s pravděpodobnostními funkcemi $f_X(x_i)$, $f_Y(y_j)$. Potom

$$\mathrm{E}(XY) = \sum_i \sum_j x_i y_j f_X(x_i) f_Y(y_j) = \\ = \Big(\sum_i x_i f_X(x_i)\Big)\Big(\sum_j y_j f_Y(y_j)\Big) = \mathrm{E}\,X\ \mathrm{E}\,Y.$$

Podobně se spočte rovnost $\mathrm{E}(XY) = \mathrm{E}\,X\ \mathrm{E}\,Y$ pro nezávislé spojité veličiny.

Zkusme nyní spočíst $\mathrm{E}(X+Y)$ pro jakékoliv náhodné veličiny. Pro diskrétní rozdělení $X$ a $Y$ dostaneme

$$\mathrm{E}(X + Y) = \sum_i \sum_j (x_i + y_j) P(X = x_i, Y = y_j) = \\ = \sum_i \Big( x_i \sum_j P(X = x_i, Y = y_j) \Big) + \\ + \sum_j \Big( y_j \sum_i P(X = x_i, Y = y_j) \Big) = \\ = \sum_i x_i P(X = x_i) + \sum_j y_j P(Y = y_j),$$

přičemž absolutní konvergence první dvojité sumy vyplývá z trojúhelníkové nerovnosti a absolutní konvergence sum pro střední hodnotu jednotlivých proměnných, při výpočtu jsme pak absolutní konvergence sum využili k záměně pořadí sčítání.

Podobně budeme postupovat u spojitých náhodných veličin $X$ a $Y$ se střední hodnotou. Připomeňme, že hustota součtu náhodných veličin je dána konvolucí jejich hustot.

$$\mathrm{E}(X + Y) = \int_{-\infty}^{\infty} z(f_X * f_Y)(z) dz = \\ = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} z f_X(x) f_Y(z - x)\, dx dz = \\ = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} (z - x) f_X(x) f_Y(z - x)\, dx dz + \\ + \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} x f_X(x) f_Y(z - x)\, dx dz = \\ = \int_{-\infty}^{\infty} u f_Y(u)\, du + \int_{-\infty}^{\infty} x f_X(x)\, dz,$$

kde jsme využili absolutní konvergenci integrálů středních hodnot $\mathrm{E}\,X$ a $\mathrm{E}\,Y$ k záměně integrálů dle Fubiniho věty.

Celkem tedy dostáváme očekávaný vztah:

$$\mathrm{E}(X + Y) = \mathrm{E}\,X + \mathrm{E}\,Y,$$

kdykoliv střední hodnoty $\mathrm{E}\,X$ a $\mathrm{E}\,Y$ existují.

Nyní již přímým použitím tohoto vztahu dostáváme:

AFINNÍ POVAHA STŘEDNÍ HODNOTY

Pro jakékoliv konstanty $a, b_1, \ldots, b_k$ a náhodné veličiny $X_1, \ldots, X_k$ platí

$$\mathrm{E}(a + b_1 X_1 + \cdots + b_k X_k) = a + b_1\,\mathrm{E}\,X_1 + \cdots + b_k\,\mathrm{E}\,X_k.$$

### F. Střední hodnota, korelace

Spočtěte střední hodnotu a rozptyl binomického rozdělení

**Řešení.** Přímý výpočet z definic je pěkné kombinatorické cvičení. My tvrzení dokážeme s využitím vlastnosti středních hodnot a rozptylu. Podle definice binomického rozdělení v 9.22 můžeme náhodnou veličinu $X \sim \mathrm{Bi}(n,p)$ vidět jako součet $X = \sum_{k=1}^{n} Y_k$, kde $Y_1, \ldots, Y_n \sim A(p)$ jsou nezávislé náhodné veličiny vyjadřující úspěch v $k$–tém pokusu. Alternativní rozdělení má zřejmě střední hodnotu $\mathrm{E}\,Y_i = p$, a proto podle věty 9.32 platí $\mathrm{E}\,X = \sum_{k=1}^{n} \mathrm{E}\,Y_k = np$. Podobně snadno vypočteme $\mathrm{E}(Y_k^2) = 1^2 \cdot p + 0^2 \cdot (1-p) = p$, a proto $\mathrm{var}\,Y_k = \mathrm{E}(Y_k^2) - (\mathrm{E}\,Y_k)^2 = p - p^2$. Podle věty 9.36 pak platí $\mathrm{var}\,X = \sum_{k=1}^{n} \mathrm{var}\,Y_k = np(1-p)$. □

**9.47.** Pravděpodobnost zásahu cíle jedním výstřelem je $0,6$. Náhodná veličina $X$ udává počet zásahů při pěti nezávislých výstřelech. Určete její rozdělení pravděpodobnosti, střední hodnotu a rozptyl.

**Řešení.** Výstřely jsou zřejmě nezávislé pokusy s alternativním rozdělením $A(\frac{3}{5})$, a proto je podle definice binomického rozdělení $X \sim \mathrm{Bi}(5, \frac{3}{5})$. Podle ‖F‖ je střední hodnota a rozptyl $\mathrm{Bi}(n,p)$ rovna $np$ respektive $np(1-p)$, což v našem případě dává $\mathrm{E}\,X = 3$ a $\mathrm{var}\,X = \frac{6}{5}$. □

**9.48.** Diskrétní náhodná veličina $X$ nabývá hodnot $k = 0, 1, 2, 3, \ldots$ s pravděpodobností $P(X = k) = p(1-p)^k$ (geometrické rozdělení). Určete $\mathrm{E}\,X$ (střední doba čekání na úspěch) a $\mathrm{var}\,X$.

**Řešení.** Z definice střední hodnoty a s využitím formule pro součet derivace geometrické řady spočítáme

$$\mathrm{E}\,X = \sum_{k=0}^{\infty} kp(1-p)^k = p(1-p)\sum_{k=0}^{\infty} k(1-p)^{k-1} = \\ = p(1-p)\frac{1}{p^2} = \frac{1-p}{p}.$$

Obdobně s využitím formule pro součet druhé derivace geometrické řady spočítáme

$$E(X^2) \quad = \quad \sum_{k=0}^{\infty} k^2 p(1-p)^k = \frac{(1-p)(2-p)}{p^2}$$

a proto je rozptyl roven $\mathrm{var}\,X = \mathrm{E}(X^2) - (\mathrm{E}\,X)^2 = \frac{1-p}{p^2}$. □

**9.49.** Náhodná veličina $X$ má hustotu $f_X(x) = \frac{3}{x^4}$ pro $x \in (1, \infty)$ a jinde nulovou. Určete její distribuční funkci, střední hodnotu a rozptyl.

Následující věta rozšiřuje toto chování vůči afinním transformacím na náhodné vektory a ukazuje, že je střední hodnota invariantní vůči afinním transformacím, stejně jako aritmetický průměr:

**Věta.** *Nechť $X = (X_1, \ldots, X_n)$ je náhodný vektor se střední hodnotou $\mathrm{E}\,X$, $a \in \mathbb{R}^m$, $B \in \mathrm{Mat}_{mn}(\mathbb{R})$ matice. Pak platí*

$$\mathrm{E}(a + B \cdot X) = a + B \cdot \mathrm{E}\,X.$$

Důkaz. Ve skutečnosti už skoro nemáme co dokazovat. Protože je střední hodnota vektoru definována jako vektor středních hodnot, stačí se nám omezit na jedinou položku v $\mathrm{E}(a + B \cdot X)$. Můžeme proto rovnou předpokládat, že $a$ je skalár a $B$ matice s jediným řádkem. Pak jde ovšem o střední hodnotu konečného součtu náhodných veličin a ta podle předchozí úvahy jednak existuje a zároveň je dána jako součet středních hodnot jednotlivých položek. To je právě dokazovaný vztah. □

**9.33. Kvantily a kritické hodnoty.** Pokračujeme v našem programu zavádění číselných charakteristik v obdobě k těm z popisné statistiky. Dalšími užitečnými charakteristikami tam byly tzv. *kvantily*.



Uvažme nejprve náhodnou veličinu s ryze monotonní distribuční funkcí $F_X$. Podmínce vyhovuje každá spojitá náhodná veličina $X$ se všude nenulovou hustotou, jako je tomu např. u normálního rozdělení. V tomto případě definujeme tzv. *kvantilovou funkci* $F_X^{-1}$ prostě jako inverzní funkci $(F_X)^{-1} : (0,1) \to \mathbb{R}$. To znamená, že hodnota $y = F^{-1}(\alpha)$ je právě takové $y$, že $P(X < y) = \alpha$. To přesně odpovídá kvantilům z popisné statistiky, když budeme za pravděpodobnosti brát relativní četnosti výskytu hodnot.

Kvantilová funkce

Obecně, pro libovolnou náhodnou veličinu $X$ s distribuční funkcí $F_X(x)$ definujeme její *kvantilovou funkci*

$$F^{-1}(\alpha) = \inf\{x \in \mathbb{R};\ F(x) \geq \alpha\},\ \alpha \in (0,1).$$

Zřejmě jde o zobecnění předchozí definice v případě ryze monotónní distribuční funkce.

Jak jsme viděli v popisné statistice, nejčastěji jsou používané kvantily s $\alpha = 0{,}5$, tzv. *medián*, s $\alpha = 0{,}25$, tzv. *první kvartil*, $\alpha = 0{,}75$, tzv. *třetí kvartil*, a podobně pro *decily* a *percentily* (kdy je $\alpha$ rovno násobkům desetin a setin).

Jak vyplývá přímo z definice, kvantilová funkce nám pro danou náhodnou veličinu $X$ umožňuje přímo určovat intervaly, do kterých nám padnou hodnoty $X$ s předem zadanou pravděpodobností. Velice často se budeme potkávat např. s hodnotou $\Phi^{-1}(0{,}975)$, která je přibližně rovna 1,96 a zadává percentil 97,5 pro normální rozdělení $\mathrm{N}(0,1)$. Tato hodnota říká, že s 2,5–procentní pravděpodobností bude hodnota takové náhodné veličiny $Z$ alespoň 1,96. Protože je přitom hustota pravděpodobnosti veličiny $Z$ symetrická kolem počátku, můžeme toto pozorování interpretovat tak, že pouze s 5–procentní pravděpodobností bude hodnota $|Z|$ větší než 1,96.

Podobné intervaly a hodnoty budeme hledat při diskusi spolehlivosti odhadů hodnot charakteristik náhodných veličin.

**Řešení.** Z definice distribuční funkce je pro $x \in (1, \infty)$

$$F_X(x) = \int_1^x \frac{3}{t^4} dt = \left[-\frac{1}{t^3}\right]_1^x = 1 - \frac{1}{x^3}.$$

Střední hodnota $X$ je rovna

$$\mathrm{E}\, X = \int_1^\infty \frac{3}{x^3} dx = \left[-\frac{3}{2x^2}\right]_1^\infty = \frac{3}{2}$$

a střední hodnota $X^2$ je

$$\mathrm{E}(X^2) = \int_1^\infty \frac{3}{x^2} dx = \left[-\frac{3}{x}\right]_1^\infty = 3.$$

Proto $\operatorname{var} X = 3 - (\frac{3}{2})^2 = \frac{3}{4}$. □

**9.50.** Náhodná veličina $X$ má hustotu rovnu $f_X(x) = \cos x$ pro $x \in \langle 0, \frac{\pi}{2}\rangle$ a jinde nulovou. Určete střední hodnotu, rozptyl a medián této veličiny.

**Řešení.** Z definice a integrací per partes spočítáme

$$\mathrm{E}\, X = \int_0^{\frac{\pi}{2}} x \cos x dx = [x \sin x + \cos x]_0^{\frac{\pi}{2}} = \frac{\pi}{2} - 1.$$

Dvojitou integrací per partes dostaneme

$$\mathrm{E}(X^2) = \int_0^{\frac{\pi}{2}} x^2 \cos x dx =$$
$$= \left[x^2 \sin x + 2x \cos x - 2 \sin x\right]_0^{\frac{\pi}{2}} = \left(\frac{\pi}{2}\right)^2 - 2,$$

a proto je rozptyl roven $\operatorname{var} X = (\frac{\pi}{2})^2 - 2 - (\frac{\pi}{2} - 1)^2 = \pi - 3$. Distribuční funkce je podle definice rovna $F_X(x) = \int_0^x \cos t dt = \sin x$ a medián $F^{-1}(0{,}5) = \frac{\pi}{6}$. □

**9.51.** Náhodná veličina $X$ má hustotu rovnu $f_X(x) = \lambda e^{-\lambda x}$ pro $x \geq 0$, kde $\lambda > 0$ je daný parametr rozdělení, a jinde nulovou (tzv. exponenciální rozdělení). Určete střední hodnotu, rozptyl, modus (reálné číslo s maximální hustotou, resp. pravděpodobnostní funkcí) a medián této veličiny.

**Řešení.** Z definice a integrací per partes

$$\mathrm{E}\, X = \int_0^\infty x\lambda e^{-\lambda x} dx = \left[-xe^{-\lambda x} - \frac{1}{\lambda} e^{-\lambda x}\right]_0^\infty = \frac{1}{\lambda},$$
$$\mathrm{E}(X^2) = \int_0^\infty x^2 \lambda e^{-\lambda x} dx =$$
$$= \left[-x^2 e^{-\lambda x} - 2x \frac{1}{\lambda} e^{-\lambda x} - \frac{2}{\lambda^2} e^{-\lambda x}\right]_0^\infty = \frac{2}{\lambda^2},$$

a proto $\operatorname{var} X = \mathrm{E}(X^2) - (\mathrm{E}\, X)^2 = \frac{1}{\lambda^2}$. Protože $F'_X(x) = -\lambda^2 e^{-\lambda x} < 0$, je hustota stále klesající funkce. Své maximum tedy nabývá v nule. Z definice je

$$F(x) = \int_0^x \lambda e^{-\lambda t} dt = 1 - e^{-\lambda x}$$

a proto je medián roven $F^{-1}(0{,}5) = -\frac{1}{\lambda} \ln(\frac{1}{2}) = \frac{\ln 2}{\lambda}$. □

KRITICKÉ HODNOTY

Pro náhodnou veličinu $X$ a reálné číslo $0 < \alpha < 1$ definujeme její *kritickou hodnotu $x(\alpha)$ na úrovni $\alpha$* předpisem

$$P(X \geq x(\alpha)) = \alpha.$$

To znamená, že $x(\alpha) = F_X^{-1}(1-\alpha)$, kde $F_X^{-1}$ je kvantilová funkce veličiny $X$.

**9.34. Rozptyl a směrodatná odchylka.** Nejjednodušší číselné charakteristiky udávající variabilitu hodnot vzorku v popisné statistice byly rozptyl a směrodatná odchylka. Pro náhodné veličiny si budeme počínat obdobně.



ROZPTYL NÁHODNÉ VELIČINY

Pro náhodnou veličinu $X$ s konečnou střední hodnotou definujeme její *rozptyl* vztahem

$$\operatorname{var} X = \mathrm{E}\left((X - \mathrm{E}\, X)^2\right),$$

pokud i střední hodnota na pravé straně výrazu existuje. V opačném případě říkáme, že veličina $X$ nemá rozptyl.

Odmocnina $\sqrt{\operatorname{var} X}$ z rozptylu se nazývá *směrodatná odchylka náhodné veličiny $X$*.

S využitím vlastností střední hodnoty snadno spočteme jednodušší vztah pro rozptyl náhodné veličiny $X$ se střední hodnotou:

$$\operatorname{var} X = \mathrm{E}(X - \mathrm{E}\, X)^2 = \mathrm{E}(X^2 - 2X(\mathrm{E}\, X) + (\mathrm{E}\, X)^2) =$$
$$= \mathrm{E}\, X^2 - 2(\mathrm{E}\, X)^2 + (\mathrm{E}\, X)^2 =$$
$$= \mathrm{E}\, X^2 - (\mathrm{E}\, X)^2.$$

Podívejme se také, jak se chová rozptyl náhodné veličiny při afinních transformacích. Pro náhodnou veličinu $X$ se střední hodnotou a rozptylem a pro reálná čísla $a$, $b$ uvažujme náhodnou veličinu $Y = a + bX$. Spočteme

$$\operatorname{var} Y = \mathrm{E}\big((a + bX) - \mathrm{E}(a + bX)\big)^2 == \mathrm{E}\big(b(X - \mathrm{E}\, X)\big)^2$$
$$= b^2 \operatorname{var} X.$$

Odvodili jsem tedy následující užitečné vztahy:

VLASTNOSTI ROZPTYLU

$$\operatorname{var} X = E(X^2) - (EX)^2 \tag{9.8}$$
$$\operatorname{var}(a + bX) = b^2 \operatorname{var} X \tag{9.9}$$
$$\sqrt{\operatorname{var}(a + bX)} = b\sqrt{\operatorname{var} X} \tag{9.10}$$

Ke každé náhodné veličině $X$ se střední hodnotou a rozptylem můžeme zadat tzv. *normovanou veličinu* (často také říkáme *standardizovanou veličinu*) jako funkci

$$Z = \frac{X - \mathrm{E}\, X}{\sqrt{\operatorname{var} X}}.$$

Je to tedy taková afinní transformace původní veličiny, která má střední hodnotu nulovou a rozptyl jednotkový.

**9.52.** Diskrétní náhodný vektor $(X_1, X_2)$ má simultánní pravděpodobnostní funkci $\pi(0,-1) = c, \pi(1,0) = \pi(1,1) = \pi(2,1) = 2c, \pi(2,0) = 3c$ a rovnou nule jinde. Určete konstantu $c$ a vypočtěte kovarianci $\operatorname{cov}(X_1, X_2)$.

**Řešení.** Součet pravděpodobnostních funkcí přes všechny možné stavy musí být roven 1, tj.

$$\sum_{i,j} \pi(i,j) = c + 3.2c + 3c = 10c = 1,$$

a odtud $c = \frac{1}{10}$. Pravděpodobnostní funkce $\pi_1$ pro $X_1$ je dána součtem simultánní funkce přes všechny možné hodnoty $X_2$ , tj. $\pi_1(i) = \sum_j \pi(i,j)$. Je tedy rovna $\pi_1(0) = c$, $\pi_1(1) = 4c$, $\pi_1(2) = 5c$ a nule jinde. Podobně pro pravděpodobnostní funkci $\pi_2$ náhodné veličiny $X_2$ dostaneme $\pi_2(-1) = c$, $\pi_2(0) = 5c$, $\pi_2(1) = 4c$ a nula jinde. Odtud $\mathrm{E}\,X_1 = \sum_i i\pi_1(i) = 14c = 1{,}4$ a $\mathrm{E}\,X_2 = \sum_j j\pi_2(j) = 3c = 0{,}3$. Z definice kovariance pak máme

$$\operatorname{cov}(X_1, X_2) = \sum_{i,j} (i - 1{,}4)(j - 0{,}3)\pi(i,j) = 0{,}18. \qquad \square$$

**9.53.** V mnoha vědních oborech se chování náhodné proměnné omezené na nějaký interval modeluje pomocí tzv. beta rozdělení. Toto spojité rozdělení je dáno pravděpodobnostní funkcí na intervalu $[0, 1]$

$$f_X(x) = \frac{1}{\mathrm{B}(\alpha,\beta)} x^{\alpha-1}(1-x)^{\beta-1},$$

kde $\alpha, \beta$ jsou vhodně zvolené parametry pro popis dané náhodné veličiny a $\mathrm{B}(\alpha,\beta)$ je normalizační konstanta, která zajišťuje, že integrál $f_X(x)$ přes celý interval $[0, 1]$ je roven jedné. Spočítejte jeho a) modus, b) střední hodnotu a c) rozptyl.

**Řešení.** a) Modus je z definice hodnota, ve které nabývá funkce $f_X(x)$ své maximum. Hledejme tedy její stacionární body. Jednoduše spočítáme, že rovnice $f'_X(x) = 0$ je ekvivalentní rovnici

$$(\alpha - 1)(1 - x) - x(\beta - 1) = 0,$$

která je splněna pro $x = \frac{\alpha-1}{\alpha+\beta-2}$. Protože $f_X(0) = f_X(1) = 0$ a funkce je kladná, jedná se evidentně o hledané maximum.
b) Z definice je

$$\mathrm{E}\,X = \frac{1}{\mathrm{B}(\alpha,\beta)} \int_0^1 x^{\alpha}(1-x)^{\beta-1}\,dx.$$

Integrací per partes pak dostáváme

$$\mathrm{E}\,X = -\frac{1}{\mathrm{B}(\alpha,\beta)\beta}[x^{\alpha}(1-x)^{\beta}]_0^1 + \frac{\alpha}{\mathrm{B}(\alpha,\beta)\beta} \int_0^1 x^{\alpha-1}(1-x)^{\beta}\,dx.$$

**9.35. Čebyševova nerovnost.** Hezkou ilustrací, k čemu je užitečný rozptyl, je skoro samozřejmá nerovnost, která dává přímo do souvislosti pravděpodobnost vzdálenosti hodnot náhodné veličiny od její střední hodnoty.



ČEBYŠEVOVA NEROVNOST

**Věta.** *Předpokládejme, že náhodná veličina $X$ má konečný rozptyl, a uvažujme libovolné $\varepsilon > 0$. Potom platí*

$$P(|X - \mathrm{E}\,X| \geq \varepsilon) \leq \frac{\operatorname{var} X}{\varepsilon^2}.$$

DŮKAZ. Uvedeme jednoduchý důkaz pro spojitou náhodnou veličinu $X$. Analogický postup pro diskrétní veličiny ponecháme na čtenáři.

Označme si $\mu = \mathrm{E}\,X$ a počítejme podle definice

$$\begin{aligned}\operatorname{var} X &= \int_{-\infty}^{\infty} (x-\mu)^2 f(x)\,dx = \\ &= \int_{|x-\mu|\geq\varepsilon} (x-\mu)^2 f(x)\,dx + \\ &\quad + \int_{|x-\mu|<\varepsilon} (x-\mu)^2 f(x)\,dx \geq \\ &\geq \int_{|x-\mu|\geq\varepsilon} \varepsilon^2 f(x)\,dx = \varepsilon^2\, P(|X-\mu| \geq \varepsilon). \end{aligned} \qquad \square$$

Když si uvědomíme, že rozptyl je kvadrát směrodatné odchylky $\sigma$, tak okamžitě vidíme, že volba $\varepsilon = k\sigma$ dává pravděpodobnost

$$P(|X - \mathrm{E}\,X| \geq k\sigma) \leq \frac{1}{k^2}.$$

Čebyševova nerovnost je mimořádně užitečná pro asymptotické odhady u limitních procesů. Uvažme např. posloupnost náhodných veličin $X_1, X_2, \ldots$ s rozložením pravděpodobnosti $X_n \sim \mathrm{Bi}(n, p)$ se stejným $0 < p < 1$. Asi bychom intuitivně očekávali, že relativní četnost zdaru by se měla s rostoucím $n$ blížit pravděpodobnosti $p$, tj. že náhodné veličiny $Y_n = \frac{1}{n}X_n$ by se měl stále více svými hodnotami blížit $p$. Evidentně máme

$$\mathrm{E}\,Y_n = \frac{np}{n} = p, \quad \operatorname{var} Y_n = \frac{np(1-p)}{n^2} = \frac{p(1-p)}{n}.$$

Přímé použití Čebyševovy nerovnosti dává pro libovolné pevné $\varepsilon > 0$

$$P\big(|Y_n - p| \geq \varepsilon\big) \leq \frac{p(1-p)}{n\varepsilon^2}.$$

Odtud ale je zřejmé, že pro každé pevně $\varepsilon > 0$ platí

$$\lim_{n\to\infty} P\Big(\Big|\frac{X_n}{n} - p\Big| \geq \varepsilon\Big) = 0.$$

Tento výsledek je známý jako *Bernoulliova věta* (jedna z mnoha).

Tomuto typu limitního chování říkáme *konvergence podle pravděpodobnosti*. Dokázali jsme tedy, že v důsledku Čebyševovy nerovnosti konvergují naše veličiny $Y_n$ podle pravděpodobnosti ke konstantní veličině $p$.

**9.36. Kovariance.** Vraťme se nyní k náhodným vektorům. U střední hodnoty jsme to měli snadné – uvažovali jsme prostě vektor středních hodnot. Pro charakterizaci variability nás však také moc zajímají závislosti mezi jednotlivými komponentami.



První člen je očividně nulový. Úpravou druhého pak dostáváme

$$\mathrm{E}\,X = \frac{\alpha}{\mathrm{B}(\alpha,\beta)\beta}\int_0^1 x^{\alpha-1}(1-x)^{\beta-1}\,dx - \\ -\frac{\alpha}{\mathrm{B}(\alpha,\beta)\beta}\int_0^1 x^{\alpha}(1-x)^{\beta-1}\,dx.$$

Nyní integrál v prvním členu je díky normalizaci roven právě $\mathrm{B}(\alpha,\beta)$ a druhý integrál udává též střední hodnotu. Předchozí rovnici tedy můžeme zapsat ve tvaru

$$\mathrm{E}\,X = \frac{\alpha}{\beta} - \frac{\alpha}{\beta}\,\mathrm{E}\,X.$$

Odtud okamžitě $\mathrm{E}\,X = \frac{\alpha}{\alpha+\beta}$.

c) Pro výpočet rozptylu potřebujeme spočítat

$$\mathrm{E}\,X^2 = \frac{1}{\mathrm{B}(\alpha,\beta)}\int_0^1 x^{\alpha+1}(1-x)^{\beta-1}\,dx.$$

Tento integrál spočítáme podobným způsobem jako v b). Konkretně

$$\mathrm{E}\,X^2 = \frac{\alpha+1}{\mathrm{B}(\alpha,\beta)\beta}\int_0^1 x^{\alpha}(1-x)^{\beta}dx = \frac{\alpha+1}{\beta}\,\mathrm{E}\,X - \frac{\alpha+1}{\beta}\,\mathrm{E}\,X^2.$$

Odtud $\mathrm{E}\,X^2 = \frac{(\alpha+1)\,\mathrm{E}\,X}{\alpha+\beta+1}$. Dosazením střední hodnoty pak máme

$$\operatorname{var} X = \mathrm{E}\,X^2 - (\mathrm{E}\,X)^2 = \frac{\alpha\beta}{(\alpha+\beta+1)(\alpha+\beta)^2}. \qquad \square$$

**9.54.** Hodíme třemi mincemi. Určete korelační koeficient veličiny $X$ udávající počet padlých líců dohromady na první a druhé minci a veličiny $Y$ udávající počet padlých líců dohromady na druhé a třetí minci.

**Řešení.** Nejprve sestavíme pravděpodobnostní tabulku vektorové diskrétní náhodné veličiny $(X, Y)$, ze které snadno určíme pravděpodobnostní rozdělení veličin, které budeme potřebovat (samozřejmě to můžeme udělat i bez tabulky):

| X \ Y | 0 | 1 | 2 |
|---|---|---|---|
| 0 | $\frac{1}{8}$ | $\frac{1}{8}$ | 0 |
| 1 | $\frac{1}{8}$ | $\frac{1}{4}$ | $\frac{1}{8}$ |
| 2 | 0 | $\frac{1}{8}$ | $\frac{1}{8}$ |

Diskrétní veličiny $X$ a $Y$ mají stejné rozdělení pravděpodobnosti a to hodnotu 0 nabývají s pravděpodobností 1/4, hodnotu 1 s pravděpodobností 1/2 a hodnotu 2 s pravděpodobností 1/4. Veličina $XY$ pak může nabývat hodnot 0, 1, 2, 4 a to postupně s pravděpodobnostmi 3/8, 1/4, 1/4, 1/8 Nyní spočítáme střední hodnoty veličin $X$, $X^2$, $Y$,

### Kovariance

Pro náhodné veličiny $X, Y$ s existujícími rozptyly definujeme jejich *kovarianci* předpisem

$$\operatorname{cov}(X,Y) = \mathrm{E}\,((X-\mathrm{E}\,X)(Y-\mathrm{E}\,Y))$$

Velmi snadno odvodíme základní vlastnosti tohoto pojmu:

**Věta.** *Pro jakékoliv náhodné veličin $X$, $Y$, $Z$, pro které existují jejich rozptyly, a reálná čísla $a, b, c, d$ platí*

$$\operatorname{cov}(X,Y) = \operatorname{cov}(Y,X) \tag{9.11}$$

$$\operatorname{cov}(X,Y) = \mathrm{E}(XY) - (\mathrm{E}\,X)(\mathrm{E}\,Y) \tag{9.12}$$

$$\operatorname{cov}(X+Y,Z) = \operatorname{cov}(X,Z) + \operatorname{cov}(Y,Z) \tag{9.13}$$

$$\operatorname{cov}(a+bX, c+dY) = bd\operatorname{cov}(X,Y) \tag{9.14}$$

$$\operatorname{var}(X+Y) = \operatorname{var} X + \operatorname{var} Y + 2\operatorname{cov}(X,Y). \tag{9.15}$$

*Jsou-li navíc naše veličiny $X$ a $Y$ nezávislé, pak* $\operatorname{cov}(X,Y) = 0$. *Zejména potom platí*

$$\operatorname{var}(X+Y) = \operatorname{var} X + \operatorname{var} Y. \tag{9.16}$$

Důkaz. Symetrie kovariance v argumentech je okamžitě vidět z definice . Druhé tvrzení ihned plyne z vlastností střední hodnoty náhodné veličiny:

$$\begin{aligned}\operatorname{cov}(X,Y) &= \mathrm{E}(X-\mathrm{E}\,X)(Y-\mathrm{E}\,Y) = \\ &= \mathrm{E}(XY) - (\mathrm{E}\,Y)X - (\mathrm{E}\,X)Y + \mathrm{E}\,X\,\mathrm{E}\,Y = \\ &= \mathrm{E}(XY) - \mathrm{E}\,X\,\mathrm{E}\,Y\end{aligned}$$

I další tvrzení vyplývá z rozepsání definičního vztahu a skutečnosti, že střední hodnota součtu náhodných veličin je součet jejich středních hodnot.

Další tvrzení opět také spočteme přímo:

$$\begin{aligned}&\operatorname{cov}(a+bX, c+dY) = \\ &\quad= \mathrm{E}\big((a+bX-\mathrm{E}(a+bX))(c+dY-\mathrm{E}(c+dY))\big) = \\ &\quad= \mathrm{E}\big((bX-b\,\mathrm{E}(X))(dY-d\,\mathrm{E}(Y))\big) = \\ &\quad= \mathrm{E}\big(bd(X-\mathrm{E}(X))(Y-\mathrm{E}(Y))\big) = \\ &\quad= bdE\big((X-\mathrm{E}\,X)(Y-\mathrm{E}\,Y)\big) = bd\operatorname{cov}(X,Y).\end{aligned}$$

Další tvrzení o rozptylu jsou už vcelku snadným důsledkem:

$$\begin{aligned}\operatorname{var}(X+Y) &= \mathrm{E}\big((X+Y)-\mathrm{E}(X+Y)\big)^2 = \\ &= \mathrm{E}\big((X-\mathrm{E}\,X)+(Y-\mathrm{E}\,Y)\big)^2 = \\ &= \mathrm{E}(X-\mathrm{E}\,X)^2 + 2\,\mathrm{E}(X-\mathrm{E}\,X)(Y-\mathrm{E}\,Y) + \\ &\quad + \mathrm{E}(Y-\mathrm{E}\,Y)^2 = \\ &= \operatorname{var} X + 2\operatorname{cov}(X,Y) + \operatorname{var} Y.\end{aligned}$$

Pokud jsou navíc $X$ a $Y$ nezávislé, jsou jistě nezávislé i náhodné veličiny $X-\mathrm{E}\,X$ a $Y-\mathrm{E}\,Y$. Pak je ovšem platí $\mathrm{E}(XY) = \mathrm{E}\,X\,\mathrm{E}\,Y$ a je tedy přímo z definice jejich kovariance nulová. $\square$

Přímo z definice také vidíme, že

$$\operatorname{var}(X) = \operatorname{cov}(X,X)$$

$Y^2$, $XY$:

$$\begin{aligned} E(X) &= E(Y) &&= 0\cdot\frac{1}{4}+1\cdot\frac{1}{2}+2\cdot\frac{1}{4}=1\\ E(X^2) &= E(Y^2) &&= 0\cdot\frac{1}{4}+1\cdot\frac{1}{2}+4\cdot\frac{1}{4}=\frac{3}{2}\\ E(XY) & &&= 0\cdot\frac{3}{8}+1\cdot\frac{1}{4}+2\cdot\frac{1}{4}+4\cdot\frac{1}{8}=\frac{5}{4} \end{aligned}$$

Máme tedy

$$\begin{aligned} \sigma^2(X) &= \varsigma^2(Y) &&= E(X^2)-[E(X)]^2=\frac{1}{2}\\ \operatorname{cov}(X,Y) & &&= E(XY)-E(X)E(Y)=\frac{1}{4} \end{aligned}$$

Celkem

$$\rho_{X,Y}=\frac{\operatorname{cov}(X,Y)}{\sigma(X)\cdot\sigma(Y)}=\frac{1}{2}$$

□

*9.55.* Nechť náhodné veličiny $U$, $V$ mají diskrétní rozdělení určené následující tabulkou ($U$ může nabývat hodnot 1, 2, veličina $V$ potom hodnot 1, 2 a 3):

| | V | | |
|---|---|---|---|
| U | 1 | 2 | 3 |
| 1 | 0,1 | 0,2 | 0,3 |
| 2 | 0,2 | 0,1 | 0,1 |

Najděte marginální rozdělení obou náhodných veličin, jejich střední hodnoty, rozptyly a korelační koeficient. ○

*9.56.* Určete střední hodnotu a rozptyl náhodné veličiny $X^2$, kde $X$ je náhodná veličina s rovnoměrným rozdělením pravděpodobnosti na intervalu $\langle -1, 1\rangle$. ○

*9.57.* Dvakrát hodíme šestibokou kostkou. Určete korelační koeficient veličiny $X$ udávající počet padlých sudých čísel a veličiny $Y$ udávající počet padlých lichých čísel. ○

*9.58.* Nechť náhodné veličiny $U$, $V$ mají rozdělení pravděpodobnosti určené následující tabulkou ($U$ může nabývat hodnot 1, 2, veličina $V$ potom hodnot 1, 2 a 3):

| | V | | |
|---|---|---|---|
| U | 1 | 2 | 3 |
| 1 | 0,1 | 0,1 | 0,4 |
| 2 | 0,2 | 0,1 | 0,1 |

Najděte marginální rozdělení obou náhodných veličin, jejich střední hodnoty, rozptyly a korelační koeficient. ○

**9.37. Korelace náhodných veličin.** Předchozí věta nám říká, že



kovariance je symetrickou bilineární formou na reálném vektorovém prostoru náhodných veličin s rozptylem. Rozptyl je pak příslušnou kvadratickou formou a kovarianci lze pak spočíst z rozptylu jednotlivých veličin a jejich součtu, tak jak jsme to viděli v lineární algebře.

Kovariance tedy do jisté míry vypovídá o závislosti dvou náhodných veličin. Hovoříme o *korelaci veličin* a v obdobě ke směrodatné odchylce zavádíme následující pojem

KORELAČNÍ KOEFICIENT

*Korelačním koeficientem* náhodných veličin $X$ a $Y$, které mají konečný nenulový rozptyl, rozumíme hodnotu

$$\rho_{X,Y}=\frac{\operatorname{cov}(X,Y)}{\sqrt{\operatorname{var}X}\sqrt{\operatorname{var}Y}}.$$

Jak je vidět z věty 9.36, korelační koeficient veličin je kovariance normovaných veličin $\frac{1}{\sqrt{\operatorname{var}X}}(X-\operatorname{E}X)$ a $\frac{1}{\sqrt{\operatorname{var}Y}}(Y-\operatorname{E}Y)$).

Okamžitě je také vidět platnost následujících vztahů, kde $a, b, c, d$, $bd \neq 0$, jsou reálné konstanty a $X$, $Y$ jsou náhodné veličiny s nenulovým konečným rozptylem,

$$\begin{aligned} \rho_{a+bX,c+dY} &= \operatorname{sgn}(bd)\rho_{X,Y}\\ \rho_{X,X} &= 1. \end{aligned}$$

Navíc je jistě $\rho_{X,Y}=0$, pokud jsou náhodné veličiny $X$ a $Y$ nezávislé.

Všimněme si, že když má náhodná veličina $X$ nulový rozptyl, pak přímo z definice vidíme, že musí nabývat hodnotu $\operatorname{E}X$ s pravděpodobností 1. Skutečně, kdyby padla hodnota $X$ do nějakého intervalu $I$ neobsahujícího $\operatorname{E}X$ s pravděpodobností $p\neq 0$, pak by musel být výraz $\operatorname{var}X=\operatorname{E}(X-\operatorname{E}X)^2$ kladný. Stochasticky se tedy veličiny s nulovým rozptylem chovají jako konstanty.

Kdyby byla kovariance pozitivně definitní symetrická bilineární forma, Cauchyova-Schwarzova nerovnost (viz 3.25) by okamžitě dala nerovnost

$$|\rho_{X,Y}|\leq 1 \tag{9.17}$$

V následující větě říkáme více. Ukazuje totiž, že korelace nebo antikorelace veličin $X$ a $Y$ říká, že jsou tyto veličiny v nějakém afinním vztahu $Y=kX+c$, přičemž znaménko $k$ odpovídá znaménku v $\rho_{X,Y}=\pm 1$. Naopak, nulový korelační koeficient vypovídá o skutečnosti, že případnou závislost veličin vůbec nejde přiblížit pomocí takového afinního vztahu (a nemusí proto nutně jít o nezávislé veličiny).

**Věta.** *Je-li korelační koeficient definován, pak platí* $|\rho_{X,Y}|\leq 1$. *Rovnost přitom nastává pouze tehdy, když existují konstanty* $k, c$ *takové, že* $P(Y=kX+c)=1$.

DŮKAZ. Protože je rozptyl vždy nezáporný, odhadneme kvadratický výraz

$$0\leq \operatorname{var}\left(\frac{Y-\operatorname{E}Y}{\sqrt{\operatorname{var}Y}}+t\,\frac{X-\operatorname{E}X}{\sqrt{\operatorname{var}X}}\right)=1+2t\rho_{X,Y}+t^2.$$

Kvadratický výraz napravo tedy jistě nemá dva reálné různé kořeny a proto musí být jeho diskriminant nekladný, tj. $4(\rho_{X,Y})^2-4\leq 0$. Odtud již dostáváme dokazovanou nerovnost a také vidíme, že rovnost nastává pouze pro $\rho_{X,Y}=\pm 1$. Pak ovšem pro jediný dvojnásobný kořen $t_0$ má příslušná veličina nulový rozptyl a má tedy s pravděpodobností jedna vhodnou konstantní hodnotu. □

### G. Transformace náhodných veličin

Uvažme spojitou funkci náhodné veličiny $Y = \psi(X)$. Za předpokladu, že transformace $\psi$ je rostoucí (analogicky klesající) funkce, dostáváme pro příslušnou distribuční funkci vztah

$$F_Y(y) = P(Y \le y) = P(\psi(X) \le y) = \\ = P(X \le \psi^{-1}(y)) = F_X(\psi^{-1}(y)),$$

kde $F_X$ je distribuční funkce $X$. Odkud pro hustotu transformované náhodné veličiny $Y$

$$f_Y(y) = \frac{dF_Y(y)}{dy} = f_X(\psi^{-1}(y)) \left| \frac{d\psi^{-1}(y)}{dy} \right|.$$

Podle pravidla pro transformaci souřadnic v integrálu pak můžeme střední hodnotu $Y$ spočítat jako

$$\mathrm{E}\, Y = \int_{-\infty}^{\infty} y f_Y(y) dy = \int_{-\infty}^{\infty} \psi(x) f_X(x) dx$$

a podobně pro rozptyl $Y$.

**9.59.** Náhodná veličina $X$ má hustotu $f(x)$. Určete hustotu náhodné veličiny $Y$ tvaru

i) $Y = e^X, x \ge 0$,
ii) $Y = \sqrt{X}, x > 0$,
iii) $Y = \ln X, x > 0$,
iv) $Y = \frac{1}{X}, x > 0$.

**Řešení.** Přímým aplikováním formule pro hustotu transformované náhodné veličiny dostaneme a) $f_Y(y) = f(\ln y)\frac{1}{y}$, b) $f_Y(y) = 2f(y^2)y$, c) $f_Y(y) = f(e^y)e^y$, d) $f_Y(y) = f(1/y)\frac{1}{y^2}$. □

**9.60.** Náhodná veličina $X$ má rovnoměrné rozdělení pravděpodobnosti na intervalu $(-\frac{\pi}{2}, \frac{\pi}{2})$. Určete jeho hustotu a hustotu transformovaných veličin $Y = \sin X$, $Z = \mathrm{tg}\, X$.

**Řešení.** Protože délka intervalu, na kterém je náhodná veličina $X$ nenulová je $\pi$, je její hustota rovna $f_X(x) = \frac{1}{\pi}$ pro $x \in (-\frac{\pi}{2}, \frac{\pi}{2})$ a nula jinde. Ze vztahu pro hustotu transformované náhodné veličiny a podle vzorce pro derivaci elementárních funkcí pak máme

$$f_Y(y) = f_X(\arcsin(y)) \arcsin'(y) = \frac{1}{\pi\sqrt{1-y^2}}$$

a

$$f_Z(y) = f_X(\mathrm{arctg}(z)) \,\mathrm{arctg}'(y) = \frac{1}{\pi(1+y^2)}.$$ □

**9.61.** Náhodná veličina $X$ má hustotu rovnu $\cos x$ pro $x \in (0, \frac{\pi}{2})$ a nulovou jinde. Určete hustotu náhodné veličiny $Y = X^2$ a vypočtěte $\mathrm{E}\, Y$, $\mathrm{var}\, Y$.

**9.38. Varianční matice.** Dostáváme se konečně k variabilitě hodnot náhodného vektoru. Nabízí se uvažovat kovariance všech dvojic komponent. Následující definice a věta ukazují, že skutečně dostaneme analogii rozptylu pro vektory, včetně chování rozptylu při afinních transformacích náhodných veličin.



VARIANČNÍ MATICE

Uvažme náhodný vektor $X = (X_1, \ldots, X_n)^T$ jehož všechny komponenty mají konečný rozptyl. *Varianční matici* náhodného vektoru $X$ definujeme pomocí střední hodnoty předpisem (vektor $X$ je sloupec náhodných veličin)

$$\mathrm{var}\, X = \mathrm{E}(X - \mathrm{E}\, X)(X - \mathrm{E}\, X)^T.$$

Použitím definice střední hodnoty vektoru a přímým rozepsáním násobení matic po složkách ověříme, že varianční matice je symetrická matice

$$\mathrm{var}\, X = \begin{pmatrix} \mathrm{var}\, X_1 & \mathrm{cov}(X_1, X_2) & \cdots & \mathrm{cov}(X_1, X_n) \\ \mathrm{cov}(X_2, X_1) & \mathrm{var}\, X_2 & \cdots & \mathrm{cov}(X_2, X_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{cov}(X_n, X_1) & \mathrm{cov}(X_n, X_2) & \cdots & \mathrm{var}\, X_n \end{pmatrix}$$

**Věta.** *Uvažujme náhodný vektor $X = (X_1, \ldots, X_n)^T$, jehož všechny komponenty mají konečný rozptyl, Uvažme dále jeho transformovanou vektorovou náhodnou veličinu $Y = BX + c$, kde $B$ je matice reálných konstant typu $m \times n$ a $c$ je vektor konstant v $\mathbb{R}^m$. Potom*

$$\mathrm{var}(Y) = \mathrm{var}(BX + c) = B(\mathrm{var}\, X)B^T.$$

DŮKAZ. Stačí provést přímý výpočet a využít přitom vlastnosti střední hodnoty

$$\mathrm{var}(Y) = \mathrm{E}\big((BX + c) - \mathrm{E}(BX + c)\big)\big((BX + c) - \\ - \mathrm{E}(BX + c)\big)^T = \\ = \mathrm{E}(B(X - \mathrm{E}\, X))(B(X - \mathrm{E}\, X))^T = \\ = B\,\mathrm{E}(X - \mathrm{E}\, X)(X - \mathrm{E}\, X)^T B^T = \\ = B(\mathrm{var}\, X)B^T.$$

□

Stejně jako u rozptylu skalární náhodné veličiny tedy vidíme, že konstantní část transformace nemá vliv, zatímco vůči lineární části transformace se varianční matice chová jako matice kvadratické formy.

**9.39. Momenty a momentová funkce.** Střední hodnota a rozptyl odráží chování střední hodnoty samotné veličiny $X$ a jejího kvadrátu. V popisné statistice jsme také zkoumali tzv. šikmost rozložení dat a je přirozené zkoumat variabilitu náhodných veličin pomocí vyšších mocnin dané náhodné veličiny $X$.



Charakteristiku $E(X^k)$ nazýváme *k-tým momentem*, charakteristiku $\mu_k = E\left((X - EX)^k\right)$ pak *k-tým centrálním momentem* náhodné veličiny $X$. Užitečný bývá také tzv. *k-tý absolutní moment* zadaný předpisem $\mathrm{E}\,|X|^k$.

Přímo z definice je tedy pro spojitou veličinu $X$

$$\mathrm{E}\, X^k = \int_{-\infty}^{\infty} x^k f_X(x)\, dx$$

**Řešení.** Podle vzorce pro hustotu transformované náhodné veličiny je

$$f_Y(y) = f_X(\sqrt{y})(\sqrt{y})' = \frac{1}{2\sqrt{y}}\cos x.$$

Střední hodnotu a rozptyl $Y$ je jednodušší počítat přímo z hustoty náhodné veličiny $X$. Platí $\mathrm{E}\,Y = \int_{-\infty}^{\infty} x^2 f_X(x)dx$ a proto

$$\mathrm{E}\,Y = \int_0^{\frac{\pi}{2}} x^2 \cos x dx = \left[x^2 \sin x + 2x\cos x - 2\sin x\right]_0^{\frac{\pi}{2}} = \frac{\pi^2 - 8}{4}.$$

Integrál jsme spočítali metodou per partes. Stejnou metodou spočítáme

$$\mathrm{E}(Y^2) = \int_0^{\frac{\pi}{2}} x^4 \cos x dx = \\ = \left[(x^4 - 12x^2 + 24)\sin x + 4(x^3 - 6x)\cos x\right]_0^{\frac{\pi}{2}}.$$

Odtud máme $\mathrm{E}(Y^2) = (\frac{\pi}{2})^4 - 12(\frac{\pi}{2})^2 + 24$, a proto $\operatorname{var} Y = \frac{\pi^4}{16} - 3\pi^2 + 24 - \frac{\pi^4 - 16\pi^2 + 64}{16} = 20 - 2\pi^2$. □

**9.62.** Nechť $X$ je náhodná veličina, která nabývá hodnoty 0 s pravděpodobností $\frac{1}{2}$ a hodnoty 1 též s pravděpodobností $\frac{1}{2}$. Podobně nechť $Y$ je náhodná veličina, která nabývá hodnoty -1 a 1 s pravděpodobnostmi $\frac{1}{2}$. Ukažte, že náhodné veličiny $X$ a $Z = XY$ jsou nekorelované, ale závislé. Udejte příklad dvou spojitých náhodných veličin, které mají tuto vlastnost.

**Řešení.** Nejprve spočítáme střední hodnoty našich náhodných veličin $\mathrm{E}\,X = 0\cdot\frac{1}{2} + 1\cdot\frac{1}{2} = \frac{1}{2}$, $\mathrm{E}\,Z = \mathrm{E}(XY) = 0\cdot\frac{1}{2} + (-1)\cdot\frac{1}{4} + 1\cdot\frac{1}{4} = 0$. Pro střední hodnotu jejich součinu máme $\mathrm{E}(XZ) = \mathrm{E}(X^2Y) = 1\cdot\frac{1}{4} + (-1)\cdot\frac{1}{4} = 0$. Podle věty 9.36 je pak kovariance rovna $\operatorname{cov}(X,Z) = 0 - \frac{1}{2}\cdot 0 = 0$. Veličiny $X$ a $Y$ jsou tedy nekorelované. Zároveň je podmíněná pravděpodobnost $P(Z = 1|X = 0)$ zřejmě nulová, tj. i $P(Z = 1, X = 0) = 0$, a přitom $P(Z = 1) = \frac{1}{4}$ a $P(X = 0) = \frac{1}{2}$, tedy $P(Z = 1)\cdot P(X = 0) = \frac{1}{8} \neq 0$. Vidíme, že $P(Z = 1)\cdot P(X = 0) \neq P(Z = 1, X = 0)$, což znamená, že $X$ a $Z$ jsou závislé.

Z příslušných definic lze lehce ověřit, že příkladem spojitých nekorelovaných závislých náhodných veličin jsou $X$ a $Y = X^2$, kde $X$ je libovolně rozložená náhodná veličina, která má nulovou střední hodnotu, konečný druhý moment a nulový třetí moment. □

### H. Nerovnosti a limitní věty

Markovova nerovnost dává hrubý odhad nezáporné náhodné veličiny v případě, že neznáme nic jiného, než její střední hodnotu. Konkrétně říká, že pro každou nezápornou náhodnou veličinu $X$ a pro libovolné $a > 0$ platí $P(X \geq a) \leq \frac{\mathrm{E}\,X}{a}$.

a obdobně víme, že pro diskrétní veličiny $X$ s pravděpodobností soustředěnou do hodnot $x_i$ bude

$$\mathrm{E}\,X^k = \sum_i x_i^k f_X(x_i).$$

Uvidíme, že bude pro výpočty velice výhodné umět pracovat s mocninnou řadou, ve které momenty budou vystupovat coby koeficienty. Protože víme, že koeficienty Taylorovy řady funkce $M(t)$ v bodě $t = 0$ dostaneme pomocí diferencování, můžeme vcelku snadno uhádnout správnou volbu takové funkce:

MOMENTOVÁ VYTVOŘUJÍCÍ FUNKCE

Pro náhodnou veličinu $X$ uvažme funkci $M_X(t) : \mathbb{R} \to \mathbb{R}$ definovanou předpisem

$$M_X(t) = \mathrm{E}\,e^{tX} = \begin{cases} \sum_i \mathrm{e}^{tx_i} f_X(x_i) & \text{pro diskrétní } X \\ \int_{-\infty}^{\infty} \mathrm{e}^{tx} f_X(x)\,dx & \text{pro spojitou } X. \end{cases}$$

Pokud tato střední hodnota existuje, hovoříme o *momentové vytvořující funkci* náhodné veličiny $X$.

Je zjevné, že tato funkce $M_X(t)$ je vždy analytickou funkcí v případě diskrétních náhodných veličin s konečně mnoha hodnotami $x_i$.

**Věta.** *Nechť $X$ je náhodná veličina pro kterou na intervalu $(-a, a)$ existuje její analytická momentová vytvořující funkce. Pak na tomto intervalu je $M_X(t)$ dána absolutně konvergující řadou*

$$M_X(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!}\mathrm{E}\,X^k.$$

DŮKAZ. Ověření tvrzení věty je jednoduchým cvičením na techniky diferenciálního a integrálního počtu. V případě diskrétní veličiny, jde buď o konečné součty nebo o počítání s absolutně a stejnoměrně konvergentními řadami, resp. v případě spojitých veličin jde o absolutně konvergující integrály. Můžeme proto prohodit limitní proces s derivováním a protože $\frac{d}{dt}\mathrm{e}^{tx} = x\,\mathrm{e}^{tx}$, dostáváme okamžitě vztah

$$\frac{d^k}{dt^k}M_X(t) = \mathrm{E}\,X^k$$

a odtud je tvrzení věty zřejmé. □

Ve skutečnosti lze ukázat, že předpoklady věty jsou splněny, kdykoliv platí současně $M_X(-a) < \infty$ a $M_X(a) < \infty$ a navíc lze dokázat, že platí-li v takovém případě rovnost momentových funkcí $M_X(t) = M_Y(t)$ na nějakém netriviálním intervalu, pak mají tyto náhodné veličiny $X$ a $Y$ také stejné distribuční funkce. Momentová funkce tedy poskytuje za těchto podmínek úplnou charakterizaci náhodné veličiny.

**9.40. Vlastnosti momentové funkce.** Díky vlastnostem exponenciální funkce lze očekávat, že snadno spočteme, jak se chová momentová vytvořující funkce při afinních transformacích náhodných veličin a při součtech nezávislých náhodných veličin.



**Lemma.** *Nechť $a, b \in \mathbb{R}$ a $X$, $Y$ jsou nezávislé náhodné veličiny s momentovými vytvořujícími funkcemi $M_X(t)$ a $M_Y(t)$. Potom*

**9.63.** Mějme nezápornou náhodnou veličinu $X$ se střední hodnotou $\mu$. Bez dalších informací o rozdělení $X$ odhadněte $P(X > 3\mu)$. Vypočtěte $P(X > 3\mu)$ víte-li, že $X \sim \mathrm{Ex}(\frac{1}{\mu})$.

**Řešení.** Pokud nezáporná náhodná veličina $X$ nenabývá pouze nulovou hodnotu, pak je její střední hodnota $\mu$ kladná. Proto můžeme danou pravděpodobnost zhruba odhadnout pomocí Markovovy nerovnosti

$$P(X \geq 3\mu) \leq \frac{\mu}{3\mu} = \frac{1}{3}.$$

Pokud víme, že $X \sim \mathrm{Ex}(\frac{1}{\mu})$, pak

$$P(X > 3\mu) = 1 - P(X \leq 3\mu) = 1 - F(3\mu),$$

kde $F$ je distribuční funkce exponenciálního rozdělení. Ta je podle definice

$$F(x) = \int_0^x \frac{1}{\mu} e^{-\frac{t}{\mu}} dt = \left[-e^{-\frac{t}{\mu}}\right]_0^x = 1 - e^{-\frac{x}{\mu}}$$

a proto $P(X > 3\mu) = \frac{1}{e^3}$. □

**9.64.** Průměrná rychlost větru je na určitém místě 20 km/hod.

- Bez ohledu na rozdělení rychlosti větru jako náhodné veličiny odhadněte pravděpodobnost, že při jednom pozorování rychlost větru nepřesáhne 60 km/h.
- Určete interval, v němž se bude rychlost větru nacházet s pravděpodobností alespoň 0,9, víte-li navíc, že směrodatná odchylka $\sigma = 1$ km/hod.

**Řešení.** Označme náhodnou veličinu udávající rychlost větru $X$. V prvním případě můžeme použít pouze hrubý odhad pomocí Markovovy nerovnosti

$$P(X \leq 60) = 1 - P(X \geq 60) \geq 1 - \frac{20}{60} = \frac{2}{3}.$$

V druhém případě známe rozptyl (resp. směrodatnou odchylku) rychlosti větru, a proto k určení daného intervalu můžeme použít Čebyševovu nerovnost 9.35

$$0,9 \leq P(|X - 20| < x) = 1 - P(|X - 20| \geq x) \leq 1 - \frac{1}{x^2}.$$

Odtud $x \geq \sqrt{10} \approx 3,2$. Hledaný interval je tedy (16,8 km/hod, 23,2 km/hod). □

**9.65.** Ke každému jogurtu běžné značky je náhodně (rovnoměrně) přibalen obrázek některého z 26 hokejových mistrů světa. Kolik jogurtů si fanynka Věrka musí koupit, aby s pravděpodobností 0,95 získala alespoň 5 kartiček Jaromíra Jágra?

**Řešení.** Označíme-li náhodnou veličinu udávající počet získaných kartiček Jágra $X$, je zřejmě $X \sim \mathrm{Bi}(n, \frac{1}{26})$, kde $n$ je celkový počet koupených jogurtů. Hledáme takovou hodnotu tohoto čísla, aby

*mají náhodné veličiny $V = a + bX$ a $W = X + Y$ momentové vytvořující funkce*

$$M_{a+bX}(t) = \mathrm{e}^{at} M_X(bt)$$
$$M_{X+Y}(t) = M_X(t) M_Y(t)$$

Důkaz. První vztah spočteme přímo z definice

$$M_V(t) = \mathrm{E}\,\mathrm{e}^{(a+bX)t} = \mathrm{E}\,\mathrm{e}^{at}\,\mathrm{e}^{(bt)X} = \mathrm{e}^{at} M_X(bt).$$

U druhého využijeme skutečnost, že střední hodnota součinu nezávislých veličin je součinem jejich středních hodnot.

$$M_W(t) = \mathrm{E}\,\mathrm{e}^{t(X+Y)} = \mathrm{E}\,\mathrm{e}^{tX}\,\mathrm{e}^{tY} = \mathrm{E}\,\mathrm{e}^{tX}\,\mathrm{E}\,\mathrm{e}^{tY} = M_X(t) M_Y(t).$$

□



Pro ilustraci si spočtěme přímo z definice momentovou funkci náhodné veličiny $X$ s normálním rozložením $\mathrm{N}(\mu, \sigma)$ a náhodné veličiny $X$ s binomiálním rozložením $\mathrm{Bi}(n, p)$. Začneme s veličinou $Z \sim \mathrm{N}(0, 1)$

$$\begin{aligned} M_Z(t) &= \int_{-\infty}^{\infty} \mathrm{e}^{tx} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{x^2}{2}}\,\mathrm{d}x = \\ &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{1}{2}(x^2 - 2tx + t^2 - t^2)}\,\mathrm{d}x = \\ &= \mathrm{e}^{\frac{t^2}{2}} \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{(x-t)^2}{2}}\,\mathrm{d}x = \\ &= \mathrm{e}^{\frac{t^2}{2}}, \end{aligned}$$

kde jsme využili při výpočtu skutečnost, že v předposledním výrazu integrujeme pro každé pevné $t$ hustotu rozdělení spojité náhodné veličiny, proto je tento integrál roven jedné.

Jde tedy o případ všude analytické funkce a zejména existují momenty všech řádů. Přímým dosazením $\frac{1}{2}t^2$ do mocninné řady pro exponenciálu je všechny okamžitě spočteme:

$$\begin{aligned} M_Z(t) &= \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{t^2}{2}\right)^k = \sum_{k=0}^{\infty} \frac{1}{k! 2^k} t^{2k} = \\ &= 1 + 0\,t + \frac{1}{2}\,t^2 + 0\,t^3 + \frac{3}{4!}\,t^4 + \ldots \end{aligned}$$

Zejména tedy znovu vidíme, že střední hodnota $Z$ je skutečně $\mathrm{E}\,Z = 0$ a její rozptyl je $\mathrm{var}\,Z = \mathrm{E}\,Z^2 - (\mathrm{E}\,Z)^2 = 1$.

Dosazením do vztahu pro momentovou vytvořující funkci $M_{\mu+\sigma Z}$ dostaneme pro $X \sim \mathrm{N}(\mu, \sigma)$

$$M_X(t) = \mathrm{e}^{\mu t}\,\mathrm{e}^{\frac{\sigma^2 t^2}{2}}$$

a odtud také okamžitě vidíme, že součet nezávislých normálních rozdělení $X \sim \mathrm{N}(\mu, \sigma)$ a $Y \sim \mathrm{N}(\mu', \sigma')$ má opět normální rozdělení $X + Y \sim \mathrm{N}(\mu + \mu', \sigma + \sigma')$.

Podobně pro veličinu $X \sim \mathrm{Bi}(n, p)$ spočteme snadno

$$\begin{aligned} M_X(t) = \mathrm{E}\,\mathrm{e}^{tX} &= \sum_{k=0}^{n} (p\,\mathrm{e}^t)^k \binom{n}{k} (1-p)^{n-k} = \\ &= (p\,\mathrm{e}^t + (1-p))^n = (p(\mathrm{e}^t - 1) + 1)^n = \\ &= 1 + npt + (\binom{n}{2} p^2 + n\frac{p}{2}) t^2 + \ldots. \end{aligned}$$

$P(X \geq 5) = 0{,}95$, tj. $F_X(4) = P(X \leq 4) = 0{,}05$. Abychom ji mohli určit, aproximujeme binomické rozdělení podle Moivreovy-Laplaceovy věty normálním rozdělením (předpokládáme hodnota $n$ bude velké, a proto chyba aproximace bude malá). Podle ‖F‖ má $X$ střední hodnotu $\mathrm{E}\,X = \frac{n}{26}$ a rozptyl $\mathrm{var}\,X = \frac{25n}{26^2}$. Označíme-li tedy $Z$ standardizovanou veličinu, pak danou podmínku můžeme ekvivalentně přepsat

$$0{,}05 = P(X \leq 4) = P\left(Z \leq \frac{4 - \frac{n}{26}}{\frac{5\sqrt{n}}{26}}\right) = F_Z\left(\frac{104 - n}{5\sqrt{n}}\right),$$

kde $F_Z \approx \Phi$ je podle aproximačního předpokladu distribuční funkce normálního rozdělení N(0, 1). Protože určitě $n > 104$, tak využitím $\Phi(-x) = 1 - \Phi(x)$ předchozí rovnice dává $n - 104 = \Phi^{-1}(0{,}95) \cdot 5\sqrt{n}$. Kvantil vystupující v této rovnici má podle tabulek hodnotu $z(0{,}95) = 1{,}65$. Vyřešením této kvadratické rovnice pak obdržíme $n \doteq 228{,}8$. Věrka tedy musí koupit aspoň 229 jogurtů. □

**9.66.** Určete pravděpodobnost, že při 1200 hodech kostkou padne šestka alespoň 150 krát a nejvýše 250 krát pomocí Čebyševovy nerovnosti a pak pomocí Moivreovy-Laplaceovy věty.

**Řešení.** Označíme-li náhodnou veličinu udávající počet šestek $X$, pak je zjevně $X \sim \mathrm{Bi}(1200, \frac{1}{6})$. Podle ‖F‖ je tedy $\mathrm{E}\,X = 1200 \cdot \frac{1}{6} = 200$ a $\mathrm{var}\,X = 200(1 - \frac{1}{6}) = \frac{500}{3}$. Podmínka na počet šestek má ze zadání tvar $150 \leq X \leq 250$, což lze zapsat také jako $|X - 200| \leq 50$. Použitím Čebyševovy nerovnosti 9.35 pak

$$P(|X - 200| \leq 50) = 1 - P(|X - 200| \geq 51) \geq 1 - \frac{500}{3 \cdot 51^2} \approx 0{,}94.$$

(2) Přesná hodnota hledané pravděpodobnosti je zřejmě dána výrazem

$$P(150 \leq X \leq 250) = F_X(250) - F_X(150),$$

kde $F_X$ je distribuční funkce binomického rozdělení. Z definice tedy

$$P(150 \leq X \leq 250) = \sum_{k=150}^{250} \binom{1200}{x} \left(\frac{1}{6}\right)^x \left(\frac{5}{6}\right)^{1200-x}.$$

Tento výraz je obtížně vyčíslitelný, a proto k jeho odhadu využijeme Moivreovu-Laplaceovu větu. Nahradíme-li $X$ standardizovanou náhodnou veličinou

$$Z = \frac{\sqrt{3}(X - 200)}{10\sqrt{5}},$$

pak podle 9.42 je $Z \sim N(0, 1)$, tj. $F_Z \approx \Phi$, a tedy

$$P(150 \leq X \leq 250) = P\left(\tfrac{\sqrt{3}(150-200)}{10\sqrt{5}} \leq Z \leq \tfrac{\sqrt{3}(250-200)}{10\sqrt{5}}\right) \approx$$
$$\approx \Phi(\sqrt{15}) - \Phi(-\sqrt{15}) = 2\Phi(\sqrt{15}) - 1.$$

Z tabulek $\Phi(\sqrt{15}) \approx 0{,}99994$, a proto je hledaná pravděpodobnost asi 99,988%. □

Samozřejmě jsme mohli totéž spočíst ještě snadněji s využitím posledního lemmatu, protože je $X$ součtem $n$ nezávislých veličin $Y \sim A(p)$ s alternativním rozdělením. Je tedy nutně

$$\mathrm{E}\,\mathrm{e}^{tX} = (\mathrm{E}\,\mathrm{e}^{tY})^n = (p\,\mathrm{e}^t + (1 - p))^n.$$

Opět odtud hned vidíme, že všechny momenty veličiny $Y$ jsou rovny $p$. Proto $\mathrm{E}\,Y = p$, zatímco $\mathrm{var}\,Y = p(1 - p)$. Z momentové funkce $M_X(t)$ odečteme snadno $\mathrm{E}\,X = np$ a $\mathrm{var}\,X = \mathrm{E}\,X^2 - (\mathrm{E}\,X)^2 = np(1 - p)$.

Všimněme si, že náhodná veličina vzniklá jako součet $n$ nezávislých náhodných veličin $Y_i$ se stejným rozložením se samozřejmě stochasticky chová zásadně odlišně od násobku $nY$.

**9.41. Šikmost a špičatost.** Protože je třetí centrální moment dán pomocí třetích mocnin odchylek od střední hodnoty, bude do jisté míry vyjadřovat, jak moc nejsou hodnoty náhodné veličiny rozprostřeny symetricky kolem střední hodnoty. To jsme v popisné statistice sledovali pomocí koeficientu šikmosti. U náhodných veličin se používá se v podobě charakteristiky



$$\gamma_1 = \frac{\mathrm{E}(X - \mathrm{E}\,X)^3}{(\sqrt{\mathrm{var}\,X})^3}$$

a říkáme jí *koeficient šikmosti náhodné veličiny* $X$.

Další běžně užívanou charakteristikou je *koeficient špičatosti* náhodné veličiny $X$, který definujeme předpisem

$$\gamma_2 = \frac{\mathrm{E}(X - \mathrm{E}\,X)^4}{(\mathrm{var}\,X)^2} - 3.$$

Viděli jsme, že u normovaného normálního rozdělení je třetí centrální moment nulový a čtvrtý je roven 3. Zvolené normování koeficientu špičatosti je voleno tak, aby jeho hodnota pro normované normální rozdělení byla nulová. Pro obecné rozložení pak špičatost dává srovnání s normálním rozdělením.

V praxi se však můžeme setkat i s jinými normováními koeficientů šikmosti a špičatosti.

**9.42. Centrální limitní věta.** Nyní se konečně dostáváme ke klíčovému nástroji, který propojuje pravděpodobnost a statistiku. Technicky se bude zdát, že jde o vcelku jednoduchou manipulaci s momentovými vytvořujícími funkcemi. Historicky však byly daleko dříve a jinak dokázány mnohé speciální případy, které samy o sobě mají velkou hodnotu, protože často podávají navíc odhady rychlosti konvergence, a ty jsou pochopitelně pro praktické využití třeba.



Před formulací výsledku se nejprve zastavme u zobecnění Bernoulliovy věty o binomickém rozdělení na konci odstavce 9.35. Náhodné veličiny $\frac{1}{n}X_n$, kde $X_n \sim \mathrm{Bi}(n, p)$ můžeme považovat za aritmetický průměr součtu $n$ nezávislých veličin s rozdělením $\mathrm{A}(p)$ a samotné Bernoulliho tvrzení pak říká, že tyto průměry konvergují k hodnotě $p$ s pravděpodobností 1. Toto tvrzení platí zcela obecně takto:

**Lemma.** *Uvažme posloupnost po dvou nekorelovaných náhodných veličin $X_1, X_2, \ldots$, které mají všechny společnou konečnou střední hodnotu $\mathrm{E}\,X_i = \mu$. Předpokládejme navíc, že tyto veličiny mají konečné rozptyly omezené konstantou $\mathrm{var}\,X_i \leq C$. Potom pro libovolné $\varepsilon > 0$ platí*

$$\lim_{n\to\infty} P\Big(\Big|\frac{1}{n}\sum_{i=1}^{n} X_i - \mu\Big| < \varepsilon\Big) = 1.$$

**9.67.** Na fakultě informatiky je 10% studentů s prospěchem do 1,2. Jak velkou skupinu je třeba vybrat, aby s pravděpodobností 0,95 v ní bylo 8-12% studentů s prospěchem do 1,2? Úlohu řešte napřed pomocí Čebyševovy a potom pomocí Moivre-Laplaceovy věty.

**Řešení.** Označme jako $X$ náhodnou veličinu udávající počet studentů s prospěchem do 1,2 z $n$ vybraných studentů. Při výběru jednotlivého studenta vyberu takového s pravděpodobností 10%, a proto při nezávislém výběru $n$ studentů je $X \sim \mathrm{Bi}(n, \frac{1}{10})$. Podle ‖F‖ je $\mathrm{E}\,X = 0{,}1n$ a $\mathrm{var}\,X = 0{,}09n$. Pro hledanou pravděpodobnost pak podle Čebyševovy nerovnosti 9.35 platí

$$P(|X - 0{,}1n| \le 0{,}02n) = 1 - P(|X - 0{,}1n| \ge 0{,}02n) \ge$$
$$\ge 1 - \frac{0{,}1 \cdot 0{,}9n}{(0{,}02n)^2} = 1 - \frac{225}{n}.$$

Nerovnost $1 - \frac{225}{n} \ge 0{,}95$ a tedy i

$$P(|X - 0{,}1n| \le 0{,}02n) \ge 0{,}95.$$

je splněna pro $n \ge 4500$. Přesná hodnota pravděpodobnosti je dána pomocí distribuční funkce $F_X$ binomického rozdělení

$$P(0{,}08n \le X \le 0{,}12n) = F_X(0{,}12n) - F_X(0{,}08n).$$

Podle Moivreovy-Laplaceovy věty z 9.42 můžeme standardizovanou náhodnou veličinu $Z = \frac{10X-n}{3\sqrt{n}}$ aproximovat normovaným normálním rozložením, $F_Z \approx \Phi$, a proto

$$\begin{aligned} 0{,}95 &= P(0{,}08n \le X \le 0{,}12n) = P(-\frac{\sqrt{n}}{15} \le Z \le \frac{\sqrt{n}}{15}) \approx \\ &\approx \Phi(\frac{\sqrt{n}}{15}) - \Phi(-\frac{\sqrt{n}}{15}) = \\ &= 2\Phi(\frac{\sqrt{n}}{15}) - 1. \end{aligned}$$

Odtud $\sqrt{n} = 15z(0{,}975)$ a z tabulek dopočítáme $n \approx 864{,}4$. Vidíme tedy, že stačí vybrat 865 studentů. □

**9.68.** Pravděpodobnost, že zasazený strom se ujme, je 0,8. Jaká je pravděpodobnost, že z 500 zasazených stromů se jich ujme aspoň 380?

**Řešení.** Náhodná veličina $X$ udávající počet stromů, které se ujaly, má binomické rozdělení $X \sim \mathrm{Bi}(500, \frac{4}{5})$. Podle ‖F‖ je $\mathrm{E}\,X = 400$ a $\mathrm{var}\,X = 80$. Standardizovaná náhodná veličina je tedy $Z = \frac{X-400}{\sqrt{80}}$. Podle Moivreovy-Laplaceovy věty je $F_Z \approx \Phi$, a proto

$$\begin{aligned} P(X \ge 380) &= P(Z \ge \frac{380 - 400}{\sqrt{80}}) \approx 1 - \Phi(-\frac{\sqrt{20}}{2}) = \\ &= \Phi(\frac{\sqrt{20}}{2}) \approx 0{,}987. \end{aligned}$$

□

Důkaz. Tvrzení ověříme pomocí Čebyševovy nerovnosti stejně, jako jsme postupovali v závěru odstavce 9.35. Spočteme

$$P\big(|\frac{1}{n}\sum_{i=1}^{n} X_i - \mu| \ge \varepsilon\big) \le \frac{\mathrm{var}\big(\frac{1}{n}\sum_{i=1}^{n} X_i - \mu\big)}{\varepsilon^2} =$$
$$= \frac{\frac{1}{n^2}\sum_{i=1}^{n} \mathrm{var}\,X_i}{\varepsilon^2} \le \frac{C}{n\varepsilon^2}.$$

Je tedy pravděpodobnost zkoumaná v našem tvrzení odhadnuta zdola výrazem

$$P\big(|\frac{1}{n}\sum_{i=1}^{n} X_i - \mu| < \varepsilon\big) \ge 1 - \frac{C}{n\varepsilon^2}$$

a lemma je dokázáno. □

Vidíme tedy, že k tomu, aby posloupnosti průměrů po dvou nekorelovaných veličin $X_i$ s nulovou střední hodnotou konvergovaly (ve smyslu pravděpodobnosti) k nule, potřebujeme jen existenci a stejnoměrnou omezenost jejich rozptylů.



Náš další cíl bude ambicióznější. Budeme asymptotické chování posloupnosti náhodných veličin $X_i$ porovnávat s normálním rozdělením. Chceme přitom uvažovat posloupnost nezávislých normovaných náhodných veličin se stejným rozdělením pravděpodobnosti, které však nemusí být ani normální ani binomické.

Předpokládáme tedy $\mathrm{E}\,X_i = 0$ a $\mathrm{var}\,X_i = 1$. Z technických důvodů dále předpokládejme, že existuje momentová vytvořující funkce $M_X(t)$ všech veličin $X_i$ a že je také stejnoměrně omezený třetí absolutní moment $\mathrm{E}\,|X_i|^3 < C$.

Aritmetický průměr $\frac{1}{n}\sum_{i=1}^{n} X_i$ je samozřejmě náhodná veličina se střední hodnotou 0, její rozptyl je ale $\frac{n}{n^2} = \frac{1}{n}$. Uvažujme proto místo aritmetických průměrů raději náhodné veličiny

$$S_n = \frac{1}{\sqrt{n}}\sum_{i=1}^{n} X_i,$$

které budou opět normované. Jejich momentové vytvořující funkce jsou (viz lemma 9.40)

$$M_{S_n}(t) = \mathrm{E}\,\mathrm{e}^{\frac{t}{\sqrt{n}}\sum_i X_i} = \Big(M_X(\frac{t}{\sqrt{n}})\Big)^n.$$

Vzhledem k předpokladu o normovanosti veličin $X_i$ platí

$$M_X(\frac{t}{\sqrt{n}}) = 1 + 0\,\frac{t}{\sqrt{n}} + 1\,\frac{t^2}{2n} + \mathrm{o}(\frac{t^2}{n}),$$

kde opět píšeme $\mathrm{o}(G(n))$ pro výraz, který jde po podělení výrazem $G(n)$ v limitě pro $n \to \infty$ k nule, viz odstavec 6.17.

V limitě tedy můžeme psát (připomeňme, že třetí absolutní moment je ohraničený konstantou $C$)

$$\lim_{n\to\infty} M_{S_n}(t) = \lim_{n\to\infty}\Big(1 + \frac{t^2}{2n} + \mathrm{o}(\frac{1}{n})\Big)^n = \mathrm{e}^{\frac{t^2}{2}}.$$

To je ale právě momentová vytvořující funkce normálního rozdělení $Z \sim \mathrm{N}(0, 1)$, viz konec odstavce 9.38. Naše normované veličiny $S_n$ tedy asymptoticky mají normované normální rozdělení. Tím jsme odvodili následující základní větu:

**Věta** (Centrální limitní věta)**.** *Uvažme posloupnost nezávislých náhodných veličin $X_i$, které mají společné střední hodnotu $\mathrm{E}\,X_i = \mu$*

**9.69.** Pomocí distribuční funkce standardního normálního rozdělení určete pravděpodobnost, že při 1600 hodech mincí bude rozdíl mezi počtem padlých hlav a orlů alespoň 82.

**Řešení.** Označíme-li jako $X$ náhodnou veličinu udávající počet padlých hlav, tak $X$ má binomické rozložení pravděpodobnosti $Bi(1600, 1/2)$ (se střední hodnotou 800 a směrodatnou odchylkou 20) a tudíž lze distribuční funkci veličiny $\frac{X-800}{20}$ lze pro dané velké $n = 1600$ podle Moivreovy-Laplaceovy věty velmi dobře odhadnout jako distribuční funkci $\Phi$ standardního normálního rozdělení. Hledaná pravděpodobnost je tedy

$$\begin{aligned} P &= 1 - P[759 \le X \le 841] \\ &= 1 - P\left[-2,05 \le \frac{X-800}{20} \le 2,05\right] \\ &\doteq 2\Phi(-2,05) \doteq 0,0404. \end{aligned}$$

□

**9.70.** Pomocí distribuční funkce standardního normálního rozdělení určete pravděpodobnost, že při 3600 hodech mincí bude rozdíl mezi počtem padlých hlav a orlů nejvýše 66.

**Řešení.** Označíme-li jako $X$ náhodnou veličinu udávající počet padlých hlav, tak $X$ má binomické rozložení pravděpodobnosti $Bi(3600, 1/2)$ (se střední hodnotou 1800 a směrodatnou odchylkou 30) a tudíž lze distribuční funkci veličiny $\frac{X-1800}{30}$ lze pro dané velké $n = 3600$ podle Moivreovy-Laplaceovy věty velmi dobře odhadnout jako distribuční funkci $\Phi$ standardního normálního rozdělení. Hledaná pravděpodobnost je tedy

$$\begin{aligned} P[1767 \le X \le 1833] &= P\left[-1,1 \le \frac{X-1800}{30} \le 1,1\right] \doteq \\ &\doteq \Phi(1,1) - \Phi(-1,1) \doteq 0,7498. \end{aligned}$$

□

**9.71.** Pravděpodobnost, že semeno vyklíčí, je 0,9. Kolik semen je třeba zasadit, aby s pravděpodobností aspoň 0,995 vyklíčilo cca 90% semen (což přesněji formulujeme se zpřesňujícím požadavkem, aby odchylka podílu vyklíčených semen od 0,9 nepřevýšila 0,034).

**Řešení.** Náhodná veličina $X$, udávající počet vyklíčených semen z $n$ zasazených, má binomické rozdělení $X \sim \mathrm{Bi}(n, \frac{9}{10})$. Podle ‖F‖ je $\mathrm{E}\,X = 0,9n$ a $\mathrm{var}\,X = 0,09n$, a proto je standardizovaná veličina $Z = \frac{X-0,9n}{\sqrt{0,09n}}$. Podmínku ze zadání lze psát ve tvaru

$$\begin{aligned} P(|X - 0,9n| \le 0,034n) &= P\left(|Z| \le \frac{0,034n}{\sqrt{0,09n}}\right) = \\ &= P\left(|Z| \le \frac{0,34}{3}\sqrt{n}\right) \ge 0,995. \end{aligned}$$

*a rozptyl* $\mathrm{var}\,X_i = \sigma^2 > 0$ *a stejnoměrně omezený třetí absolutní moment* $\mathrm{E}\,|X_i|^3 < C$. *Pro rozdělení náhodné veličiny*

$$S_n = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \left(\frac{X_i - \mu}{\sigma}\right)$$

*platí v limitě vztah*

$$\lim_{n\to\infty} P(S_n < x) = \Phi(x),$$

*kde* $\Phi$ *je distribuční funkce normovaného normálního rozdělení.*

Všimněme si, že v případě centrální limitní věty dostáváme jako výsledek asymptotické chování, které říká, že distribuční funkce jistých veličin se blíží k distribuční funkci normovaného normálního rozdělení. Takovému chování říkáme *konvergence podle distribuční funkce*. Je zřejmé, že tato konvergence je slabší než je konvergence podle pravděpodobnosti.

**9.43. Moivreova-Laplaceova věta.** Historicky asi první formulací centrální limitní věty byl případ veličin $Y_n$ s binomickým rozdělením $\mathrm{Bi}(n, p)$. Ty můžeme chápat jako součet $n$ nezávislých veličin $X_i$ s alternativním rozdělením $A(p)$, $0 < p < 1$. Přitom jsme viděli, že tyto veličiny mají momentovou vytvořující funkci a $\mathrm{E}\,|X_i|^3 = p < 1$.

Centrální limitní věta v tomto případě tedy říká, že náhodné veličiny

$$S_n = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \left(\frac{X_i - p}{\sqrt{p(1-p)}}\right) = \frac{X - np}{\sqrt{np(1-p)}}$$

se asymptoticky chovají stejně jako normované normální rozdělení.

To také můžeme formulovat tak, že náhodná veličina $X \sim \mathrm{Bi}(n, p)$ se s rostoucím $n$ chová jako veličina s normálním rozdělením $\mathrm{N}(np, np(1-p))$.

V praxi se považuje za vyhovující aproximace binomického rozdělení pomocí normálního, jestliže platí $np(1-p) > 9$.

Zkusme si výsledek ilustrovat na konkrétním příkladu. Řekněme, že chceme s chybou nejvýše 5% zjistit, kolik procent studentů má v oblibě danou přednášku. Počet osob majících přednášku v oblibě mezi $n$ náhodně vybranými bude nejspíš mít charakter náhodné veličiny $X \sim \mathrm{Bi}(n, p)$. Dejme tomu, že přitom chceme, abychom dosáhli správného výsledku se spolehlivostí (tj. opět pravděpodobností) alespoň 90%. Chceme tedy zajistit

$$P\left(\left|\frac{1}{n}X - p\right| < 0,05\right) \simeq 0,9$$

tím, že zvolíme dostatečně veliký počet dotázaných studentů $n$.

Nyní můžeme přibližně počítat

$$\begin{aligned} 0,9 &\simeq P\left(\left|\frac{1}{n}X - p\right| < 0,05\right) = \\ &= P\left(-\frac{0,05n}{\sqrt{np(1-p)}} < \frac{X-np}{\sqrt{np(1-p)}} < \frac{0,05n}{\sqrt{np(1-p)}}\right) \simeq \\ &\simeq \Phi\left(\frac{0,05n}{\sqrt{np(1-p)}}\right) - \Phi\left(-\frac{0,05n}{\sqrt{np(1-p)}}\right) = \\ &= 2\Phi\left(\frac{0,05n}{\sqrt{np(1-p)}}\right) - 1. \end{aligned}$$

Podle Moivreovy-Laplaceovy věty lze pro velké $n$ distribuční funkci aproximovat distribuční funkcí $\Phi$ normálního rozdělení. Proto

$$P\left(|Z| \le \frac{0{,}34}{3}\sqrt{n}\right) \approx \Phi\left(\frac{0{,}34}{3}\sqrt{n}\right) - \Phi\left(-\frac{0{,}34}{3}\sqrt{n}\right) = \\ = 2\Phi\left(\frac{0{,}34}{3}\sqrt{n}\right) - 1.$$

Celkem tedy dostáváme podmínku

$$2\Phi\left(\frac{0{,}34}{3}\sqrt{n}\right) - 1 \ge 0{,}995.$$

Odtud vypočítáme $n \ge \left(\frac{3z(0{,}9975)}{0{,}34}\right)^2 \approx 615$. □

**9.72.** Životnost (v hodinách) určité elektrické součástky má exponenciální rozdělení s parametrem $\lambda = \frac{1}{10}$. Pomocí centrální limitní věty odhadněte pravděpodobnost, že celková životnost 100 takových součástek bude mezi 900 a 1050 hodinami.

**Řešení.** V příkladu ‖9.51‖ jsem spočítali, že střední hodnota a rozptyl náhodné veličiny $X_i$ s exponenciálním rozdělením jsou rovny $\mathrm{E}\,X_i = \frac{1}{\lambda}$ a $\mathrm{var}\,X_i = \frac{1}{\lambda^2}$. Střední životnost každé z našich součástek je tedy $\mathrm{E}\,X_i = \mu = 10$ hodin s rozptylem $\mathrm{var}\,X_i = \sigma^2 = 100$. Podle centrální limitní věty se rozdělení transformované náhodné veličiny $\frac{1}{\sqrt{n}}\sum_{i=1}^{n}\left(\frac{X_i-\mu}{\sigma}\right) = \frac{1}{100}\sum_{i=1}^{100} X_i - 10$ pro rostoucí $n$ blíží normovanému normálnímu rozdělení. Proto hledanou pravděpodobnost pro životnost 100 součástek

$$P(900 \le \sum X_i \le 1050) = P\left(-1 \le \frac{1}{100}\sum_{i=1}^{100} X_i - 10 \le 0,5\right)$$

můžeme aproximovat pomocí distribuční funkce normálního rozdělení

$$P(900 \le \sum X_i \le 1050) \approx \Phi(0{,}5) - \Phi(-1) \approx 0{,}533.$$ □

**9.73.** Do bedny ukládáme výrobky se střední hodnotou 3 kg a směrodatnou odchylkou 0,8 kg. Jaký maximální počet výrobků můžeme do bedny uložit, aby celková hmotnost s pravděpodobností 99% nepřekročila jednu tunu?

**Řešení.** Označíme-li náhodnou veličinu, udávající hmotnost $i$-tého výrobku $X_i$, pak ze zadání $\mu = \mathrm{E}\,X_i = 3$ a $\sigma = \sqrt{\mathrm{var}\,X_i} = 0{,}8$ (vše v kg) a má platit

$$P(\sum_{i=1}^{n} X_i \le 1000) = 0{,}99.$$

Podle centrální limitní věty 9.42 lze rozdělení náhodné veličiny

$$S_n = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}\left(\frac{X_i - 3}{0{,}8}\right) = \frac{1}{0{,}8\sqrt{n}}\sum_{i=1}^{n} X_i - \frac{3\sqrt{n}}{0{,}8}$$

Chceme tedy dosáhnout

$$\Phi\left(\frac{0{,}05n}{\sqrt{np(1-p)}}\right) \simeq \frac{1}{2}(1 + 0{,}9) = 0{,}95.$$

Tento požadavek vede na volbu (připomeňme definici kritických hodnot $z(\alpha)$ pro veličinu s normovaným normálním rozdělením $Z$ v odstavci 9.33)

$$\Phi\left(\frac{0{,}05n}{\sqrt{np(1-p)}}\right) \simeq z(0{,}05) = 1{,}64485.$$

Protože $p(1-p)$ nabývá největší hodnoty $\frac{1}{4}$, můžeme odtud odhadnout potřebný počet $n > 270$ nezávisle na $p$.

**9.44. Přehled charakteristik některých rozdělení.** V dalším se



vrátíme ke statistice a jistě nás nepřekvapí, že budeme pracovat s charakteristikami náhodných vektorů, které budou obdobné výběrovému průměru a rozptylu, ale také s relativními poměry takových charakteristik atd. Podíváme se proto teď na několik takových případů předem.

Uvažme náhodnou veličinu $Z \sim \mathrm{N}(0, 1)$ a spočtěme hustotu $f_Y(x)$ náhodné veličiny $Y = Z^2$. Evidentně je $f_Y(x) = 0$ pro $x \le 0$, zatímco pro kladná $x$

$$F_Y(x) = P(Y < x) = P(-\sqrt{x} < Z < \sqrt{x}) = \\ = \int_{-\sqrt{x}}^{\sqrt{x}} \frac{1}{\sqrt{2\pi}}\,\mathrm{e}^{-z^2/2}\,dz = \int_0^x \frac{1}{\sqrt{2\pi}}\,t^{-1/2}\,\mathrm{e}^{-t/2}\,dt.$$

Hustotu dostaneme derivací

$$f_Y(x) = \frac{d}{dx}F_Y(x) = \frac{1}{\sqrt{2\pi}}x^{-1/2}\,\mathrm{e}^{-x/2}.$$

Tomuto rozdělení se říká $\chi^2$ *s jedním stupněm volnosti*, píšeme $Y \sim \chi^2$.

Budeme pracovat se součty takovýchto nezávislých veličin, ty ale všechny padnou do obecné třídy rozdělení s podobnými hustotami tvaru

$$f_X(x) = cx^{a-1}\,\mathrm{e}^{-bx}$$

pro $x > 0$, zatímco $f_X(x) = 0$ pro nekladná $x$, tj. naše rozdělení $\chi^2$ odpovídá volbě $a = b = 1/2$. Tento případ jsme již podrobně diskutovali jako příklad v odstavci 9.25 a proto již víme, že taková funkce bude hustotou pro konstantu $c = \frac{b^a}{\Gamma(a)}$. Jde tedy o rozdělení $\Gamma(a, b)$ s hustotou pro kladná $x$

$$f_X(x) = \frac{b^a}{\Gamma(a)}x^{a-1}\,\mathrm{e}^{-bx}.$$

Obecně lze snadno spočíst $k$-tý moment takové veličiny $X$:

$$\mathrm{E}\,X^k = \int_0^\infty x^k\,\frac{b^a}{\Gamma(a)}x^{a-1}\,\mathrm{e}^{-bx}\,dx = \\ = \frac{\Gamma(a+r)}{\Gamma(a)b^r}\int_0^\infty x^k\,\frac{b^{a+r}}{\Gamma(a+r)}x^{a-1+r}\,\mathrm{e}^{-bx}\,dx = \\ = \frac{\Gamma(a+r)}{\Gamma(a)b^r},$$

protože integrál z hustoty rozdělení $\Gamma(a+r, b)$ v posledním upravovaném výrazu je nutně roven jedné.

Zejména tedy vidíme, že $\mathrm{E}\,X = \frac{\Gamma(a+1)}{b\Gamma(a)} = \frac{a}{b}$, zatímco

$$\mathrm{var}\,X = \frac{\Gamma(a+2)}{b^2\Gamma(a)} - \frac{a^2}{b^2} = \frac{(a+1)a - a^2}{b^2} = \frac{a}{b^2}.$$

aproximovat normovaným normálním rozdělením, a proto

$$P(\sum_{i=1}^{n} X_i \le 1000) = P(S_n \le \frac{1000}{0{,}8\sqrt{n}} - \frac{3\sqrt{n}}{0{,}8}) \approx \Phi(\frac{1000}{0{,}8\sqrt{n}} - \frac{3\sqrt{n}}{0{,}8}).$$

Z tabulek najdeme $z(0{,}99) \approx 2{,}326$, takže pro hledané $n$ dostáváme kvadratickou rovnici

$$\frac{1000}{0{,}8\sqrt{n}} - \frac{3\sqrt{n}}{0{,}8} = 2{,}326,$$

ze které vypočítáme $n \approx 322$. □

### I. Testování výběrů z normálního rozdělení

V 9.50 jsme se seznámili s tak zvaným oboustranným intervalovým odhadem neznámého parametru $\mu$ normálního rozložení $\mathrm{N}(\mu, \sigma^2)$. V některých případech nás zajímá pouze horní nebo dolní odhad, tj. statistika $U$ respektive $L$, pro niž $P(\mu < U)$ respektive $P(L < \mu)$. Mluvíme pak o jednostranném intervalu spolehlivosti $(-\infty, U)$ respektive $(L, \infty)$. Vztah pro výpočet těchto intervalů se odvodí obdobně jako u oboustranného intervalu. Pro náhodnou veličinu $Z = \sqrt{n}\frac{\bar{X}-\mu}{\sigma} \sim \mathrm{N}(0, 1)$ tentokrát máme

$$1 - \alpha = \Phi(z(1-\alpha)) = P(Z < z(1-\alpha)).$$

Odtud okamžitě

$$1 - \alpha = P(\bar{X} - \frac{\sigma}{\sqrt{n}} z(1-\alpha) < \mu),$$

tedy $L = \bar{X} - \frac{\sigma}{\sqrt{n}} z(1-\alpha)$. Obdobně zjistíme $U = \bar{X} + \frac{\sigma}{\sqrt{n}} z(1-\alpha)$ a pro rozdělení s neznámým rozptylem $\mu \ge \bar{X} - \frac{S}{\sqrt{n}} t_{n-1}(1-\alpha)$ a $\mu \le \bar{X} + \frac{S}{\sqrt{n}} t_{n-1}(1-\alpha)$.

Pokud potřebujeme odhadnout rozptyl $\sigma^2$ náhodného rozložení, pak stejně jako u odvození odhadu střední hodnoty využijeme větu 9.49. Tentokrát ovšem využijeme její druhou část, podle které má náhodná veličina $\frac{n-1}{\sigma^2} S^2$ rozložení $\chi^2$. Okamžitě je pak vidět, že platí

$$1 - \alpha = P\left(\chi^2_{n-1}(\alpha/2) \le \frac{n-1}{\sigma^2} S^2 \le \chi^2_{n-1}(1-\alpha/2)\right).$$

Oboustranný $100(1-\alpha)\%$ interval spolehlivosti pro rozptyl je tedy

$$\left(\frac{(n-1)S^2}{\chi^2_{n-1}(1-\alpha/2)}, \frac{(n-1)S^2}{\chi^2_{n-1}(\alpha/2)}\right)$$

a podobně pro jednostranný horní a dolní odhad dostaneme

$$\sigma^2 \le \frac{(n-1)S^2}{\chi^2_{n-1}(\alpha)}, \text{ resp. } \frac{(n-1)S^2}{\chi^2_{n-1}(1-\alpha)} \le \sigma^2.$$

Úplně obdobně spočteme momentovou vytvořující funkci pro všechny hodnoty $-b < t < b$

$$\begin{aligned} M_X(t) &= \int_0^\infty \mathrm{e}^{tx} \frac{b^a}{\Gamma(a)} x^{a-1} \mathrm{e}^{-bx}\, dx = \\ &= \frac{b^a}{(b-t)^a} \int_0^\infty x^k \frac{(b-t)^a}{\Gamma(a)} x^{a-1} \mathrm{e}^{-(b-t)x}\, dx = \\ &= \frac{b^a}{(b-t)^a}. \end{aligned}$$

Pro součet nezávislých rozdělení $Y = X_1 + \cdots + X_n$ s rozděleními $X_i \sim \Gamma(a_i, b)$ tedy okamžitě dostáváme momentovou vytvořující funkci (pro hodnoty $|t| < b$)

$$M_Y(t) = \left(\frac{b}{b-t}\right)^{a_1+\cdots+a_n},$$

tj. $Y \sim \Gamma(a_1 + \cdots + a_n, b)$. Velmi podstatný je ovšem přitom předpoklad, že všechna gamma rozdělení sdílí stejnou hodnotu $b$.

Jako okamžitý důsledek nyní dostáváme hustotu rozdělení veličiny $Y = Z_1^2 + \cdots + Z_n^2$, kde všechna $Z_i \sim \mathrm{N}(0, 1)$. Jde totiž podle právě dokázaného o gamma rozdělení $Y \sim \Gamma(n/2, 1/2)$ a má proto hustotu

$$f_Y(x) = \frac{1}{2^{n/2}\Gamma(n/2)} x^{n/2-1} \mathrm{e}^{-x/2}.$$

Tomuto speciálnímu případu gamma rozdělení říkáme rozdělení $\chi^2$ *s n stupni volnosti*. Značíme jej zpravidla $Y \sim \chi^2_n$.

**9.45. F-rozdělení a t-rozdělení.** Ve statistických úvahách často chceme porovnávat dva různé výběrové rozptyly a bude tedy třeba uvažovat veličiny, které jsou dány podílem



$$U = \frac{X/k}{Y/m},$$

přičemž $X \sim \chi^2_k$ a $Y \sim \chi^2_m$.

Budeme chtít spočíst hustotu takového rozdělení a začneme obecnější úvahou. Předpokládejme, že $f_X(x)$ a $f_Y(x)$ jsou hustoty nezávislých náhodných veličin $X$ a $Y$ a $f_Y$ je nenulové pouze pro kladná $x$. Spočteme si distribuční funkci náhodné veličiny $U = cX/Y$, kde $c > 0$ je libovolná konstanta. Při výpočtu použijeme Fubiniho větu o záměnnosti integrování podle jednotlivých proměnných.

$$\begin{aligned} F_U(u) = P(X < (u/c)Y) &= \int_0^\infty \int_{-\infty}^{uy/c} f_X(x) f_Y(y)\, dx\, dy = \\ &= \int_0^\infty \left(\int_{-\infty}^{u} \frac{y}{c} f_X(ty/c) f_Y(y)\, dt\right) dy = \\ &= \int_{-\infty}^{u} \left(\frac{1}{c} \int_0^\infty y f_X(ty/c) f_Y(y)\, dy\right) dt. \end{aligned}$$

Z tohoto výrazu pro $F_U(u)$ okamžitě plyne, že hustota $f_U$ náhodné proměnné $U$ je rovna

$$f_U(u) = \frac{1}{c} \int_0^\infty y f_X(uy/c) f_Y(y)\, dy.$$

Když teď dosadíme hustoty příslušných speciálních gamma rozdělení za $X \sim \chi^2_k$ a $Y \sim \chi^2_m$ a za konstantu $c$ zvolíme

**9.74.** Při 600 hodech kostkou padla šestka celkem 45 krát. Je možné tvrdit, že jde o ideální kostku na hladině $\alpha = 0{,}01$?

**Řešení.** Pro ideální kostku je pravděpodobnost hodu šestky při každém hodu rovna $p = \frac{1}{6}$. Počet šestek v 600 hodech je pak dán náhodnou veličinou $X$, která má binomické rozdělení $X \sim \mathrm{Bi}(600, \frac{1}{6})$. Toto rozdělení můžeme podle 9.42 aproximovat rozdělením $\mathrm{N}(100, \frac{250}{3})$. Naměřenou hodnotu $X = 45$ můžeme považovat za náhodný výběr o jednom členu. Pokládáme-li rozptyl za známý, pak podle 9.50 je pak 99% (oboustranný) interval spolehlivosti pro střední hodnotu $\mu$ roven $(45 - \sqrt{\frac{250}{3}}z(0{,}995),\ 45 + \sqrt{\frac{250}{3}}z(0{,}995))$. Z tabulek zjistíme, že kvantil přibližně $z(0{,}995) \approx 2{,}58$, což dává interval $(21, 69)$. Na ideální kostce je ale zřejmě $\mu = 100$, a proto nejde v tomto smyslu o ideální kostku na hladině $\alpha = 0{,}01$. □

**9.75.** Předpokládejme, že výška desetiletých chlapců má normální rozdělení $\mathrm{N}(\mu, \sigma^2)$ s neznámou střední hodnotou $\mu$ a rozptylem $\sigma^2 = 39{,}112$. Změřením výšky 15 chlapců jsme určili výběrový průměr $\bar{X} = 139{,}13$. Určete

i) 99% oboustranný interval spolehlivosti pro parametr $\mu$,

ii) dolní odhad $\mu$ na hladině významnosti 95%.

**Řešení.** a) Podle 9.50 je $100(1-\alpha)\%$ oboustranný interval spolehlivosti pro neznámou střední hodnotu $\mu$ normálního rozložení dán výrazem

$$\mu \in \left(\bar{X} - \frac{\sigma}{\sqrt{n}}z(1-\alpha/2),\ \bar{X} + \frac{\sigma}{\sqrt{n}}z(1-\alpha/2)\right), \tag{9.3}$$

kde $\bar{X}$ je výběrový průměr z $n$ hodnot, $\sigma^2$ je známý rozptyl a $z(1-\alpha/2)$ je příslušný kvantil. Přímým dosazením ze zadání $n = 15$, $\sigma \approx 6{,}254$ a z tabulek $z(0{,}995) \approx 2{,}576$ dostaneme $\frac{\sigma}{\sqrt{n}}z(\alpha/2) \approx 4{,}16$, tj. $\mu \in (134{,}97,\ 143{,}29)$.

b) Dolní odhad $L$ parametru $\mu$ na hladině významnosti 95% je určen výrazem $L = \bar{X} - \frac{\sigma}{\sqrt{n}}z(0{,}95)$. Z tabulek $z(0{,}95) \approx 1{,}645$, a proto přímým dosazením dostáváme $\mu \in (136{,}474, \infty)$. □

**9.76.** Odběratel provádí kontrolu jakosti námi dodaných výrobků namátkovou kontrolou testovaného rozměru u 21 náhodně vybraných výrobků. Dodávka bude přijata, pokud nebude výběrová směrodatná odchylka překračovat hodnotu 0,2 mm. Víme přitom, že naše stroje produkují výrobky, u nichž má sledovaný rozměr normální rozdělení tvaru $\mathrm{N}(10\,\mathrm{mm};\ 0{,}0734\,\mathrm{mm}^2)$. S využitím statistických tabulek určete pravděpodobnost, s níž bude dodávka přijata. Jak se změní odpověď, pokud odběratel kvůli nákladům na testy začne testovat pouze 4 výrobky?

$c = m/k$, dostaneme pro náhodnou veličinu $U = \frac{X/k}{Y/m}$ hustotu $f_U(u)$

$$\frac{(k/m)^{k/2}}{2^{(k+m)/2}u^{k/2-1}\Gamma(k/2)\Gamma(m/2)}\int_0^\infty y^{(k+m)/2-1}\,\mathrm{e}^{-y(1+ku/m)/2}\,dy.$$

(Ověřte si sami!) Poslední integrál obsahuje, až na konstantní násobek hustotu rozdělení $\Gamma((k+m)/2, (1+ku/m)/2)$, takže hledaná hustota bude mít tvar

$$f_U(u) = \frac{\Gamma((k+m)/2)}{\Gamma(k/2)\Gamma(m/2)}\Big(\frac{k}{m}\Big)^{k/2}u^{k/2-1}\Big(1+\frac{k}{m}u\Big)^{-(k+m)/2}.$$

Takovému rozdělení se říká *Fisherovo-Snedecorovo rozdělení s k a m stupni volnosti*, zkráceně také *F-rozdělení*.

Další potřebné rozdělení se objevuje při zkoumání podílu veličin $Z \sim \mathrm{N}(0,1)$ a $\sqrt{X/n}$, kde $X \sim \chi^2_n$ (tj. zajímá nás poměr $Z$ a směrodatné odchylky nějakého výběru).

Spočteme nejdříve opět snadno distribuční funkci pro $Y = \sqrt{X}$ (všimněme si, že $X$ a tedy i $Y$ nabývají s nenulovou pravděpodobností pouze kladných hodnot)

$$\begin{aligned} F_Y(y) &= P(\sqrt{X} < y) = P(X < y^2) = \\ &= \int_0^{y^2} \frac{1}{2^{n/2}\Gamma(n/2)}x^{n/2-1}\,\mathrm{e}^{-x/2}\,dy = \\ &= \int_0^{y} \frac{1}{2^{n/2-1}\Gamma(n/2)}t^{n-1}\,\mathrm{e}^{-t^2/2}\,dt. \end{aligned}$$

Odtud již vidíme, že hustota náhodné veličiny $Y$ je

$$f_Y(y) = \frac{1}{2^{n/2-1}\Gamma(n/2)}y^{n-1}\,\mathrm{e}^{-y^2/2}.$$

Nyní můžeme použít stejný postup jako v předchozím odstavci u náhodné veličiny $U = cZ/Y$ a volíme $c = \sqrt{n}$, $Y = \sqrt{X}$. Dostaneme tedy pro náhodnou veličinu

$$T = \frac{Z}{\sqrt{X/n}}$$

po krátkém výpočtu, podobném jako výše, hustotu $f_T(t)$ ve tvaru

$$f_T(t) = \frac{\Gamma((n+1)/2)}{\Gamma(n/2)\sqrt{n\pi}}\left(1+\frac{t^2}{n}\right)^{-(n+1)/2}.$$

Tomuto rozdělení říkáme *Studentovo t-rozdělení s n stupni volnosti*.

**9.46. Vícerozměrné normální rozdělení.** Jestliže má náhodný vektor $Z = (Z_1, \dots, Z_n)$ nezávislé komponenty $Z_i \sim \mathrm{N}(0,1)$, je jeho varianční matice jednotkovou maticí, tj. $\mathrm{var}\,Z = \mathbb{I}_n$.



Často ale potkáváme v praktických problémech náhodné vektory, které z takového vektoru $Z$ vznikají obecnou afinní transformací $U = a + BZ$, kde $a$ je libovolný konstantní vektor v $\mathbb{R}^m$ a $B$ je konstantní matice typu $(m, n)$.

Jak jsme odvodili ve větách 9.32 a 9.38, takové náhodné vektory mají střední hodnotu $\mathrm{E}\,U = a$ a varianční matici $\mathrm{var}\,U = V = BB^T$ (protože varianční matice $Z$ je identická). Je tedy tato varianční matice vždy pozitivně semidefinitní.

Říkáme, že náhodný vektor $U$ má *mnohoměrné normální rozdělení* $\mathrm{N}_m(a, V)$.

Pro libovolné mnohoměrné normální rozdělení $\mathrm{N}_m(a, V)$ můžeme znovu uvážit afinní transformaci

$$W = c + DU$$

**Řešení.** Podle zadání hledáme pravděpodobnost $P(S \leq 0{,}2)$. Využijeme větu 9.49, podle které má při náhodném výběru $n$ výrobků náhodná veličina $\frac{n-1}{\sigma^2}S^2$ rozdělení $\chi^2_{n-1}$. V našem případě $n = 21$ a $\sigma^2 = 0{,}0734$, a proto

$$P(S \leq 0{,}2) = P\left(\frac{20}{0{,}0734}S^2 \leq \frac{20}{0{,}0734}0{,}2^2\right) = \chi^2_{20}\left(\frac{20 \cdot 0{,}2^2}{0{,}0734}\right)$$

Výraz v argumentu distribuční funkce je roven přibližně 10,9 a z tabulek pro $\chi^2$ rozložení zjistíme $\chi^2_{20}(10{,}9) \approx 0{,}05$. Pravděpodobnost , že odběratel dodávku přijme je tedy pouze 5%. To, že tato pravděpodobnost bude malá lze odvodit i bez počítání, platí totiž $\mathrm{E}\,S^2 = \sigma^2 = 0{,}0734 > 0{,}2^2$. Pokud bude odběratel testovat pouze 4 výrobky, pak je zřejmě pravděpodobnost přijetí dodávky dána výrazem $\chi^2_3\left(\frac{3 \cdot 0{,}2^2}{0{,}0734}\right) \approx \chi^2_3(1{,}63)$. Hodnotu distribuční funkce $\chi^2$ v tomto argumentu nelze ve většině statistických tabulek nalézt. Proto ji odhadneme lineární interpolací. Jsou-li například nejbližší body $\chi^2_3(0{,}58) = 0{,}1$ a $\chi^2_3(6{,}25) = 0{,}9$, pak

$$\chi^2_3(1{,}63) \approx (1{,}63 - 0{,}58)\frac{0{,}9 - 0{,}1}{6{,}25 - 0{,}58} + 0{,}1 \approx 0{,}24.$$

Tento výsledek je sice jen odhad, ale určitě bude pravděpodobnost přijetí dodávky v případě testování 4 výrobků výrazně vyšší než v předchozím případě. □

**9.77.** Ze základního souboru, z rozdělení $N(\mu, \sigma^2)$, kde $\sigma^2 = 0{,}06$ jsme pořídili náhodný výběr s realizacemi 1,3; 1,8; 1,4; 1,2; 0,9; 1,5; 1,7. Určete oboustranný 95% interval spolehlivosti pro neznámou střední hodnotu.

**Řešení.** Ze zadání se jedná o náhodný výběr rozsahu $n = 7$ z normálního rozložení se známým rozptylem $\sigma^2 = 0{,}06$. Výběrový průměr je

$$\bar{X} = \frac{1}{7}(1{,}3 + 1{,}8 + 1{,}4 + 1{,}2 + 0{,}9 + 1{,}5 + 1{,}7) = 1{,}4$$

a z tabulek pro danou hladinu spolehlivosti $\alpha = 0{,}05$ zjistíme $z(1 - \alpha/2) = z(0{,}975) \approx 1{,}96$. Dosazením do (‖9.3‖) pak ihned dostaneme hledaný interval (1,22, 1,58). □

**9.78.** Nechť $X_1, \ldots, X_n$ je náhodný výběr z rozdělení $N(\mu, 0{,}04)$. Určete nejmenší počet měření, který je třeba provést, aby šířka 95% intervalu spolehlivosti pro $\mu$ nepřesáhla 0,16.

**Řešení.** Protože se jedná o normální rozložení se známým rozptylem, je šířka $(1 - \alpha)$% intervalu spolehlivosti je podle (‖9.3‖) rovna $\frac{2\sigma}{\sqrt{n}}z(1 - \alpha/2)$. Dosazením hodnot ze zadání tedy dostaneme pro počet měření $n$ nerovnici

$$\frac{2 \cdot 0{,}2}{\sqrt{n}}z(0{,}975) \leq 0{,}16.$$

s vektorem konstant $c \in \mathbb{R}^k$ a libovolnou konstantní maticí typu $(k, m)$. Přímým výpočtem vidíme, že

$$W = c + D(a + BZ) = (c + Da) + (DB)Z,$$

což je samozřejmě náhodný vektor $W \sim \mathrm{N}_k(c + Da, DB^T BD^T)$. Chová se tedy kovarianční matice mnohoměrného normálního rozdělení při afinních transformacích jako kvadratická forma.

Tato přímočará úvaha ukazuje, že jakákoliv lineární kombinace komponent složek náhodného vektoru s mnohoměrným normálním rozdělením je náhodná veličina s normálním rozdělením. Stejně je každý vektor vzniklý výběrem jen některých komponent vektoru $U$ opět náhodným vektorem s mnohoměrným normálním rozdělením.

Poznamenejme závěrem, že když pro transformaci náhodného vektoru $Z \sim \mathrm{N}_n(0, \mathbb{I}_n)$ použijeme ortogonální transformaci s maticí $Q^T$, pak můžeme přímo spočíst sdruženou distribuční funkci náhodného vektoru $U = Q^T Z$. Skutečně, jestliže transformaci budeme v souřadnicích psát jako $t = Q^T z$, pak její inverze je $z = Qt$ a Jakobián této transformace je roven jedné. Proto (všimněme si že také jistě platí $\sum_i z_i^2 = \sum_i t_i^2$)

$$\begin{aligned}
F_U(u) &= P(U_i < u_i, i = 1, \ldots, n) = \\
&= \int \cdots \int_{z;\, Q^T z < u} (2\pi)^{-n/2}\, \mathrm{e}^{-\sum z_i^2/2}\, dz_1 \cdots dz_n = \\
&= \int \cdots \int_{t;\, t < u} (2\pi)^{-n/2}\, \mathrm{e}^{-\sum t_i^2/2}\, dt_1 \cdots dt_n = \\
&= \left(\int_{-\infty}^{u_1} (2\pi)^{-1/2}\, \mathrm{e}^{-t_1^2}\, dt_1\right) \cdots \\
&\quad \cdots \left(\int_{-\infty}^{u_n} (2\pi)^{-1/2}\, \mathrm{e}^{-t_n^2}\, dt_1\right) = \\
&= F_{U_1}(u_1) \cdots F_{U_n}(u_n)
\end{aligned}$$

Odtud okamžitě plyne, že všechny komponenty náhodného vektoru $U$ jsou opět nezávislé a opět je $U \sim \mathrm{N}_n(0, \mathbb{I}_n)$.

### 3. Matematická statistika



Jakkoli je zpracování dat v matematické statistice založené na velmi sofistikované matematice, skutečné aplikace již matematiku jako vědu dalece přesahují a vždy jsou založeny také na vstupech z těch oborů, pro které má být použití podstatné.

I proto se omezíme v této učebnici jen na skromné poznámky o statistických metodách a postupech a odkazujeme zájemce na volbu speciální literatury (odrážející i zamýšlené oblasti aplikace).

**9.47. Přípravné úvahy.** V popisné statistice jsme se na začátku kapitoly snažili datové soubory opatřit charakteristikami, které nám o nich vypovídaly podstatné údaje typu výběrového průměru, rozptylu apod.

Matematická statistika pracuje s nějakým výběrem z daného základního souboru a snaží se postihnout, do jaké míry jsou zjištěné statistiky relevantní, případně se ze zjištěných dat pokouší zjistit nebo upřesnit vhodný teoretický model pro chování celého souboru (a z něj pak třeba odhadovat pravděpodobnost nějakého budoucího jevu).

Protože $z(0{,}975) \approx 1{,}96$, dostáváme odtud $n \geq 24{,}01$. Je tedy třeba provést aspoň 25 pokusů. □

**9.79.** Náhodná veličina $X$ má normální rozdělení $N(\mu, \sigma^2)$, kde $\mu, \sigma^2$ nejsou známy. V následující tabulce jsou uvedeny četnosti jednotlivých realizací této náhodné veličiny.

| $X_i$ | 8 | 11 | 12 | 14 | 15 | 16 | 17 | 18 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|
| $n_i$ | 1 | 2 | 3 | 4 | 7 | 5 | 4 | 3 | 2 | 1 |

Vypočtěte výběrový průměr, výběrový rozptyl, výběrovou směrodatnou odchylku a určete 99% interval spolehlivosti pro střední hodnotu $\mu$.

**Řešení.** Výběrový průměr je dán výrazem $\bar{X} = \sum n_i X_i / \sum n_i$. Dosazením hodnot ze zadání máme $\bar{X} = 490/32 \approx 15{,}3$. Výběrový rozptyl je z definice $S = \sum n_i (X_i - \bar{X})^2 / (\sum n_i - 1)$. Po dosazení daných hodnot dostaneme $S^2 = 1943/256 \approx 7{,}6$, a proto výběrová směrodatná odchylka splňuje $S \approx 2{,}8$. Vzorec pro oboustranný $(1-\alpha)$% interval spolehlivosti pro střední hodnotu $\mu$ při neznámém rozptylu jsme odvodili na konci části 9.50

$$\mu \in \left( \bar{X} - \frac{S}{\sqrt{n}} t_{n-1}(1-\alpha/2),\, \bar{X} + \frac{S}{\sqrt{n}} t_{n-1}(1-\alpha/2) \right).$$

Přímým dosazením $\bar{X} = 15{,}3$, $n = 32$, $S \approx 2{,}8$, $\alpha = 0{,}01$ a z tabulek $t_{31}(0{,}995) \approx 2{,}75$ pak zjistíme, že 99% interval spolehlivosti je $\mu \in (14{,}0, 16{,}7)$. □

**9.80.** Pomocí přiložené tabulky distribuční funkce standardního normálního rozdělení určete pravděpodobnost, že při 3600 hodech mincí bude rozdíl mezi počtem padlých hlav a orlů větší než 90.



Uvažme jednoduchý příklad, kdy si sami zhotovíme dřevěnou minci s rubem a lícem. Hodíme jí $n$-krát a víme, že přitom padlo $k \leq n$ líců. Chceme z tohoto experimentu vyvodit závěr, s jakou pravděpodobností v dalších dvou hodech padne vždy líc.

K této úloze můžeme mít dva základní přístupy. Jedním je tzv. klasická statistika (neboli *frekvenční statistika*). Vyjdeme z předpokladu, že jednotlivé hody jsou nezávislé a ve všech je stejná pravděpodobnost líce dána objektivně existujícím parametrem $\theta = p$ (který jen dosud neznáme). Jednotlivé hody tedy považujeme za realizaci náhodné veličiny $X$ s alternativním rozdělením pravděpodobnosti. Pravděpodobnost, že padlo $k$ líců z $n$ pokusů je dána binomiálním rozdělením a lze očekávat že „nejlepší možný“ odhad parametru $p$ bude dán poměrem $\theta = k/n$. Obvyklým cílem je pak opatřit takový odhad vyjádřením o jeho spolehlivosti, který můžeme odvinout od znalosti celkového počtu pokusů $n$ a znalosti asymptotického chování modelu při rostoucím $n$. Jestliže tedy např. padne 8 líců z 10 pokusů, budeme s jistou (matematicky odhadnutou) spolehlivostí tvrdit, že pravděpodobnost dvou následujících líců bude $0{,}8^2 = 0{,}64$, tj. výrazně více než polovina.

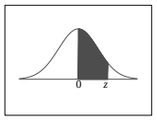
Druhou možností je postupovat víceméně naopak. Můžeme totiž považovat parametr $\theta$ za náhodnou proměnnou, data získaná experimentem za konstanty a pokoušet se z nich vydedukovat informace o rozložení pravděpodobnosti této náhodné veličiny $\theta$. Vycházíme přitom z nějakých vstupních informací o tomto rozložení. Jestliže tedy např. budeme předpokládat, že mince vznikla z homogenního materiálu vcelku přesným soustružením a následným rozlišením lícu a rubu barevným nátěrem, můžeme jako vstupní předpoklad o $\theta$ použít rovnoměrné rozdělení pravděpodobnosti rozložené na malinkém intervalu odpovídajím přesnosti soustruhu. Pak ovšem lze očekávat, že stejný experiment také povede k vychýlení odhadu pravděpodobnosti dvou následujících líců od hodnoty $0{,}5^2 = 0{,}25$ pro dokonalou minci, půjde ale patrně o poněkud menší pravděpodobnost než v předchozím postupu. Hovoříme tu o tzv. *bayesovské statistice*.

První přístup vychází z ryze matematické abstrakce, že pravděpodobnosti jsou dány četnostmi výskytů jevů v tak velkých vzorcích dat, že je můžeme dobře aproximovat nekonečnými modely a využít pro odhady spolehlivosti centrální limitní věty. Statistik zde na pravděpodobnost pohlíží jako na idealizaci relativní četnosti případů, v nichž se vyskytne určitý výsledek při opakovaných pokusech. Tato zdánlivá výhoda/rigorózност se může ale rychle stát nevýhodou, jakmile se začneme zabývat spolehlivostí samotných dat a vhodností zvoleného experimentu. Stejně tak je obtížné frekvenční statistiku dobře použít pro odhad pravděpodobnosti výskytu jednorázového děje.

Bayesovská statistika je naopak příkladem matematizace „selského rozumu“, když chceme naše původní přesvědčení postupně pozměňovat ve světle nových dat.

Je zajímavé, že historicky byl zjevně první bayesovský přístup (např. Laplace a další již v 18. století), který byl prakticky zcela vystřídán frekvenční statistikou ve 20. století. V posledních desetiletích se však ale bayesovská statistika vrátila, společně s dalšími novými přístupy, do popředí zájmu.

Standard Normal Distribution Table




| z | .00 | .01 | .02 | .03 | .04 | .05 | .06 | .07 | .08 | .09 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0.0 | .0000 | .0040 | .0080 | .0120 | .0160 | .0199 | .0239 | .0279 | .0319 | .0359 |
| 0.1 | .0398 | .0438 | .0478 | .0517 | .0557 | .0596 | .0636 | .0675 | .0714 | .0753 |
| 0.2 | .0793 | .0832 | .0871 | .0910 | .0948 | .0987 | .1026 | .1064 | .1103 | .1141 |
| 0.3 | .1179 | .1217 | .1255 | .1293 | .1331 | .1368 | .1406 | .1443 | .1480 | .1517 |
| 0.4 | .1554 | .1591 | .1628 | .1664 | .1700 | .1736 | .1772 | .1808 | .1844 | .1879 |
| 0.5 | .1915 | .1950 | .1985 | .2019 | .2054 | .2088 | .2123 | .2157 | .2190 | .2224 |
| 0.6 | .2257 | .2291 | .2324 | .2357 | .2389 | .2422 | .2454 | .2486 | .2517 | .2549 |
| 0.7 | .2580 | .2611 | .2642 | .2673 | .2704 | .2734 | .2764 | .2794 | .2823 | .2852 |
| 0.8 | .2881 | .2910 | .2939 | .2967 | .2995 | .3023 | .3051 | .3078 | .3106 | .3133 |
| 0.9 | .3159 | .3186 | .3212 | .3238 | .3264 | .3289 | .3315 | .3340 | .3365 | .3389 |
| 1.0 | .3413 | .3438 | .3461 | .3485 | .3508 | .3531 | .3554 | .3577 | .3599 | .3621 |
| 1.1 | .3643 | .3665 | .3686 | .3708 | .3729 | .3749 | .3770 | .3790 | .3810 | .3830 |
| 1.2 | .3849 | .3869 | .3888 | .3907 | .3925 | .3944 | .3962 | .3980 | .3997 | .4015 |
| 1.3 | .4032 | .4049 | .4066 | .4082 | .4099 | .4115 | .4131 | .4147 | .4162 | .4177 |
| 1.4 | .4192 | .4207 | .4222 | .4236 | .4251 | .4265 | .4279 | .4292 | .4306 | .4319 |
| 1.5 | .4332 | .4345 | .4357 | .4370 | .4382 | .4394 | .4406 | .4418 | .4429 | .4441 |
| 1.6 | .4452 | .4463 | .4474 | .4484 | .4495 | .4505 | .4515 | .4525 | .4535 | .4545 |
| 1.7 | .4554 | .4564 | .4573 | .4582 | .4591 | .4599 | .4608 | .4616 | .4625 | .4633 |
| 1.8 | .4641 | .4649 | .4656 | .4664 | .4671 | .4678 | .4686 | .4693 | .4699 | .4706 |
| 1.9 | .4713 | .4719 | .4726 | .4732 | .4738 | .4744 | .4750 | .4756 | .4761 | .4767 |
| 2.0 | .4772 | .4778 | .4783 | .4788 | .4793 | .4798 | .4803 | .4808 | .4812 | .4817 |
| 2.1 | .4821 | .4826 | .4830 | .4834 | .4838 | .4842 | .4846 | .4850 | .4854 | .4857 |
| 2.2 | .4861 | .4864 | .4868 | .4871 | .4875 | .4878 | .4881 | .4884 | .4887 | .4890 |
| 2.3 | .4893 | .4896 | .4898 | .4901 | .4904 | .4906 | .4909 | .4911 | .4913 | .4916 |
| 2.4 | .4918 | .4920 | .4922 | .4925 | .4927 | .4929 | .4931 | .4932 | .4934 | .4936 |
| 2.5 | .4938 | .4940 | .4941 | .4943 | .4945 | .4946 | .4948 | .4949 | .4951 | .4952 |
| 2.6 | .4953 | .4955 | .4956 | .4957 | .4959 | .4960 | .4961 | .4962 | .4963 | .4964 |
| 2.7 | .4965 | .4966 | .4967 | .4968 | .4969 | .4970 | .4971 | .4972 | .4973 | .4974 |
| 2.8 | .4974 | .4975 | .4976 | .4977 | .4977 | .4978 | .4979 | .4979 | .4980 | .4981 |
| 2.9 | .4981 | .4982 | .4982 | .4983 | .4984 | .4984 | .4985 | .4985 | .4986 | .4986 |
| 3.0 | .4987 | .4987 | .4987 | .4988 | .4988 | .4989 | .4989 | .4989 | .4990 | .4990 |
| 3.1 | .4990 | .4991 | .4991 | .4991 | .4992 | .4992 | .4992 | .4992 | .4993 | .4993 |
| 3.2 | .4993 | .4993 | .4994 | .4994 | .4994 | .4994 | .4994 | .4995 | .4995 | .4995 |
| 3.3 | .4995 | .4995 | .4995 | .4996 | .4996 | .4996 | .4996 | .4996 | .4996 | .4997 |
| 3.4 | .4997 | .4997 | .4997 | .4997 | .4997 | .4997 | .4997 | .4997 | .4997 | .4998 |
| 3.5 | .4998 | .4998 | .4998 | .4998 | .4998 | .4998 | .4998 | .4998 | .4998 | .4998 |

Gilles Cazelais. Typeset with LaTeX on April 20, 2006.

**Řešení.** Označíme-li jako $X$ náhodnou veličinu udávající počet padlých hlav, tak $X$ má binomické rozložení pravděpodobnosti $Bi(3600, 1/2)$ (se střední hodnotou 1800 a směrodatnou odchylkou 30) a tudíž lze distribuční funkci veličiny $\frac{X-1800}{30}$ lze pro dané velké $n = 3600$ podle Moivreovy-Laplaceovy věty velmi dobře odhadnout jako distribuční funkci $\Phi$ standardního normálního rozdělení. Hledaná pravděpodobnost je tedy

$$P = 1 - P[1755 \le X \le 1845] =$$
$$= 1 - P\left[-1,5 \le \frac{X-1800}{30} \le 1,5\right] = 2\Phi(-1{,}5) \doteq 0{,}1336,$$

kde poslední hodnotu jsme zjistili z přiložené tabulky. □

**9.81.** Pravděpodobnost narození chlapce je 0,515. Jaká je pravděpodobnost, že mezi deseti tisíci novorozenci bude stejně nebo více děvčat než chlapců.

**Řešení.**

$$P[X < 5000] = P[\underbrace{\frac{X-5150}{\sqrt{5150 \cdot 0{,}485}}}_{\sim N(0,1)} < \underbrace{\frac{-150}{\sqrt{5150 \cdot 0{,}485}}}_{-3{,}001\ldots}] \doteq$$
$$\doteq 0{,}00135$$

□

**9.48. Náhodný výběr z populace.** Budeme se nejprve zabývat



prvním přístupem z předchozího odstavce. Předpokládejme tedy, že máme k dispozici (velký) základní statistický soubor s $N$ jednotkami, který nazýváme *populace*, a zároveň nějaký číselný znak pro každou z jednotek, tj. soubor hodnot $(x_1, \ldots, x_N)$. Z něj ovšem máme k dispozici pouze *výběrový soubor* s hodnotami $(X_1, \ldots, X_n)$.

Abychom se vyhnuli diskusi skutečné velikosti základního statistického souboru s $N$ jednotkami, budeme předpokládat, že vybíráme položky výběrového souboru jednu po druhé a každou vybranou jednotku poté do populace vracíme. Zároveň předpokládáme, že každá položka má stejnou pravděpodobnost výběru $1/N$. Hovoříme pak o *náhodném výběru*.

Způsob realizace náhodného výběru nyní interpretujeme tak, že pracujeme s vektorem $(X_1, \ldots, X_n)$ nezávislých náhodných veličin a že všechny tyto veličiny mají stejné rozdělení pravděpodobnosti. Zejména tedy budou sdílet distribuční funkci $F_X(x)$ a momenty

$$\mathrm{E}\, X_i = \mu, \quad \mathrm{var}\, X_i = \sigma^2.$$

Dalším naším krokem musí být odvození charakteristik výběrového průměru $\bar{X}$ a *výběrového rozptylu*

$$S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - \bar{X})^2,$$

přičemž následující věta dává hned zdůvodnění, proč volíme koeficient $\frac{1}{n-1}$ místo $\frac{1}{n}$, jak tomu bylo u $s^2$ v odstavci 9.6.

**Věta.** *Pro výběrový průměr $\bar{X}$ spočítaný z náhodného výběru rozsahu $n$ z rozdělení s konečnou střední hodnotou $\mu$ a konečným rozptylem $\sigma^2$ platí*

$$\mathrm{E}\, \bar{X} = \mu, \quad \mathrm{var}\, \bar{X} = \frac{1}{n}\sigma^2.$$

*Pro výběrový rozptyl $S^2$ platí*

$$\mathrm{E}\, S^2 = \sigma^2.$$

Důkaz. Jak jsme odvodili v odstavci 9.32, je

$$\mathrm{E}\, \bar{X} = \frac{1}{n}\mathrm{E}\sum_{i=1}^{n} X_i = \frac{1}{n} n\mu = \mu.$$

Díky nezávislosti veličin $X_i$ můžeme použít aditivnost rozptylu odvozenou v odstavci 9.36 a viděli jsme také, že vůči násobení skalárem se rozptyl chová jako kvadratická forma. Dostáváme proto

$$\mathrm{var}\, \bar{X} = \frac{1}{n^2}\,\mathrm{var}\sum_{i=1}^{n} X_i = \frac{1}{n^2} n\sigma^2 = \frac{1}{n}\sigma^2.$$

Přímým roznásobením se ověří vztah

$$\sum_{i=1}^{n}(X_i - \mu)^2 = \sum_{i=1}^{n}(X_i - \bar{X})^2 + n(\bar{X} - \mu)^2.$$

**9.82.** Pomocí distribuční funkce standardního normálního rozdělení určete pravděpodobnost, že při 18000 hodech šestibokou kostkou padne alespoň 3100 šestek.

**Řešení.** Obdobně, jako v předchozích příkladech. $X$ má binomické rozdělení pravděpodobnosti $Bi(18000, 1/6)$. Určíme střední hodnotu $((1/6)(18000) = 3000)$, směrodatnou odchylku $\sqrt{((1/6)(1-1/6)18000)} = 50$, tedy veličinu $\frac{X-3000}{50}$ lze odhadnout jako distribuční funkci $\Phi$ standardního normálního rozložení:

$$P[X \geq 3100] = P\left[\frac{X-3000}{50} \geq \frac{3100-3000}{50}\right] = \\ = P\left[\frac{X-3000}{50} \geq 2\right] \doteq 1 - \Phi(2) \doteq 0{,}0228.$$

□

**9.83.** Agentura pro výzkum veřejného mínění pořádá průzkum volebních preferencí pěti vybraných politických stran. Kolik náhodně vybraných respondentů se musí výzkumu zúčastnit, aby byly s pravděpodobností 0,95 výsledky průzkumu byly u všech zkoumaných stran v rozmezí ±2% od skutečných preferencí?

**Řešení.** Nechť $p_i, i = 1 \ldots 5$ je skutečná relativní četnost příznivců $i$-té politické strany v populaci a nechť náhodná veličina $X_i$ udává počet příznivců této strany mezi náhodně zvolenými $n$ voliči. Budeme považovat za nezávislé jevy, že do daného intervalu padne $X_i/n$. Pokud zvolíme $n$ takové, že pro všechna $i$ padne $X_i/n$ do daného intervalu s pravděpodobností alespoň $\sqrt[5]{0{,}95} \doteq 0{,}99$, bude požadavek zadání splněn. Hledejme tedy $n$ takové, že $P[|\frac{X}{n} - p| < 0{,}02] \geq 0{,}99$. Nejprve upravme vyjádření hledané pravděpodobnosti:

$$\begin{aligned} & P\left[\left|\frac{X}{n} - p\right| < 0{,}02\right] \\ &= P\left[-0{,}02 < \frac{X}{n} - p < 0{,}02\right] = \\ &= P\left[-0{,}02 \cdot n < X - pn < 0{,}02 \cdot n\right] = \\ &= P\left[\frac{-0{,}02 \cdot n}{\sqrt{np(1-p)}} < \frac{X-pn}{\sqrt{np(1-p)}} < \frac{0{,}02 \cdot n}{\sqrt{np(1-p)}}\right] = \\ &= \Phi\left(\frac{0{,}02 \cdot n}{\sqrt{np(1-p)}}\right) - \Phi\left(-\frac{0{,}02 \cdot n}{\sqrt{np(1-p)}}\right) = \\ &= 2\Phi\left(\frac{0{,}02 \cdot n}{\sqrt{np(1-p)}}\right) - 1, \end{aligned}$$

Můžeme tedy spočíst:

$$\mathrm{E}\, s^2 = \frac{1}{n}\mathrm{E}\sum_{i=1}^{n}(X_i - \mu)^2 - \frac{n}{n}(\bar{X} - \mu)^2 = \\ = \frac{1}{n}\sum_{i=1}^{n}\operatorname{var} X_j - \operatorname{var}\bar{X} = \\ = \left(1 - \frac{1}{n}\right)\sigma^2.$$

Proto upravujeme rozptyl $s^2$ vynásobením koeficientem $\frac{n}{n-1}$ a dostáváme právě výběrový rozptyl $S^2$ a jeho střední hodnotu $\sigma$. Tato poslední úprava samozřejmě nemá smysl pro $n = 1$. □

**9.49. Náhodný výběr z normálního rozdělení.** V praktických úlohách je třeba znát nejen číselné charakteristiky výběrového průměru a rozptylu, ale jejich úplné rozdělení pravděpodobnosti. To můžeme samozřejmě odvodit, pouze známe-li konkrétní rozdělení pravděpodobnosti $X_i$. Jako užitečnou ilustraci si spočtěme výsledek pro náhodný výběr z normálního rozdělení.



Již jsme ověřili jako příklad na vlastnosti momentových vytvořujících funkcí v 9.40, že součet náhodných veličin s normálními rozděleními je opět normální rozdělení. Odtud je zřejmé, že i výběrový průměr musí mít normální rozdělení a protože již známe jeho střední hodnotu a rozptyl, bude $\bar{X} \sim \mathrm{N}(\mu, \frac{1}{n}\sigma^2)$.

O něco složitější je to s odvozením rozdělení pravděpodobnosti výběrového rozptylu. Tady si pomůžeme úvahami o mnohoměrných normálních rozděleních z odstavce 9.40. Uvažme vektor $Z$ normovaných normálních veličin

$$Z_i = \frac{X_i - \mu}{\sigma}.$$

Stejnou vlastnost má i vektor $U = Q^T Z$ s jakoukoliv ortogonální maticí $Q$. Vždy přitom také platí $\sum_i U_i^2 = \sum_i X_i^2$. Zvolíme si takovou matici $Q$, aby první komponenta $U_1$ byla, až na násobek, rovna výběrovému průměru $\bar{Z}$. Tzn. zvolíme si první sloupec matice $Q$ ve tvaru $(\sqrt{n})^{-1}(1, \ldots, 1)$. Pak tedy $U_1^2 = n\bar{Z}^2$ a můžeme počítat:

$$\sum_{i=1}^{n} U_i^2 = \sum_{i=1}^{n} Z_i^2 = \sum_{i=1}^{n}(Z_i - \bar{Z})^2 + n\bar{Z}^2$$

$$\sum_{i=2}^{n} U_i^2 = \sum_{i=1}^{n}(Z_i - \bar{Z})^2 = \frac{1}{\sigma^2}\sum_{i=1}^{n}(X_i - \bar{X})^2.$$

Je tedy násobek výběrového rozptylu $\frac{n-1}{\sigma^2}S^2$ součtem $n-1$ kvadrátů normalizovaných normálních veličin a dokázali jsme následující tvrzení:

**Věta.** *Je-li $(X_1, \ldots, X_n)$ náhodný výběr z rozdělení $\mathrm{N}(\mu, \sigma^2)$, pak jsou $\bar{X}$ a $S^2$ nezávislé veličiny a platí*

$$\bar{X} \sim \mathrm{N}(\mu, \frac{1}{n}\sigma^2), \quad \frac{n-1}{\sigma^2}S^2 \sim \chi^2_{n-1}.$$

Okamžitým důsledkem je, že normalizovaný výběrový průměr

$$T = \sqrt{n}\frac{\bar{X} - \mu}{S}$$

má studentovo t-rozdělení pravděpodobnosti s $n-1$ stupni volnosti.

kde $\Phi$ je distribuční funkce normálního rozdělení. Řešme tedy nerovnici:

$$\begin{aligned} 2\Phi\left(\frac{0{,}02\cdot n}{\sqrt{np(1-p)}}\right)-1 &\geq 0{,}99 \\ \Phi\left(\frac{0{,}02\cdot n}{\sqrt{np(1-p)}}\right) &\geq 0{,}995 \end{aligned}$$

Protože distribuční funkce je rostoucí je poslední podmínka ekvivalentní

$$\begin{aligned} \frac{0{,}02\cdot n}{\sqrt{np(1-p)}} &\geq \Phi^{-1}(0{,}995) \\ \frac{0{,}02\cdot n}{\sqrt{np(1-p)}} &\geq 2{,}576 \\ \sqrt{n} &\geq 50\cdot 2{,}576\cdot \underbrace{\sqrt{p(1-p)}}_{\leq \frac{1}{2}} \Longrightarrow \\ \Longrightarrow n &\geq (25\cdot 2{,}276)^2\cdot 4147 \end{aligned}$$

Při tom jsme použili faktu, že funkce $p(1-p)$ nabývá svého maxima pro $p=\frac{1}{2}$ a tímto maximem je $\frac{1}{4}$. Vidíme, že pokud např. $p \doteq 0{,}1$, pak je $\sqrt{p(1-p)}=0{,}3$ a hodnota minimálního $n$ je menší. To odpovídá očekávání: k odhadu méně populárních stran, stačí méně respondentů (pokud agentura odhadne zisk takové strany jako 2% bez toho, aniž by se někoho ptala, tak má požadovanou přesnost téměř jistě zaručenu).

□

**9.84. Dvouvýběrový test.** Uvažme dva náhodné vektory $Y_1$ a $Y_2$, jejichž všechny složky jsou po dvou nezávislé náhodné veličiny s normálním rozdělením, a předpokládejme, že složky vektoru $Y_i$ mají stejnou střední hodnotu $\mu_i$, zatímco rozptyl $\sigma$ je stejný pro všechny komponenty.

Použijte obecný lineární model pro testování hypotézy, zda $\mu_1 = \mu_2$.

**Řešení.** Budeme postupovat velmi podobně jako v odstavci 9.57 vedlejšího sloupce. Tentokrát můžeme zapsat oba vektory $Y_i$ do jednoho sloupce pod sebe a budeme uvažovat model

$$\begin{pmatrix} Y_{11} \\ \vdots \\ Y_{1n_1} \\ Y_{21} \\ \vdots \\ Y_{2n_2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \vdots & \vdots \\ 1 & 0 \\ 1 & 1 \\ \vdots & \vdots \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} + \sigma Z.$$

**9.50. Bodové a intervalové odhady.** Nyní máme vše připravené pro odhady hodnot parametrů v kontextu frekvenční statistiky. Budeme si postup ilustrovat na konkrétním jednoduchém příkladu. Řekněme, že máme v kurzu s 500 studenty výsledky jejich spokojenosti z ankety z minulého semestru ve formě bodů 1-10. Předpokládejme, že spokojenost jednotlivých studentů $X_i$ je aproximována náhodnou veličinou s rozdělením $\mathrm{N}(\mu,\sigma^2)$, přičemž zjištěné hodnoty z celé populace minulého semestru jsou $\mu=6$, $\sigma=2$.



V běžícím semestru je provedeno namátkové šetření u 15 studentů, protože panuje obava, že nový vyučující má ještě výrazně horší ohlasy. Výsledkem je hodnocení, kde se vyskytují dvě 3, tři 4, tři 5, pět 6 a dvě 7. Výběrový průměr je tedy $\bar{X}=5{,}133$, výběrový rozptyl $S^2=1{,}695$.

Díky našim předpokladům víme, že $\bar{X}\sim \mathrm{N}(\mu,\sigma^2/n)$ a tedy $Z=\sqrt{n}\frac{\bar{X}-\mu}{\sigma}\sim \mathrm{N}(0,1)$. Pro vyjádření spolehlivosti našeho odhadu tedy můžeme počítat interval, který bude odhadovaný parametr obsahovat s předem zvolenou pravděpodobností $100(1-\alpha)\%$. Hovoříme přitom o hladině spolehlivosti $0<\alpha<1$. Nejprve považujme za neznámý nový parametr $\mu$, zatímco o rozptylu budeme (ať už oprávněně nebo ne) předpokládat, že zůstal stejný. Dostaneme okamžitě

$$\begin{aligned} 1-\alpha = P(|Z|<z(\alpha/2)) &= P\left(\left|\sqrt{n}\frac{\bar{X}-\mu}{\sigma}\right|<z(\alpha/2)\right) \\ &= P\left(\bar{X}-\frac{\sigma}{\sqrt{n}}z(\alpha/2)<\mu<\bar{X}+\frac{\sigma}{\sqrt{n}}z(\alpha/2)\right) \end{aligned}$$

a našli jsme interval, jehož hranice jsou náhodné veličiny a který s předem zadanou pravděpodobností bude obsahovat odhadovaný parametr $\mu$. Střed tohoto intervalu nazýváme *bodovým odhadem* pro parametr $\mu$, celý interval pak *intervalovým odhadem*. Výsledek pak můžeme interpretovat i tak, že na hladině spolehlivosti $\alpha$ odhadovaný parametr $\mu$ je nebo není odlišný od jiné hodnoty $\mu_0$.

V případě našich dat vyjdou např. pro hodnoty $\alpha=0{,}05$ a $\alpha=0{,}1$ intervaly

$$\mu\in(4{,}121,\ 6{,}145),\quad \mu\in(4{,}284,\ 5{,}983).$$

Na hladině spolehlivosti 5% tedy nemůžeme potvrdit, že se názor studentů na výuku nového učitele oproti minulému zhoršil, protože uvedený interval obsahuje i hodnotu $\mu_0=6$. Na úrovni 10% už takový úsudek uděláme, protože dřívější hodnota z minulého semestru $\mu_0=6$ už do našeho intervalu nepadne.

Pokud bychom ale předpokládali, že u jiného (horšího) učitele bude patrně i rozptyl odpovědí jiný (třeba se studenti více shodnou na špatném hodnocení), museli bychom postupovat trochu odlišně. Místo normalizované veličiny $Z$ výše budeme stejně postupovat s veličinou

$$T=\sqrt{n}\frac{\bar{X}-\mu}{S}.$$

Jak jsme viděli, má tato náhodná veličina rozdělení pravděpodobnosti $T\sim \mathrm{t}_{n-1}$, kde v našem případě je $n=15$. Vyjde tak intervalový odhad

$$\bar{X}-\frac{S}{\sqrt{n}}t_{n-1}(\alpha/2)<\mu<\bar{X}+\frac{S}{\sqrt{n}}t_{n-1}(\alpha/2)$$

a po dosazení našich dat na úrovních $\alpha=0{,}05$ a $\alpha=0{,}03$ máme

$$\mu\in\big(4{,}412,\ 5{,}854\big),\quad \mu\in\big(4{,}321,\ 5{,}945\big),$$

Budeme pracovat s aritmetickými průměry jednotlivých vektorů $\bar{Y}_1$ a $\bar{Y}_2$. Přímá aplikace obecného vzorce z teorie dává odhad $b$ ve tvaru

$$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} n_1+n_2 & n_2 \\ n_2 & n_2 \end{pmatrix}^{-1} \begin{pmatrix} n_1\bar{Y}_1 + n_2\bar{Y}_2 \\ n_2\bar{Y}_2 \end{pmatrix} =$$
$$= \frac{1}{n_1 n_2} \begin{pmatrix} n_2 & -n_2 \\ -n_2 & n_1+n_2 \end{pmatrix} \begin{pmatrix} n_1\bar{Y}_1 + n_2\bar{Y}_2 \\ n_2\bar{Y}_2 \end{pmatrix} = \begin{pmatrix} \bar{Y}_1 \\ \bar{Y}_2 - \bar{Y}_1 \end{pmatrix}$$

a matice $C = (X^T X)^{-1}$, kde $X$ je dvousloupcová matice s nulami a jedničkami z našeho modelu, vychází

$$C = \begin{pmatrix} \frac{1}{n_1} & -\frac{1}{n_1} \\ -\frac{1}{n_1} & \frac{1}{n_1} + \frac{1}{n_2} \end{pmatrix}.$$

Testujeme tedy hypotézu $\mu_1 = \mu_2$, to znamená, že testujeme, zda je $\beta_2 = 0$. K tomu je proto vhodné použít statistiku

$$T = \frac{\bar{Y}_2 - \bar{Y}_1}{S} \left( \frac{n_1 n_2}{n_1 + n_2} \right)^{\frac{1}{2}},$$

kde za směrodatnou odchylku $S$ dosazujeme

$$S^2 = \frac{1}{n_1 + n_2 - 2} \left( \sum_{i=1}^{n_1} (Y_{1i} - \bar{Y}_1)^2 + \sum_{i=1}^{n_2} (Y_{2i} - \bar{Y}_2)^2 \right).$$

Tato statistika má rozdělení $\mathrm{t}_{n_1+n_2-2}$ a nulovou hypotézu $\mu_1 = \mu_2$ proto zamítáme na hladině $\alpha$, když platí

$$|T| \geq \mathrm{t}_{n_1+n_2-2}(\alpha). \qquad \square$$

**9.85.** V JZD[1] Tempo sledovali v pěti různých dnech dojivost krav a naměřili postupně tyto výsledky: 15, 14, 13, 16 a 17 hektolitrů. V JZD Boj, ve kterém mají stejný počet krav, měřili přibližně ve stejnou dobu, nicméně v sedmi různých dnech: 12, 16, 13, 15, 13, 11, 18 hektolitrů.

a) Určete 95% interval spolehlivosti pro dojivost krav v JZD Boj, a 95% interval spolehlivosti pro dojivost krav v JZD Tempo.

b) Na pětiprocentní hladině otestujte hypotézu, že v obou družstvech mají stejně kvalitní krávy.

Předpokládejte, že dojivost krav v jednotlivých dnech se řídí normálním rozdělením. Oba výpočty proveďte jak za předpokladu, že v družstvech mají k dispozici údaje z předchozích dlouhodobých měření, ve kterých byla směrodatná odchylka $\sigma = 2\ hl$ mléka, tak v případě, že údaje z předchozích měření nejsou k dispozici.

**Řešení.** Nejprve spočítejme výsledky za předpokladu známého rozptylu. K určení intervalu spolehlivosti použijeme statistiku

$$U = \frac{\overline{X} - \mu}{\sigma/\sqrt{n}},$$

takže už na úrovni 3% spolehlivosti máme za to, že je názor na učitele skutečně horší. To odpovídá intuici, že nejspíš by výrazně menší výběrová směrodatná odchylka $S = 1,302$ než odchylka $\sigma = 2$ z minulého šetření také měla být podstatná pro naše úvahy.

**9.51. Věrohodnost odhadů.** Matematicky jsou intervalové a bodové odhady jednoduché a patrně dobře pochopitelné. Daleko horší je to s interpretací praktickou. Jednak je problematické ověřit všechny předpoklady o náhodnosti výběru, ale hlavně ve složitějších případech budeme mít problém s „věrohodností odhadů".



Jako matematici se praktickému problému nejlépe vyhneme tak, že podáme definici chybějícího pojmu. Obecně chceme pracovat s náhodným výběrem o rozsahu $n$. Implicitně stále předpokládáme, že jde o nezávislé náhodné veličiny $X_i$ se shodným rozdělením pravděpodobnosti, které ale závisí na neznámém, obecně vektorovém, parametru $\theta$.

Snažíme se najít nějakou *výběrovou statistiku* $T$, tj. funkci náhodných veličin $X_1, X_2, \ldots$, která v nějakém (matematickém) smyslu bude dobře odhadovat skutečnou hodnotu parametru $\theta$. Říkáme, že je $T$ *nestranným odhadem* parametru $\theta$, jestliže je $\mathrm{E}\,T = \theta$. Střední hodnota $\mathrm{E}(T - \theta)$ se nazývá *vychýlení odhadu* $T$.

Často nás zajímá také asymptotické chování odhadu, tj. jak se chová při limitním přechodu $n \to \infty$. Říkáme, že je $T = T(n)$ *konzistentním odhadem* parametru $\theta$, jestliže konverguje $T(n)$ v pravděpodobnosti k $\theta$, tj. pro každé $\varepsilon > 0$

$$\lim_{n\to\infty} P(|T(n) - \theta| < \varepsilon) = 1.$$

Čebyševova nerovnost nám okamžitě dává

$$P(|T(n) - \mathrm{E}\,T_n| < \varepsilon) \geq 1 - \frac{\operatorname{var} T(n)}{\varepsilon^2}.$$

Pokud předpokládáme, že $\lim_{n\to\infty} \mathrm{E}\,T(n) = \theta$, pak zároveň pro dostatečně velká $n$ platí

$$P(|T(n) - \theta| < 2\varepsilon) \geq P(|T(n) - \mathrm{E}\,T(n)| < \varepsilon) \geq 1 - \frac{\operatorname{var} T(n)}{\varepsilon^2}.$$

Dokázali jsme užitečné tvrzení:

**Věta.** *Předpokládejme, že platí* $\lim_{n\to\infty} \mathrm{E}\,T(n) = \theta$ *a zároveň předpokládejme* $\lim_{n\to\infty} \operatorname{var} T(n) = 0$. *Pak je* $T(n)$ *konzistentním odhadem pro* $\theta$.

Jednoduchým příkladem pro použití této věty je rozptyl

$$\hat{\sigma}^2 = \frac{1}{n} \sum_{i=1}^{n} (X_i - \bar{X})^2 = \frac{n-1}{n} S^2.$$

Protože nestranným odhadem je podle věty z odstavce 9.48 $S^2$, víme, že $\hat{\sigma}^2$ nestranný odhad není. Zřejmě však platí $\lim_{n\to\infty} \hat{\sigma}^2 = \sigma^2$ a lze přímo spočíst také

$$\lim_{n\to\infty} \operatorname{var} \hat{\sigma}^2 = \lim_{n\to\infty} \operatorname{var} S^2 = \lim_{n\to\infty} \frac{2\sigma}{n-1} = 0.$$

Je tedy statistika $s^2$ konzistentním odhadem rozptylu.

[1] JZD — jednotné zemědělské družstvo — zemědělské družstvo vzniklé násilnou kolektivizací v padestátých letech dvacátého století.

která má standardizované normální rozdělení pravděpodobnosti (viz 9.26). Interval spolehlivosti pak je (viz 9.50)

$$\left(\bar{X} - \frac{\sigma}{\sqrt{n}} z(\alpha/2),\, \bar{X} + \frac{\sigma}{\sqrt{n}} z(\alpha/2)\right),$$

kde $\alpha = 0,05$. Nyní pouze dosadíme číselné hodnoty. Pro údaje z JZD Tempo tak dostáváme výběrový průměr

$$\overline{X}_1 = \frac{15 + 14 + 13 + 16 + 17}{5} = 15,$$

z tabulek či matematického softwaru zjistíme, že $z(0{,}025) = 1{,}96$ a dostáváme interval

$$\left(15 - \frac{2}{\sqrt{5}} 1{,}96,\, 15 + \frac{2}{\sqrt{5}} 1{,}96\right) \doteq (13{,}25;\, 16{,}75).$$

Pro JZD Boj pak dostáváme

$$\overline{X}_2 = \frac{12 + 16 + 13 + 15 + 13 + 11 + 18}{7} = 14,$$

a 95% interval spolehlivosti pro hodnotu dojivosti krav v JZD Boj tak je

$$(12{,}52;\, 15{,}48).$$

Pokud je rozptyl měření neznámý, použijeme k jeho odhadu tzv. výběrový rozptyl a k určení intervalu spolehlivosti pak statistiku

$$T = \frac{\overline{X} - \mu}{S\sqrt{n}},$$

která má Studentovo rozložení pravděpodobnosti s $n-1$ stupni volnosti (viz též 9.50). Potom analogicky obdržíme 95% interval spolehlivosti

$$\left(\bar{X} - \frac{S}{\sqrt{n}} t_{n-1}(\alpha/2),\, \bar{X} + \frac{S}{\sqrt{n}} t_{n-1}(\alpha/2)\right).$$

Pro konkrétní hodnoty pak dostáváme pro JZD Tempo výběrový rozptyl

$$S_1^2 = \frac{0^2 + (-1)^2 + (-2)^2 + 1^2 + 2^2)}{4} = 2{,}5,$$

tedy $S \doteq 1{,}58$. Dále je $t_4(0,025) \doteq 2,78$. 95% interval spolehlivosti hodnot dojivosti krav v JZD Tempo tedy je

$$(13{,}03;\, 16{,}97).$$

Pro JZD Boj pak dostáváme výběrový rozptyl $S_2^2 = 6$ a hledaný interval spolehlivosti je pak

$$(11{,}73;\, 16{,}27).$$

b) Jestliže srovnáváme střední hodnoty dojivosti v obou družstvech, jedná se o porovnání středních hodnot dvou nezávislých výběrů z normálních rozložení. V případě neznámých rozptylů měření navíc předpokládejme, že rozptyl měření je v obou družstvech stejný.



Je vcelku zřejmé, že pro stejný parametr můžeme mít k dispozici spoustu nestranných odhadů. Např. jsme viděli, že aritmetický průměr $\bar{X}$ je nestranným odhadem střední hodnoty $\theta$ rozdělení veličin $X_i$. Samozřejmě je ale třeba hodnota $X_1$ také nestranným odhadem $\theta$. Chceme proto najít nejlepší odhad $T$ ve třídě uvažovaných statistik, které jsou nestrannými nebo konsistentními odhady. Zpravidla máme za to, že nejlepším odhadem je ten, který má ze všech uvažovaných nejmenší možný rozptyl. Připomeňme, že rozptyl vektorové statistiky $T$ je dán kovarianční maticí, která bude, v případě nezávislých komponent, diagonální maticí s jednotlivými rozptyly komponent na diagonále. Nerovnostem mezi pozitivně definitními maticemi jsme již dříve dali jednoznačný smysl.

**9.52. Maximální věrohodnost.** Předpokládejme tedy, že náš výběr má komponenty s rozdělením, jehož hustota je dána funkcí $f(x, \theta)$ závislou na neznámém (obecně vektorovém) parametru $\theta$. Sdružená hustota vektoru $(X_1, \ldots, X_n)$ je díky předpokládané nezávislosti dána součinem funkcí

$$f(x_1, \ldots, x_n, \theta) = f(x_1, \theta) \cdots f(x_n, \theta),$$

které říkáme *věrohodnostní funkce*.

Zajímáme se o takovou hodnotu $\hat{\theta}$, která maximalizuje na množině všech dostupných hodnot parametru věrohodnostní funkci. V diskrétním případě to znamená, že vybíráme takový parametr, při kterém vychází největší pravděpodobnost zjištěného výběru.

Zpravidla ale pracujeme s tzv. *logaritmickou věrohodnostní funkcí*

$$\ell(x_1, \ldots, x_n, \theta) = \ln f(x_1, \ldots, x_n, \theta) = \sum_{i=1}^{n} \ln f(x_i, \theta),$$

protože díky monotonnímu chování funkce ln je maximalizace věrohodnostní funkce ekvivalentní požadavku maximalizace logaritmické věrohodnostní funkce. Pokud je pro nějaké hodnoty $f(x_1, \ldots, x_n) = 0$, klademe $\ell(x_1, \ldots, x_n, \theta) = -\infty$.

V případě diskrétních náhodných veličin použijeme stejnou definici s pravděpodobnostní funkcí místo hustoty, tj.

$$\ell(x_1, \ldots, x_n, \theta) = \sum_{i=1}^{n} \ln(P(X_i = x_i|\theta)).$$

Princip je dobře vidět na náhodném výběru z normálního rozdělení $\mathrm{N}(\mu, \sigma^2)$ o rozsahu $n$. Neznámé parametry jsou $\mu$ nebo $\sigma$, nebo oba. Uvažovaná hustota je

$$f(x, \mu, \sigma) = \frac{1}{2\pi\sigma^2}\, \mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

a tedy logaritmováním okamžitě vidíme

$$\ell(x, \mu, \sigma) = -n\frac{1}{2}\ln(2\pi\sigma^2) - \frac{1}{2\sigma^2}\sum_{i=1}^{n}(x_i - \mu)^2.$$

Vyšetřeme tedy hypotézu za předpokladů známých, uvedených rozptylů $\sigma_1^2 = \sigma_2^2 = 4$. Použijeme statistiku

$$\begin{aligned} U &= \frac{(\overline{X}_1 - \overline{X}_2) - (\mu_1 - \mu_2)}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}} = \\ &= \frac{\overline{X}_1 - \overline{X}_2}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}} \sim N(0,1), \end{aligned}$$

kde $\mu_1$ a $\mu_2$ jsou neznámé střední hodnoty dojivosti ve zkoumaných družstvech a $n_1$, $n_2$ jsou počty měření. Tato statistika má, jak naznačeno, standardizované normální rozdělení. Hypotézu na 5% hladině zamítneme, právě když absolutní hodnota statistiky $U$ bude větší než $z_{0{,}025}$, neboli právě když 0 nebude ležet v 95% intervalu spolehlivosti pro rozdíl středních hodnot dojivosti v jednotlivých družstvech. Po dosazení číselných hodnot dostáváme

$$U = \frac{15 - 14}{\sqrt{\frac{4}{5} + \frac{4}{7}}} \doteq 0{,}854.$$

Je tedy $|U| < z(0{,}025) = 1{,}96$ a hypotézu o rovnosti středních hodnot dojivosti v obou družstvech na 5% hladině nezamítáme. Dosažená $p$-hodnota testu (viz 9.55) je 39, 4%, tudíž jsme se k zamítnutí hypotézy moc nepřiblížili (pravděpodobnost, že hodnota zkoumané statistiky bude menší než 0,854 je při platnosti nulové hypotézy 60, 6%).

Pokud neznáme rozptyly měření, ale víme, že v obou družstvech musí být stejné, použijeme statistiku

$$\begin{aligned} K &= \frac{(\overline{X}_1 - \overline{X}_2) - (\mu_1 - \mu_2)}{S_* \sqrt{\frac{1}{n_1} + \frac{1}{n_2}}} = \\ &= \frac{\overline{X}_1 - \overline{X}_2}{S_* \sqrt{\frac{1}{n_1} + \frac{1}{n_2}}} \sim t_{n_1+n_2-2}, \end{aligned}$$

kde

$$S_* = \frac{(n_1 - 1)S_1^2 + (n_2 - 1)S_2^2}{n_1 + n_2 - 2}.$$

Po dosazení číselných hodnot dostáváme $K \doteq 0{,}796$, $|K| < t_{10}(0, 025) = 2{,}2281$, nulovou hypotézu tedy opět nezamítáme. Dosažená $p$-hodnota testu je 44,6%, tedy ještě větší než v testu předešlém. □

**9.86. Analýza rozptylu jednoduchého třídění.** Pro $k \geq 2$ nezávislých výběrů $Y_i$ o rozsahu $n_i$ z normálních rozdělení se stejným rozptylem použijte lineární model na testování hypotézy, že všechny střední hodnoty jednotlivých výběrů jsou shodné.

Maximum najdeme pomocí derivací (všimněme si, že $\sigma^2$ chápeme při derivování jako symbol pro proměnnou):

$$\begin{aligned} \frac{\partial \ell}{\partial \mu} &= -\frac{1}{2\sigma^2} \sum_{i=1}^{n} (-2)(x_i - \mu) = \frac{1}{\sigma^2}\Big(-n\mu + \sum_{i=1}^{n} x_i\Big) \\ \frac{\partial \ell}{\partial \sigma^2} &= -\frac{n}{2\sigma^2} + \frac{1}{\sigma^4} \sum_{i=1}^{n} (x_i - \mu)^2 = \\ &= \frac{1}{2\sigma^4}\Big(-n\sigma^2 + \sum_{i=1}^{n} (x_i - \mu)^2\Big). \end{aligned}$$

Vidíme tedy, že jediné kritické body jsou dány právě volbou $\hat{\mu} = \bar{X}$ a $\hat{\sigma}^2 = s^2$. Dosazením těchto hodnot do matice druhých derivací dostaneme Hessián funkce $\ell$

$$\begin{pmatrix} -\frac{n}{\hat{\sigma}^2} & 0 \\ 0 & -\frac{n}{2(\hat{\sigma}^2)^2} \end{pmatrix}.$$

Je tedy vidět že jde skutečně o dosažené maximum a protože je jediné, musí jít o globální maximum. Ověřili jsme tedy, že střední a hodnota a rozptyl jsou skutečně maximálně věrohodné odhady pro $\mu$ a $\sigma$, tak jak jsme je používali výše.

**9.53. Bayesovské odhady.** Vraťme se teď k příkladu z odstavce 9.50 z pohledu Bayesovské statistiky. Úplně tedy otáčíme náš přístup a zjištěná data $X_1, \ldots, X_{15}$, tj. body vyjadřující spokojenost dotázaných studentů na škále $1, \ldots, 10$ bodů, budeme chápat jako konstanty. Naopak, odhadovaný parametr $\mu$, tj. střední hodnota bodů vyjadřujících spokojenost, bude náhodnou veličinou, jejíž rozložení chceme odhadnout.



Za tímto účelem zkusme interpretovat Bayesův vzorec pro podmíněnou pravděpodobnost na úrovni pravděpodobnostních funkcí, resp. hustot pravděpodobností, následujícím způsobem. Má-li vektor $(X, \Theta)$ sdruženou hustotu $f(x, \theta)$, pak podmíněná pravděpodobnost komponenty $\Theta$ za podmínky $X = x$ je dána hustotou

$$g(\theta|x) = \frac{f(x|\theta)g(\theta)}{f(x)},$$

kde $f(x)$ a $g(\theta)$ jsou marginální hustoty pravděpodobností.

Jestliže tedy máme dánu *apriorní* hustotu rozložení pravděpodobnosti $g(\theta)$ odhadovaného parametru $\theta$ a známe také hustotu pravděpodobnosti $f(x|\theta)$, můžeme ze vztahu spočíst *aposteriorní* hustotu pravděpodobnosti $g(\theta|x)$ vycházející právě ze zjištěných dat. Protože data $X$ jsou přitom konstantní, nepotřebujeme ve skutečnosti vůbec počítat s hodnotou $f(x)$ a při úvahách budeme pracovat jen „až na konstantní násobek“. Ten je totiž stejně určen na konci úvah jednoznačně požadavkem, aby vyšla dobře definovaná hustota rozdělení pravděpodobnosti $g(\theta|x)$. Budeme pro tento účel používat zápis $Q \propto R$, jestliže existuje konstanta $C$ taková, že pro výrazy $Q$ a $R$ platí $Q = CR$.

Abychom byli technicky co nejblíže k úvahám v odstavci 9.50, budeme pracovat s normálními rozděleními $\mathrm{N}(\mu, \sigma^2)$. Předpokládejme, že na univerzitě je spokojenost studentů v jednotlivých předmětech náhodná veličina $X \sim \mathrm{N}(\theta, \sigma^2)$, zatímco parametr $\theta$ dosahovaný jednotlivými učiteli je náhodná veličina $\theta \sim \mathrm{N}(a, b)$.

**Řešení.** Postup je zde velice podobný minulému příkladu, platnost testované hypotézy je ale ekvivalentní tvrzení, že platí podmodel, ve kterém mají všechny složky náhodného vektoru $Y$ vzniklého sloučením daných $k$ vektorů $Y_i$ stejnou střední hodnotu.

Použitý model tedy bude mít tvar

$$\begin{pmatrix} Y_{11} \\ \vdots \\ Y_{1n_1} \\ Y_{21} \\ \vdots \\ Y_{k1} \\ \vdots \\ Y_{kn_k} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_k \end{pmatrix} + \sigma Z.$$

Snadno spočteme odhady středních hodnot $\mu_i$ pomocí aritmetických průměrů

$$\bar{Y}_i = \frac{1}{n_i} \sum_{j=1}^{n_i} Y_{ij}.$$

Odtud dostaneme odhad $\hat{Y}_{ij} = \bar{Y}_i$ a proto dostaneme reziduální součet čtverců ve tvaru

$$RSS = \sum_{i=1}^{k} \sum_{j=1}^{n_i} (Y_{ij} - \bar{Y}_i)^2.$$

Odhadem společné střední hodnoty v uvažovaném podmodelu je

$$\bar{Y} = \frac{1}{n} \sum_{i=1}^{k} \sum_{j=1}^{n_i} Y_{ij} = \frac{1}{n} \sum_{i=1}^{k} n_i \bar{Y}_i,$$

kde $n = n_1 + \cdots + n_k$, a reziduální součet čtverců v tomto podmodelu je

$$RSS^0 = \sum_{i=1}^{k} \sum_{j=1}^{n_i} (Y_{ij} - \bar{Y})^2.$$

V původním modelu máme $k$ nezávislých parametrů $\mu_i$, zatímco v podmodelu zůstal jediný parametr $\mu$, testovaná statistika má proto tvar

$$F = \frac{(n-k)}{(k-1)} \frac{(RSS^0 - RSS)}{RSS}.$$

□

## J. Lineární regrese

S lineární regresí jsme se už setkali ve třetí kapitole, v odstavci ‖3.46‖. Nyní se stejný princip budeme snažit využít k vyřešení problémů, které bývají studovány statistiky.

Standardním příkladem užití lineární regrese je „proložení přímky“ danými daty. Máme tedy posloupnost měření, ve kterých zaznamenáváme hodnoty dvou veličin u nichž předpokládáme lineární závislost. Klasickým příkladem je závislost výšky syna na výšce otce.

Můžeme tedy počítat (pořád až na konstantní násobky, tj. ignorujeme součinitele, ve kterých nevystupuje ani $x$ ani $\theta$)

$$\begin{aligned} g(\theta|x) &\propto f(x|\theta) g(\theta) \\ &\propto \exp\left( -\frac{(x-\theta)^2}{2\sigma^2} - \frac{(\theta-a)^2}{2b^2} \right) \\ &\propto \exp\left( -\frac{1}{2} \left( \theta^2 \left( \frac{1}{\sigma^2} + \frac{1}{b^2} \right) - 2\theta \left( \frac{x}{\sigma^2} + \frac{a}{b^2} \right) \right) \right) \\ &\propto \exp\left( -\frac{1}{2} \left( \theta - \frac{b^2 x + \sigma^2 a}{\sigma^2 b^2} \frac{\sigma^2 b^2}{b^2 + \sigma^2} \right)^2 \left( \frac{b^2 \sigma^2}{b^2 + \sigma^2} \right)^{-1} \right). \end{aligned}$$

Tím jsme ale už ukázali, že hledané rozložení pro $\theta$ je

$$\theta \sim \mathrm{N}\left( \frac{b^2}{b^2 + \sigma^2} x + \frac{\sigma^2}{b^2 + \sigma^2} a, \frac{b^2 \sigma^2}{b^2 + \sigma^2} \right).$$

Tento výsledek bychom mohli interpretovat např. tak, že když z dlouhodobého vyhodnocování anket známe parametry $a$, $b$, $\sigma$, můžeme po vyjádření nějakého studenta upřesnit apriorní představu o parametrech pro jeden konkrétní předmět. Ve výsledném odhadu rozložení je pak střední hodnota dána váženým průměrem zjištěné hodnoty $x$ a apriorně předpokládané střední hodnoty $a$, v závislosti na rozptylech $\sigma$ a $b$.

**9.54. Interpretace v Bayesovské statistice.** Zkusíme teď porozumět úvahám z předchozího odstavce ve srovnání s frekventistickou interpretací z 9.50. Asi namítneme, že jediný dotaz těžko má tolik ovlivnit náš názor.



Ve skutečnosti ale pro $\sigma \to 0$ je váha jednoho názoru stále rostoucí a v našem výsledku tomu odpovídá 100% váha u $x$ v případě $\sigma = 0$. Je to plně v souladu s interpretací, že Bayesovská statistika je pravděpodobnostní rozšíření standardní diskrétní matematické logiky. Jestliže máme rozptyl $\sigma$ prakticky nulový, pak je tedy v tomto smyslu skoro jisté, že názor kteréhokoliv studenta je naprosto vypovídající o celé populaci.

Ve skutečnosti jsme v odstavci 9.50 pracovali s výběrovým průměrem $\bar{X}$ výsledku šetření. Ten můžeme použít i v předchozím výpočtu, protože jde opět o normální rozdělení, jen budeme místo $\sigma^2$ dosazovat $\sigma^2/n$. Pro zjednodušení zápisu si definujme konstantu

$$c_n = \frac{nb^2}{nb^2 + \sigma^2}$$

a aposteriorní odhad pro $\theta$ na základě zjištěni výběrového průměru $\bar{X}$ má rozložení s parametry

$$\theta \sim \mathrm{N}(c_n \bar{X} + (1 - c_n)a, c_n \sigma^2/n).$$

Jak se dalo očekávat, pro rostoucí $n$ se bude střední hodnota našeho rozdělení pro $\theta$ stále více blížit výběrovému průměru a jeho rozptyl půjde k nule. Čím je tedy $n$ větší, tím více se blížíme bodovému odhadu z frekventistického přístupu.

Přínosem Bayesovského přístupu je, že s použitím odhadnutého rozdělení můžeme odpovídat na dotazy typu „s jakou pravděpodobností je nový vyučující horší než předchozí?“ Použijeme stejná data jako v 9.50 a přidáme potřebné apriorní údaje. Předpokládejme, že máme docela dobře hodnocené učitele (protože by asi jinak na škole nevydrželi), takže uvažujme pro určitost $a = 7{,}5$, $b = 2{,}5$ a a ponecháváme směrodatnou odchylku $\sigma = 2$.

**9.87.** Určete lineární regresní model pro závislost veličiny $Y$ na veličině $X$ na základě naměřených seznamů dat: $X = [1, 4, 5, 7, 10]$, $Y = [3, 7, 8, 12, 18]$.

**Řešení.** K určení parametrů regresní přímky použije vztahů odvozených v 9.57. Podle metody nejmenších čtverců se snažíme se minimalizovat vzdálenost vektoru $b_1X + b_0$ od vektoru $Y$ v závislosti na parametrech $b_1$ a $b_0$. Tato vzdálenost, jak víme například ze druhé kapitoly, je minimální pro kolmý průmět vektoru $Y$ do vektorového podprostoru generovaného vektory $(1, \ldots, 1)$ a $(x_1, \ldots, x_n)$. Pro parametry $b_0, b_1$ regresní přímky $Y = b_1X + b_0$ tak dostáváme

$$b_1 = \frac{\sum_{i=1}^n (x_i - \bar{x})(Y_i - \bar{Y})}{\sum_{i=1}^n (x_i - \bar{x})^2} =$$
$$= \frac{(1-5{,}4)(3-9{,}6) + \cdots + (10-5{,}4)(18-9{,}6)}{((1-5{,}4)^2 + (4-5{,}4)^2 + (5-5{,}4)^2 + (7-5{,}4)^2 + (10-5{,}4)^2} =$$
$$= 1{,}677.$$

Teď již snadno dopočteme i koeficient $b_0$:

$$b_0 = \bar{Y} - b_1\bar{x} = 0{,}5442.$$

Hledaná lineární závislost je tedy

$$Y = 1{,}677 \cdot X + 0{,}5442.$$

Poznamenejme, že v tomto modelu hrají veličiny $X$ a $Y$ naprosto rovnocennou úlohu. Stejnou metodou jsme mohli získat závislost $X$ na $Y$:

$$X = 0{,}5867 \cdot Y - 0{,}2322.$$

□

**Poznámka.** Rozmyslete si, proč lineární regresní model závislosti $X$ na $Y$ nelze získat pouhým vyjádřením $X$ z lineárního regresního modelu závislosti $Y$ na $X$.

**Poznámka.** V řadě reálných situací je závislost veličin jasně dána, například je-li jednou z veličin čas.

**9.88.** Orbitální stanice naměřila v pěti po sobě jdoucích dnech, ve stejnou hodinu následující rychlosti neznámého vesmírného tělesa (v km/s): 10, 11,4, 13,1, 15,8 a 18,7. Odhadněte rychlost tělesa desátého dne.

**Řešení.** Zde je vhodné si všimnout, že rychlost se v čase „od pohledu“ nemění lineárně (nárůsty rychlosti se neustále zvyšují). Lze tedy vyslovit domněnku, že je těleso přitahováno gravitační silou k nějakému jinému tělesu. Potom by jeho rychlost byla kvadratickou funkcí času. Zkusme tedy metodou nejmenších čtverců proložit co nejpřesněji kvadratickou funkci danými daty. Postup je stejný, jako

Měli jsme $n = 15$ a výběrový průměr 5,133. Dosazením dostaneme aposteriorní odhad pro rozdělení

$$\theta \sim \mathrm{N}(5{,}230,\ 0{,}256).$$

Zajímá nás teď $P(\theta < 6)$. Odpověď získáme dotazem na hodnotu distribuční funkce příslušného normálního rozdělení pro argument 6 (umí to i excel). Dostaneme odpověď přibližně 93, 6%. Je tedy podobná, jako jsme viděli v odstavci 9.50 v případě předpokladu o konstantním známém rozptylu.

Všimněme si, jak se tady projevuje apriorní předpoklad o rozložení parametru $\theta$ u všech učitelů, tj. jistá míra naší důvěry, že by měli být učitelé spíše lepší. Kdyby měl statistik důvod předpokládat, že pro konkrétně poptávaného učitele je skutečná střední hodnota $a$ posunutá, řekněme na $a = 6$ stejně jako u ankety minulého učitele (např. protože jde o těžký a neoblíbený předmět), pak bychom dostali pravděpodobnost, že je jeho skutečný parametr menší než 6, přibližně 95,0% (pokud bychom ale za viditelně horší považovali až střední hodnotu menší než 5,5, pak už to bude jen přibližně 75%). V případě dosazení $a = 5$ to již bude 96,8%. Stejně tak hraje roli i rozptyl $b^2$. Např. apriorní odhad $a = 6$, $b = 3{,}5$ vede na pravděpodobnost 95,2%.

Právě jsme se mimoděk dotkli jiného velice podstatného bodu a to *analýzy citlivosti*. Jistě bychom rádi pracovali ve výše uvedeném příkladu s modelem, kde malá změna apriorního předpokladu bude mít jen malý vliv na aposteriorní výsledek. Zdá se, že v našem případě to tak skutečně je, nepůjdeme tu do detailních úvah.

Úplně stejný model s exponenciálními rozděleními se prakticky používá při posouzení relevance výstupu z IQ testu u jedné osoby (nebo jiné obdobné zkoušky, kde lze očekávat dobré přiblížení rozdělení pravděpodobnosti výsledků v populaci pomocí normálního rozdělení), o které máme apriorní předpoklad, do jaké skupiny by měla patřit. Jiným dobrým příkladem (ovšem s jinými rozloženími) mohou být praktické úlohy z pojišťovnictví, kde je účelné odhadovat parametry tak, aby byly zahrnuty jak vlivy experimentu na konkrétní položce, tak celková očekávání přes populaci.

**9.55. Poznámky o testování hypotéz.** Vrátíme se zpět k možnostem rozhodování, zda nějaký jev nastal či nenastal v kontextu frekvenční statistiky. Opřeme se o postup v intervalových odhadech výše.



Uvažujme tedy nějaký náhodný vektor $X = (X_1, \ldots, X_n)$ (vzniklý z náhodného výběru) se sdruženou distribuční funkcí $F_X(x)$. Za *hypotézu* budeme považovat nějaké tvrzení o rozdělení určeném touto distribuční funkcí. Zpravidla přitom formulujeme dvě hypotézy $H_0$ a $H_A$, kde první se tradičně říká *nulová hypotéza* a druhé *alternativní hypotéza*. Výsledkem testu je rozhodnutí založené na konkrétní realizaci náhodného vektoru $X$ (hovoříme také o *testu*), zda hypotézu $H_0$ zamítnout nebo nezamítnout ve prospěch hypotézy $H_A$.

Vznikají nám přitom možné chyby dvou typů. *Chyba prvního druhu* nastává, když zamítneme $H_0$, přestože je platná. *Chyba druhého druhu* nastane, když naopak nezamítneme $H_0$, ačkoliv platná není. Rozhodování frekventistického statistika probíhá tak, že si vybere tzv. *kritický obor* $W$, tj. množinu výsledků realizace testu, při kterých hypotézu zamítá. Velikost kritického oboru přitom volí tak, aby platnou hypotézu zamítal s pravděpodobností nejvýše $\alpha$. To znamená, že požadujeme předem dané ohraničení pravděpodobnosti chyby prvního druhu tzv. *hladinou testu* $\alpha$. Často se volí

kdybychom prováděli lineární regresi vektoru $v = (v_1, v_2, \ldots, v_n)$ závislého na vektoru $x = (x_1, \ldots, x_n)$ a vektoru $x^2 = (x_1^2, \ldots, x_n^2)$. Této metodě se říká *kvadratická regrese*. Hledáme tedy vektor parametrů $b = (b_0,\ b_1,\ b_2)$ tak aby veličina $b_2x^2 + b_1x + b_0$ odhadovala $y$. Sestavme tedy matici $X$ hodnot nezávislých proměnných:

$$X = \begin{pmatrix} 1 & x_1 & x_1^2 \\ \vdots & \vdots & \vdots \\ 1 & x_n & x_n^2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \\ 1 & 4 & 25 \end{pmatrix},$$

a vektor parametrů $b = (b_0, b_1, b_2)$ dopočítáme podle (9.18):

$$b = (X^T X)^{-1} X^T v \doteq (9{,}26;\ 0{,}47;\ 0{,}29).$$

Hledaný kvadratický odhad je potom

$$v = 0{,}29x^2 + 0{,}47x + 9{,}26,$$

Odhadovaná rychlost desátého dne je tedy přibližně 42,96 km/s. V modelu klasické lineární regrese bychom dostali přiblížení

$$v = 2{,}18x + 7{,}26,$$

což by pro rychlost desátého dne dávalo 29,06 km/s. Rozdíl v odhadech je značný. Ukazuje to, že analýza situace je velmi významnou součástí statistiky. □

### K. Bayesovská analýza dat

**9.89.** Mějme Bernoulliův proces definovaný náhodnou veličinou $X \sim \mathrm{Bi}(n, \theta)$ s binomickým rozdělením pravděpodobnosti a předpokládejme, že parametr $\theta$ je přitom náhodnou veličinou s rovnoměrným rozdělením pravděpodobnosti na intervalu $(0, 1)$. Definujme *šanci na úspěch* v našem procesu jako veličinu $\gamma = \frac{\theta}{1-\theta}$. Jakou hustotu rozdělení má veličina $\gamma$?

**Řešení.** Intuitivně asi cítíme, že nepůjde o rovnoměrné rozdělení.

Označíme hledanou hustotu pravděpodobnosti $f(s)$ a ze vztahu mezi $\theta$ a $\gamma$ spočteme $\theta = \frac{\gamma}{1+\gamma}$. Také okamžitě vidíme, že hustota pravděpodobnosti veličiny $\gamma$ bude nenulová pouze pro kladné hodnoty proměnné. Zadání můžeme nyní zformulovat tak, že požadujeme

$$\Theta = P(\theta < \Theta) = P\Big(\gamma < \frac{\Gamma}{1+\Gamma}\Big) = \int_0^\Gamma f(s)ds, \tag{9.4}$$

kde $\Gamma = \frac{\Theta}{1-\Theta}$. Na pravé straně máme ovšem v horní mezi právě měnící se ohraničení $\gamma$ a dostáváme tedy definiční vztah pro $f(s)$

$$f(s) = \left(\frac{s}{s+1}\right)' = \frac{1}{(s+1)^2}.$$

Hledaná hustota skutečně dává daleko větší pravděpodobnost malým hodnotám šance než velkým. □

hladiny testů $\alpha = 0{,}05$ nebo $\alpha = 0{,}01$. Prakticky užitečný je také postup, kdy určíme nejnižší možnou hladinu $p$ testu, při které ještě hypotézu zamítáme a mluvíme pak o *dosažené hladině testu*, resp. *p–hodnotě testu*.

Zbývá tedy najít rozumný postup, jak volit kritické obory. Jistě to budeme chtít dělat tak, abychom zároveň co nejvíce omezili výskyt chyby druhého druhu. Zpravidla se k tomu čelu hodí věrohodnostní funkce $f(x, \theta)$, kterou jsme přiřadili náhodnému vektoru $X$ již v odstavci 9.52. Pro jednoduchost předpokládejme, že máme jednorozměrný parametr $\theta$ a nulovou hypotézu formulujme tak, že rozdělení $X$ je dáno funkcí $f(x, \theta_0)$, zatímco alternativní hypotéza je dána rozdělením $f(x, \theta_1)$ pro dvě různé konkrétní hodnoty $\theta_0$ a $\theta_1$. Naše představy o zamítání nebo přijímání hypotéz napovídají, že po dosazení hodnot konkrétního pokusu do věrohodnostní funkce budeme chtít hypotézu spíše přijímat, je-li $f(x, \theta_0)$ výrazně větší než $f(x, \theta_1)$.

Nabízí se tedy pro každou konstantu $c > 0$ uvažovat kritický obor

$$W_c = \{x;\ f(x, \theta_1) \geq c f(x, \theta_0)\}.$$

Když si vybereme zamýšlenou hladinu testu, budeme chtít zvolit takové $c$, aby platilo

$$\int_{W_c} f(x, \theta_0) = \alpha.$$

Tím máme zajištěno, že pro výsledek testu $x \in W_c$ při platnosti $H_0$ se skutečně dopustíme maximálně předepsané chyby prvního druhu. To ale můžeme zajistit i jinými kritickými obory $W$ splňujícími také

$$\int_{W} f(x, \theta_0) = \alpha.$$

Zajímá nás ale také pravděpodobnost chyby druhého druhu, zkusíme si tedy odhadnout rozdíl

$$D = \int_{W_c} f(x, \theta_1) - \int_{W} f(x, \theta_1).$$

Oblasti, přes které integrujeme můžeme v obou případech rozdělit na společnou část $W \cap W_c$ a zbývající množinový rozdíl. Příspěvky společné části se přitom odečtou a zbude

$$D = \int_{W_c \setminus W} f(x, \theta_1) - \int_{W \setminus W_c} f(x, \theta_1).$$

Díky naší definici kritického oboru $W_c$ ale nyní můžeme snadno odhadnout (opět přidáváme zpět stejné integrály přes společnou část množin)

$$\begin{aligned} D &\geq c \int_{W_c \setminus W} f(x, \theta_0) - c \int_{W \setminus W_c} f(x, \theta_0) = \\ &= c \int_{W_c} f(x, \theta_0) - c \int_{W} f(x, \theta_0) = c\alpha - c\alpha = 0. \end{aligned}$$

Tím jsme odvodili důležité tvrzení, tzv. *Neymanovo–Pearsonovo lemma*, že za výše uvedených předpokladů je $W_c$ optimální kritický obor, který na předepsané úrovni minimalizuje chybu druhého druhu.



Intervalový odhad, jak jsme jej ilustrovali na příkladu v odstavci 9.50, je speciálním případem testování hypotéz, kdy $H_0$ má formu „střední hodnota spokojenosti studentů zůstala $\mu_0$“, zatímco $H_A$ říká, že bude rovna nějaké jiné hodnotě $\mu_1$. Uvidíme za chvilku, že předchozí obecný

V odstavci 9.53 jsme viděli, že jestliže pracujeme v bayesovském přístupu s binomickým modelem rozdělení pravděpodobnosti náhodné veličiny $X \sim \mathrm{Bi}(n,\theta)$, bude nás zajímat její pravděpodobnostní funkce $f_X(k) = \binom{n}{k}\theta^k(1-\theta)^{n-k}$. Na tuto funkci se ale můžeme také dívat jako na podmíněnou pravděpodobnost $P(\theta|X=k)$ při apriorním rovnoměrném rozdělení pravděpodobnosti veličiny $\theta$ na intervalu $(0,1)$. Je to tedy právě aposteriorní rozdělení pravděpodobnosti veličiny $\theta$ odpovídající výsledku pokusu $X=k$. Následující příklad se týká obecné třídy takovýchto rozdělení pravděpodobnosti.

**9.90.** Najděte základní charakteristiky tzv. *Beta rozdělení* $\beta(a,b)$ s hustotou pravděpodobnosti tvaru

$$f_Y = \begin{cases} C\,y^{a-1}(1-y)^{b-1} & y \in (0,1) \\ 0 & \text{jinak.} \end{cases}$$

**Řešení.** Konstantu $C$ je třeba volit jako reciprokou hodnotu integrálu $\int_0^1 y^{a-1}(1-y)^{b-1}dy$, což je funkce $\mathrm{B}(a,b)$, v matematické analýze (ale také technických vědách či fyzice) známá pod názvem *Beta funkce*. Když už známe funkci Gama, která zobecňuje diskrétní hodnoty faktoriálů, vyskočí na nás např. při následujícím výpočtu:

$$\begin{aligned}
\Gamma(x)\Gamma(y) &= \int_0^\infty \mathrm{e}^{-t}\,t^{x-1}\,dt \cdot \int_0^\infty \mathrm{e}^{-s}\,s^{y-1}\,ds = \\
&= \int_0^\infty \int_0^\infty \mathrm{e}^{-t-s}\,t^{x-1}s^{y-1}\,dt\,ds = \\
&\quad \text{(substituce } t = rq,\ s = r(1-q)\text{)} \\
&= \int_{r=0}^\infty \int_{q=0}^1 \mathrm{e}^{-r}(rq)^{x-1}\big(r(1-q)\big)^{y-1} r\,dq\,dr = \\
&= \int_{r=0}^\infty \mathrm{e}^{-r}\,r^{x+y-1}\,dr \cdot \int_{t=0}^1 q^{x-1}(1-q)^{y-1}dq = \\
&= \Gamma(x+y)\mathrm{B}(x,y).
\end{aligned}$$

dostáváme tedy obecný vztah

$$\mathrm{B}(a,b) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}$$

a z vlastností Gamma funkce již snadno plyne, že pro přirozená kladná $a, b$ bude platit

$$\mathrm{B}(n-k+1,k+1) = \frac{k!(n-k)!}{(n+1)!} = \frac{1}{n+1}\binom{n}{k}^{-1}.$$

Přímým výpočtem vidíme, že střední hodnota veličiny $X \sim \beta(a,b)$ s beta rozdělením je (využíváme vztah $\Gamma(z+1) = z\Gamma(z)$)

$$\mathrm{E}\,X = \frac{\mathrm{B}(a+1,b)}{\mathrm{B}(a,b)} = \frac{a}{a+b}.$$

Je-li $a=b$ vyjde střední hodnota i medián $\frac{1}{2}$.

postup povede v tomto případě na kritický obor zadaný požadavkem

$$|Z| = \left|\frac{\bar X - \mu_0}{\sigma}\sqrt{n}\right| \geq z(\alpha/2).$$

Všimněme si, že v definici kritického oboru není skutečná hodnota $\mu_1$ podstatná a zformalizovali jsme proto v kontextu klasické pravděpodobnosti úlohu rozhodnout na předepsané hladině $\alpha$, zda se střední hodnota $\mu$ změnila.

Jestliže ale chceme testovat z nějakého důvodu pouze, zda spokojenost poklesla, pak musíme předem předpokládat, že $\mu_1 < \mu_0$. Rozeberme si tento případ podrobněji. Kritický obor z Neymanova–Pearsonova lemmatu je určen nerovností

$$\frac{f(x,\mu_1,\sigma^2)}{f(x,\mu_0,\sigma)^2} = \mathrm{e}^{-\frac{1}{2\sigma^2}\sum_{i=1}^n\left((x_i-\mu_1)^2-(x_i-\mu_0)^2\right)} \geq c.$$

Logaritmováním dostaneme, po drobné úpravě,

$$2\bar x(\mu_1-\mu_0) - (\mu_1^2-\mu_0^2) \geq \frac{2\sigma^2}{n}\ln c$$

a protože předpokládáme $\mu_1 < \mu_0$, dostáváme konečně

$$\bar x \leq \frac{\mu_1+\mu_0}{2} + \frac{\sigma^2}{n(\mu_1-\mu_0)}\ln c = y.$$

Konstantu $c$, tj. také rozhodující parametr $y$, přitom pro zvolenou hladinu $\alpha$ máme určenu tak, aby za předpokladu platnosti hypotézy $H_0$ platilo

$$\alpha = P(\bar X \leq y) = P\Big(\frac{\bar X-\mu_0}{\sigma}\sqrt{n} \leq \frac{y-\mu_0}{\sigma}\sqrt{n}\Big).$$

Díky předpokladu o platnosti hypotézy $H_0$ je veličina

$$Z = \frac{\bar X-\mu_0}{\sigma}\sqrt{n} \sim \mathrm{N}(0,1)$$

a proto znamená náš požadavek volbu $Z \leq -z(\alpha)$, která jednoznačně určuje optimální $W_c$.

Všimněme si, že tento kritický obor skutečně nezávisí na volbě hodnoty $\mu_1$ a skutečnou hodnotu pro $y$ jsem vůbec nepotřebovali vyjádřit. Podstatný byl pouze předpoklad $\mu_1 < \mu_0$.

V našem ilustračním příkladu v odstavci 9.50 tedy máme $H_0$ : $\mu = 6$ a alternativní hypotéza je $H_A$ : $\mu < 6$. Rozptyl je $\sigma^2 = 4$. Test s $n = 15$ nám dal $\bar x = 5{,}133$. Dosazením dostaneme hodnotu $z = \frac{5{,}133-6}{4}\sqrt{15} = -1{,}678$ zatímco $-z(0{,}05) = -1{,}645$.



Hypotézu tedy na hladině 5% zamítáme a usuzujeme, že skutečně došlo ke zhoršení názoru studentů.

Když si za kritický obor zvolíme sjednocení oborů pro případy $\mu_1 < \mu_0$ a $\mu_1 > \mu_0$, dostaneme právě výsledek shodný s intervalovým odhadem, jak bylo zmíněno výše.

Poznamenejme závěrem, že v bayesovském přístupu je také možné přijímat nebo zamítat hypotézy víceméně v přímé vazbě na aposteriorní pravděpodobnosti jevů, jak jsme do jisté míry naznačili v odstavci 9.54 při interpretaci našeho konkrétního příkladu.

**9.56. Lineární modely.** Jako obvykle v analýze matematických problémů buď vystačíme s afinními závislostmi nebo skutečné vztahy jejich pomocí aproximujeme. Stejně tak ve statistice patří mnoho metod do tzv. lineárních modelů. Probereme si stručně jeden případ z frekvenční statistiky.



Přímo se také spočte rozptyl

$$\operatorname{var} X = \mathrm{E}(X - \mathrm{E}\,X)^2 = \frac{ab}{(a+b)^2(a+b+1)}.$$

Pro $a = b$ tedy dostáváme $\operatorname{var} X = \frac{1}{8a+4}$, což ukazuje, že pro rostoucí $a = b$ klesá rozptyl. V případě $a = b = 1$ dostáváme obyčejné rovnoměrné rozdělení na intervalu $(0, 1)$. □

**9.91.** V situaci stejné jako v předposledním příkladu předpokládejme, že v Bernoulliho procesu je šance zdaru $\theta$ náhodná veličina s rozdělením pravděpodobnosti $\beta(a, b)$. Jak bude vypadat rozdělení pravděpodobnosti veličiny $\gamma = \frac{\theta}{1-\theta}$? V čem bude zvláštní při $a = b = p$?

**Řešení.** V již řešeném příkladě jsme měli speciální případ s rovnoměrným rozdělením $\beta(1, 1)$. Můžeme tedy pokračovat v řešení v rovnosti $\|\|9.4\|\|$, kdy jsme tvar tohoto rozdělení použili. Dostáváme nyní na levé straně místo $\Theta$ výraz

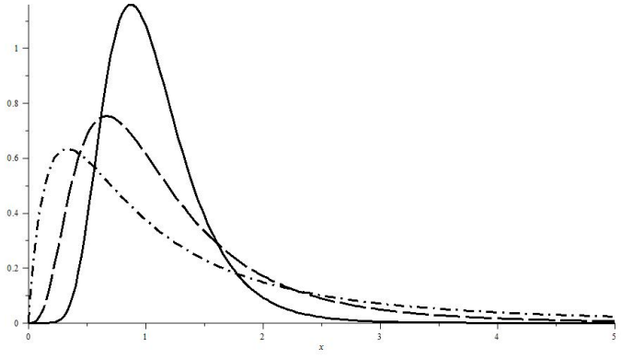
$$\frac{1}{\mathrm{B}(a, b)} \int_0^{\Theta} t^{a-1}(1-t)^{b-1} dt$$

a při derivování musíme použít pravidlo pro derivování integrálu s proměnnou horní mezí. Dostáváme proto pro hledanou hustotu

$$\mathrm{B}(a, b) f(s) = \left(\frac{s}{s+1}\right)^{a-1} \left(1 - \frac{s}{s+1}\right)^{b-1} \frac{1}{(s+1)^2} =$$

$$= \left(\frac{s^{a-1}}{s+1}\right)^{a+b}.$$

Na obrázku jsou vyneseny hustoty pro hodnoty $a = b = p = 2, 5, 15$.




Vidíme, že se naplňuje představa, že stejné a nepříliš malé hodnoty $a = b = p$ odpovídají nejvíce pravděpodobné hodnotě $\theta = \frac{1}{2}$, proto je hustota šance největší v okolí jedničky. Čím větší $p$, tím menší je rozptyl této veličiny. □

Budeme uvažovat náhodný vektor $Y = (Y_1, \ldots, Y_n)^T$ a budeme předpokládat, že platí

$$Y = X \cdot \beta + \sigma Z,$$

kde $X = (x_{ij})$ je konstantní matice reálných čísel s $n$ řádky a $k < n$ sloupci a hodností $k$, $\beta$ je neznámý konstantní vektor $k$ parametrů modelu, $Z$ je náhodný vektor, jehož $n$ komponent má rozdělení $\mathrm{N}(0, 1)$, a $\sigma > 0$ je neznámý kladný parametr modelu. Hovoříme o *lineárním modelu* s úplnou hodností.

V praktických problémech jde často o to, že známe veličiny $x_{ij}$ a snažíme se odhadnout nebo predikovat hodnotu $Y$. Například $x_{ij}$ může vyjadřovat hodnocení $i$–tého studenta v $j$–tém semestru ($j = 1, 2, 3$) z matematiky a chceme vědět, jak tento student asi dopadne ve čtvrtém semestru. K tomu potřebujeme znát vektor $\beta$. Ten odhadneme na základě úplných pozorování, tj. ze znalosti $Y$ (např. z výsledků v předchozích letech).

K odhadu vektoru $\beta$ se často používá *metoda nejmenších čtverců*. To znamená, že chceme najít odhad $b \in \mathbb{R}^k$ tak, aby vektor $\hat{Y} = Xb$ minimalizoval druhou mocninu délky vektoru $Y - X\beta$.

To je ale jednoduchá úloha lineární algebry a víme, že jde o nalezení kolmého průmětu vektoru $Y$ do podprostoru $\langle X\rangle \subset \mathbb{R}^n$ generovaném sloupci matice $X$. Minimalizujeme přitom funkci

$$\|Y - X\beta\|^2 = \sum_{i=1}^{n} \Big(Y_i - \sum_{j=1}^{k} x_{ij}\beta_j\Big)^2.$$

Zvolme libovolnou ortonormální bázi vektorového podprostoru $\langle X\rangle$ a napišme ji do sloupců matice $P$. Pro jakoukoliv takovou volbu báze bude kolmý průmět realizován pomocí násobení maticí $PP^T$. Zobrazení dané touto maticí je přitom na podprostoru $\langle X\rangle$ identické, tj. dostáváme

$$\hat{Y} = PP^TY = PP^T(X\beta + \sigma Z) = X\beta + \sigma PP^TZ.$$

Matice $PP^T$ je pozitivně semidefinitní. Nyní doplníme bázi ze sloupců v $P$ na ortonormální bázi celého $\mathbb{R}^n$, tj. vytvoříme matici $Q = (P\ R)$ vepsáním nově přidaných vektorů báze do matice $R$ s $n - k$ sloupci a $n$ řádky. Označme si dále $V = P^TZ$ a $U = R^TZ$ náhodné vektory s $k$ a $n - k$ komponentami. Budou na sebe vzájemně kolmé a jejich součtem v $\mathbb{R}^n$ dostaneme vektor $(V^TU^T)^T = Q^TZ$.

Evidentně tedy (viz odstavec 9.46) mají oba vektory $V$ a $U$ mnohoměrné normální rozdělení s nulovou střední hodnotou a jednotkovou kovarianční maticí. Náhodný vektor $Y$ jsme rozložili na součet konstantního vektoru $X\beta$ a dvou kolmých projekcí

$$Y = X\beta + \sigma PV + \sigma RU$$

a hledaný kolmý průmět je součet prvních dvou sčítanců. V odstavci 9.46 jsme také pro takové náhodné vektory odvodili jejich rozdělení.

Velikost $\|Y - \hat{Y}\|^2$ nazýváme *reziduální součet čtverců*, zpravidla se značí *RSS*. Definujeme také *reziduální rozptyl* jako

$$S^2 = \frac{\|Y - Xb\|^2}{n-k}.$$

Připomeňme, že $\hat{Y} = Xb$ a že, díky našemu předpokladu o maximální hodnosti $X$, je matice $X^TX$ invertibilní. Můžeme proto rovnou spočíst $b = (X^TX)^{-1}X^T\hat{Y}$. Zároveň ale víme, že

**9.92.** Ukažte, že v případě Bernoulliho procesu popsaného náhodnou veličinou $X \sim \mathrm{Bi}(n,\theta)$ a apriorní pravděpodobnosti náhodné veličiny $\theta$ s beta rozdělením, má i aposteriorní pravděpodobnost opět beta rozdělení s vhodnými parametry závislými na výsledku pokusu. Jaká bude aposteriorní střední hodnota veličiny $\theta$ (tj. bayesovský bodový odhad této náhodné veličiny)?

**Řešení.** Jak je zdůvodněno v odstavci 9.53 teoretického sloupce, bude aposteriorní hustota pravděpodobnosti, až na násobek vhodnou konstantou, dána jako součin apriorní hustoty pravděpodobnosti

$$g(\theta) = \frac{1}{\mathrm{B}(a,b)}\theta^{a-1}(1-\theta)^{b-1}$$

a pravděpodobnosti sledované veličiny $X$ za podmínky, že nastala hodnota $\theta$. Dostáváme tedy za předpokladu, že v Bernoulliho procesu nastalo $k$ zdarů, aposteriorní hustotu (použitý znak místo rovnosti značí „proporcionální“)

$$\begin{aligned} g(\theta|X=k) &\propto P(X=k|\theta)g(\theta) \propto \\ &\propto \theta^k(1-\theta)^{n-k}\theta^{a-1}(1-\theta)^{b-1} = \\ &= \theta^{a+k-1}(1-\theta)^{b+n-k-1}. \end{aligned}$$

Dostali jsme tedy, až na konstantu, kterou nemusíme vůbec vyčíslovat, skutečně hustotu aposteriorního rozdělení pro veličinu $\theta$ s rozdělením $\mathrm{B}(a+k, b+n-k)$.

Její aposteriorní střední hodnota je

$$\hat\theta = \frac{a+k}{a+b+n}.$$

Pro $n$ a $k$ jdoucí do nekonečna, tak aby $k/n \to p$, bude i pro náš aposteriorní odhad platit $\hat\theta \to p$. Je tedy vidět, že při velkých hodnotách $n$ a $k$ bude převažovat pozorovaný podíl úspěšných pokusů nad apriorním předpokladem. Nicméně pro menší hodnoty je apriorní předpoklad naopak velice významný. □

**9.93.** Máme data o nehodovosti $N = 20$ řidičů za posledních $n = 10$ let ($k$–tá položka označuje počet roků, ve kterých došlo k nehodě u $k$–tého řidiče):

$$0, 0, 2, 0, 0, 2, 2, 0, 6, 4, 3, 1, 1, 1, 0, 0, 5, 1, 1, 0.$$

Předpokládáme, že pravděpodobnosti nehod u jednotlivých řidičů jsou konstanty $p_j$, $j = 1, \ldots, N$.

Odhadněte pro každého řidiče pravděpodobnost, že bude mít nehodu v následujícím roce (např. pro určení jeho individuálního pojistného). [2]

[2] Tento příklad je převzat z příspěvku M. Friesl, Bayesovské odhady v některých modelech, publikováno v: Analýza dat 2004/II (K. Kupka, ed.), Trilobyte Statistical Software, Pardubice, 2005, pp. 21-33.

$X^T(Y-\hat Y) = \sigma X^T(RU) = 0$, protože jsou sloupce v $X$ a $R$ po dvou ortogonální. Platí proto ve skutečnosti také

$$b = (X^TX)^{-1}X^TY. \tag{9.18}$$

Ještě můžeme lépe využít zvolenou matici $P$. Protože její sloupce generují tentýž podprostor jako sloupce $X$, jistě existuje čtvercová matice $T$ taková, že $X = PT$ (její sloupce jsou koeficienty lineárních kombinací, které vyjadřují sloupce $X$ pomocí báze v $P$). Nyní již jen dosadíme (použijeme přitom, že $P^TP$ je jednotková matice a $T$ je invertibilní):

$$\begin{aligned} b &= (T^TP^TPT)^{-1}T^TP^TY = \\ &= T^{-1}(T^T)^{-1}T^TP^T(PT\beta+\sigma Z) = \\ &= \beta + \sigma T^{-1}V. \end{aligned}$$

Tím jsme z velké části již odvodili vlastnosti lineárního modelu:

**Věta.** *Uvažujme lineární model $Y = X\beta + \sigma Z$.*
*(1) Pro odhad $\hat Y$ platí*

$$\hat Y = X\beta + \sigma PV, \quad \hat Y \sim \mathrm{N}(X\beta, \sigma^2PP^T).$$

*(2) Reziduální součet čtverců RSS a normovaný čtverec velikosti rezidua mají rozdělení:*

$$Y - \hat Y \sim \mathrm{N}(0, \sigma^2RR^T), \quad \|Y-Y\|^2/\sigma^2 \sim \chi^2_{n-k}.$$

*(3) Náhodná veličina $b = \beta + \sigma T^{-1}V$ má rozdělení*

$$b \sim \mathrm{N}(\beta, \sigma^2(X^TX)^{-1}).$$

*(4) Pro reziduální rozptyl platí $(n-k)S^2/\sigma^2 \sim \chi^2_{n-k}$.*
*(5) Střední hodnota reziduálního rozptylu je $\mathrm{E}\,S^2 = \sigma^2$.*
*(6) Veličiny $b$ a $S^2$ jsou nezávislé.*

Důkaz. Tvar i rozdělení $\hat Y$ jsme již odvodili. Odtud je ale již zřejmé, že $Y - \hat Y = \sigma RU$ a tím máme ověřené i druhé tvrzení. Dále máme

$$\|Y-Y\|^2/\sigma^2 = \|RU\|^2 = \|U\|^2,$$

kde poslední rovnost plyne z toho, že v naší konstrukci je $U$ vektor souřadnic průmětu $Z$ do komplementu $\langle X\rangle$ a $RU$ je tímto průmětem. Velikost vektoru je přitom dána právě jako součet kvadrátů souřadnic v libovolné ortonormální bázi.

Je proto náhodný vektor $\|Y-Y\|^2/\sigma^2$ součtem $(n-k)$ kvadrátů náhodných veličin s rozdělením $\mathrm{N}(0,1)$, tedy jde o rozdělení $\chi^2_{n-k}$ a dokázali jsme zbytek (2).

Další tvrzení vyplývá přímo z našich definic a výpočtů, zbývá jen odhadnout varianční matici pro $b$. Z obecných vlastností víme, že má vyjít matice $T^{-1}(T^T)^{-1}$. To je ale stejná matice jako $(X^TX)^{-1} = ((PT)^T(PT))^{-1}$.

Tvrzení z (4) je jen přepsáním informace z (2) a další tvrzení plyne z toho, že střední hodnota rozdělení $\chi^2$ je rovna počtu stupňů volnosti.

Konečně, nezávislost veličin $b$ a $S$ je důsledkem toho že první je funkcí vektoru $V$, zatímco druhá je funkcí vektoru $U$ a tyto vektory jsou nezávislé, protože vznikly jako dvě komplementární části z ortogonální transformace vektoru $Z$. □



V praktických úlohách někdy testujeme hypotézu, zda pro odhadu středních hodnot nestačí méně parametrů. Říkáme, že náhodný vektor $Y$ splňuje *podmodel*, když platí zároveň $Y = X\beta + \sigma Z$ a

**Řešení.** Zavedeme si náhodné veličiny $X_{ij}$ s hodnotami 0, když $i$-tý řidič v $j$-tém roce neměl žádnou nehodu, a hodnotami 1 pokud nehodu měl. Jednotlivé roky považujeme za nezávislé, můžeme proto předpokládat, že náhodné veličiny $S_j = \sum_{i=1}^{n} X_{ji}$ udávající počet nehod za všech $n = 10$ let mají rozdělení $\mathrm{Bi}(n, p_j)$.

Samozřejmě bychom mohli odhadnout pravděpodobnosti pro všechny řidiče společně, tj. pomocí aritmetického průměru

$$\hat{p} = \frac{1}{N}\sum_{j=1}^{n} S_j \frac{1}{n} = \frac{1}{20}\frac{29}{10} = 0{,}145.$$

Když ale uvážíme homogennost rozdělení veličin $X_j$, těžko je lze považovat za shodné, proto bude takovýto odhad jistě zavádějící.

Opačný extrém, tj. zcela nezávislý a individuální odhad

$$\hat{p}_j = \frac{1}{n} S_j$$

je samozřejmě také nevhodný, protože jistě nechceme předepisovat nulové pojistné, dokud nedojde k první nehodě.

Jako realistický se jeví postup, ve kterém využijeme stejný předpoklad apriorního rozdělení pravděpodobnosti $p_j$ nehodovosti u jednotlivých řidičů. V praxi se zpravidla používá model s Poissonovým rozdělením $\mathrm{Po}(\lambda_j)$ u $j$-tého řidiče s dalšími předpoklady o rozdělení parametru $\lambda$ mezi řidiči. Docela dobře (a hlavně jednoduše) můžeme také předpokládat, že v našem případě půjde o rozdělení $p_j \sim \beta(a, b)$ s vhodnými parametry $a, b$, které by měly odrážet kumulované výsledky všech řidičů. Pojďme tedy touto cestou.

Z předchozího příkladu pak víme, že aposteriorní rozdělení pravděpodobností bude $(p_j | S_j = k) = \beta(a + k, b + n - k)$, takže příslušná střední hodnota bude

$$\hat{p}_j^b = \frac{a + k}{a + b + n}.$$

Srovnejme si tento odhad s výše uvedeným společným odhadem $\hat{p}$ a individuálním $\hat{p}_j$. Zaveďme si k tomu hodnoty $p_0 = \frac{a}{a+b}$, tj. střední hodnotu apriorního společného rozdělení pro všechny řidiče, a $n_0 = a + b$. Dostáváme

$$\hat{p}_j^b = \frac{(a+b)a}{(a+b+n)(a+b)} + \frac{nk}{(a+b+n)n} = \frac{n_0}{n_0+n} p_0 + \frac{n}{n_0+n}\hat{p}_j,$$

což je lineární kombinace střední hodnoty $p_0$ a individuálního odhadu $\hat{p}_j$.

Zbývá nám tedy už jen smysluplně odhadnout neznámé parametry $a, b$. Víme přitom

$$\mathrm{E}\, X_{ji} = \mathrm{E}\,\mathrm{E}(X_{ji}\,|\,p) = \mathrm{E}\, p = p_0$$
$$\frac{\mathrm{E}\,\mathrm{var}(X_{ji}\,|\,p)}{\mathrm{var}\,\mathrm{E}(X_{ji}\,|\,p)} = \frac{\mathrm{E}(p(1-p))}{\mathrm{var}\, p} = a + b = n_0$$

$$Y = X^0 \beta^0 + \sigma Z,$$

kde $X^0$ má jen $q < k$ sloupců a předpokládáme, že sloupce $X^0$ generují podprostor v $\langle X \rangle$, tj. jsou všechny lineárními kombinacemi sloupců v $X$.

Nyní můžeme zopakovat předchozí konstrukci a zvolit přitom matici $P$ tak, aby jejích prvních $q$ vektorů generovalo $\langle X^0 \rangle$. Celé $P$ tak bude mít tvar $(P^0\ P^1)$ a stejně tak se rozpadne i vektor $V$

$$V = \begin{pmatrix} V^0 \\ V^1 \end{pmatrix} = \begin{pmatrix} (P^0)^T Z \\ (P^1)^T Z \end{pmatrix}.$$

Dostáváme tak jemnější rozklad vektorů a jejich velikostí a příslušných reziduí

$$\hat{Y}^0 = P^0 (P^0)^T Y = X^0 \beta^0 + \sigma P^0 V^0$$
$$Y - \hat{Y}^0 = \sigma P^1 V^1 + \sigma R U$$
$$\|Y - \hat{Y}^0\|^2 = \sigma^2 \|V^1\|^2 + \sigma^2 \|U\|^2 (\mathrm{RSS}^0 - \mathrm{RSS})/\sigma^2 = \|V^1\|^2.$$

Normovaný rozdíl reziduí má tedy rozdělení $\chi^2_{k-q}$. Odtud okamžitě vyplývá, že statistika $F$ zadaná jako relativní rozdíl reziduí má Fischerovo-Snedecorovo rozdělení

$$F = \frac{(\mathrm{RSS}^0 - \mathrm{RSS})/(k-q)}{\mathrm{RSS}\,/(n-k)} \sim \mathrm{F}_{k-q,n-k}\ .$$

Často v praktických situacích skutečně neznáme parametr $\sigma$ a nahrazujeme jej jeho odhadem $S^2$. Místo jednotlivých složek $b_j \sim \mathrm{N}(\beta_j, \sigma^2 c_{jj})$ náhodného vektoru $b$, kde $c_{jj}$ jsou diagonální prvky v matici $C = (X^T X)^{-1}$, pak pracujeme se statistikami

$$T_j = \frac{b_j - \beta_j}{S\sqrt{c_{jj}}} \sim \mathrm{t}_{n-k}\ .$$

Tyto veličiny již samozřejmě nemusí být nezávislé.

V případě, že bychom nepředpokládali plnou hodnost matice $X$, používali bychom v obdobných úvahách místo matice $C = (X^T X)^{-1}$ matici pseudoinverzní.

**9.57. Příklady testů.** Jako ilustraci velmi stručně zmíníme



několik příkladů použití lineárních modelů v nejjednodušších typech testů. Úplně nejjednodušší je to v případě jediného výběru, kdy testujeme, zda jediný parametr $\beta$ je roven dané hodnotě $\beta_0$.

Pro tento případ můžeme zvolit matici $X$ s jediným sloupcem plným jedniček. Výraz

$$Y = X\beta + \sigma Z$$

tedy značí, že jednotlivé komponenty v $Y$ jsou nezávislé veličiny $Y_i \sim N\beta, \sigma^2$, jde tedy obvyklý náhodný výběr rozsahu $n$ z normálního rozdělení. Z našich obecných úvah okamžitě vidíme odhad

$$b = (X^T X)^{-1} X^T Y = \frac{1}{n}\sum_{i=1}^{n} Y_i = \bar{Y}$$

$$S^2 = \frac{1}{n-1}\|Y - X\bar{Y}\|^2 = \frac{1}{n-1}\sum_{i=1}^{n}(Y_i - \bar{Y})^2,$$

což jsou právě výběrový průměr a rozptyl, se kterými jsme již počítali.

Zajímavá je v tomto kontextu hlavně statistika

$$T = \frac{\bar{Y} - \beta_0}{S}\sqrt{n}$$

a přitom veličiny na levých stranách můžeme přímo odhadnout.

$$\mathrm{E}\,X_{ij} = \mathrm{E}\,\mathrm{E}(X_{ji}\,|\,p) \simeq \frac{1}{N}\sum_{j=1}^{N}\hat{p}_j$$

$$\mathrm{E}\,\mathrm{var}(X_{ji}\,|\,p) \simeq \frac{1}{N}\sum_{j=1}^{N}\Big(\frac{n}{n-1}\hat{p}_j(1-\hat{p}_j)\Big)$$

$$\mathrm{var}\,\mathrm{E}(X_{ji}\,|\,p) \simeq s^2_{\hat{p}_j} - \frac{1}{nN}\sum_{j=1}^{N}\Big(\frac{n}{n-1}\hat{p}_j(1-\hat{p}_j)\Big),$$

kde $s^2_{\hat{p}_j}$ označuje výběrový rozptyl mezi individuálními odhady (čtenář si může promyslet, že odečtením posledního výrazu vpravo zajišťujeme, aby i poslední odhad byl nestranný).

Protože pro uvedená data takto dostáváme $n_0 \simeq 3{,}8643$ a $p_0 \simeq 0{,}1450$, vyjde nám bayesovský odhad individuální pravděpodobnosti nehod

$$\hat{p}^b_j = 0{,}154 \cdot 0{,}145 + 0{,}846 \cdot \hat{p}_j.$$

Jde tedy o kombinaci spolehlivého odhadu $\hat{p} = 0{,}145$ kolektivní pravděpodobnosti $p_0$ s individuálním (frekvenčním) odhadem $\hat{p}_j$, který je pořízen z malého počtu pozorování $n = 10$ u jediného řidiče. □

### L. Zpracování vícerozměrných dat

Někdy potřebujeme zpracovat vícerozměrná data: u každého z $n$ objektů určujeme $p$ znaků. Například můžeme zkoumat známky různých žáků z různých předmětů.

**9.94.** Ve svých pokusech pozoroval J.G.Mendel 10 rostlin hrachu a na každé z nich počet žlutých a zelených semen. Výsledky pokusu jsou shrnuty v následující tabulce:

| číslo rostliny | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| počet žlutých | 25 | 32 | 14 | 70 | 24 | 20 | 32 | 44 | 50 | 44 |
| počet zelených | 11 | 7 | 5 | 27 | 13 | 6 | 13 | 9 | 14 | 18 |
| celkem | 36 | 39 | 19 | 97 | 37 | 26 | 45 | 53 | 64 | 62 |

Z genetických modelů vyplývá, že pravděpodobnost výskytu žlutého semene by měla být 0,75 a zeleného 0,25. Na asymptotické hladině významnosti 0,05 testujte hypotézu, že se výsledky Mendelových pokusů shodují s modelem.

**Řešení.** Hypotézu budeme testovat *testem dobré shody*. Použijeme statistiku

$$K = \sum_{j=1}^{r}\frac{(n_j - np_j)}{np_j},$$

Testování hypotézy $\beta = \beta_0$ se nazývá *jednovýběrový t-test*. Na hladině $\alpha$ hypotézu zamítáme, když je $|T| \geq t_{n-1}(\alpha)$.

Obdobné jednoduché využití obecného modelu se nazývá *párový t-test*. Je vhodný na případy, kdy testujeme dvojice náhodných vektorů $W_1 = (W_{i1})$ a $W_2 = (W_{i2})$, o rozdílech jejichž komponent $Y_i = W_{i1} - W_{i2}$ víme, že mají rozdělení $\mathrm{N}(\beta, \sigma^2)$. Potřebujeme navíc, aby byly veličiny $Y_i$ nezávislé (což neříká, že musí být nezávislé jednotlivé dvojice $W_{i1}$ a $W_{i2}$!). Můžeme si v kontextu našeho ilustračního příkladu z 9.50 představit třeba hodnocení dvou různých vyučujících týmž studentem.

Testujeme hypotézu, že pro všechna $i$ je $\mathrm{E}\,W_{i1} = \mathrm{E}\,W_{i2}$. Je zjevné, že $Y = W_1 - W_2$ bude splňovat Používáme tedy statistiku

$$T = \frac{\bar{W}_1 - \bar{W}_2}{S}\sqrt{n}.$$

Zmíníme ještě jeden jednoduchý příklad s více parametry. Půjde o klasický případ *regresní přímky*.

Předpokládáme, že veličiny $Y_i$, $i = 1, \ldots, n$ mají rozdělení $\mathrm{N}(\beta_0 + \beta_1 x_i, \sigma^2)$, kde $x_i$ jsou dané konstanty. Zkoumáme tedy co nejlepší aproximaci

$$Y_i = b_0 + b_1 x_i$$

a matice $X$ příslušného lineárního modelu je

$$X^T = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \end{pmatrix}.$$

Dosazením do obecných vztahů snadno spočteme odhad

$$\begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = \begin{pmatrix} n & \bar{x} \\ n\bar{x} & \sum_{i=1}^n x_i^2 \end{pmatrix}^{-1} \begin{pmatrix} n\bar{Y} \\ \sum_{i=1}^n x_i Y_i \end{pmatrix} =$$
$$= \left(\sum_{i=1}^n (x_i - \bar{x})^2\right)^{-1} \begin{pmatrix} \frac{1}{n}\sum_{i=1}^n x_i^2 & -\bar{x} \\ -\bar{x} & 1 \end{pmatrix} \begin{pmatrix} n\bar{Y} \\ \sum_{i=1}^n x_i Y_i. \end{pmatrix}$$

Odtud už po drobné úpravě vychází

$$b_1 = \frac{\sum_{i=1}^n (x_i - \bar{x})(Y_i - \bar{Y})}{\sum_{i=1}^n (x_i - \bar{x})^2}$$

a konečně spočteme $b_0 = \bar{Y} - b_1\bar{x}$. Z výpočtu je přitom vidět, že

$$\mathrm{var}\,b_1 = \sigma^2 / \sum_{i=1}^n (x_i - \bar{x})^2.$$

Pro testování hypotézy, zda střední hodnota veličiny $Y$ nezávisí na $x$, tj. $H_0$ je tvaru $\beta_1 = 0$, můžeme tedy použít statistiku

$$T = \frac{b_1}{S}\left(\sum_{i=1}^n (x_i - \bar{x})^2\right)^{1/2} \sim \mathrm{t}_{n-2}\,.$$

Úplně obdobně vypadá statistická analýza vícenásobné regrese, kde máme několik sad hodnot $x_{ij}$ a vyhodnocujeme statistickou relevanci aproximace

$$Y_i = b_0 + b_1 x_{1i} + \cdots + b_k x_{ki}.$$

Jednotlivé statistiky $T_j$ zde umožňují t-test závislosti regrese na jednotlivých parametrech. Softwarové balíčky zpravidla uvádí také parametr vyjadřující, jak dobře jsou celkově hodnoty $Y_i$ aproximovány. Říkává se mu koeficient determinace

$$R^2 = 1 - \frac{\mathrm{RSS}}{\sum_{i=1}^n (Y_i - \bar{Y})^2}.$$

kde $r$ je počet třídících intervalů (měření; v našem případě $r = 10$), $n_j$ je skutečně naměřená četnost znaku ve zvoleném třídícím intervalu (budeme počítat množství žlutých semen), $p_j$ očekávaná četnost (podle předpokládaného rozložení), v našem případě $p_j = 0{,}75$, $j = 1, \ldots, 10$. Pokud by se výsledky pokusu skutečně řídily naším modelem, pak by $K \approx \chi^2(r - 1 - p)$, kde $p$ je počet odhadovaných parametrů v předpokládaném rozložení pravděpodobnosti. V našem případě je to obzvláště jednoduché, neboť náš model žádné neznámé parametry neobsahuje, je tedy $p = 0$ (parametry se mohou vyskytnout, pokud například předpokládáme, že rozložení pravděpodobnosti v našem pokusu bude normální, ovšem s neznámým rozptylem a střední hodnotou; potom by $p = 2$). Bude tedy $K \approx \chi^2(9)$. Statistika se doporučuje používat, pokud je očekávaná četnost znaku v každém z třídících intervalů alespoň pět.

Zapišme data do tabulky:

| $j$ | $n_j$ | $p_j$ | $np_j$ | $\frac{(n_j - np_j)^2}{np_j}$ |
|---|---|---|---|---|
| 1 | 25 | 0,75 | 27 | 0,148148 |
| 2 | 32 | 0,75 | 29, 25 | 0,258547 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 10 | 44 | 0,75 | 46,5 | 0,134409 |

Hodnota statistiky $K$ pro daná data je

$$K = 0{,}148148 + 0{,}258547 + \cdots + 0{,}134409 = 1{,}797495.$$

Tato hodnota je menší než $\chi^2_{095}(9) = 16{,}9$, nulovou hypotézu na hladině významnosti 0,05 tedy nezamítáme (nevylučujeme tedy, že známý model dědičnosti skutečně platí).

□

**9.58.** V praktických situacích se velmi často setkáváme s problémy, kdy jsou buď rozdělení základních statistických souborů úplně neznámá nebo jsou v modelu předpokládané chyby a odchylky s nenulovou střední hodnotou a jiným než normálním rozdělením. V těchto situacích je využití klasické frekvenční statistiky buď velmi obtížné nebo zcela nemožné.



Existují ale přístupy, jak pracovat přímo nad výběrovým souborem a odvozovat statistiky bodových či intervalových odhadů nebo pravděpodobnostní úsudky v obdobě k předchozím bodům, včetně vyčíslování standardních chyb.

Jedním ze zásadních průkopnických článků v tomto směru byla již v roce 1981 publikovaná stručná práce Bradleyho Efrona ze Stanfordu *Nonparametric estimates of standard error: The jackknife, the bootstrap and other methods*.[4]. Klíčová slova v tomto článku jsou: Balanced repeated replications; Bootstrap; Delta method; Half-sampling; Jackknife; Infinitesimal jackknife; Influence function.

Nemáme tu prostor pro podrobnější rozbor těchto technik, které jsou základem neparametrických metod v současných softwarových statistických nástrojích. Pro ilustraci jen stručně zmiňme postup v metodě *bootstrap*. Softwarovými prostředky v tomto případě z daného výběrového souboru vytváříme nové a nové výběrové soubory stejného rozsahu (přičemž skutečně provádíme výběr s vrácením vybrané jednotky do základního souboru) a pro každý z nich sledujeme potřebné statistiky (výběrový průměr, rozptyl apod.). Po velkém počtu opakování tohoto postupu tak získáme soubor, který považujeme za relevantní přiblíženi pravděpodobnostního rozložení zkoumané statistiky. Charakteristiky tohoto souboru považujeme za dobré přiblížení charakteristik zkoumané statistiky při bodových či intervalových odhadech, analýze rozptylu apod.

[4] Biometrika (1981), 68, 3, pp. 589-99

### Řešení cvičení

*9.21.* $\frac{3}{5} \cdot \frac{2}{3} + \frac{2}{5} \cdot 1 = \frac{4}{5}$.

*9.41.* Jednoduše $a = \frac{3}{8}$. Distribuční funkce náhodné veličiny $X$ je tedy $F_X(t) = \frac{1}{8}t^3$ pro $t \in (0, 2)$, pro menší $t$ je tato funkce nulová, pro větší rovna 1. Označme $Z = X^3$ náhodnou veličinu označující objem krychle. Ten je v intervalu $(0, 8)$, pro $t \in (0, 8)$ a distribuční funkci $F_Z$ náhodné veličiny $Z$ tedy můžeme psát $F_Z(t) = P[Z < t] = P[X^3 < t] = P[X < \sqrt[3]{t}] = F_X(\sqrt[3]{t}) = \frac{1}{8}t$, hustota pravděpodobnosti je pak $f_Z(t) = \frac{1}{8}$ na intervalu $(0, 8)$, jinak nula, jedná se tedy o rovnoměrné rozdělení pravděpodobnosti na daném intervalu, střední hodnota je tudíž 4.

*9.55.* $EU = 1 \cdot 0{,}6 + 2 \cdot 0{,}4 = 1{,}4$, $EU^2 = 0{,}4 + 4 \cdot 0{,}4 = 2{,}2$ $EV = 0{,}3 + 0{,}6 + 1{,}2 = 2{,}1$, $EV^2 = 0{,}3 + + 1, 2 + 3{,}6 = 5{,}1$, $E(UV) = 2{,}8$, $\mathrm{var}(U) = 2{,}2 - 1{,}4^2 = 2{,}2 - 1{,}96 = 0{,}24$, $\mathrm{var}(V) = 5{,}1 - 4{,}41 = 0{,}69$, $\mathrm{cov}(UV) = 2{,}8 - 1{,}4 \cdot 2{,}1 = -0{,}14$, $\rho_{U,V} = \frac{-0{,}14}{\sqrt{0{,}24 \cdot 0{,}69}} \doteq 0, 39$.

*9.56.* $EX = 1/3$, $\mathrm{var}^2\, X = 4/45$.

*9.57.*

$$\rho_{X,Y} = -1.$$

*9.58.* $\varrho_{U,V} \doteq -0, 421$.

KAPITOLA 10

# Teorie čísel

*God created the integers, all else is the work of man.*
*Leopold Kronecker*




## A. Základní vlastnosti dělitelnosti

**Dělitelnost přirozených čísel.** Připomeňme si základní vlastnosti



dělitelnosti, jejichž důkaz plyne přímo z definice: číslo 0 je dělitelné každým celým číslem; jediné celé číslo, které je dělitelné 0, je 0; pro libovolné číslo $a$ platí $a \mid a$; pro libovolná čísla $a, b, c$ platí tyto čtyři implikace:

$$\begin{aligned} a \mid b \ \wedge\ b \mid c \ &\Longrightarrow\ a \mid c, \\ a \mid b \ \wedge\ a \mid c \ &\Longrightarrow\ a \mid b+c \ \wedge\ a \mid b-c, \\ c \neq 0 \ &\Longrightarrow\ (a \mid b \iff ac \mid bc), \\ a \mid b \ \wedge\ b > 0 \ &\Longrightarrow\ a \leq b. \end{aligned}$$

Již se znalostí těchto základních pravidel jsme schopni řešit mnohé úlohy.

**10.1.** Zjistěte, pro která přirozená čísla $n$ je číslo $n^3+1$ dělitelné číslem $n-1$.

V této kapitole se budeme zabývat úlohami o celých číslech. Převážně v nich půjde o dělitelnost celých čísel, popřípadě o řešení rovnic v oboru celých nebo přirozených čísel (zde vzhledem k obvyklé oborové konvenci na rozdíl od zbytku knihy nebudeme nulu počítat mezi přirozená čísla). Ačkoli jsou přirozená a celá čísla v jistém smyslu nejjednodušší matematickou strukturou, zkoumání jejich vlastností postavilo před generace matematiků celou řadu velice obtížných problémů. Často jsou to problémy, které je možno snadno formulovat, přesto však dodnes neznáme řešení některých z nich.

Uveďme některé z nejznámějších:

- *problém prvočíselných dvojčat* – rozhodnout, zda existuje nekonečně mnoho prvočísel $p$ takových, že i $p+2$ je prvočíslo,[1]
- *prvočísla Sophie Germainové* – rozhodnout, zda existuje nekonečně mnoho prvočísel $p$ takových, že i $2p+1$ je prvočíslo,
- *problém existence lichého dokonalého čísla* – tj. čísla, jehož součet dělitelů je roven dvojnásobku tohoto čísla,
- *Goldbachova hypotéza* – jde o to rozhodnout, zda každé sudé číslo větší než 2 je možno psát jako součet dvou prvočísel,
- klenot mezi problémy teorie čísel *velkou Fermatovu větu* (Fermat's Last Theorem) – jde o otázku, zda existují přirozená čísla $n, x, y, z$ tak, že $n > 2$ a platí $x^n + y^n = z^n$; Pierre de Fermat ji formuloval kolem roku 1637, vyřešil ji po značném úsilí celých generací (a s pomocí výsledků z mnoha oblastí matematiky) Andrew Wiles až v roce 1995.

## 1. Základní pojmy

**10.1. Dělitelnost.** Připomeňme, že říkáme, že celé číslo $a$ *dělí*



celé číslo $b$ (neboli číslo $b$ je *dělitelné* číslem $a$, též $b$ je *násobek* $a$), pokud existuje celé číslo $c$ tak, že platí $a \cdot c = b$. Píšeme pak $a \mid b$. Pojem dělitelnosti lze definovat a jeho vlastnosti zkoumat i mnohem obecněji – více v části 11.18.

Jednou z nejdůležitějších vlastností celých čísel, kterou budeme často využívat, je možnost jednoznačného *dělení se zbytkem*.

**Věta.** *Pro libovolně zvolená čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, m-1\}$ tak, že $a = qm + r$.*

Důkaz. Dokážeme nejprve existenci čísel $q, r$. Předpokládejme, že přirozené číslo $m$ je dáno pevně a dokažme tvrzení pro

[1] Tato otázka stále patří mezi otevřené problémy – v roce 2013 ale Zhang Yitang publikoval důkaz slibného tvrzení, že pro některé $n < 7 \cdot 10^7$ existuje nekonečně mnoho dvojic prvočísel lišících se právě o $n$. Viz Z. Yitang, *Bounded gaps between primes*, Annals of Mathematics, 2013.

**Řešení.** Platí $n^3-1=(n-1)(n^2+n+1)$, a tedy pro libovolné $n$ je číslo $n^3-1$ dělitelné číslem $n-1$. Má-li $n-1$ dělit i číslo $n^3+1$, musí dělit i rozdíl $(n^3+1)-(n^3-1)=2$. Protože $n\in\mathbb{N}$, platí $n-1\geq 0$, a tedy z $n-1\mid 2$ plyne $n-1=1$ nebo $n-1=2$, a proto $n=2$ nebo $n=3$. Uvedenou vlastnost mají tedy pouze přirozená čísla 2 a 3. □

**10.2.** Dokažte, že pro libovolné $a\in\mathbb{Z}$ platí:

i) $a^2$ dává po dělení čtyřmi zbytek 0 nebo 1,
ii) $a^2$ dává po dělení osmi zbytek 0,1 nebo 4,
iii) $a^4$ dává po dělení šestnácti zbytek 0 nebo 1.

**Řešení.**

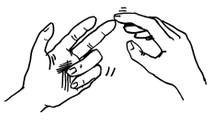
- Z věty o dělení se zbytkem plyne, že každé celé číslo $a$ lze zapsat jednoznačně v jednom z tvarů $a=2k$ nebo $a=2k+1$. Po umocnění dostaneme $a^2=4k^2$ nebo $a^2=4(k^2+k)+1$, což jsme měli dokázat.
- S využitím předchozího výsledku ihned dostaneme tvrzení pro (sudá) čísla tvaru $a=2k$. Pro lichá čísla jsme dostali $a^2=4k(k+1)+1$, odkud dostaneme tvrzení, uvědomíme-li si, že $k(k+1)$ je jistě sudé.
- Použijeme výsledek předchozích částí, tedy $a^2=4\ell$ nebo $a^2=8\ell+1$. Po opětovném umocnění dostaneme požadované tvrzení, neboť $a^4=(a^2)^2=16\ell^2$ pro $a$ sudé a $a^4=(a^2)^2=(8\ell+1)^2=64\ell^2+16\ell+1=16(4\ell^2+\ell)+1$ pro $a$ liché. □

**10.3.** Dokažte, že dávají-li čísla $a,b\in\mathbb{Z}$ po dělení číslem $m\in\mathbb{N}$ zbytek jedna, je 1 i zbytek po dělení čísla $ab$ číslem $m$.

**Řešení.** Podle věty o dělení se zbytkem existují $s,t\in\mathbb{Z}$ tak, že $a=sm+1, b=tm+1$. Vynásobením dostaneme vyjádření

$$ab=(sm+1)(tm+1)=(stm+s+t)m+1,$$

kde $stm+s+t$ je neúplný podíl a zbytek po dělení čísla $ab$ číslem $m$ je roven 1. □



Z věty o dělení se zbytkem plyne existence a jednoznačnost největšího společného dělitele libovolných dvou celých čísel $a,b$ a rovněž to, že jej lze efektivně vypočítat pomocí Euklidova algoritmu. Zároveň jsme schopni současně s největším společným dělitelem určit i koeficienty do Bezoutovy rovnosti – totiž taková celá čísla $k,l$, že platí $ak+bl=(a,b)$. Rovněž lze snadno dokázat přímo z vlastností dělitelnosti, že jako celočíselnou lineární kombinaci čísel $a,b$ lze vyjádřit právě násobky největšího společného dělitele.

libovolné $a\in\mathbb{Z}$. Nejprve budeme předpokládat, že $a\in\mathbb{N}_0$ a existenci čísel $q,r$ dokážeme indukcí vzhledem k $a$:

Je-li $0\leq a<m$, stačí volit $q=0, r=a$ a rovnost $a=qm+r$ platí.

Předpokládejme nyní, že $a\geq m$ a že jsme existenci čísel $q,r$ dokázali pro všechna $a'\in\{0,1,2,\ldots,a-1\}$. Speciálně pro $a'=a-m\geq 0$ tedy existují $q',r'$ tak, že $a'=q'm+r'$ a přitom $r'\in\{0,1,\ldots,m-1\}$. Zvolíme-li $q=q'+1, r=r'$, platí $a=a'+m=(q'+1)m+r'=qm+r$, což jsme chtěli dokázat.

Je-li nyní $a$ záporné, pak ke kladnému číslu $-a$ podle výše dokázaného existují $q'\in\mathbb{Z}$, $r'\in\{0,1,\ldots,m-1\}$ tak, že $-a=q'm+r'$. Je-li $r'=0$, položíme $r=0$, $q=-q'$; je-li $r'>0$, položíme $r=m-r'$, $q=-q'-1$. V obou případech $a=q\cdot m+r$, a tedy čísla $q,r$ s požadovanými vlastnostmi existují pro každé $a\in\mathbb{Z}$, $m\in\mathbb{N}$.

Nyní dokážeme jednoznačnost. Předpokládejme, že pro některá čísla $q_1,q_2\in\mathbb{Z}$ a $r_1,r_2\in\{0,1,\ldots,m-1\}$ platí $a=q_1m+r_1=q_2m+r_2$. Úpravou dostaneme $r_1-r_2=(q_2-q_1)m$, a tedy $m\mid r_1-r_2$. Ovšem z toho, že $0\leq r_1<m$, $0\leq r_2<m$ plyne $-m<r_1-r_2<m$, odkud $r_1-r_2=0$, a tedy i $(q_2-q_1)m=0$, a proto $q_1=q_2, r_1=r_2$. □

Číslo $q$, resp. $r$, z věty se nazývá *(neúplný) podíl*, resp. *zbytek*, při dělení čísla $a$ číslem $m$ se zbytkem. Volba těchto názvů je srozumitelnější, upravíme-li rovnost $a=mq+r$ do tvaru

$$\frac{a}{m}=q+\frac{r}{m},\quad \text{přitom}\quad 0\leq\frac{r}{m}<1.$$

**10.2. Největší společný dělitel.** Jedním z nejpotřebnějších nástrojů výpočetní teorie čísel je algoritmus pro výpočet největšího společného dělitele. Protože jde, jak si ukážeme, o relativně rychlou proceduru, je i v moderních algoritmech velmi často využívána.



NEJVĚTŠÍ SPOLEČNÝ DĚLITEL

Mějme celá čísla $a,b$. Libovolné celé číslo $m$ takové, že $m\mid a$, $m\mid b$ se nazývá *společný dělitel* čísel $a,b$. Společný dělitel $m\geq 0$ čísel $a,b$, který je dělitelný libovolným společným dělitelem čísel $a,b$, se nazývá *největší společný dělitel* čísel $a,b$ a značí se $(a,b)$ (někdy též $\gcd(a,b)$ nebo $\mathrm{nsd}(a,b)$).

Duálně definujeme pojem *nejmenší společný násobek* a značíme $[a,b]$ (případně $\mathrm{lcm}(a,b)$ nebo $\mathrm{nsn}(a,b)$).

Přímo z definice plyne, že pro libovolné $a,b\in\mathbb{Z}$ platí $(a,b)=(b,a)$, $[a,b]=[b,a]$, $(a,1)=1$, $[a,1]=|a|$, $(a,0)=|a|$, $[a,0]=0$.

Dosud jsme nijak nezdůvodnili, že pro každou dvojici celých čísel $a,b$ jejich největší společný dělitel a nejmenší společný násobek vůbec existují. Pokud ale dokážeme, že existují, jsou již určena jednoznačně, protože pro každá dvě nezáporná celá čísla $k,l$ podle definice platí, že pokud $k\mid l$ a zároveň $l\mid k$, pak nutně $k=l$. V obecném případě dělitelnosti v oboru integrity je ale situace složitější – viz 11.21. I v případě tzv. euklidovských okruhů,[2]

[2] Wikipedia, *Euclidean domain*, `http://en.wikipedia.org/wiki/Euclidean_domain` (as of July 18, 2013, 18:19 GMT).

**10.4.** Určete největší společný dělitel čísel $a = 10175, b = 2277$ a určete příslušné koeficienty v Bezoutově rovnosti.

**Řešení.** Postupujme Euklidovým algoritmem:

$$\begin{aligned}
10175 &= 4 \cdot 2277 + 1067,\\
2277 &= 2 \cdot 1067 + 143,\\
1067 &= 7 \cdot 143 + 66,\\
143 &= 2 \cdot 66 + 11,\\
66 &= 6 \cdot 11 + 0.
\end{aligned}$$

Největším společným dělitelem je tedy číslo 11, které postupně vyjádříme z jednotlivých rovností jako lineární kombinaci čísel $a, b$:

$$\begin{aligned}
11 &= 143 - 2 \cdot 66 =\\
&= 143 - 2 \cdot (1067 - 7 \cdot 143) =\\
&= -2 \cdot 1067 + 15 \cdot 143 =\\
&= -2 \cdot 1067 + 15 \cdot (2277 - 2 \cdot 1067) =\\
&= 15 \cdot 2277 - 32 \cdot 1067 =\\
&= 15 \cdot 2277 - 32 \cdot (10175 - 4 \cdot 2277) =\\
&= -32 \cdot 10175 + 143 \cdot 2277.
\end{aligned}$$

Hledané vyjádření je tedy $11 = (-32) \cdot 10175 + 143 \cdot 2277$. □

**10.5.** Určete největšího společného dělitele čísel $2^{49} - 1$ a $2^{35} - 1$ a určete koeficienty do příslušné Bezoutovy rovnosti.

**Řešení.** Užijeme Euklidův algoritmus. Platí

$$\begin{aligned}
2^{49} - 1 &= 2^{14}(2^{35} - 1) + 2^{14} - 1,\\
2^{35} - 1 &= (2^{21} + 2^7)(2^{14} - 1) + 2^7 - 1,\\
2^{14} - 1 &= (2^7 + 1)(2^7 - 1).
\end{aligned}$$

Hledaný největší společný dělitel je tedy $2^7 - 1 = 127$. Všimněme si, že $7 = (63, 91)$ – viz též následující příklad ‖10.6‖. Obrácením postupu dostaneme hledané koeficienty $k, \ell$ do Bezoutovy rovnosti $2^7 - 1 = (2^{49} - 1)k + (2^{35} - 1)\ell$:

$$\begin{aligned}
2^7 - 1 &= (2^{35} - 1) - (2^{21} + 2^7)(2^{14} - 1) =\\
&= (2^{35} - 1) - (2^{21} + 2^7)((2^{49} - 1) - 2^{14}(2^{35} - 1)) =\\
&= (2^{35} + 2^{21} + 1)(2^{35} - 1) - (2^{21} + 2^7)(2^{49} - 1).
\end{aligned}$$

Je tedy $k = -(2^{21} + 2^7)$, $\ell = 2^{35} + 2^{21} + 1$. Pro jistotu poznamenejme, že tyto koeficienty nejsou určeny jednoznačně. □

které garantují existenci největšího společného dělitele, je výsledek určen jednoznačně až na asociovanost, tedy na násobek jednotky – v našem případě celých čísel se asociovaná čísla liší znaménkem. Jednoznačnost jsme tak zajistili požadavkem na nezápornost největšího společného dělitele.



**Věta** (Euklidův algoritmus)**.** *Nechť $a_1, a_2$ jsou přirozená čísla. Pro každé $n \geq 3$, pro které $a_{n-1} \neq 0$, označme $a_n$ zbytek po dělení čísla $a_{n-2}$ číslem $a_{n-1}$. Pak po konečném počtu kroků dostaneme $a_k = 0$ a platí $a_{k-1} = (a_1, a_2)$.*

Důkaz. Podle věty o dělení se zbytkem platí $a_2 > a_3 > a_4 > \ldots$. Protože jde o nezáporná celá čísla, nemůže být tato klesající posloupnost nekonečná, a po konečném počtu kroků tak dostaneme $a_k = 0$, přičemž $a_{k-1} \neq 0$. Z definice čísel $a_n$ přitom plyne, že existují celá čísla $q_1, q_2, \ldots, q_{k-2}$ tak, že

$$\begin{aligned}
a_1 &= q_1 \cdot a_2 + a_3,\\
a_2 &= q_2 \cdot a_3 + a_4,\\
&\vdots\\
a_{k-3} &= q_{k-3} \cdot a_{k-2} + a_{k-1},\\
a_{k-2} &= q_{k-2} \cdot a_{k-1}.
\end{aligned}$$

Z poslední rovnosti plyne, že $a_{k-1} \mid a_{k-2}$, dále $a_{k-1} \mid a_{k-3}, \ldots, a_{k-1} \mid a_2, a_{k-1} \mid a_1$. Je tedy $a_{k-1}$ společný dělitel čísel $a_1, a_2$.

Naopak libovolný společný dělitel čísel $a_1, a_2$ dělí i číslo $a_3 = a_1 - q_1 a_2$, a proto dělí i čísla $a_4 = a_2 - q_2 a_3, a_5, \ldots$, a zejména i $a_{k-1} = a_{k-3} - q_{k-3} a_{k-2}$. Dokázali jsme tak, že $a_{k-1}$ je největší společný dělitel čísel $a_1, a_2$. □

Z předchozího tvrzení a z toho, že pro libovolná $a, b \in \mathbb{Z}$ platí $(a, b) = (a, -b) = (-a, b) = (-a, -b)$, plyne existence největšího společného dělitele libovolných dvou celých čísel.

Navíc dostáváme z Euklidova algoritmu i následující zajímavé a často využívané tvrzení.

**10.3. Věta** (Bezoutova)**.** *Pro libovolná celá čísla $a, b$ existují celá čísla $k, l$ tak, že $(a, b) = ka + lb$.*

Důkaz. Jistě stačí větu dokázat pro $a, b \in \mathbb{N}$. Všimněme si, že jestliže je možné nějaká čísla $r, s \in \mathbb{Z}$ vyjádřit ve tvaru $r = r_1 a + r_2 b$, $s = s_1 a + s_2 b$, kde $r_1, r_2, s_1, s_2 \in \mathbb{Z}$, můžeme tak vyjádřit i

$$r + s = (r_1 + s_1)a + (r_2 + s_2)b$$

a také

$$c \cdot r = (c \cdot r_1)a + (c \cdot r_2)b$$

pro libovolné $c \in \mathbb{Z}$. Z Euklidova algoritmu (pro $a_1 = a, a_2 = b$) plyne, že takto můžeme vyjádřit i $a_3 = a_1 - q_1 a_2$, $a_4 = a_2 - q_2 a_3$, …, a tedy i číslo $a_{k-1} = a_{k-3} - q_{k-3} a_{k-2}$, což je ovšem $(a_1, a_2)$.

Zdůrazněme přitom, že hledaná čísla $k, l$ zdaleka nejsou určena jednoznačně. □

**Poznámka.** Výpočet největšího společného dělitele pomocí Euklidova algoritmu je s využitím výpočetní techniky i pro relativně velká čísla poměrně rychlý. V našem příkladu to vyzkoušíme na 2 číslech $A, B$, z nichž každé je součinem dvou 101-ciferných prvočísel. Všimněme si, že výpočet největšího společného dělitele

**10.6.** Zobecněme nyní výsledek předchozího příkladu a dokažme, že pro $a, m, n \in \mathbb{N}$, $a \neq 1$, platí: $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

**Řešení.** Požadované tvrzení snadno vyplyne z toho, že pro libovolná přirozená čísla $k, \ell$ platí $a^k - 1 \mid a^\ell - 1$, právě když $k \mid \ell$. A to dokážeme tak, že vydělíme číslo $\ell$ číslem $k$ se zbytkem, tj. položíme $\ell = kq + r$, kde $q, r \in \mathbb{N}_0$, $r < k$, a uvážíme, že

$$a^{kq+r} - 1 = (a^k - 1)(a^{k(q-1)+r} + a^{k(q-2)+r} + \cdots + a^{k+r} + a^r) + a^r - 1$$

je dělením čísla $a^{kq+r} - 1$ číslem $(a^k - 1)$ se zbytkem (zřejmě totiž $a^r - 1 < a^k - 1$). Odtud je již snadno vidět, že zbytek $r$ je nulový, právě když je zbytek $a^r - 1$ nulový, což jsme potřebovali dokázat. □

**10.7.** Dokažte, že pro všechna $n \in \mathbb{N}$ : $25 \mid 4^{2n+1} - 10n - 4$.

**Řešení.** Toto tvrzení lze dokázat několika způsoby (nejsnadněji pomocí vlastností kongruencí, které zavedeme o něco později), my jej zde dokážeme nejprve indukcí a potom jako důsledek binomické věty.

Tvrzení zřejmě platí pro $n = 0$ (byť se v zadání o platnosti pro $n = 0$ nemluvilo, jistě můžeme dokázat požadovanou vlastnost pro rozšířenou množinu $n \in \mathbb{N}_0$ a tím si usnadnit první krok indukce). V druhém kroku, předpokládáme-li, že $25 \mid 4^{2n-1} - 10(n-1) - 4$, pak rovněž $25 \mid 16(4^{2n-1} - 10(n-1) - 4) = 4^{2n+1} - 10n - 4 - 150n + 100$, odkud snadno plyne, že platí potřebný vztah $25 \mid 4^{2n+1} - 10n - 4$.

Druhý důkaz využívá binomickou větu – podle ní totiž

$$(5-1)^{2n+1} = \sum_{k=0}^{2n+1} \binom{2n+1}{k} 5^{2n+1-k}(-1)^k,$$

přičemž jsou zřejmě všechny sčítance násobky 25, s výjimkou posledních dvou, tj. s výjimkou součtu $\binom{2n+1}{2n}5^1(-1)^{2n} + 5^0(-1)^{2n+1}$. Jinak řečeno, $4^{2n+1}$ dává po dělení 25 stejný zbytek jako $10n + 4$, což je ekvivalentní dokazovanému tvrzení. □

**Prvočísla.** V teoretické části uvádíme Euklidův důkaz nekonečnosti prvočísel a podrobně se zabýváme tím, jak jsou prvočísla v množině přirozených čísel rozložena (v některých případech jsme ale byli nuceni ponechat uváděná tvrzení bez důkazu). Uveďme nyní několik souvisejících příkladů.

**10.8.** Pro libovolné přirozené číslo $n > 2$ existuje mezi čísly $n$ a $n!$ alespoň jedno prvočíslo.



**Řešení.** Označme $p$ libovolné prvočíslo dělící číslo $n! - 1$ (takové existuje podle Základní věty aritmetiky 10.7, protože $n! - 1 > 1$). Kdyby $p \leq n$, muselo by $p$ dělit číslo $n!$ a nedělilo by $n! - 1$. Je tedy $n < p$. Protože $p \mid (n! - 1)$, platí $p \leq n! - 1$, tedy $p < n!$. Prvočíslo $p$ splňuje podmínky úlohy. □

i takto velkých čísel trval zanedbatelný čas. Pozorovatelem zaznamenatelný čas zabere tento výpočet až ve druhé ukázce, v níž jsou vstupem dvě čísla mající více než milion cifer.

Příklad v systému SAGE :

```
sage: p=next_prime(5*10^100)
sage: q=next_prime(3*10^100)
sage: r=next_prime(10^100)
sage: A=p*q;B=q*r;
sage: time G=gcd(A,B); print G

Time: CPU 0.00 s, Wall: 0.00 s
3000000000000000000000000000000000000000\
0000000000000000000000000000000000000000\
00000000000000000000000000223

time G=gcd(A^10000+1,B^10000+1);
Time: CPU 2.47 s, Wall: 2.48 s
```

Euklidův algoritmus a Bezoutova věta jsou základními výsledky elementární teorie čísel a tvoří jeden z pilířů algoritmů algebry a teorie čísel.

**10.4. Nejmenší společný násobek.** Zatím jsme vlastnosti



nejmenšího společného násobku trochu ignorovali, ale vzhledem k následujícímu tvrzení vše podstatné odvodíme z vlastností největšího společného dělitele.

**Lemma.** *Pro libovolná celá čísla $a, b$ existuje jejich nejmenší společný násobek $[a, b]$ a platí $(a, b) \cdot [a, b] = |a \cdot b|$.*

Důkaz. Tvrzení jistě platí, je-li některé z čísel $a, b$ rovno nule. Můžeme navíc předpokládat, že obě nenulová čísla $a, b$ jsou kladná, neboť jejich znaménka se v dokazovaném vzorci neprojeví. Budeme hotovi, ukážeme-li, že $q = a \cdot b/(a, b)$ je nejmenším společným násobkem čísel $a, b$.

Protože $(a, b)$ je společný dělitel čísel $a, b$, jsou $a/(a, b)$ i $b/(a, b)$ celá čísla, a proto

$$q = \frac{ab}{(a,b)} = \frac{a}{(a,b)} \cdot b = \frac{b}{(a,b)} \cdot a$$

společný násobek čísel $a, b$. Podle Bezoutovy věty existují $k, l \in \mathbb{Z}$ tak, že $(a, b) = ka + lb$. Předpokládejme, že $n \in \mathbb{Z}$ je libovolný společný násobek čísel $a, b$ a ukážeme, že je dělitelný číslem $q$. Je tedy $n/a, n/b \in \mathbb{Z}$, a proto je celé i číslo

$$\frac{n}{b} \cdot k + \frac{n}{a} \cdot l = \frac{n(ka+lb)}{ab} = \frac{n(a,b)}{ab} = \frac{n}{q}.$$

To ovšem znamená, že $q \mid n$, což jsme chtěli dokázat. □

**10.5. Nesoudělnost.** Analogicky jako v případě dvou čísel se de-



finuje i největší společný dělitel a nejmenší společný násobek více než dvou celých čísel a snadno se následně dokáže, že platí

$$(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n),$$
$$[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n].$$

Z tohoto příkladu rovněž vyplývá nekonečnost prvočísel (stačí uvážit posloupnost $a_0 = 3, a_{n+1} = a_n!$ pro $n \in \mathbb{N}$). Toto tvrzení je ale (oproti skutečnosti) velice slabé, protože konstruovaná posloupnost obsahuje jen „velmi malou“ podmnožinu prvočísel.

Na druhou stranu, jak ukazuje následující příklad, jsme schopni zkonstruovat libovolně dlouhou posloupnost po sobě jdoucích čísel, z nichž žádné není prvočíslem.

**10.9.** Dokažte, že pro libovolné přirozené číslo $n$ existuje $n$ po sobě jdoucích přirozených čísel, z nichž žádné není prvočíslo.

**Řešení.** Zkoumejme čísla $(n+1)! + 2$, $(n+1)! + 3$, $\cdots$, $(n+1)! + (n+1)$. Mezi těmito $n$ po sobě jdoucími čísly není žádné prvočíslo, protože pro libovolné $k \in \{2, 3, \ldots, n+1\}$ platí $k \mid (n+1)!$, a tedy $k \mid (n+1)! + k$, a proto $(n+1)! + k$ nemůže být prvočíslo. □

**10.10.**

i) Dokažte, že jsou-li přirozená čísla $m, n$ nesoudělná, jsou nesoudělná rovněž čísla

$$m^2 + mn + n^2 \quad \text{a} \quad m^2 - mn + n^2.$$

ii) Dokažte, že jsou-li lichá přirozená čísla $m, n$ nesoudělná, jsou nesoudělná rovněž čísla

$$m + 2n \quad \text{a} \quad m^2 + 4n^2.$$

**Řešení.**

i) Předpokládejme pro spor, že nějaké prvočíslo $p$ dělí obě čísla $m^2 + mn + n^2$ i $m^2 - mn + n^2$. Pak také dělí jejich rozdíl $2mn$, odkud buď $p = 2$ nebo $p$ dělí některé z čísel $m, n$. Je-li $p = 2$, pak je číslo $m^2 + mn + n^2$ sudé, a proto musí být obě čísla $m$ i $n$ sudá, což je spor s předpokladem jejich nesoudělnosti. Pokud $p$ dělí $m$ spolu s $m^2 + mn + n^2$, pak nutně dělí rovněž $n^2$ a podle Euklidovy věty 10.6 tak dělí i $n$. To je ale opět spor s nesoudělností $m, n$. Analogicky postupujeme i v případě $p \mid n$.

ii) Podobně jako v předchozím příkladu předpokládejme, že nějaké prvočíslo $p$ dělí $m + 2n$ i $m^2 + 4n^2$. Pak musí dělit i číslo $(m^2 + 4n^2) - (m + 2n)(m - 2n) = 8n^2$, a protože $p \neq 2$ (kdyby bylo $m + 2n$ sudé, bylo by sudé i $m$), nutně $p \mid n$. Protože ale $p$ dělí i $m + 2n$, dostáváme $p \mid m$, což je spor. □

Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *nesoudělná*, jestliže platí $(a_1, a_2, \ldots, a_n) = 1$. Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *po dvou nesoudělná*, jestliže pro každé $i, j$ takové, že $1 \leq i < j \leq n$, platí $(a_i, a_j) = 1$.

**Poznámka.** Uvědomme si ještě, že je rozdíl mezi pojmy *po dvou nesoudělná čísla* a *nesoudělná čísla*. Máme totiž například $(6, 10, 15) = 1$, přitom jsou ale libovolná dvě z čísel $6, 10, 15$ soudělná.

**Lemma.** *Pro libovolná přirozená čísla $a, b, c$ platí*

*(1)* $(ac, bc) = (a, b) \cdot c$,
*(2) jestliže* $a \mid bc$, $(a, b) = 1$, *pak* $a \mid c$,
*(3)* $d = (a, b)$ *právě tehdy, když existují* $k, l \in \mathbb{N}$ *tak, že* $a = dk$, $b = dl$ *a* $(k, l) = 1$.

Důkaz. (1) Protože $(a, b)$ je společný dělitel čísel $a, b$, je $(a, b) \cdot c$ společný dělitel čísel $ac$, $bc$, proto $(a, b) \cdot c \mid (ac, bc)$. Podle Bezoutovy věty existují $k, l \in \mathbb{Z}$ tak, že $(a, b) = ka + lb$. Protože $(ac, bc)$ je společný dělitel čísel $ac$, $bc$, dělí i číslo $kac + lbc = (a, b) \cdot c$. Dokázali jsme, že $(a, b) \cdot c$ a $(ac, bc)$ jsou dvě přirozená čísla, která dělí jedno druhé, proto se rovnají.

(2) Předpokládejme, že $(a, b) = 1$ a $a \mid bc$. Podle Bezoutovy věty existují $k, l \in \mathbb{Z}$ tak, že $ka + lb = 1$, odkud plyne, že $c = c(ka + lb) = kca + lbc$. Protože $a \mid bc$, plyne odsud, že i $c$ je násobkem čísla $a$.

(3) Nechť $d = (a, b)$, pak existují $q_1, q_2 \in \mathbb{N}$ tak, že $a = dq_1$, $b = dq_2$. Pak podle 1. části platí $d = (a, b) = (dq_1, dq_2) = d \cdot (q_1, q_2)$, a tedy $(q_1, q_2) = 1$. Naopak, je-li $a = dq_1$, $b = dq_2$ a $(q_1, q_2) = 1$, pak $(a, b) = (dq_1, dq_2) = d(q_1, q_2) = d \cdot 1 = d$ (opět užitím 1. části tohoto tvrzení). □

### 2. Prvočísla



Prvočíslo je jeden z nejdůležitějších pojmů elementární teorie čísel. Jeho důležitost je dána především větou o jednoznačném rozkladu libovolného přirozeného čísla na součin prvočísel, která je silným a účinným nástrojem při řešení celé řady úloh z teorie čísel.

Prvočíslo

Každé přirozené číslo $n \geq 2$ má aspoň dva kladné dělitele: 1 a $n$. Pokud kromě těchto dvou jiné kladné dělitele nemá, nazývá se *prvočíslo*. V opačném případě hovoříme o *složeném čísle*.

V dalším textu budeme zpravidla prvočíslo značit písmenem $p$. Nejmenší prvočísla jsou 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... (zejména číslo 1 za prvočíslo ani za číslo složené nepovažujeme, je totiž invertibilní, neboli jednotkou okruhu celých čísel). Prvočísel je, jak brzy dokážeme, nekonečně mnoho, máme ovšem poměrně limitované výpočetní prostředky na zjištění, zda je dané číslo prvočíslem; číslo $2^{57\,885\,161} - 1$, které bylo v roce 2013 největším známým prvočíslem, má pouze 17 425 170 cifer a jeho dekadické vyjádření by se tak vešlo na kdejaký prehistorický datový nosič, při tisku knihy o 60 řádcích na stránku a 80 znacích na řádek by nicméně i tak zabralo 3 631 stran.

Uveďme nyní větu, která udává ekvivalentní podmínku prvočíselnosti a je základní ingrediencí při důkazu jednoznačnosti rozkladu na prvočísla.

## B. Kongruence



V tomto odstavci si procvičíme, jak může zvládnutí základních operací s kongruencemi přispět k elegantnímu vyjádření řešení příkladů, které bychom sice byli schopni vyřešit pouze s pomocí základních vlastností dělitelnosti, s využitím kongruencí bude ale zápis řešení obvykle podstatně stručnější.

**10.11.**

i) Nalezněte zbytek po dělení čísla $7^{30}$ číslem 50.

ii) Určete dvě poslední cifry dekadického zápisu čísla $7^{30}$.

**Řešení.**

i) Protože $7^2 = 49 \equiv -1 \pmod{50}$, s využitím vlastností kongruencí uvedených v teoretické části dostáváme

$$7^{30} \equiv (-1)^{15} = -1 \pmod{50},$$

a tedy zbytek po dělení čísla $7^{30}$ číslem 50 je 49.

ii) Máme vlastně určit zbytek po dělení $7^{30}$ číslem 100. Z předchozího víme, že zbytek po dělení 50 je 49, proto poslední dvě cifry jsou buď 49 nebo 99. Víme již tedy zejména, že $7^{30} \equiv -1 \pmod{25}$ a snadno spočítáme, že $7^{30} \equiv (-1)^{30} = 1 \pmod 4$. Protože $(4, 25) = 1$, dostáváme odtud, že hledaným dvojčíslím je 49 (dává totiž požadovaný zbytek modulo 25 i modulo 4). □

**10.12.** Dokažte, že pro libovolné $n \in \mathbb{N}$ je $37^{n+2} + 16^{n+1} + 23^n$ dělitelné sedmi.

**Řešení.** Platí $37 \equiv 16 \equiv 23 \equiv 2 \pmod 7$, a tedy podle základních vlastností kongruencí platí

$$37^{n+2}+16^{n+1}+23^n \equiv 2^{n+2}+2^{n+1}+2^n = 2^n(4+2+1) \equiv 0 \pmod 7.$$

□

**10.13.** Dokažte, že číslo $n = (835^5 + 6)^{18} - 1$ je dělitelné číslem 112.

**Řešení.** Rozložíme $112 = 7 \cdot 16$. Protože $(7, 16) = 1$, stačí ukázat, že $7 \mid n$ a $16 \mid n$. Platí $835 \equiv 2 \pmod 7$, a tedy

$$n \equiv (2^5 + 6)^{18} - 1 = 38^{18} - 1 \equiv 3^{18} - 1 = \\ = 27^6 - 1 \equiv (-1)^6 - 1 = 0 \pmod 7,$$

**10.6. Věta** (Euklidova o prvočíslech)**.** *Přirozené číslo $p \geq 2$ je prvočíslo, právě když platí: pro každá celá čísla $a, b$ z toho, že $p \mid ab$, plyne $p \mid a$ nebo $p \mid b$.*

Důkaz. „⇒“ Předpokládejme, že $p$ je prvočíslo a $p \mid ab$, kde $a, b \in \mathbb{Z}$. Protože $(p, a)$ je kladný dělitel $p$, platí $(p, a) = p$ nebo $(p, a) = 1$. V prvním případě $p \mid a$, ve druhém $p \mid b$ podle části 2. předchozí věty.

„⇐“ Jestliže $p$ není prvočíslo, musí existovat jeho kladný dělitel různý od 1 a $p$. Označíme jej $a$. Pak ovšem $b = \frac{p}{a} \in \mathbb{N}$ a platí $p = ab$, odkud $1 < a < p$, $1 < b < p$. Našli jsme tedy celá čísla $a, b$ tak, že $p \mid ab$ a přitom $p$ nedělí ani $a$, ani $b$. □

**10.7. Základní věta aritmetiky.**



**Věta.** *Libovolné přirozené číslo $n$ je možné vyjádřit jako součin prvočísel, přičemž je toto vyjádření jediné, nebereme-li v úvahu pořadí činitelů. (Je-li $n$ prvočíslo, pak jde o „součin“ jednoho prvočísla, $n = 1$ je součinem prázdné množiny[3] prvočísel)*

**Poznámka.** Jak je uvedeno v části 11.18, dělitelnost je možné obdobným způsobem definovat v libovolném oboru integrity. V některých oborech integrity přitom žádné prvky s vlastností prvočísla (říkáme jim *ireducibilní*) neexistují (např. $\mathbb{Q}$), v jiných sice ireducibilní prvky existují, ale zase tam neplatí věta o jednoznačném rozkladu. Podobné je to se zobecněním výše uvedené Euklidovy věty – prvky splňující $p \mid ab \implies p \mid a$ nebo $p \mid b$ jsou vždy ireducibilní, ale obrácení obecně neplatí. Uveďme alespoň příklad nejednoznačného rozkladu – v $\mathbb{Z}(\sqrt{-5})$ platí:[4] $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. To, že všichni uvedení činitelé jsou skutečně v $\mathbb{Z}(\sqrt{-5})$ ireducibilní, je ovšem třeba zdůvodnit.

Důkaz Základní věty aritmetiky. Nejprve dokážeme úplnou matematickou indukcí, že každé přirozené číslo $n$ je možné vyjádřit součinem prvočísel. Tvrzení je zřejmé pro $n = 1$.

Předpokládejme nyní, že $n \geq 2$ a že jsme již dokázali, že libovolné menší přirozené číslo je možné rozložit na součin prvočísel. Jestliže je $n$ prvočíslo, je tvrzení zřejmé. Pokud $n$ prvočíslo není, pak existuje jeho dělitel $d$, $1 < d < n$. Označíme-li $e = n/d$, platí také $1 < e < n$. Z indukčního předpokladu dostáváme, že $d$ i $e$ je možné vyjádřit jako součin prvočísel, a proto je takto možné vyjádřit i jejich součin $d \cdot e = n$.

Předpokládejme nyní, že platí rovnost součinů $p_1 \cdot p_2 \cdots p_s = q_1 \cdot q_2 \cdots q_t$, kde $p_i$, $q_j$ jsou prvočísla pro všechna $i \in \{1, \ldots, s\}$, $j \in \{1, \ldots, t\}$, a nechť navíc platí $p_1 \leq p_2 \leq \cdots \leq p_s$, $q_1 \leq q_2 \leq \cdots \leq q_t$ a $1 \leq s \leq t$. Indukcí vzhledem k $s$ dokážeme, že $s = t$ a že $p_1 = q_1, \ldots, p_s = q_s$.

Je-li $s = 1$, je $p_1 = q_1 \cdots q_t$ prvočíslo. Pokud by platilo $t > 1$, mělo by číslo $p_1$ dělitele $q_1$ takového, že $1 < q_1 < p_1$ (neboť $q_2 q_3 \cdots q_t > 1$), což není možné. Je tedy $t = 1$ a platí $p_1 = q_1$.

Předpokládejme dále, že $s \geq 2$ a že tvrzení platí pro $s - 1$. Z rovnosti $p_1 \cdot p_2 \cdots p_s = q_1 \cdot q_2 \cdots q_t$, dělí $p_s$ součin $q_1 \cdots q_t$, což je podle Euklidovy věty možné jen tehdy, jestliže $p_s$ dělí nějaké $q_j$

[3] V řeči teorie okruhů jde o jedničku okruhu celých čísel, která je dle obvyklé konvence součinem prázdné množiny prvků okruhu.

[4] Symbol $\mathbb{Z}(\sqrt{-5})$ zde značí rozšíření celých čísel o kořen rovnice $x^2 = -5$, které se definuje obdobně, jako jsem získali komplexní čísla z reálných přidáním čísla $\sqrt{-1}$.

proto $7 \mid n$. Podobně $835 \equiv 3 \pmod{16}$, a tedy

$$n \equiv (3^5+6)^{18} - 1 = (3\cdot 81+6)^{18} - 1 \equiv (3\cdot 1+6)^{18} - 1 = \\ = 9^{18} - 1 = 81^9 - 1 \equiv 1^9 - 1 = 0 \pmod{16},$$

proto $16 \mid n$. Celkem tedy $112 \mid n$, což jsme měli dokázat. □

**10.14.** Dokažte, že pro libovolné prvočíslo $p$ platí:



i) Je-li $k \in \{1, \ldots, p-1\}$, pak $p \mid \binom{p}{k}$.
ii) Jsou-li $a, b \in \mathbb{Z}$, pak $a^p + b^p \equiv (a+b)^p \pmod{p}$.

**Řešení.**

i) Protože binomický koeficient splňuje

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!},$$

přičemž jde o přirozené číslo, víme odtud, že $k!$ dělí součin $p(p-1)\cdots(p-k+1)$. Protože je ale číslo $k!$ nesoudělné s prvočíslem $p$, dostáváme odtud, že $k! \mid (p-1)\cdots(p-k+1)$, odkud již plyne $p \mid \binom{p}{k}$.

ii) Podle binomické věty platí

$$(a+b)^p = a^p + \tbinom{p}{1}a^{p-1}b + \cdots + \tbinom{p}{p-1}ab^{p-1} + b^p.$$

Díky předchozímu bodu platí $\binom{p}{k} \equiv 0 \pmod{p}$ pro libovolné $k \in \{1, \ldots, p-1\}$, odkud již plyne tvrzení. □

**10.15.** Dokažte, že pro libovolná přirozená čísla $m, n$ a libovolná $a, b \in \mathbb{Z}$ taková, že $a \equiv b \pmod{m^n}$, platí

$$a^m \equiv b^m \pmod{m^{n+1}}.$$

**Řešení.** Protože zřejmě platí $m \mid m^n$, dostáváme s využitím vlastnosti (5) z 10.14 rovněž platnost kongruence $a \equiv b \pmod{m}$.

V algebraické identitě

$$a^m - b^m = (a-b)(a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1})$$

jsou proto všechny sčítance ve druhé závorce modulo $m$ kongruentní s $a^{m-1}$, a tedy

$$a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1} \equiv m \cdot a^{m-1} \equiv 0 \pmod{m}.$$

Protože $m^n$ dělí $a-b$ a druhá závorka $a^{m-1}+a^{m-2}+\cdots+ab^{m-2}+b^{m-1}$ je dělitelná $m$, nutně $m^{n+1}$ dělí jejich součin, což znamená, že $a^m \equiv b^m \pmod{m^{n+1}}$. □

pro vhodné $j \in \{1, 2, \ldots, t\}$. Protože $q_j$ je prvočíslo, plyne odtud $p_s = q_j$ (neboť $p_s > 1$). Analogicky se dokáže, že $q_t = p_i$ pro vhodné $i \in \{1, 2, \ldots, s\}$. Odtud

$$q_t = p_i \le p_s = q_j \le q_t,$$

takže $p_s = q_t$. Vydělením obou stran původní rovnosti dostaneme $p_1 \cdot p_2 \cdots p_{s-1} = q_1 \cdot q_2 \cdots q_{t-1}$, a z indukčního předpokladu pak obdržíme $s-1 = t-1$, $p_1 = q_1, \ldots, p_{s-1} = q_{s-1}$. Celkem tedy platí $s = t$ a $p_1 = q_1, \ldots, p_{s-1} = q_{s-1}$, $p_s = q_s$. Jednoznačnost, a tedy i celá věta, je dokázána. □

**10.8. Praktické poznámky.** Jak si ukážeme, je velmi složité



o velkých číslech s jistotou rozhodnout, jde-li o prvočíslo (na druhou stranu je o naprosté většině složených čísel snadné prokázat, že jsou skutečně složená – viz dále v části 10.38). Přesto se v roce 2002 indickým matematikům [5] podařilo dokázat, že problém prvočíselnosti je možné rozhodnout algoritmem s časovou složitostí polynomiálně závislou na počtu cifer vstupního čísla.

Nic podobného se zatím neumí v otázce rozkladu čísla na prvočísla (třebaže se obecně nevěří, že je to možné, exaktní důkaz zatím nebyl podán). Nejrychlejší obecně použitelný faktorizační algoritmus, tzv. *síto v číselném tělese*, je sub-exponenciální časové složitosti $O\left(\mathrm{e}^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$.

Peter Shor v roce 1994 vymyslel algoritmus, který číslo $N$ faktorizuje v kubickém čase (tento algoritmus je tedy časové složitosti $O\left(\log^3 N\right)$) na kvantovém počítači. Je k tomu nicméně třeba sestrojit počítače s dostatečným počtem kvantových bitů (tzv. qubits) – jak je to obtížné, lze vysledovat z toho, ze v roce 2001 se IBM podařilo pomocí kvantového počítače rozložit číslo 15 a v roce 2012 byl dosažen další faktorizační rekord rozkladem čísla 21.

Že je problém rozkladu přirozeného čísla na prvočísla výpočetně složitý, o tom svědčí i (již neplatná) výzva učiněná v roce 1991 firmou RSA Security.[6] Pokud se komukoliv podařilo rozložit čísla označená podle počtu cifer jako RSA-100, ..., RSA-704, RSA-768, ..., RSA-2048, mohl obdržet 1 000,..., 30 000, 50 000, ..., resp. 200 000 dolarů (číslo RSA-100 rozložil v témže roce Arjen Lenstra, číslo RSA-704 bylo rozloženo v roce 2012, některá další ale dosud rozložena nebyla).

Díky jednoznačnosti rozkladu na prvočísla jsme schopni (se



znalostí tohoto rozkladu) snadno odpovědět i na otázky ohledně počtu či součtu dělitelů konkrétního čísla. Stejně snadno dostaneme i (z dřívějška intuitivně známý) postup na výpočet největšího společného dělitele dvou čísel ze znalosti jejich rozkladu na prvočísla.

**Tvrzení.** *Každý kladný dělitel čísla* $a = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$ *je tvaru*

$$p_1^{\beta_1} \cdot \cdots \cdot p_k^{\beta_k},$$

*kde* $\beta_1, \ldots, \beta_k \in \mathbb{N}_0$ *a* $\beta_1 \le \alpha_1$, $\beta_2 \le \alpha_2, \ldots, \beta_k \le \alpha_k$.

*Číslo* $a$ *má tedy právě*

$$\tau(a) = (\alpha_1+1)(\alpha_2+1)\cdot \cdots \cdot (\alpha_k+1)$$

[5] M. Agrawal, N. Kayal, N. Saxena. *PRIMES is in P*. Annals of Mathematics 160 (2): 781–793. 2004.

[6] Viz http://www.rsasecurity.com/rsalabs/node.asp?id=2093.

**10.16.** S využitím předchozího příkladu (viz též příklad ‖10.2‖) dokažte, že:

i) lichá čísla $a$ splňují $a^4 \equiv 1 \pmod{16}$,

ii) pro čísla $a$ nedělitelná třemi platí $a^3 \equiv \pm 1 \pmod 9$.

**Řešení.**

i) Toto tvrzení jsme již dokázali v třetí části příkladu ‖10.2‖. Zde si ukážeme ještě jeden důkaz. Díky části (ii) zmiňovaného příkladu víme, že pro liché číslo $a$ platí $a^2 \equiv 1 \pmod{2^3}$, odkud umocněním na druhou (s využitím výsledku předchozího příkladu) dostaneme $a^4 \equiv 1^2 \pmod{2^4}$.

ii) Umocníme na třetí (se zvýšením exponentu modulu) kongruenci $a \equiv \pm 1 \pmod 3$ a dostaneme $a^3 \equiv \pm 1 \pmod{3^2}$. □

**10.17. Pravidla dělitelnosti.** Všichni si jistě pamatujeme ze školní docházky základní pravidla dělitelnosti (alespoň čísly 2, 3, 4, 5, 6, 9 a 10) na základě dekadického zápisu daného čísla. Jak ale tato pravidla dokázat a dají se nějak rozšířit i na jiná čísla?



Už víme, že se stačí omezit na pravidla dělitelnosti mocninami prvočísel (tedy například dělitelnost šesti testujeme pomocí dělitelnosti 2 a 3).

Pravidlo pro dělitelnost devíti uvádí, že dané číslo je dělitelné devíti, právě když je dělitelný devíti jeho ciferný součet. Dokážeme jej jako důsledek silnějšího tvrzení. Platí totiž, že každé číslo je kongruentní se svým ciferným součtem modulo 9 (speciálně je tedy kongruentní s nulou, právě když je kongruentní s nulou jeho ciferný součet). Dokázat to je ale triviální. Ciferný součet čísla $n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0$ je roven $S(n) = a_k + a_{k-1} + \cdots + a_0$, a protože $10^\ell \equiv 1^\ell = 1 \pmod 9$ pro libovolné $\ell \in \mathbb{N}_0$, dostáváme

$$n = a_k 10^k + \cdots + a_0 \equiv a_k + \cdots + a_0 = S(n) \pmod 9.$$

Stejné odvození funguje i tehdy, nahradíme-li devítku číslem 3.

Velmi podobně pak funguje dosud nezmiňované pravidlo pro dělitelnost 11. Zde totiž platí $10^\ell \equiv (-1)^\ell \pmod{11}$, a tak dostaneme

$$n = a_k 10^k + \cdots + a_0 \equiv a_k(-1)^k + \cdots + a_1(-1) + a_0 \equiv$$
$$\equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) \pmod{11}.$$

Číslo je tedy dělitelné jedenácti, právě když je dělitelný jedenácti rozdíl součtu dekadických cifer na sudých a součtu dekadických cifer na lichých místech.

Pro dělitelnost 7 a 13 lze použít hezký trik. Platí totiž $1001 = 7 \cdot 11 \cdot 13$, proto pro číslo $n = 1000a + b$ platí,

*kladných dělitelů, jejichž součet je*

$$\sigma(a) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

*Nechť $p_1, \ldots, p_k$ jsou navzájem různá prvočísla a $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_k$ nezáporná celá čísla. Označíme-li $\gamma_i = \min\{\alpha_i, \beta_i\}$, $\delta_i = \max\{\alpha_i, \beta_i\}$ pro každé $i = 1, 2, \ldots, k$, pak platí*

$$(p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}, p_1^{\beta_1} \cdot \cdots \cdot p_k^{\beta_k}) = p_1^{\gamma_1} \cdot \cdots \cdot p_k^{\gamma_k},$$
$$[p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}, p_1^{\beta_1} \cdot \cdots \cdot p_k^{\beta_k}] = p_1^{\delta_1} \cdot \cdots \cdot p_k^{\delta_k}.$$

Důkaz. Důkazy všech zmíněných tvrzení jsou jednoduchým důsledkem prvního tvrzení o tom, jak vypadají kladní dělitelé čísla $a$. Pro počet kladných dělitelů pak jednoduchou kombinatorickou úvahou (pravidlo součinu) dostaneme $\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \cdots \cdot (\alpha_k + 1)$. Tvrzení o součtu těchto dělitelů uvidíme, zapíšeme-li si tento součet ve tvaru

$$(1 + p_1 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_k + \cdots + p_k^{\alpha_k})$$

a uvědomíme-li si, že každá závorka v tomto součinu je součtem konečné geometrické řady. Další tvrzení jsou již zřejmá z definice. □

**10.9. Dokonalá čísla a jejich vztah k prvočíslům.**



Se součtem všech kladných dělitelů daného čísla souvisí pojem tzv. *dokonalého čísla*. Řekneme, že $a$ je dokonalé, pokud splňuje podmínku $\sigma(a) = 2a$, resp. slovně, pokud *součet všech kladných dělitelů čísla a menších než a samotné je roven číslu a*.

Takovými čísly jsou např. $6 = 1+2+3$, $28 = 1+2+4+7+14$, 496 a 8128 (jde o všechna dokonalá čísla menší než 10 000).

Lze ukázat, že sudá dokonalá čísla jsou v úzkém vztahu s tzv. *Mersenneho prvočísly*. Platí totiž následující fakt.

**Tvrzení.** *Přirozené číslo $a$ je sudé dokonalé číslo, právě když je tvaru $a = 2^{q-1}(2^q - 1)$, kde $2^q - 1$ je prvočíslo.*

Důkaz. Je-li $a = 2^{q-1}(2^q - 1)$, kde $p = 2^q - 1$ je prvočíslo, pak z předchozího tvrzení plyne

$$\sigma(a) = \frac{2^q - 1}{2 - 1} \cdot (p + 1) = (2^q - 1) \cdot 2^q = 2a.$$

Takové číslo $a$ je tedy dokonalé.

Pro důkaz opačného směru uvažme libovolné sudé dokonalé číslo $a$ a pišme

$$a = 2^k \cdot m, \text{ kde } m, k \in \mathbb{N} \text{ a } 2 \nmid m.$$

Protože je funkce $\sigma$ multiplikativní (viz 10.15), je $\sigma(a) = \sigma(2^k) \cdot \sigma(m) = (2^{k+1} - 1) \cdot \sigma(m)$. Přitom ale z dokonalosti čísla $a$ plyne $\sigma(a) = 2a = 2^{k+1} \cdot m$, odkud

$$2^{k+1} \cdot m = (2^{k+1} - 1) \cdot \sigma(m).$$

Protože je $2^{k+1} - 1$ liché, nutně $2^{k+1} - 1 \mid m$ a můžeme položit $m = (2^{k+1} - 1) \cdot n$ pro vhodné $n \in \mathbb{N}$. Úpravou dostáváme $2^{k+1} \cdot n = \sigma(m)$. Mezi dělitele čísla $m$ přitom patří čísla $m$ i $n$ (a protože $\frac{m}{n} = 2^{k+1} - 1 > 1$, jsou tato čísla nutně různá), proto

$$2^{k+1} \cdot n = \sigma(m) \geq m + n = 2^{k+1} \cdot n,$$

a tedy $\sigma(m) = m + n$. To znamená, že $m$ je prvočíslo s jedinými děliteli $m$ a $n = 1$, odkud $a = 2^k \cdot (2^{k+1} - 1)$, kde $2^{k+1} - 1 = m$ je prvočíslo. □

že $n \equiv -a + b \pmod{m}$, kde $m$ je kterékoliv z čísel 7, 11, 13. Je tedy 2015 dělitelné 13, neboť $015 - 2 = 13$. Podobně 2016 je dělitelné 7, neboť $016 - 2 = 14$ je násobek čísla 7. Stejně bychom mohli zdůvodnit i to, že 2013 je násobek 11, ale dříve uvedené kritérium $11 \mid (3 + 0) - (1 + 2)$ je přece jen elegantnější.

**Využití dělitelnosti při detekci chyb.** Poznamenejme, že dělitelnost jedenácti je často využívána pro tvorbu dekadických kódů, kde jsme schopni detekovat chybu v jedné číslici. Když totiž uděláme takovou chybu při přepisu čísla dělitelného jedenácti, výsledek jistě dělitelný jedenácti nebude (viz výše zmíněné kritérium dělitelnosti jedenácti). Podrobněji v kapitole 11.59 o kódování. Každý si to může vyzkoušet na svém rodném čísle, které by mělo být vždy dělitelné jedenácti.



Podobně čísla bankovních účtů vedených u českých bank musí dle směrnice České národní banky podléhat podobné (jen o málo složitější) proceduře. Jak (transformované) šestimístné předčíslí $a_5a_4a_3a_2a_1a_0$, tak desetimístné číslo účtu $b_9b_8b_7b_6b_5b_4b_3b_2b_1b_0$ musí splňovat podmínku dělitelnosti jedenácti (zde uvedeme pouze pro číslo bez předčíslí):

$$\begin{aligned} 0 \equiv b_9 2^9 + b_8 2^8 + b_7 2^7 + \cdots + b_3 2^3 + b_2 2^2 + b_1 2^1 + b_0 2^0 \equiv \\ \equiv -5b_9 + 3b_8 - 4b_7 - 2b_6 - b_5 + \\ + 5b_4 - 3b_3 + 4b_2 + 2b_1 + b_0 \pmod{11}. \end{aligned}$$

Tuto podmínku lze stručně popsat tak, že dělitelné jedenácti má být číslo chápané jako zápis ve dvojkové soustavě (ovšem s využitím dekadických cifer).

**10.18.** Ověřte, že číslo bankovního účtu Masarykovy univerzity 85636621/0100 je korektně sestaveno.

**Řešení.** Otestujeme podmínku dělitelnosti jedenácti:

$$\begin{aligned} -5b_9 + 3b_8 - 4b_7 - 2b_6 - b_5 + 5b_4 - 3b_3 + 4b_2 + 2b_1 + b_0 \equiv \\ \equiv -4 \cdot 8 - 2 \cdot 5 - 1 \cdot 6 + 5 \cdot 3 - 3 \cdot 6 + 4 \cdot 6 + 2 \cdot 2 + 1 \cdot 1 \equiv \\ \equiv 0 \pmod{11}. \end{aligned}$$

□

**Eulerova funkce.** Eulerova funkce $\varphi$ pro přirozené číslo $m$ udává počet přirozených čísel nesoudělných s $m$ a nepřevyšujících $m$, je tedy definována předpisem



$$\varphi(m) = |\{a \in \mathbb{N} \mid 0 < a \leq m,\ (a, m) = 1\}|.$$

K jejímu efektivnímu vyčíslení je ale třeba znát rozklad čísla $m$ na prvočinitele. V takovém případě pro $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ máme

$$\varphi(m) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}.$$

**Poznámka.** Na druhou stranu, popsat lichá dokonalá čísla se dodnes nepodařilo, dokonce se ani neví, jestli vůbec nějaké liché dokonalé číslo existuje.

Mersenneho prvočísla jsou právě prvočísla tvaru $2^k - 1$. Není bez zajímavosti, že právě Mersenneho prvočísla jsou mezi všemi prvočísly nejlépe „vidět" – pro Mersenneho čísla existuje poměrně jednoduchý a rychlý postup, jak ověřit, že jde o prvočísla. Proto není náhodou, že největší známá prvočísla jsou obvykle tvaru $2^k - 1$.

To, jakým způsobem poměrně efektivně testovat, jsou-li Mersenneho čísla prvočísly, si ukážeme později (viz Lucas-Lehmerův test v části 10.43).

Jakkoliv může být hledání největšího známého prvočísla chápáno jako pochybná zábava bez valného praktického užitku, jednak posunuje hranice matematického poznání a zdokonaluje použité metody (a často i hardware), navíc může přinést benefit i samotným objevitelům (Electronic Frontier Foundation vypsala odměny EFF Cooperative Computing Awards za nalezení prvočísla majícího alespoň $10^6$, $10^7$, $10^8$ a $10^9$ číslic – odměny 50, resp. 100 tisíc dolarů za první dvě kategorie byly vyplaceny v letech 2000, resp. 2009 – v obou případech projektu GIMPS – na další odměny si ještě zřejmě nějaký čas počkáme).

**10.10. Rozložení prvočísel.**



*There are two facts about the distribution of prime numbers. The first is that, [they are] the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision.*

Don Zagier

Nyní se budeme snažit zodpovědět následující otázky: Je prvočísel nekonečně mnoho? Je prvočísel nekonečně mnoho v každé (nebo aspoň některé) aritmetické posloupnosti? Jak jsou prvočísla rozložena mezi přirozenými čísly?

Základní větou, kterou je potřeba v této souvislosti zmínit, je fakt známý již kolem roku 300 př. n.l. Euklidovi.

**10.11. Věta** (Eukleidés)**.** *Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.*

Důkaz. Předpokládejme, že prvočísel je konečně mnoho a označme je $p_1, p_2, \ldots, p_n$. Položme $N = p_1 \cdot p_2 \ldots p_n + 1$. Toto číslo je buď samo prvočíslem nebo je dělitelné nějakým prvočíslem různým od $p_1, \ldots, p_n$ (čísla $p_1, \ldots, p_n$ totiž dělí číslo $N - 1$), což je spor. □

Uveďme nyní docela silné tvrzení, jehož důkaz je sice poměrně pracný (a proto jej zde neuvádíme), ale lze jej provést elementárními prostředky[7].

[7] Viz Wikipedia, *Proof of Bertrand's postulate*, http://en.wikipedia.org/wiki/Proof_of_Bertrand's_postulate (as of July 15, 2013, 12:05 GMT) nebo viz M. Aigner, G. Ziegler, *Proofs from THE BOOK*, Springer, 2009.

Víme tedy zejména, že $\varphi(p^\alpha) = (p-1)\cdot p^{\alpha-1}$ a že pro $(m,n)=1$ platí $\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$.

**10.19.** Vypočtěte $\varphi(72)$.

**Řešení.** $72 = 2^3\cdot 3^2 \implies \varphi(72) = 72\cdot(1-\frac{1}{2})\cdot(1-\frac{1}{3}) = 24$, alternativně $\varphi(72)=\varphi(8)\cdot\varphi(9)=4\cdot 6=24$. □

**10.20.**

i) Určete všechna $n$, pro něž je $\varphi(n)$ liché.

ii) Dokažte, že $\forall n\in\mathbb{N}:\ \varphi(4n+2)=\varphi(2n+1)$.

**Řešení.**

i) Zřejmě je $\varphi(1)=\varphi(2)=1$. Každé $n\geq 3$ je buď dělitelné lichým prvočíslem $p$ (v takovém případě je $\varphi(n)$ dělitelné číslem $p-1$, které je sudé) nebo je $n$ vyšší než první mocninou dvojky (i nyní $\varphi(2^\alpha)=2^{\alpha-1}$ je sudé). Je tedy $\varphi(n)$ liché pouze pro $n=1,2$.

ii) Číslo $2n+1$ je liché, tedy $(2,2n+1)=1$, proto $\varphi(4n+2)=$ $=\varphi(2\cdot(2n+1))=\varphi(2)\cdot\varphi(2n+1)=\varphi(2n+1)$. □

**10.21.** Nalezněte všechna přirozená čísla $m$, pro něž je:



i) $\varphi(m)=30$,
ii) $\varphi(m)=34$,
iii) $\varphi(m)=20$,
iv) $\varphi(m)=\frac{m}{3}$.

**Řešení.** Ve všech případech hledáme vzory konkrétního čísla $a$ ve tvaru $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ a postupujeme následovně:

- Protože $\varphi(m)=(p_1-1)p_1^{\alpha_1-1}\cdots(p_k-1)p_k^{\alpha_k-1}$, musí každé prvočíslo $p$ vystupující v rozkladu $m$ na prvočísla splňovat
$$p-1\mid a.$$
- Podobně každé prvočíslo $p$ vystupující v rozkladu $m$ ve vyšší než první mocnině musí dělit $a$. Přesněji, musí platit $p^{\alpha-1}\mid a$.
- Uvedeným postupem získáme konečnou množinu kandidátů pro $m$, kterou vhodným způsobem eliminujeme.

Řešme tedy úlohy i)-iii):

i) Pro každé prvočíslo $p$ z rozkladu $m$ na prvočinitele musí platit $p-1\mid 30$, tedy $p-1\in\{1,2,3,5,6,10,15,30\}$, což splňují prvočísla $p\in\{2,3,7,11,31\}$, z nichž pouze 2 a 3 mohou v rozkladu vystupovat ve vyšší než první mocnině. Je tedy
$$m=2^\alpha 3^\beta 7^\gamma 11^\delta 31^\varepsilon,$$
kde $\alpha,\beta\in\{0,1,2\}$, $\gamma,\delta,\varepsilon\in\{0,1\}$. Rozbor možností nám dále usnadní, když si uvědomíme, že $\varphi(3)=2$, $\varphi(3^2)=\varphi(7)=6$, $\varphi(11)=10$ jsou všechno čísla

**Věta** (Čebyševova, Bertrandův postulát)**.** *Pro libovolné číslo $n>1$ existuje alespoň jedno prvočíslo $p$ splňující $n<p<2n$.*

Prvočísla jsou relativně rovnoměrně rozložena v tom smyslu, že v libovolné „rozumné“ aritmetické posloupnosti (tj. takové, jejíž členy jsou nesoudělné s diferencí) je jich nekonečně mnoho. Například zbytek 1 po dělení čtyřmi, stejně jako zbytek 3 po dělení čtyřmi dá vždy nekonečně mnoho prvočísel (zbytek 0 nedá samozřejmě žádné prvočíslo a zbytek 2 pouze jediné). Obdobná situace je pak při uvažování zbytků po dělení libovolným jiným přirozeným číslem, jak uvádí následující věta, jejíž důkaz je ovšem velmi obtížný.

**10.12. Věta** (Dirichletova o prvočíslech)**.** *Jsou-li $a$, $m$ nesoudělná přirozená čísla, existuje nekonečně mnoho přirozených čísel $k$ tak, že $mk+a$ je prvočíslo. Jinými slovy, mezi čísly $1\cdot m+a$, $2\cdot m+a$, $3\cdot m+a$, ... existuje nekonečně mnoho prvočísel.*

Uveďme alespoň důkaz tohoto tvrzení ve speciálním případě, který je modifikací Euklidova důkazu nekonečnosti prvočísel.

**Tvrzení.** *Existuje nekonečně mnoho prvočísel tvaru $4k+3$, kde $k\in\mathbb{N}_0$.*

Důkaz. Předpokládejme naopak, že existuje pouze konečně mnoho prvočísel tohoto tvaru a označme je $p_1=3$, $p_2=7$, $p_3=11,\ldots,p_n$. Položme $N=4p_2\cdot p_3\cdot\cdots\cdot p_n+3$. Rozložíme-li $N$ na součin prvočísel, musí v tomto rozkladu (v souladu s výsledkem příkladu ‖10.3‖) vystupovat aspoň jedno prvočíslo $p$ tvaru $4k+3$. V opačném případě by bylo $N$ součinem prvočísel tvaru $4k+1$, proto by i $N$ bylo tvaru $4k+1$, což není pravda. Prvočíslem $p$ ovšem nemůže být žádné z prvočísel $p_1,p_2,\ldots,p_n$, protože pokud by pro nějaké $i\in\{2,\ldots,n\}$ platilo $p_i\mid N$, dostali bychom $p_i\mid 3$. Rovněž $3\nmid N$ a dostáváme tak spor s předpokládanou konečností počtu prvočísel daného tvaru. □

Analogický elementární důkaz lze použít pro prvočísla tvaru $3k+2$ nebo $6k+5$, neprojde ale stejně snadno pro prvočísla tvaru $3k+1$ nebo $4k+1$ (rozmyslete si proč; ve druhém případě to budeme schopni napravit v části 10.32 o kvadratických kongruencích).

Z tvrzení uvedených v této kapitole je možné si udělat hrubou představu o tom, jak „hustě“ se mezi přirozenými čísly prvočísla vyskytují. Přesněji (i když „pouze“ asymptoticky) to popisuje následující velmi důležitá věta, dokázaná nezávisle J. Hadamardem a Ch. J. de la Vallée-Poussinem v roce 1896.

**10.13. Věta** (Prime Number Theorem, věta o hustotě prvočísel)**.** *Nechť $\pi(x)$ udává počet prvočísel menších nebo rovných číslu $x\in\mathbb{R}$. Pak*
$$\pi(x)\sim\frac{x}{\ln x},$$
*tj. podíl funkcí $\pi(x)$ a $x/\ln x$ se pro $x\to\infty$ limitně blíží k 1.*

To, jak dobře odpovídá asymptotický odhad $\pi(x)\sim x/\ln(x)$ realitě v některých konkrétních případech, ukazuje následující tabulka:

| $x$ | $\pi(x)$ | $x/\ln(x)$ | relativní chyba |
|---|---|---|---|
| 100 | 25 | 21,71 | 0,13 |
| 1000 | 168 | 144,76 | 0,13 |
| 10000 | 1229 | 1085,73 | 0,11 |
| 100000 | 9592 | 8685,88 | 0,09 |
| 500000 | 41538 | 38102,89 | 0,08 |

taková, že dělíme-li jimi číslo 30, dostaneme liché číslo větší než 1. Kdyby tedy např. bylo $m = 7 \cdot m_1$, kde $7 \nmid m_1$, pak by muselo platit $\varphi(m_1) = 5$, což, jak víme z předchozího příkladu, nemá řešení.

Dostáváme tedy $\beta = \gamma = \delta = 0$ a $m = 2^\alpha \cdot 31^\varepsilon$, odkud již snadno získáme řešení $m \in \{31, 62\}$.

ii) Podobně jako výše mohou být v rozkladu $m$ pouze prvočísla $p \in \{2, 3\}$, přičemž prvočíslo 3 nejvýše v první mocnině. Protože ale $\frac{34}{\varphi(3)} = 17$, prvočíslo 3 v rozkladu $m$ nebude vůbec. Zbývá tedy možnost $m = 2^\alpha$, pak ale $34 = 2^{\alpha-1}$, což rovněž není možné. Takové $m$ tedy neexistuje.

iii) Pro každé prvočíslo $p$ z rozkladu $m$ na prvočinitele musí platit $p - 1 \mid 20$, tedy $p - 1 \in \{1, 2, 4, 5, 10, 20\}$, což splňují prvočísla $p \in \{2, 3, 5, 11\}$, z nichž pouze 2 a 5 mohou v rozkladu vystupovat ve vyšší než první mocnině. Je tedy

$$m = 2^\alpha 3^\beta 5^\gamma 11^\delta,$$

kde $\alpha \in \{0, 1, 2, 3\}$, $\gamma \in \{0, 1, 2\}$, $\beta, \delta \in \{0, 1\}$.

Nejprve uvažme $\delta = 1$. Pak $\varphi(2^\alpha 3^\beta 5^\gamma) = 2$, odkud snadno $\gamma = 0$ a $(\alpha, \beta) \in \{(2, 0), (1, 1), (0, 1)\}$, což nám dá trojici řešení $m \in \{44, 66, 33\}$.

Dále tedy $\delta = 0$. Je-li $\gamma = 2$, pak $\varphi(2^\alpha 3^\beta) = 1$, odkud $(\alpha, \beta) \in \{(1, 0), (0, 0)\}$. Máme tedy další dvě řešení $m \in \{50, 25\}$.

Je-li $\gamma = 1$, pak stejně jako v minulé úloze dostaneme $\frac{20}{\varphi(5)} = 5$, což je liché číslo a v tomto případě tedy řešení nedostaneme. Podobně pro $\gamma = 0$, neboť ani rovnice $\varphi(2^\alpha) = 20$ řešení nemá. Dostali jsme tak celkem pět řešení $m \in \{25, 33, 44, 50, 66\}$.

iv) Tato úloha je jiného typu než předchozí a musíme k ní proto i jinak přistoupit. Ze vztahu $\varphi(m) = \frac{m}{3}$ vidíme, že $m$ musí být násobek tří (vždyť levá strana je přirozené číslo). Proto hledáme řešení ve tvaru $m = 3^\alpha \cdot n$, kde $3 \nmid n, \alpha \geq 1$. Pak $\varphi(m) = 2 \cdot 3^{\alpha-1} \cdot \varphi(n) = \frac{m}{3} = 3^{\alpha-1} \cdot n$. Po zkrácení dostáváme $2\varphi(n) = n$ nebo ekvivalentně $\varphi(n) = \frac{n}{2}$. Zde nutně $2 \mid n$ a píšeme-li $n = 2^\beta \cdot k$, kde $(k, 6) = 1, \beta \leq 1$, dostaneme $\varphi(k) = k$, což je zřejmě splněno pouze pro $k = 1$.

Řešením úlohy jsou tedy všechna přirozená čísla tvaru $2^\alpha 3^\beta$, kde $\alpha, \beta \geq 1$ . □

**10.22.** Určete všechna dvojciferná čísla $n$, pro něž $9 | \varphi(n)$.

**Řešení.** Uvažujme, jak může vypadat rozklad čísla $n$ na prvočísla. Je-li $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, pak $\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}$ a aby platilo $9 \mid \varphi(n)$, musí být splněna některá z podmínek:



Hustotu rozmístění prvočísel v množině přirozených čísel, rovněž částečně popisuje následující Eulerův výsledek.

**Tvrzení.** *Je-li $P$ množina všech prvočísel, pak*

$$\sum_{p \in P} \frac{1}{p} = \infty.$$

**Poznámka.** Přitom např. $\sum_{n \in \mathbb{N}} \frac{1}{n^2} = \frac{\pi^2}{6}$, což znamená, že prvočísla jsou v $\mathbb{N}$ rozmístěna „hustěji“ než druhé mocniny.

Důkaz. Buď $n$ libovolné přirozené číslo a $p_1, \ldots, p_{\pi(n)}$ všechna prvočísla nepřevyšující $n$. Položme

$$\lambda(n) = \prod_{i=1}^{\pi(n)} \left(1 - \frac{1}{p_i}\right)^{-1}.$$

Jednotlivé činitele lze chápat jako součet geometrické řady, proto

$$\lambda(n) = \prod_{i=1}^{\pi(n)} \left(\sum_{\alpha_i=0}^{\infty} \frac{1}{p_i^{\alpha_i}}\right) = \sum \frac{1}{p_1^{\alpha_1} \cdots p_{\pi(n)}^{\alpha_{\pi(n)}}},$$

kde sčítáme přes všechny $\pi(n)$-tice nezáporných celých čísel $(\alpha_1, \ldots, \alpha_{\pi(n)})$. Protože každé číslo nepřevyšující $n$ se rozkládá pouze na prvočísla z množiny $\{p_1, \ldots, p_{\pi(n)}\}$, je určitě každé takové číslo v tomto součtu zahrnuto. Tedy $\lambda(n) > 1 + \frac{1}{2} + \cdots + \frac{1}{n}$, a protože harmonická řada diverguje (viz příklad ‖5.108‖), je i $\lim_{n \to \infty} \lambda(n) = \infty$.

S využitím rozvoje funkce $\ln(1 + x)$ do mocninné řady (viz příklad ‖6.14‖) dále dostáváme

$$\ln \lambda(n) = -\sum_{i=1}^{\pi(n)} \ln\left(1 - \tfrac{1}{p_i}\right) = \sum_{i=1}^{\pi(n)} \sum_{m=1}^{\infty} \left(m p_i^m\right)^{-1} =$$

$$= p_1^{-1} + \cdots + p_{\pi(n)}^{-1} + \sum_{i=1}^{\pi(n)} \sum_{m=2}^{\infty} \left(m p_i^m\right)^{-1}.$$

Protože vnitřní součet lze shora odhadnout jako

$$\sum_{m=2}^{\infty} \left(m p_i^m\right)^{-1} < \sum_{m=2}^{\infty} p_i^{-m} =$$

$$= p_i^{-2} \left(1 - p_i^{-1}\right)^{-1} \leq 2 p_i^{-2},$$

umíme shora odhadnout i divergující posloupnost $\ln \lambda(n) < \sum_{i=1}^{\pi(n)} p_i^{-1} + 2 \sum_{i=1}^{\pi(n)} p_i^{-2}$. Druhý součet přitom zřejmě konverguje (viz konvergence řady $\sum_{n=1}^{\infty} n^{-2}$), proto musí nutně divergovat první součet $\sum_{i=1}^{\pi(n)} p_i^{-1}$, což jsme chtěli dokázat. □

### 3. Kongruence



Pojem kongruence zavedl C. F. Gauss v roce 1801 ve své knize *Disquisitiones Arithmeticae*. Je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel se ale projevuje zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

i) pro některé $i \in \{1, \dots, k\}$ je $p_i \equiv 1 \pmod 9$,
ii) pro některé $i \in \{1, \dots, k\}$ je $p_i = 3$ a $\alpha_i \geq 3$,
iii) pro některá různá $i, j \in \{1, \dots, k\}$ je $p_i = 3$ a $\alpha_i = 2$ a $p_j \equiv 1 \pmod 3$,
iv) pro některá různá $i, j \in \{1, \dots, k\}$ je $p_i \equiv 1 \pmod 3$ a $p_j \equiv 1 \pmod 3$.

Pokud se (dle zadání) omezíme na čísla $n < 100$, pak podmínce

i) odpovídají prvočísla 19, 37 a 73 (spolu s násobky 38, 57, 76, 95 a 74),
ii) odpovídají čísla $3^3 = 27$, $3^4 = 81$ (spolu s násobkem 54),
iii) odpovídá číslo $3^2 \cdot 7 = 63$,
iv) odpovídá číslo $7 \cdot 13 = 91$. □

**10.23. (Malá) Fermatova věta.** Dokážeme ještě dvěma jinými



způsoby (matematickou indukcí a kombinatorickou úvahou) Fermatovu větu, která udává, že pro $a \in \mathbb{Z}$ a prvočíslo $p$ nedělící $a$ platí $a^{p-1} \equiv 1 \pmod p$.

**Řešení.** Dokážeme nejprve (indukcí vzhledem k $a$), že ekvivalentní tvrzení $a^p \equiv a \pmod p$ platí pro libovolné $a \in \mathbb{N}$ a prvočíslo $p$. Pro $a = 1$ není co dokazovat, dále tedy z platnosti tvrzení pro $a$ dokážeme jeho platnost i pro $a+1$. Z indukčního předpokladu a příkladu ‖10.14‖ dostáváme

$$(a+1)^p \equiv a^p + 1^p \equiv a + 1 \pmod p,$$

což jsme potřebovali dokázat.

Tvrzení dále triviálně platí pro $a = 0$ a v případě $a < 0$, $p = 2$. Pro $a < 0$ a $p$ liché dostaneme z předchozího, protože $-a$ je přirozené číslo, že $-a^p = (-a)^p \equiv -a \pmod p$, odkud již snadno $a^p \equiv a \pmod p$.

Kombinatorický důkaz jde na věc poněkud „od lesa“: podobně jako v úlohách využívajících Burnsideovo lemma (viz příklad ‖11.57‖) máme za úkol určit počet náhrdelníků dané délky (ty vzniknou navlečením několika šperků na šňůrku a jejím svázáním) vytvořených z několika typů šperků s tím, že nerozlišujeme náhrdelníky, které je možné na sebe převést otočením (a liší se tedy jen tím, kde je zavázaný „uzlík“). Vcelku snadno si lze rozmyslet, že navlékáme-li $n$ šperků, lze v některých konstelacích převést náhrdelník sám na sebe při otočení o určitý počet šperků (vždy ale pouze o počet dělící $n$ – např. navlečeme-li 8 šperků dvou druhů, které pravidelně střídáme, pak při otočení o 2,4 nebo 6 obdržíme původní náhrdelník). Předpokládejme nyní, že máme $a$ typů šperků a požadovaný počet použitých šperků na jeden náhrdelník je dán prvočíslem $p$. Zřejmě pro každý náhrdelník využívající alespoň dvou typů šperků dostáváme

### Kongruence

Jestliže dvě celá čísla $a, b$ mají při dělení přirozeným číslem $m$ týž zbytek $r$, kde $0 \leq r < m$, nazývají se $a, b$ *kongruentní modulo* $m$ (též *kongruentní podle modulu* $m$), což zapisujeme

$$a \equiv b \pmod m.$$

V opačném případě řekneme, že $a, b$ nejsou kongruentní modulo $m$, a píšeme

$$a \not\equiv b \pmod m.$$

V případech, kdy je zřejmé, že pracujeme s kongruencemi, často symbol mod vynecháváme a píšeme jen $a \equiv b\,(m)$.

**Lemma.** *Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ jsou následující podmínky ekvivalentní:*

*(1)* $a \equiv b \pmod m$,
*(2)* $a = b + mt$ *pro vhodné* $t \in \mathbb{Z}$,
*(3)* $m \mid a - b$.

Důkaz. (1)⇒(3) Jestliže $a = q_1 m + r$, $b = q_2 m + r$, pak $a - b = (q_1 - q_2)m$.

(3)⇒(2) Jestliže $m \mid a - b$, pak existuje $t \in \mathbb{Z}$ tak, že $m \cdot t = a - b$, tj. $a = b + mt$.

(2)⇒(1) Jestliže $a = b + mt$, pak z vyjádření $b = mq + r$ plyne $a = m(q + t) + r$, tedy $a$ i $b$ mají při dělení číslem $m$ týž zbytek $r$, tj. $a \equiv b \pmod m$. □

**10.14. Základní vlastnosti kongruencí.** Přímo z definice plyne, že kongruence podle modulu $m$ je relací *ekvivalence*.

Dokážeme nyní další vlastnosti kongruencí.

### Vlastnosti kongruencí

(1) Kongruence podle téhož modulu můžeme sčítat. K některé straně kongruence můžeme přičíst libovolný násobek modulu.
(2) Kongruence podle téhož modulu můžeme násobit.
(3) Obě strany kongruence je možné umocnit na totéž přirozené číslo.
(4) Obě strany kongruence můžeme vydělit jejich společným dělitelem, jestliže je tento dělitel nesoudělný s modulem. Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem.
(5) Jestliže kongruence platí podle modulu $m$, platí podle libovolného modulu $d$, který je dělitelem čísla $m$.
(6) Jestliže je jedna strana kongruence a modul dělitelný nějakým celým číslem, musí být tímto číslem dělitelná i druhá strana kongruence.
(7) Jestliže kongruence platí podle modulů $m_1, \dots, m_k$, platí i podle modulu, kterým je nejmenší společný násobek $[m_1, \dots, m_k]$ těchto čísel.

Důkaz. (1) Je-li $a \equiv b \pmod m$ a $c \equiv d \pmod m$, existují podle předchozího lemmatu čísla $s, t \in \mathbb{Z}$ tak, že $a = b + ms$, $c = d + mt$. Pak ovšem $a + c = b + d + m(s + t)$ a opět podle lemmatu $a + c \equiv b + d \pmod m$.

Sečteme-li kongruenci $a \equiv b \pmod m$ s kongruencí $mk \equiv 0 \pmod m$, jejíž platnost je zřejmá, dostaneme $a + mk \equiv b \pmod m$.

různým umístěním uzlíku $p$ různých $p$-tic šperků na šňůrce (což ale není případ náhrdelníků sestavených pouze z jednoho typu šperku). Vidíme tedy, že počet různých náhrdelníků je roven

$$\frac{a^p - a}{p} + a,$$

což zejména znamená, že musí platit $p \mid a^p - a$.

Například pro hodnoty $a = 2, p = 5$ tak určujeme počet náhrdelníků dvou typů šperků $(A, B)$ délky pět. Dáme-li ze všech $2^5$ různě navlečených šňůrek stranou 2 náhrdelníky tvořené pouze jedním typem $(AAAAA, BBBBB)$, pak dále máme $\frac{2^5-2}{5} = 6$ náhrdelníků, které na sebe nelze převést otáčením $(ABBBB, AABBB, AAABB, AAAAB, ABABB, AABAB)$. □

**Eulerova věta a řády čísel modulo $m$.** Díky Eulerově větě máme pro každé $a \in \mathbb{Z}$ nesoudělné s modulem $m$ zajištěnu existenci jeho řádu, tj. nejmenšího přirozeného čísla $n$ splňujícího $a^n \equiv 1 \pmod m$. Významná jsou zejména ta čísla $a$, která mají řád roven $\varphi(m)$, tzv. primitivní kořeny modulo $m$.

**10.24.** Určete poslední dvojčíslí čísla $7^{2013}$.



**Řešení.** Snadno se uvidí, že řád 7 modulo 100 je roven čtyřem – např. proto, že $7^2 = 49$ a $49^2 = (50-1)^2 = 50^2 - 2 \cdot 50 + 1 \equiv 1 \pmod{100}$. Stačí tedy určit zbytek $r$ čísla 2013 po dělení čtyřmi, pak totiž $7^{2013} \equiv 7^r \pmod{100}$. Ale zřejmě $r = 1$, proto je hledané poslední dvojčíslí rovno 07. □

*10.25.* Určete poslední cifru čísel

i) $3^{5^{7^9}}$,

ii) $37^{37^{37}}$,

iii) $12^{13^{14}}$.

○

**10.26.**

i) Určete zbytek po dělení čísla $2^{50} + 3^{50} + 4^{50}$ číslem 17.

ii) Určete zbytek po dělení čísla $2^{181} + 3^{181} + 5^{181}$ číslem 37.

**Řešení.**

i) Podle Fermatovy věty je $2^{16} \equiv 3^{16} \equiv 4^{16} \equiv 1 \pmod{17}$. Protože $50 \equiv 2 \pmod{16}$, dostáváme
$2^{50} + 3^{50} + 4^{50} \equiv 2^2 + 3^2 + 4^2 \equiv 12 \pmod{17}$.

ii) Podobně $2^{36} \equiv 3^{36} \equiv 5^{36} \equiv 1 \pmod{37}$, proto
$2^{181} + 3^{181} + 5^{181} \equiv 2 + 3 + 5 \equiv 10 \pmod{37}$. □

*10.27.* Dokažte, že pro všechna lichá $n \in \mathbb{N}$ platí $n \mid 2^{n!} - 1$. ○

(2) Je-li $a \equiv b \pmod m$ a $c \equiv d \pmod m$, existují $s, t \in \mathbb{Z}$ tak, že $a = b + ms$, $c = d + mt$. Pak

$$ac = (b + ms)(d + mt) = bd + m(bt + ds + mst),$$

odkud dostáváme $ac \equiv bd \pmod m$.

(3) Nechť $a \equiv b \pmod m$, pak pro přirozené číslo $n$ ze vztahu

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$$

plyne rovněž $a^n \equiv b^n \pmod m$.

(4) Předpokládejme, že $a \equiv b \pmod m$, $a = a_1 \cdot d$, $b = b_1 \cdot d$ a $(m, d) = 1$. Podle lemmatu je rozdíl $a - b = (a_1 - b_1) \cdot d$ dělitelný číslem $m$, a protože $(m, d) = 1$, je podle lemmatu 10.5 číslo $a_1 - b_1$ také dělitelné číslem $m$. Odtud plyne $a_1 \equiv b_1 \pmod m$. Dále pokud $ad \equiv bd \pmod{md}$, tj. $md \mid ad - bd$, dostáváme přímo z definice dělitelnosti, že $m \mid a - b$.

(5) Jestliže $a \equiv b \pmod m$, je $a - b$ násobkem $m$, a proto také násobkem dělitele $d$ čísla $m$, odkud $a \equiv b \pmod d$.

(6) Předpokládejme, že $a \equiv b \pmod m$, $b = b_1 d$, $m = m_1 d$. Pak existuje $t \in \mathbb{Z}$ tak, že $a = b + mt = b_1 d + m_1 dt = (b_1 + m_1 t)d$, a tedy $d \mid a$.

(7) Je-li $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, …, $a \equiv b \pmod{m_k}$, pak je rozdíl $a - b$ společným násobkem čísel $m_1, m_2, \ldots, m_k$, a je tedy dělitelný jejich nejmenším společným násobkem $[m_1, m_2, \ldots, m_k]$, odkud plyne $a \equiv b \pmod{[m_1, \ldots, m_k]}$.

□

**Poznámka.** Některé vlastnosti kongruencí jsme dosud používali, aniž bychom to explicitně zmínili – výsledek příkladu ‖10.3‖ lze nyní přeformulovat do tvaru „jestliže $a \equiv 1 \pmod m$, $b \equiv 1 \pmod m$, pak také $ab \equiv 1 \pmod m$“, což je speciální případ bodu (2) z předchozího tvrzení.

Nejde o náhodu, protože libovolné tvrzení používající kongruence můžeme přepsat pomocí dělitelnosti. Užitečnost kongruencí netkví v tom, že bychom pomocí nich mohli řešit více úloh, než bez nich, ale v tom, že jde o velmi vhodný způsob zápisu, který výrazným způsobem zjednodušuje jak vyjadřování, tak některé prováděné úvahy.

**10.15. Aritmetické funkce.**



Aritmetickou funkcí zde rozumíme jakoukoliv funkci, jejímž definičním oborem je množina přirozených čísel.

**Definice.** Rozložme přirozené číslo $n$ na prvočísla: $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Hodnotu *Möbiovy funkce* $\mu(n)$ definujeme rovnu 0, pokud pro některé $i$ platí $\alpha_i > 1$ a rovnu $(-1)^k$ v opačném případě. Dále definujeme $\mu(1) = 1$ (což je v souladu s dřívější konvencí, že 1 se rozkládá na „součin“ nulového počtu prvočísel).

**Příklad.** $\mu(4) = \mu(2^2) = 0$, $\mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1$, $\mu(2) = \mu(3) = -1$.

Dokážeme nyní několik důležitých vlastností Möbiovy funkce, zejména tzv. *Möbiovu inverzní formuli*.

**Lemma.** *Pro $n \in \mathbb{N} \setminus \{1\}$ platí $\sum_{d \mid n} \mu(d) = 0$.*

Důkaz. Zapíšeme-li $n$ ve tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, pak všichni dělitelé $d$ čísla $n$ jsou tvaru $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$, kde $0 \le \beta_i \le \alpha_i$ pro

**10.28.**

i) Určete poslední číslici čísla $7^{9^{5^7}}$.

ii) Určete zbytek po dělení jedenácti čísla $15^{14^{13}}$.

**Řešení.**

i) Řád 7 modulo 100 je podle příkladu ‖10.24‖ roven čtyřem, proto stačí zjistit zbytek (nehorázně velkého) exponentu po dělení čtyřmi. Protože platí $9 \equiv 1 \pmod 4$, dává i celý exponent zbytek 1 po dělení čtyřmi, a proto je hledaná poslední číslice rovna $7^1 = 7$.

ii) Řád čísla $15 \equiv 4 \pmod{11}$ je roven 5 (což zjistíme buď přímým výpočtem, nebo protože 2 je primitivní kořen modulo 11 (viz též příklad ‖10.32‖), pak z věty 10.18 dostaneme, že řád $4 = 2^2$ je roven $\frac{10}{(10,2)} = 5$). Stačí tedy určit zbytek exponentu modulo 5, tedy

$$14^{13} \equiv (-1)^{13} = -1 \equiv 4 \pmod 5,$$

proto je hledaný zbytek roven $4^4 = 2^8 = 256 \equiv 6 - 5 + 2 = 3 \pmod{11}$. (Mohli jsme též postupovat tak, že $4^4 \equiv 4^{-1} \equiv 3 \pmod{11}$.) □

**10.29.** Určete poslední dvě cifry v dekadickém rozvoji čísla $14^{14^{14}}$.



**Řešení.** Zajímá nás zbytek čísla $a = 14^{14^{14}}$ po dělení 100. Protože je ale $(14, 100) > 1$, nelze hovořit o řádu čísla 14 modulo 100 a raději proto rozložíme modul na nesoudělné faktory $100 = 4 \cdot 25$. Zřejmě $4 \mid a$, stačí tedy zjistit, s čím je $a$ kongruentní modulo 25. Podle Eulerovy věty je

$$14^{\varphi(25)} = 14^{20} \equiv 1 \pmod{25},$$

proto nás bude zajímat zbytek čísla $14^{14}$ po dělení $20 = 4 \cdot 5$. Opět triviálně $4 \mid 14^{14}$ a dále $14^{14} \equiv (-1)^{14} = 1 \pmod 5$, proto je

$$14^{14} \equiv 16 \pmod{20}.$$

Celkem tedy

$$14^{14^{14}} \equiv 14^{16} = 2^{16} \cdot 7^{16} \pmod{25}.$$

Další výpočty si značně usnadníme, uvědomíme-li si, že

$$7^2 \equiv -1 \pmod{25} \text{ a } 2^5 \equiv 7 \pmod{25}.$$

Pak totiž

$$14^{14^{14}} \equiv 2^{16} \cdot 7^{16} \equiv (2^5)^3 \cdot 2 \cdot 7^{16} \equiv$$
$$\equiv 7^3 \cdot 2 \cdot 7^{16} \equiv 2 \cdot 7^{19} \equiv 2 \cdot (-1)^9 \cdot 7 = 11 \pmod{25}.$$

Hledáme tedy číslo menší než 100, které je násobkem čtyř a po dělení 25 dává zbytek 11 – takovým je zřejmě pouze číslo 36. □

všechna $i \in \{1, \dots, k\}$. Proto

$$\sum_{d|n} \mu(d) = \sum_{\substack{(\beta_1,\dots,\beta_k)\in(\mathbb{N}\cup\{0\})^k \\ 0\le\beta_i\le\alpha_i}} \mu\left(p_1^{\beta_1}\cdots p_k^{\beta_k}\right) =$$
$$= \sum_{(\beta_1,\dots,\beta_k)\in\{0,1\}^k} \mu\left(p_1^{\beta_1}\cdots p_k^{\beta_k}\right) =$$
$$= \binom{k}{0} + \binom{k}{1}\cdot(-1) + \binom{k}{2}\cdot(-1)^2 + \cdots + \binom{k}{k}\cdot(-1)^k =$$
$$= (1 + (-1))^k = 0.$$

přičemž jsme ve třetí rovnosti využili kombinatorickou úvahu – sčítanec $\binom{k}{\ell}(-1)^\ell$ udává příspěvek dělitelů $d = p_1^{\beta_1}\cdots p_k^{\beta_k}$ s vlastností, že právě $\ell$ z exponentů $\beta_1, \dots, \beta_k$ je rovno jedné; těch je totiž $\binom{k}{\ell}$ a pro každý z nich platí, že $\mu(p_1^{\beta_1}\cdots p_k^{\beta_k}) = (-1)^\ell$. □

S Möbiovou funkcí úzce souvisí pojem Dirichletův součin (též Dirichletova konvoluce).

**Definice.** Buďte $f, g$ aritmetické funkce. Jejich *Dirichletův součin* je definován předpisem

$$(f \circ g)(n) = \sum_{d|n} f(d)\cdot g\left(\tfrac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1)\cdot g(d_2).$$

**Lemma.** *Dirichletův součin je asociativní.*

Důkaz.

$$((f\circ g)\circ h)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1)\cdot g(d_2)\cdot h(d_3) = (f\circ(g\circ h))(n)$$

□

**Příklad.** Definujme dvě pomocné funkce $\mathbb{I}$ a $I$ předpisem $\mathbb{I}(1) = 1$, $\mathbb{I}(n) = 0$ pro všechna $n > 1$, resp. $I(n) = 1$ pro všechna $n \in \mathbb{N}$. Pak pro každou aritmetickou funkci $f$ platí:

$$f\circ\mathbb{I} = \mathbb{I}\circ f = f \quad \text{a} \quad (I\circ f)(n) = (f\circ I)(n) = \sum_{d|n} f(d).$$

Dále platí $I\circ\mu = \mu\circ I = \mathbb{I}$, neboť

$$(I\circ\mu)(n) = \sum_{d|n} I(d)\mu\left(\tfrac{n}{d}\right) = \sum_{d|n} I\left(\tfrac{n}{d}\right)\mu(d) =$$
$$= \sum_{d|n}\mu(d) = 0 \quad \text{pro všechna } n > 1$$

podle lemmatu za definicí Möbiovy funkce (pro $n = 1$ je tvrzení zřejmé).

**Věta** (Möbiova inverzní formule)**.** *Nechť je aritmetická funkce $F$ definovaná pomocí aritmetické funkce $f$ předpisem $F(n) = \sum_{d|n} f(d)$. Pak lze funkci $f$ vyjádřit ve tvaru*

$$f(n) = \sum_{d|n}\mu\left(\tfrac{n}{d}\right)\cdot F(d).$$

Důkaz. Vztah $F(n) = \sum_{d|n} f(d)$ lze jiným způsobem zapsat jako $F = f\circ I$. Proto $F\circ\mu = (f\circ I)\circ\mu = f\circ(I\circ\mu) = f\circ\mathbb{I} = f$, což je tvrzení věty. □

**Definice.** *Multiplikativní funkcí* přirozených čísel rozumíme takovou aritmetickou funkci, která pro všechny dvojice nesoudělných čísel $a, b \in \mathbb{N}$ splňuje

$$f(a\cdot b) = f(a)\cdot f(b).$$

**10.30.** Určete poslední tři cifry čísla $12^{10^{11}}$.

**Řešení.** Podobně jako v předchozím příkladu budeme zkoumat zbytky po dělení nesoudělnými čísly 125 a 8. Víme, že $(12, 125) = 1$ a $\varphi(125) = 100$, proto

$$12^{10^{11}} \equiv 12^{10^2 \cdot 10^9} = \left(12^{10^2}\right)^{10^9} \equiv 1^{10^9} \equiv 1 \pmod{125}.$$

Protože $4 \mid 12$, je $12^{10^{11}}$ dělitelné dokonce číslem $4^{10^{11}}$, tím spíše i číslem 8, tedy $12^{10^{11}} \equiv 0 \pmod 8$. Podle Čínské zbytkové věty existuje mezi čísly $0, 1, \ldots, 999$ právě jedno takové, že dává zbytek 1 po dělení číslem 125 a je dělitelné osmi. To je číslo 376 (toto číslo můžeme snadno najít například tak, že procházíme násobky čísla 125, zvětšíme je o jedna a poté zkoumáme dělitelnost osmi). Poslední tři cifry čísla $12^{10^{11}}$ jsou tedy 376. □

**10.31.** Rozhodněte, pro která přirozená čísla $n$ je číslo $5^n - 4^n - 3^n$ dělitelné jedenácti.



**Řešení.** Řády čísel 3, 4 i 5 jsou ve všech případech rovny pěti, proto stačí prozkoumat $n \in \{0, 1, 2, 3, 4\}$. Z tabulky

| $n$ | | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|
| $5^n$ | mod 11 | 1 | 5 | 3 | 4 | 9 |
| $4^n$ | mod 11 | 1 | 4 | 5 | 9 | 3 |
| $3^n$ | mod 11 | 1 | 3 | 9 | 5 | 4 |

je vidět, že jedině v případě $n \equiv 2 \pmod 5$ je $3-5-9 \equiv 0 \pmod{11}$.

Řešením jsou tedy všechna přirozená čísla splňující $n \equiv 2 \pmod 5$. □

**10.32. Primitivní kořeny.** Ukažte, že neexistují primitivní kořeny modulo 8 a nalezněte některý primitivní kořen modulo 11.

**Řešení.** Sudá čísla zřejmě nemohou být primitivními kořeny modulo 8, stačí tedy vyzkoušet lichá. Lehce se spočítá $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$ a přitom $\varphi(8) = 4 > 2$.

Ověříme, že 2 je primitivním kořenem modulo 11. Řád čísla 2 dělí $\varphi(11) = 10$, proto stačí ověřit, že $2^2 \not\equiv 1 \pmod{11}$ a $2^5 = 32 \equiv -1 \not\equiv 1 \pmod{11}$. Je tedy skutečně 10 řádem čísla 2 modulo 11. □

**10.33.** Postupně určíme (s využitím tvrzení z teoretické části) primitivní kořeny modulo $41$, $41^2$ a $2 \cdot 41^2$.



**Řešení.** Protože $\varphi(41) = 40 = 2^3 \cdot 5$, je libovolné celé číslo $g$, které je s 41 nesoudělné, primitivním kořenem modulo 41 právě tehdy, když

$$g^{20} \not\equiv 1 \pmod{41} \wedge g^8 \not\equiv 1 \pmod{41}.$$

**Příklad.** Multiplikativními funkcemi jsou (jak se lze snadno přesvědčit přímo z jejich definice) např. funkce $\sigma(n)$, $\tau(n)$, či $\mu(n)$ nebo, jak brzy dokážeme, tzv. Eulerova funkce $\varphi(n)$.

EULEROVA FUNKCE $\varphi$

Pro přirozené číslo $n$ definujme Eulerovu funkci $\varphi$ předpisem

$$\varphi(n) = |\{a \in \mathbb{N} \mid 0 < a \leq n,\ (a, n) = 1\}|$$

**Příklad.** $\varphi(1) = 1, \varphi(5) = 4, \varphi(6) = 2$. Je-li p prvočíslo, je zřejmě $\varphi(p) = p - 1$ (všechna přirozená čísla menší než $p$ jsou s ním nesoudělná).

Nyní dokážeme několik důležitých tvrzení o funkci $\varphi$.

**Lemma.** *Nechť $n \in \mathbb{N}$. Pak $\sum_{d \mid n} \varphi(d) = n$.*

DŮKAZ. Uvažme $n$ zlomků

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}.$$

Zkrátíme-li zlomky na základní tvar a seskupíme podle jmenovatelů, snadno dostaneme právě uvedené tvrzení. □

**Věta.** *Nechť $n \in \mathbb{N}$, jehož prvočíselný rozklad je tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Pak*

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

DŮKAZ. S využitím předchozího lemmatu a Möbiovy inverzní formule dostáváme

$$\begin{aligned}\varphi(n) &= \sum_{d \mid n} \mu(d) \frac{n}{d} = \\ &= n - \frac{n}{p_1} - \cdots - \frac{n}{p_k} + \cdots + (-1)^k \frac{n}{p_1 \cdots p_k} = \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

□

**Poznámka.** Předchozí výsledek lze obdržet i bez použití Möbiovy inverzní formule pomocí principu inkluze a exkluze na základě zjištění počtu čísel soudělných s $n$ v určitém intervalu.

Z věty přímo vyplývá, že Eulerova funkce je multiplikativní aritmetická funkce.

**Důsledek.** *Nechť $a, b \in \mathbb{N}$, $(a, b) = 1$. Pak*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

**Poznámka.** Rovněž toto tvrzení lze odvodit nezávisle na základě poznatku $(n, ab) = 1 \iff (n, a) = 1 \wedge (n, b) = 1$. Spolu se snadno odvoditelným výsledkem

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1) \cdot p^{\alpha-1}$$

pak lze odvodit vztah pro výpočet $\varphi$ již třetím způsobem.

Vyzkoušejme tedy potenciální kandidáty po řadě od nejmenšího:

$$\begin{aligned}
g=2:\quad & 2^8=2^5\cdot 2^3\equiv -9\cdot 8\equiv 10 \pmod{41},\\
& 2^{20}=(2^5)^4\equiv(-9)^4=81^2\equiv(-1)^2=1 \pmod{41},\\
g=3:\quad & 3^8=(3^4)^2\equiv(-1)^2=1 \pmod{41},\\
g=4:\quad & \text{řád } 4=2^2 \text{ vždy dělí řád } 2,\\
g=5:\quad & 5^8=(5^2)^4\equiv(-2^4)^4=2^{16}=(2^8)^2\equiv\\
& \equiv 10^2\equiv 18 \pmod{41},\\
& 5^{20}=(5^2)^{10}\equiv(-2^4)^{10}=2^{40}=(2^{20})^2\equiv 1 \pmod{41},\\
g=6:\quad & 6^8=2^8\cdot 3^8\equiv 10\cdot 1=10 \pmod{41},\\
& 6^{20}=2^{20}\cdot 3^{20}\equiv 2^{20}\cdot(3^8)^2\cdot 3^4\equiv\\
& \equiv 1\cdot 1\cdot(-1)=-1 \pmod{41}.
\end{aligned}$$

Dokázali jsme tak, že 6 je (nejmenší kladný) primitivní kořen modulo 41 (pokud by nás zajímaly i ostatní primitivní kořeny modulo 41, tak bychom je dostali umocněním 6 na všechna čísla od 1 do 40, která jsou se 40 nesoudělná – je jich právě $\varphi(40)=\varphi(2^3\cdot 5)=16$ a jsou jimi tyto zbytky modulo 41: $\pm 6, \pm 7, \pm 11, \pm 12, \pm 13, \pm 15, \pm 17, \pm 19$).

Dokážeme-li nyní, že $6^{40}\not\equiv 1 \pmod{41^2}$, budeme vědět, že 6 je i primitivním kořenem modulo libovolná mocnina 41 (pokud bychom „měli smůlu“ a vyšlo by, že $6^{40}\equiv 1 \pmod{41^2}$, pak by primitivním kořenem modulo $41^2$ bylo číslo $47=6+41$). Při ověření podmínky si vypomůžeme několika triky (tzv. modulární reprezentace čísel), abychom se obešli bez manipulace s velkými čísly.

Nejprve vypočtěme zbytek po dělení $6^8$ číslem $41^2$; k tomu se nám bude hodit vypočítat zbytek po dělení čísel $2^8$ a $3^8$:

$$\begin{aligned}
& 2^8=256=6\cdot 41+10 \pmod{41^2},\\
& 3^8=(3^4)^2=(2\cdot 41-1)^2\equiv -4\cdot 41+1 \pmod{41^2}.
\end{aligned}$$

Pak

$$\begin{aligned}
6^8=2^8\cdot 3^8&\equiv(6\cdot 41+10)(-4\cdot 41+1)\equiv\\
&\equiv -34\cdot 41+10\equiv 7\cdot 41+10 \pmod{41^2}
\end{aligned}$$

a

$$\begin{aligned}
6^{40}=(6^8)^5&\equiv(7\cdot 41+10)^5\equiv(10^5+5\cdot 7\cdot 41\cdot 10^4)=\\
&=10^4(10+35\cdot 41)\equiv(-2\cdot 41-4)(-6\cdot 41+10)\equiv\\
&\equiv(4\cdot 41-40)=124\not\equiv 1 \pmod{41^2}.
\end{aligned}$$

Přitom jsme využili toho, že $10^4=6\cdot 41^2-86$, tj. $10^4\equiv -2\cdot 41-4 \pmod{41^2}$.

**10.16. Malá Fermatova věta, Eulerova věta.** Tato tvrzení patří mezi nejdůležitější výsledky elementární teorie čísel a budeme je velmi často využívat v dalších nejen teoretických, ale zejména i praktických, úlohách.



**Věta** (Fermatova, Malá Fermatova)**.** *Nechť $a\in\mathbb{Z}$, $p$ prvočíslo, $p\nmid a$. Pak*

$$a^{p-1}\equiv 1 \pmod{p}.$$

Důkaz. Tvrzení vyplyne jako snadný důsledek Eulerovy věty (a spolu s ní je tak důsledkem obecnějšího tvrzení Lagrangeovy věty 11.10). Dá se ale dokázat i přímo (např. matematickou indukcí nebo kombinatoricky, jak je uvedeno v příkladu ‖10.23‖). □

Někdy se Fermatova věta uvádí v následující podobě, která je zřejmě ekvivalentní původnímu tvrzení.

**Důsledek.** *Nechť $a\in\mathbb{Z}$, $p$ prvočíslo. Pak*

$$a^p\equiv a \pmod{p}.$$

Předtím než zformulujeme a dokážeme Eulerovu větu, zaveďme ještě potřebné pojmy.

Soustava zbytků

*Úplná soustava zbytků* modulo $m$ je libovolná $m$-tice čísel po dvou nekongruentních modulo $m$ (nejčastěji je používána $m$-tice $0,1,\dots,m-1$ nebo pro lichá $m$ její „symetrická“ varianta $-\frac{m-1}{2},\dots,-1,0,1,\dots,\frac{m-1}{2}$).

*Redukovaná soustava zbytků* modulo $m$ je libovolná $\varphi(m)$-tice čísel nesoudělných s $m$ a po dvou nekongruentních modulo $m$.

**Lemma.** *Nechť $x_1,x_2,\dots,x_{\varphi(m)}$ tvoří redukovanou soustavu zbytků modulo $m$. Je-li $a\in\mathbb{Z}$, $(a,m)=1$, pak i čísla $a\cdot x_1,\dots,a\cdot x_{\varphi(m)}$ tvoří redukovanou soustavu zbytků modulo $m$.*

Důkaz. Protože $(a,m)=1$ a $(x_i,m)=1$, platí $(a\cdot x_i,\,m)=1$. Dále kdyby pro nějaká $i$, $j$ platilo $a\cdot x_i\equiv a\cdot x_j \pmod{m}$, po vydělení obou stran kongruence číslem $a$ nesoudělným s $m$ bychom dostali $x_i\equiv x_j \pmod{m}$, což by znamenalo, že ani původní $\varphi(m)$-tice netvořila redukovanou soustavu zbytků. □

**Věta** (Eulerova)**.** *Nechť $a\in\mathbb{Z}$, $m\in\mathbb{N}$, $(a,m)=1$. Pak*

$$a^{\varphi(m)}\equiv 1 \pmod{m}.$$

Důkaz. Buď $x_1,x_2,\dots,x_{\varphi(m)}$ libovolná redukovaná soustava zbytků modulo $m$. Podle předchozího lemmatu je i $a\cdot x_1,\dots,a\cdot x_{\varphi(m)}$ redukovaná soustava zbytků modulo $m$. Platí tedy, že pro každé $i\in\{1,2,\dots,\varphi(m)\}$ existuje jediné $j\in\{1,2,\dots,\varphi(m)\}$ tak, že $a\cdot x_i\equiv x_j \pmod{m}$. Vynásobením těchto kongruencí dostáváme $(a\cdot x_1)\cdot(a\cdot x_2)\cdots(a\cdot x_{\varphi(m)})\equiv x_1\cdot x_2\cdots x_{\varphi(m)} \pmod{m}$. Po úpravě

$$a^{\varphi(m)}\cdot x_1\cdot x_2\cdots x_{\varphi(m)}\equiv x_1\cdot x_2\cdots x_{\varphi(m)} \pmod{m}$$

a vydělením číslem $x_1\cdot x_2\cdots x_{\varphi(m)}$ dostaneme požadované. □

**Poznámka.** Eulerova věta je rovněž důsledkem Lagrangeovy věty (viz 11.10) uplatněným na grupu $(\mathbb{Z}_m^\times,\cdot)$. Důkaz Eulerovy věty využíval toho, že násobení číslem $a$ nesoudělným s $m$ je v algebraické řeči automorfismem grupy $(\mathbb{Z}_m^\times,\cdot)$.

Je tedy 6 primitivním kořenem modulo $41^2$ a protože je to sudé číslo, je primitivním kořenem modulo $2 \cdot 41^2$ číslo $1687 = 6 + 41^2$ (nejmenším kladným primitivním kořenem modulo $2 \cdot 41^2$ je přitom číslo 7). □

**Möbiova inverzní formule a ireducibilní polynomy.** V teoretické



části dokazujeme vlastnosti Eulerovy funkce pomocí tzv. Möbiovy inverzní formule.

Tato formule ve svém standardním tvaru dává do souvislosti vyjádření aritmetické funkce přirozených čísel $F$ pomocí funkce $f$ ve tvaru

$$F(n) = \sum_{d|n} f(d)$$

s inverzním vyjádřením funkce $f$ pomocí funkce $F$ ve tvaru

$$f(n) = \sum_{d|n} \mu(\tfrac{n}{d}) \cdot F(d).$$

Hodnota funkce $\mu(n)$ je určena rozkladem jejího argumentu na prvočinitele takto:

- je-li v rozkladu některé prvočíslo ve vyšší než první mocnině, pak je $\mu(n) = 0$,
- jinak je $\mu(n) = (-1)^k$, kde $k$ je počet prvočísel v rozkladu.

Tuto formuli lze přitom zobecnit mnoha způsoby – zejména platí v situaci, kdy jsou $F$ a $f$ funkcemi z $\mathbb{N}$ do libovolné abelovské grupy $(G, \cdot)$. V takovém případě má (při chápání operace v $G$ jako multiplikativní) formule tvar

$$f(n) = \sum_{d|n} F(d)^{\mu\left(\frac{n}{d}\right)}.$$

Ukažme si použití Möbiovy inverzní formule na komplexnějším příkladu z teorie konečných těles. Uvažme $p$-prvkové těleso $\mathbb{F}_p$ (tedy okruh zbytkových tříd modulo libovolné prvočíslo $p$) a zkoumejme počet $N_d$ normovaných ireducibilních polynomů daného stupně $d$ nad tímto tělesem. Označme $S_d(x)$ součin všech takových polynomů. Z teorie konečných těles si vypůjčíme (nepříliš těžké) tvrzení, které říká, že pro libovolné $n \in \mathbb{N}$ platí

$$x^{p^n} - x = \prod_{d|n} S_d(x).$$

Porovnáním stupňů polynomů na obou stranách dostaneme vztah

$$p^n = \sum_{d|n} dN_d,$$

odkud ihned aplikací standardní Möbiovy inverzní formule dostaneme

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

S Eulerovou funkcí a Eulerovou větou úzce souvisí důležitý pojem *řád čísla modulo m* – i v tomto případě jde jen o jinak nazvaný řád prvku v grupě invertibilních zbytkových tříd modulo $m$:

ŘÁD ČÍSLA

Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$ $(a, m) = 1$. *Řádem čísla a modulo m* rozumíme nejmenší přirozené číslo $n$ splňující

$$a^n \equiv 1 \pmod{m}.$$

To, že je řád vůbec definován, plyne z Eulerovy věty – pro každé číslo nesoudělné s modulem je totiž jistě jeho řád nejvýše roven $\varphi(m)$. Jak později uvidíme, velmi důležitá jsou právě ta čísla, jejichž řád je roven právě $\varphi(m)$ – tato čísla nazýváme primitivními kořeny modulo $m$ a hrají důležitou roli mj. při řešení binomických kongruencí. Tento pojem je přitom jen jiným názvem pro generátor grupy $(\mathbb{Z}_m^\times, \cdot)$.

**Příklad.** Řád čísla 2 modulo 7 je roven 3, neboť $2^1 = 2 \not\equiv 1 \pmod 7$, $2^2 = 4 \not\equiv 1 \pmod 7$, $2^3 = 8 \equiv 1 \pmod 7$.

Uveďme nyní několik tvrzení udávajících vlastnosti řádu čísla modulo $m$:

**Lemma.** *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. Jestliže $a \equiv b \pmod m$, pak obě čísla $a, b$ mají stejný řád modulo $m$.*

DŮKAZ. Umocněním kongruence $a \equiv b \pmod m$ na $n$-tou dostaneme $a^n \equiv b^n \pmod m$, tedy

$$a^n \equiv 1 \pmod m \iff b^n \equiv 1 \pmod m.$$ □

**Lemma.** *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Je-li řád čísla $a$ modulo $m$ roven $r \cdot s$, (kde $r, s \in \mathbb{N}$), pak řád čísla $a^r$ modulo $m$ je roven $s$.*

DŮKAZ. Protože žádné z čísel $a, a^2, a^3, \ldots, a^{rs-1}$ není kongruentní s 1 modulo $m$, není ani žádné z čísel $a^r, a^{2r}, a^{3r}, \ldots, a^{(s-1)r}$ kongruentní s 1. Platí ale $(a^r)^s \equiv 1 \pmod m$, proto je řád $a^r$ modulo $m$ roven $s$. □

Opak obecně neplatí – z toho, že řád čísla $a^r$ modulo $m$ je roven $s$, ještě neplyne, že řád čísla $a$ modulo $m$ je $r \cdot s$.

**Příklad.** Např pro $m = 13$ a čísla $a = 3$, $b = -4$ máme $a^2 = 9$, $a^3 = 27 \equiv 1 \pmod{13}$, proto je řád $a$ mod 13 roven 3. Podobně $b^2 = 16 \not\equiv 1 \pmod{13}$, $b^3 = -64 \equiv 1 \pmod{13}$ a $b$ má tedy modulo 13 řád 3. Přitom $b^2 = (-4)^2 = 16 \equiv 3 = a \pmod{13}$ má stejný řád 3 jako číslo $a$, ale číslo $b$ nemá řád $2 \cdot 3$.

Přesný popis závislosti řádu na exponentu dávají následující dvě věty.

**10.17. Věta.** *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Označme $r$ řád čísla $a$ modulo $m$. Pak pro libovolná $t, s \in \mathbb{N} \cup \{0\}$ platí*

$$a^t \equiv a^s \pmod m \iff t \equiv s \pmod r.$$

DŮKAZ. Bez újmy na obecnosti lze předpokládat, že $t \geq s$. Vydělíme-li číslo $t - s$ číslem $r$ se zbytkem, dostaneme $t - s = q \cdot r + z$, kde $q, z \in \mathbb{N}_0$, $0 \leq z < r$.

„⇐“ Protože $t \equiv s \pmod r$, máme $z = 0$, a tedy $a^{t-s} = a^{qr} = (a^r)^q \equiv 1^q \pmod m$. Vynásobením obou stran kongruence číslem $a^s$ dostaneme tvrzení.

Zejména pak odtud plyne, že pro libovolné $n \in \mathbb{N}$ je $N_n = \frac{1}{n}(p^n - \cdots + \mu(n)p) \neq 0$, neboť výraz v závorce je součtem různých mocnin $p$ vynásobených koeficienty $\pm 1$, a nemůže tak být roven 0. Proto existují ireducibilní polynomy nad $\mathbb{F}_p$ libovolného stupně $n$, a existují tedy i konečná tělesa $\mathbb{F}_{p^n}$, která mají $p^n$ prvků pro libovolné prvočíslo $p$ a přirozené číslo $n$ (v kapitole 11 si ukážeme, že takové těleso se konstruuje jako faktorokruh $\mathbb{F}_p[x]/(f)$ okruhu polynomů nad $\mathbb{F}_p$ podle ideálu generovaného ireducibilním polynomem $f \in \mathbb{F}_p[x]$ stupně $n$, jehož existenci jsme právě dokázali).

**10.34.** Určete počet ireducibilních polynomů nad $\mathbb{Z}_2$ stupně 5 a počet normovaných ireducibilních polynomů nad $\mathbb{Z}_3$ stupně 4.

**Řešení.** Podle dokázaného vztahu je počet (normovaných) ireducibilních polynomů nad $\mathbb{Z}_2$ stupně 5 roven

$$N_5 = \frac{1}{5}\sum_{d|5} \mu\left(\tfrac{5}{d}\right) 2^d = \frac{1}{5}\left(\mu(1)\cdot 2^5 + \mu(5)\cdot 2\right) = 6.$$

Nad $\mathbb{Z}_3$ je počet normovaných ireducibilních polynomů stupně čtyři roven

$N_4 = \frac{1}{4}\sum_{d|4} \mu\left(\frac{4}{d}\right) 3^d = \frac{1}{4}\left(\mu(1)\cdot 3^4 + \mu(2)\cdot 3^2 + \mu(4)3^1\right) =$
$= \frac{1}{4}(81 - 9) = 18\,.$ □

## C. Řešení kongruencí

**Lineární kongruence.** Následující příklad ukáže, že postup uvedený v důkazu věty 10.24 o řešitelnosti lineárních kongruencí (který využívá Eulerovu větu) obvykle není tím nejefektivnějším – s výhodou lze použít jak Bezoutovu větu, tak ekvivalentní úpravy řešené kongruence.



**10.35.** Řešte kongruenci

$$39x \equiv 41 \pmod{47}.$$

**Řešení.**

i) Nejprve využijeme Eulerovu větu.
Protože $(39, 47) = 1$, platí

$$39^{\varphi(47)} = 39^{46} \equiv 1 \pmod{47},$$

tj.

$$\underbrace{39^{45}\cdot 39}_{39^{46}\equiv 1} x \equiv 39^{45}\cdot 41 \pmod{47},$$

z čehož už dostáváme

$$x \equiv 39^{45}\cdot 41 \pmod{47}.$$

„⇒“ Ze vztahu $a^t \equiv a^s \pmod m$ plyne $a^s \cdot a^{qr+z} \equiv a^s \pmod m$. Protože je $a^r \equiv 1 \pmod m$, je rovněž $a^{qr+z} \equiv a^z \pmod m$. Celkem po vydělení obou stran první kongruence číslem $a^s$ (které je nesoudělné s modulem), dostáváme $a^z \equiv 1 \pmod m$. Protože $z < r$, plyne z definice řádu, že $z = 0$, a tedy $r \mid t - s$. □

Zřejmým důsledkem předchozí věty a Eulerovy věty je následující tvrzení (jehož druhá část je přeformulováním Lagrangeovy věty 11.10 pro naši situaci):

**Důsledek.** *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Označme $r$ řád čísla $a$ modulo $m$.*

*(1) Pro libovolné $n \in \mathbb{N} \cup \{0\}$ platí*

$$a^n \equiv 1 \pmod m \iff r \mid n.$$

*(2) $r \mid \varphi(m)$*

Následující věta je zobecněním předchozího lemmatu.

**10.18. Věta.** *Nechť $m, n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Je-li řád čísla $a$ modulo $m$ roven $r$, je řád čísla $a^n$ modulo $m$ roven $\frac{r}{(n,r)}$.*

Důkaz. Protože $\frac{r\cdot n}{(r,n)} = [r, n]$, což je zřejmě násobek $r$, máme

$$(a^n)^{\frac{r}{(r,n)}} = a^{[r,n]} \equiv 1 \pmod m$$

(poslední vztah plyne z předchozího důsledku, neboť $r \mid [r, n]$). Na druhou stranu je-li $k \in \mathbb{N}$ libovolné takové, že $(a^n)^k = a^{n\cdot k} \equiv 1 \pmod m$, dostáváme (protože $r$ je řád $a$), že $r \mid n \cdot k$. Dále víme, že $\frac{r}{(n,r)} \mid \frac{n}{(n,r)} \cdot k$, odkud díky nesoudělnosti čísel $\frac{r}{(n,r)}$ a $\frac{n}{(n,r)}$ dostáváme $\frac{r}{(n,r)} \mid k$. Proto je $\frac{r}{(n,r)}$ řádem čísla $a^n$ modulo $m$. □

Poslední z této řady tvrzení dává do souvislosti řády dvou čísel a řád jejich součinu:

**Lemma.** *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. Jestliže $a$ je řádu $r$ a $b$ je řádu $s$ modulo $m$, kde $(r, s) = 1$, pak číslo $a \cdot b$ je řádu $r \cdot s$ modulo $m$.*

Důkaz. Označme $\delta$ řád čísla $a \cdot b$. Pak $(ab)^\delta \equiv 1 \pmod m$, z čehož umocněním obou stran kongruence na $r$-tou dostaneme $a^{r\delta} b^{r\delta} \equiv 1 \pmod m$. Protože je $r$ řádem čísla $a$, je $a^r \equiv 1 \pmod m$, tj. $b^{r\delta} \equiv 1 \pmod m$, a proto $s \mid r\delta$. Z nesoudělnosti $r$ a $s$ plyne $s \mid \delta$. Analogicky dostaneme i $r \mid \delta$, a tedy (opět s využitím nesoudělnosti $r, s$) $r \cdot s \mid \delta$. Obráceně zřejmě platí $(ab)^{rs} \equiv 1 \pmod m$, proto $\delta \mid rs$. Celkem tedy $\delta = rs$. □

**10.19. Primitivní kořeny.** Mezi čísly nesoudělnými s modulem $m$ (tedy mezi prvky redukované soustavy zbytků modulo $m$) jsou nejdůležitější ta z nich, která mají řád roven $\varphi(m)$. Postupným umocňováním takového čísla lze totiž získat všechny možné prvky redukované soustavy zbytků (resp. čísla s nimi kongruentní) a místo uvažování prvků redukované soustavy zbytků modulo $m$ v různých úlohách tak můžeme pracovat s mocninami konkrétního čísla, což je obvykle jednodušší (viz např. důkaz věty 10.31 o binomických kongruencích).



Primitivní kořen

Nechť $m \in \mathbb{N}$. Celé číslo $g \in \mathbb{Z}$, $(g, m) = 1$ nazveme *primitivním kořenem* modulo $m$, pokud je jeho řád modulo $m$ roven $\varphi(m)$.

Úplné řešení vyžaduje ještě vypočtení zbytku po dělení čísla $39^{45} \cdot 41$ číslem 47, ale to již jistě laskavý čtenář zvládne sám a zjistí výsledek $x \equiv 36 \pmod{47}$.

ii) Další možností je využít Bezoutovu větu.
Euklidovým algoritmem pro vypočtení (39, 47) dostáváme

$$47 = 1 \cdot 39 + 8,$$
$$39 = 4 \cdot 8 + 7,$$
$$8 = 1 \cdot 7 + 1.$$

Z čehož zpětným odvozením dostáváme

$$1 = 8 - 7 = 8 - (39 - 4 \cdot 8) = 5 \cdot 8 - 39 =$$
$$= 5 \cdot (47 - 39) - 39 = 5 \cdot 47 - 6 \cdot 39.$$

Uvážíme-li tuto rovnost modulo 47, dostaneme

$$1 \equiv -6 \cdot 39 \pmod{47}, \quad / \cdot 41$$
$$41 \equiv \underbrace{41 \cdot (-6)} \cdot 39 \pmod{47}, \quad / \cdot 41$$
$$x \equiv 41 \cdot (-6) \pmod{47},$$
$$x \equiv -246 \pmod{47},$$
$$x \equiv 36 \pmod{47}.$$

Poznamenejme, že tento způsob je obvykle používán v příslušných softwarových nástrojích – je totiž efektivní a dobře algoritmizovatelný.

iii) Obvykle nejrychlejším (alespoň při ručním počítání), ale nejhůře algoritmizovatelným způsobem řešení je metoda využívající takových úprav kongruence, které zachovávají množinu řešení:

$$39x \equiv 41 \pmod{47},$$
$$-8x \equiv -6 \pmod{47}, \quad / : -2$$
$$4x \equiv 3 \pmod{47},$$
$$4x \equiv -44 \pmod{47}, \quad / : 4$$
$$x \equiv -11 \pmod{47},$$
$$x \equiv 36 \pmod{47}.$$

□

**Soustavy kongruencí.** Pro řešení soustav (nejen lineárních) kongruencí je důležitá Čínská zbytková věta, která garantuje jednoznačnost řešení v případě, že jsou moduly jednotlivých kongruencí po dvou nesoudělné.

**Lemma.** *Je-li $g$ primitivní kořen modulo $m$, pak pro každé číslo $a \in \mathbb{Z}$, $(a, m) = 1$, existuje jediné $x_a \in \mathbb{Z}$, $0 \le x_a < \varphi(m)$ s vlastností $g^{x_a} \equiv a \pmod{m}$.*

Zobrazení $a \mapsto x_a$ se nazývá *diskrétní logaritmus*, příp. *index* čísla $a$ (vzhledem k danému $m$ a zafixovanému primitivnímu kořeni $g$) a je bijekcí mezi množinami

$$\{a \in \mathbb{Z};\ (a, m) = 1, 0 < a < m\} \text{ a } \{x \in \mathbb{Z};\ 0 \le x < \varphi(m)\}.$$

Důkaz. Předpokládejme, že pro $x, y \in \mathbb{Z}$, $0 \le x, y < \varphi(m)$ je $g^x \equiv g^y \pmod{m}$. Z vlastností řádu pak $x \equiv y \pmod{\varphi(m)}$, tj. $x = y$, proto je zobrazení injektivní. Vzhledem k tomu, že jde o zobrazení mezi dvěma konečnými množinami o stejném počtu prvků, je nutně i surjektivní. □

Pokud pro přirozené číslo existují primitivní kořeny, tak jich mezi čísly $1, 2, \ldots, m$ existuje právě $\varphi(\varphi(m))$. Je-li totiž $g$ primitivní kořen a $a \in \{1, 2, \ldots, \varphi(m)\}$ libovolné, pak $g^a$ má podle věty 10.18 řád $\frac{\varphi(m)}{(a,\varphi(m))}$, což je rovno $\varphi(m)$ právě tehdy, je-li $(a, \varphi(m)) = 1$. Takových $a$ je v množině $\{1, 2, \ldots, \varphi(m)\}$ právě $\varphi(\varphi(m))$.

Nyní ukážeme, že primitivní kořeny existují pro dostatečné množství modulů $m$.

**10.20. Věta** (Existence primitivních kořenů). *Buď $m \in \mathbb{N}$, $m > 1$. Primitivní kořeny modulo $m$ existují právě tehdy, když $m$ splňuje některou z následujících podmínek:*

- *$m = 2$ nebo $m = 4$,*
- *$m$ je mocnina lichého prvočísla,*
- *$m$ je dvojnásobek mocniny lichého prvočísla.*



Důkaz věty provedeme v několika krocích. Snadno je vidět, že primitivní kořen modulo 2 je 1 a že modulo 4 je primitivním kořenem číslo 3. Dále ukážeme, že primitivní kořeny existují modulo libovolné liché prvočíslo (v algebraické terminologii tak vlastně jiným způsobem dokážeme, že grupa $(\mathbb{Z}_m^\times, \cdot)$ invertibilních zbytkových tříd modulo prvočíselné $m$ je cyklická, viz též 11.8).

**Tvrzení.** *Nechť $p$ je liché prvočíslo. Pak existují primitivní kořeny modulo $p$.*

Důkaz. Označme $r_1, r_2, \ldots, r_{p-1}$ řády čísel $1, 2, \ldots, p-1$ modulo $p$. Buď $\delta = [r_1, r_2, \ldots, r_{p-1}]$ nejmenší společný násobek těchto řádů. Ukážeme, že mezi čísly $1, 2, \ldots, p-1$ existuje číslo řádu $\delta$ a že $\delta = p - 1$.

Nechť $\delta = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ je rozklad $\delta$ na prvočísla. Pro libovolné $s \in \{1, \ldots, k\}$ existuje $c \in \{1, \ldots, p-1\}$ tak, že $q_s^{\alpha_s} \mid r_c$ (jinak by existoval menší společný násobek čísel $r_1, r_2, \ldots, r_{p-1}$ než je $\delta$), proto existuje $b \in \mathbb{Z}$ tak, že $r_c = b \cdot q_s^{\alpha_s}$. Protože $c$ má řád $r_c$, má číslo $g_s := c^b$ podle věty 10.18 o řádech mocnin řád roven $q_s^{\alpha_s}$.

Provedením předchozí úvahy pro libovolné $s \in \{1, \ldots, k\}$ dostaneme čísla $g_1, \ldots, g_k$ a můžeme položit $g := g_1 \cdots g_k$. Z vlastností řádu součinu dostáváme, že řád $g$ je roven součinu řádů čísel $g_1, \ldots, g_k$, tj. číslu $q_1^{\alpha_1} \cdots q_k^{\alpha_k} = \delta$.

Nyní dokážeme, že $\delta = p - 1$. Protože řády čísel $1, 2, \ldots, p-1$ dělí $\delta$, dostáváme pro libovolné $x \in \{1, 2, \ldots, p-1\}$ vztah $x^\delta \equiv 1 \pmod{p}$. Kongruence stupně $\delta$ modulo prvočíslo $p$ má podle věty 10.29 nejvýše $\delta$ řešení (v algebraické terminologii jde vlastně o hledání kořenů polynomů nad tělesem, kterých, jak uvidíme v části 11.19, je nejvýše tolik, kolik je stupeň polynomu). Ukázali jsme ale, že tato kongruence má $p - 1$ řešení, proto nutně

**10.36. Čínská zbytková věta.** Jsou-li $m_1, m_2, \ldots, m_r$ po dvou nesoudělná přirozená čísla a $a_1, a_2, \ldots, a_r$ libovolná celá čísla, pak má soustava kongruencí



$$\begin{aligned} x &\equiv a_1 \pmod{m_1},\\ x &\equiv a_2 \pmod{m_2},\\ &\vdots\\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

o neznámé $x$ právě jedno řešení patřící do množiny $\{1, 2, \ldots, m_1 m_2 \cdots m_r\}$. Toto tvrzení dokažte a řešení explicitně vyjádřete.

**Řešení.** Označme $M := m_1 m_2 \cdots m_r$ a $n_i = M/m_i$ pro každé $i$, $1 \le i \le r$. Potom pro libovolné $i$ je $m_i$ nesoudělné s $n_i$, existuje proto nějaké $b_i \in \{1, \ldots, m_i - 1\}$ tak, že $b_i n_i \equiv 1 \pmod{m_i}$. Všimněme si, že $b_i n_i$ je dělitelné všemi $m_j$, $1 \le j \le r$, $i \ne j$. Proto je hledaným řešením soustavy číslo

$$x = a_1 b_1 n_1 + a_2 b_2 n_2 + \cdots + a_r b_r n_r\ . \qquad \square$$

**10.37.** Řešte soustavu kongruencí

$$\begin{aligned} x &\equiv\ \ 1 \pmod{10},\\ x &\equiv\ \ 5 \pmod{18},\\ x &\equiv -4 \pmod{25}. \end{aligned}$$

**Řešení.** Množinu čísel $x$ vyhovujících první kongruenci můžeme popsat tak, že jde o všechna celá čísla $x = 1+10t$, kde $t \in \mathbb{Z}$ je libovolné. Tento výraz dosadíme do druhé kongruence a vyřešíme ji vzhledem k neznámé $t$:

$$\begin{aligned} 1 + 10t &\equiv\ \ 5 \pmod{18},\\ 10t &\equiv\ \ 4 \pmod{18},\\ 5t &\equiv\ \ 2 \pmod{9},\\ 5t &\equiv 20 \pmod{9},\\ t &\equiv\ \ 4 \pmod{9}, \end{aligned}$$

neboli $t = 4+9s$, kde $s \in \mathbb{Z}$ je libovolné. Prvním dvěma kongruencím tedy vyhovují ta $x$, která splňují $x = 1 + 10t = 1 + 10(4 + 9s) = 41 + 90s$.

$\delta \ge p-1$. Přitom $\delta$ je (jakožto řád čísla $g$) zároveň dělitelem $p-1$, odkud konečně dostáváme požadovanou rovnost $\delta = p - 1$. $\square$

Nyní ukážeme, že primitivní kořeny existují dokonce modulo mocniny lichých prvočísel. K tomu budeme potřebovat dvě pomocná tvrzení.

**Lemma.** *Buď $p$ liché prvočíslo, $\ell \ge 2$ libovolné. Pak pro libovolné $a \in \mathbb{Z}$ platí*

$$(1 + ap)^{p^{\ell-2}} \equiv 1 + ap^{\ell-1} \pmod{p^\ell}.$$

Důkaz. Plyne snadno z binomické věty s využitím matematické indukce vzhledem $\ell$.
I. Pro $\ell = 2$ tvrzení zřejmě platí.
II. Nechť tvrzení platí pro $\ell$, dokážeme jej i pro $\ell + 1$. S využitím příkladu ‖10.15‖, kdy tvrzení pro $\ell$ umocníme na $p$-tou, dostaneme

$$(1 + ap)^{p^{\ell-1}} \equiv (1 + ap^{\ell-1})^p \pmod{p^{\ell+1}}.$$

Z binomické věty přitom plyne

$$(1 + ap^{\ell-1})^p = 1 + p \cdot a \cdot p^{\ell-1} + \sum_{k=2}^{p} \binom{p}{k} a^k p^{(\ell-1)k}$$

a vzhledem k tomu, že podle příkladu ‖10.14‖ pro $1 < k < p$ platí $p \mid \binom{p}{k}$, stačí ukázat $p^{\ell+1} \mid p^{1+(\ell-1)k}$, což je ekvivalentní s $1 \le (k-1)(\ell-1)$. Rovněž pro $k = p$ dostáváme díky předpokladu $\ell \ge 2$ vztah $p^{\ell+1} \mid p^{(\ell-1)p}$. $\square$

**Lemma.** *Buď $p$ liché prvočíslo, $\ell \ge 2$ libovolné. Pak pro libovolné $a \in \mathbb{Z}$ splňující $p \nmid a$ platí, že řád čísla $1 + ap$ modulo $p^\ell$ je roven $p^{\ell-1}$.*

Důkaz. Podle předchozího lemmatu je

$$(1 + ap)^{p^{\ell-1}} \equiv 1 + ap^{\ell} \pmod{p^{\ell+1}},$$

a uvážíme-li tuto kongruenci modulo $p^\ell$, dostaneme $(1 + ap)^{p^{\ell-1}} \equiv 1 \pmod{p^\ell}$. Přitom přímo z předchozího lemmatu a faktu $p \nmid a$ plyne $(1 + ap)^{p^{\ell-2}} \not\equiv 1 \pmod{p^\ell}$, což dává požadované. $\square$

**Tvrzení.** *Buď $p$ liché prvočíslo. Pak pro každé $\ell \in \mathbb{N}$ existuje primitivní kořen modulo $p^\ell$.*

Důkaz. Nechť $g$ je primitivní kořen modulo $p$. Ukážeme, že pokud $g^{p-1} \not\equiv 1 \pmod{p^2}$, je $g$ dokonce primitivním kořenem modulo $p^\ell$ pro libovolné $\ell \in \mathbb{N}$. (Pokud by přitom platilo $g^{p-1} \equiv 1 \pmod{p^2}$, pak $(g+p)^{p-1} \equiv 1 + (p-1)g^{p-2}p \not\equiv 1 \pmod{p^2}$, a mohli bychom tedy místo $g$ volit za původní primitivní kořen s ním kongruentní číslo $g + p$.)

Nechť tedy $g$ splňuje $g^{p-1} \not\equiv 1 \pmod{p^2}$. Pak existuje $a \in \mathbb{Z}$, $p \nmid a$ tak, že $g^{p-1} = 1 + p \cdot a$. Ukážeme, že $g$ je modulo $p^\ell$ řádu $\varphi(p^\ell) = (p-1)p^{\ell-1}$. Buď $n \in \mathbb{N}$ nejmenší číslo, splňující $g^n \equiv 1 \pmod{p^\ell}$. Podle předchozího lemmatu je $g^{p-1} = 1 + p \cdot a$ řádu $p^{\ell-1}$ modulo $p^\ell$. Pak ale podle důsledku za větou 10.17

$$(g^{p-1})^n = (g^n)^{p-1} \equiv 1 \pmod{p^\ell} \Longrightarrow p^{\ell-1} \mid n.$$

Zároveň z kongruence $g^n \equiv 1 \pmod{p}$ plyne $p - 1 \mid n$. Z nesoudělnosti čísel $p - 1$ a $p^{\ell-1}$ dostáváme $(p-1)p^{\ell-1} \mid n$. Proto $n = \varphi(p^\ell)$ a $g$ je tedy primitivní kořen modulo $p^\ell$. $\square$

Dosadíme do třetí kongruence a soustavu dořešíme:

$$\begin{aligned} 41 + 90s &\equiv -4 \pmod{25},\\ 90s &\equiv 5 \pmod{25},\\ 18s &\equiv 1 \pmod{5},\\ 3s &\equiv 6 \pmod{5},\\ s &\equiv 2 \pmod{5}, \end{aligned}$$

neboli $s = 2 + 5r$, kde $r \in \mathbb{Z}$. Celkem $x = 41 + 90s = 41 + 90(2 + 5r) = 221 + 450r$.

Řešením jsou všechna celá $x$ splňující $x \equiv 221 \pmod{450}$. □

**10.38.** Vyřešte soustavu

$$\begin{aligned} x &\equiv 7 \pmod{27},\\ x &\equiv -3 \pmod{11}. \end{aligned}$$

**Řešení.** (a) Euklidovým algoritmem najdeme koeficienty v Bezoutově rovnosti $1 = 5 \cdot 11 - 2 \cdot 27$. Odtud $[11]_{27}^{-1} = [5]_{27}$ a $[27]_{11}^{-1} = [-2]_{11}$. Řešení je tedy $x \equiv 7 \cdot 11 \cdot 5 - 3 \cdot 27 \cdot (-2) = 547 \equiv 250 \pmod{297}$.

(b) Postupným dosazením: z druhé kongruence je $x = 11t - 3$, dosazením do první máme $11t \equiv 10 \pmod{27}$. Vynásobením číslem 5 získáme $55t \equiv 50$, tj. $t \equiv -4 \pmod{27}$. Dohromady $x = 11 \cdot 27 \cdot s - 4 \cdot 11 - 3 = 297s - 47$ pro $s \in \mathbb{Z}$, neboli $x \equiv -47 \pmod{297}$. □

**10.39.** Skupině třinácti pirátů se podařilo uloupit bednu zlatých mincí (kterých bylo přibližně dva tisíce). Zkusili je rozdělit rovným dílem na třináct hromádek, ale deset mincí jim zbylo. O zbylé mince se strhla rvačka, při níž jednoho piráta propíchli. Přestali tedy bojovat a zkusili mezi sebe znovu rozdělit mince rovným dílem. Tentokrát zbyly tři mince, o které opět začali bojovat. V boji zahynul další pirát a tak si ostatní opět zkusili mince spravedlivě rozdělit, tentokrát úspěšně. Kolik bylo mincí, které piráti ukradli?

**Řešení.** Úloha vede na soustavu kongruencí

$$\begin{aligned} x &\equiv 10 \pmod{13},\\ x &\equiv 3 \pmod{12},\\ x &\equiv 0 \pmod{11}, \end{aligned}$$

jejímž řešením je $x \equiv 231 \pmod{11 \cdot 12 \cdot 13}$. Protože počet mincí $x$ je přibližně 2000 a $x \equiv 231 \pmod{1716}$, snadno dopočítáme, že mincí bylo $231 + 1716 = 1947$. □

**10.40.** Když na Sokolském sletu vytvořili cvičenci osmistupy, zbývali 3 navíc, při cvičení v kruzích o 17 lidech jich přebývalo 7 a při tvorbě pyramid (na každou je potřeba $21 = 4^2 + 2^2 + 1$ lidí), byly dvě pyramidy neúplné – bez člověka „na vrcholu“. Kolik cvičenců se

**Tvrzení.** *Buď $p$ liché prvočíslo a $g$ primitivní kořen modulo $p^\ell$ pro $\ell \in \mathbb{N}$. Pak liché z čísel $g$, $g + p^\ell$ je primitivním kořenem modulo $2p^\ell$.*

Důkaz. Nechť $c$ je liché přirozené číslo. Pak pro libovolné $n \in \mathbb{N}$ platí $c^n \equiv 1 \pmod{p^\ell}$, právě když $c^n \equiv 1 \pmod{2p^\ell}$. Protože $\varphi(2p^\ell) = \varphi(p^\ell)$, je každý lichý primitivní kořen modulo $p^\ell$ rovněž primitivním kořenem modulo $2p^\ell$. □

Další tvrzení popisuje případ mocnin dvojky. K tomu využijeme obdobných pomocných tvrzení jako v případě lichých prvočísel.

**Lemma.** *Buď $\ell \in \mathbb{N}$, $\ell \geq 3$. Pak $5^{2^{\ell-3}} \equiv 1 + 2^{\ell-1} \pmod{2^\ell}$.*

Důkaz. Obdobně jako výše pro $2 \nmid p$. □

**Lemma.** *Buď $\ell \in \mathbb{N}$, $\ell \geq 3$. Pak řád čísla 5 modulo $2^\ell$ je $2^{\ell-2}$.*

Důkaz. Snadný z předchozího lemmatu. □

**Tvrzení.** *Nechť $\ell \in \mathbb{N}$. Primitivní kořeny existují modulo $2^\ell$ právě tehdy, když $\ell \leq 2$.*

Důkaz. Buď $\ell \geq 3$. Pak množina

$$S = \{(-1)^a \cdot 5^b;\, a \in \{0, 1\}, 0 \leq b < 2^{\ell-2};\, b \in \mathbb{Z}\}$$

tvoří redukovanou soustavu zbytků modulo $2^\ell$ (má totiž $\varphi\left(2^\ell\right)$ prvků o kterých se snadno ukáže, že jsou po dvou nekongruentní modulo $2^\ell$).

Přitom zřejmě (s využitím předchozího lemmatu) řád každého prvku $S$ dělí $2^{\ell-2}$, proto v této (a tedy ani v žádné jiné) redukované soustavě nemůže existovat prvek řádu $\varphi(2^\ell) = 2^{\ell-1}$. □

Posledním kamínkem do mozaiky tvrzení, která společně dokazují větu 10.20, je tvrzení popisující neexistenci primitivních kořenů pro složená čísla, která nejsou mocninou prvočísla (ani jejím dvojnásobkem).

**Tvrzení.** *Nechť $m \in \mathbb{N}$ je dělitelné alespoň 2 prvočísly a není dvojnásobkem mocniny lichého prvočísla. Pak modulo $m$ neexistují primitivní kořeny.*

Důkaz. Nechť je rozklad $m$ na prvočísla tvaru $2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, kde $\alpha \in \mathbb{N}_0, \alpha_i \in \mathbb{N}, 2 \nmid p_i$ a buď platí $k \geq 2$ nebo $k \geq 1$ a $\alpha \geq 2$. Označíme-li $\delta = [\varphi(2^\alpha), \varphi(p_1^{\alpha_1}), \ldots, \varphi(p_1^{\alpha_1})]$, pak se snadno vidí, že $\delta < \varphi(2^\alpha) \cdot \varphi(p_1^{\alpha_1}) \cdots \varphi(p_1^{\alpha_1}) = \varphi(m)$ a že pro libovolné $a \in \mathbb{Z}$, $(a, m) = 1$ platí $a^\delta \equiv 1 \pmod{m}$. Proto modulo $m$ neexistují primitivní kořeny. □



Obecně je pro daný modul nalezení primitivního kořene velmi výpočetně náročná operace. Následující věta nám udává ekvivalentní podmínku pro to, aby zkoumané číslo bylo primitivním kořenem. Její ověření je přitom snazší než přímý výpočet řádu tohoto čísla.

**10.21. Věta.** *Buď $m$ takové, že modulo $m$ existují primitivní kořeny. Zapišme $\varphi(m) = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$, kde $q_1, \ldots, q_k$ jsou prvočísla a $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Pak pro libovolné $g \in \mathbb{Z}$, $(g, m) = 1$ platí, že $g$ je primitivní kořen modulo $m$, právě když neplatí ani jedna z kongruencí*

$$g^{\frac{\varphi(m)}{q_1}} \equiv 1 \pmod{m}, \ldots, g^{\frac{\varphi(m)}{q_k}} \equiv 1 \pmod{m}.$$

vystoupení zúčastnilo, když jich bylo určitě méně než 4000, ale více než 2000?

**Řešení.** Standardním způsobem řešíme soustavu lineárních kongruencí

$$\begin{aligned} c &\equiv \ \ 3 \pmod 8,\\ c &\equiv \ \ 7 \pmod{17},\\ c &\equiv -2 \pmod{21} \end{aligned}$$

a dostaneme řešení $c \equiv 1027 \pmod{2856}$, z něhož pomocí dodatečné informace zjistíme, že na ploše bylo 3883 cvičenců. □

*10.41.* Určete, která z následujících (soustav) kongruencí má řešení.

i) $x \equiv \ \ 1 \pmod 3$,
$x \equiv -1 \pmod 9$;
ii) $8x \equiv 1 \pmod{12345678910111213}$;
iii) $x \equiv 3 \pmod{29}$,
$x \equiv 5 \pmod{47}$.

○

Čínskou zbytkovou větu můžeme použít také „v opačném směru“ k tomu, abychom si zjednodušili řešení lineární kongruence v případě, kdy umíme modul rozložit na součin po dvou nesoudělných faktorů.

**10.42.** Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

**Řešení.** Rozložme $3564 = 2^2 \cdot 3^4 \cdot 11$. Protože žádné z čísel 2, 3, 11 nedělí číslo 23 941, platí $(23\,941, 3564) = 1$ a kongruence má tedy řešení. Díky tomu, že $\varphi(3564) = 2 \cdot (3^3 \cdot 2) \cdot 10 = 1080$, je řešení tvaru $x \equiv 915 \cdot 23\,941^{1079} \pmod{3564}$. Úprava čísla stojícího na pravé straně by však vyžádala značné úsilí. Proto budeme kongruenci řešit poněkud jinak – sestavíme ekvivalentní soustavu kongruencí, jejichž řešení je snazší než řešení původní kongruence.

Víme, že $x \in \mathbb{Z}$ je řešením dané kongruence, právě když je řešením soustavy

$$\begin{aligned} 23941x &\equiv 915 \pmod{2^2},\\ 23941x &\equiv 915 \pmod{3^4},\\ 23941x &\equiv 915 \pmod{11}. \end{aligned}$$

Vyřešíme-li postupně každou z kongruencí soustavy, dostaneme ekvivalentní soustavu

$$\begin{aligned} x &\equiv \ \ 3 \pmod 4,\\ x &\equiv -3 \pmod{81},\\ x &\equiv -4 \pmod{11}, \end{aligned}$$

Důkaz. Pokud by platila některá z uvedených kongruencí, znamenalo by to, že řád $g$ je menší než $\varphi(m)$.

Obráceně pokud $g$ není primitivní kořen, pak existuje $d \in \mathbb{N}$, $d \mid \varphi(m)$, kde $d < \varphi(m)$ a $g^d \equiv 1 \pmod m$. Je-li $u = \frac{\varphi(m)}{d} > 1$, nutně existuje $i \in \{1, \dots, k\}$ tak, že $q_i \mid u$. Pak ale

$$g^{\frac{\varphi(m)}{q_i}} = g^{d \cdot \frac{u}{q_i}} \equiv 1 \pmod m.$$

□

### 4. Řešení kongruencí a jejich soustav



V této části se budeme věnovat analogii k řešení rovnic v nějakém číselném oboru. Ve skutečnosti opravdu budeme řešit rovnice (a jejich soustavy) v okruhu zbytkových tříd $(\mathbb{Z}_m, +, \cdot)$, budeme ale hovořit o řešení kongruencí modulo $m$ a zapisovat to přehlednějším způsobem pomocí kongruencí.

Kongruence o jedné neznámé

Nechť $m \in \mathbb{N}$, $f(x), g(x) \in \mathbb{Z}[x]$. Zápis

$$f(x) \equiv g(x) \pmod m$$

nazýváme *kongruencí o jedné neznámé* $x$ a rozumíme jím úkol nalézt *množinu řešení*, tj. množinu všech takových čísel $c \in \mathbb{Z}$, pro která $f(c) \equiv g(c) \pmod m$.

Dvě kongruence o jedné neznámé nazveme *ekvivalentní*, mají-li stejnou množinu řešení.

Uvedená kongruence je ekvivalentní s kongruencí

$$f(x) - g(x) \equiv 0 \pmod m.$$

Jedinou metodou, kterou vždy umíme nalézt řešení, je vyzkoušení všech možností (jde ale samozřejmě z časových důvodů často o neproveditelný způsob). Tuto metodu formalizuje následující tvrzení.

**10.22. Tvrzení.** *Nechť $m \in \mathbb{N}$, $f(x) \in \mathbb{Z}[x]$. Pro libovolná $a, b \in \mathbb{Z}$ platí*

$$a \equiv b \pmod m \implies f(a) \equiv f(b) \pmod m.$$

Důkaz. Nechť je $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, kde $c_0, c_1, \dots, c_n \in \mathbb{Z}$. Protože $a \equiv b \pmod m$, pro každé $i = 0, 1, \dots, n$ platí $c_i a^i \equiv c_i b^i \pmod m$, odkud sečtením těchto kongruencí pro $i = 0, 1, 2, \dots, n$ dostaneme

$$c_n a^n + \cdots + c_1 a + c_0 \equiv c_n b^n + \cdots + c_1 b + c_0 \pmod m,$$

tj. $f(a) \equiv f(b) \pmod m$. □

**Důsledek.** *Množina řešení libovolné kongruence modulo $m$ je sjednocením některých zbytkových tříd modulo $m$.*

**Definice.** *Počtem řešení* kongruence o jedné neznámé modulo $m$ rozumíme počet zbytkových tříd modulo $m$ obsahujících řešení této kongruence.

**Příklad.** Právě definovaný pojem *počet řešení kongruence* je možná trochu neintuitivní v tom, že závisí na modulu kongruence a že tak dvě ekvivalentní kongruence (jejichž řešeními jsou táž celá čísla) mohou mít jiný počet řešení.

(1) Kongruence $2x \equiv 3 \pmod 3$ má právě jedno řešení (modulo 3).
(2) Kongruence $10x \equiv 15 \pmod{15}$ má pět řešení (modulo 15).
(3) Kongruence z příkladu (1) a (2) jsou ekvivalentní.

odkud snadno postupem pro řešení soustav kongruencí dostaneme $x \equiv -1137 \pmod{3564}$, což je také řešení zadané kongruence. □

**10.43.** Vyřešte lineární kongruenci $3446x \equiv 8642 \pmod{208}$.

**Řešení.** $208 = 2^4 \cdot 13$ a $(3446, 208) = 2 \mid 8642$. Kongruence má tedy právě 2 řešení modulo 208 a je ekvivalentní soustavě

$$\begin{aligned} 3x &\equiv 1 \pmod{8}, \\ x &\equiv 10 \pmod{13}. \end{aligned}$$

Ta má řešení $x \equiv 75$ a $x \equiv 179 \pmod{208}$. □

*10.44.* Dokažte, že v posloupnosti $(2^n - 3)_{n=1}^{\infty}$ je nekonečně mnoho násobků 5 a nekonečně mnoho násobků 13, ale žádný násobek 65. ◯

**Modulární reprezentace čísel.** Při počítání s velkými čísly je někdy výhodnější než s dekadickým či binárním zápisem čísel pracovat s tzv. *modulární reprezentací* (též *residue number system*), která umožňuje snadnou paralelizaci výpočtů s velkými čísly. Takový systém je určen $k$-ticí modulů (obvykle po dvou nesoudělných) a každé číslo menší než jejich součin je pak jednoznačně reprezentováno $k$-ticí zbytků (jejichž hodnoty nepřevyšují příslušné moduly).

**10.45.** Pětice modulů 3, 5, 7, 11, 13 umožňuje jednoznačně reprezentovat čísla menší než jejich součin (tedy menší než 15015) a efektivně provádět (v případě potřeby distribuovaně) běžné aritmetické operace. Určete reprezentaci čísel 1234 a 5678 v této modulární soustavě a pomocí této reprezentace vypočtěte jejich součet a součin.

**Řešení.** Vypočítáme zbytky po dělení zadaných čísel jednotlivými moduly a získáme jejich modulární reprezentaci, kterou zapíšeme jako pětice (1, 4, 2, 2, 12) a (2, 3, 1, 2, 10).

Součet provedeme po složkách (včetně výpočtu zbytku po dělení příslušným modulem) a obdržíme pětici (3, 2, 3, 4, 9), kterou lze pomocí Čínské zbytkové věty převést na číslo 6912. Součin vypočteme analogicky a dostaneme příslušnou pětici zbytků (2, 2, 2, 4, 3), což pomocí Čínské zbytkové věty převedeme zpět na číslo 9662, které je skutečně modulo 15015 totéž jako $1234 \cdot 5678$. □

**10.46.** Často je uvažována modulární reprezentace pomocí trojice modulů $2^n - 1, 2^n, 2^n + 1$ (uvědomte si, že tato čísla jsou skutečně po dvou nesoudělná), jednoznačně pokrývající čísla mající až $3n$ bitů.

Uvažte $n = 3$ a zapište modulární reprezentaci čísla 118 v této soustavě.

**10.23. Lineární kongruence o jedné neznámé.** Podobně jako je tomu v případě rovnic, i u kongruencí je situace nejsnazší v případě kongruencí lineárních, kdy jsme nejen schopni snadno rozhodnout o jejich řešitelnosti, ale rovněž umíme řešení efektivně nalézt. Konkrétní postup naznačuje následující věta a její důkaz.

**10.24. Věta.** *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Označme $d = (a, m)$. Pak kongruence (o jedné neznámé $x$)*

$$ax \equiv b \pmod{m}$$

*má řešení právě tehdy, když $d \mid b$.*

*Pokud platí $d \mid b$, má tato kongruence právě $d$ řešení (modulo $m$).*

Důkaz. Dokážeme nejprve, že uvedená podmínka je nutná. Je-li celé číslo $c$ řešením této kongruence, pak nutně $m \mid a \cdot c - b$. Protože $d = (a, m)$, pak nutně $d \mid m$ i $d \mid a \cdot c - b$, a tedy $d \mid a \cdot c - (a \cdot c - b) = b$.

Obráceně dokážeme, že pokud $d \mid b$, pak má daná kongruence právě $d$ řešení modulo $m$. Označme $a_1, b_1 \in \mathbb{Z}$ a $m_1 \in \mathbb{N}$ tak, že $a = d \cdot a_1$, $b = d \cdot b_1$ a $m = d \cdot m_1$. Řešená kongruence je tedy ekvivalentní s kongruencí

$$a_1 \cdot x \equiv b_1 \pmod{m_1},$$

kde $(a_1, m_1) = 1$. Tuto kongruenci můžeme vynásobit číslem $a_1^{\varphi(m_1)-1}$ a díky Eulerově větě obdržíme

$$x \equiv b_1 \cdot a_1^{\varphi(m_1)-1} \pmod{m_1}.$$

Tato kongruence má jediné řešení modulo $m_1$ a tedy $d = m/m_1$ řešení modulo $m$. □

Pomocí věty o řešitelnosti lineárních kongruencí lze dokázat mj. důležitou Wilsonovu větu udávající nutnou (i postačující) podmínku prvočíselnosti. Takové podmínky jsou velmi významné ve výpočetní teorii čísel, kdy je třeba efektivně poznat, je-li dané velké číslo prvočíslem. Bohužel dosud není známo, jak rychle vypočítat modulární faktoriál velkého čísla, proto není v praxi Wilsonova věta k tomuto účelu používána.

**Věta** (Wilsonova)**.** *Přirozené číslo $n > 1$ je prvočíslo, právě když*

$$(n-1)! \equiv -1 \pmod{n}.$$

Důkaz. Dokážeme nejprve, že pro libovolné složené číslo $n > 4$ platí $n \mid (n-1)!$, tj. $(n-1)! \equiv 0 \pmod{n}$. Nechť $1 < d < n$ je netriviální dělitel $n$. Je-li $d \neq n/d$, pak z nerovností $1 < d, n/d \leq n-1$ plyne požadovaný vztah $n = d \cdot n/d \mid (n-1)!$. Pokud $d = n/d$, tj. $n = d^2$, pak protože je $n > 4$, je i $d > 2$ a $n \mid (d \cdot 2d) \mid (n-1)!$. Pro $n = 4$ snadno dostáváme $(4-1)! \equiv\equiv 2 \not\equiv -1 \pmod{4}$.

Nechť je nyní $p$ prvočíslo. Čísla z množiny $\{2, 3, \ldots, p-2\}$ seskupíme do dvojic vzájemně inverzních čísel modulo $p$, resp. dvojic čísel, jejichž součin dává zbytek 1 po dělení $p$. Pro libovolné číslo $a$ z této množiny dostaneme podle předchozí věty jediné řešení kongruence $a \cdot x \equiv 1 \pmod{p}$. Protože $a \neq 0, 1, p-1$, je zřejmé, že rovněž pro řešení $c$ této kongruence platí $c \not\equiv 0, 1, -1 \pmod{p}$. Číslo $a$ rovněž nemůže být ve dvojici samo se sebou; kdyby totiž platil vztah $a \cdot a \equiv 1 \pmod{p}$, pak by (díky tomu, že $p \mid a^2 - 1 = (a+1)(a-1)$) nutně platila i kongruence $a \equiv \pm 1 \pmod{p}$. Součin všech čísel uvedené množiny je tedy

**Řešení.** Vypočtěme nejprve přímo, že $118 \equiv 6 \pmod 7$, $118 \equiv 6 \pmod 8$ a $118 \equiv 1 \pmod 9$, proto je hledaná reprezentace dána trojicí $(6, 6, 1)$.

Při praktickém použití je ale zejména důležité, že tuto modulární reprezentaci čísla jsme schopni efektivně převádět na binární reprezentaci a zpět. V našem případě zjistíme snadno zbytek po dělení čísla $118 = (1110110)_2$ číslem $2^3$ – ten je dán posledním binárním trojčíslím $(110)_2$, tedy je roven 6. Ani zjištění zbytku modulo $2^n + 1 = 9$ a $2^n - 1 = 7$ ale není nikterak obtížné. Zde je totiž poměrně rychle vidět (pomůže přitom rozdělení daného čísla do bloků po $n$ bitech), že

$$(001110110)_2 \equiv (001)_2 + (110)_2 + (110)_2 \equiv 6 \pmod{2^3 - 1},$$
$$(001110110)_2 \equiv (001)_2 - (110)_2 + (110)_2 \equiv 1 \pmod{2^3 + 1}.$$

Věříme, že pozornému čtenáři jistě neunikla úzká souvislost s kritérii dělitelnosti 9 a 11 diskutovanými v odstavci ‖10.17‖. □

**10.47. Kongruence vyššího stupně.** Postupem z věty 10.27 řešte kongruenci



$$x^4 + 7x + 4 \equiv 0 \pmod{27}.$$

**Řešení.** Řešme nejprve tuto kongruenci modulo 3 (např. dosazením) – snadno zjistíme, že řešení je $x \equiv 1 \pmod 3$. Zapišme řešení ve tvaru $x = 1 + 3t$, kde $t \in \mathbb{Z}$ a řešme kongruenci modulo 9:

$$\begin{aligned} x^4 + 7x + 4 &\equiv 0 \pmod 9,\\ (1+3t)^4 + 7(1+3t) + 4 &\equiv 0 \pmod 9,\\ 1 + 4\cdot 3t + 7 + 7\cdot 3t + 4 &\equiv 0 \pmod 9,\\ 33t &\equiv -12 \pmod 9,\\ 11t &\equiv -4 \pmod 3,\\ t &\equiv 1 \pmod 3. \end{aligned}$$

Zapsáním $t = 1 + 3s$, kde $s \in \mathbb{Z}$ dostaneme $x = 4 + 9s$ a po dosazení

$$\begin{aligned} (4+9s)^4 + 7(4+9s) + 4 &\equiv 0 \pmod{27},\\ 4^4 + 4\cdot 4^3\cdot 9s + 28 + 63s + 4 &\equiv 0 \pmod{27},\\ 256\cdot 9s + 63s &\equiv -288 \pmod{27},\\ 256s + 7s &\equiv -32 \pmod 3,\\ 2s &\equiv 1 \pmod 3,\\ s &\equiv 2 \pmod 3. \end{aligned}$$

Celkem dostáváme řešení $x = 4 + 9s = 4 + 9(2 + 3r) = 22 + 27r$, kde $r \in \mathbb{Z}$, neboli $x \equiv 22 \pmod{27}$. □

tvořen součinem $(p-3)/2$ dvojic (jejichž součin je vždy kongruentní s 1 modulo $p$). Proto máme

$$(p-1)! \equiv 1^{(p-3)/2}\cdot(p-1) \equiv -1 \pmod p.$$ □

**10.25. Soustavy lineárních kongruencí.** Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme podle předchozí věty rozhodnout o řešitelnosti každé z nich. V případě, kdy aspoň jedna z kongruencí nemá řešení, nemá řešení ani celá soustava. Naopak jestliže každá kongruence této soustavy řešení má, upravíme ji do tvaru $x \equiv c_i \pmod{m_i}$.



Dostaneme tak soustavu kongruencí

$$\begin{aligned} x &\equiv c_1 \pmod{m_1},\\ &\vdots\\ x &\equiv c_k \pmod{m_k}. \end{aligned}$$

Zřejmě stačí vyřešit případ $k = 2$, řešení soustavy více kongruencí snadno obdržíme opakovaným řešením soustav dvou kongruencí.

**Tvrzení.** *Nechť $c_1, c_2$ jsou celá čísla, $m_1, m_2$ čísla přirozená. Označme $d = (m_1, m_2)$. Soustava dvou kongruencí*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1},\\ x &\equiv c_2 \pmod{m_2} \end{aligned}$$

*v případě $c_1 \not\equiv c_2 \pmod d$ nemá řešení. Jestliže naopak $c_1 \equiv c_2 \pmod d$, pak existuje celé číslo $c$ tak, že $x \in \mathbb{Z}$ vyhovuje soustavě, právě když vyhovuje kongruenci*

$$x \equiv c \pmod{[m_1, m_2]}.$$

Důkaz. Má-li mít zadaná soustava nějaké řešení $x \in \mathbb{Z}$, musí nutně platit $x \equiv c_1 \pmod d$, $x \equiv c_2 \pmod d$, a tedy i $c_1 \equiv c_2 \pmod d$. Odtud plyne, že v případě $c_1 \not\equiv c_2 \pmod d$ soustava řešení mít nemůže.

Předpokládejme dále, že $c_1 \equiv c_2 \pmod d$. První kongruenci řešené soustavy vyhovují všechna celá čísla $x$ tvaru $x = c_1 + tm_1$, kde $t \in \mathbb{Z}$ je libovolné. Toto $x$ bude vyhovovat i druhé kongruenci soustavy, právě když bude platit $c_1 + tm_1 \equiv c_2 \pmod{m_2}$, tj. $tm_1 \equiv c_2 - c_1 \pmod{m_2}$. Podle věty o řešitelnosti lineárních kongruencí má tato kongruence (vzhledem k neznámé $t$) řešení, neboť $d = (m_1, m_2)$ dělí $c_2 - c_1$, a $t \in \mathbb{Z}$ splňuje tuto kongruenci, právě když

$$t \equiv \frac{c_2 - c_1}{d}\cdot\left(\frac{m_1}{d}\right)^{\varphi\left(\frac{m_2}{d}\right)-1} \pmod{\frac{m_2}{d}},$$

tj. právě když $x = c_1 + tm_1 = c_1 + (c_2 - c_1)\cdot\left(\frac{m_1}{d}\right)^{\varphi\left(\frac{m_2}{d}\right)} + r\frac{m_1 m_2}{d} = c + r\cdot[m_1, m_2]$, kde $r \in \mathbb{Z}$ je libovolné a $c = c_1 + (c_2 - c_1)\cdot(m_1/d)^{\varphi(m_2/d)}$, neboť $m_1 m_2 = d\cdot[m_1, m_2]$. Našli jsme tedy takové $c \in \mathbb{Z}$, že libovolné $x \in \mathbb{Z}$ splňuje soustavu, právě když $x \equiv c \pmod{[m_1, m_2]}$, což jsme chtěli dokázat. □

Všimněme si, že důkaz této věty je konstruktivní, tj. udává vzorec, jak číslo $c$ najít. Věta nám tedy dává metodu, jak pomocí jediné kongruence zachytit podmínku, že $x$ vyhovuje této soustavě. Přitom je tato nová kongruence téhož tvaru jako kongruence původní. Můžeme proto tento postup aplikovat i na soustavu o více

**10.48.** S využitím znalosti primitivního kořene modulo 41 z příkladu ‖10.33‖ řešte kongruenci

$$7x^{17} \equiv 11 \pmod{41}.$$

**Řešení.** Vynásobením zadané kongruence číslem 6 dostáváme ekvivalentní kongruenci $42x^{17} \equiv 66$, tj. $x^{17} \equiv 25 \pmod{41}$. Protože primitivním kořenem modulo 41 je např. číslo 6, substituce $x = 6^t$ vede na kongruenci $6^{17t} \equiv 25 \equiv 6^4 \pmod{41}$, a ta je ekvivalentní kongruenci $17t \equiv 4 \pmod{40}$, která je splněna právě pro $t \equiv 12 \pmod{40}$. Řešením kongruence jsou tedy právě celá čísla $x$ splňující $x \equiv 6^{12} \equiv 4 \pmod{41}$. □

**10.49.** Řešte kongruenci $x^5 + 1 \equiv 0 \pmod{11}$.

**Řešení.** Protože je $(5, \varphi(11)) = 5$ a

$$(-1)^{\frac{\varphi(11)}{5}} \equiv 1 \pmod{11},$$

má kongruence

$$x^5 \equiv -1 \pmod{11}$$

pět řešení. Ta můžeme nalézt buď vyzkoušením všech (deseti) možností nebo tak, že úlohu pomocí primitivního kořene převedeme na řešení lineární kongruence. Protože $2^{10/2} \equiv -1 \not\equiv 1 \pmod{11}$ a $2^{10/5} \equiv 4 \not\equiv 1 \pmod{11}$, je 2 primitivním kořenem modulo 11 (viz též příklad ‖10.32‖) a substitucí $x \equiv 2^y$ převedeme úlohu na řešení kongruence

$$2^{5y} \equiv 2^5 \pmod{11},$$

která je ekvivalentní lineární kongruenci

$$5y \equiv 5 \pmod{10},$$
$$y \equiv 1 \pmod{2}.$$

Řešením jsou tedy všechna $y$ z množiny $\{-3, -1, 1, 3, 5\}$, což odpovídá po zpětné substituci $x \equiv 2^y \pmod{11}$ řešení původní kongruence $x \in \{-1, 2, -3, -4, -5\}$. □

**10.50.** Řešte kongruenci $x^3 - 3x + 5 \equiv 0 \pmod{105}$.

**Řešení.** Protože modul je možné rozložit na součin po dvou nesoudělných faktorů $105 = 3 \cdot 5 \cdot 7$, je řešená kongruence ekvivalentní soustavě

$$x^3 - 3x + 5 \equiv 0 \pmod{3},$$
$$x^3 - 3x + 5 \equiv 0 \pmod{5},$$
$$x^3 - 3x + 5 \equiv 0 \pmod{7}.$$

První kongruence je přitom zřejmě ekvivalentní s $x^3 \equiv 1 \pmod{3}$, a protože z Malé Fermatovy věty plyne $x^3 \equiv x \pmod{3}$ pro všechna $x \in \mathbb{Z}$, rovněž s kongruencí $x \equiv 1 \pmod{3}$.

kongruencích – nejprve z první a druhé kongruence vytvoříme kongruenci jedinou, které vyhovují právě ta $x$, která vyhovovala původním dvěma kongruencím, pak z nově vzniklé a z třetí kongruence vytvoříme další atd. Při každém kroku se nám počet kongruencí soustavy sníží o jednu, po konečném počtu kroků tak dostaneme kongruenci jedinou, která bude popisovat všechna řešení dané soustavy.

Z právě popsaného způsobu plyne (při níže uvedeném dodatečném předpokladu), že soustava kongruencí má vždy řešení, a to je navíc jednoznačně určené.

**Věta** (Čínská zbytková věta)**.** *Nechť $m_1, , \ldots, m_k \in \mathbb{N}$ jsou po dvou nesoudělná, $a_1, \ldots, a_k \in \mathbb{Z}$. Pak platí: soustava*

$$x \equiv a_1 \pmod{m_1},$$
$$\vdots$$
$$x \equiv a_k \pmod{m_k}$$

*má jediné řešení modulo $m_1 \cdot m_2 \cdots m_k$.*

**Poznámka.** Důvodem nezvyklého pojmenování této věty je fakt, že se ve čtvrtém století čínský matematik Sun Tzu ve svém textu ptal na číslo, které při dělení třemi dává zbytek 2, při dělení pěti zbytek 3 a při dělení sedmi je zbytek opět 2.

Odpověď je (prý) ukryta v následující písni:

孫子歌 Sunzi Ge

三人同行七十里
五樹梅花廿一枝
七子團圓正月半
一百零五轉回起

Důkaz. Jde o jednoduchý důsledek předchozího tvrzení o tvaru řešení soustavy dvou kongruencí. Tento výsledek je ale možné rovněž elegantně dokázat přímo, jak je ukázáno v příkladu ‖10.36‖. □

Uvědomme si, že jde o docela silné tvrzení (které ve skutečnosti platí v podstatně obecnějších algebraických strukturách) umožňující nám při předepsání libovolných zbytků podle zvolených (po dvou nesoudělných) modulů garantovat, že existuje číslo s těmito předepsanými zbytky.

**10.26. Kongruence vyššího stupně.** Vraťme se nyní



k obecnějšímu případu kongruence

$$f(x) \equiv 0 \pmod{m},$$

kde $f(x)$ je mnohočlen s celočíselnými koeficienty a $m \in \mathbb{N}$. Zatím máme k dispozici jednu sice pracnou, ale univerzální metodu řešení, totiž vyzkoušet všechny možné zbytky modulo $m$. Při řešení takové kongruence tedy stačí zjistit, pro která celá čísla $a$, $0 \le a < m$, platí $f(a) \equiv 0 \pmod{m}$. Nevýhodou této metody je její náročnost, která se zvyšuje se zvětšující se hodnotou $m$. Je-li $m$ složené, tj. $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, kde $p_1, \ldots, p_k$ jsou různá

Druhá kongruence je ekvivalentní s $x(x^2-3) \equiv 0 \pmod 5$, jejíž řešení splňuje buď $x \equiv 0 \pmod 5$ nebo $x^2 \equiv 3 \pmod 5$. Protože je ale 3 kvadratický nezbytek modulo 5 (Legendreův symbol (3/5) je roven -1), je $x \equiv 0 \pmod 5$ jediné řešení druhé kongruence soustavy.

Třetí kongruenci je možné upravit na tvar $x^3 - 3x - 2 \equiv 0 \pmod 7$, a protože $x^3 - 3x - 2 = (x-2)(x+1)^2$, dostáváme řešení $x \equiv -1 \pmod 7$ nebo $x \equiv 2 \pmod 7$ – na to lze také přijít vyzkoušením všech možností modulo 7. Celkem dostáváme dvě řešení původní kongruence, totiž $x \equiv 55$, resp. $x \equiv 100$ modulo 105. □

**10.51.** Určete počet řešení kongruence



$$x^5 \equiv 534 \pmod{23^2}.$$

**Řešení.** Zadaná kongruence je ekvivalentní kongruenci $x^5 \equiv 5 \pmod{23^2}$, a protože $(5, \varphi(23)) = 1$, z věty o řešitelnosti binomických kongruencí víme, že tatáž kongruence modulo 23 má právě jedno řešení. Navíc, toto řešení jistě není násobkem modulu 23, proto násobkem modulu není ani číslo, které obdržíme dosazením tohoto řešení do derivace polynomu, jehož kořeny hledáme, tedy do $(x^5-5)' = 5x^4$. S pomocí Henselova lemmatu tedy můžeme učinit závěr, že původní kongruence má jediné řešení (aniž bychom toto řešení hledali). □

**10.52.** Udejte příklad polynomiální kongruence, která má více řešení než je její stupeň.

**Řešení.** Vzhledem k platnosti věty 10.29 je nutné uvážit buď modul, který nebude prvočíselný nebo polynom, jehož všechny koeficienty budou násobkem modulu.

Příkladem kongruence prvního typu je

$$x^2 \equiv 1 \pmod 8,$$

která je kvadratická a má přitom čtyři řešení 1, 3, 5, 7.

Příkladem požadované kongruence v případě prvočíselného modulu je například kvadratická kongruence $10x^2 - 15 \equiv 0 \pmod 5$, která má pět řešení. □

**10.53. Další typy kongruencí.** Dokažte, že pro libovolné přirozené číslo $n$ je číslo



$$111 + 2^{2^{2^{2n-1}}}$$

dělitelné číslem 127.

**Řešení.** Máme za úkol dokázat, že pro každé $n \in \mathbb{N}$ je splněna kongruence

$$2^{2^{2^{2n-1}}} \equiv -111 \pmod{127},$$

prvočísla, a je-li navíc $k > 1$, můžeme kongruenci nahradit soustavou kongruencí

$$\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{\alpha_1}}, \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_k^{\alpha_k}}, \end{aligned}$$

která má stejnou množinu řešení, a řešit každou kongruenci této soustavy zvlášť. Tím získáme obecně několik soustav lineárních kongruencí, které už řešit umíme. Výhoda této metody spočívá v tom, že moduly kongruencí soustavy jsou menší než modul původní kongruence.

**Příklad.** Řešme kongruenci

$$x^3 - 2x + 11 \equiv 0 \pmod{105}.$$

Kdybychom chtěli vyzkoušet všechny možnosti, museli bychom spočítat pro $f(x) = x^3 - 2x + 11$ sto pět hodnot $f(0), f(1), \ldots, f(104)$. Proto raději rozložíme $105 = 3 \cdot 5 \cdot 7$ a budeme řešit kongruence $f(x) \equiv 0$ postupně pro moduly 3, 5, 7. Vypočteme hodnoty polynomu $f(x)$ ve vhodných číslech:

| $x$ | $-3$ | $-2$ | $-1$ | $0$ | $1$ | $2$ | $3$ |
|---|---|---|---|---|---|---|---|
| $f(x)$ | $-10$ | $7$ | $12$ | $11$ | $10$ | $15$ | $32$ |

Kongruence $f(x) \equiv 0 \pmod 3$ má tedy řešení $x \equiv -1 \pmod 3$ (pouze první z čísel 12, 11, 10 je násobkem 3); kongruence $f(x) \equiv 0 \pmod 5$ má řešení $x \equiv 1$ a $x \equiv 2 \pmod 5$; řešením kongruence $f(x) \equiv 0 \pmod 7$ je $x \equiv -2 \pmod 7$.

Zbývá tedy vyřešit dvě soustavy kongruencí:

$$\begin{aligned} x &\equiv -1 \pmod 3, \\ x &\equiv \phantom{-}1 \pmod 5, \\ x &\equiv -2 \pmod 7 \end{aligned} \qquad \text{a} \qquad \begin{aligned} x &\equiv -1 \pmod 3, \\ x &\equiv \phantom{-}2 \pmod 5, \\ x &\equiv -2 \pmod 7. \end{aligned}$$

Vyřešením těchto soustav zjistíme, že řešeními dané kongruence $f(x) \equiv 0 \pmod{105}$ jsou všechna celá čísla $x$ splňující $x \equiv 26 \pmod{105}$ nebo $x \equiv 47 \pmod{105}$.



Ne vždy je (tak jako v předchozím příkladu) možné kongruenci nahradit soustavou kongruencí modulo prvočísla – je-li původní modul násobkem vyšší mocniny prvočísla, tak se této mocniny výše uvedeným postupem „nezbavíme“. Ani takovou kongruenci modulo mocnina prvočísla ale nemusíme řešit zkoušením všech možností. Efektivnější nástroj nám dává následující věta.

**10.27. Věta** (Henselovo lemma)**.** *Nechť $p$ je prvočíslo, $f(x) \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$ je takové, že $p \mid f(a)$, $p \nmid f'(a)$. Pak pro každé $n \in \mathbb{N}$ má soustava*

$$\begin{aligned} x &\equiv a \pmod p, \\ f(x) &\equiv 0 \pmod{p^n} \end{aligned}$$

*právě jedno řešení modulo $p^n$.*

Důkaz. Budeme postupovat indukcí vzhledem k $n$. V případě $n = 1$ jde v případě kongruence $f(x) \equiv 0 \pmod{p^1}$ pouze o jinak zapsaný předpoklad, že číslo $a$ splňuje $p \mid f(a)$. Nechť dále $n > 1$ a věta platí pro $n-1$. Je-li $x$ řešením dané soustavy pro $n$, je řešením této soustavy i pro $n-1$. Označíme-li jedno z řešení soustavy pro $n-1$ jako $c_{n-1}$, pak můžeme hledat řešení soustavy pro $n$ ve tvaru

$$x = c_{n-1} + k \cdot p^{n-1}, \quad \text{kde } k \in \mathbb{Z}.$$

která je ekvivalentní kongruenci

$$2^{2^{2^{2n-1}}} \equiv 2^{2^2} \pmod{127}.$$

Protože $2^7 = 128 \equiv 1 \pmod{127}$, je řád čísla 2 modulo 127 roven sedmi a dokazovaná kongruence je tak podle 10.17 ekvivalentní s kongruencí

$$2^{2^{2n-1}} \equiv 2^2 \pmod{7}.$$

Podobně protože řádem dvojky modulo 7 je číslo 3, dostaneme ekvivalentní kongruenci

$$2^{2n-1} \equiv 2 \pmod{3},$$
$$(-1)^{2n-1} \equiv -1 \pmod{3},$$

která je zřejmě splněna (mohli jsme rovněž mechanicky postupovat dále – řád 2 modulo 3 je roven 2, atd.). Tvrzení je tak dokázáno. □

**10.54.** Rozhodněte, pro která přirozená čísla $n$ je číslo $n \cdot 2^n + 1$ dělitelné sedmi.



**Řešení.** Hledáme řešení kongruence

$$n \cdot 2^n \equiv -1 \pmod{7}.$$

Možná je vhodné upozornit, že zde není možné využít tvrzení 10.22, protože $n \cdot 2^n$ není polynom v $n$ a nemáme zaručeno (a ani tomu tak není), že čísla kongruentní modulo sedm budou dávat stejné zbytky modulo 7 i pod dosazení do tohoto výrazu.

Všimněme si ale, že číslo 2 modulo 7 má řád 3 a rozlišme proto přirozená čísla $n$ podle toho, jaký dávají zbytek po dělení třemi.

Pro $n \equiv 0 \pmod 3$ dostaneme $2^n \equiv 1 \pmod 7$ a řešená kongruence je tak ekvivalentní s kongruencí $n \equiv -1 \pmod 7$. Spojením podmínek $n \equiv 0 \pmod 3$ a $n \equiv -1 \pmod 7$ pomocí Čínské zbytkové věty dostaneme řešení $n \equiv 6 \pmod{21}$.

Pro $n \equiv 1 \pmod 3$ nyní máme $2^n \equiv 2 \pmod 7$ a řešená kongruence je tak tvaru $2n \equiv -1 \pmod 7$, což je ekvivalentní s kongruencí $n \equiv 3 \pmod 7$. Z podmínek $n \equiv 1 \pmod 3$ a $n \equiv 3 \pmod 7$ dostaneme řešení $n \equiv 10 \pmod{21}$.

Konečně pro $n \equiv 2 \pmod 3$ je $2^n \equiv 4 \pmod 7$ a řešením kongruence $4n \equiv -1 \pmod 7$ je $n \equiv 5 \pmod 7$ a celkově $n \equiv 5 \pmod{21}$.

Hledanými řešeními jsou všechna přirozená čísla $n$ splňující $n \equiv 5, 6, 10 \pmod{21}$. □

Je třeba zjistit, pro která $k$ platí $f\left(c_{n-1} + k \cdot p^{n-1}\right) \equiv 0 \pmod{p^n}$. Víme, že $p^{n-1} \mid f\left(c_{n-1} + k \cdot p^{n-1}\right)$ a užijme binomickou větu pro $f(x) = a_m x^m + \cdots + a_1 x + a_0$, kde $a_0, \ldots, a_m \in \mathbb{Z}$. Máme

$$\left(c_{n-1} + k \cdot p^{n-1}\right)^i \equiv c_{n-1}^i + i \cdot c_{n-1}^{i-1} \cdot k p^{n-1} \pmod{p^n},$$

a proto

$$f\left(c_{n-1} + k \cdot p^{n-1}\right) \equiv f(c_{n-1}) + k \cdot p^{n-1} f'(c_{n-1}).$$

Odtud

$$f\left(c_{n-1} + k \cdot p^{n-1}\right) \equiv 0 \pmod{p^n} \iff$$
$$\iff 0 \equiv \frac{f(c_{n-1})}{p^{n-1}} + k \cdot f'(c_{n-1}) \pmod{p}.$$

Protože $c_{n-1} \equiv a \pmod p$, dostaneme $f'(c_{n-1}) \equiv f'(a) \not\equiv 0 \pmod p$, tedy $(f'(c_{n-1}), p) = 1$. Podle věty o řešitelnosti lineárních kongruencí odtud vidíme, že (modulo $p$) existuje právě jedno řešení $k$ této kongruence, a protože $c_{n-1}$ bylo podle indukčního předpokladu jediné řešení modulo $p^{n-1}$, je číslo $c_{n-1} + k \cdot p^{n-1}$ jediným řešením dané soustavy modulo $p^n$. □

**Příklad.** Řešme kongruenci

$$3x^2 + 4 \equiv 0 \pmod{49}.$$

Ekvivalentními úpravami (např. tak, že vyřešíme lineární kongruenci $3y \equiv 1 \pmod{49}$ a vynásobíme číslem $y \equiv 33$ obě strany kongruence) upravíme kongruenci na tvar $x^2 \equiv 15 \pmod{7^2}$. Dále postupujeme podle konstruktivního důkazu Henselova lemmatu.

Nejprve řešíme kongruenci $x^2 \equiv 15 \equiv 1 \pmod 7$, která má nejvýše 2 řešení a těmi zřejmě jsou $x \equiv \pm 1 \pmod 7$. Tato řešení vyjádříme ve tvaru $x = \pm 1 + 7t$, kde $t \in \mathbb{Z}$, a dosadíme do kongruence modulo 49, odkud dostaneme řešení $x \equiv \pm 8 \pmod{49}$ (pokud by nás zajímal pouze počet řešení, tak bychom ani nemuseli výpočet dokončit, protože přímo z Henselova lemmatu plyne, že každé řešení modulo 7 dá jediné řešení modulo 49, neboť pro $f(x) = x^2 - 15$ máme $7 \nmid f'(\pm 1)$).

**10.28. Kongruence s prvočíselným modulem.** Řešení obecných kongruencí vyššího stupně jsme tedy převedli na řešení kongruencí modulo prvočíslo. Ukazuje se, že zde je největší „kámen úrazu“, protože pro tyto kongruence žádný o mnoho efektivnější obecný postup než je vyzkoušení všech možností není znám. Uvedeme alespoň několik obecných tvrzení ohledně řešitelnosti a počtu řešení takových kongruencí. V dalších odstavcích poté dokážeme podrobnější výsledky v některých speciálních případech.



**Věta.** *Buď $p$ prvočíslo, $f(x) \in \mathbb{Z}[x]$. Libovolná kongruence $f(x) \equiv 0 \pmod p$ je ekvivalentní s kongruencí stupně nejvýše $p - 1$.*

Důkaz. Protože pro libovolné $a \in \mathbb{Z}$ platí $p \mid a^p - a$ (důsledek Malé Fermatovy věty), jsou řešením kongruence $x^p - x \equiv 0 \pmod p$ všechna celá čísla. Vydělíme-li polynom $f(x)$ se zbytkem polynomem $x^p - x$, dostaneme

$$f(x) = q(x) \cdot \left(x^p - x\right) + r(x)$$

pro vhodné $f(x), r(x) \in \mathbb{Z}$, kde stupeň $r(x)$ je menší než stupeň dělitele tedy než $p$. Dostáváme tak, že kongruence $r(x) \equiv 0$

**10.55.** Dokažte, že pro libovolné přirozené číslo $n$ je číslo $2n^4+n^3+$ $+50$ dělitelné šesti, právě když je číslo $2\cdot4^n+3^n+50$ dělitelné třinácti.



**Řešení.** Výraz $f(n) = 2n^4 + n^3 + 50$ je polynomem v $n$, a je proto možné využít tvrzení 10.22, tj. stačí prověřit všechny možné zbytky modulo 6. Vzhledem k tomu, že řád čísla 4 modulo 13 je roven 6 a řád 3 modulo 13 je roven 3, stačí i ve druhém případě podle 10.17 prověřit všechny možné zbytky $n$ po dělení šesti.

V prvním případě vypočteme

| $n$ | | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| $f(n)$ | mod 6 | 2 | 5 | 0 | 5 | 2 | 3 |

a kongruenci $f(n) \equiv 0 \pmod 6$ tak vyhovují ta přirozená čísla $n$, pro něž platí $n \equiv 2 \pmod 6$.

Ve druhém případě postupně vypočítáme

| $n$ | | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| $4^n$ | mod 13 | 1 | 4 | 3 | $-1$ | $-4$ | $-3$ |
| $3^n$ | mod 13 | 1 | 3 | 9 | 1 | 3 | 9 |
| $2\cdot4^n+3^n-2$ | mod 13 | 1 | 9 | 0 | $-3$ | $-7$ | 1 |

a stejně jako v prvním případě kongruenci $2\cdot4^n + 3^n + 50 \equiv 0 \pmod{13}$ vyhovují právě ta $n$, pro něž $n \equiv 2 \pmod 6$. □

**10.56. Jiný důkaz Wilsonovy věty.** Dokažte, že pro každé prvočíslo $p$ platí



$$(p-1)! \equiv -1 \pmod p.$$

**Řešení.** Pro $p = 2$ je tvrzení zřejmé, dále uvažujme jen lichá prvočísla $p$. Řešením kongruence

$$(x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \pmod p$$

je podle Fermatovy věty libovolné $a \in \mathbb{Z}$, které není násobkem $p$, tj. kongruence má $p-1$ řešení. Přitom je ale její stupeň roven $p-2$ (tedy menší než počet řešení), proto jsou podle 10.28 všechny koeficienty polynomu na levé straně kongruence násobkem $p$, speciálně absolutní člen, který je roven $(p-1)!+1$. Tím je Wilsonova věta dokázána. □

**10.57.** Řešte kongruenci

$$x^2 \equiv 18 \pmod{63}.$$

**Řešení.** Protože je $(18, 63) = 9$, musí platit $9 \mid x^2$, tj. $3 \mid x$. Položíme-li $x = 3x_1$, $x_1 \in \mathbb{Z}$, dostáváme ekvivalentní kongruenci $x_1^2 \equiv 2 \pmod 7$, která již splňuje omezení na nesoudělnost modulu a pravé strany kongruence. Podle věty 10.29 víme, že má nejvýše 2 řešení a snadno se vidí, že jimi jsou $x_1 \equiv \pm3 \pmod 7$, tj. $x_1 \equiv \pm3, \pm10, \pm17, \pm24, \pm31, \pm38, \pm45, \pm52, \pm59 \pmod{63}$. $\pmod p$ je ekvivalentní kongruenci $f(x) \equiv 0 \pmod p$ a je přitom stupně nejvýše $p-1$. □

**10.29. Věta.** *Buď $p$ prvočíslo, $f(x) \in \mathbb{Z}[x]$. Má-li kongruence $f(x) \equiv 0 \pmod p$ více než $\deg(f)$ řešení, pak jsou všechny koeficienty polynomu $f$ násobkem $p$.*

Důkaz. V jazyce algebry jde vlastně o počet kořenů nenulového polynomu nad konečným tělesem $\mathbb{Z}_p$, kterých je podle 11.17 nejvýše $\deg(f)$. □

**10.30. Binomické kongruence.** V této části se zaměříme na řešení speciálních typů polynomiálních kongruencí vyššího stupně, tzv. *binomických kongruencí*. Jde o analogii binomických rovnic, kdy polynomem $f(x)$ je dvojčlen $x^n - a$. Snadno se ukáže, že se můžeme omezit na případ, kdy je $a$ nesoudělné s modulem kongruence – v opačném případě totiž vždy můžeme pomocí ekvivalentních úprav kongruenci na tento případ buď převést nebo rozhodnout, že kongruence není řešitelná.



Kvadratický a mocninný zbytek

Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Číslo $a$ nazveme *$n$-tým mocninným zbytkem modulo $m$*, pokud je kongruence

$$x^n \equiv a \pmod m$$

řešitelná. V opačném případě $a$ nazveme *$n$-tým mocninným nezbytkem modulo $m$*.

Pro $n = 2, 3, 4$ používáme termíny kvadratický, kubický a bikvadratický zbytek, resp. nezbytek modulo $m$.

Ukážeme, jakým způsobem řešit binomické kongruence modulo $m$, pokud modulo $m$ existují primitivní kořeny (tedy zejména je-li modul liché prvočíslo nebo jeho mocnina).

**10.31. Věta.** *Buď $m \in \mathbb{N}$ takové, že modulo $m$ existují primitivní kořeny. Dále nechť $a \in \mathbb{Z}$, $(a, m) = 1$. Pak kongruence $x^n \equiv a \pmod m$ je řešitelná (tj. $a$ je $n$-tý mocninný zbytek modulo $m$), právě když $a^{\varphi(m)/d} \equiv 1 \pmod m$, kde $d = (n, \varphi(m))$. Přitom je-li tato kongruence řešitelná, má právě $d$ řešení.*

Důkaz. Nechť $g$ je primitivní kořen modulo $m$. Pak existuje pro libovolné $x$ nesoudělné s $m$ jediné $y \in \mathbb{Z}$ (jeho diskrétní logaritmus), s vlastností $0 \le y < \varphi(m)$ tak, že $x \equiv g^y \pmod m$. Podobně pro dané $a$ existuje jediné $b \in \mathbb{Z}$; $0 \le b < \varphi(m)$ tak, že $a \equiv g^b \pmod m$. Řešená binomická kongruence je tedy po této substituci ekvivalentní s kongruencí $(g^y)^n \equiv g^b \pmod m$ a s využitím věty 10.17 tedy i s lineární kongruencí $n\cdot y \equiv b \pmod{\varphi(m)}$.

Tato kongruence

$$n \cdot y \equiv b \pmod{\varphi(m)}$$

je ale řešitelná, právě když $d = (n, \varphi(m)) \mid b$ (a je-li řešitelná, pak má $d$ řešení).

Zbývá dokázat, že $d \mid b$, právě když platí $a^{\varphi(m)/d} \equiv 1 \pmod m$. Kongruence

$$1 \equiv a^{\varphi(m)/d} \equiv g^{b\varphi(m)/d} \pmod m$$

ale platí, právě když $\varphi(m) \mid \frac{b\varphi(m)}{d}$, což je právě když $d \mid b$. □

**Důsledek.** *Za předpokladů předchozí věty, je-li navíc $(n, \varphi(m)) = 1$, má kongruence $x^n \equiv a \pmod m$ vždy řešení, a to jediné. Jinými slovy, umocňování na $n$-tou (kde $n$*

Řešeními původní kongruence jsou tedy $x \equiv 3x_1 \pmod{63}$, tj. $x \equiv \pm 9, \pm 12, \pm 30 \pmod{63}$. □

**10.58.** Řešte kongruenci

$$x^3 \equiv 3 \pmod{18}.$$

**Řešení.** Protože je $(3, 18) = 3$, nutně $3 \mid x$. Užijeme-li, podobně jako výše, substituci $x = 3 \cdot x_1$, dostáváme kongruenci

$$27x_1^3 \equiv 3 \pmod{18},$$

která zřejmě nemá řešení, protože $(27, 18) \nmid 3$. □

**10.59. Kvadratické kongruence.** Nejprve uvedeme několik úloh, v nichž dokážeme, že vlastnosti Jacobiho symbolu jsou obdobné vlastnostem Legendreova symbolu, čímž se zbavíme nutnosti rozkládat čísla, která se objevují v úpravách Legendreova symbolu, na prvočísla.



Dokažte, že pro lichá přirozená čísla $b$, $b'$ a celá čísla $a$, $a_1$, $a_2$ platí (ve všech případech jde o Jacobiho symbol):

i) je-li $a_1 \equiv a_2 \pmod{b}$, pak $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$,
ii) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$,
iii) $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$.

**Řešení.** Důkazy ihned vyplývají z definice Jacobiho symbolu a z vlastnosti multiplikativity Legendreova symbolu. □

**10.60.** Dokažte, že pro lichá $a, b \in \mathbb{N}$ platí

i) $\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}$,
ii) $\frac{a^2b^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod{2}$.

**Řešení.**

i) Protože číslo $(a-1)(b-1) = (ab-1) - (a-1) - (b-1)$ je násobek čtyř, dostáváme $(ab-1) \equiv (a-1) + (b-1) \pmod{4}$, odkud vydělením dvěma dostaneme potřebné.
ii) Podobně jako výše $(a^2-1)(b^2-1) = (a^2b^2-1) - (a^2-1) - (b^2-1)$ je násobek 16, proto dostáváme $(a^2b^2-1) \equiv (a^2-1)+(b^2-1) \pmod{16}$, odkud vydělením osmi (viz též příklad ‖10.2‖) dostaneme potřebné. □

**10.61.** Dokažte, že pro lichá $a_1, \ldots, a_k \in \mathbb{N}$ platí

i) $\frac{\prod_{\ell=1}^k a_\ell - 1}{2} \equiv \sum_{\ell=1}^k \frac{a_\ell - 1}{2} \pmod{2}$,
ii) $\frac{\prod_{\ell=1}^k a_\ell^2 - 1}{8} \equiv \sum_{\ell=1}^k \frac{a_\ell^2 - 1}{8} \pmod{2}$.

**Řešení.** Obě tvrzení plynou snadno matematickou indukcí z předchozího příkladu. □

*je nesoudělné s $\varphi(m)$) je bijekce na množině $\mathbb{Z}_m^\times$ invertibilních zbytkových tříd modulo $m$ (jde dokonce o automorfismus grupy $(\mathbb{Z}_m^\times, \cdot)$).*

**10.32. Kvadratické kongruence a Legendreův symbol.** Naším úkolem nyní bude najít efektivní podmínku, jak zjistit, jestli je řešitelná (a případně kolik má řešení) kvadratická kongruence



$$ax^2 + bx + c \equiv 0 \pmod{m}.$$

Z teorie uvedené dříve je snadné vidět, že k rozhodnutí, je-li tato kongruence řešitelná, stačí určit, je-li řešitelná (binomická) kongruence

$$x^2 \equiv a \pmod{p},$$

kde $p$ je liché prvočíslo a $a$ číslo s ním nesoudělné. Kongruenci modulo složené $m$ totiž můžeme rozložit na ekvivalentní soustavu kongruencí modulo jednotlivé faktory čísla $m$, které jsou mocninami prvočísel. Každou takovou kongruenci jsme schopni postupem popsaným v Henselově lemmatu 10.27 převést na kvadratickou kongruenci s prvočíselným modulem. Tuto kongruenci posléze normujeme a doplníme na čtverec a obdržíme výše uvedený tvar.

Pro určení řešitelnosti kongruence můžeme samozřejmě využít větu 10.31 o řešitelnosti binomických kongruencí. Její využití ale často naráží na výpočetní složitost, proto se (nejen) v kvadratickém případě snažíme najít kritérium jednodušší na výpočet.

**Příklad.** Určeme počet řešení kongruence $x^2 \equiv 219 \pmod{383}$.

Protože 383 je prvočíslo a $(2, \varphi(383)) = 2$, z věty 10.31 plyne, že daná kongruence je řešitelná (a má 2 řešení) právě tehdy, když platí $219^{\frac{\varphi(383)}{2}} = 219^{191} \equiv 1 \pmod{383}$. Ověření platnosti není bez použití výpočetní techniky snadné (i když je to v tomto případě ještě „na papíře“ vyčíslitelné). Ukážeme ale, jak tuto podmínku ověřit s pomocí vlastností tzv. Legendreova symbolu daleko snadněji.

### Legendreův symbol

Nechť je $p$ liché prvočíslo, $a$ celé číslo. *Legendreův symbol* definujeme předpisem

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{pro } p \nmid a,\ a \text{ je kvadratický zbytek modulo } p, \\ 0 & \text{pro } p \mid a, \\ -1 & \text{je-li } a \text{ kvadratický nezbytek modulo } p. \end{cases}$$

Legendreův symbol často zapisujeme rovněž jako $(a/p)$ a symbol čteme jako „$a$ vzhledem k $p$“.

**Příklad.** Protože je kongruence $x^2 \equiv 1 \pmod{p}$ řešitelná pro libovolné liché prvočíslo $p$, je $(1/p) = 1$. Dále, $(-1/5) = (4/5) = 1$, protože kongruence $x^2 \equiv -1 \pmod{5}$ je ekvivalentní s kongruencí $x^2 \equiv 4 \pmod{5}$, jejímiž řešeními jsou $x \equiv \pm 2 \pmod{5}$.

Tvrzení následujícího lemmatu budeme velmi často využívat při praktickém vyčíslení Legendreova symbolu.

**10.33. Lemma.** *Nechť $p$ je liché prvočíslo, $a, b \in \mathbb{Z}$ libovolná. Pak platí:*

*(1)* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
*(2)* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

**10.62.** Dokažte zákon kvadratické reciprocity pro Jacobiho symbol, tj. dokažte, že pro lichá $a, b \in \mathbb{N}$ platí

i) $\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}$,

ii) $\left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}$,

iii) $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) \cdot (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$.

**Řešení.** Nechť jako v definici Jacobiho symbolu je $a = p_1 p_2 \cdots p_k$ rozklad čísla $a$ na (lichá) prvočísla.

i) Z vlastností Legendreova symbolu a z výše uvedeného tvrzení plyne

$$\begin{aligned}\left(\frac{-1}{a}\right) &= \left(\frac{-1}{p_1}\right) \cdot \left(\frac{-1}{p_2}\right) \cdots \left(\frac{-1}{p_k}\right) = \\ &= (-1)^{\frac{p_1-1}{2}} \cdots (-1)^{\frac{p_k-1}{2}} = \\ &= (-1)^{\sum_{i=1}^{k} \frac{p_i-1}{2}} = \\ &= (-1)^{\frac{\prod_{i=1}^{k} p_i - 1}{2}} = (-1)^{\frac{a-1}{2}}.\end{aligned}$$

ii) Analogicky jako výše.

iii) Buď dále $b = q_1 q_2 \cdots q_\ell$ rozklad čísla $b$ na (lichá) prvočísla. Platí-li pro některá $p_i, q_j$, že $p_i = q_j$, pak jsou symboly na obou stranách dokazované rovnosti nulové. V opačném případě podle zákona kvadratické reciprocity pro Legendreův symbol platí pro všechny dvojice $p_i, q_j$ vztah

$$\left(\frac{p_i}{q_j}\right) = \left(\frac{q_i}{p_j}\right) \cdot (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}.$$

Proto

$$\begin{aligned}\left(\frac{a}{b}\right) &= \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{p_i}{q_j}\right) = \\ &= \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{q_j}{p_i}\right) \cdot (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = \\ &= \prod_{i=1}^{k}(-1)^{\frac{p_i-1}{2}\sum_{j=1}^{\ell}\frac{q_j-1}{2}} \prod_{j=1}^{\ell}\left(\frac{q_j}{p_i}\right) = \\ &= \prod_{i=1}^{k}(-1)^{\frac{p_i-1}{2}\frac{\prod_{j=1}^{\ell} q_j - 1}{2}} \prod_{j=1}^{\ell}\left(\frac{q_j}{p_i}\right) = \\ &= \prod_{i=1}^{k}(-1)^{\frac{p_i-1}{2}\frac{b-1}{2}} \prod_{j=1}^{\ell}\left(\frac{q_j}{p_i}\right) = \\ &= (-1)^{\frac{b-1}{2}\sum_{i=1}^{k}\frac{p_i-1}{2}} \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{q_j}{p_i}\right) = \\ &= (-1)^{\frac{a-1}{2}\frac{b-1}{2}}\left(\frac{b}{a}\right).\end{aligned}$$

*(3) Pro $a \equiv b \pmod p$ platí $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

Důkaz. (1) Pro $p \mid a$ je tvrzení zřejmé; pokud je $a$ kvadratický zbytek modulo $p$, pak tvrzení plyne z věty o řešitelnosti binomických kongruencí, které udává (v tomto případě je $(\varphi(p), 2) = 2$) jako nutnou a postačující podmínku řešitelnosti kongruence $x^2 \equiv a \pmod p$ splnění vztahu

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Z téže věty plyne, že v případě kvadratického nezbytku je $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. Pak ale, protože podle Fermatovy věty platí $p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$, nutně $p \mid a^{\frac{p-1}{2}} + 1$, tj. $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

(2) Podle (1) je

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Protože jsou ale hodnoty Legendreova symbolu prvky množiny $\{-1, 0, 1\}$, z této kongruence ihned plyne rovnost levé a pravé strany.

(3) Zřejmé z definice.

□

**Důsledek.** *(1) V libovolné redukované soustavě zbytků modulo $p$ je stejný počet kvadratických zbytků a nezbytků.*

*(2) Součin dvou kvadratických zbytků je zbytek, součin dvou nezbytků je zbytek, součin zbytku a nezbytku je nezbytek.*

*(3) $(-1/p) = (-1)^{\frac{p-1}{2}}$, tj. kongruence $x^2 \equiv -1 \pmod p$ je řešitelná právě tehdy, když $p \equiv 1 \pmod 4$.*

Důkaz. (1) Mezi prvky redukované soustavy zbytků modulo $p$ (můžeme uvážit např. množinu $\{-\frac{p-1}{2}, \ldots, -1, 1, \frac{p-1}{2}\}$) jsou kvadratickými zbytky právě čísla kongruentní s některým z čísel $(\pm 1)^2, \ldots, (\pm\frac{p-1}{2})^2$. Těch je ale právě $\frac{p-1}{2}$, těch ostatních (tedy kvadratických nezbytků) je pak $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$.

(2) Plyne ihned z části (2) předchozího lemmatu.

(3) Z části (1) lemmatu plyne, že $(-1/p) \equiv (-1)^{\frac{p-1}{2}} \pmod p$, obě strany ale nabývají pouze hodnot $\pm 1$, proto si musí být rovny.

□



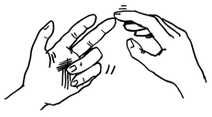
Již s využitím těchto základních tvrzení o hodnotách Legendreova symbolu jsme schopni dokázat větu o nekonečnosti počtu prvočísel tvaru $4k+1$ (viz odstavec 10.10).

**Tvrzení.** *Prvočísel tvaru $4k + 1$ je nekonečně mnoho.*

Důkaz. Budeme postupovat sporem. Předpokládejme, že $p_1, p_2, \ldots, p_\ell$ jsou všechna prvočísla tvaru $4k + 1$ a uvažme číslo $N = (2p_1 \cdots p_\ell)^2 + 1$. Toto číslo je opět tvaru $4k + 1$. Pokud je $N$ prvočíslo, dostáváme ihned spor (protože $N$ je jistě větší než kterékoliv z $p_1, p_2, \ldots, p_\ell$). Pokud je naopak složené, musí existovat prvočíslo $p$ dělící $N$. Zřejmě přitom žádné z prvočísel $2, p_1, p_2, \ldots, p_\ell$ není dělitelem $N$, proto ke sporu stačí dokázat, že $p$ je rovněž tvaru $4k + 1$. Z platnosti kongruence $(2p_1 \cdots p_\ell)^2 \equiv -1 \pmod p$, dostáváme, že $(-1/p) = 1$, a to platí podle předchozího důsledku právě tehdy, je-li $p \equiv 1 \pmod 4$. I v případě složeného $N$ jsme tedy obdrželi prvočíslo $p$,

Během výpočtu jsme využili výsledek z části (i) předchozího příkladu. □

**Aplikace Legendreova a Jacobiho symbolu.**



Primární motivací k zavedení Jacobiho symbolu byla potřeba vyčíslení Legendreova symbolu (a tedy rozhodnutí o řešitelnosti kvadratických kongruencí) bez nutnosti rozkladu čísel na prvočísla. Ukažme si proto příklad takového výpočtu.

**10.63.** Rozhodněte o řešitelnosti kongruence $x^2 \equiv 219 \pmod{383}$.

**Řešení.** 383 je prvočíslo, proto bude kongruence řešitelná, bude-li Legendreův symbol $(219/383) = 1$.

$$\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right) = \textit{(Jacobi) 383 i 219 dávají po dělení 4 zbytek 3}$$
$$= -\left(\frac{164}{219}\right) = -\left(\frac{41}{219}\right) = \qquad 164 = 2^2 \cdot 41$$
$$= -\left(\frac{219}{41}\right) = \quad \textit{(Jacobi) 41 dává po dělení 4 zbytek 1}$$
$$= -\left(\frac{14}{41}\right) = -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) =$$
$$= -\left(\frac{7}{41}\right) = \quad \textit{41 dává po dělení 8 zbytek 1}$$
$$= -\left(\frac{41}{7}\right) = \quad \textit{41 dává po dělení 4 zbytek 1}$$
$$= -\left(\frac{-1}{7}\right) = 1 \quad \textit{7 dává po dělení 4 zbytek 3.}$$

□

**10.64.** Nalezněte všechna čísla vyhovující kongruenci

$$x^2 \equiv 7 \pmod{43}.$$

**Řešení.** Legendreův symbol je

$$\left(\frac{7}{43}\right) = -\left(\frac{43}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Odtud plyne, že 7 je kvadratický nezbytek modulo 43, proto neexistuje žádné řešení dané kongruence. □

**10.65.** Nalezněte všechna celá čísla $a$, pro něž bude řešitelná kongruence

$$x^2 \equiv a \pmod{43}.$$

**Řešení.** Úloha navazuje na předchozí příklad, v němž jsme viděli, že číslo 7 této úloze nevyhoví. Stejným způsobem bychom mohli vyzkoušet celou soustavu zbytků modulo 43, ale jde to i jednodušeji – takovými čísly jsou jednak násobky 43 (v tom případě má kongruence nepatřící do původního seznamu všech prvočísel tvaru $4k+1$, což je opět ve sporu s předpokladem konečnosti jejich počtu. □



Nejdůležitější tvrzení, umožňující efektivně určit hodnotu Legendreova symbolu (a tak rozhodnout o řešitelnosti kvadratické kongruence), je tzv. *zákon kvadratické reciprocity*.

ZÁKON KVADRATICKÉ RECIPROCITY

**10.34. Věta.** *Nechť $p, q$ jsou lichá prvočísla. Pak*

*(1)* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

*(2)* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$,

*(3)* $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Věta se v tomto tvaru uvádí zejména proto, že pomocí těchto tří vztahů a základních pravidel pro úpravy Legendreova symbolu jsme schopni vypočítat hodnotu $(a/p)$ pro libovolné celé číslo $a$.



V literatuře se uvádí celá řada důkazů [8], obvykle ovšem využívajících (zejména u těch stručnějších z nich) hlubších znalostí z algebraické teorie čísel. Zde ukážeme elementární důkaz tohoto tvrzení.

Označme jako $S$ redukovanou soustavu nejmenších zbytků (v absolutní hodnotě) modulo $p$, tedy

$$S = \left\{-\tfrac{p-1}{2}, -\tfrac{p-3}{2}, \ldots, -1, 1, \ldots, \tfrac{p-3}{2}, \tfrac{p-1}{2}\right\}.$$

Pro $a \in \mathbb{Z}$, $p \nmid a$, pak dále označme $\mu_p(a)$ počet záporných nejmenších zbytků (v absolutní hodnotě) čísel

$$1 \cdot a, 2 \cdot a, \ldots, \frac{p-1}{2} \cdot a,$$

tj. pro každé z těchto čísel určíme, se kterým číslem z množiny $S$ je kongruentní a spočítáme počet záporných z nich. Budeme přitom (v případě, že je z kontextu jasné, o které hodnoty $a$, $p$ jde) parametry u $\mu$ vynechávat a místo $\mu_p(a)$ psát pouze $\mu$.

**Příklad.** Pro prvočíslo $p = 11$ a číslo $a = 3$ určíme $\mu_p(a)$.

Uvažovanou redukovanou soustavou zbytků je v tomto případě $S = \{-5, \ldots, -1, 1, , \ldots, 5\}$ a pro $a = 3$ vypočteme

$$1 \cdot 3 \equiv \quad 3 \pmod{11}$$
$$2 \cdot 3 \equiv -5 \pmod{11}$$
$$3 \cdot 3 \equiv -2 \pmod{11}$$
$$4 \cdot 3 \equiv \quad 1 \pmod{11}$$
$$5 \cdot 3 \equiv \quad 4 \pmod{11},$$

odkud $\mu_{11}(3) = 2$.

V následujícím tvrzení ukážeme, že toto číslo úzce souvisí s Legendreovým symbolem – ukážeme, že hodnotu symbolu $(3/11)$ lze vypočítat s pomocí funkce $\mu$ jako $(-1)^{\mu_{11}(3)} = (-1)^2 = 1$.

**Lemma** (Gaussovo)**.** *Je-li $p$ liché prvočíslo, $a \in \mathbb{Z}$, $p \nmid a$, pak pro hodnotu Legendreova symbolu platí*

$$\left(\frac{a}{p}\right) = (-1)^{\mu_p(a)}.$$

[8] V roce 2000 uváděl F. Lemmermeyer 233 důkazů – viz F. Lemmermeyer, *Reciprocity laws. From Euler to Eisenstein*, Springer. 2000

jedno řešení) a jednak kvadratické zbytky modulo 43, které nejsnáze určíme tak, že spočítáme druhé mocniny všech prvků některé redukované soustavy zbytků modulo 43.

Kvadratickými zbytky jsou čísla kongruentní s čísly $(\pm1)^2, (\pm2)^2, (\pm3)^2, \dots, (\pm21)^2$ modulo 43 a řešením úlohy je tedy množina všech celých čísel kongruentních s některým z čísel 1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41. □

**10.66.** Odvoďte přímým výpočtem z Gaussova lemmatu, že



$$(-1/p) = (-1)^{\frac{p-1}{2}} \quad \text{a} \quad (2/p) = (-1)^{\frac{p^2-1}{8}}.$$

**Řešení.** Pro výpočet $(-1/p)$ v prvním případě uvažme, že $\mu$ udává počet záporných nejmenších zbytků (v absolutní hodnotě) čísel z množiny

$$\left\{-1, -2, \dots, -\tfrac{p-1}{2}\right\}.$$

Ta jsou ale zřejmě přímo požadovanými zbytky a jsou všechna záporná, proto je v tomto případě $\mu = \frac{p-1}{2}$ a $(-1/p) = (-1)^{\frac{p-1}{2}}$.

Ve druhém případě potřebujeme vyjádřit počet záporných nejmenších zbytků (v absolutní hodnotě) čísel z množiny

$$\left\{1 \cdot 2, 2 \cdot 2, 3 \cdot 2 \dots, \tfrac{p-1}{2} \cdot 2\right\}.$$

Pro libovolné $k \in \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ dá číslo $2k$ záporný zbytek, právě když je $2k > \frac{p-1}{2}$, tj. pro $k > \frac{p-1}{4}$. Zbývá pouze určit počet vyhovujících $k$.

Je-li $p \equiv 1 \pmod 4$, pak je tento počet roven $\frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$, proto

$$\left(\frac{-1}{p}\right) = (-1)^{\mu} = (-1)^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}\cdot\frac{p+1}{2}} = (-1)^{\frac{p^2-1}{8}},$$

neboť $\frac{p+1}{2}$ je v tomto případě liché.

Podobně pro $p \equiv 3 \pmod 4$ je počet takových $k$ roven číslu $\frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$, proto

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p+1}{4}} = (-1)^{\frac{p+1}{4}\cdot\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}},$$

neboť $\frac{p-1}{2}$ je v tomto případě liché. □

**10.67.** Rozhodněte, zda je řešitelná kongruence $x^2 \equiv 38 \pmod{165}$.

**Řešení.** Jacobiho symbol je roven

$$\left(\tfrac{38}{165}\right) = \left(\tfrac{2}{165}\right)\cdot\left(\tfrac{19}{165}\right) = \left(\tfrac{2}{3}\right)\cdot\left(\tfrac{2}{5}\right)\cdot\left(\tfrac{2}{11}\right)\cdot\left(\tfrac{19}{3}\right)\cdot\left(\tfrac{19}{5}\right)\cdot\left(\tfrac{19}{11}\right) =$$
$$= (-1)^3\left(\tfrac{1}{3}\right)\cdot\left(\tfrac{-1}{5}\right)\cdot\left(\tfrac{2}{11}\right)^3 = 1.$$

Důkaz. Pro každé číslo $i \in \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ určíme $m_i \in \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ tak, že $i \cdot a \equiv \pm m_i \pmod p$. Snadno se vidí, že pokud $k, l \in \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ jsou různá, jsou různé i hodnoty $m_k, m_l$ (rovnost $m_k = m_l$ by znamenala, že $k \cdot a \equiv \pm l \cdot a \pmod p$, a tedy $k \equiv \pm l \pmod p$, což nelze splnit jinak, než že $k = l$).

Proto splývají obě množiny $\{1, 2, \dots, \frac{p-1}{2}\}$ a $\{m_1, m_2, \dots, m_{\frac{p-1}{2}}\}$, což ilustruje též předchozí příklad. Vynásobením kongruencí

$$1 \cdot a \equiv \pm m_1 \pmod p,$$
$$2 \cdot a \equiv \pm m_2 \pmod p,$$
$$\vdots$$
$$\frac{p-1}{2} \cdot a \equiv \pm m_{\frac{p-1}{2}} \pmod p$$

dostáváme

$$\tfrac{p-1}{2}! \cdot a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \cdot \tfrac{p-1}{2}! \pmod p,$$

neboť mezi pravými stranami kongruencí je právě $\mu$ záporných hodnot. Po vydělení obou stran číslem $\frac{p-1}{2}!$ dostáváme požadované tvrzení s využitím toho, že podle lemmatu 10.33 platí $(a/p) \equiv a^{\frac{p-1}{2}} \pmod p$, □

S využitím Gaussova lemmatu nyní *zákon kvadratické reciprocity* dokážeme.

Důkaz zákona kvadratické reciprocity. První část již máme dokázánu, v dalším nejprve odvodíme mezivýsledek, který využijeme v důkazu obou zbylých částí.

Nechť je dále $a \in \mathbb{Z}$, $p \nmid a$, $k \in \mathbb{N}$ a nechť $[x]$ (resp. $\langle x\rangle$) značí celou (resp. necelou) část reálného čísla $x$. Pak

$$\left[\frac{2ak}{p}\right] = \left[2\left[\frac{ak}{p}\right] + 2\left\langle\frac{ak}{p}\right\rangle\right] = 2\left[\frac{ak}{p}\right] + \left[2\left\langle\frac{ak}{p}\right\rangle\right].$$

Tento výraz je lichý právě tehdy, když je $\langle\frac{ak}{p}\rangle > \frac{1}{2}$, tj. právě tehdy, je-li nejmenší zbytek (v absolutní hodnotě) čísla $ak$ modulo $p$ záporný (zde by měl pozorný čtenář zaznamenat návrat od výpočtů zdánlivě nesouvisejících výrazů k podmínkám blízkým Legendreovu symbolu). Číslo $\mu_p(a)$ má tedy stejnou paritu jako $\left[\frac{2ak}{p}\right]$, odkud s využitím Gaussova lemmatu dostáváme

$$\left(\frac{a}{p}\right) = (-1)^{\mu_p(a)} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{2ak}{p}\right]}.$$

Je-li navíc $a$ liché, je $a + p$ sudé číslo a dostáváme

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{2}{p}\right)^2\cdot\left(\frac{\frac{a+p}{2}}{p}\right) =$$
$$= (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{(a+p)k}{p}\right]} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]}\cdot(-1)^{\sum_{k=1}^{\frac{p-1}{2}}k}.$$

Protože součtem aritmetické řady $\sum_{k=1}^{\frac{p-1}{2}} k$ je $\frac{1}{2}\,\frac{p-1}{2}\,\frac{p+1}{2} = \frac{p^2-1}{8}$, dostáváme (pro liché $a$) vztah

$$\left(\frac{2}{p}\right)\cdot\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]}\cdot(-1)^{\frac{p^2-1}{8}},$$

Odtud nelze vyloučit existenci řešení. Ovšem rozdělením na soustavu kongruencí podle faktorů modulu máme

$$\begin{aligned} x^2 &\equiv -1 \pmod 3,\\ x^2 &\equiv \ \ 3 \pmod 5,\\ x^2 &\equiv \ \ 5 \pmod{11} \end{aligned}$$

a lehce se vidí, že první dvě z těchto kongruencí nemají řešení, a proto nemá řešení ani zadaná kongruence. Konkrétně

$$\left(\tfrac{-1}{3}\right) = -1 \quad \text{a} \quad \left(\tfrac{3}{5}\right) = \left(\tfrac{5}{3}\right) = \left(\tfrac{2}{3}\right) = -1\,. \qquad \square$$

**10.68.** Řešte kongruenci $x^2 - 23 \equiv 0 \pmod{77}$.

**Řešení.** Rozdělením modulu na faktory dostaneme

$$\begin{aligned} x^2 - 1 &\equiv 0 \pmod{11},\\ x^2 - 2 &\equiv 0 \pmod 7. \end{aligned}$$

Je ihned vidět, že 1 je kvadratický zbytek modulo 11 a že první kongruence soustavy má (jediná dvě) řešení $x \equiv \pm 1 \pmod{11}$. Dále $(2/7) = (9/7) = 1$ a rovněž zde je ihned vidět řešení $x \equiv \pm 3 \pmod 7$.

Dostáváme čtyři jednoduché soustavy (vždy dvou) lineárních kongruencí, jejichž vyřešením obdržíme řešení původní kongruence $x \equiv 10,\ 32,\ 45$ nebo $67 \pmod{77}$. $\square$

**10.69.** Určete modulo která prvočísla je uvedené číslo kvadratickým zbytkem:



i) $3$, ii) $-3$, iii) $6$.

**Řešení.**

i) Hledáme prvočísla $p \neq 3$ taková, že $x^2 \equiv 3 \pmod p$ má řešení. Protože $p = 2$ zjevně vyhovuje, uvažujme dále pouze lichá $p \neq 3$. Pro $p \equiv 1 \pmod 4$ dostáváme ze zákona kvadratické reciprocity $1 = (3/p) = (p/3)$, což nastane právě pro $p \equiv 1 \pmod 3$. Je-li naopak $p \equiv -1 \pmod 4$, pak $1 = (3/p) = -(p/3)$, což platí pro $p \equiv -1 \pmod 3$. Zkombinováním podmínek v těchto dvou případech dostaneme $p \equiv \pm 1 \pmod{12}$, což dá spolu s $p = 12$ množinu všech prvočísel, vyhovujících zadání.

ii) Podmínka $1 = (-3/p) = (-1/p)(3/p)$ bude splněna buď v případě, že $(-1/p) = (3/p) = 1$, nebo pokud $(-1/p) = (3/p) = -1$. V prvním případě (i s využitím řešení předchozí úlohy) to znamená, že $p \equiv 1 \pmod 4$ a $p \equiv \pm 1 \pmod{12}$, ve druhém případě musí zároveň platit $p \equiv -1 \pmod 4$ a $p \equiv \pm 5 \pmod{12}$ – redukovaná soustava zbytků modulo 12 je totiž tvořena např. množinou $\{-5, -1, 1, 5\}$ a protože $(3/p) = 1$ pro $p \equiv \pm 1 \pmod{12}$, nutně pro což pro $a = 1$ dává požadované tvrzení z bodu 2.

Podle již dokázané části 2 a z předchozí rovnosti nyní dostáváme pro lichá čísla $a$

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ak}{p}\right]}. \tag{10.1}$$

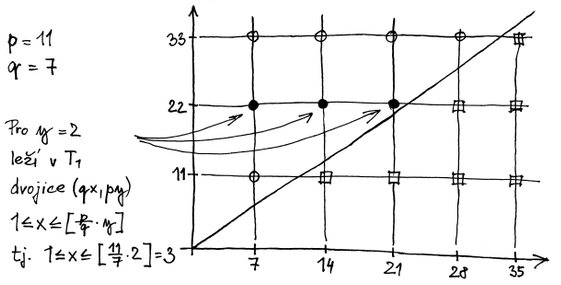
Uvažme nyní pro daná prvočísla $p \neq q$ množinu

$$\begin{aligned} T = \{q \cdot x;\ x \in \mathbb{Z},\ 1 \le x \le (p-1)/2\}\times\\ \times \{p \cdot y;\ y \in \mathbb{Z},\ 1 \le y \le (q-1)/2\}. \end{aligned}$$

Zřejmě je $|T| = \frac{p-1}{2} \cdot \frac{q-1}{2}$. Ukážeme, že rovněž

$$(-1)^{|T|} = (-1)^{\sum_{k=1}^{\frac{2-1}{2}} \left[\frac{pk}{q}\right]} \cdot (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right]},$$

čímž budeme vzhledem k předchozímu hotovi.




Protože pro žádná $x, y$ z přípustného rozsahu nemůže nastat rovnost $qx = py$, můžeme množinu $T$ rozložit na dvě disjunktní podmnožiny $T_1$ a $T_2$ tak, že $T_1 = T \cap \{(u, v);\ u, v \in \mathbb{Z}, u < v\}$, $T_2 = T \setminus T_1$. Zřejmě je $T_1$ počet dvojic $(qx, py)$, kde $x < \frac{p}{q}y$. Protože $\frac{p}{q}y \le \frac{p}{q} \cdot \frac{q-1}{2} < \frac{p}{2}$, je $\left[\frac{p}{q}y\right] \le \frac{p-1}{2}$. Pro pevné $y$ tedy v $T_1$ leží právě ty dvojice $(qx, py)$, pro které $1 \le x \le \left[\frac{p}{q}y\right]$, a tedy $|T_1| = \sum_{y=1}^{(q-1)/2} \left[\frac{p}{q}y\right]$. Analogicky $|T_2| = \sum_{x=1}^{(p-1)/2} \left[\frac{q}{p}x\right]$.

Podle 10.1 je tedy $\left(\frac{p}{q}\right) = (-1)^{|T_1|}$ a $\left(\frac{q}{p}\right) = (-1)^{|T_2|}$ a zákon kvadratické reciprocity je dokázán. $\square$

**Důsledek.** *Buďte $p, q$ lichá prvočísla.*

*(1) $-1$ je kvadratický zbytek pro prvočísla $p$ splňující $p \equiv 1 \pmod 4$ a nezbytek pro prvočísla splňující $p \equiv 3 \pmod 4$.*

*(2) $2$ je kvadratický zbytek pro prvočísla $p$ splňující $p \equiv \pm 1 \pmod 8$ a nezbytek pro prvočísla splňující $p \equiv \pm 3 \pmod 8$.*

*(3) Je-li $p \equiv 1 \pmod 4$ nebo $q \equiv 1 \pmod 4$, je $(p/q) = (q/p)$, pro ostatní lichá $p, q$ je $(p/q) = -(q/p)$.*

Důkaz. (1) Číslo $\frac{p-1}{2}$ je sudé, právě když $4 \mid p - 1$.

(2) Potřebujeme zjistit, pro které lichá prvočísla $p$ je exponent $\frac{p^2-1}{8}$ sudý. Lichá prvočísla mohou dávat modulo 8 zbytek $\pm 1$ nebo $\pm 3$, odkud podle ‖10.15‖ buď $p^2 \equiv 1 \pmod{16}$, nebo $p^2 \equiv 9 \pmod{16}$.

(3) Zřejmé ze zákona kvadratické reciprocity.

$\square$

**Příklad.** Vypočtěme s využitím vlastnosti Legendreova symbolu hodnotu $(79/101)$.

$p \equiv \pm 5 \pmod{12}$ platí $(3/p) = -1$ Dostali jsme tak čtyři soustavy dvou kongruencí, z nichž dvě soustavy řešení nemají a řešením zbylých dvou jsou $p \equiv 1 \pmod{12}$, resp. $p \equiv -5 \pmod{12}$.

iii) V tomto případě $(6/p) = (2/p)(3/p)$ a opět dostáváme dvě možnosti: buď $(2/p) = (3/p) = 1$, nebo $(2/p) = (3/p) = -1$. První případ nastává, pokud $p$ splňuje $p \equiv \pm 1 \pmod{8}$ a současně $p \equiv \pm 1 \pmod{12}$. Vyřešením příslušných soustav lineárních kongruencí získáme podmínku $p \equiv \pm 1 \pmod{24}$. Ve druhém případě pak $p \equiv \pm 3 \pmod{8}$ a zároveň $p \equiv \pm 5 \pmod{12}$, což celkem dá $p \equiv \pm 5 \pmod{24}$.

Poznamenejme ještě, že díky Dirichletově větě 10.12 je ve všech třech případech počet vyhovujících prvočísel nekonečný. □

**10.70.** Následující příklad ukazuje, že pokud je modul kvadratické kongruence prvočíslo $p$ splňující $p \equiv 3 \pmod{4}$, pak umíme nejen rozhodnout o řešitelnosti kongruenci, ale umíme rovněž snadno popsat všechna řešení této kongruence.



Uvažme prvočíslo $p \equiv 3 \pmod{4}$ a číslo $a \in \mathbb{Z}$ splňující $(a/p) = 1$. Dokažte, že pak má kongruence $x^2 \equiv a \pmod{p}$ řešení

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}.$$

**Řešení.** Ověříme snadno zkouškou (s využitím lemmatu 10.33), že platí

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot \left(\tfrac{a}{p}\right) \equiv a \pmod{p}\,. \qquad \square$$

**10.71.** Rozhodněte, je-li kongruence

$$x^2 \equiv 3 \pmod{59}$$

řešitelná a v kladném případě nalezněte její řešení.

**Řešení.** Výpočtem Legendreova symbolu

$$\left(\frac{3}{59}\right) = -\left(\frac{59}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$$

zjistíme, že kongruence má dvě řešení. Z předchozího příkladu navíc ihned vidíme ($59 \equiv 3 \pmod{4}$), že řešením jsou čísla

$$x \equiv \pm 3^{\frac{59+1}{4}} = \pm 3^{15} \equiv (3^5)^3 \equiv$$
$$\equiv \pm 7^3 = \pm 343 \equiv \mp 11 \pmod{59},$$

neboť $3^5 = 243 \equiv 7 \pmod{59}$. □

$$\left(\frac{79}{101}\right) = \left(\frac{101}{79}\right) = \quad \textit{neboť } 101 \textit{ dává po dělení } 4 \textit{ zbytek } 1$$
$$= \left(\frac{22}{79}\right) =$$
$$= \left(\frac{2}{79}\right) \cdot \left(\frac{11}{79}\right) =$$
$$= \left(\frac{11}{79}\right) = \quad \textit{neboť } 79 \textit{ dává po dělení } 8 \textit{ zbytek } -1$$
$$= (-1)\left(\frac{79}{11}\right) = \quad \textit{neboť } 11 \equiv 79 \equiv 3 \pmod{4}$$
$$= (-1)\left(\frac{2}{11}\right) = 1 \quad \textit{neboť } 11 \equiv 3 \pmod{8}$$



Vyčíslení Legendreova symbolu (jak jsme viděli i v předchozím příkladu) umožňuje používat zákon kvadratické reciprocity jen na prvočísla a nutí nás tak provádět v průběhu výpočtu faktorizaci čísel na prvočísla, což je výpočetně velmi náročná operace. Toto lze obejít rozšířením definice Legendreova symbolu na tzv. *Jacobiho symbol* s podobnými vlastnostmi.

**Definice.** Nechť $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $2 \nmid b$. Nechť $b = p_1 p_2 \cdots p_k$ je rozklad $b$ na (lichá) prvočísla (výjimečně neseskupujeme stejná prvočísla do mocniny, ale vypisujeme každé zvlášť, např. $135 = 3 \cdot 3 \cdot 3 \cdot 5$). Symbol

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right)$$

se nazývá *Jacobiho symbol*.

Níže ukážeme, že Jacobiho symbol má podobné vlastnosti jako symbol Legendreův. S jednou podstatnou odchylkou – neplatí totiž obecně, že z $(a/b) = 1$ plyne řešitelnost kongruence $x^2 \equiv a \pmod{b}$.

**Příklad.**

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$$

a přitom kongruence

$$x^2 \equiv 2 \pmod{15}$$

není řešitelná (kongruence $x^2 \equiv 2$ totiž není řešitelná modulo 3 ani modulo 5).

**Věta** (zákon kvadratické reciprocity pro Jacobiho symbol)**.** *Nechť $a, b \in \mathbb{N}$ jsou lichá. Pak*

*(1)* $\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}$,

*(2)* $\left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}$,

*(3)* $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) \cdot (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$.

Důkaz. Důkaz je snadný s využitím zákona kvadratické reciprocity pro Legendreův symbol. Viz příklad ‖10.62‖. □

### D. Diofantické rovnice

Už ve třetím století našeho letopočtu se Diofantos z Alexandrie zabýval řešením rovnic, ve kterých za řešení připouštěl jen celá čísla. Není se čemu divit, vždyť v mnoha praktických úlohách, vedoucích k rovnicím, nemusí mít neceločíselná řešení rozumnou interpretaci. Jde například o úlohu, jak pomocí existujících (korunových či eurových) mincí přesně zaplatit konkrétní částku. Takové rovnice, u nichž nás zajímají jen celočíselná řešení, se na Diofantovu počest se nazývají *diofantické rovnice*.

Hezkým příkladem diofantické rovnice je i Eulerův vztah

$$s - h + v = 2$$

z teorie grafů dávající do souvislosti počet stěn, hran a vrcholů rovinného grafu. Hledáme-li navíc pouze pravidelné grafy, dostáváme se k otázce existence tzv. Platónských těles, která je možné elegantně popsat právě jako řešení této diofantické rovnice – více viz 12.28.

Pro řešení těchto rovnic bohužel neexistuje žádná univerzální metoda. Dokonce neexistuje ani metoda (jinými slovy algoritmus), která by určila, jestli má obecná polynomiální diofantická rovnice řešení. Tato otázka je známá pod názvem *10. Hilbertův problém* a důkaz neexistence algoritmu podal Юрий Матиясевич (Yuri Matiyasevich) v roce 1970.[1]

V některých případech je ale možné řešení diofantických rovnic zcela nebo alespoň zčásti převést na řešení kongruencí, což je kromě již zmiňovaných aplikací další motivací pro studium kongruencí. Uveďme si alespoň některé z nich.

**Lineární diofantické rovnice.** Lineární diofantické rovnice jsou rovnice tvaru



$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

kde $x_1, \ldots, x_n$ jsou neznámé a $a_1, \ldots, a_n, b$ daná nenulová celá čísla.

[1] Viz elementárně psaný text M. Davis, *Hilbert's Tenth Problem is Unsolvable*, The American Mathematical Monthly 80(3): 233–269. 1973.

Další aplikací zákona kvadratické reciprocity je v jistém smyslu opačná otázka: *Pro která prvočísla je dané číslo $a$ kvadratickým zbytkem?* Tuto otázku již umíme odpovědět např. pro $a = 2$. Prvním krokem je zodpovězení této otázky pro prvočísla, odpověď pro složená $a$ pak závisí na tom, jak se $a$ rozkládá na prvočísla.



**Věta.** *Nechť $q$ je liché prvočíslo.*

- *Je-li $q \equiv 1 \pmod 4$, pak je $q$ kvadratický zbytek modulo ta prvočísla $p$, která splňují $p \equiv r \pmod q$, kde $r$ je kvadratický zbytek modulo $q$.*
- *Je-li $q \equiv 3 \pmod 4$, pak je $q$ kvadratický zbytek modulo ta prvočísla $p$, která splňují $p \equiv \pm b^2 \pmod{4q}$, kde $b$ je liché a nesoudělné s $q$.*

Důkaz. První tvrzení plyne triviálně ze zákona kvadratické reciprocity. Uvažujme tedy $q \equiv 3 \pmod 4$, tj. $(q/p) = (-1)^{\frac{p-1}{2}}(p/q)$. Nechť nejprve $p \equiv +b^2 \pmod{4q}$, kde $b$ je liché, a tedy $b^2 \equiv 1 \pmod 4$. Pak $p \equiv b^2 \equiv 1 \pmod 4$ a $p \equiv b^2 \pmod q$. Tedy $(-1)^{\frac{p-1}{2}} = 1$ a $(p/q) = 1$, odkud $(q/p) = 1$. Je-li nyní $p \equiv -b^2 \pmod{4q}$, pak obdobně $p \equiv -b^2 \equiv 3 \pmod 4$ a $p \equiv -b^2 \pmod q$. Tedy $(-1)^{\frac{p-1}{2}} = -1$ a $(p/q) = -1$, odkud opět $(q/p) = 1$.

Obráceně, mějme $(q/p) = 1$. Máme dvě možnosti – buď $(-1)^{\frac{p-1}{2}} = 1$ a $(p/q) = 1$, anebo $(-1)^{\frac{p-1}{2}} = -1$ a $(p/q) = -1$. V prvním případě je $p \equiv 1 \pmod 4$ a existuje $b$ tak, že $p \equiv b^2 \pmod q$. Přitom lze bez újmy na obecnosti předpokládat, že $b$ liché (kdyby totiž bylo $b$ sudé, mohli bychom místo něj vzít $b + q$). Pak ale $b^2 \equiv 1 \equiv p \pmod 4$ a celkem $p \equiv b^2 \pmod{4q}$.

V druhém případě je $p \equiv 3 \pmod 4$ a $(-p/q) = (-1/q)(p/q) = (-1)(-1) = 1$, proto existuje $b$ (které lze opět vybrat liché) tak, že $-p \equiv b^2 \pmod q$. Tedy $-b^2 \equiv 3 \equiv p \pmod 4$ a celkem $p \equiv -b^2 \pmod{4q}$. □

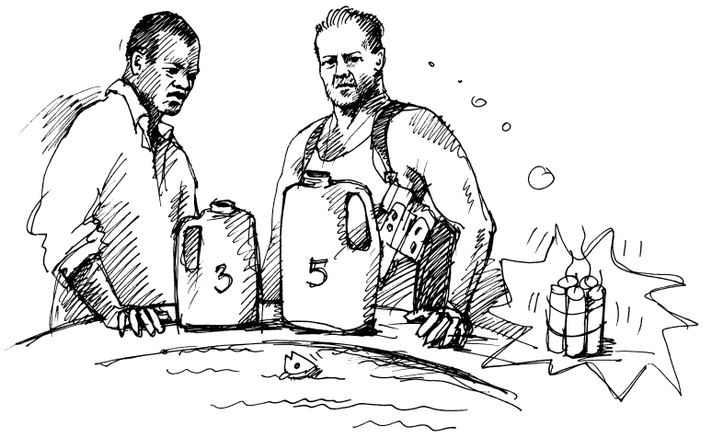
### 5. Aplikace – počítání s velkými čísly, kryptografie

**10.35. Výpočetní aspekty teorie čísel.** V mnoha praktických úlohách využívajících výsledky teorie čísel je zapotřebí umět rychle provést jeden či více z následujících výpočtů:



- běžné aritmetické operace (součet, součin, dělení se zbytkem) na celých číslech,
- určit zbytek mocniny celého čísla $a$ (na přirozené číslo $n$) po dělení daným $m$.
- určit inverzi celého čísla $a$ modulo $m \in \mathbb{N}$,
- určit největší společný dělitel dvou celých čísel (a případně koeficienty do Bezoutovy rovnosti),
- rozhodnout o daném čísle, je-li prvočíslo nebo složené,
- v případě složenosti rozložit dané číslo na součin prvočísel.

Základní aritmetické operace se i na velkých číslech obvykle provádějí obdobně jako jsme se to učili na základní a střední škole, kdy umíme sčítat v *lineárním* a násobit a dělit se zbytkem v *kvadratickém* čase. Pro násobení, které je základem mnoha dalších operací, existují asymptoticky rychlejší algoritmy (typu *rozděl a panuj*) - např. první takový Karatsubův (1960) časové náročnosti $\Theta\left(n^{\log_2 3}\right)$ nebo algoritmus Schönhage-Strassenův (1971) časové náročnosti $\Theta(n \log n \log\log n)$, který využívá rychlou Fourierovu




*To, že řešení diofantických rovnic je občas užitečné i „v praktickém životě“, dokazuje Bruce Willis a Samuel Jackson ve filmu Smrtonosná past 3 (Die Hard: With a Vengeance), kde mají za úkol zlikvidovat bombu pomocí 4 galonů vody, přičemž k dispozici mají pouze nádoby na 3, resp. 5 galonů. Matematik by řekl, že pánové měli za úkol nalézt alespoň jedno řešení diofantické rovnice* $3x + 5y = 4$.

K řešení těchto rovnic je možné užít kongruencí. Zřejmě je nutnou podmínkou řešitelnosti této rovnice to, že číslo $d = (a_1, \ldots, a_n)$ dělí $b$. Pokud je tato podmínka splněna, vydělením obou stran rovnice číslem $d$ dostaneme ekvivalentní rovnici

$$a'_1x_1 + a'_2x_2 + \cdots + a'_nx_n = b',$$

kde $a'_i = a_i/d$ pro $i = 1, \ldots, n$ a $b' = b/d$. Přitom platí

$$d \cdot (a'_1, \ldots, a'_n) = (da'_1, \ldots, da'_n) = (a_1, \ldots, a_n) = d,$$

a tedy $(a'_1, \ldots, a'_n) = 1$.

Dále ukážeme, že rovnice

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

kde $a_1, a_2, \ldots, a_n, b$ jsou celá čísla taková, že $(a_1, \ldots, a_n) = 1$, má vždy celočíselné řešení a že všechna celočíselná řešení této rovnice je možné popsat pomocí $n - 1$ celočíselných parametrů.

Důkaz povedeme matematickou indukcí vzhledem k počtu neznámých $n$. Pro $n = 1$ je tvrzení triviální, rovnice má zřejmě jediné řešení (tedy řešení nezávisí na žádném parametru). Je-li dále $n \geq 2$ a předpokládáme-li, že tvrzení platí pro rovnice o $n - 1$ neznámých, pak označíme $d = (a_1, \ldots, a_{n-1})$ a libovolná $n$-tice $x_1, \ldots, x_n$, která je hledaným řešením rovnice musí splnit kongruenci

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{d}.$$

transformaci (FFT) – viz též 7.30. Ten je ale přes svou asymptotickou převahu výhodný až pro násobení čísel majících alespoň desítky tisíc cifer (a používá se tak např. pro hledání největších známých prvočísel v projektu GIMPS).

**10.36. Největší společný dělitel a modulární inverze.** Jak už jsme ukazovali dříve, výpočet řešení kongruence $a \cdot x \equiv 1 \pmod{m}$ s neznámou $x$ lze snadno (díky Bezoutově větě) převést na výpočet největšího společného dělitele čísel $a$ a $m$ a na hledání koeficientů $k, l$ do Bezoutovy rovnosti $k \cdot a + l \cdot m = 1$ (nalezené $k$ je pak onou hledanou inverzí $a$ modulo $m$).

```
function extended_gcd(a,m)
    if m == 0
        return (1,0)
    else
        (q,r) := divide (a,m)
        (k,l) := extended_gcd(m,r)
        return (l,k - q*l)
```

Podrobná analýza[9] ukazuje, že problém výpočtu největšího společného dělitele je *kvadratické* časové složitosti.

**10.37. Modulární umocňování.** Algoritmus modulárního umocňování je založen na myšlence, že např. při počítání $2^{64} \pmod{1000}$ není třeba nejprve počítat $2^{64}$ a poté jej vydělit se zbytkem číslem 1000, ale lépe je postupně násobit „dvojky“ a kdykoliv je výsledek větší než 1000, provést redukci modulo 1000. Zejména ale není třeba provádět takové množství násobení (v tomto případě 63 naivních násobení je možné nahradit pouze šesti umocněními na druhou, neboť

$$2^{64} = (((((2^2)^2)^2)^2)^2)^2.$$

```
function modular_pow  (base, exp, mod)
    result := 1
    while exp > 0
      if (exp % 2 == 1):
        result := (result * base) % mod
      exp := exp >> 1
      base := (base * base) % mod
    return result
```

V průběhu algoritmu se pro každou binární číslici exponentu provede umocnění základu na druhou modulo $n$ (což je operace proveditelná v nejhůře kvadratickém čase) a pro každou „jedničku“ v binárním zápisu se navíc provede jedno násobení. Celkově jsme tedy schopni provést modulární umocňování nejhůře v *kubickém* čase. Je přitom vidět, že složitost významně závisí na zápisu exponentu ve dvojkové soustavě

**Příklad.** Vypočtěme $2^{560} \pmod{561}$.

Protože $560 = (1000110000)_2$, dostaneme uvedeným algoritmem

[9] Viz např. D. Knuth, *Art of Computer Programming, Volume 2: Seminumerical Algorithms*, Addison-Wesley 1997 nebo Wikipedia, *Euclidean algorithm*, http://en.wikipedia.org/wiki/Euclidean_algorithm (as of July 16, 2013, 11:32 GMT).

Vzhledem k tomu, že $d$ je společný dělitel čísel $a_1, \ldots, a_{n-1}$, je tato kongruence tvaru

$$a_n x_n \equiv b \pmod{d},$$

která má díky tomu, že $(d, a_n) = (a_1, \ldots, a_n) = 1$, jediné řešení

$$x_n \equiv c \pmod{d},$$

kde $c$ je vhodné celé číslo, neboli $x_n = c + d \cdot t$, kde $t \in \mathbb{Z}$ je libovolné. Dosazením do původní rovnice a úpravou obdržíme rovnici

$$a_1 x_1 + \cdots + a_{n-1} x_{n-1} = b - a_n c - a_n d t$$

o $n-1$ neznámých s jedním parametrem $t$. Přitom je číslo $(b - a_n c)/d$ celé, proto lze tuto rovnici vydělit číslem $d$. Dostaneme tak rovnici

$$a'_1 x_1 + \cdots + a'_{n-1} x_{n-1} = b',$$

kde $a'_i = a_i/d$ pro $i = 1, \ldots, n-1$ a $b' = ((b - a_n c)/d) - a_n t$, splňující

$$(a'_1, \ldots, a'_{n-1}) = (da'_1, \ldots, da'_{n-1}) \cdot \tfrac{1}{d} = (a_1, \ldots, a_{n-1}) \cdot \tfrac{1}{d} = 1,$$

která má podle indukčního předpokladu pro libovolné $t \in \mathbb{Z}$ řešení popsatelné pomocí $n-2$ celočíselných parametrů (jiných než $t$), což spolu s podmínkou $x_n = c + dt$ dává požadované tvrzení.

**10.72.** Rozhodněte, zda je možné na dvouramenných vahách, mají-



cích ramena stejné délky, odvážit 50g nějakého zboží, máme-li k dispozici pouze (libovolný počet) závaží tří hmotností (770g, 630g a 330g). Pokud ano, jak to udělat?

**Řešení.** Naším úkolem je vyřešit rovnici

$$770x + 630y + 330z = 50,$$

kde $x, y, z \in \mathbb{Z}$ (záporná hodnota ve výsledku přitom bude znamenat, že závaží klademe na druhou misku). Po vydělení obou stran rovnice číslem $(770, 630, 330) = 10$ dostaneme ekvivalentní rovnici

$$77x + 63y + 33z = 5.$$

Nyní tuto rovnici uvážíme modulo $(77, 63) = 7$ a získáme lineární kongruenci, kterou vyřešíme:

$$\begin{aligned} 33z &\equiv 5 \pmod{7}, \\ 5z &\equiv 5 \pmod{7}, \\ z &\equiv 1 \pmod{7}. \end{aligned}$$

Řešeními jsou tedy všechna celá čísla $z$ tvaru $z = 1 + 7t$, kde $t \in \mathbb{Z}$ je celočíselný parametr.

| exp | base | result | poslední cifra exp |
|---|---|---|---|
| 560 | 2 | 1 | 0 |
| 280 | 4 | 1 | 0 |
| 140 | 16 | 1 | 0 |
| 70 | 256 | 1 | 0 |
| 35 | 460 | 1 | 1 |
| 17 | 103 | 460 | 1 |
| 8 | 511 | 256 | 0 |
| 4 | 256 | 256 | 0 |
| 2 | 460 | 256 | 0 |
| 1 | 103 | 256 | 1 |
| 0 | 511 | 1 | 0 |

A tedy $2^{560} \equiv 1 \pmod{561}$.

**10.38. Testování prvočíselnosti a složenosti.** Přestože platí zá-



kladní věta aritmetiky, která nám garantuje, že každé přirozené číslo se dá jednoznačným způsobem rozložit na součin prvočísel, praktické nalezení tohoto rozkladu je obvykle velmi výpočetně náročná operace, obvykle prováděná v několika krocích:

(1) nalezení všech dělitelů nepřevyšujících určitou hranici (metodou pokusného dělení všemi prvočísly až do této hranice, typicky je touto hranicí cca $10^6$),
(2) otestování zbylého faktoru na složenost (tzv. test na složenost, testující některou nutnou podmínku prvočíselnosti),
   (a) pokud test složenosti dopadl s výsledkem, že zkoumané číslo je asi prvočíslo, pak testem na prvočíselnost ověřit, že je to opravdu prvočíslo,
   (b) pokud test složenosti dopadl s výsledkem, že zkoumané číslo je složené, pak nalézt netriviálního dělitele.

Takto je posloupnost kroků prováděna z toho důvodu, že jednotlivé algoritmy mají postupně (výrazně) rostoucí časovou složitost. V roce 2002 sice Agrawal, Kayal a Saxena publikovali algoritmus, který testuje prvočíselnost v polynomiálním čase, prakticky je ale zatím stále efektivnější používat výše uvedený postup.

**10.39. Testy na složenost - jak s jistotou poznat složená čísla?** Takzvané testy na složenost testují některou nutnou podmínku prvočíselnosti. Nejjednodušší takovou podmínkou je Malá Fermatova věta.

**Tvrzení** (Fermatův test)**.** *Existuje-li pro dané $N$ nějaké $a \not\equiv 0 \pmod{N}$ takové, že $a^{N-1} \not\equiv 1 \pmod{N}$, pak $N$ není prvočíslo.*

Bohužel nemusí být pro dané složené $N$ snadné najít takové $a$, že Fermatův test odhalí složenost $N$. Pro některá výjimečná $N$ dokonce jedinými takovými čísly $a$ jsou ta čísla, jež jsou soudělná s $N$. Jejich nalezení je tedy ekvivalentní s nalezením dělitele, a tedy i s rozkladem $N$ na prvočísla.

Skutečně existují taková nehezká (nebo extrémně hezká?) složená čísla $N$, která splňují, že pro libovolné $a$ nesoudělné s $N$ platí $a^{N-1} \equiv 1 \pmod{N}$. Taková čísla se nazývají *Carmichaelova*, nejmenší[10] z nich je $561 = 3 \cdot 11 \cdot 17$ a teprve v roce 1992 se podařilo dokázat[11], že jich je dokonce nekonečně mnoho.

[10] Za objevitele nejmenších sedmi Carmichaelových čísel se považuje český kněz a matematik Václav Šimerka (1819–1887), který se jimi zabýval podstatně dříve než americký matematik R. D. Carmichael (1879–1967), po němž nesou své jméno.

[11] W. R. Alford, A. Granville and C. Pomerance, *There are Infinitely Many Carmichael Numbers*, Annals of Mathematics, Vol. 139, No. 3 (1994), pp. 703-722.

Po dosazení do rovnice za $z$ a úpravě dostaneme

$$77x + 63y = 5 - 33(1 + 7t),$$
$$11x + 9y = -4 - 33t.$$

Tuto (parametrizovanou) rovnici uvážíme modulo 11:

$$9y \equiv -4 - 33t \pmod{11},$$
$$-2y \equiv -4 \pmod{11},$$
$$y \equiv 2 \pmod{11}.$$

Řešeními kongruence jsou tedy celá čísla $y = 2 + 11s$ pro libovolné $s \in \mathbb{Z}$. Nyní již zbývá jen dopočítat $x$:

$$11x = -4 - 33t - 9(2 + 11s),$$
$$11x = -22 - 33t - 9 \cdot 11s,$$
$$x = -2 - 3t - 9s.$$

Zjistili jsme, že řešení tvoří všechny trojice celých čísel $(x, y, z)$ z množiny

$$\{(-2 - 3t - 9s, 2 + 11s, 1 + 7t);\, s, t \in \mathbb{Z}\}.$$

Konkrétní řešení dostaneme dosazením hodnot za $t$, $s$. Například pro $t = s = 0$ je řešením trojice $(-2, 2, 1)$ nebo pro $t = -4$, $s = 1$ trojice $(1, 13, -27)$.

Poznamenejme, že neznámé lze samozřejmě eliminovat v jiném pořadí – v takovém případě výsledek může vypadat „syntakticky" jinak, ale bude samozřejmě popisovat stejnou množinu řešení (ta je dána konkrétní třídou rozkladu komutativní grupy $\mathbb{Z}^n$ podle vhodné podgrupy – v našem případě $(2, 2, 1) + (3, 0, 7)\mathbb{Z} + (-9, 11, 0)\mathbb{Z} \subseteq \mathbb{Z}^3$ – což je zřejmou analogií toho, že řešením takové rovnice nad tělesem je afinní podprostor příslušného vektorového prostoru). □

**10.73. Další typy diofantických rovnic řešitelných s využitím kongruencí.** Při řešení některých diofantických rovnic je možné jednu z neznámých explicitně vyjádřit jako funkci ostatních – v takovém případě budeme zkoumat, pro které celočíselné hodnoty neznámých je i hodnota této funkce celočíselná.

Například pro rovnici tvaru

$$mx_n = f(x_1, \ldots, x_{n-1}),$$

kde $m$ je přirozené číslo a $f(x_1, \ldots, x_{n-1}) \in \mathbb{Z}[x_1, \ldots, x_{n-1}]$ mnohočlen s celočíselnými koeficienty, je nutnou a dostatečnou podmínkou toho, že $n$-tice celých čísel $x_1, \ldots, x_n$ je jejím řešením, podmínka

$$f(x_1, \ldots, x_{n-1}) \equiv 0 \pmod{m}.$$

**Příklad.** Dokážeme, že 561 je Carmichaelovo, tj. že pro každé $a \in \mathbb{N}$, které je nesoudělné s $3 \cdot 11 \cdot 17$, platí $a^{560} \equiv 1 \pmod{561}$.

Z vlastností kongruencí víme, že stačí dokázat tuto kongruenci modulo 3, 11 i 17. To ale dostaneme přímo z Malé Fermatovy věty, protože takové $a$ splňuje $a^2 \equiv 1 \pmod 3$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$, přičemž 2, 10 i 16 dělí 560, proto $a^{560} \equiv 1$ modulo 3, 11 i 17 pro všechna $a$ nesoudělná s 561 (viz též Korseltovo kritérium uvedené níže).

**10.40. Tvrzení** (Korseltovo kritérium)**.** *Složené číslo $n$ je Carmichaelovým číslem, právě když*

- *je nedělitelné čtvercem (square-free),*
- *pro všechna prvočísla $p$ dělící $n$ platí $p - 1 \mid n - 1$.*

Důkaz. „⇐" Ukážeme, že pokud $n$ splňuje uvedené dvě podmínky a je složené, pak pro libovolné $a \in \mathbb{Z}$ nesoudělné s $n$ platí $a^{n-1} \equiv 1 \pmod n$. Rozložme tedy $n$ na součin různých lichých prvočísel ve tvaru $n = p_1 \cdots p_k$, kde navíc $p_i - 1 \mid n - 1$ pro všechna $i \in \{1, , \ldots, k\}$. Protože $(a, p_i) = 1$ dostáváme z Malé Fermatovy věty $a^{p_i - 1} \equiv 1 \pmod{p_i}$, odkud díky podmínce $p_i - 1 \mid n - 1$ rovněž $a^{n-1} \equiv 1 \pmod{p_i}$. Toto platí pro všechna $i$, proto $a^{n-1} \equiv 1 \pmod n$ a číslo $n$ je Carmichaelovo.

„⇒" Carmichaelovo číslo $n$ nemůže být sudé, protože pak pro $a = -1$ dostaneme $a^{n-1} \equiv -1 \pmod n$, což ale vzhledem k podmínce $a^{n-1} \equiv 1 \pmod n$ znamená, že $n$ musí být rovno dvěma (a tedy není složené). Mějme tedy rozklad $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, kde $p_i$ jsou různá lichá prvočísla a $\alpha_i \in \mathbb{N}$. Pro každé $i$ můžeme díky větě 10.20 zvolit primitivní kořen $g_i$ modulo $p_i^{\alpha_i}$ a z Čínské zbytkové věty pak dostaneme celé číslo $a$ splňující $a \equiv g_i \pmod{p_i^{\alpha_i}}$ pro všechna $i$, které je zřejmě nesoudělné s $n$. Z předpokladu víme, že $a^{n-1} \equiv 1 \pmod n$, tedy i modulo $p_i^{\alpha_i}$, a proto rovněž $g_i^{n-1} \equiv 1 \pmod{p_i^{\alpha_i}}$. Protože je $g_i$ primitivním kořenem modulo $p_i^{\alpha_i}$, musí být číslo $n - 1$ násobkem jeho řádu, tedy násobkem $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1)$. Přitom je ale $(p_i, n-1) = 1$ (vždyť $p_i | n$), nutně tedy $\alpha_i = 1$ a $p_i - 1 \mid n - 1$. □

Fermatův test lze mírně vylepšit na Eulerův test nebo ještě více s využitím Jacobiho symbolu, ale výše zmíněný problém se ani tak zcela neodstraní.

**Tvrzení** (Eulerův test)**.** *Existuje-li pro dané liché $N$ číslo $a \not\equiv 0 \pmod N$ takové, že $a^{\frac{N-1}{2}} \not\equiv \pm 1 \pmod N$, pak $N$ není prvočíslo.*

Důkaz. Plyne ihned z Fermatovy věty a z toho, že pro liché $N$ platí $a^{N-1} = (a^{\frac{N-1}{2}} - 1)(a^{\frac{N+1}{2}} - 1)$. □

**Tvrzení** (Euler-Jacobiho test)**.** *Existuje-li pro dané liché $N$ číslo $a \not\equiv 0 \pmod N$ takové, že $a^{\frac{N-1}{2}} \not\equiv \left(\frac{a}{N}\right) \pmod N$, pak $N$ není prvočíslo.*

Důkaz. Plyne ihned z lemmatu 10.33. □

**Příklad.** Mějme stejně jako dříve $N = 561 = 3 \cdot 11 \cdot 17$ a uvažme $a = 5$. Pak platí $5^{280} \equiv 1 \pmod 3$ a $5^{280} \equiv 1 \pmod{10}$, přitom $5^{280} \equiv -1 \pmod{17}$, proto určitě $5^{280} \not\equiv \pm 1 \pmod{561}$. Zde došlo k tomu, že neplatilo $a^{(N-1)/2} \equiv \pm 1 \pmod N$, proto ani nebylo třeba testovat hodnotu Jacobiho symbolu $(5/561)$. Často ale právě Euler-Jacobiho test může odhalit složené číslo i v případě, kdy tato mocnina je rovna $\pm 1$.

**10.74.** Řešte diofantickou rovnici $x(x+3) = 4y - 1$.

**Řešení.** Rovnici upravíme na tvar $4y = x^2 + 3x + 1$ a budeme řešit kongruenci

$$x^2 + 3x + 1 \equiv 0 \pmod 4.$$

Tato kongruence nemá žádné řešení, protože pro libovolné celé číslo $x$ je hodnota výrazu $x^2 + 3x + 1$ lichá (což lze zjistit rovněž prostým dosazením všech možných zbytků modulo 4 přímo do kongruence). □

**10.75.** Řešte v oboru celých čísel rovnici



$$379x + 314y + 183y^2 = 210.$$

**Řešení.** Rovnice je lineární vzhledem k neznámé $x$, druhá neznámá $y$ tedy musí vyhovět kongruenci

$$183y^2 + 314y - 210 \equiv 0 \pmod{379}.$$

Polynom na levé straně normujeme a doplníme na čtverec (abychom se zbavili lineárního členu). Nejprve je třeba určit $t \in \mathbb{Z}$ tak, aby $183 \cdot t \equiv 1 \pmod{379}$. (jinými slovy: potřebujeme určit inverzi čísla 183 modulo 379). K tomu využijeme Euklidova algoritmu:

$$379 = 2 \cdot 183 + 13,$$
$$183 = 14 \cdot 13 + 1,$$

odkud

$$1 = 183 - 14 \cdot 13 = 183 - 14 \cdot (379 - 2 \cdot 183) =$$
$$= 29 \cdot 183 - 14 \cdot 379.$$

Hledaným $t$ je tedy např. číslo 29. Po vynásobení obou stran kongruence číslem $t = 29$ a úpravě tak dostáváme ekvivalentní kongruenci

$$y^2 + 10y - 26 \equiv 0 \pmod{379}.$$

Nyní levou stranu doplníme na čtverec a upravíme pomocí substituce $(z = y + 5)$:

$$(y+5)^2 - 5^2 - 26 \equiv 0 \pmod{379},$$
$$z^2 \equiv 51 \pmod{379}.$$

S využitím zákona kvadratické reciprocity vypočteme Legendreův symbol (51/379):

$$\left(\frac{51}{379}\right) = \left(\frac{3}{379}\right) \cdot \left(\frac{17}{379}\right) = \left(\frac{379}{3}\right) \cdot (-1) \cdot \left(\frac{379}{17}\right) \cdot (+1) =$$
$$= \left(\frac{1}{3}\right) \cdot (-1) \cdot \left(\frac{5}{17}\right) = (1) \cdot (-1) \cdot \left(\frac{17}{5}\right) \cdot (+1) =$$
$$= (-1) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1,$$

**Příklad.** Eulerův test neodhalí například složenost čísla $N = 1729 = 7 \cdot 13 \cdot 19$, neboť číslo $\frac{N-1}{2} = 864 = 2^5 \cdot 3^3$ je dělitelné 6, 12 i 18 a tedy z Fermatovy věty plyne, že pro všechna celá čísla $a$ nesoudělná s $N$ platí $a^{(N-1)/2} \equiv 1 \pmod N$. Přitom ale pro $a = 11$ dostaneme $(11/1729) = -1$ a Euler-Jacobiho test již tedy složenost čísla 1729 odhalí.

Poznamenejme, že hodnotu Legendreova nebo Jacobiho symbolu $(a/n)$ lze díky zákonu kvadratické reciprocity spočítat velmi efektivně[12] v čase $O((\log a)(\log n))$.

### Pseudoprvočíslo

Složené číslo $n$ se nazývá *pseudoprvočíslo*, pokud projde příslušným testem na složenost a není jím odhaleno jako složené. Máme tak

(1) Fermatova pseudoprvočísla o základu $a$,
(2) Eulerova (nebo Euler-Jacobiho) pseudoprvočísla o základu $a$,
(3) silná pseudoprvočísla o základu $a$, což jsou složená čísla, která projdou následujícím testem na složenost:

Následující test je jednoduchým, ale (jak se ukazuje ve větě 10.42) velice účinným, zpřesněním úvodního Fermatova testu.

**10.41. Věta.** *Nechť $p$ je liché prvočíslo. Pišme $p - 1 = 2^t \cdot q$, kde $t$ je přirozené číslo a $q$ je liché. Pak pro každé celé číslo $a$ nedělitelné $p$ buď platí $a^q \equiv 1 \pmod p$ nebo existuje $e \in \{0, 1, \ldots, t-1\}$ splňující $a^{2^e q} \equiv -1 \pmod p$.*

Důkaz. Z Fermatovy věty plyne

$$p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) =$$
$$= (a^{\frac{p-1}{4}} - 1)(a^{\frac{p-1}{4}} + 1)(a^{\frac{p-1}{2}} + 1) =$$
$$\vdots$$
$$= (a^q - 1)(a^q + 1)(a^{2q} + 1) \cdots (a^{2^{t-1}q} + 1),$$

odkud díky prvočíselnosti $p$ zřejmě plyne tvrzení. □

**Tvrzení** (test na složenost Millera a Rabina). *Nechť je dáno liché číslo $N$ a přirozená čísla $t, q$ splňující $N - 1 = 2^t \cdot q$, $2 \nmid q$. Existuje-li číslo $a \not\equiv 0 \pmod N$ takové, že*

$$a^q \not\equiv 1 \pmod N$$
$$a^{2^e q} \not\equiv -1 \pmod N \quad \text{pro} \quad e \in \{0, 1, \ldots, t-1\},$$

*pak $N$ není prvočíslo.*

Důkaz. Korektnost testu plyne přímo z předchozí věty. □

[12] Viz H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993.

odkud plyne, že kongruence je řešitelná a má dvě řešení modulo 379.

Podle tvrzení v příkladu ‖10.70‖ jsou řešení tvaru

$$z \equiv \pm 51^{\frac{380}{4}},$$

přitom $51^3 \equiv 1 \pmod{379}$, odkud $51^{95} = (51^3)^{31} \cdot 51^2 \equiv -52 \pmod{379}$. Řešeními jsou tedy $z \equiv \pm 52 \pmod{379}$ a odtud zpětným dosazením dostaneme

$$y \equiv 47 \pmod{379}, \qquad y \equiv -57 \pmod{379}.$$

Zadaná diofantická rovnice má tedy jako řešení všechny dvojice $(x, y)$, kde $y \in \{47 + 379 \cdot k;\ k \in \mathbb{Z}\} \cup \{-57 + 379 \cdot k;\ k \in \mathbb{Z}\}$ a $x = \frac{1}{379} \cdot (210 - 314y - 183y^2)$, tedy např. dvojice čísel $(-1105, 47)$ nebo $(-1521, -57)$ (což jsou jediná dvě řešení s $|x| < 10^5$). □

**10.76.** Řešte v množině celých čísel rovnici $2^x = 1 + 3^y$.

**Řešení.** Je-li $y < 0$, platí $1 < 1 + 3^y < 2$, odkud $0 < x < 1$, což zjevně není celé číslo. Je tedy $y \geq 0$, a proto $2^x = 1 + 3^y \geq 2$, odkud $x \geq 1$. Ukážeme, že také platí $x \leq 2$. Kdyby totiž bylo $x \geq 3$, platilo by

$$1 + 3^y = 2^x \equiv 0 \pmod{8},$$

odkud plyne

$$3^y \equiv -1 \pmod{8}.$$

To ale není možné, protože řád čísla 3 modulo 8 je roven dvěma a mocniny trojky jsou tedy kongruentní pouze s čísly 3 a 1. Zbývá tedy prověřit pouze možnosti $x = 1$ a $x = 2$.

Pro $x = 1$ dostáváme

$$3^y = 2^1 - 1 = 1,$$

a tedy $y = 0$. Z $x = 2$ plyne

$$3^y = 2^2 - 1 = 3,$$

takže $y = 1$. Rovnice má tedy dvě řešení: $x = 1$, $y = 0$ a $x = 2$, $y = 1$. □

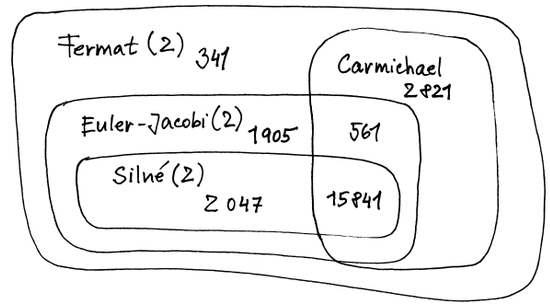
**10.77. Pythagorova rovnice.** V tomto odstavci se zabýváme otázkou hledání všech pravoúhlých trojúhelníků s celočíselnými délkami stran. Jde o diofantickou rovnici, při níž se metody uvedené výše objeví pouze okrajově, vzhledem k jejímu významu ji ale přesto uvedeme.



Úkolem je v množině přirozených čísel řešit rovnici

$$x^2 + y^2 = z^2.$$

**Řešení.** Zřejmě se můžeme omezit na situaci, kdy $(x, y, z) = 1$ (v opačném případě obě strany rovnice vydělíme číslem $d = (x, y, z)$.




*Různé typy pseudoprvočísel*

Ukazuje se, že tento snadný test výrazně zesiluje schopnost rozpoznávat složená čísla. Nejmenší silné pseudoprvočíslo o základu 2 je 2047 (přitom nejmenší Fermatovo o základu 2 bylo již 341) a při otestování základů 2, 3 a 5 dostaneme nejmenší silné pseudoprvočíslo 25326001. Jinými slovy, pokud nám stačí testovat pouze čísla do $2 \cdot 10^7$, pak stačí tento test na složenost provést pouze pro základy 2, 3 a 5. Pokud číslo není odhaleno jako složené, pak je určitě prvočíslem.Na druhou stranu bylo dokázáno, že žádná konečná báze není dostatečná pro otestování všech přirozených čísel.

Test Millera a Rabina je praktickou aplikací předchozího tvrzení, kdy jsme navíc díky následující větě uvedené bez důkazu schopni omezit pravděpodobnost neúspěchu.

**10.42. Věta.** *Nechť $N > 10$ je liché složené číslo. Pišme $N - 1 = 2^t \cdot q$, kde $t$ je přirozené číslo a $q$ je liché. Pak nejvýše čtvrtina z čísel množiny $\{a \in \mathbb{Z};\ 1 \leq a < N,\ (a, N) = 1\}$ splňuje následující podmínku:*

$$a^q \equiv 1 \pmod{N}$$

*nebo existuje $e \in \{0, 1, \ldots, t - 1\}$ splňující*

$$a^{2^e q} \equiv -1 \pmod{N}.$$

V praktických implementacích se obvykle testuje cca 20 náhodných základů (příp. nejmenších prvočíselných základů). V takovém případě dostáváme díky předchozí větě, že pravděpodobnost neodhalení složeného čísla je menší než $2^{-40}$.

Časová náročnost algoritmu je asymptoticky stejná jako složitost modulárního umocňování, tedy nejhůře *kubická*. Je ale třeba si uvědomit, že test je nedeterministický a spolehlivost jeho deterministické verze závisí na tzv. zobecněné Riemannově hypotéze (GRH[13]).

**10.43. Testy na prvočíselnost.** Testy na prvočíselnost přicházejí na řadu obvykle ve chvíli, kdy některý test na složenost prohlásí, že jde *pravděpodobně o prvočíslo*, případně se provádějí rovnou u speciálních typů čísel. Uveďme nejprve přehled nejznámějších testů, mezi nimiž jsou jak historické testy, tak i některé testy velmi moderní.



(1) AKS – obecný polynomiální test na prvočísla objevený indickými matematiky Agrawalem, Kayalem a Saxenou v roce 2002.

(2) Pocklington-Lehmerův test – test na prvočíselnost subexponenciální složitosti

[13] Wikipedia, *Riemann hypothesis*, `http://en.wikipedia.org/wiki/Riemann_hypothesis` (as of July 25, 2013, 21:23 GMT).

Ukážeme navíc, že čísla $x$, $y$, $z$ jsou dokonce po dvou nesoudělná: kdyby nějaké prvočíslo $p$ dělilo dvě z nich, nutně by dělilo i třetí, což vzhledem k podmínce nesoudělnosti není možné. Z čísel $x$, $y$ je tedy nejvýše jedno sudé. Kdyby byla obě lichá, nutně by platilo

$$z^2 \equiv x^2 + y^2 \equiv 1 + 1 \pmod 8,$$

což není možné (viz příklad ‖10.2‖). Z čísel $x$, $y$ je tedy právě jedno sudé. Protože ale v Pythagorově rovnici vystupují $x$ a $y$ symetricky, můžeme předpokládat, že sudé je $x$ a položit $x = 2r$, $r \in \mathbb{N}$. Odtud pak plyne

$$4r^2 = z^2 - y^2$$

a tedy

$$r^2 = \frac{z+y}{2} \cdot \frac{z-y}{2}.$$

Označme nyní $u = \frac{1}{2}(z+y)$, $v = \frac{1}{2}(z-y)$, s inverzní substitucí $z = u + v$, $y = u - v$. Protože $y$ a $z$ jsou nesoudělná, jsou nesoudělná i $u$, $v$ (případné prvočíslo $p$ dělící $y$ a $z$ by totiž bylo rovněž společným dělitelem jejich součtu i rozdílu, tedy $y$ a $z$). Ze vztahu

$$r^2 = u \cdot v$$

pak plyne, že existují nesoudělná přirozená čísla $a$, $b$ tak, že $u = a^2$, $v = b^2$. Navíc vzhledem k tomu, že platí $u > v$, nutně $a > b$. Celkem tedy dostáváme

$$\begin{aligned} x &= 2dr = 2ab, \\ y &= u - v = (a^2 - b^2), \\ z &= u + v = (a^2 + b^2), \end{aligned}$$

což skutečně vyhovuje dané rovnici pro libovolná nesoudělná $a, b \in \mathbb{N}$ taková, že $a > b$. Další řešení dostaneme záměnou $x$ a $y$. Další trojice řešení obdržíme, pokud vynásobíme všechny složky řešení libovolným přirozeným číslem $d$. □

**10.78. Velká Fermatova věta pro n = 4.** Z právě odvozené parametrizace pythagorejských čísel budeme schopni poměrně snadno dokázat neexistenci řešení (v oboru přirozených čísel) slavné Fermatovy rovnice



$$x^n + y^n = z^n$$

pro $n = 4$.

Dokažte, že rovnice $x^4 + y^4 = z^2$ nemá řešení v $\mathbb{N}$.

**Řešení.** Budeme postupovat tzv. metodou nekonečného sestupu (infinite descent), se kterou poprvé přišel Pierre de Fermat a která využívá toho, že libovolná neprázdná množina přirozených čísel má nejmenší prvek (jinými slovy, že $\mathbb{N}$ je dobře uspořádaná množina).

(3) Lucas-Lehmerův test – test prvočíselnosti pro Mersenneho čísla
(4) Pépinův test – test prvočíselnosti pro Fermatova čísla z roku 1877
(5) ECPP - test prvočíselnosti založený na tzv. eliptických křivkách

Uveďme nyní klasický test prvočíselnosti pro Mersenneho čísla.

**Tvrzení** (Lucas-Lehmerův test)**.** *Buď $q \neq 2$ prvočíslo a definujme posloupnost $(s_n)_{n=0}^{\infty}$ rekurzivně předpisem*

$$s_0 = 4,\ s_{n+1} = s_n^2 - 2.$$

*Pak je číslo $M_q = 2^q - 1$ prvočíslo, právě když $M_q$ dělí $s_{q-2}$.*

Důkaz. Budeme pracovat v okruhu $R = \mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}; a, b \in \mathbb{Z}\}$, kde dělení se zbytkem funguje analogicky jako v celých číslech (viz též 11.18). Položme $\alpha = 2 + \sqrt{3}$, $\beta = 2 - \sqrt{3}$ a zmiňme, že $\alpha + \beta = 4$, $\alpha \cdot \beta = 1$.

Nejprve indukcí dokážeme, že pro všechna $n \in \mathbb{N}_0$ platí

$$s_n = \alpha^{2^n} + \beta^{2^n} = \beta^{2^n}\left(1 + \alpha^{2^{n+1}}\right). \tag{10.2}$$

Pro $n = 0$ tvrzení platí, neboť $s_0 = 4 = \alpha + \beta$. Předpokládejme, že tvrzení platí pro $n - 1$, pak je $s_n = s_{n-1}^2 - 2$ podle indukčního předpokladu rovno $\left(\alpha^{2^{n-1}} + \beta^{2^{n-1}}\right)^2 - 2 = \alpha^{2^n} + \beta^{2^n}$.

Dále protože $M_q \equiv -1 \pmod 8$, je $(2/M_q) = 1$ a kromě toho ze zákona kvadratické reciprocity plyne

$$\left(\frac{3}{M_q}\right) = -\left(\frac{M_q}{3}\right) = -\left(\frac{2^q - 1}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

neboť pro liché $q$ je $2^q - 1 \equiv 1 \pmod 3$. Obě vyjádření platí i pokud $M_q$ není prvočíslo (v takovém případě jde o Jacobiho symbol).

Poznamenejme, že ve zbytku důkazu využijeme rozšíření relace kongruence na prvky z oboru $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3};\ a, b \in \mathbb{Z}\}$; stejně jako v případě celých čísel i pro $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$ píšeme $\alpha \equiv \beta \pmod p$, pokud $p \mid \alpha - \beta$. Dále i zde platí analogie tvrzení (ii) z příkladu ‖10.14‖ – pro prvočíslo $p$ je $(\alpha + \beta)^p \equiv \alpha^p + \beta^p \pmod p$ (důkaz je identický s důkazem tvrzení pro celá čísla).

„⇒“ Předpokládáme, že $M_q$ je prvočíslo a dokážeme, že $\alpha^{2^{q-1}} \equiv -1 \pmod{M_q}$, z čehož vzhledem k (10.2) vyplyne $M_q \mid s_{q-2}$. Protože $2^{(M_q-1)/2} \equiv (2/M_q) = 1 \pmod{M_q}$, existuje $y \in \mathbb{Z}$ tak, že $2y^2 \equiv 1 \pmod{M_q}$. Platí

$$(y(1 + \sqrt{3}))^2 = y^2(4 + 2\sqrt{3}) \equiv \alpha \pmod{M_q},$$

odkud s využitím Fermatovy věty a vztahu $2^{q-1} = \frac{M_q+1}{2}$ dostáváme

$$\begin{aligned} \alpha^{2^{q-1}} &\equiv \left(y\left(1 + \sqrt{3}\right)\right)^{M_q+1} \equiv \\ &\equiv y^2 \cdot y^{M_q-1}\left(1 + \sqrt{3}\right) \cdot \left(1 + \sqrt{3}\right)^{M_q} \equiv \\ &\equiv y^2\left(1 + \sqrt{3}\right) \cdot \left(1 - \sqrt{3}\right) = -2y^2 \equiv \\ &\equiv -1 \pmod{M_q}. \end{aligned}$$

Předpokládejme tedy, že množina řešení rovnice $x^4 + y^4 = z^2$ je neprázdná a uvažme takové řešení, které má mezi všemi řešeními nejmenší hodnotu $z$. Tato $x, y, z$ jsou nutně po dvou nesoudělná. Protože lze tuto rovnici psát ve tvaru

$$(x^2)^2 + (y^2)^2 = z^2,$$

z předchozího příkladu dostáváme existenci $r, s \in \mathbb{N}$, splňujících

$$x^2 = 2rs, \quad y^2 = r^2 - s^2, \quad z = r^2 + s^2.$$

Odtud $y^2 + s^2 = r^2$, kde $(y, s) = 1$ (kdyby nějaké prvočíslo $p$ dělilo $y$ i $s$, pak by díky předchozím vztahům dělilo i $x$ a $z$, což nelze kvůli předpokladu nesoudělnosti $x, y, z$). Opětovným využitím řešení pythagorejské rovnice dostáváme existenci přirozených čísel $a, b$ s vlastnostmi ($y$ je liché)

$$y = a^2 - b^2, \quad s = 2ab, \quad r = a^2 + b^2.$$

Zpětnou substitucí dostaneme

$$x^2 = 2rs = 2 \cdot 2ab(a^2 + b^2),$$

a protože $x$ je sudé, plyne odtud

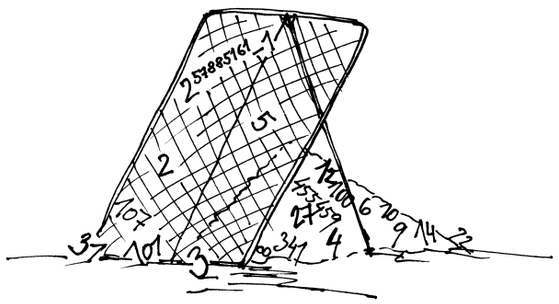
$$\left(\frac{x}{2}\right)^2 = ab(a^2 + b^2).$$

Čísla $a, b, a^2 + b^2$ jsou přitom po dvou nesoudělná (což se odvodí snadno z nesoudělnosti $y$ a $s$), proto je každé z nich druhou mocninou přirozeného čísla:

$$a = c^2, \quad b = d^2, \quad a^2 + b^2 = e^2,$$

odkud $c^4 + d^4 = e^2$ a protože platí $e \leq a^2 + b^2 = r < z$, dostáváme spor s minimalitou $z$. □

### E. Testy prvočíselnosti



**10.79. Mersenneho prvočísla.** Následujících několik úloh má úzký vztah k testování Mersenneho čísel na prvočíselnost.



Pro libovolné $q \in \mathbb{N}$ uvažte číslo $M_q = 2^q - 1$ a dokažte:

i) Je-li $q$ složené, je složené i $M_q$.

Při odvození jsme dále využili toho, že 3 je kvadratický nezbytek modulo $M_q$, a tedy že platí

$$\left(1 + \sqrt{3}\right)^{M_q} \equiv 1 + \left(\sqrt{3}\right)^{M_q} = 1 + 3^{(M_q-1)/2} \cdot \sqrt{3} \equiv$$
$$\equiv 1 - \sqrt{3} \pmod{M_q}.$$

„⇐“ Nechť nyní naopak $M_q \mid s_{q-2}$. Pak ale

$$M_q \mid s_{q-2} \cdot \alpha^{2^{q-2}} = 1 + \alpha^{2^{q-1}}.$$

Je-li $p \neq 2, 3$ libovolný prvočíselný dělitel $M_q$, pak rovněž $\alpha^{2^{q-1}} \equiv -1 \pmod{p}$ a $\alpha^{2^q} \equiv 1 \pmod{p}$. Odtud vyplývá, že $2^q$ je řád $\alpha$ v multiplikativní grupě $T_p = \{a+b\sqrt{3};\ 0 \leq a, b < p\} \setminus \{0\}$.

Kdyby platilo $(3/p) = 1$, pak bychom obdrželi

$$\alpha^{p-1} = \beta \cdot \alpha^p \equiv \beta \cdot \left(2^p + \left(\sqrt{3}\right)^p\right) \equiv$$
$$\equiv \beta \cdot \left(2 + \sqrt{3} \cdot 3^{(p-1)/2}\right) \equiv \beta \cdot \left(2 + \sqrt{3}\right) = 1,$$

odkud plyne, že $p-1$ je násobkem řádu $\alpha$, tedy $2^q$. To ale znamená, že $p > p - 1 \geq 2^q > 2^q - 1 = M_q$ a to je spor s tím, že $p$ je dělitel $M_q$. Proto je $(3/p) = -1$ a

$$\alpha^{p+1} \equiv \left(2 + \sqrt{3}\right)\left(2 + \sqrt{3}\right)^p \equiv$$
$$\equiv \left(2 + \sqrt{3}\right)\left(2 - \sqrt{3}\right) \equiv$$
$$\equiv 1 \pmod{p}.$$

Řádem $\alpha$ modulo $p$ je $2^q$, proto $2^q \mid p+1$ a zejména $p \geq 2^q - 1 = M_q$. Zároveň je ale $p$ prvočíselný dělitel $M_q$, proto je $M_q = p$ prvočíslo. □

Na rozdíl od důkazu je naprogramování tohoto algoritmu velmi jednoduchou záležitostí.



**Algoritmus (Lucas-Lehmerův test prvočíselnosti):**

```
function LL_is_prime(q)
    s := 4; M = 2^q − 1
    repeat q − 2 times
      s := s^2 − 2 (mod M)
    if s = 0, return PRIME.
    else return COMPOSITE.
```

Časová složitost testu je asymptoticky stejná jako v případě Miller-Rabinova testu, v konkrétních případech je ale efektivnější.

*Fermatova čísla* jsou čísla tvaru $F_n = 2^{2^n} + 1$. Pierre de Fermat v 17. století vyslovil hypotézu, že všechna čísla tohoto tvaru jsou prvočísla (zřejmě veden snahou zobecnit pozorování pro $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ a $F_4 = 65537$). V 18. století ale Leonhard Euler zjistil, že $F_5 = 641 \times 6700417$ a dodnes se nepodařilo nalézt žádné další Fermatovo prvočíslo. Vzhledem k rychle rostoucí velikosti těchto čísel je počítání s nimi velmi časově náročné (a ani následující test tak není příliš používán). V současné době nejmenší netestované Fermatovo číslo je $F_{33}$, které má 2 585 827 973 číslic a je tak výrazně větší než největší dosud nalezené prvočíslo.



ii) Je-li $q$ prvočíslo, $q \equiv 3 \pmod 4$, pak $2q+1$ dělí $M_q$, právě když $2q+1$ je prvočíslo (odtud plyne, že je-li $q \equiv 3 \pmod 4$ prvočíslo Sophie Germainové[2], pak $M_q$ není prvočíslo).

iii) Pokud prvočíslo $p$ dělí $M_q$, pak $p \equiv \pm 1 \pmod 8$ a $p \equiv 1 \pmod q$.

**Řešení.**

i) Platí-li $n \mid q$, pak podle příkladu ‖10.6‖ platí $2^n - 1 \mid 2^q - 1$, tedy $M_n \mid M_q$ a pro $n > 1$ tak $M_q$ není prvočíslem.

ii) Nechť $n = 2q + 1$ je dělitel $M_q$. S využitím Lucasovy věty 10.44 ukážeme, že $n$ je prvočíslo. Protože $n - 1 = 2q$ má pouze dva prvočíselné dělitele, stačí najít svědky složenosti pro čísla 2 a $q$. Platí $2^{\frac{n-1}{q}} = 2^2 \not\equiv 1 \pmod n$, $(-2)^{\frac{n-1}{2}} = -2^q \equiv -1 \not\equiv 1 \pmod n$, díky předpokladu $n \mid M_q = 2^q - 1$. Protože dále $(-2)^{n-1} = 2^{n-1} = 2^{2q} - 1 = (2^q + 1)M_q \equiv 0 \pmod n$, dostáváme z Lucasovy věty, že $n$ je prvočíslo.

Nechť je nyní $p = 2q + 1 \equiv -1 \pmod 8$ prvočíslo. Protože $(2/p) = 1$, existuje $m$ tak, že $2 \equiv m^2 \pmod p$. Odtud $2^q \equiv 2^{\frac{p-1}{2}} \equiv m^{p-1} \equiv 1 \pmod p$, a tedy $p \mid 2^q - 1 = M_q$.

iii) Pokud $p \mid M_q = 2^q - 1$, pak řád 2 modulo $p$ musí dělit prvočíslo $q$, a proto je roven $q$. Odtud $q \mid p - 1$ a existuje $k \in \mathbb{Z}$ tak, že $2qk = p - 1$. Celkem dostáváme

$$(2/p) \equiv 2^{\frac{p-1}{2}} \equiv 2^{qk} \equiv 1 \pmod p,$$

tj. $p \equiv \pm 1 \pmod 8$. □

**10.80.** Rozhodněte, zda jsou Mersenneho čísla $2^{11} - 1$, $2^{15} - 1$, $2^{23} - 1$, $2^{29} - 1$ a $2^{83} - 1$ prvočísla nebo čísla složená.



**Řešení.** V případě čísla $2^{15} - 1$ je exponent složený, proto je toto číslo rovněž složené (víme dokonce, že je dělitelné čísly $2^3 - 1$ a $2^5 - 1$), ve všech ostatních případech je exponentem prvočíslo. Můžeme si všimnout, že tato prvočísla $q = 11, 23, 29$ a 83 jsou dokonce prvočísly Sophie Germainové (tedy $2q + 1$ je rovněž prvočíslo), proto z části (ii) předchozího příkladu plyne, že $23 \mid 2^{11} - 1$, $47 \mid 2^{23} - 1$ a $167 \mid 2^{83} - 1$.

Ve zbylém případě nemůžeme toto tvrzení použít, protože $29 \not\equiv 3 \pmod 4$ a skutečně $59 \nmid 2^{29} - 1$. Zde ale z části (iii) předchozího příkladu dostáváme, že případné prvočíslo $p$ dělící $2^{89} - 1$ musí

[2]Viz Wikipedia, *Sophie Germain prime*, http://en.wikipedia.org/wiki/Sophie_Germain_prime (as of July 28, 2013, 14:43 GMT).

**Tvrzení** (Pépinův test)**.** *Nutnou a postačující podmínkou toho, aby $n$-té Fermatovo číslo $F_n$ bylo prvočíslem, je*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Vidíme, že jde o velmi jednoduchý test, který je vlastně pouze malou částí Eulerova testu na složenost.

Důkaz korektnosti Pépinova testu. Předpokládejme nejprve, že $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Pak $3^{F_n-1} \equiv 1 \pmod{F_n}$, a protože je $F_n - 1$ mocninou dvojky, je nutně $F_n - 1$ řádem čísla 3 modulo $F_n$. Řád každého čísla modulo $F_n$ je ale nejvýše roven $\varphi(F_n) \le F_n - 1$, proto je v tomto případě $\varphi(F_n) = F_n - 1$, což znamená, že $F_n$ je prvočíslo.

Obráceně, nechť je $F_n$ prvočíslo. Z části (i) lemmatu 10.33 dostáváme, že $3^{(F_n-1)/2} \equiv (3/F_n) \pmod{F_n}$, stačí nám tedy určit hodnotu $(3/F_n)$. To je ale snadné, protože $F_n \equiv 2 \pmod 3$ a tedy $(F_n/3) = -1$. Dále $F_n \equiv 1 \pmod 4$, proto díky zákonu kvadratické reciprocity dostáváme $(3/F_n) = -1$, což jsme měli dokázat. □



Nyní si uvedeme sice starší, ale i v moderních výpočetních systémech hojně využívaný obecně použitelný *Pocklington-Lehmerův* test na prvočíselnost. Nejprve si ale kvůli názornosti uveďme jednodušší *Lucasův test* prvočíselnosti:

**10.44. Věta** (Lucasova)**.** *Pokud pro libovolný prvočíselný dělitel $q$ čísla $N - 1$ existuje $a$ tak, že $a^{N-1} \equiv 1 \pmod N$, $a^{\frac{N-1}{q}} \not\equiv 1 \pmod N$, pak je $N$ prvočíslo.*

Důkaz. Stačí dokázat, že $N - 1$ dělí $\varphi(N)$ (což je podmínka, které složená čísla zjevně nevyhovují). Pokud ne, tak existuje prvočíslo $q$ a $r \in \mathbb{N}$ tak, že $q^r$ dělí $N - 1$, ale nedělí $\varphi(N)$. Řád $e$ čísla $a$ dělí $N - 1$ (první podmínka) a nedělí $(N - 1)/q$ (druhá podmínka), proto $q^r$ dělí $e$. Navíc $e$ dělí $\varphi(N)$, tedy i $q^r$ dělí $\varphi(N)$, spor. □

Číslo $a$ z předchozí věty se nazývá *svědek prvočíselnosti* čísla $N$ (podobně i v dalších testech na prvočíselnost).

Z tohoto testu vychází obecný test na prvočíselnost, který použijeme, pokud chceme vysokou pravděpodobnost odpovědi Miller-Rabinova testu na složenost proměnit v jistotu.

**10.45. Věta** (Pocklingtona a Lehmera)**.** *Nechť $N$ je přirozené číslo, $N > 1$. Nechť $p$ je prvočíslo dělící $N - 1$. Předpokládejme dále, že existuje $a_p \in \mathbb{Z}$ tak, že*

$$a_p^{N-1} \equiv 1 \pmod N \quad a \quad \left(a_p^{\frac{N-1}{p}} - 1, N\right) = 1.$$

*Nechť $p^{\alpha_p}$ je nejvyšší mocnina $p$ dělící $N-1$. Pak pro každý kladný dělitel $d$ čísla $N$ platí*

$$d \equiv 1 \pmod{p^{\alpha_p}}.$$

Důkaz věty Pocklingtona a Lehmera. Každý kladný dělitel $d$ čísla $N$ je součinem prvočíselných dělitelů čísla $N$, větu proto stačí dokázat pouze pro prvočíselné hodnoty $d$. Z podmínky $a_p^{N-1} \equiv 1 \pmod N$ plyne nesoudělnost čísel $a_p, N$ (jejich společný dělitel musí dělit i pravou stranu kongruence). Pak rovněž $(a_p, d) = 1$ a podle Fermatovy věty platí $a_p^{d-1} \equiv 1 \pmod d$. Protože $\left(a_p^{(N-1)/p} - 1, N\right) = 1$, platí $a_p^{(N-1)/p} \not\equiv 1 \pmod d$.

splňovat

$$p \equiv \pm 1 \pmod 8$$
$$p \equiv \quad 1 \pmod{29},$$

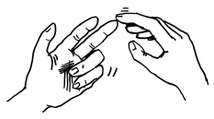
neboli $p \equiv 1 \pmod{232}$ nebo $p \equiv 175 \pmod{232}$. Hledáme-li prvočíselného dělitele čísla $n = 2^{29} - 1 = 536\,870\,911$, pak stačí prověřit prvočísla tohoto tvaru do $\sqrt{n} \approx 23\,170$. Těch je celkem 50, proto otestování toho, zda je $n$ prvočíslo, je jednoduše zvládnutelné (s trochou píle dokonce i na papíře). V tomto případě je navíc hledaným dělitelem hned nejmenší z těchto prvočísel, číslo 233. □

**10.81.** Ukažte, že číslo 341 je Fermatovo pseudoprvočíslo o základu 2, ale že není Euler-Jacobiho pseudoprvočíslo o základu 2. Dále dokažte, že číslo 561 je Euler-Jacobiho pseudoprvočíslo o základu 2, ale ne o základu 3 a že naopak číslo 121 je Euler-Jacobiho pseudoprvočíslo o základu 3, ale nikoliv o základu 2.



**Řešení.** Číslo 341 je Fermatovo pseudoprvočíslo o základu 2, protože $2^{10} \equiv 1 \Rightarrow 2^{340} \equiv 1 \pmod{341}$. Není Euler-Jacobiho, protože sice $2^{170} \equiv 1 \pmod{341}$, ale $\left(\frac{2}{341}\right) = -1$, což plyne z toho, že $341 \equiv -3 \pmod 8$. Pro číslo 561 platí $2^{280} \equiv 1 \pmod{561}$ a $\left(\frac{2}{561}\right) = 1$, protože $561 \equiv 1 \pmod 8$. Je tedy Euler-Jacobiho pseudoprvočíslo o základu 2. O základu 3 nikoli, protože $3 \mid 561$. Naopak, číslo 121 splňuje $3^5 \equiv 1 \pmod{121} \Rightarrow 3^{60} \equiv 1 \pmod{121}$ a $\left(\frac{3}{121}\right) = 1$, ale $2^{60} \equiv 89 \not\equiv 1 \pmod{121}$. □

**10.82.** Dokažte, že čísla 2465, 2821 a 6601 jsou Carmichaelova, tj. že označíme-li $n$ kterékoliv z nich, pak pro každé $a \in \mathbb{Z}$, $(a, n) = 1$ platí



$$a^{n-1} \equiv 1 \pmod n.$$

**Řešení.** Platí $2465 = 5 \cdot 17 \cdot 29$, $2821 = 7 \cdot 13 \cdot 31$, $6601 = 7 \cdot 23 \cdot 41$ a tvrzení plyne z Korseltova kritéria 10.40, neboť čísla 4, 16 i 28 dělí $2464 = 2^5 \cdot 7 \cdot 11$, čísla 6, 12 i 30 dělí $2820 = 2^2 \cdot 3 \cdot 5 \cdot 47$ a čísla 6, 22, 40 dělí $6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$. □

**10.83.** Dokažte, že 2047 je silné pseudoprvočíslo o základu 2, ale ne o základu 3. Dále dokažte, že 1905 je Euler-Jacobiho pseudoprvočíslo o základu 2, které ale není silným pseudoprvočíslem o stejném základu.



**Řešení.** To, zda 2047 je silné pseudoprvočíslo o základu 2, ověříme pomocí rozkladu

$$(2^{2046} - 1) = (2^{1023} - 1)(2^{1023} + 1).$$

Označme $e$ řád $a_p$ modulo $d$. Pak platí $e \mid d - 1$, $e \mid N - 1$ a $e \nmid (N-1)/p$.

Kdyby $p^{\alpha_p} \nmid e$, pak by z $e \mid N - 1$ plynulo $e \mid \frac{N-1}{p}$, což je spor. Platí tedy $p^{\alpha_p} \mid e$, a tedy rovněž $p^{\alpha_p} \mid d - 1$. □

**10.46. Věta.** *Nechť $N \in \mathbb{N}$, $N > 1$. Předpokládejme, že můžeme psát $N - 1 = F \cdot U$, kde $(F, U) = 1$ a $F > \sqrt{N}$, přičemž známe rozklad čísla $F$ na prvočinitele. Pak platí:*

- *jestliže pro každé prvočíslo $p \mid F$ můžeme najít $a_p \in \mathbb{Z}$ z předchozí věty, pak je $N$ prvočíslo;*
- *je-li $N$ prvočíslo, pak pro libovolné prvočíslo $p \mid N - 1$ existuje $a_p \in \mathbb{Z}$ s požadovanými vlastnostmi.*

Důkaz. Podle věty 10.45 pro potenciálního dělitele $d > 1$ čísla $N$ platí $d \equiv 1 \pmod{p^{\alpha_p}}$ pro všechny prvočíselné faktory $F$, proto je $d \equiv 1 \pmod F$, a tedy $d > \sqrt{N}$. Pokud $N$ nemá netriviálního dělitele nepřevyšujícího $\sqrt{N}$, je nutně prvočíslem. Obráceně stačí za $a_p$ zvolit primitivní kořen modulo prvočíslo $N$ (nezávisle na $p$). Pak z Fermatovy věty plyne $a_p^{N-1} \equiv 1 \pmod N$ a z toho, že $a_p$ je primitivní kořen, dostáváme $a_p^{(N-1)/p} \not\equiv 1 \pmod N$ pro libovolné $p \mid N - 1$.

Čísla $a_p$ opět nazýváme svědky prvočíselnosti čísla $N$. □

**Poznámka.** Předchozí test v sobě zahrnuje Pépinův test (zde totiž pro $N = F_n$ máme $p = 2$, kterému vyhovuje svědek prvočíselnosti $a_p = 3$).

**10.47. Hledání dělitele.** Máme-li testem na složenost provedeným na nějakém konkrétním čísle potvrzeno, že jde o číslo složené, obvykle chceme najít netriviálního dělitele. Jde ale o výrazně obtížnější úkol než pouhé odhalení jeho složitosti – připomeňme, že testy na složenost nám sice poskytnou garanci, ale nikoliv dělitele (což je na druhou stranu výhodné pro RSA a podobné kryptografické protokoly), proto si k tématu uvedeme jen stručný přehled používaných metod a krátkou ukázku pro inspiraci.



(1) Pokusné dělení
(2) Pollardova $\rho$-metoda
(3) Pollardova $p - 1$ metoda
(4) Faktorizace pomocí eliptických křivek (ECM)
(5) Metoda kvadratického síta (QS)
(6) Metoda síta v číselném tělesa (NFS)

Zde si pro ilustraci ukážeme konkrétní případ použití jednoho z těchto algoritmů – Pollardovy $\rho$-metody. Tento algoritmus je speciálně vhodný pro hledání *relativně* malých dělitelů (jeho očekávaná složitost totiž závisí na velikosti těchto dělitelů) a je založený na myšlence, že pro náhodnou funkci $f : S \to S$, kde $S$ je konečná $n$-prvková množina, se musí posloupnost $(x_n)_{n=0}^{\infty}$, kde $x_{n+1} = f(x_n)$, zacyklit. Přitom předperioda i perioda má očekávanou délku $\sqrt{\pi \cdot n/8}$.

Protože je $2^{1023} \equiv 1 \pmod{2047}$, je tvrzení pravdivé. Přitom ale není silným prvočíslem o základu 3, protože

$$3^{1023} \equiv 1565 \not\equiv \pm 1 \pmod{2047}.$$

Všimněme si, že v případě čísla 2047 je test na silné pseudoprvočíslo shodný s Eulerovým testem (je to dáno tím, že číslo 2046 není dělitelné čtyřmi).

Číslo 1905 je Euler-Jacobiho pseudoprvočíslo o základu 2, protože $2^{1904/2} \equiv 1 \pmod{1905}$ a rovněž Jacobiho symbol $(2/1905)$ je roven 1. Protože $1904 = 2^4 \cdot 7 \cdot 17$, je k tomu, aby bylo 1905 silné pseudoprvočíslo o základu 2, třeba, aby byla splněna některá z kongruencí

$$2^{952} \equiv -1 \pmod{1905},$$
$$2^{476} \equiv -1 \pmod{1905},$$
$$2^{238} \equiv -1 \pmod{1905},$$
$$2^{119} \equiv \pm 1 \pmod{1905}.$$

Platí ale $2^{952} \equiv 2^{476} \equiv 1 \pmod{1905}$, $2^{238} \equiv 1144 \pmod{1905}$ a $2^{119} \equiv 128 \pmod{1905}$, proto číslo 1905 silným pseudoprvočíslem o základu 2 není. □

**10.84.** Pomocí Pocklington-Lehmerova testu ukažte, že 1321 je prvočíslo.



**Řešení.** Položme $N = 1321$, pak $N - 1 = 1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$.

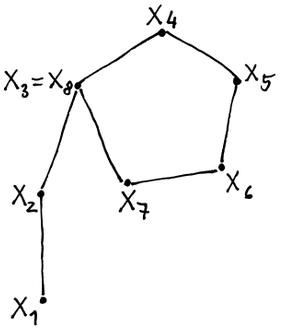
Budeme-li pro ilustraci předpokládat, že pokusné dělení provádíme jen prvočísly menšími než 10, pak $F = 2^3 \cdot 3 \cdot 5 = 120$, $U = 11$, kde $(F, U) = (120, 11) = 1$.

Abychom Pocklington-Lehmerovým testem prokázali prvočíselnost 1321, potřebujeme pro každé $p \in \{2, 3, 5\}$ najít svědka prvočíselnosti $a_p$.

Protože je $\left(2^{\frac{1320}{3}} - 1, 1321\right) = 1$ a $\left(2^{\frac{1320}{5}} - 1, 1321\right) = 1$, lze klást $a_3 = a_5 = 2$. Pro $p = 2$ je ale $\left(2^{\frac{1320}{2}} - 1, 1321\right) = 1321$, proto musíme hledat jiného svědka prvočíselnosti. Vyhoví například $a_2 = 7$, protože $\left(7^{\frac{1320}{2}} - 1, 1321\right) = 1$. V obou případech platí, že $2^{1320} \equiv 7^{1320} \equiv 1 \pmod{1321}$. Svědkové prvočíselnosti čísla 1321 jsou tedy $a_2 = 7, a_3 = a_5 = 2$. Případně bylo možné (ale nikoliv nutné) zvolit pro všechna prvočísla $p$ totéž číslo (např. 13), které je primitivním kořenem modulo 1321. □

**10.85.** Pomocí Pollardovy $\rho$-metody rozložte číslo 221 na prvočísla. Využijte přitom funkci $f(x) = x^2 + 1$ s iniciální hodnotou $x_0 = 2$.






Níže uvedený algoritmus je opět přímočarou implementací popsaných úvah.

**Algoritmus (Pollardova $\rho$-metoda):**

```
Vstup: n, rozkládané číslo a
vhodná funkce f(x)

a := 2; b := 2; d := 1
While d = 1 do
   a := f(a)
   b := f(f(b))
   d := gcd(a − b, n)
If d = n, return FAILURE.
Else return d.
```

**10.48. Kryptografie s veřejným klíčem.** V současné praxi je nejdůležitější aplikací teorie čísel tzv. kryptografie s veřejným klíčem. Jejími hlavními úkoly je zajistit



- šifrování, kdy zprávu *zašifrovanou* veřejným klíčem příjemce není schopen rozšifrovat nikdo kromě něj (resp. držitele jeho soukromého klíče);
- podepisování, kdy integrita zprávy *podepsané* soukromým klíčem odesílatele může být ověřena kýmkoliv s přístupem k veřejnému klíči odesílatele.

Mezi základní a nejčastěji používané protokoly v kryptografii s veřejným klíčem patří:

- RSA (šifrování) a odvozený systém pro podepisování zpráv,
- algoritmus digitálního podpisu (Digital Signature Algorithm – DSA) a jeho varianta založená na eliptických křivkách (ECDSA),
- Rabinův kryptosystém (a podepisování),
- kryptosystém ElGamal (a podepisování),
- kryptografie eliptických křivek (ECC),
- Diffie-Hellmanův protokol na výměnu klíčů (DH).

**10.49. Šifrování – RSA.** Popišme nejprve nejznámější šifru s veřejným klíčem – RSA. Princip protokolu *RSA*[14] je následující:



[14] Ron Rivest, Adi Shamir, Leonard Adleman (1977); C. Cocks, tajná služba GCHQ (neveřejně) již 1973

**Řešení.** Položme $x = y = 2$ a postupem z 10.47 počítejme:

| $x := f(x)$ | $y := f(f(y))$ | $(\lvert x - y\rvert, 221)$ | mod 221 |
|---|---|---|---|
| 5 | 26 | 1 | |
| 26 | 197 | 1 | |
| 14 | 104 | 1 | |
| 197 | 145 | 13 | |

Nalezli jsme tedy netriviálního dělitele a snadno dopočteme $221 = 13 \cdot 17$. □

**10.86.** Nalezněte netriviálního dělitele čísla 455459.

**Řešení.** Uvažujme funkci $f(x) = x^2 + 1$ (mlčky předpokládáme, že se tato funkce modulo neznámý prvočíselný dělitel $p$ čísla $n$ chová náhodně a má tak požadované vlastnosti) a v jednotlivých iteracích počítáme $a \leftarrow f(a) \pmod n$, $b \leftarrow f(f(b)) \pmod n$ spolu s vyčíslením $d = (a - b, n)$.

| a | b | d |
|---|---|---|
| 5 | 26 | 1 |
| 26 | 2871 | 1 |
| 677 | 179685 | 1 |
| 2871 | 155260 | 1 |
| 44380 | 416250 | 1 |
| 179685 | 43670 | 1 |
| 121634 | 164403 | 1 |
| 155260 | 247944 | 1 |
| 44567 | 68343 | 743 |

Hledaným dělitelem je tedy číslo 743 a snadno dopočítáme, že $455459 = 613 \cdot 743$. □

## F. Šifrování

**10.87. RSA.** Šifrou RSA s veřejným klíčem (7, 33) byla poslána čísla 29, 7, 21. Pokuste se šifru prolomit a zjistit zasílané zprávy (čísla).



**Řešení.** Pro zjištění soukromého klíče $d$ potřebujeme řešit kongruenci $7d \equiv 1 \pmod{\varphi(33)}$. Protože číslo 33 je dost malé na to, abychom určili jeho rozklad na prvočísla, jednoduše spočítáme $\varphi(33) = (3 - 1)(11 - 1) = 20$. Hledáme tedy $d$ tak, aby platilo $7d \equiv 1 \pmod{20}$, čemuž vyhovuje $d \equiv 3 \pmod{20}$. Protože $29^3 \equiv (-4)^3 \equiv 2$, $7^3 \equiv 13$ a $21^3 \equiv 21 \pmod{33}$, jsou zašifrovanou zprávou čísla 2, 13 a 21. □

- Každý účastník $A$ potřebuje dvojici klíčů – veřejný $V_A$ a soukromý $S_A$.
- Generování klíčů: uživatel zvolí dvě velká prvočísla $p, q$, vypočte $n = pq$, $\varphi(n) = (p - 1)(q - 1)$. Číslo $n$ je přitom veřejné, princip tkví v tom,že $\varphi(n)$ nelze snadno spočítat.
- Dále si zvolí *veřejný klíč* $e$ a ověří, že $(e, \varphi(n)) = 1$.
- Například pomocí Euklidova algoritmu spočítá *soukromý klíč* $d$ tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$

PRINCIP RSA

Vlastní šifrovaná komunikace pak probíhá v těchto krocích (v dalším budeme pro zjednodušení vyjadřování ztotožňovat šifrovací proceduru s veřejným klíčem $V_A$ a dešifrovací proceduru se soukromým klíčem $S_A$):

- Zašifrování numerického *kódu* zprávy $M$ pro účastníka $A$ (jakýmkoliv jiným účastníkem s přístupem k veřejnému klíči $V_A$):
$$C = V_A(M) \equiv M^e \pmod n.$$
- Dešifrování šifry $C$ účastníkem $A$:
$$OT = S_A(C) \equiv C^d \pmod n.$$

Důkaz korektnosti tohoto protokolu (tj. toho, že $A$ skutečně obdrží to, co bylo zamýšleno) je přímočarou aplikací Eulerovy věty. Pro libovolnou zprávu $M$, která je nesoudělná s $n$, totiž díky větě 10.17 platí, že $(M^e)^d \equiv M^1 = M \pmod n$. V (extrémně nepravděpodobné) situaci, kdy zpráva $M$ bude soudělná s $n$, tvrzení platí také, i když důkaz je třeba modifikovat s pomocí Čínské zbytkové věty (uvědomte si ale, že pokud je zpráva $M$ s vlastností $0 < M < n$ soudělná s $n$, tak to znamená, že $(M, n)$ je netriviální dělitel $n$ a klíč příjemce je tak vlastně kompromitován).

Bezpečnost RSA je testována od vzniku šifry v roce 1977 a dosud se (s výjimkou postranních kanálů či některých singulárních klíčů) nepodařilo objevit výraznou slabinu (při použití dostatečně velkého klíče, nyní se doporučuje alespoň 2048 bitů). Přesto se dodnes neumí dokázat, že problém RSA *skutečně* závisí na nesnadnosti rozkladu přirozených čísel na součin prvočísel.

Mezi požadavky na bezpečnou volbu klíče vyplývající z praxe jsou zejména:

- $d$ je dostatečně velké (obrana proti tzv. Wienerově útoku),
- $p$ a $q$ nejsou příliš blízká (viz příklad ‖10.87‖),
- volba veřejného klíče o velikosti alespoň $e = 65537$ (přestože není znám žádný přímý útok proti malému veřejnému klíči $e$).

**10.50. Rabinův kryptosystém.** Uveďme si dále zjednodušenou variantu protokolu s názvem *Rabinův kryptosystém*[15], který je prvním veřejným kryptosystémem, k jehož prolomení je prokazatelně potřeba faktorizovat modul (na rozdíl od RSA, kde to zatím prokázáno není):



- Každý účastník $A$ potřebuje dvojici klíčů – veřejný $V_A$ a soukromý $S_A$.
- Generování klíčů: $A$ zvolí dvě podobně velká prvočísla $p, q \equiv 3 \pmod 4$, vypočte $n = pq$.
- Veřejným klíčem je $V_A = n$, soukromým klíčem je dvojice $S_A = (p, q)$.

[15] Rabin, Michael. *Digitalized Signatures and Public-Key Functions as Intractable as Factorization* (in PDF). MIT Laboratory for Computer Science, January 1979.

**Útoky na RSA.**



Pomocí tzv. Fermatovy faktorizace se můžeme pokusit rozložit $n = p \cdot q$, pokud máme důvod se domnívat, že rozdíl $p$ a $q$ je malý.

Pak totiž

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2,$$

kde $s = (p-q)/2$ je malé a $t = (p+q)/2$ je pouze o málo větší než $\sqrt{n}$. Stačí tedy postupně testovat, zda[3] $t = \lceil\sqrt{n}\rceil, t = \lceil\sqrt{n}\rceil + 1, t = \lceil\sqrt{n}\rceil + 2, \ldots$, a to tak dlouho dokud nebude $t^2 - n$ druhou mocninou (což je podmínka, kterou lze efektivně testovat).

**10.88.** Pokusme se tímto způsobem rozložit na prvočísla číslo



$n = 23104222007$, o němž víme, že vzniklo součinem dvou podobně velkých prvočísel.

**Řešení.** Vypočteme

$$\sqrt{n} \approx 152000{,}731$$

a testujeme kandidáty na $t$:

Pro $t = 152001$ je $\sqrt{t^2 - n} \approx 286{,}345$.
Pro $t = 152002$ je $\sqrt{t^2 - n} \approx 621{,}287$.
Pro $t = 152003$ je $\sqrt{t^2 - n} \approx 830{,}664$.
Konečně pro $t = 152004$ je $\sqrt{t^2 - n} = 997 \in \mathbb{Z}$.
Je tedy $s = 997$ a snadno dopočítáme prvočísla z rozkladu: $p = t + s = 153001, q = t - s = 151007$. □

**10.89.** RSA modul $n = p \cdot q$ lze rovněž snadno rozložit, pokud je známo (kompromitováno) číslo $\varphi(n)$. Pak totiž platí

$$\varphi(n) = (p-1)(q-1) = pq-(p+q)+1, \text{ odkud} p+q = n+1-\varphi(n).$$

Máme tedy nalézt dvě čísla, jejichž součet i součin je znám, což lze učinit snadno například s využitím Viètových vztahů mezi kořeny a koeficienty polynomu, z nichž plyne, že $p$ a $q$ jsou kořeny polynomu

$$x^2 - (n + 1 - \varphi(n))x + n.$$

[3] Symbol $\lceil x\rceil$ pro reálné číslo $x$ znamená tzv. horní celou část, tedy takové celé číslo $\lceil x\rceil$, které splňuje $\lceil x\rceil - 1 < x \leq \lceil x\rceil$.

Vlastní šifrovaná komunikace pak probíhá takto:

- Zašifrování numerického *kódu* zprávy $M$: $C = V_A(M) \equiv M^2 \pmod{n}$.
- Dešifrování šifry $C$: vypočtou se (čtyři) odmocniny z $C$ modulo $n$ a snadno se zjistí, která z nich byla původní zprávou (např. tak, že ostatní tři zprávy nebudou dávat smysl nebo tak, že součástí zprávy bude domluvená identifikace).

Jak je vidět z popisu protokolu, je v rámci dešifrování třeba provést *výpočet druhé odmocniny* z $C$ modulo $n = pq$, kde $p \equiv q \equiv 3 \pmod 4$. Tento výpočet se provede následovně:

- Vypočtou se hodnoty $r \equiv C^{(p+1)/4} \pmod{p}$ a $s \equiv C^{(q+1)/4} \pmod{q}$.
- Dále je třeba určit koeficienty $a, b$ do Bezoutovy rovnosti, tj. taková čísla, pro něž $ap + bq = 1$.
- Položí se $x \equiv (aps + bqr) \pmod{n}$, $y \equiv (aps - bqr) \pmod{n}$.
- Druhými odmocninami z $C$ modulo $n$ jsou pak $\pm x, \pm y$.

Rozmysleme si, že jde vlastně o aplikaci Čínské zbytkové věty a toho, že jsme schopni snadno nalézt řešení kvadratické kongruence $x^2 \equiv a \pmod{p}$, je-li $p \equiv 3 \pmod 4$ (viz příklad ‖10.70‖). Platí totiž, že

$$(\pm x)^2 = (aps + bqr)^2 \equiv (bqr)^2 \equiv$$
$$\equiv r^2 \equiv C^{(p+1)/2} \equiv C \pmod{p}.$$

Při výpočtu jsme využili toho, že $bq \equiv 1 \pmod{p}$ a že $C \equiv M^2 \pmod{p}$ je kvadratický zbytek modulo $p$, a proto $C^{(p-1)/2} \equiv \equiv (C/p) = 1 \pmod{p}$. Podobně rovněž $(\pm x)^2 \equiv C \pmod{q}$, proto je $\pm x$ druhou odmocninou z $C$ modulo $n$. Odvození pro $y$ je takřka identické.

**10.51. Digitální podpis.** Uveďme nyní stručně princip digitálního podepisování.

PRINCIP DIGITÁLNÍHO PODPISU

**Vytvoření podpisu:**

(1) Vygeneruje se otisk (hash) $H_M$ zprávy pevně stanovené délky (např. 160 nebo 256 bitů) – je vhodné si uvědomit, že takové zobrazení jistě nebude prosté (tedy mnoho zpráv bude mít stejný hash).
(2) Vytvoří se podpis zprávy $S_A(H_M)$ z tohoto hashe s nutností znalosti soukromého klíče podepisujícího (analogie dešifrování textu zprávy).
(3) Odešle se zpráva $M$ (případně zašifrovaná veřejným klíčem příjemce) spolu s takto vytvořeným podpisem.

**Ověření podpisu** následně probíhá takto:

(1) K přijaté zprávě $M$ se (po jejím případném dešifrování) vygeneruje otisk $H'_M$
(2) S pomocí veřejného klíče (deklarovaného) odesílatele zprávy se rekonstruuje původní otisk zprávy $V_A(S_A(H_M)) = H_M$.
(3) Oba otisky se porovnají, tj. zjistí se, zda $H_M = H'_M$.

**10.90.** Uvažte stejně jako výše $n = 23104222007$ a s dodatečnou znalostí $\varphi(n) = 23103918000$ rozložte $n$ na prvočísla.



**Řešení.** Podle výše popsaného postupu dostaneme kvadratickou rovnici

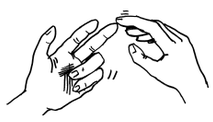
$$x^2 - 304008x + 23104222007 = 0,$$

jejímiž řešeními jsou

$$p = \frac{1}{2}(304008 + \sqrt{304008^2 - 4 \cdot 23104222007} = 153001,$$
$$q = \frac{1}{2}(304008 - \sqrt{304008^2 - 4 \cdot 23104222007} = 151007.$$

□

**10.91. ElGamal.** Martin a Honza chtějí komunikovat šifrou ElGamal navrženou egyptským matematikem Taherem Elgamalem podle protokolu Diffieho a Hellmana na výměnu klíčů. Martin si zvolil prvočíslo 41 a jemu příslušný primitivní kořen $g = 11$ a dále si zvolil číslo 10. Následně zveřejnil trojici $(41, 11, A)$, kde $A \equiv 11^{10} \pmod{41}$; číslo 10 přitom utajil – je to jeho soukromý klíč. Honza mu poslal veřejným kanálem dvojici (22, 6). Jakou zprávu Honza poslal?



**Řešení.** Nejprve pro úplnost vypočítáme celý veřejný klíč $A = 9$ (uvědomte si ale, že toto číslo potřeboval Honza k zašifrování zprávy pro Martina, k dešifrování již není třeba). Zprávu $Z$ dostaneme jako $Z \equiv (6/22^{10}) \pmod{41}$. Spočtěme nejprve

$$22^{10} \equiv 22^2 \cdot \left(22^2\right)^2 \cdot \left(\left(22^2\right)^2\right) \equiv$$
$$\equiv (-8) \cdot (-8)^2 \cdot (-8)^2 \equiv$$
$$\equiv (-8) \cdot 23 \cdot 23 \equiv -9 \pmod{41}$$

a $(-9)^{-1} \equiv 9 \pmod{41}$. Proto je dešifrovanou zprávou číslo

$$Z = 9 \cdot 6 \equiv 13 \pmod{41}.$$

□

**10.92. Rabinův kryptosystém.** V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 23$, $q = 31$, veřejným klíčem je pak $n = pq = 713$. Zašifrujte pro Alici zprávu $M = 327$ a ukažte, jak bude Alice tuto zprávu dešifrovat.



**Řešení.** Vypočteme $C = (327)^2 \equiv 692 \pmod{713}$ a tuto šifru pošleme Alici. Podle postupu pro dešifrování určíme

$$r \equiv C^{(p+1)/4} \equiv 692^{\frac{23+1}{4}} \equiv 18 \pmod{23},$$
$$s \equiv C^{(q+1)/4} \equiv 692^{\frac{31+1}{4}} \equiv 14 \pmod{31}$$

Výše zmiňovaná (kryptografická) hashovací funkce má mít následující vlastnosti:

- Pro libovolnou zprávu je snadné nalézt její hash.
- Nelze (v reálném čase) zjistit (jakoukoliv) zprávu s požadovaným hashem.
- Nelze (v reálném čase) nalézt dvě zprávy se stejným hashem (požadavek na to, aby funkce byla tzv. *odolná vůči kolizím*).
- Každá změna zprávy se projeví změnou hashe.

Nejznámějšími příklady takových funkcí jsou

- MD5 (128 bit, Rivest 1992) – není ale odolná vůči kolizím
- SHA-1 (160 bit, NSA 1995) – od roku 2005 rovněž považována za nedostatečně odolnou vůči kolizím
- RIPEMD-320
- SHA-3

**10.52. Diffie-Hellmanův systém výměny klíčů.** Dalším důležitým typem protokolu, který je v praxi velmi často používán, je *protokol na výměnu klíčů pro symetrickou kryptografii – Diffie-Hellman key exchange*,[16] jehož objev způsobil průlom v této oblasti a umožnil nahradit jednorázové klíče, kurýry s kufříky apod. matematickými prostředky, a to zejména bez požadavku na nutnost předchozí komunikace obou stran.



Princip protokolu pro dohodu dvou stran (Alice, Bob) na společném klíči (čísle) je následující:

PRINCIP DH PROTOKOLU VÝMĚNY KLÍČŮ

- Obě strany se dohodnou na prvočíslu $p$ a primitivním kořenu $g$ modulo $p$ (tuto dohodu není třeba tajit).
- Alice vybere náhodné $a$ a pošle $g^a \pmod{p}$.
- Bob vybere náhodné $b$ a pošle $g^b \pmod{p}$.
- Společným klíčem pro komunikaci je pak $g^{ab} \pmod{p}$.

Bezpečnost tohoto protokolu závisí na obtížnosti výpočtu diskrétního logaritmu (tzv. *discrete logarithm problem*) – viz též část 10.19.

Z protokolu Diffieho a Hellmana na výměnu klíčů je dále odvozen šifrovací *algoritmus ElGamal*, který rovněž stručně popíšeme:

- Každý uživatel si zvolí prvočíslo $p$ spolu s primitivním kořenem $g$.
- Dále zvolí *soukromý klíč* $x$, spočítá $h = g^x \pmod{p}$ a zveřejní *veřejný klíč* $(p, g, h)$.

Vlastní šifrovaná komunikace pak probíhá takto:

- Šifrování numerického kódu zprávy $M$: zvolíme náhodné $y$ a vypočteme $C_1 = g^y \pmod{p}$ a $C_2 = M \cdot h^y \pmod{p}$ a pošleme uživateli $A$ dvojici $(C_1, C_2)$.
- Dešifrování zprávy uživatelem $A$ se provede výpočtem $C_2/C_1^x$.

**Poznámka.** I z algoritmu ElGamal lze analogicky jako v případě RSA odvodit mechanismus digitálního podepisování.

[16] Whitfield Diffie, Martin Hellman (1976); M. Williamson (tajná služba GCHQ) již 1974 (nezveřejněno)

a dále pomocí Euklidova algoritmu koeficienty $a$, $b$ do Bezoutovy rovnosti $23 \cdot a + 31 \cdot b = 1$. Dostaneme $a = -4$, $b = 3$, kandidáty původní zprávy jsou tedy čísla $\mp 4 \cdot 23 \cdot 14 \pm 3 \cdot 31 \cdot 18 \pmod{713}$. Víme tedy, že některé z čísel

$$386,\ 603,\ 110,\ 327$$

je odeslanou zprávou. □

**10.93.** Ukažte, jak pomocí Rabinova kryptosystému s $n = 437$ zašifrovat a dešifrovat zprávu $M = 321$.

**Řešení.** Zašifrovaný text dostaneme jako kvadrát modulo $n$: $C = 321^2 \equiv (-116)^2 = 13456 \equiv 346 \pmod{437}$. Naopak při dešifrování použijeme rozklad (znalost rozkladu je soukromým klíčem příjemce zprávy) $n = 437 = 19 \cdot 23$ a spočítáme $r = 346^{\frac{19+1}{4}} = 346^5 \equiv 17 \equiv -2 \pmod{19}$ a $s = 346^{\frac{23+1}{4}} = 346^6 \equiv 1 \pmod{23}$. Euklidovým algoritmem pro $(19, 23) = 1$ určíme koeficienty v Bezoutově rovnosti

$$19 \cdot (-6) + 23 \cdot 5 = 1.$$

Zpráva je pak jedno z čísel $\pm 6 \cdot 19 \cdot 1 \pm 5 \cdot 23 \cdot (-2) \pmod{437}$, tj. $M = \pm 116$ nebo $M = \pm 344$. Opravdu $M = -116 \equiv 321 \pmod{437}$. □

## G. Doplňující příklady k celé kapitole

*10.94.* Dokažte, že existuje nekonečně mnoho lichých přirozených čísel $k$ s vlastností, že čísla $2^{2^n}+k$ jsou složená pro všechna $n \in \mathbb{N}$. ○

*10.95.* Dokažte, že pro každé celé číslo $k \neq 1$ existuje nekonečně mnoho přirozených čísel $n$ s vlastností, že číslo $2^{2^n}+k$ je složené. ○

*10.96.* Uvažte posloupnost $(a_n)_{n=1}^{\infty}$, kde

$$a_n = 2^n + 3^n + 6^n - 1$$

a dokažte, že pro libovolné prvočíslo $p$ existuje v této posloupnosti člen, který je násobkem tohoto prvočísla. ○

*10.97.* Dokažte, že pro žádné $n \in \mathbb{N}$, $n > 1$ neplatí $n \mid 2^n - 1$. ○

*10.98.* Dokažte, že pro každé liché prvočíslo $p$ existuje nekonečně mnoho přirozených čísel $n$, splňujících $p \mid n \cdot 2^n + 1$. ○

*10.99.* Nechť pro funkci $f : \mathbb{N} \to \mathbb{N}$ platí $(f(a), f(b)) = (f(a), f(|a-b|))$. Dokažte, že pak $(f(a), f(b)) = f((a,b))$. Ukažte, že odtud vyplývá tvrzení příkladu ‖10.6‖ i fakt $(F_a, F_b) = F_{(a,b)}$, kde $F_a$ značí $a$-tý člen Fibonacciho posloupnosti. ○

## Řešení cvičení

*10.25*.

i) Číslo 3 je řádu 4 modulo 10, proto stačí zjistit zbytek exponentu po dělení čtyřmi. Ten je roven jedné, proto je poslední číslice rovna $3^1 = 3$.

ii) $37 \equiv -3 \pmod{10}$ je řádu 4. Opět stačí spočítat, jaký zbytek dává exponent po dělení čtyřmi. Zřejmě ale $37 \equiv 1 \pmod 4$, proto je hledaný zbytek po dělení desíti roven $(-3)^1 \equiv 7$, a tedy poslední cifrou je 7.

iii) Protože $(12, 10) > 1$, nelze mluvit o řádu čísla 12 modulo 10. Zřejmě je ale zkoumané číslo sudé, proto stačí zjistit, jaký zbytek dává po dělení 5. Řád čísla $12 \equiv 2 \pmod 5$ je čtyři a exponent splňuje $13^{14} \equiv 1^{14} = 1 \pmod 4$, proto je $12^{13^{14}} \equiv 2^1 \pmod 5$ a protože je 2 číslo sudé, je i hledanou poslední číslicí.

*10.27*. Protože je $\varphi(n) \leq n$, pak určitě $\varphi(n) \mid n!$, odkud již plyne tvrzení, protože pro lichá $n$ rovněž platí $2^{\varphi(n)} \equiv 1 \pmod n$.

*10.41*. i) Největší společný dělitel modulů je 3, přitom $1 \not\equiv -1 \pmod 3$, proto soustava řešení nemá.

ii) Podmínka pro řešitelnost lineárních kongruencí $(8, 12345678910111213) = 1$ je triviálně splněna, kongruence má tedy jedno řešení.

iii) Moduly jsou nesoudělné, z Čínské zbytkové věty proto plyne existence jediného řešení modulo $29 \cdot 47$.

*10.44*. Protože číslo 2 je primitivním kořenem jak modulo 5, tak modulo 13, dostáváme, že

$$2^n \equiv 3 \pmod 5 \iff 2^n \equiv 2^3 \pmod 5 \iff n \equiv 3 \pmod 4$$

a

$$2^n \equiv 3 \pmod{13} \iff 2^n \equiv 2^4 \pmod{13} \iff n \equiv 4 \pmod{12}.$$

Odtud na jednu stranu dostáváme nekonečnost počtu násobků 5 i 13 mezi čísly tvaru $2^n - 3$, na druhou stranu ale vidíme, že žádné takové číslo nemůže být násobkem 5 i 13 současně, protože soustava kongruencí $n \equiv 3 \pmod 4$, $n \equiv 4 \pmod{12}$ řešení nemá.

*10.94*. Pro všechna přirozená čísla $n$ je $2^{2^n} \equiv 1 \pmod 3$, proto stačí za $k$ zvolit lichá čísla s vlastností $k \equiv 2 \pmod 3$, kterých je jistě nekonečně mnoho – jsou to právě čísla splňující $k \equiv 5 \pmod 6$ – a dostaneme čísla $2^{2^n} + k > 3$, která jsou násobkem 3 a tedy jistě složená.

*10.95*. Uvažme pevné $k \in \mathbb{Z} \setminus \{1\}$ a libovolné $a \in \mathbb{N}$. Ukážeme, že pro $a$ libovolně velké dokážeme najít $n$ takové, že číslo $2^{2^n} + k$ bude složené a větší než $a$. Tím bude důkaz hotov.

Buďte dále $s \in \mathbb{N}_0$, $h \in \mathbb{Z}$ taková, že $k - 1 = 2^s \cdot h$, $2 \nmid h$, a $m \in \mathbb{N}$ splňující $2^{2^m} > a - k$. Nechť nyní pro $\ell$ platí $\ell \geq s$, $\ell \geq m$. Je-li číslo $2^{2^\ell} + k$ složené, pak jsme hotovi, protože $2^{2^\ell} + k \geq 2^{2^m} + k > a$. Nechť je tedy dále $2^{2^\ell} + k$ rovno prvočíslu $p$. S pomocí Eulerovy věty najdeme číslo požadovaného tvaru, které je jeho násobkem. Máme

$$p - 1 = 2^{2^\ell} + 2^s \cdot h = 2^s \cdot h_1,$$

kde $h_1 \in \mathbb{N}$ je liché. Platí tedy $2^{\varphi(h_1)} \equiv 1 \pmod{h_1}$, odkud $2^{s+\varphi(h_1)} \equiv 2^s \pmod{p-1}$ a protože je $l \geq s$, rovněž

$$2^{\ell+\varphi(h_1)} \equiv 2^\ell \pmod{p-1}.$$

Z Malé Fermatovy věty nyní plyne, že

$$2^{2^{\ell+\varphi(h_1)}} + k \equiv 2^{2^\ell} + k \equiv 0 \pmod p.$$

Protože ale $2^{\ell+\varphi(h_1)} > 2^\ell$, je i $2^{2^{\ell+\varphi(h_1)}} + k > 2^{2^\ell} + k = p > a$ a dostali jsme tak složené číslo požadovaného tvaru, které je větší než (libovolně velká) předepsaná hodnota $a$.

Poznamenejme na závěr, že pro $k = 1$ jde o otevřený problém zkoumající existenci nekonečně mnoha Fermatových prvočísel.

*10.96*. Snadno vidíme, že $2 \mid a_1 = 10$ a $3 \mid a_2 = 48$. Ukážeme dále, že pro libovolné prvočíslo $p > 3$ platí $p \mid a_{p-2}$. Podle Fermatovy věty je $2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod{p}$. Proto platí

$$6a_{p-2} = 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \equiv 3 + 2 + 1 - 6 = 0 \pmod{p}.$$

Poznamenejme, že se znalostí algebry budeme schopni postupovat ještě přímočařeji: pro $p > 3$ uvážíme $p$-prvkové těleso $\mathbb{F}_p$, v němž existují inverzní prvky čísel 2, 3, 5 a pro součet těchto prvků platí $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$.

*10.97*. Úvahy vycházející z rozkladu $n$ na prvočísla jsou poměrně komplikované, zde ukážeme řešení využívající menšího triku. Předpokládejme, že $n$ splňující podmínky $n \mid 2^n - 1, n > 1$, existuje a uvažme nejmenší takové. Určitě bude $n$ liché, proto $n \mid 2^{\varphi(n)} - 1$. S využitím tvrzení příkladu ‖10.6‖ dostaneme, že $n \mid 2^d - 1$ , kde $d = (n, \varphi(n))$ (a odtud zejména plyne $2^d - 1 > 1$ a $d > 1$). Přitom je $d \leq \varphi(n) < n$ a $d \mid n$, odkud konečně $d \mid 2^d - 1$ a to je spor s předpokladem, že $n$ bylo nejmenší přirozené číslo větší než 1, které vyhovuje zadání.

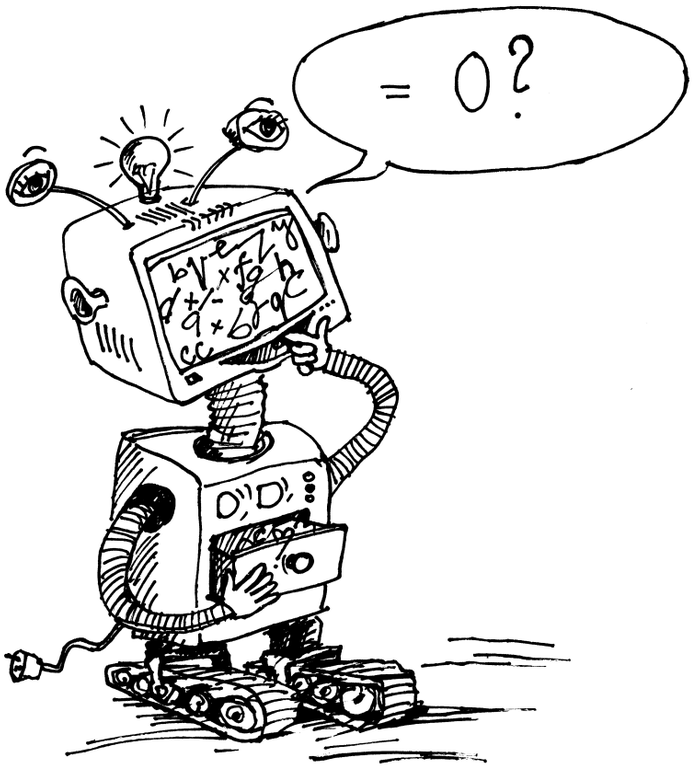
*10.98*. Protože je $2^{p-1} \equiv 1 \pmod{p}$, stačí např. za $n$ volit vhodné násobky $p - 1$, tedy nalézt $k$ tak, aby $n = k(p-1)$ splnilo podmínku $n \cdot 2^n \equiv -1 \pmod{p}$. Ta je ale díky $p - 1 \mid n$ ekvivalentní s podmínkou $k \equiv 1 \pmod{p}$ a takových $k$ zřejmě vyhovuje nekonečně mnoho.

*10.99*. Rozborem Eukleidova algoritmu na hledání největšího společného dělitele.

KAPITOLA 11

# Algebraické struktury

*čím větší abstrakce, tím větší zmatek?*
*– ne, často to bývá naopak ...*




V této kapitole se budeme věnovat zdánlivě velice formálnímu studiu pojmů, které ale ve skutečnosti odráží spoustu skutečných vlastností věcí kolem nás.

Abstrahujeme z nich přitom jen ty nejjednodušší operace a „algebru“ tak lze vnímat jako algoritmické manipulace s písmeny, které zpravidla mají nějaké souvislosti s výpočty nebo popisem procesů. Zároveň si budeme trochu všímat, kde všude jsme takové objekty potkávali v předchozích kapitolách (aniž by ale bylo nutné mít tyto kapitoly předem pročtené). Přímo navážeme víceméně jen na první a šestou část první kapitoly, kde jsme podobně abstraktně pohlíželi na čísla, se kterými počítáme, a obecněji na vztahy mezi objekty, když jsme je abstrahovali do tzv. relací.

V první části této kapitoly se zastavíme u té nejjednodušší situace – budeme se zamýšlet nad případem, kdy máme jen jednu jedinou operaci, která se chová podobně jako násobení čísel. Pak si přidáme druhou operaci, podobně jako jsou u čísel k dispozici společně sčítání a násobení. To nám umožní vysvětlit elementární základy tzv. počítačové algebry, tj. algoritmických postupů, díky kterým počítače umí manipulovat s formálními výrazy a počítat s nimi, včetně řešení systémů polynomiálních rovnic.

V další části se vrátíme k jiné abstrakci situací s jedinou operací a budeme přitom vycházet z uspořádání čísel podle velikosti nebo množinové inkluze. V poslední části kapitoly se pak zastavíme u několika poznámek ohledně využití algebraických nástrojů pro návrhy (samoopravných) kódů využívaných hojně při přenosech dat.

## A. Algebraické struktury

Nejprve si procvičme obecné vlastnosti operací a zkusíme zjistit, co vlastně známé množiny se známými operacemi tvoří za struktury.

**11.1.** Rozhodněte o následujících množinách a operacích, jaké tvoří algebraické struktury (grupoid, pologrupa, zda existují levé (pravé) neutrální prvky, grupa):

i) podmnožiny množiny přirozených čísel spolu s operací sjednocení,

## 1. Grupy



Naše první úvahy se budou týkat objektů a situací, ve kterých je možné rovnice tvaru $a \cdot x = b$ vždy jednoznačně řešit (tak jako u lineárních rovnic jsou objekty $a$ a $b$ dány, zatímco $x$ hledáme). Půjde o tzv. teorii grup. Všimněme si, že zatím nic nevíme o povaze objektů, ani co znamená ta tečka. Jen předpokládáme, že dvěma objektům $a$ a $x$ umíme přiřadit objekt $a \cdot x$.

Nejprve si oprášíme a rozšíříme náš slovník pojmů ohledně operací, jak jsme jej zavedli již v kapitole první a projdeme přitom příklady čísel a transformací roviny a prostoru, ve kterých se s takovými „grupovými“ objekty potkáváme. Teprve pak se budeme chvíli věnovat základům obecné teorie.

**11.1. Příklady a pojmy.** Pro libovolnou množinu $A$ jsme již dříve definovali *binární operaci* na $A$ jako libovolné zobrazení $A \times A \to A$. Výsledek takové operace budeme často značit

$$(a, b) \mapsto a \cdot b.$$

Množina s binární operací se nazývá *grupoid*.

ii) přirozená čísla spolu s binární operací největší společný dělitel,
iii) kladná celá čísla spolu s binární operací nejmenší společný násobek,
iv) množina všech invertibilních matic $2\times 2$ nad $\mathbb{R}$ spolu se sčítáním,
v) množina všech matic $2\times 2$ nad $\mathbb{R}$ spolu s násobením matic,
vi) množina všech matic $2\times 2$ spolu s odčítáním matic,
vii) množina všech invertibilních matic $2\times 2$ nad $\mathbb{Z}_2$ s násobením matic,
viii) množina $\mathbb{Z}_6$ spolu s násobením (modulo 6),
ix) množina $\mathbb{Z}_7$ spolu s násobením (modulo 7).

U třetího příkladu od konce sestavte tabulku dané operace.

**Řešení.**

i) monoid (prázdná množina je neutrálním prvkem),
ii) pologrupa (bez neutrálního prvku),
iii) monoid (číslo 1 je neutrálním prvkem),
iv) není ani grupoid (uvážíme $A+(-A)$ pro nějakou invertibilní matici $A$),
v) monoid,
vi) grupoid (není asociativní),
vii) grupa,
viii) monoid (třída [1] je neutrálním prvkem),
ix) monoid (třída [1] je neutrálním prvkem),

V případě vii) má grupa následující prvky: $A = \begin{pmatrix}1&0\\0&1\end{pmatrix}$, $B = \begin{pmatrix}0&1\\1&0\end{pmatrix}$, $C = \begin{pmatrix}1&1\\0&1\end{pmatrix}$, $D = \begin{pmatrix}1&1\\1&0\end{pmatrix}$, $E = \begin{pmatrix}0&1\\1&1\end{pmatrix}$, $F = \begin{pmatrix}1&0\\1&1\end{pmatrix}$. Potom tabulka operace násobení matic vypadá následovně:

| | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ |
|---|---|---|---|---|---|---|
| $A$ | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ |
| $B$ | $B$ | $A$ | $E$ | $F$ | $C$ | $D$ |
| $C$ | $C$ | $D$ | $A$ | $B$ | $F$ | $E$ |
| $D$ | $D$ | $C$ | $F$ | $E$ | $A$ | $B$ |
| $E$ | $E$ | $F$ | $B$ | $A$ | $D$ | $C$ |
| $F$ | $F$ | $E$ | $D$ | $C$ | $B$ | $A$ |

Všimněme si, že v tabulce se v každém řádku i sloupci (bez prvního řádku a sloupce) vyskytuje každý prvek právě jednou (proč tomu tak je?). Nemusíme tedy všechny součiny počítat a můžeme si v jisté fázi doplňování tabulky zahrát „Sudoku“. □

Abychom mohli něco podstatného říci, potřebujeme nějaké další vlastnosti operací. Binární operace je *asociativní*, jestliže pro všechny prvky v $A$ platí

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c.$$

### Binární operace a pologrupy

Grupoid s asociativní binární operací se nazývá *pologrupa*. Binární operace je *komutativní*, jestliže pro všechny prvky v $A$ platí $a\cdot b=b\cdot a$.

Přirozená čísla $\mathbb{N}=\{0,1,2,\dots\}$ spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupou. Celá čísla $\mathbb{Z}=\{\dots,-2,-1,0,1,2,\dots\}$ jsou grupoidem vůči kterékoliv z operací sčítání, odčítání, násobení. Operace odčítání ale není asociativní, např.

$$(5-3)-2=0\neq 5-(3-2)=4,$$

ani komutativní, protože $a-b=-(b-a)$.

### Jednotky, inverze a grupy

*Levá jednotka* v grupoidu $(A,\cdot)$ je takový prvek $e\in A$, že pro všechny prvky v $A$ platí $e\cdot a=a$; obdobně pro *pravou jednotku* musí platit pro všechny prvky $a\cdot e=a$. *Jednotka* binární operace je prvek $e$, který je pravou i levou jednotkou zároveň.

Prvek $a^{-1}$ je *levou inverzí* k prvku $a$ v pologrupě $(A,\cdot)$ s jednotkou $e$, jestliže platí $a^{-1}\cdot a=e$; obdobně je *pravou inverzí* $a^{-1}$ takový prvek, pro který je $a\cdot a^{-1}=e$.

Prvek $a^{-1}$ je *inverzní* k $a$ v pologrupě s jednotkou, jestliže je levou i pravou inverzí zároveň.

*Monoid* $(M,\cdot)$ je pologrupa s jednotkou. *Grupa* $(G,\cdot)$ je pologrupa s jednotkou, ve které má každý prvek inverzi.

*Komutativní grupa*, resp. *komutativní pologrupa*, je taková, kde je operace $\cdot$ komutativní.

Komutativní grupy se také často nazývají *abelovské*. počest mladého matematika Abela ... V angličtině se používá přídavné jméno

Podívejme se na přímé jednoduché důsledky definic. V monoidu nemohou být pravé a levé inverze různé. Je-li totiž $a\cdot x=x\cdot b=e$, pak také

$$a=a\cdot(x\cdot b)=(a\cdot x)\cdot b=b.$$

Podstatná je zde pouze asociativita operace. Všimněme si, že pro odečítání na celých číslech (tady operace není asociativní) je nula *pravou jednotkou*, tj. $a-0=a$ pro všechna celá čísla $a$, není však levou jednotkou. Dokonce v tomto případě levý neutrální prvek neexistuje.

Celá čísla jsou zjevně pologrupou vůči sčítání i násobní. Grupou jsou přitom jen vůči sčítání, protože pro násobení neexistují inverzní prvky, kromě čísel $\pm 1$.

Je-li $(A,\cdot)$ grupa, pak její podmnožinu $B\subseteq A$, která je uzavřená vůči zúžení operace $\cdot$ a zároveň je spolu s touto operací grupou, nazýváme *podgrupa*.

Jestliže zadáme v grupě $G$ nějakou množinu prvků $M\subset G$, pak *podgrupa generovaná množinou* $M$ je nejmenší podgrupou, která věechny prvky $M$ obsahuje. Zjevně půjde o průnik všech podgrup, které $M$ obsahují.

**11.2.** Nechť $X$ je libovolná množina. Nechť $\mathcal{P}(X)$ značí systém všech podmnožin množiny $X$. Určete, zda množina $\mathcal{P}(X)$ tvoří s danou operací grupoid, pologrupu, pologrupu s neutrálním prvkem (monoid), grupu a zda je zadaná operace komutativní.

i) průnik množin,
ii) sjednocení množin,
iii) symetrický rozdíl množin.

**Řešení.** Je-li množina $X$ prázdná, potom tvoří $\mathcal{P}(X)$ se všemi operacemi komutativní grupu. V ostatních případech

i) s operací průnik tvoří daná množina komutativní pologrupu s neutrálním prvkem,
ii) s operací sjednocení tvoří daná množina komutativní pologrupu s neutrálním prvkem,
iii) s operací symetrický rozdíl tvoří daná množina komutativní grupu, neutrálním prvkem je prázdná množina a každý prvek je samoinverzní $A^{-1} = A$. □

*11.3.* Rozhodněte o následujících množinách a operacích, jaké tvoří struktury (grupoid, pologrupa, grupa). Určete zda existují levé (pravé) neutrální prvky a zda ja daná operace komutativní.

i) množina všech invertibilních matic $3\times3$ nad $\mathbb{R}$ spolu se sčítáním,
ii) množina všech matic $3 \times 3$ nad $\mathbb{R}$ spolu s násobením matic,
iii) množina všech matic $3 \times 3$ spolu se sčítáním matic,
iv) množina všech invertibilních matic $3\times3$ nad $\mathbb{Z}_2$ s násobením matic,
v) množina $(\mathbb{Z}_9, +)$,
vi) množina $(\mathbb{Z}_9, \cdot)$.

○

*11.4.* Rozhodněte, zda podmnožina $G$ komplexních čísel tvoří spolu s operací násobení komplexních čísel grupoid, pologrupu, pologrupu s neutrálním prvkem (monoid), grupu a zda je zadaná operace komutativní.

i) $G = \{a + bi \mid a, b \in \mathbb{Z}\}$,
ii) $G = \{a + bi \mid a, b \in \mathbb{R}, a^2 + b^2 = 1\}$,
iii) $G = \{a + b \cdot \sqrt{5} \mid a, b \in \mathbb{Q}, a^2 + b^2 \neq 0\}$.

○

*11.5.* Rozhodněte, zda daná množina $\mathbb{Z}$ tvoří spolu s operací $\heartsuit$ (komutativní) grupoid, (komutativní) pologrupu, (komutativní) monoid, (komutativní) grupu:



Racionální čísla $\mathbb{Q}$ jsou komutativní grupou vzhledem ke sčítání a nenulová racionální čísla jsou také komutativní grupou vůči násobení. Celá čísla spolu se sčítáním jsou jejich podgrupou.

Pro každé kladné přirozené číslo $k$ je množina všech $k$-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$, konečnou grupou vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.

Množina $\mathrm{Mat}_n$, $n > 1$, všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic (viz odstavce 2.2–2.5).

Množina všech lineárních zobrazení $\mathrm{Hom}(V, V)$ na vektorovém prostoru je pologrupa vzhledem ke skládání zobrazení a komutativní grupa vzhledem ke sčítání zobrazení (viz odstavec 2.34).

V obou předchozích příkladech tvoří podmnožina invertibilních objektů uvažované pologrupy grupu. V prvním případě jde o tzv. grupu invertibilních matic, ve druhém o grupu lineárních transformací vektorového prostoru.

V dřívějších kapitolách jsme již potkali mnoho (polo)grupových struktur, občas asi i docela nečekaně. Vzpomeňme např. různé podgrupy grupy matic nebo grupovou strukturu na eliptických křivkách.

**11.2. Grupy permutací.** Velmi často grupy a pologrupy potkáváme jako množiny zobrazení na pevně dané množině $M$, které jsou uzavřeny vůči skládání zobrazení. Ne vždy si ale tuto skutečnost přímo uvědomujeme, protože vidíme jen některá zobrazení a na všechna ostatní vznikající složeními nemyslíme.



Nejsnáze je tato souvislost vidět na konečných množinách $M$, kde nám každá podmnožina invertibilních zobrazení vygeneruje pomocí skládání jistou grupu.

Na každé takové množině o $m = |M| \in \mathbb{N}$ prvcích (prázdná množina má 0 prvků) totiž máme k dispozici $m^m$ možných definic zobrazení (každý z $m$ prvků můžeme zobrazit na kterýkoliv v $M$) a všechna taková zobrazení umíme skládat. Protože skládání zobrazení je samozřejmě asociativní operace, dostáváme grupoid.

Pokud chceme, aby existovala k zobrazení $\alpha : M \to M$ jeho inverze $\alpha^{-1}$, musí být $\alpha$ bijekcí. Složením dvou bijekcí vznikne opět bijekce, a proto podmnožina $\Sigma_m$ všech bijekcí na množině $M$ o $m$ prvcích je grupa. Říkáme jí *grupa permutací* (na $m$ prvcích) a je příkladem konečné grupy.[1]

Sám název grupy $\Sigma_m$ přitom uvádí jinou souvislost, kdy místo bijekcí na konečné množině vnímáme permutace jako přerovnání rozlišitelných prvků. Potkávali jsme se s permutacemi v tomto smyslu např. při studiu determinantů, viz odstavec 2.14 na straně 76.

Promysleme si podrobněji, jak vlastně násobení v takové grupě vypadá. U (malé) konečné grupy si můžeme snadno sestavit úplnou tabulku všech operací. Jestliže v grupě permutací $\Sigma_3$ na číslech $\{1, 2, 3\}$ označíme jednotlivá pořadí

$$a = (1, 2, 3),\ b = (2, 3, 1),\ c = (3, 1, 2),$$
$$d = (1, 3, 2),\ e = (3, 2, 1),\ f = (2, 1, 3),$$

[1] Lze dokázat, že každá konečná grupa je podgrupou ve vhodné konečné grupě permutací. To si můžeme interpretovat tak, že grupy $\Sigma_m$ jsou tak nekomutativní a složité, jak to jen jde.

i) $a \heartsuit b = (a, b)$,
ii) $a \heartsuit b = a^{|b|}$,
iii) $a \heartsuit b = 2a + b$,
iv) $a \heartsuit b = |a|$,
v) $a \heartsuit b = a + b + a \cdot b$,
vi) $a \heartsuit b = a + b - a \cdot b$,
vii) $a \heartsuit b = a + (-1)^a b$.

○

**11.6.** Určete, kolika způsoby lze doplnit tabulka tak, aby $(\{a, b, c\}, \divideontimes)$ byl

i) grupoid
ii) komutativní grupoid
iii) grupoid s neutrálním prvkem
iv) pologrupa s neutrálním prvkem
v) grupa

| $\divideontimes$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $c$ | $b$ | $a$ |
| $b$ | | | $b$ |
| $c$ | | | |

**Řešení.**

i) $3^5$
ii) 9
iii) 9
iv) 1
v) 0

□

**11.7.** Určete počet všech grupoidů na dané trojprvkové množině.

**Řešení.** Grupoid je určen tím, jak na něm působí daná operace. V grupoidu může být výsledkem aplikace operace na libovolné dva prvky libovolný prvek grupoidu. Pro každou uspořádanou dvojici tedy máme nezávisle na výběr ze tří možností výsledku operace na ní. Podle pravidla součinu tak dostáváme

$$3^{3 \cdot 3} = 19683$$

různých grupoidů. □

*11.8.* Rozhodněte, zda množina $G = (\mathbb{R} \setminus \{0\} \times \mathbb{R})$ s operací $\triangle$ tvoří grupoid, pologrupu, pologrupu s neutrálním prvkem (monoid), grupu a zda je zadaná operace komutativní, jestliže je operace $\triangle$ definována takto: $(x, y) \triangle (u, v) = (xu, xv + y)$, pro libovolná $(x, y), (u, v) \in G$.

○

pak skládání našich permutací je zadáno tabulkou

| $\cdot$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
|---|---|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
| $b$ | $b$ | $c$ | $a$ | $f$ | $d$ | $e$ |
| $c$ | $c$ | $a$ | $b$ | $e$ | $f$ | $d$ |
| $d$ | $d$ | $e$ | $f$ | $a$ | $b$ | $c$ |
| $e$ | $e$ | $f$ | $d$ | $c$ | $a$ | $b$ |
| $f$ | $f$ | $d$ | $e$ | $b$ | $c$ | $a$ |

Všimněme si podstatného rozdílu mezi permutacemi $a$, $b$ a $c$ a dalšími třemi. Ty první tři tvoří tzv. *cyklus* generovaný prvkem $b$ nebo prvkem $c$:

$$b^2 = c,\ b^3 = a,\ c^2 = b,\ c^3 = a.$$

Samy o sobě jsou tyto tři prvky komutativní podgrupou. V této podgrupě je $a$ jednotka a prvky $b$ a $c$ jsou vzájemně inverzní. Je tedy tato podgrupa stejná jako je grupa $\mathbb{Z}_3$ zbytkových tříd celých čísel modulo 3, resp. jako grupa třetích odmocnin z jedničky.

Další tři prvky jsou samy sobě inverzí a každý z nich je tedy společně s jednotkou $a$ podgrupou stejnou jako je $\mathbb{Z}_2$. Říkáme, že $b$ a $c$ jsou *prvky řádu* 3, zatímco prvky $d$, $e$ a $f$ jsou řádu 2.

Tabulka ale není symetrická podle diagonály, naše operace $\cdot$ tedy není komutativní.

Obdobně se chovají všechny grupy permutací $\Sigma_m$ konečných množin o $m$ prvcích. Každá permutace $\sigma$ rozkládá množinu $M$ na disjunktní sjednocení maximálních invariantních podmnožin, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu $M_x$ přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \ldots$, dokud není $\sigma^k(x) = x$. Každou permutaci tak dostáváme jako složení jednodušších permutací, tzv. cyklů, které se chovají jako identická permutace vně $M_x$ a tak jako $\sigma$ na $M_x$. Pokud přitom očíslujeme prvky v $M_x$ jako pořadí $(1, 2, \ldots, |M_x|)$ tak, aby $i$ odpovídalo $\sigma^i(x)$, pak je naše permutace prostým posunutím o jednu pozici v cyklu (tj. poslední prvek je zobrazen zpátky na první). Odtud název *cyklus*. Zjevně přitom tyto cykly komutují, takže je jedno, v jakém pořadí z nich permutaci $\sigma$ složíme.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace $\sigma$ a dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$. Těm se říká *transpozice*. Protože každý cyklus zjevně můžeme poskládat z permutací sousedních prvků (necháme „probublat“ první prvek na konec), lze každou permutaci napsat jako složení transpozic sousedních prvků.

Vraťme se k případu $\Sigma_3$. Tam máme jednak možnost cyklu, který zahrne všechny tři prvky a v něm dostaneme permutace $a$, $b$, $c$. Kromě toho ještě můžeme mít jeden cyklus o délce 2 a zbývající prvek bude pevným bodem – tak dostaneme zbývající 3 permutace. Více možností není. Z postupu je zřejmé, že u větších počtů prvků bude možností velmi mnoho.

Jednotlivé permutace můžeme obecně vyjádřit pomocí transpozic mnoha způsoby. Přitom ale skutečnost, jestli potřebujeme sudý nebo lichý počet transpozic, je na volbách nezávislá (můžeme tuto skutečnost vyjádřit pomocí počtu tzv. inverzí a poslední tvrzení pak plyne z toho, že každá transpozice mění počet inverzí o lichý počet, viz úvahy v odstavci 2.15 na straně 77).

Máme tedy dobře definováno zobrazení

$$\operatorname{sgn} : \Sigma_m \to \mathbb{Z}_2 = \{\pm 1\},$$

## B. Grupy

Začneme připomenutím permutací a některých jejich vlastností. S permutacemi jsme se již setkali ve druhé kapitole, viz 2.14, kde jsme je potřebovali k definici determinantu matice.

*11.9.* Určete všechny permutace $\pi \in \mathbb{S}_7$ tak, aby

i) $\pi^4 = (1,2,3,4,5,6,7)$

ii) $\pi^2 = (1,2,3) \circ (4,5,6)$

iii) $\pi^2 = (1,2,3,4)$

○

**11.10.** Určete znaménka daných permutací

i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 3n-2 & 3n-1 & 3n \\ 2 & 3 & 1 & 5 & 6 & 4 & \dots & 3n-1 & 3n & 3n-2 \end{pmatrix}$,

ii) $\begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & n+2 & \dots & 2n \\ 2 & 4 & 6 & \dots & 2n & 1 & 3 & \dots & 2n-1 \end{pmatrix}$.

**Řešení.** Znaménko permutace je dáno paritou počtu traspozic v rozkladu permutace, ekvivalentně také paritou počtu inverzí permutace, viz 2.15. Počet inverzí snadno spočítáme z dvojřádkového zápisu permutace. Procházíme postupně čísla ve druhém řádku a za každé připočteme počet čísel menších než právě vybrané ležících v řádku dále než právě vybrané. Dostáváme tak, že v prvním případě je permutace sudá (znaménko je 1), ve druhém případě závisí znaménko permutace na $n$ a je rovno $(-1)^{\frac{n\cdot(n+1)}{2}}$. □

**11.11.** Určete všechny permutace $\rho \in \mathbb{S}_9$ takové, že

$$[\rho \circ (1,2,3)]^2 \circ [\rho \circ (2,3,4)]^2 = (1,2,3,4).$$

**Řešení.** Žádná taková neexistuje, na levé straně je totiž vždy sudá permutace, na pravé straně je permutace lichá. □

*11.12.* Určete všechny permutace $\rho \in \mathbb{S}_9$ takové, že

$$\rho^2 \circ (1,2) \circ \rho^2 = (1,2) \circ \rho^2 \circ (1,2).$$

○

**11.13.** Mějme permutaci $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 2 & 4 \end{pmatrix}$. Určete řád $\sigma$ v grupě $(\mathbb{S}_7, \circ)$, inverzi k $\sigma$ a určete $\sigma^{2013}$. Ukažte, že $\sigma$ nekomutuje s transpozicí $\tau = (2,3)$.

**Řešení.** $\sigma = (1,3,5)\circ(2,6)\circ(4,7)$. Řád $\sigma$ je tedy 6, nejmeší společný násobek čísel 3, 2, 2. Dále $\sigma^{-1} = (1,5,3) \circ (2,6) \circ (4,7)$ a

$$\sigma^{2013} = (\sigma^3 35)^6 \circ \sigma^3 = \sigma^3 = (2,6) \circ (4,7).$$

tzv. *paritu*. Dokázali jsme si znovu tvrzení, která jsme již využívali při studiu determinantů (viz 2.14 a dále):

**Věta.** *Každá permutace konečné množiny je složením cyklů. Cyklus délky $\ell$ lze vyjádřit jako složení $\ell - 1$ transpozic. Parita cyklu délky $\ell$ je $(-1)^{\ell-1}$.*

*Parita složení permutací $\sigma \circ \tau$ je součinem parit $\sigma$ a $\tau$.*

Poslední tvrzení věty říká, že zobrazení sgn převádí složení permutací $\sigma \circ \tau$ na součin $\operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$ v komutativní grupě $\mathbb{Z}_2$.

### Homomorfismy (polo)grup

Obecně říkáme, že zobrazení $f : G_1 \to G_2$ je homomorfismus (polo)grup, jestliže respektuje grupové operace, tzn.

$$f(a \cdot b) = f(a) \cdot f(b).$$

Zejména tedy vidíme, že je naše právě zavedená signatura permutací homomorfismem $\operatorname{sgn} : \Sigma_m \to \mathbb{Z}_2$.

**11.3. Symetrie rovinných útvarů.** V páté části první kapitoly jsme podrobně a elementárně rozebrali souvislosti invertibilních matic se dvěma řádky a dvěma sloupci a lineárními transformacemi v rovině.



Viděli jsme přitom, že matice v $\mathrm{Mat}_2(\mathbb{R})$ zadávají lineární zobrazení $\mathbb{R}^2 \to \mathbb{R}^2$, která zachovávají standardní vzdálenosti, právě když jsou jejich sloupce ortonormální bází $\mathbb{R}^2$ (což je jednoduchá podmínka na souřadnice matice, viz odstavec 1.29 na straně 31).

Ve skutečnosti je snadné dokázat, že každé zobrazení roviny do sebe, které zachovává velikosti, je afinní euklidovské, tj. je složením lineárního a vhodné translace.[2]

Jak jsme již připomněli, lineární část takového zobrazení přitom musí navíc být ortogonální. Všechna taková zobrazení tedy tvoří grupu všech ortogonálních transformací (nebo také euklidovských transformací) v rovině. Navíc jsme ukazovali, že kromě translací $T_a$ o vektor $a$ jde pouze o rotace $R_\varphi$ o jakýkoliv úhel $\varphi$ kolem počátku a zrcadlení $Z_\ell$ vůči jakékoliv přímce $\ell$ procházející počátkem (povšimněme si, že středová souměrnost je totéž jako rotace o $\pi$).



Zastavíme se teď u ilustrace obecných grupových pojmů na problému symetrií rovinných obrazců. Budeme přitom uvažovat objekty typu dlaždiček. Nejprve jednotlivě, tj. ve formě ohraničeného obrázku v rovině, později ještě s požadavkem dláždění v rovinném pásu nebo v celé rovině.

[2] Jestliže totiž má zobrazení $F : \mathbb{R}^2 \to \mathbb{R}^2$ zachovávat velikosti, totéž musí být pravda pro přenášené vektory rychlostí, tj. Jacobiho matice $DF(x,y)$ musí být v každém bodě ortogonální. Rozepsání této podmínky pro dané zobrazení $F = (f(x,y), g(x,y)) : R^2 \to \mathbb{R}^2$ vede na systém diferenciálních rovnic, který má pouze afinní řešení, protože snadno uvidíme, že všechny druhé derivace $F$ musí být nulové (a pak už je naše tvrzení okamžitým důsledkem Taylorovy věty se zbytkem). Zkuste si promyslet detaily! Ve skutečnosti vede stejný postup k výsledku pro euklidovské prostory libovolné dimenze. Všimněte si přitom, že dokazovaná podmínka je nezávislá na volbě afinních souřadnic, proto se složením $F$ s lineárním zobrazením výsledek nemění. Můžeme proto pro pevný bod $(x,y)$ složit $(DF)^{-1} \circ F$ a bez újmy na obecnosti rovnou předpokládat, že $DF(x,y)$ je matice identického zobrazení. Derivováním rovnic pak dostáváme důsledky, které přímo říkají požadované tvrzení.

Dále $\sigma\circ\tau = (1,3,6,2,5)\circ(4,7)$ a $\tau\circ\sigma = (1,2,6,3,5)\circ(4,7)$. □

**11.14.** Určete $\sigma^{-1}$ a $\sigma^{2013}$, kde

- (a) $\sigma = \begin{pmatrix}1&2&3&4&5&6&7\\4&5&7&6&1&2&3\end{pmatrix}$ v grupě permutací $(\mathbb{S}_7,\circ)$.
- (b) $\sigma = [4]_{11}$ v grupě $(\mathbb{Z}_{11}^\times,\cdot)$.

**Řešení.** (a) $\sigma = (1,4,6,2,5)\circ(3,7)$, $\sigma^{-1} = (1,5,2,6,4)\circ(3,7)$, řád cyklu $(1,4,6,2,5)$ je pět, řád transpozice $(3,7)$, a protože jsou čísla 2 a 5 nesoudělná je řád $\sigma$ roven deseti, tedy $\sigma^{10} = 1$. Pak

$$\sigma^{2013} = (\sigma^{10})^{201}\circ\sigma^3 = \sigma^3 = (1,2,4,5,6)\circ(3,7)$$

.

(b) Místo třídy $[k]_{11}$, $k\in\mathbb{Z}$, budeme psát pro zjednodušení zápisu pouze reprezentanta této třídy, tj. číslo $k$. Potom

$$\begin{aligned} 4^5\equiv 1 \pmod 1 1 \Rightarrow \sigma^{-1} &= 4^4\equiv 3 \pmod 1 1\\ \sigma^{2013} &= 4^{2013}\equiv 4^3\equiv 9 \pmod 1 1. \end{aligned}$$

□

**11.15.** Dokažte, že v každé grupě o sudém počtu prvků existuje prvek, který je sám sobě inverzním a přesto to není neutrální prvek.

**Řešení.** Seřaďme prvky dané grupy do dvojic, přičemž ve dvojici bude vždy prvek a jeho inverze. Sám potom zůstane neutrální prvek. To je však celkem lichý počet prvků. □

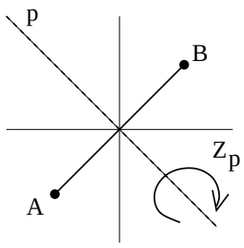
**11.16.** Dokažte, že neexistuje čtyřprvková nekomutativní grupa.

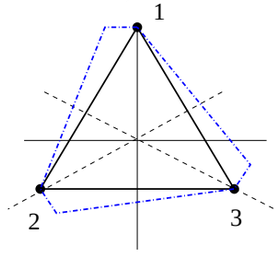
**Řešení.** Podle Lagrangeovy věty (viz 11.10) mohou být řády prvků, které nejsou neutrální, ve čtyřprvkové grupě pouze dva nebo čtyři. Pokud je v grupě prvek řádu čtyři, je tato grupa cyklická, tedy komutativní. Pokud grupa obsahuje kromě neutrálního prvku ještě tři prvky řádu dva, které jsou inverzní samy k sobě (říkejme samoinverzní), musí být součin libovolných dvou z nich roven třetímu (nemůže to být žádný z těch dvou, protože ani jeden není neutrálním prvkem, a nemůže to být neutrální prvek, protože inverze je určena jednoznačně a prvky jsou samoinverzní) a to bez ohledu na pořadí. Ukázali jsme dokonce, že existuje až na isomorfismus jediná čtyřprvková grupa taková, že řády jejích prvků jsou kromě neutrálního rovny dvěma. Této grupě se říká Kleinova grupa a je tedy izomorfní $\mathbb{Z}_2\times\mathbb{Z}_2$. □

**11.17.** Ukažte, že neexistuje pětiprvková nekomutativní grupa.

**Řešení.** Řád prvku, který není neutrální, může být podle Lagrangeovy věty (11.10) pouze pět, taková grupa je tudíž cyklická. □

Pro začátek uvažme třeba úsečku a rovnostranný trojúhelník. Ptáme se, jak moc jsou symetrické, tzn. vůči kterým transformacím (zachovávajícím velikost) jsou invariantní. Jinak řečeno chceme, aby obraz našeho obrazce byl od původního k nerozeznání, dokud si nepopíšeme nějaké význačné body, třeba vrcholy trojúhelníka $A$, $B$ a $C$ a konce úseček. Zároveň je předem jasné, že všechny symetrie pevně zvoleného útvaru budou vždy tvořit grupu (většinou pouze s jediným prvkem, identickým zobrazením).




U úsečky je situace obzvlášť jednoduchá – na první pohled je zřejmé, že jedinými jejími netriviálními symetriemi jsou rotace o $\pi$ kolem středu úsečky, zrcadlení vůči ose této úsečky a zrcadlení vůči úsečce samotné. Všechny tyto symetrie jsou samy sobě inverzí. Celá grupa symetrií úsečky má tedy čtyři prvky. Její tabulka násobení vypadá takto:

| $\cdot$ | $R_0$ | $R_\pi$ | $Z_H$ | $Z_V$ |
|---|---|---|---|---|
| $R_0$ | $R_0$ | $R_\pi$ | $Z_H$ | $Z_V$ |
| $R_\pi$ | $R_\pi$ | $R_0$ | $Z_V$ | $Z_H$ |
| $Z_H$ | $Z_H$ | $Z_V$ | $R_0$ | $R_\pi$ |
| $Z_V$ | $Z_V$ | $Z_H$ | $R_\pi$ | $R_0$ |

.

Je tedy celá tato grupa komutativní.

Pro rovnostranný trojúhelník už symetrií nacházíme víc: můžeme rotovat o $2\pi/3$ nebo můžeme zrcadlit vůči osám stran. Abychom dostali grupu celou, musíme přidat všechna složení takovýchto transformací. Už v 1.29 jsme viděli, že složení dvou zrcadlení je vždy otočením. Zároveň je zřejmé, že složení takových zrcadlení v opačném pořadí dá otočení o stejný úhel, ale s opačnou orientací. V našem případě tedy zrcadlení kolem dvou různých os vygenerují postupnou opakovanou aplikací všechny symetrie, kterých bude dohromady šest. Jestliže si umístíme trojúhelník v souřadnicích jako na obrázku, bude našich šest transformací zadáno maticemi

$$a = \begin{pmatrix}1&0\\0&1\end{pmatrix},\quad b = \begin{pmatrix}-\frac12&\frac{\sqrt3}{2}\\-\frac{\sqrt3}{2}&-\frac12\end{pmatrix},\quad c = \begin{pmatrix}-\frac12&-\frac{\sqrt3}{2}\\\frac{\sqrt3}{2}&-\frac12\end{pmatrix},$$
$$d = \begin{pmatrix}-1&0\\0&1\end{pmatrix},\quad e = \begin{pmatrix}\frac12&-\frac{\sqrt3}{2}\\-\frac{\sqrt3}{2}&-\frac12\end{pmatrix},\quad f = \begin{pmatrix}\frac12&\frac{\sqrt3}{2}\\\frac{\sqrt3}{2}&-\frac12\end{pmatrix}.$$

Sestavením tabulky pro násobení, tak jak jsme ji udělali pro grupu permutací $\Sigma_3$ obdržíme právě stejný výsledek. Pro větší názornost jsou vrcholy označeny čísly, takže jsou příslušné permutace přímo čitelné.

Obdobně umíme nacházet grupy symetrií s $k$ různými rotacemi a $k$ zrcadleními. Stačí si k tomu vzít pravidelný $k$-úhelník. Takové grupy symetrií se často označují jako grupy $D_k$ a říká se jim *dihedrální grupy* řádu $k$. Tyto grupy jsou nekomutativní pro všechna $k\geq 3$, zatímco $D_2$ je komutativní. Název je patrně odvozen od skutečnosti, že $D_2$ je grupa symetrií molekuly vodíku $H_2$, ve které jsou dva atomy vodíku a geometricky si ji lze představit jako úsečku.

**Poznámka.** Stejný argument ukazuje, že cyklické, tedy komutativní grupy, jsou i grupy o libovolném prvočíselném počtu prvků, zejména dvou a tříprvkové grupy. Jak jsme ukázali v ‖11.16‖, tak neexistuje ani čtyřprvková nekomutativní grupa. Nejmenší řád, který by nekomutativní grupa mohla mít je tedy řád šest. Jak jsme viděli v ‖11.1‖(vii) je tomu skutečně tak.

**11.18.** Dokažte, že každá grupa sestávající výhradně ze samoinverzních prvků je komutativní.

**Řešení.** Nechť $a, b \in G$. Potom $ba, b, a$ jsou samoinverzní, tudíž

$$ab = ab((ba)(ba)) = a(bb)aba = (aa)ba = ba.$$

□

**11.19.** Dokažte, že každá grupa řádu 6 je izomorfní buď grupě $\mathbb{Z}_6$ nebo $\mathbb{S}_3$.

**Řešení.** Podle Lagrangeovy věty 11.10 je řád každého prvku takové grupy (různého od neutrálního) 2, 3 nebo 6. Pokud existuje prvek řádu 6, pak je grupa cyklická, tedy izomorfní grupě $\mathbb{Z}_6$. Nyní si uvědomme, že žádný prvek řádu tři není samoinverzní (pro $a$ řádu tři je totiž $a^{-1} = a^2$, neboť $a \cdot a^2 = a^3 = 1$). Pokud by grupa obsahovala pouze prvky řádu tři, tak bychom měli spor s tvrzením příkladu ‖11.15‖ (v grupě o sudém počtu prvků bychom neměli kromě neutrálního prvku žádný jiný samoinverzní).

Víme tedy, že grupa musí obsahovat aspoň jeden samoinverzní prvek (=řádu 2). Ukažme, že v grupě musí být též prvek řádu 3. Pro spor předpokládejme, že všechny prvky $G$ jsou samoinverzní. Pak by $G$ byla podle ‖11.18‖ komutativní. Uvažme dva různé prvky $a, b$ různé od jednotky $e$. Stejně jako v ‖11.16‖ vidíme, že $\{e, a, b, ab\}$ je čtyřprvková podmnožina $G$, ale protože $G$ by byla komutativní, tato množina by byla uzavřená (na danou operaci). Byla by to tedy čtyřprvková podgrupa $G$. To je však ve sporu Lagrangeovou větou (11.10).

Nechť tedy $a$ je prvek řádu 2 a $b$ prvek řádu 3. Grupa tedy obsahuje různé prvky $1, a, b, b^2$ ($a$ je řádu dva, $b$ i $b^2$ řádu tři, takže musí být různé. V grupě dále musí být prvky $ab, ba, ab^2, b^2a$, vzhledem k jednoznačnosti inverze opět žádný z nich nemůže být roven neutrálnímu prvku, dále pak ani žádnému z prvků $a, b, b^2$. Protože grupa má šest prvků, tak množina $\{ab, ba, ab^2, b^2a\}$ má pouze dva prvky. Pokud by se rovnaly prvky začínající stejným písmenkem, tak dospějeme ke sporu. Je tedy buď $ab = ba$, pak ale $(ab)^2 = a^2b^2 = b^2 \neq 1$ a $(ab)^3 = a^3b^3 = a \neq 1$ a prvek $ab$ má nutně řád vyšší než tři, což je spor s naším předpokladem. V tomto případě je tedy grupa cyklická a tudíž izomorfní $\mathbb{Z}_6$. Pokud $ab = b^2a$, pak $ba = a^2b$, jedná se o grupu symetrií rovnostranného trojúhelníka ($a$ odpovídá některé z osových

Stejně tak lze snadno najít obrazce, které mají pouze rotační symetrie a jde tedy o komutativní grupy, které se v chemii značí jako $C_k$. Říkáme jim *cyklické grupy* řádu $k$. K tomu postačí např. uvažovat pravidelný mnohoúhelník, u kterého nesymetricky, ale pořád stejně, pozměníme chování hran, viz čerchované rozšíření trojúhelníka na obrázku. Všimněme si, že grupu $C_2$ lze realizovat dvěma způsoby – buď jedinou netriviální rotací o $\pi$ nebo jediným zrcadlením.

Jako první ukázku síly našich abstraktních úvah dokážeme následující větu. Řekneme, že obrazec má *diskrétní grupu symetrií*, jestliže množina obrazů libovolného bodu při působení všemi prvky grupy je diskrétní podmnožinou v rovině (tj. všechny její body mají okolí, ve kterém už žádný další bod množiny není).

Všimněme si, že každá diskrétní grupa symetrií ohraničeného obrazce je nutně konečná.

**Věta.** *Nechť je $M$ ohraničená množina v rovině $\mathbb{R}^2$ s diskrétní grupou symetrií $G$. Pak je grupa $G$ buď triviální nebo jedna z grup $C_k$, $D_k$ s $k > 1$.*

Důkaz. Kdyby nějaká množina $M$ připouštěla jako svoji symetrii translaci, nemůže být ohraničená. Pokud by $M$ připouštěla rotaci o úhel, jehož žádný celočíselný násobek není $2\pi$ (tj. rotaci o iracionální násobek $2\pi$), pak bychom iteracemi této rotace obdrželi hustou podmnožinu obrazů na příslušné kružnici. Grupa symetrií by tedy nemohla být diskrétní.



Pokud by $M$ připouštěla netriviální rotace s různými středy, opět nemůže být ohraničená. Napíšeme-li totiž příslušné rotace v komplexní rovině jako

$$R : z \mapsto (z - a)\zeta + a, \quad Q : z \mapsto z\eta$$

pro komplexní jednotky $\zeta = \mathrm{e}^{2\pi i/k}$, $\eta = \mathrm{e}^{2\pi i/\ell}$ a libovolné $a \neq 0 \in \mathbb{C}$, pak okamžitě vidíme

$$Q \circ R \circ Q^{-1} \circ R^{-1} : z \mapsto z + a\eta(1 - \zeta),$$

což je translace o netriviální vektor, pokud není úhel rotace $Q$ nulový. Množina $M$ by tedy nemohla být ohraničená.

Totéž platí pro případ, že by existovala rotační symetrie a zrcadlení podél přímky, která neprochází středem rotace.

Máme tedy k dispozici pouze rotace se společným středem a zrcadlení podél přímek tímto středem procházejících.

Zbývá tedy dokázat, že je celá grupa složena vždy buď pouze z rotací nebo vždy ze stejného počtu rotací a zrcadlení. Připomeňme, že vždy složením dvou různých zrcadlení dostáváme rotaci o úhel rovný polovině úhlu svíraného osami zrcadlení (viz 1.29). Proto je i naopak složením zrcadlení podle přímky $p$ s rotací o úhel $\varphi/2$ zase zrcadlení podél přímky svírající úhel $\varphi$ s $p$. Odtud již vcelku snadno plyne požadované tvrzení. □

**11.4. Symetrie rovinných dláždění.** Složitější chování lze vypozorovat u rovinných obrazců v pásech nebo v celé rovině (řekněme, že abstraktně zkoumáme možnosti symetrií pro různé dlažby).

Nejprve uvažme množinu tvořenou pásem v rovině uzavřeném mezi dvěma rovnoběžkami a předpokládejme, že je celý tento pás pokryt disjunktními obrazy ohraničené podmnožiny $M$ pomocí nějaké translace. Tato translace bude samozřejmě symetrií zvoleného dláždění rovinného pásu. Grupa symetrií tedy bude vždy nekonečná.

symetrií podle výšky trojúhelníka, $b$ je rotace kolem středu trojúhelníka o 120°), viz též 11.3. Také si tuto grupu můžeme představit jako grupu permutací na tříprvkové množině ($a$ odpovídá transpozici, $b$ pak cyklu délky tři). Rozebrali jsme tedy všechny možné případy a tím je důkaz dokončen. □

**11.20.** Najděte všechny (až na izomorfismus) komutativní grupy řádu 8. Potom určete, se kterými z těchto nalezených grup jsou izomorfní následující grupy (operací je násobení):

- $\mathbb{Z}_{15}^{\times}$,
- $\mathbb{Z}_{16}^{\times}$,
- $\mathbb{Z}_{17}^{\times}/\{[1],[-1]=[16],\cdot\}$,
- komplexní kořeny polynomu $z^8-1$ (s násobením komplexních čísel.

**Řešení.**

Podle věty v 11.8 je komutativní grupa součinem cyklických. Jejich řád přitom podle 11.10 dělí 8. To znamená, že jediné možnosti jsou $\mathbb{Z}_8$, $\mathbb{Z}_2\times\mathbb{Z}_4$ a $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

- Prvky grupy $\mathbb{Z}_{15}^{\times}$ jsou zbytky nesoudělné s 15. Těch je $\varphi(15)=(5-1)(3-1)=8$, tedy opravdu $|\mathbb{Z}_{15}^{\times}|=8$. Konkrétně jsou to čísla 1, 2, 4, 7, 8, 11, 13, 14. Výpočtem se lze lehce přesvědčit, že řád každého z těchto prvků je buď 2 (4,11,14) nebo 4 (2,7,8,13). $\mathbb{Z}_{15}^{\times}$ je tedy izomorfní grupě $\mathbb{Z}_2\times\mathbb{Z}_4$.
- $\mathbb{Z}_{16}^{\times}=\{1,3,5,7,9,11,13,15\}$. Jde tedy o osmiprvkovou množinu a řád prvků je opět buď 2 (7,9,15) nebo 4 (3,5,11,13). $\mathbb{Z}_{16}^{\times}$ je tedy opět izomorfní grupě $\mathbb{Z}_2\times\mathbb{Z}_4$.
- $\mathbb{Z}_{17}^{\times}=\{\pm1,\pm2,\ldots,\pm8\}$ a tedy přechodem ke kvocientu dostaneme osmiprvkovou množinu $\mathbb{Z}_{17}^{\times}/(\pm1)=\{1,2,\ldots,8\}$. Výpočtem ověříme, že prvek 3 má řád 8 a tedy tuto grupu generuje. To znamená $\mathbb{Z}_{17}^{\times}/(\pm1)\cong\mathbb{Z}_8$.
- Komplexní kořeny polynomu $z^8-1$ jsou $e^{\frac{n\pi}{4}i}$, kde $n=1,2,\ldots,8$. Ty zjevně tvoří cyklickou grupu řádu 8 izomorfní $\mathbb{Z}_8$. □

**11.21.** Nechť $G$ je komutativní grupa. Označme $H=\{g\in G\mid g^2==e\}$, kde $e$ je neutrální prvek grupy $G$. Dokažte, že $H$ tvoří podgrupu grupy $G$.

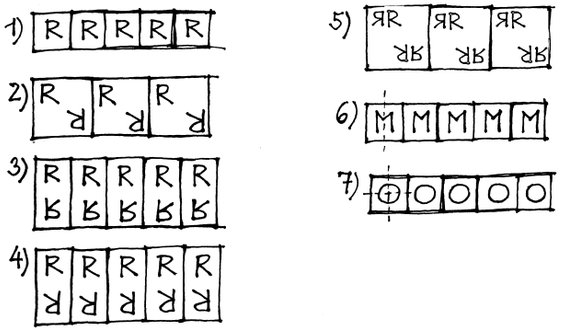
**Řešení.** Z definice $H$ je $e\in H$. Pokud $a\in H$, pak i inverzní prvek k $a$ leží v $H$, neboť $a=a^{-1}$ (protože $a^2=e$). Dále pokud $b\in H$, tak $(ab)^2=a^2b^2=e$ (tady jsme použili komutativity $G$), tedy $ab\in H$ a množina $H$ je uzavřená vůči dané grupové operaci v $G$. Jedná se tudíž o podgrupu. □

Pro symetrie takové množiny nepřicházejí v úvahu žádné netriviální rotace, kromě $R_\pi$, a jediná možná zrcadlení jsou buď horizontální podle osy pásu nebo vertikální podle kterékoliv přímky kolmé na hranice pásu. Zůstávají ještě případné translace zadané vektorem rovnoběžným s osou pásu.

Nepříliš složitá diskuse vede k popisu všech diskrétních grup symetrií pro rovinné pásy. Každá taková grupa je generována některými z následujících možných symetrií: translace $T$, posunuté zrcadlení $G$ (tj. složení horizontálního zrcadlení s translací), vertikální zrcadlení $V$, horizontální zrcadlení $H$ a rotace $R$ o $\pi$.

**Věta.** *Každá diskrétní grupa symetrií dláždění pásu v rovině je jednoho z následujících sedmi typů, tj. je izomorfní s jednou z grup generovaných následujícími symetriemi:*
*(1) jedinou translací $T$,*
*(2) jediným posunutým zrcadlením $G$,*
*(3) jednou translací $T$ a jedním vertikálním zrcadlením $V$,*
*(4) jednou translací $T$ a jednou rotací $R$,*
*(5) jednou posunutou translací $G$ a jednou rotací $R$,*
*(6) jednou translací $T$ a horizontálním zrcadlením $H$,*
*(7) jednou translací $T$, horizontálním zrcadlením $H$ a jedním vertikálním zrcadlením $V$.*

Důkaz zde nyní nebudeme uvádět. Příklady schematických náznaků vzorů s příslušnými symetriemi jsou aspoň na obrázku:




Ještě složitější je to se symetriemi dláždění, které vyplní celou rovinu. Nemáme zde prostor pro podrobnější zkoumání, nicméně alespoň poznamenejme, že všech takových grup symetrií v rovině je pouze sedmnáct. Říká se jim dvourozměrné krystalografické grupy.

Obdobná úplná diskuse je známa i pro trojrozměrné diskrétní grupy symetrií. Bohatá teorie byla vypracována zejména v 19. století v souvislosti se studiem symetrií krystalů a molekul chemických prvků.

**11.5. Homomorfismy grup.** Připomeňme, že zobrazení $f: G\to H$ mezi dvěma grupami $G$ a $H$ se nazývá homomorfismus grup, jestliže respektuje násobení, tj. pro všechny prvky $a,b\in G$ platí



$$f(a\cdot b)=f(a)\cdot f(b).$$

Povšimněme si, že násobení vlevo je uvnitř grupy $G$ předtím, než zobrazujeme, zatímco vpravo jde o násobení v $H$ poté, co zobrazujeme.

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

**Tvrzení.** *Pro každý homomorfismus $f: G\to H$ grup platí*
*(1) obraz jednotky $e\in G$ je jednotka v $H$,*

*11.22.* Označme $\mathcal{GL}_n(\mathbb{R})$ množinu všech regulárních čtvercových matic s reálnými koeficienty. Dokažte, že $G = \mathcal{GL}_2(\mathbb{R})$ tvoří grupu a rozhodněte, zda množina $H$ tvoří podgrupu grupy $G$:

i) $H = \mathcal{GL}_2(\mathbb{Q})$,
ii) $H = \mathcal{GL}_2(\mathbb{Z})$,
iii) $H = \{A \in \mathcal{GL}_2(\mathbb{Z}) \mid |A| = 1\}$,
iv) $H = \left\{\begin{pmatrix} 0 & a \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Q}\right\}$,
v) $H = \left\{\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \mid a \in \mathbb{Z}\right\}$,
vi) $H = \left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q}\right\}$,
vii) $H = \left\{\begin{pmatrix} 0 & a \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{R}\right\}$,
viii) $H = \left\{\begin{pmatrix} 1 & a \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{R}\right\}$.

○

*11.23.*

i) Rozhodněte, zda množina $H = \{a \in \mathbb{R}^* \mid a^2 \in \mathbb{Q}\}$ tvoří podgrupu grupy $(\mathbb{R}^*, \cdot)$
ii) Rozhodněte, zda množina $H = \{a \in \mathbb{R} \mid a^2 \in \mathbb{Q}\}$ tvoří podgrupu grupy $(\mathbb{R}, +)$

○

*11.24.* Najděte přirozené číslo $m$ různé od pěti tak, aby byla grupa $\mathbb{Z}_m^\times$ izomorfní s $\mathbb{Z}_5^\times$. ○

**11.25.** Kolik existuje v $\mathbb{S}_n$ cyklů délky $p$ $(1 < p \leq n)$?

**Řešení.** Prvky, které se v cyklu „motají“, můžeme vybrat $\binom{n}{p}$ možnostmi. Z vybraných $p$ prvků potom jeden pevně vybereme (pokud permutujeme čísla, řekněme, že vybereme nejmenší číslo) a to se může v cyklu zobrazit na libovolný z $p-1$ zbývajících prvků. Tento obraz se pak může zobrazit 1na $p-2$ prvků atd. Podle pravidla součinu tak celkem máme $(p-1)!$ různých cyklů. Výběrem úvodního čísla nezatěžujeme naše úvahy žádným dodatečným omezením, neboť pevně vybraný prvek se musí v každém cyklu někam zobrazit. □

**11.26.** Nechť $G$ je množina reálných matic majících nuly nad diagonálou a jedničky na diagonále. Dokažte, že $G$ spolu s maticovým násobením tvoří grupu, tj. podgrupu v $\mathcal{GL}(3, \mathbb{R})$ a určete centrum $G$. Centrum grupy $G$ je podgrupa $Z(G) = \{z \in G \mid \forall g \in G : zg = gz\}$.

**Řešení.** Buď můžeme ověřit všechny definiční vlastnosti grupy, nebo využijeme známého faktu, že $\mathcal{GL}(3, \mathbb{R})$ je grupa a ověříme pouze

*(2) obraz inverze k prvku je inverzí obrazu. tj.*

$$f(a^{-1}) = f(a)^{-1},$$

*(3) obraz podgrupy $K \subseteq G$ je podgrupa $f(K) \subseteq H$,*
*(4) vzorem $f^{-1}(K) \subseteq G$ podgrupy $K \subseteq H$ je podgrupa,*
*(5) je-li $f$ zároveň bijekcí, pak i inverzní zobrazení $f^{-1}$ je homomorfismus,*
*(6) $f$ je injektivní zobrazení, právě když $f^{-1}(e) = \{e\}$.*

Důkaz. Je-li $K \subseteq G$ podgrupa, pak pro každé dva prvky $y = f(a)$, $z = f(b)$ v $H$ nutně také $y \cdot z = f(a \cdot b)$ patří do obrazu. Je proto vždy obrazem podgrupy opět podpologrupa (tj. bude to podgrupa, pokud obraz nutně obsahuje i inverze a jednotku).

Speciálně triviální podgrupa $\{e\}$ má za obraz opět podpologrupu. Protože z rovnosti $z \cdot z = z$ v grupě $H$ vynásobením prvkem $z^{-1}$ dostáváme $z = e$, ověřili jsme, že jedinou jednoprvkovou podpologrupou v grupě je triviální podgrupa $\{e\}$. Zejména tedy $f(e) = e$.

Přímo z definice homomorfismu nyní vidíme, že

$$f(a^{-1}) \cdot f(a) = f(e) = e,$$

tj. $f(a)^{-1} = f(a^{-1})$. Dokázali jsme tedy první tři tvrzení.

Stejně postupujeme u vzorů: jestliže $a, b \in G$ splňují $f(a)$, $f(b) \in K \subseteq H$, potom také $f(a \cdot b) \in K$.

Předpokládejme, že existuje inverzní zobrazení $g = f^{-1}$ a zvolme libovolné $y = f(a), z = f(b) \in H$. Pak $f(a \cdot b) = y \cdot z = f(a) \cdot f(b)$, což je ekvivalentní výrazu $g(y) \cdot g(z) = a \cdot b = g(y \cdot z)$. Je tedy inverze skutečně homomorfismem.

Pokud platí $f(a) = f(b)$, pak $f(a \cdot b^{-1}) = e \in H$. Pokud je tedy jediným vzorem jednotky v $H$ jednotka v $G$, pak $a \cdot b^{-1} = e$, tj. $a = b$. Opačná implikace je zřejmá. □

Podgrupa $f^{-1}(e)$ jednotkového prvku $e \in H$ se nazývá *jádro* homomorfismu $f$ a značíme ji $\ker f$. Bijektivní homomorfismus grup nazýváme *izomorfismus*.

Z předchozích tvrzení okamžitě vyplývá, že homomorfismus $f : G \to H$ s triviálním jádrem je izomorfismem na obraz $f(G)$.

**11.6. Příklady.** Grupy zbytkových tříd $\mathbb{Z}_k$ jsou izomorfní grupám



komplexních $k$–tých odmocnin z jedničky, což jsou zároveň izomorfní obrazy konečných grup otočení v rovině o celé násobky úhlu $2\pi/k$. Nakreslete si obrázek, počítání s tzv. komplexními jednotkami $e^{2\pi i/k}$ je velmi efektivní.

Zobrazení $\exp : \mathbb{R} \to \mathbb{R}_+$ je izomorfismus aditivní grupy reálných čísel na multiplikativní grupu kladných reálných čísel.

Tento izomorfismus se přirozeně rozšiřuje na morfismus $\exp : \mathbb{C} \to \mathbb{C} \setminus 0$ aditivní grupy komplexních čísel na multiplikativní grupu všech nenulových komplexních čísel. Pro komplexní čísla přitom ale dostáváme netriviální jádro. Viděli jsme totiž, že zúžení exp na ryze imaginární čísla (což je podgrupa izomorfní $\mathbb{R}$) je homomorfismem

$$it \mapsto e^{it} = \cos t + i \sin t,$$

tzn. že čísla $2k\pi i$, $k \in \mathbb{Z}$, jsou v jádru. Snadno se dopočítá, že je to celé jádro. Je-li totiž $e^{s+it} = e^s \cdot e^{it} = 1$ pro reálná $s$ a $t$, musí být $e^s = 1$, tj. $s = 0$, a pak zbývá pouze $t = 2k\pi$ pro libovolné celé $k$.

Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár v $\mathbb{K}$ (pracovali jsme s $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$).

uzavřenost množiny $G$ vzhledem k násobení a braní inverze. Neutrální prvek, tedy jednotková matice, totiž do $G$ z definice patří.

$$\begin{pmatrix}1&0&0\\a&1&0\\b&c&1\end{pmatrix}\begin{pmatrix}1&0&0\\a_1&1&0\\b_1&c_1&1\end{pmatrix}=\begin{pmatrix}1&0&0\\a+a_1&1&0\\b+ca_1+b_1&c+c_1&1\end{pmatrix}\in G,$$

$$\begin{pmatrix}1&0&0\\a&1&0\\b&c&1\end{pmatrix}^{-1}=\begin{pmatrix}1&0&0\\-a&1&0\\-b+ac&-c&1\end{pmatrix}\in G.$$

Z tvaru součinu prvků v $G$ plyne, že centrum je tvořeno prvky

$$Z(G)=\begin{pmatrix}1&0&0\\0&1&0\\b&0&1\end{pmatrix}.$$ □

**11.27.** Pro libovolnou podmnožinu $X\subseteq G$ definujeme její centralizér $C_G(X)=\{y\in G\mid xy=yx,\text{ pro všechna } x\in X\}$. Dokažte, že pokud $X\subseteq Y$, pak $C_G(Y)\subseteq C_G(X)$. Dále dokažte, že $X\subseteq C_G(C_G(X))$ a že $C_G(X)=C_G(C_G(C_G(X)))$.

**Řešení.** První tvrzení je zřejmé - prvky $G$, které komutují se všemi prvky $Y$ komutují zejména se všemi prvky z $X$. Z definice je $C_G(C_G(X))=\{y\in G\mid xy=yx,\forall x\in C_G(X)\}$ a to splňují zejména prvky $y\in X$. Poslední tvrzení dostaneme jednoduše aplikací předchozích dvou. Dosazením $X:=C_G(X)$ do druhého máme $C_G(X)\subseteq C_G(C_G(C_G(X)))$ a aplikováním prvního tvrzení na druhé máme $C_G(X)\supseteq C_G(C_G(C_G(X)))$. □

**11.28.** Předpokládejme, že grupa $G$ má netriviální podgrupu $H$, která je obsažena v každé jiné netriviální podgrupě $G$. Dokažte, že $H$ je obsažena v centru $G$.

**Řešení.** Pro každé $g\in G$ je centralizér $C_G(g)=\{x\in G\mid xg=gx\}$ netriviální podgrupa, protože $g\in C_G(g)$ a $C_G(e)=G$. Grupa $H$ je tedy obsažena v každém $C_G(g)$. Tím pádem je obsažena i v jejich průniku, kterým je podle definice právě centrum. □

**11.29.** Nechť je $G$ konečná grupa. Třída konjugace pro $a\in G$ je množina tvaru

$$Cl(a)=\{xax^{-1}\mid x\in G\}.$$

Dokažte, že

i) množina všech tříd konjugace prvků v $G$ tvoří rozklad $G$,

ii) počet prvků v třídě konjugace dělí řád grupy $G$,

iii) pokud má $G$ pouze dvě třídy konjugace, pak je její řád 2.

**Řešení.** (i) Stačí ukázat, že pro dva prvky $a,b\in G$ je buď $Cl(a)=Cl(b)$, nebo $Cl(a)\cap Cl(b)=\emptyset$. Mají-li však $Cl(a)$ a $Cl(b)$ neprázdný průnik, pak z definice existují $x,y\in G$ tak, že $xax^{-1}=yby^{-1}$, tedy vynásobením rovnosti prvkem $y^{-1}$ zleva a prvkem $y$ zprava obdržíme $y^{-1}xax^{-1}y=b$, ovšem $(y^{-1}x)^{-1}=x^{-1}y$, Cauchyova věta o determinantu součinu čtvercových matic

$$\det(A\cdot B)=(\det A)\cdot(\det B)$$

je tedy tvrzením, že pro grupu $G=GL(n,\mathbb{K})$ invertibilních matic je $\det: G\to\mathbb{K}\setminus 0$ homomorfismem grup.

**11.7. Součin grup.** Jestliže máme k dispozici dvě grupy, můžeme snadno vytvořit složitější grupu následující konstrukcí:

SOUČIN GRUP

Pro každé dvě grupy $G$, $H$ definujeme *součin grup* $G\times H$ takto: Jako množina je $G\times H$ skutečně součin a násobení definujeme po složkách. tj.

$$(a,x)\cdot(b,y)=(a\cdot b,x\cdot y),$$

kde nalevo vystupuje součin, který definujeme, zatímco napravo používáme tečku k naznačení součinů v jednotlivých grupách $G$ a $H$.

Projekce na jednotlivé komponenty $G$ a $H$ v součinu:

$$p_G: G\times H\ni(a,b)\mapsto a\in G,\quad p_H: G\times H\ni(a,b)\mapsto b$$

jsou surjektivní homomorfismy grup s jádry

$$\ker p_G=\{(e_G,b);\ b\in H\}\simeq H,$$
$$\ker p_H=\{(a,e_H);a\in G\}\simeq G.$$

Grupa $\mathbb{Z}_6$ je izomorfní součinu $\mathbb{Z}_2\times\mathbb{Z}_3$. Docela snadno můžeme toto tvrzení vidět při multiplikativní realizaci grup zbytkových tříd $\mathbb{Z}_k$ jakožto komplexních $k$-tých odmocnin z jedničky. Skutečně tak vidíme, že $\mathbb{Z}_6$ je tvořeno body na jednotkové kružnici v komplexní rovině ve vrcholech pravidelného šestiúhelníka. $\mathbb{Z}_2$ pak odpovídá $\pm1$, $\mathbb{Z}_3$ pravidelnému trojúhelníku s jedním vrcholem v jedničce. Jestliže budeme ztotožňovat příslušné body s otočeními v rovině, které jedničku převede právě do nich, pak skládání dvou takových otočení bude vždy komutativní a kombinacemi jednoho otočení ze $\mathbb{Z}_2$ a jednoho ze $\mathbb{Z}_3$ dostaneme právě všechna otočení ze $\mathbb{Z}_6$. Nakreslete si obrázek! Takto tedy dostaneme (při obvyklejší aditivní notaci pro zbytkové třídy) izomorfismus:

$$[0]_6\mapsto([0]_2,[0]_3),$$
$$[1]_6\mapsto([1]_2,[2]_3),$$
$$[2]_6\mapsto([0]_2,[1]_3),$$
$$[3]_6\mapsto([1]_2,[0]_3),$$
$$[4]_6\mapsto([0]_2,[2]_3),$$
$$[5]_6\mapsto([1]_2,[1]_3).$$

Vzápětí uvidíme, že jsou podobné konstrukce k dispozici pro konečné komutativní grupy úplně obecně.

**11.8. Komutativní grupy.** Libovolný prvek $a$ v grupě $G$ je obsažen v minimální podgrupě $\{\dots,a^{-2},a^{-1},e,a,a^2,a^3,\dots\}$, která jej obsahuje. Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa $G$ konečná, nutně musí jednou nastat případ $a^k=e$. Nejmenší $k$ s touto vlastností nazýváme *řád prvku* $a$ v $G$. Grupa $G$ je *cyklická grupa*, je-li celé $G$ generované nějakým svým prvkem $a$ výše uvedeným způsobem. Pokud je řád $k$ generátoru grupy konečný, jde právě o grupy $C_k$ z naší diskuse symetrií obrazců v rovině.

tedy $b$ je tvaru $zaz^{-1}$ pro $z = y^{-1}x$, tudíž je prvkem $Cl(a)$. Ze symetrie je i $a \in Cl(b)$, a tak se obě třídy konjugace rovnají.

(ii) Všimněme si, že prvky v $Cl(a)$ jsou v jednoznačné korespondenci s třídami rozkladu určeného centralizérem $C_G(a) = \{x \in G \mid xax^{-1} = a\}$. Skutečně, pro prvky $b$ a $c$ ležící ve stejné třídě rozkladu (tj. splňující $b = cz$ pro nějaké $z \in C_G(a)$) platí

$$bab^{-1} = cza(cz)^{-1} = czaz^{-1}c^{-1} = czz^{-1}ac^{-1} = cac^{-1}.$$

Podle věty 9.10 je $|G| = |C_G(a)| \cdot |G/C_G(a)|$ a tedy $|Cl(a)| = |G/C_G(a)|$ dělí $|G|$.

(iii) Neutrální prvek tvoří vždy samostatnou třídu konjugace $Cl(e) = \{e\}$. Mají-li tedy existovat pouze dvě třídy, pak nutně musí být všechny ostatní prvky $a \neq e$ v jedné třídě. Ta má zjevně $|G| - 1$ prvků a podle předchozího musí $|G| - 1$ dělit $|G|$, tj. $|G| = 2$. □

**11.30.** Nechť prvky $a, b$ komutativní grupy $G$ mají nesoudělné řády $r, s$. Ukažte, že řád prvku $ab$ je $rs$.

**Řešení.** Víme, že

$$(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = e^s e^r = e,$$

takže řád $ab$ je nejvýše $rs$. Kdyby $(ab)^q = e$ pro nějaké $q < rs$, pak vzhledem k nesoudělnosti $r$ a $s$ nedělí jedno z těchto čísel číslo $q$. Bez újmy na obecnosti předpokládejme, že je to $r$. Pak

$$e = e^s = ((ab)^q)^s = (ab)^{qs} = a^{qs}b^{qs} = a^{qs}.$$

Řád prvku $a$ musí tedy dělit $qs$. Ale $r$ je nesoudělné s $q$, musí tedy dělit $q$. Spor. □

**11.31.** Dokažte, že každá konečná grupa $G$ řádu většího jak 2 má netriviální automorfismus.

**Řešení.** Pokud $G$ není komutativní a prvek $a$ není z centra, pak konjugace $x \mapsto axa^{-1}$ zadává netriviální automorfismus. Pro cyklickou grupu řádu $m$ máme pro $n$ nesoudělné s $m$ automorfismus $x \mapsto x^n$. Je-li $G$ komutativní, pak podle věty v 9.8 je součinem cyklických grup. V případě, že řád aspoň jednoho z faktorů je větší než 2, můžeme použít předchozí automorfismus pro cyklické grupy. Pokud je řád všech faktorů 2, pak je automorfismem permutace libovolných dvou faktorů. □

**11.32.** Nechť $(\mathbb{Q}, +)$ je grupa racionálních čísel se sčítáním a nechť $(\mathbb{Q}^+, \cdot)$ je grupa kladných racionálních čísel s násobením. Určete všechny homomorfismy $(\mathbb{Q}, +) \to (\mathbb{Q}^+, \cdot)$.

**Řešení.** Jediný takový je triviální homomorfismus. Předpokládejme, že by existoval netriviální homomorfismus $\varphi$, tj. $\varphi(a) = b \neq 1$ pro nějaká $a, b \in \mathbb{Q}$. Pak pro všechna $n \in \mathbb{N}$ je

Z definice přímo vyplývá, že každá cyklická grupa je izomorfní buď grupě celých čísel $\mathbb{Z}$ (pokud je nekonečná) nebo některé grupě zbytkových tříd $\mathbb{Z}_k$ (když je konečná). Ve skutečnosti z takových jednoduchých stavebních kamenů můžeme poskládat všechny konečné komutativní grupy.

**Věta.** *Každá konečná komutativní grupa $G$ je izomorfní součinu cyklických grup $C_k$.*

*Je-li $n = p_1^{k_1} \cdots p_r^{k_r}$ rozklad přirozeného čísla $n$ na prvočísla, pak je grupa $C_n$ izomorfní součinu*

$$C_n = C_{p_1^{k_1}} \times \cdots \times C_{p_r^{k_r}}.$$

Důkaz. Obecné první tvrzení věty zde vůbec nebudeme dokazovat. Několika poznámkami se ještě k problematice vrátíme v odstavci 11.12.

Důkaz druhého tvrzení začneme jednodušším speciálním případem, kdy $n = pq$ s nesoudělnými $p$ a $q$. Zvolme generátory $a$ grupy $C_n$, $b$ grupy $C_p$ a $c$ grupy $C_q$. Nabízí se definovat zobrazení $f : C_n \to C_p \times C_q$ vztahem

$$f(a^k) = (b^k, c^k).$$

Protože platí $a^k \cdot a^\ell = a^{k+\ell}$ a podobně pro $b$ a $c$, dostáváme

$$f(a^k \cdot a^\ell) = (b^{k+\ell}, c^{k+\ell}) = (b^k, c^k) \cdot (b^\ell, c^\ell),$$

a jde tedy o homomorfismus. Jestliže je obrazem jednotka, pak $k$ musí být zároveň násobkem $p$ i $q$. Protože jsou $p$ a $q$ nesoudělné, znamená to, že je $k$ i násobkem $n$ a je proto $f$ injektivní. Přitom zřejmě mají grupy $C_n$ i $C_p \times C_q$ stejně prvků, takže jde o izomorfismus. Odtud již vyplývá tvrzení věty o rozkladu cyklických grup řádu $k$ na součiny menších cyklických grup. □

Všimněme si, že naopak $C_{p^2}$ nikdy není izomorfní součinu $C_p \times C_p$. Zatímco $C_{p^2}$ je totiž generované prvkem řádu $p^2$, největší dostupný řád prvku v $C_p \times C_p$ je jenom $p$.

Vzhledem k tomu, že všechny konečné komutativní grupy jsou izomorfní součinu cyklických grup, můžeme pro malé počty prvků najít všechny takové grupy až na izomorfismus. Např. máme jen dvě grupy s 12 prvky

$$C_{12} = C_4 \times C_3, \quad C_2 \times C_2 \times C_3 = C_2 \times C_6.$$

Podobně si můžeme povšimnout, že mají-li všechny prvky v grupě $G$ kromě jednotky řád 2, pak jde o grupu $(C_2)^n$ pro nějaké $n$, zejména tedy má $2^n$ prvků. Skutečně kdybychom totiž v rozkladu $G$ na součin cyklických grup povolili $C_p$ s $p > 2$, pak by tam nutně musely vzniknout prvky vyššího řádu.

**11.9. Rozklady podle podgrup.** Volbou libovolné podgrupy $H$ v grupě $G$ dostáváme další informace o struktuře celé grupy. Na množině prvků grupy $G$ nyní definujeme relaci $a \sim_H b$, jestliže $b^{-1} \cdot a \in H$. Tato relace vystihuje, kdy jsou prvky v $G$ „stejné“, až na násobení něčím z $H$ zprava. Snadno ověříme, že je takto definovaná relace ekvivalence:



Platí $a^{-1} \cdot a = e \in H$, je tedy relace reflexivní. Je-li $b^{-1} \cdot a = h \in H$, potom $a^{-1} \cdot b = (b^{-1} \cdot a)^{-1} = h^{-1} \in H$, je proto relace symetrická. Konečně je-li $c^{-1} \cdot b \in H$ a zároveň je $b^{-1} \cdot a \in H$, potom $c^{-1} \cdot a = c^{-1} \cdot b \cdot b^{-1} \cdot a \in H$, ověřili jsme tedy i tranzitivitu.

Celá grupa $G$ se proto jako množina rozpadá na tzv. *levé třídy rozkladu* podle podgrupy $H$ vzájemně ekvivalentních prvků. Třídu

$b = \varphi(a) = \varphi(n\frac{a}{n}) = \varphi(\frac{a}{n})^n$. To je ovšem spor, protože jen některé $n$-té odmocniny z $b$ jsou racionální (srovnej s ‖1.95‖). □

**11.33.** Nechť $G$ je grupa matic tvaru $\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}$, kde $a, b \in \mathbb{R}$ a $a > 0$ a $N$ je množina matic tvaru $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$, kde $b \in \mathbb{R}$. Ukažte, že $N$ je normální podgrupa $G$ a dokažte, že $G/N$ je izomorfní $\mathbb{R}$.

**Řešení.** Klíčem k důkazu je formule pro násobení v $G$:

$$\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ b_1 & a_1^{-1} \end{pmatrix} = \begin{pmatrix} aa_1 & 0 \\ ba_1 + a^{-1}b_1 & a^{-1}a_1^{-1} \end{pmatrix}.$$

Z této formule je vidět, že zobrazení $\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix} \mapsto a$ je homomorfismus, jehož jádro je $N$. $N$ je tedy normální podgrupa $G$. Navíc $G/N$ je izomorfní $\mathbb{R}^+$, což je izomorfní aditivní grupě $\mathbb{R}$. □

**11.34.** Nechť $G$ je grupa řádu 14, která má normální podgrupu řádu 2. Dokažte, že $G$ je komutativní.

**Řešení.** Označme danou normální podgrupu $N$. Pak $G/N$ je grupa a její řád je $|G/N| = \frac{|G|}{|N|} = 7$. Podle Lagrangeovy věty 11.10 je řád každého jejího prvku buď 1 nebo 7. To ovšem znamená, že řád aspoň jednoho prvku je 7 a tedy že $G/N$ je cyklická. Nechť $N = \{e, n\}$, kde $e$ je neutrální prvek $G$ a generátor grupy $G/N$ je $[a]$. Protože $N$ je normální, je $ana^{-1} \in N$, ale protože $ana^{-1} = e \Longrightarrow n = e$, musí být $ana^{-1} = n$, tedy $na = an$. Protože $[a]$ generuje $G/N$, je každý prvek $G/N$ tvaru $[a]^k$, $k = 0, \ldots, 6$, tedy $[a^k]$. Každý prvek $G$ je tak tvaru $a^k$, nebo $a^k n$, a protože prvky $a$ a $n$ spolu komutují, komutují spolu libovolné prvky $G$. □

*11.35.* Rozhodněte, o platnosti tvrzení: Je-li faktorgrupa $G/N$ komutativní a $N$ normální, pak je $G$ je rovněž komutativní. ◯

**11.36.** Dokažte, že libovolná podgrupa $G$ grupy permutací $\mathbb{S}_n$ obsahuje buď pouze sudé permutace, nebo stejný počet sudých a lichých permutací.

**Řešení.** Uvažme homomorfismus $p : G \to \mathbb{Z}_2$ přiřazující každé permutaci její paritu. Potom $p^{-1}(0) = \mathrm{Ker}(p)$ je normální podgrupa $G$: nechť $h \in \mathrm{Ker}(p)$, pak

$$p(ghg^{-1}) = p(g)p(h)p(g^{-1}) = p(g)p(g^{-1}) = p(gg^{-1}) =$$

$$= p(e) = 0,$$

což znamená, že $ghg^{-1} \in \mathrm{Ker}(p)$, tedy $\mathrm{Ker}(p)$ je normální. $Z_2$ má pouze dva prvky, takže $G/\mathrm{Ker}(p)$ je buď jednoprvková ($\mathrm{im}(p) = 0$), nebo má dvě a to stejně početné třídy rozkladu, tedy $G$ je tvořena buď samými sudými pertmutacemi, nebo lichých ($p^{-1}(1)$) a sudých permutací musí být v $G$ stejně. □

příslušející prvku $a$ značíme $a \cdot H$ a skutečně platí, že

$$a \cdot H = \{a \cdot h;\ h \in H\},$$

neboť prvek $b$ je ve stejné třídě s $a$, právě když jde takovýmto způsobem vyjádřit.

Množinu všech levých tříd rozkladu podle podgrupy $H$ označujeme $G/H$.

Obdobně definujeme pravé třídy rozkladu $H \cdot a$. Příslušná ekvivalence je: $a \sim b$, jestliže $a \cdot b^{-1} \in H$. Proto

$$H \setminus G = \{H \cdot a;\ a \in G\}.$$

**Tvrzení.** *Pro třídy rozkladu grupy $G$ podle podgrupy $H$ platí:*

*(1) Levé a pravé třídy rozkladu podle podgrupy $H \subseteq G$ splývají, právě když pro každé $a \in G$, $h \in H$ platí*

$$a \cdot h \cdot a^{-1} \in H.$$

*(2) Všechny třídy (levé i pravé) mají shodnou mohutnost s podgrupou $H$.*

Důkaz. Obě vlastnosti vyplývají bezprostředně z definičních vlastností. V prvém případě chceme, aby pro jakékoliv $a \in G$, $h \in H$ platilo $h \cdot a = a \cdot h'$ pro vhodné $h' \in H$. To ale nastane právě tehdy, když $a^{-1} \cdot h \cdot a = h' \in H$.

Ve druhém případě si stačí uvědomit, že pokud $a \cdot h = a \cdot h'$, pak také vynásobením $a^{-1}$ zleva obdržíme $h = h'$. □

Jako okamžitý důsledek předchozího jednoduchého tvrzení dostáváme:

**11.10. Věta.** *Nechť $G$ je konečná grupa s $n$ prvky, $H$ její podgrupa. Potom*

*(1) mohutnost $n = |G|$ je součinem mohutnosti $H$ a mohutnosti $G/H$, tj.*

$$|G| = |G/H| \cdot |H|,$$

*(2) přirozené číslo $|H|$ je dělitelem čísla $n$,*
*(3) je-li $a \in G$ prvek řádu $k$, pak $k$ dělí $n$,*
*(4) pro každé $a \in G$ je $a^n = e$,*
*(5) je-li mohutnost grupy $G$ prvočíslo, pak je $G$ izomorfní cyklické grupě $\mathbb{Z}_n$.*

Druhému tvrzení se říkává *Lagrangeova věta*, předposlednímu *malá Fermatova věta*.

Důkaz. Viděli jsme, že každá třída levého rozkladu má právě $|H|$ prvků. Přitom dvě různé třídy rozkladu musí mít nutně prázdný průnik. Odtud vyplývá první tvrzení.

Druhé tvrzení je okamžitým důsledkem prvního.

Každý prvek $a \in G$ generuje cyklickou podgrupu $\{a, a^2, \ldots, a^k = e\}$ a právě počet prvků této podgrupy je řádem prvku $a$. Proto musí řád dělit počet prvků v $G$.

Jelikož je řád $k$ prvku $a$ dělitelem čísla $n$ a $a^k = e$, je také $a^n = (a^k)^s = e$ pro nějaké $s$.

Jestliže je $n > 1$, pak existuje prvek $a \in G$ různý od jednotky $e$. Jeho řád je přirozené číslo $k$ různé od jedničky a nutně dělí $n$. Proto musí být $k$ rovno $n$. Pak ovšem jsou všechny prvky $G$ tvaru $a^k$ pro $k = 1, \ldots, n$. □

S Lagrangeovou i malou Fermatovou větou se čtenář již mohl potkat v desáté kapitole, kde byly speciální případy dokázány pro speciální případy v jiném kontextu.

**11.37.** Popište grupu symetrií tetraedru (pravidelného čtyřstěnu) a nalezněte všechny její podgrupy.

**Řešení.** Označme vrcholy tetraedru $a$, $b$, $c$, $d$. Každou symetrii lze popsat permutací vrcholů (který vrchol přejde na který). Je tedy grupa symetrií tetraedru izomorfní jisté podgrupě grupy $\mathbb{S}_4$. Pro libovolnou dvojici vrcholů tetraedru existuje vhodná symetrie, která vymění právě tuto dvojici (je to zrcadlení podle roviny kolmé na hranu určenou těmito vrcholy, která prochází středem této hrany). Hledaná podgrupa je tedy generovaná všemi transpozicemi v grupě $\mathbb{S}_4$. To je však grupa $\mathbb{S}_4$ samotná.

Popišme tedy všechny podgrupy grupy $\mathbb{S}_4$. Tato grupa má 24 prvků, do úvahy tedy přicházejí podgrupy o počtu prvků 1, 2, 3, 4, 6, 8, 12, 24. (viz 11.10). Rozebereme postupně všechny netriviální možnosti počtu prvků podgrupy $H \subseteq \mathbb{S}_4$.

(i) $|H| = 2$. $H$ musí sestávat z neutrálního prvku a nějakého samoinverzního prvku ($a^2 = \mathrm{id}$). Samoinverzní prvky jsou transpozice nebo složení dvou disjunktních transpozic (geometricky toto zobrazení odpovídá otáčení o 180° okolo osy procházející středy protilehlých hran tetraedru). Dostáváme tak devět podgrup: $\{\mathrm{id}, (a,b)\}$, $\{\mathrm{id}, (a,c)\}$, $\{\mathrm{id}, (a,d)\}$, $\{\mathrm{id}, (b,c)\}$, $\{\mathrm{id}, (b,d)\}$, $\{\mathrm{id}, (c,d)\}$, $\{\mathrm{id}, (a,b)\circ(c,d)\}$, $\{\mathrm{id}, (a,c)\circ(b,d)\}$, $\{\mathrm{id}, (a,d)\circ(b,c)\}$.

(ii) $|H| = 3$. Taková podgrupa musí být podle Lagrangeovy věty nutně cyklická, musí tedy jít o grupu tvaru $\{\mathrm{id}, p, p^2\}$, $p^3 = \mathrm{id}$. Rozklad $p$ na nezávislé cykly tedy nutně obsahuje pouze cyklus délky tři, je tedy $p$ právě tento cyklus. Cyklů délky tři je podle ‖11.25‖ $4 \cdot 2$ a ty vytvoří společně s identitou čtyři podgrupy: $\{\mathrm{id}, (a,b,c), (a,c,b)\}$, $\{\mathrm{id}, (a,c,d), (a,d,c)\}$, $\{\mathrm{id}, (a,b,d), (a,d,b)\}$, $\{\mathrm{id}, (b,c,d), (b,d,c)\}$. Dodejme, že cyklus délky tři geometricky odpovídá rotaci o 120° okolo osy procházející jedním z vrcholů a středem (těžištěm) protější stěny.

(iii) $|H| = 4$. V úvahu připadá pouze cyklická grupa izomorfní $\mathbb{Z}_4$ nebo grupa izomorfní $\mathbb{Z}_2 \times \mathbb{Z}_2$. Uvážíme-li rozklad permutace na nezávislé cykly, tak zjišťujeme, že jedinou permutací na čtyřech prvcích, která má řád 4, je cyklus na čtyřech prvcích. Cyklické grupy musí tedy obsahovat cyklus délky čtyři. A to právě dva, neboť je-li $p$ prvek řádu 4, pak i $p^{-1} = p^3$ je prvek řádu 4, tedy cyklus délky 4. Permutace $p^2$ je pak prvek řádu 2, a musí to být složení dvou nezávislých transpozic ($p^2$ nemá pevných bodů). Cyklů délky 4 je šest (viz ‖11.25‖). Vždy dva spadnou do jedné podgrupy, dostáváme tedy tři čtyřprvkové podgrupy tohoto typu:

$$\{\mathrm{id}, (a,b,c,d), (a,c)\circ(b,d), (a,d,c,b)\},$$

**11.11. Normální podgrupy a faktorgrupy.** Podgrupy $H$, pro které platí, že $a \cdot h \cdot a^{-1} \in H$ pro všechny $a \in G$, $h \in H$, se nazývají *normální podgrupy*.



Pro normální podgrupy je dobře definováno násobení na $G/H$ vztahem

$$(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H.$$

Skutečně volbou jiných reprezentantů $a \cdot h$, $b \cdot h'$ dostaneme opět stejný výsledek

$$(a \cdot h \cdot b \cdot h') \cdot H = ((a \cdot b) \cdot (b^{-1} \cdot h \cdot b) \cdot h') \cdot H = (a \cdot b) \cdot H.$$

Totéž si můžeme odůvodnit tak, že nezáleží na tom, jestli pracujeme s pravými nebo levými třídami. Můžeme proto rovnou naše třídy psát jako $H \cdot a \cdot H$ a potom snadno definujeme $(H \cdot a) \cdot (b \cdot H) = H \cdot (a \cdot b) \cdot H$.

Zřejmě jsou splněny pro nové násobení na $G/H$ všechny vlastnosti grupy: jednotkou je sama grupa $H$ jakožto třída $e \cdot H$ jednotky, inverzí k $a \cdot H$ je zřejmě $a^{-1} \cdot H$ a asociativita násobení je zřejmá z definice. Hovoříme o *faktorové grupě* $G/H$ grupy $G$ podle normální podgrupy $H$.

V komutativních grupách jsou samozřejmě všechny podgrupy normální. Podmnožina

$$n\mathbb{Z} = \{na;\ a \in \mathbb{Z}\} \subseteq \mathbb{Z}$$

zadává v celých číslech podgrupu a její faktorgrupou je právě (aditivní) grupa zbytkových tříd $\mathbb{Z}_n$.

Z definice je zřejmé, že všechna jádra homomorfismů jsou normální podgrupy. Naopak jestliže je podgrupa $H \subseteq G$ normální, pak zobrazení

$$p : G \to G/H, \quad a \mapsto a \cdot H$$

je surjektivní homomorfismus grup s jádrem $H$. Skutečně $p$ je dobře definované. Přímo z definice násobení na $G/H$ je vidět, že $p$ je homomorfismus a $p$ je zjevně surjektivní. Je tedy vidět, že normální podgrupy jsou právě všechna jádra homomorfismů.

Dále pro libovolný homomorfismus grup $f : G \to K$ s jádrem $H = \ker f$ je dobře definován také homomorfismus

$$\tilde{f} : G/\ker f \to K,\ \tilde{f}(a \cdot H) = f(a),$$

který je injektivní.

Zdánlivě paradoxní je příklad homomorfismu grup $\mathbb{C}^* \to \mathbb{C}^*$, který je definovaný na nenulových komplexních číslech vztahem $z \mapsto z^k$ s přirozeným $k$. Zjevně jde o surjektivní homomorfismus a jeho jádro je množina $k$-tých odmocnin z jedničky, tj. cyklická podgrupa $\mathbb{Z}_k$. Předchozí úvaha tedy dává pro všechna přirozená $k$ izomorfismus

$$\tilde{f} : \mathbb{C}^*/\mathbb{Z}_k \to \mathbb{C}^*.$$

Tento příklad ukazuje, že u nekonečných grup nejsou počty s mohutnostmi tak přehledné, jako tomu bylo u konečných grup ve Větě 11.10.

**11.12. Exaktní posloupnosti.** Kdykoliv zvolíme normální podgrupu $H$ v grupě $G$, dostáváme tzv. *krátkou exaktní posloupnost grup*

$$e \to H \to G \to G/H \to e,$$

kde šipky postupně znázorňují jediný homomorfismus triviální grupy $\{e\}$ do grupy $H$, vložení $\iota$ podgrupy $H \subseteq G$, projekci $\nu$ na faktorgrupu $G/H$ a konečně jediný homomorfismus grupy $G/H$

$\{\mathrm{id}, (a,c,b,d), (a,b)\circ(b,d), (a,d,b,c)\}$,

$\{\mathrm{id}, (a,b,d,c), (a,d)\circ(bc), (a,c,d,b)\}$.

Co se týče podgrup izomorfních $\mathbb{Z}_2\times\mathbb{Z}_2$, tak prvky řádu dva jsou v $\mathbb{S}_4$ dvojího typu: buď transpozice, nebo složení dvou nezávislých (disjunktních) transpozic. V podgrupě nemohou být dvě závislé transpozice: složením dvou závislých transpozic dostaneme cyklus délky tři, tedy prvek řádu tři. Pouze jedna transpozice nemůže být v podgrupě taktéž (diskusi přenecháváme čtenáři). Tudíž transpozice mohou být v podgrupě buď dvě nezávislé nebo žádná. Dostáváme tak tři podgrupy složené mimo indentity ze dvou disjunktních transpozic a permutace dané jejich složením. Snadno ověříme, že též tři permutace, které jsou složením nezávislých transpozic, také tvoří společně s identitou grupu. Celkem dostáváme: $\{\mathrm{id}, (a,b), (a,b)\circ(c,d), (c,d)\}$, $\{\mathrm{id}, (a,c), (a,c)\circ(b,d), (b,d)\}$, $\{\mathrm{id}, (a,d), (a,d)\circ(b,c), (b,c)\}$ a $\{\mathrm{id}, (a,b)\circ(c,d), (a,c)\circ(b,d), (a,d)\circ(b,c)\}$.

(iv) $|H|=6$. Podle příkladu ‖11.19‖ a tomu, že řád libovolné permutace na čtyřech prvcích je maximálně 4, se jedná o podrupu izomorfní grupě $\mathbb{S}_3$ permutací tří prvků. Dostáváme tak čtyři podgrupy.

(v) $|H|=8$. Grupa nemůže být podgrupu grupy sudých permutací (těch je 12 a osm nedělí 12. Tedy podle ‖11.36‖, musí obsahovat čtyři sudé a čtyři liché permutace. Sudé permutace musí tvořit podgrupu grupy sudých permutací, tedy i podgrupu $\mathbb{S}_{12}$ a v bodě (iii) jsme viděli, že jedinou čtyřprvkovou podgrupou pouze sudých permutací je podgrupa $\{\mathrm{id}, (a,b)\circ(c,d), (a,c)\circ(b,d), (a,d)\circ(b,c)\}$, která je normální. Pokud pro libovolnou lichou permutaci uvážíme třídu rozkladu odpovídající této permutaci v rozkladu podle zmíněné normální podgrupě, tak tato třída má čtyři prvky a společně s uvedenou normální podgrupou tvoří podgrupu $\mathbb{S}_4$. Dostáváme tak tři podgrupy $\mathbb{S}_4$. Není těžké si rozmyslet, že každá z nich je izomorfní grupě symetrií čtverce (tzv. dihedrální grupě $D_4$). Geometricky si ji popíšeme následovně. Uvážíme kolmý průmět čtyřstěnu do rovniny kolmé na přímku procházející středy protějších hran. Hranice průmětu je čtverec. Ze symetrií čtyřstěnu vezmeme pouze ty, které indukují skutečnou symetrii tohoto čtverce (například symetrie zaměňující pouze dva v průmětu sousední vrcholy čtyřstěnu, tedy transpozice, to nebude). Dvojice protějších hran jsou v tetraedru tři, dostáváme tedy tři různé osmiprvkové podgrupy isomorfní dihedrální grupě $D_4$. (vi) $|H|=12$. Taková podgrupa musí obsahovat podle ‖11.36‖ buď pouze sudé permutace, nebo šest lichých a šest sudých permutací (ty pak musí tvořit podgrupu $\mathbb{S}_4$. V bodě (iv) jsme ovšem viděli, že šestiprvková podgrupa $\mathbb{S}_4$ složená pouze ze sudých permutací neexistuje. Jedinou podgrupou o tomto počtu prvků je tak alternující grupa $\mathbb{A}_4$ všech sudých permutací v $\mathbb{S}_4$. Geometricky na triviální grupu $\{e\}$. Ve všech případech je vidět, že obraz předcházející šipky je přesně jádrem následující. To je definice *exaktnosti* posloupnosti homomorfismů.

Jestliže existuje homomorfismus $\sigma : G/H \to G$ takový, že $\nu\circ\sigma = \mathrm{id}_{G/H}$, říkáme, že se naše exaktní posloupnost *štěpí*.

**Lemma.** *Každá rozštěpená krátká exaktní posloupnost komutativních grup zadává izomorfismus* $G = H\times G/H$.

Důkaz. Definujeme zobrazení $f : H\times G/H\to G$ vztahem

$$f(a,b) = a\cdot\sigma(b).$$

Protože pracujeme s komutativními grupami, jde zjevně o homomorfismus

$$f\left(aa', bb'\right) = aa'\sigma(b)\sigma(b') = (a\sigma(b))\left(a'\sigma\left(b'\right)\right).$$

Jestliže $f(a,b)=e$, pak $\sigma(b)=a^{-1}\in H$, tj. $b=\nu(\sigma(b))$ je tedy jednotkový prvek v $G/H$. Pak ovšem jeho obraz musí být $\sigma(b)=e$ a je proto i $a=e$. Protože jsou levé a pravé třídy rozkladu u komutativních grup totožné, je zobrazení $f$ zjevně surjektivní. Dokázali jsme tedy, že je $f$ izomorfismus. □



Můžeme nyní naznačit hlavní ideu důkazu Věty 11.8. Kdybychom totiž věděli, že se všechny krátké exaktní posloupnosti vzniklé volbou cyklických podgrup $H$ v konečných komutativních grupách $G$ štěpí, pak bychom snadno důkaz vedli indukcí. V grupě $G$ o mohutnosti $n$, která není cyklická, bychom totiž zvolili prvek s řádem $p<n$ a našli jím generovanou cyklickou podgrupu $H$ a štěpení příslušné krátké exaktní posloupnosti. Tím bychom dostali grupu $G$ vyjádřenou jako součin zvolené cyklické podgrupy $H$ a grupy $G/H$ s mohutností $n/p$.

Hlavním technickým bodem důkazu je tedy ověření, že v každé konečné komutativní grupě najdeme prvky řádu $p^r$ s patřičnými mocninami prvočíselných $p$ a že se skutečně výše uvedené krátké exaktní posloupnosti pro tyto grupy štěpí.

**11.13. Akce grupy.** Již jsme viděli, že často potkáváme grupy jako množiny transformací nějaké pevné množiny. Musí přitom být všechny invertibilní a zároveň musí být naše množina transformací uzavřená na skládání. Často ale také chceme pracovat s pevně zvolenou grupou, jejíž prvky reprezentujeme jako zobrazení na nějaké množině, přitom ale ne nutně jsou zobrazení příslušná různým prvkům grupy různá. Např. všechna otočení roviny kolem počátku o všechny možné úhly odpovídají grupě reálných čísel. Otočení o $2\pi$ je ale identické zobrazení.



Formálně si můžeme takovou situaci popsat následovně.

Akce grupy

Levá *akce grupy $G$ na množině $S$* je homomorfismus grupy $G$ do podgrupy invertibilních prvků v pologrupě $S^S$ všech zobrazení $S\to S$. Takový homomorfismus si také můžeme představit jako zobrazení $\varphi : G\times S\to S$, které splňuje

$$\varphi(a\cdot b, x) = \varphi(a,\varphi(b,x)),$$

odtud název „levá akce“. Často budeme k vyjádření akce prvku grupy na prvku $S$ používat pouze zápis $a\cdot x$ (byť jde o jinou tečku než u násobení uvnitř grup). Definiční vlastnost pak vypadá takto:

$$(a\cdot b)\cdot x = a\cdot(b\cdot x).$$

se jedná o přímé symetrie, tedy ty, které můžeme dosáhnout pouze rotacemi čtyřstěnu (tedy nikoliv zrcadleními). □

**Poznámka.** Obecně je grupa symetrií nějakého tělesa o $n$ vrcholech podgrupou grupy $\mathbb{S}_n$ permutací $n$ prvků.

**11.38.** Které z podgrup grupy $\mathbb{S}_4$ jsou normální?

**Řešení.** Aby byla podgrupa $H \subseteq \mathbb{S}_4$ normální, musí být $gHg^{-1} \subseteq H$ pro libovolné $g \in \mathbb{S}_4$. Vzhledem k tomu, že každou permutaci lze napsat jako složení transpozic a inverzi pak můžeme získat pouze zapsáním permutací z rozkladu v opačném pořadí, stačí danou vlastnost ověřit pouze pro transpozice $g$. Toto ověření necháváme na čtenáři. Zjišťujeme tak, že jedinými normálními podgrupami jsou: triviální grupa, celá grupa $\mathbb{S}_4$, alternující grupa, tj. grupa všech sudých permutací v $\mathbb{S}_4$ a čtyřprvková podgrupa s prvky řádu dva, tzv. Kleinova grupa, se kterou jsme se setkali již v ‖11.16‖. □

**11.39.** Určete grupu symetrií krychle (popište všechny symetrie). Je tato grupa komutativní?

**Řešení.** Grupa má 48 prvků, z nichž 24 je generováno pouze rotacemi, tzv. přímými symetriemi, zbytek tvoří nepřímé symetrie, které vzniknou složením přímých s nějakým zrcadlením. Grupa není komutativní (uvažte například v různém pořadí složení zrcadlení podle roviny dané středy čtyř rovnoběžných hran a rotace o 90° kolem osy ležící v uvedené rovině a procházející středy nějakých dvou protějších stěn. Grupa je izomorfní grupě $\mathbb{S}_4 \times \mathbb{Z}_2$. □

*11.40.* V grupě symetrií krychle určete podgrupu (popište symetrie v podgrupě a uveďte tabulku operace skládání na této podgrupě) generovanou zrcadlením podle roviny procházející středy čtyř rovnoběžných hran a rotací o 180° kolem osy ležící ve zmíněné rovině procházející středy dvou protějších stěn. Je tato podgrupa normální? ○

**11.41.** Rozhodněte, zda jsou podgrupy generované

- cyklem $(1, 2, 3)$ v $\mathbb{S}_3$,
- cyklem $(1, 2, 3, 4)$ v $\mathbb{S}_4$,
- cyklem $(1, 2, 3)$ v $\mathbb{A}_4$

normální. V posledním případě určete pravé třídy rozkladu $\mathbb{A}_4$ podle uvažované podgrupy. Určete, kdy je podmnožina všech cyklů délky $n$ podgrupou grupy $\mathbb{S}_n$ (pro $n \geq 3$. Ukažte, že se pak jedná o normální podgrupu.

**Řešení.**

- Jde o normální podgrupu $A_3$.

Obraz prvku $x \in S$ v akci celé grupy $G$ nazýváme *orbita* $S_x$ prvku $x$, tj.

$$S_x = \{y = \varphi(a, x);\ a \in G\}.$$

Pro každý bod $x \in S$ definujeme *izotropní podgrupu* $G_x \subseteq G$ akce $\varphi$:

$$G_x = \{a \in G;\ \varphi(a, x) = x\}.$$

Jestliže pro každé dva prvky $x, y \in S$ existuje $a \in G$ tak, že $\varphi(a, x) = y$, pak říkáme, že akce $\varphi$ je *tranzitivní*.

Jestliže zvolíme dva body $x, y \in S$ a prvek $g \in G$ zobrazující $x$ na $y = g \cdot x$, pak je zjevně množina $\{ghg^{-1};\ h \in G_x\}$ izotropní podgrupou $G_y$. Zobrazení $h \mapsto ghg^{-1}$ je přitom homomorfismem grup $G_x \to G_y$.

Snadno se vidí, že u tranzitivních akcí je celý prostor jedinou orbitou a všechny izotropní podgrupy mají stejnou mohutnost.

Jako příklad tranzitivní akce konečné grupy můžeme uvést např. zjevnou akci grupy permutací pevně zvolené množiny $X$ na samotné množině $X$. Přirozená akce všech invertibilních lineárních transformací na nenulových prvcích vektorového prostoru $V$ je také tranzitivní. Pokud vezmeme ale prostor $V$ celý, je nulový vektor zvláštní orbitou.

Výše uváděný příklad akce aditivní grupy reálných čísel prostřednictvím rotací kolem pevného středu $O$ v rovině není tranzitivní. Orbity jednotlivých bodů jsou právě kružnice se středem $O$ procházející těmito body.

Typický příklad tranzitivní akce grupy $G$ je přirozená akce na množině levých tříd $G/H$ pro jakoukoliv podgrupu $H$. Definujeme ji vztahem

$$g \cdot (aH) = (ga)H.$$

Snadno ukážeme, že takto v podstatě vypadají všechny tranzitivní akce grup. Pro libovolnou tranzitivní akci $G \times S \to S$ a pevně zvolený bod $x \in G$ můžeme totiž ztotožnit $S$ s množinou levých tříd $G/G_x$ pomocí vztahu $gG_x \mapsto g \cdot x$. Toto zobrazení je zjevně surjektivní a obrazy $g \cdot x = h \cdot x$ splývají, právě když $h^{-1}g \in G_x$ a to je ekvivalentní s $gG_x = hG_x$. Konečně si všimněme, že toto ztotožnění převádí původní akci $G$ na $S$ právě na výše uvedenou akci $G$ na $G/G_x$.

**11.14. Věta.** *Pro každou akci konečné grupy $G$ na konečné množině $S$ platí:*

*(1) pro každý prvek $x \in S$ je*

$$|G| = |G_x| \cdot |S_x|,$$

*(2) (Burnsideovo lemma) je-li $N$ počet orbit akce $G$ na $S$, pak*

$$|G| = \frac{1}{N} \sum_{g \in G} |S_g|,$$

*kde $S_g = \{x \in S;\ g \cdot x = x\}$ označuje množinu pevných bodů akce prvku $g$.*

Důkaz. Uvažme libovolný bod $x \in S$ a izotropní podgrupu $G_x \subseteq G$ tohoto bodu. Stejný argument jako na konci minulého odstavce u tranzitivních grup můžeme uplatnit na každou akci grupy $G$. Dostáváme zobrazení $G/G_x \to S_x$, $g \cdot G_x \mapsto g \cdot x$. Pokud $(g \cdot S_x) \cdot x = (h \cdot S_x) \cdot x$, pak zjevně $g^{-1}h \in S_x$, je tedy naše zobrazeni injektivní. Zároveň je zjevně surjektivní, proto pro mohutnosti našich konečných množin platí $|G/G_x| = |S_x|$. Odtud již vyplývá první vlastnost z věty, protože $|G| = |G/G_x| \cdot |G_x|$.

- Není to normální podgrupa ( $(1,2)\circ(1,3)\circ(2,4)\circ(1,2) = (4,1)\circ(2,3)$ ).
- Podgrupa není normální. Pravé třídy rozkladu jsou pak

$$\{(1,2,4),(2,4,3),(1,3)\circ(2,4)\},$$
$$\{(1,4,2),(1,4,3),(1,4)\circ(2,3)\},$$
$$\{(2,3,4),(1,2)\circ(3,4),(1,3,4)\},$$
$$\{\mathrm{Id},(1,2,3),(1,3,2)\}.$$

Podmnožina je podgrupou pouze pro $n = 3$. Potom jde o podgrupu $A_3$ sudých permutací v $\mathbb{S}_3$, jedná se tedy o normální podgrupu. (Pro jiná $n$ snadno najdeme dva cykly délky $n$, jejichž složením není cyklus délky $n$). □

**11.42.** Určete podgrupu v $\mathbb{S}_6$ generovanou permutacemi $(1,2)\circ(3,4)\circ(5,6)$, $(1,2,3,4)$ a $(5,6)$. Je tato podgrupa normální? Pokud ano, popište třídy rozkladu $S_6/H$.

**Řešení.** Nejprve si všimněme, že všechny zadané permutace leží v podgrupě $\mathbb{S}_4 \times S_2 \subseteq S_6$ (uvažujeme přirozenou inkluzi $\mathbb{S}_4 \times \mathbb{S}_2$ tedy pro $s \in \mathbb{S}_4 \times \mathbb{S}_2$ je zúžení $s$ na množinu $\{1,2,3,4\}$ permutací na této množině a zúžení na množinu $\{5,6\}$ rovněž permutací na této množině). Proto i jimi generovaná podgrupa bude ležet v této podgrupě. Dále je zřejmě (protože mezi generátory je transpozice $(5,6)$) hledaná podgrupa tvaru $H \times \mathbb{S}_2$, kde $H \subseteq \mathbb{S}_4$. Stačí tedy popsat $H$. Tato grupa je generována prvky $(1,2)\circ(3,4)$ a $(1,2,3,4)$ (projekce generátorů na $\mathbb{S}_4$). Máme

$$(1,2,3,4)^2 = (1,3)\circ(2,4),$$
$$(1,2,3,4)^3 = (4,3,2,1),$$
$$(1,2,3,4)^4 = \mathrm{id},$$
$$[(1,2)\circ(3,4)]^2 = \mathrm{id},$$
$$[(1,2)\circ(3,4)]\circ(1,2,3,4) = (2,4),$$
$$(1,2,3,4)\circ[(1,2)\circ(3,4)] = (1,3),$$
$$[(1,2)\circ(3,4)]\circ(4,3,2,1) = (1,3),$$
$$(4,3,2,1)\circ[(1,2)\circ(3,4)] = (2,4),$$
$$[(1,2)\circ(3,4)]\circ[(1,3)\circ(2,4)] = (1,4)\circ(2,3),$$
$$[(1,3)\circ(2,4)]\circ[(1,2)\circ(3,4)] = (1,4)\circ(2,3),$$
$$[(1,2)\circ(3,4)]\circ(4,2) = (1,2,3,4),$$
$$(1,3)\circ(4,2) = (1,3)\circ(2,4).$$

V tomto okamžiku si všimněme, že generující permutace $(1,2,3,4)$ i $(1,2)\circ(3,4)$ jsou obě symetriemi čtverce o vrholech $1,2,3,4$, tedy nemohou vygenerovat více, než grupu symetrií čtverce, totiž dihedrální

Druhé tvrzení dokážeme tak, že dvěma způsoby spočteme mohutnost množiny pevných bodů akce:

$$F = \{(x,g) \in S \times G;\ g(x) = x\} \subseteq S \times G.$$

Protože jde o konečné množiny, můžeme si představit prvky součinu $S \times G$ jako prvky v matici (sloupce označujeme prvky v $S$, řádky pak podle prvků v $G$). Sčítáním po řádcích i sloupcích obdržíme

$$|F| = \sum_{g\in G} |S_g| = \sum_{x\in S} |G_x|.$$

Nyní si pro přehlednost vyberme po jednom reprezentantu $x_1,\dots,x_N$ z každé orbity v $S$ a připomeňme, že mohutnosti izotropních grup pro body ve stejné orbitě jsou stejné. Využitím již dokázaného tvrzení (1) nyní vcelku snadno dostáváme

$$|F| = \sum_{g\in G} |S_g| = \sum_{i=1}^{N} \sum_{x\in S_{x_i}} |G_x| = \sum_{i=1}^{N} |S_{x_i}||G_{x_i}| = N\cdot|G|$$

a důkaz je ukončen. □

Doporučujeme si pečlivě promyslet, jak užitečná jsou tvrzení věty pro řešení kombinatorických úloh, viz příklady v části B vedlejšího sloupce.

## 2. Okruhy polynomů



Grupové operace byly podstatné u skalárů i vektorů. Vystupovalo nám tam ovšem několik obdobných struktur zároveň. Zaměříme se teď právě na takové případy. Budeme přitom mít na mysli zejména obvyklé skaláry, tj. celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, komplexní čísla $\mathbb{C}$ a množiny polynomů nad takovými skaláry $\mathbb{K}$. Budeme přitom ale pečlivě budovat abstraktní algebraickou teorii.

**11.15. Okruhy a tělesa.** Celá čísla mají následující vlastnosti tzv. okruhu:

### Okruhy a obory integrity

**Definice.** Komutativní grupa $(M,+)$ s neutrálním prvkem $0 \in M$ spolu s další operací $\cdot$ splňující

- $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ pro všechna $a,b,c \in M$;
- $a\cdot b = b\cdot a$ pro všechna $a,b \in M$;
- existuje prvek 1 takový, že pro všechna $a \in M$ platí $1\cdot a = a$;
- $a\cdot(b+c) = a\cdot b + a\cdot c$ pro všechna $a,b,c \in M$

se nazývá *komutativní okruh.*

Jestliže v okruhu $\mathbb{K}$ platí $c\cdot d = 0$, práv, když alespoň jeden z prvků $c$ a $d$ je nulový, pak nazýváme okruh $\mathbb{K}$ *oborem integrity*.

Poslední vlastnosti v našem výčtu axiomů okruhu se říká *distributivita* sčítání vůči násobení. Pokud neplatí vlastnost komutativity operace $\cdot$, hovoříme o *nekomutativním okruhu*. V dalším se ovšem omezíme zpravidla na okruhy komutativní. Operaci $+$ budeme říkat sčítání a operaci $\cdot$ násobení, aniž by to znamenalo, že jde skutečně o tyto operace na některém z našich číselných oborů. Navíc budeme vždy předpokládat existenci jedničky 1 pro operaci násobení. Neutrálnímu prvku pro sčítání říkáme nula.

grupu $D_4$, o osmi prvcích, což už se stalo. Dalším skládáním tedy již nemůžeme dostat žádné další permutace. Podgrupa $H \subseteq \mathbb{S}_4$ má tedy osm prvků (osm je dělitel čísla 24, tedy podle Lagrangeovy věty je to skutečně možný počet prvků podgrupy).

$$H = \{\mathrm{id}, (1,2,3,4), (1,3)\circ(2,4), (4,3,2,1), (1,2)\circ(3,4),$$
$$(1,3), (2,4), (1,4)\circ(2,3)\}.$$

Všech prvků hledané podgrupy v $\mathbb{S}_6$ je tedy 16: pro každý prvek $h \in H$ jsou v ní prvky $(h, \mathrm{id})$ a $(h, (56))$. □

**11.43.** Určete podgrupu v $\mathbb{S}_4$ generovanou permutacemi $(1,2)\circ(3,4)$, $(1,2,3)$.

**Řešení.** Oba zadané generátory jsou sudé permutace, jejich libovolným složením tedy vznikne opět pouze sudá permutace. Hledaná podgrupa tedy bude i podgrupou grupy $A_4$ všech sudých permutací. Máme

$$[(1,2)\circ(3,4)]^2 = \mathrm{id},$$
$$(1,2,3)^2 = (3,2,1),$$
$$[(1,2)\circ(3,4)]\circ(1,2,3) = (2,4,3),$$
$$(1,2,3)\circ[(1,2)\circ(3,4)] = (1,3,4),$$
$$[(1,2)\circ(3,4)]\circ(3,2,1) = (3,1,4),$$
$$(3,2,1)\circ[(1,2)\circ(3,4)] = (2,3,4)$$

a v tomto okamžiku máme již sedm prvků hledané podgrupy $A_4$, protože $A_4$ má dvanáct prvků a počet prvků podgrupy musí být dělitelem čísla dvanáct, musí být hledanou podgrupou celá grupa $A_4$. □

**11.44.** Najděte všechny podgrupy grupy invertibilních čtvercových matic $2\times 2$ nad $\mathbb{Z}_2$ (operací je násobení matic). Je některá z nich normální?

**Řešení.** V příkladě ‖11.1‖ jsme sestavili tabulku operace ve zkoumané grupě. Dle Lagrangeovy věty (11.10) je možný počet prvků v podgrupě dělitelem čísla šest. Kromě triviálních podgrup (podgrupa složená pouze z jednotkového prvku a celá grupa) přicházejí tedy do úvahy podgrupy o dvou či třech prvcích. Dvouprvkové grupy musejí mít tu vlastnost, že prvek, který není jednotka musí být inverzní sám sobě. Tato vlastnost je i postačující. Dostáváme tak podgrupy $\{A, B\}$, $\{A, C\}$, $\{A, F\}$, které nejsou normální, jak lehce ověříme. Jednotkovým prvkem těchto grup je matice $A$. Dále díky jejich samoinverznosti je součinem libovolné z matic $B, C, F$ s nějakou další (nejednotkovou) maticí nejednotková matice třetí. Tedy žádná z těcho matic nemůže být prvkem trojprvkové podgrupy. Zbývá možnost $P = \{A, D, E\}$, což vskutku podgrupa je. Navíc výpočtem konjugací $BDB = E$,

### Tělesa

Netriviální (komutativní) okruh, ve kterém jsou všechny nenulové prvky invertibilní, se nazývá (komutativní) *těleso*. Komutativní těleso se také nazývá *pole*.

Typickým příkladem komutativních těles, tj. polí, jsou číselné obory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dále pak všechny okruhy zbytkových tříd $\mathbb{Z}_p$ s prvočíselným $p$. Dobrým příkladem nekomutativního okruhu s jedničkou je množina $\mathrm{Mat}_k(\mathbb{K})$ všech čtvercových matic nad okruhem $\mathbb{K}$ s $k$ řádky a sloupci. Jak jsme viděli dávno, není to ani obor integrity. Jako příklad nekomutativního tělesa uveďme těleso kvaternionů $\mathbb{H}$, které vznikne opětovným rozšířením komplexních čísel o druhou imaginární jednotku $j$, tj. $\mathbb{H} = \mathbb{C}\oplus j\mathbb{C} \simeq \mathbb{R}^4$, stejně jako jsme dostali komplexní čísla z reálných. Navíc označíme další „nový“ prvek $k = ij$, který je součinem imaginárních jednotek $i$ a $j$. Z konstrukce už vyplyne, že $ij = -ji$. Přitom ale ostatní vlastnosti tělesa zůstávají zachovány. Zkuste si promyslet nebo dohledat podrobnosti jako ne úplně triviální cvičení!

**Lemma.** *V každém komutativním okruhu $\mathbb{K}$ s jedničkou platí následující vztahy (které nám jistě připadají samozřejmé u skalárů):*

*(1)* $0\cdot c = c\cdot 0 = 0$ *pro všechna* $c \in \mathbb{K}$,
*(2)* $-c = (-1)\cdot c = c\cdot(-1)$ *pro všechna* $c \in \mathbb{K}$,
*(3)* $-(c\cdot d) = (-c)\cdot d = c\cdot(-d)$ *pro všechna* $c, d \in \mathbb{K}$,
*(4)* $a\cdot(b-c) = a\cdot b - a\cdot c$,
*(5) celý okruh* $\mathbb{K}$ *je triviální množinou* $\{0\} = \{1\}$, *právě když* $0 = 1$.

Důkaz. Všechna tvrzení vyplývají z jednoduché úvahy a definičních axiomů. V prvém případě počítáme pro jakákoliv $c, a$:

$$c\cdot a = c\cdot(a+0) = c\cdot a + c\cdot 0,$$

a protože jediným neutrálním prvkem vůči sčítání je nula, dostáváme $a\cdot 0 = 0$. Stejně se dokáže i $0\cdot a = 0$.

Ve druhém případě teď stačí spočíst

$$0 = c\cdot 0 = c\cdot(1+(-1)) = c + c\cdot(-1),$$

proto je $c\cdot(-1)$ opačný prvek k prvku $c$, což jsme chtěli dokázat.

Další dvě tvrzení jsou už přímým důsledkem druhého vztahu a základních axiomů. Jestliže je celý okruh tvořen jediným prvkem, je pochopitelně $0 = 1$. Naopak jestliže platí $1 = 0$, pak pro jakékoliv $c \in \mathbb{K}$ je $c = 1\cdot c = 0\cdot c = 0$. □

**11.16. Polynomy nad okruhy.** Definice komutativního okruhu s jedničkou abstrahuje právě vlastnosti potřebné k násobení a sčítání. Můžeme je hned využít pro práci s tzv. polynomy. Rozumíme jimi jakýkoliv konečný výraz, který lze poskládat ze známých konstantních prvků $\mathbb{K}$ a jedné neznámé proměnné pomocí operací sčítání a násobení. Formálně můžeme definovat polynomy takto:[3]



### Polynomy

**Definice.** Nechť $\mathbb{K}$ je jakýkoliv komutativní okruh skalárů s jedničkou. Polynomem nad $\mathbb{K}$ rozumíme konečný výraz

$$f(x) = \sum_{i=0}^{k} a_i x^i,$$

[3] Ne náhodou je pro okruh použit symbol $\mathbb{K}$ – nadále si pod ním představujte třeba kterýkoliv okruh našich číselných oborů.

$CDC = E$, $FDF = E$ (z čehož vyplývá $BEB = D$, $CEC = D$, $FEF = D$) zjišťujeme, že daná podgrupa je normální. □

**11.45.** Popište všechny podgrupy grupy $(\mathbb{Z}_{10}, +)$.

**Řešení.** Podgrupy jsou izomorfní $(\mathbb{Z}_d, +)$, kde $d|10$, tj. $\{0\} \cong \mathbb{Z}_1$, $\{0, 5\} \cong \mathbb{Z}_2$, $\{0, 2, 4, 6, 8\} \cong \mathbb{Z}_5$, a $\mathbb{Z}_{10}$. □

**11.46.** Určete řády prvků 2, 4, 5 v grupě $(\mathbb{Z}_{35}^\times, \cdot)$ a v grupě $(\mathbb{Z}_{35}, +)$.

**Řešení.** Řád prvku $x$ v grupě $(\mathbb{Z}_{35}^\times, \cdot)$ je nejmenší $k$ takové, že $x^k \equiv 1 \mod 35$. Z Eulerovy věty je pro $x = 2$ a $x = 4$ řád $k \leq \varphi(35) = 24$. Výpočtem příslušných modulárních mocnin zjistíme, že řád $x = 2$ je 12. Odtud přímo plyne, že řád $x = 4$ je 6. Číslo $x = 5$ do grupy $(\mathbb{Z}_{35}^\times, \cdot)$ nepatří. Konkrétně modulo 35 máme

| $x$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ | $x^7$ | $x^8$ | $x^9$ | $x^{10}$ | $x^{11}$ | $x^{12}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 4 | 8 | 16 | 32 | 29 | 23 | 11 | 22 | 9 | 18 | 1 |
| 4 | 16 | 29 | 11 | 9 | 1 | | | | | | |

V grupě $(\mathbb{Z}_{35}, +)$ je řád nejmenší $k$ takové, že $k \cdot x \equiv 0 \mod 35$. Toto lze jednoduše spočítat jako $k = \frac{35}{(35,x)}$. To znamená, že řád prvků 2 a 4 je 35 a řád 5 je 7. □

**11.47.** Popište všechny konečné podgrupy grupy $(\mathbb{R}^*, \cdot)$[1]

**Řešení.** Pokud v podgrupě grupy $(\mathbb{R}^*, \cdot)$ existuje prvek $a$, $|a| \neq 1$, pak tvoří prvky $a, a^2, a^3, \ldots$ nekonečnou geometrickou posloupnost po dvou různých prvků, které všechny musí ležet v uvažované podgrupě. Tato je tedy nekonečná. Konečná podgrupa může tedy obsahovat pouze prvky 1 a $-1$. Dostáváme tak dvě podgrupy: $\{1\}$, $\{-1, 1\}$. □

**11.48.** Rozhodněte, zda předpis $\varphi$ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jeho jádro. Rozhodněte o surjektivitě a injektivitě $\varphi$:

i) $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi([a]_4, [b]_3)) = [a - b]_{12}$,
ii) $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi([a]_4, [b]_3)) = [6a + 4b]_{12}$,
iii) $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi([a]_4, [b]_3)) = [0]_{12}$.

**Řešení.**

i) Není zobrazení. Vezmeme-li dva různé reprezentanty téhož prvku v $\mathbb{Z}_4 \times \mathbb{Z}_3$, totiž $([6]_4, [1]_3) = ([2]_4, [1]_3)$, dostáváme $\varphi([6]_4, [1]_3) = [5]_{12}$ a $\varphi([2]_4, [1]_3) = [1]_{12}$), tudíž zobrazení není korektně definováno.

ii) Je homomorfismus, který není ani injektivní ani surjektivní. Jádrem $\mathrm{Ker}(\varphi)$ je množina $\{([2]_4, [0]_3), ([0]_4, [0]_3)\}$.

iii) Je homomorfismus, který není ani injektivní ani surjektivní. Jádrem je celá grupa $\mathbb{Z}_4 \times \mathbb{Z}_3$.

[1] Grupu invertibilních prvků značíme pro $\mathbb{R}$ a $\mathbb{C}$ jako $\mathbb{R}^*$, $\mathbb{C}^*$, pro $\mathbb{Z}_n$ pak $\mathbb{Z}_n^\times$.

kde $a_i \in \mathbb{K}$, $i = 0, 1, \ldots, k$ jsou tzv. *koeficienty polynomu*. Je-li $a_k \neq 0$, říkáme, že $f(x)$ má *stupeň* $k$, píšeme $\deg f = k$. Nulový polynom nemá stupeň, polynomy stupně nula jsou právě nenulové prvky v $\mathbb{K}$, kterým říkáme konstantní polynomy.

Polynomy $f(x)$ a $g(x)$ jsou stejné, jestliže mají stejné nenulové koeficienty. Množinu všech polynomů nad okruhem $\mathbb{K}$ budeme značit $\mathbb{K}[x]$.

Každý polynom zadává zobrazení $f : \mathbb{K} \to \mathbb{K}$, jehož hodnota vznikne dosazením hodnoty $c$ za nezávislou proměnnou $x$, tj.

$$f(c) = a_0 + a_1 c + \cdots + a_k c^k.$$

Všimněme si, že konstantní polynomy odpovídají právě konstantním zobrazením.

*Kořen polynomu* $f(x)$ je takový prvek $c \in \mathbb{K}$, pro který je $f(c) = 0 \in \mathbb{K}$.

Obecně mohou různé polynomy definovat stejná zobrazení. Např. polynom $x^2 + x \in \mathbb{Z}_2[x]$ zadává identicky nulové zobrazení. Obecněji, pro každý konečný okruh $\mathbb{K} = \{a_0, a_1, \ldots, a_k\}$ zadává polynom $f(x) = (x - a_0)(x - a_1) \ldots (x - a_k)$ identicky nulové zobrazení.

Dva polynomy $f(x) = \sum_i a_i x^i$ a $g(x) = \sum_i b_i x^i$ umíme přirozeně také sčítat i násobit:

$$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k,$$
$$(f \cdot g)(x) = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + \ldots$$
$$\cdots + (a_0 b_r + a_1 b_{r-1} + a_r b_0)x^r + \cdots + a_k b_\ell x^{k+\ell},$$

kde $k \geq \ell$ jsou stupně polynomů $f$ a $g$ a uvažujeme nulové koeficienty všude tam, kde v původním výrazu pro polynomy nenulové koeficienty nejsou.[4].

Tato definice vskutku odpovídá příslušným operacím sčítání a násobení hodnot zobrazení $f, g : \mathbb{K} \to \mathbb{K}$ díky vlastnostem „skalárů“ v původním okruhu $\mathbb{K}$.

Přímo z definice vyplývá, že množina polynomů $\mathbb{K}[x]$ nad komutativním okruhem s jedničkou je opět komutativním okruhem s jedničkou, přičemž jedničkou v $\mathbb{K}[x]$ je opět jednička 1 v okruhu $\mathbb{K}$ vnímaná jako polynom stupně nula. Nulou pro sčítání je nulový polynom.

**Lemma.** *Okruh polynomů nad oborem integrity je opět obor integrity.*

Důkaz. Máme ukázat, že v $\mathbb{K}[x]$ mohou být netriviální dělitelé nuly pouze, jestliže jsou už v $\mathbb{K}$. To je ale zřejmé z výrazu pro násobení polynomů. Jsou-li $f(x)$ a $g(x)$ polynomy stupně $k$ a $\ell$ jako výše, pak koeficient u $x^{k+\ell}$ v součinu $f(x) \cdot g(x)$ je součin $a_k \cdot b_\ell$ a ten musí být nenulový, pokud nejsou dělitelé nuly v $\mathbb{K}$. □

**11.17. Polynomy více proměnných.** Často se setkáváme s objekty popsanými pomocí polynomiálních výrazů ale s více proměnnými. Např. kružnici v rovině se středem $S = (x_0, y_0)$ a poloměrem $r$ zapíšeme pomocí rovnice



$$(x - x_0)^2 + (y - y_0)^2 - r^2 = 0.$$

[4] Formálně bychom mohli naopak za polynom považovat nekonečný výraz pro $i = 0, \ldots, \infty$ s podmínkou, že jen konečně mnoho koeficientů je nenulových.

□

**11.49.** Rozhodněte, zda předpis $\varphi$ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě $\varphi$:

i) $\varphi : \mathbb{Z}_4 \to \mathbb{C}^*, \varphi([a]_4) = i^a$,
ii) $\varphi : \mathbb{Z}_5 \to \mathbb{C}^*, \varphi([a]_5) = i^a$,
iii) $\varphi : \mathbb{Z}_4 \to \mathbb{C}^*, \varphi([a]_4) = (-1)^a$,
iv) $\varphi : \mathbb{Z} \to \mathbb{C}^*, \varphi(a) = i^a$.

**Řešení.**

i) Platí, že $\varphi([a]_4 + [b]_4) = i^{a+b} = i^a \cdot i^b = \varphi([a]) \cdot \varphi([b])$, navíc $\varphi([4]) = i^4 = 1$, takže pokud $[c]_4 = [d]_4$, tedy $c = d + 4k, k \in \mathbb{Z}$, pak $\varphi([c]_4) = i^c = i^{d+4k} = i^d = \varphi([d]_4)$, zobrazení je tedy korektně zadané a homomorfismus. Tento je injektivní (to je ekvivalentní s tím, že $\mathrm{Ker}(\varphi) = \{[0]_4]\}$) ale zjevně není surjektivní.
ii) Není zobrazení, neboť $[0]_5 = [5]_5$, ale $\varphi([0]_5) = i^0 = 1$, ale $\varphi([5]_5) = i^5 = i$.
iii) Je homomorfismus, který není injektivní ($-1 = \varphi(1) = \varphi(3) = (-1)^3$) a zřejmě ani surjektivní, $\mathrm{Ker}(\varphi) = \{[0]_4, [2]_4]\}$.
iv) Je homomorfismus, který není ani injektivní ani surjektivní. $\mathrm{Ker}(\varphi) = \{4 \cdot k,\ k \in \mathbb{Z}\}$. □

*11.50.* Rozhodněte, zda předpis $\varphi$ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus. Rozhodněte o surjektivitě a injektivitě $\varphi$:

i) $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*, \varphi\left(\frac{p}{q}\right) = \frac{q}{p}$
ii) $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*, \varphi\left(\frac{p}{q}\right) = \frac{p^2}{q^2}$
iii) $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*, \varphi\left(\frac{p}{q}\right) = \frac{p^2+q^2}{pq}$

○

*11.51.* Rozhodněte, zda předpis $\varphi$ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus. Rozhodněte o surjektivitě a injektivitě $\varphi$:

i) $\varphi : \mathbb{C} \to \mathbb{R}, \varphi(a + bi) = a + b$,
ii) $\varphi : \mathbb{C} \to \mathbb{R}, \varphi(a + bi) = a$,
iii) $\varphi : \mathbb{C}^* \to \mathbb{R}^*, \varphi(a + bi) = a^2 + b^2$,
iv) $\varphi : \mathbb{C}^* \to \mathbb{R}^*, \varphi(c) = 2|c|$,
v) $\varphi : \mathbb{C}^* \to \mathbb{R}^*, \varphi(c) = |c|^3$,
vi) $\varphi : \mathbb{C}^* \to \mathbb{R}^*, \varphi(c) = 1/|c|$.

Okruhy polynomů v proměnných $x_1, \ldots, x_r$ můžeme zavést úplně podobně jako jsme postupovali s $\mathbb{K}[x]$. Místo mocnin jediné proměnné $x^k$ budeme uvažovat tzv. *monomy*

$$x_1^{k_1} \cdots x_r^{k_r}$$

a jejich formální lineární kombinace s koeficienty $a_{k_1 \cdots k_r} \in \mathbb{K}$.

Formálně i technicky je ale jednodušší je definovat induktivně vztahem

$$\mathbb{K}[x_1, \ldots, x_r] := \big(\mathbb{K}[x_1, \ldots, x_{r-1}]\big)[x_r].$$

Např. $\mathbb{K}[x, y] = \mathbb{K}[x][y]$, tzn. že uvažujeme polynomy v proměnné $y$ nad okruhem $\mathbb{K}[x]$. Snadno si každý ověří (promyslete si to!), že polynomy v proměnných $x_1, \ldots, x_r$ lze i při této definici chápat jako výrazy vzniklé z písmen $x_1, \ldots, x_n$ a prvků okruhu $\mathbb{K}$ konečným počtem (formálního) sčítání a násobení v komutativním okruhu. Například prvky v $\mathbb{K}[x, y]$ jsou tvaru

$$\begin{aligned} f &= a_n(x)y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x) = \\ &= (a_{mn}x^m + \cdots + a_{0n})y^n + \cdots + (b_{p0}x^p + \cdots + b_{00}) = \\ &= c_{00} + c_{10}x + c_{01}y + c_{20}x^2 + c_{11}xy + c_{02}y^2 + \ldots. \end{aligned}$$

Pro zjednodušení zápisu si zavedeme tzv. multiindexovou symboliku.

### Multiindexy

*Multiindex* $\alpha$ délky $r$ je $r$-tice nezáporných celých čísel $(\alpha_1, \ldots, \alpha_r)$. Celé číslo $|\alpha| = \alpha_1 + \cdots + \alpha_r$ nazýváme *velikost* multiindexu $\alpha$.

Stručně zapisujeme monomy $x^\alpha$ místo $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_r^{\alpha_r}$. Pro polynomy v $r$ proměnných pak máme symbolické vyjádření velice podobné obvyklému značení pro polynomy v jedné proměnné:

$$f = \sum_{|\alpha| \le n} a_\alpha x^\alpha,\ g = \sum_{|\beta| \le m} a_\beta x^\beta \in \mathbb{K}[x_1, \ldots, x_r].$$

Říkáme, že $f$ má celkový stupeň $n$, je-li alespoň jeden z koeficientů s multiindexem $\alpha$ velikosti $n$ nenulový.

Okamžitě se také nabízejí analogické vzorce pro sčítání a násobení polynomů

$$\begin{aligned} f + g &= \sum_{|\alpha| \le \max(m,n)} (a_\alpha + b_\alpha)x^\alpha, \\ fg &= \sum_{|\gamma|=0}^{m+n} \left( \sum_{\alpha+\beta=\gamma} (a_\alpha b_\beta)x^\gamma \right), \end{aligned}$$

kde multiindexy se sčítají po složkách a formálně neexistující koeficienty považujeme za nulové.

**Lemma.** *Tyto vzorce opravdu popisují sčítání a násobení v induktivně definovaném okruhu polynomů v r proměnných.*

Důkaz. Tvrzení lze snadno dokázat indukcí přes počet proměnných. Předpokládejme, že vztahy platí v $\mathbb{K}[x_1, \ldots, x_{r-1}]$ a počítejme součet



○

*11.52.* Rozhodněte, zda předpis $\varphi$ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus. Rozhodněte o surjektivitě a injektivitě $\varphi$:

i) $\varphi : \mathcal{GL}_2(\mathbb{R}) \to \mathbb{R}^*, \varphi(A) = |A|$

ii) $\varphi : \mathcal{GL}_2(\mathbb{R}) \to \mathbb{R}^*, \varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a^2 + b^2.$

iii) $\varphi : \mathcal{GL}_2(\mathbb{R}) \to \mathbb{R}^*, \varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ac + bd.$

○

*11.53.* Rozhodněte, zda předpis $\varphi$ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus. Rozhodněte o surjektivitě a injektivitě $\varphi$:

i) $\varphi : \mathbb{Z}_3 \to \mathbb{A}_4, \varphi([a]_3) = (1,2,4) \circ (1,3,2)^a \circ (1,4,2)$

ii) $\varphi : \mathbb{Z}_3 \to \mathbb{A}_4, \varphi([a]_3) = (1,2) \circ (1,3,2)^a$

○

*11.54.* Rozhodněte, zda předpis $\varphi$ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus. Rozhodněte o surjektivitě a injektivitě $\varphi$:

i) $\varphi : \mathbb{Z} \to \mathbb{Z}, \varphi(a) = 2a$

ii) $\varphi : \mathbb{Z} \to \mathbb{Z}, \varphi(a) = a + 1$

iii) $\varphi : \mathbb{Z} \to \mathbb{Z}, \varphi(a) = 3|a|$

iv) $\varphi : \mathbb{Z} \to \mathbb{Z}, \varphi(a) = 1$

○

*11.55.* Rozhodněte, zda předpis $\varphi$ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus. Rozhodněte o surjektivitě a injektivitě $\varphi$:

i) $\varphi : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}^*, \varphi((a,b,c)) = 2^a 3^b 12^c$

ii) $\varphi : \mathbb{Z}_3^\times \times \mathbb{Z}_5 \to \mathbb{Z}_5, \varphi((a,b)) = b^a$

iii) $\varphi : \mathbb{Z}_2 \times \mathbb{Z} \to \mathbb{Z}, \varphi(([a]_2, b)) = b$

○

**11.56.** Dokažte, že neexistuje izomorfismus multiplikativní grupy komplexních čísel do multiplikativní grupy reálných čísel.

**Řešení.** Při homomorfismu se musí zobrazovat neutrální prvek grupy na neutrální prvek (viz 11.5). Číslo 1 se tedy musí zobrazovat samo na sebe. Kam se může zobrazovat číslo $-1$? Víme, že $f(-1)^2 =$

$$
\begin{aligned}
f &= a_k(x_1,\dots,x_{r-1})x_r^k + \cdots + a_0(x_1,\dots,x_{r-1}) = \\
&= \left(\sum_\alpha a_{k,\alpha} x^\alpha\right) x_r^k + \dots, \\
g &= b_l(x_1,\dots,x_{r-1})x_r^l + \cdots + b_0(x_1,\dots,x_{r-1}) = \\
&= \left(\sum_\beta b_{l,\beta} x^\beta\right) x_r^k + \dots, \\
f+g &= \big(a_0(x_1,\dots,x_{r-1}) + b_0(x_1,\dots,x_{r-1})\big) + \\
&\quad + \big(a_1(x_1,\dots,x_{r-1}) + b_1(x_1,\dots,x_{r-1})\big)x_r + \cdots = \\
&= \left(\sum_\gamma (a_{k,\gamma} + b_{k,\gamma})(x_1,\dots,x_{r-1})^\gamma\right) x_r^k + \dots \\
&\quad \cdots + \left(\sum_\gamma (a_{0,\gamma} + b_{0,\gamma})(x_1,\dots,x_{r-1})^\gamma\right) = \\
&= \sum_{(\gamma,j)} (a_{j,\gamma} + b_{j,\gamma})(x_1,\dots,x_{r-1})^\gamma x_r^j .
\end{aligned}
$$

Podobně lze vést důkaz pro součin (udělejte samostatně!). □

Jako důsledek naší definice a předchozích výsledků pro polynomy nad obecnými komutativními okruhy dostaneme:

**Důsledek.** *Jestliže v okruhu $\mathbb{K}$ nejsou dělitelé nuly, pak také v okruhu polynomů $\mathbb{K}[x_1,\dots,x_r]$ nejsou dělitelé nuly.*

Důkaz. Budeme postupovat indukcí přes počet proměnných $r$.[5] Polynomy v jediné proměnné mají tvar $f = a_n x_1^n + \cdots + a_0$ a $g = b_m x^m + \cdots + b_0$, přičemž $b_m \neq 0$ a $a_n \neq 0$. Vedoucí člen součinu $fg$ je $a_n b_m x^{n+m}$, protože $a_n b_m \neq 0$, zejména tedy je součin nenulových polynomů opět nenulový.

Pokud tvrzení platí pro $r-1$ proměnných, pak použijeme předchozí úvahu pro okruh polynomů v jedné proměnné $x_r$ s koeficienty v $\mathbb{K}[x_1,\dots,x_{r-1}]$. □

**11.18. Dělitelnost a nerozložitelnost.** Naším dalším cílem bude



pochopit, jak je to v obecném případě polynomů nad oborem integrity s jejich rozkladem na součin polynomů jednodušších, tj. ve speciálním případě polynomů s jedinou proměnnou budeme diskutovat kořeny polynomů. U polynomů s více proměnnými půjde o rozklad na jednodušší faktory nižších stupňů. Protože již víme, že polynomy ve více proměnných můžeme definovat induktivně, stačí nám nyní uvažovat jen polynomy v jedné proměnné, ovšem nad obecným oborem integrity, a směřujeme ke zobecnění úvah o dělitelnosti, které byly základem našeho počínání v teorii čísel v desáté kapitole.

Uvažujme nějaký pevně zvolený obor integrity $\mathbb{K}$. Příkladem nám stále mohou sloužit celá čísla $\mathbb{Z}$ nebo okruh $\mathbb{Z}_p$ s prvočíselným $p$.

[5] Důkaz lze vést také přímo s použitím multiindexových formulí pro součin, když si zavedeme vhodné uspořádání monomů tak, jak to budeme za chvíli stejně dělat.

$f((-1)^2) = f(1) = 1$. Obraz čísla $-1$ je tedy nějaká druhá odmocnina z čísla 1. Hledáme-li tedy pouze bijektivní homomorfismy, musí být $f(-1) = -1$. Pak ovšem $f(i)^2 = f(i^2) = f(-1) = -1$, je tedy $f(i)$ druhou odmocninou čísla $-1$ v $\mathbb{R}^*$, ale víme, že taková odmocnina neexistuje. Ani bijektivní homomorfismus tedy nemůže existovat. □

**Poznámka.** Zobrazení, které komplexnímu číslu přiřadí jeho velikost, je homomorfismem $\mathbb{C}^*$ do multiplikativní grupy kladných reálných čísel.

### C. Burnsidovo lemma

**11.57.** Kolika způsoby můžeme vytvořit náhrdelník z 3 černých a 6 bílých korálků stejného tvaru? Kusy stejné barvy nerozlišujeme a za stejné náhrdelníky považujeme všechny, které lze na sebe převést symetrií v rovině.

**Řešení.** Pro řešení úlohy si náhrdelník představíme jako obarvení pevně označených vrcholů pravidelného devítiúhelníka. Za množinu $S$ volíme všechna možná taková obarvení. Každé takové obarvení je jednoznačně určeno pozicí tří černých korálků. Velikost množiny $S$ je tedy $\binom{9}{3} = 84$.

Víme, že grupou všech symetrií je grupa $D_9$ složená z 9 rotací (včetně identity) a stejného počtu reflexí. Stejné náhrdelníky jsou ty, které leží ve stejné orbitě akce grupy $D_9$ na množině všech konfigurací $S$. Zajímá nás tedy počet orbit $N$. Pro výpočet $N$ stačí probrat prvky grupy $D_9$ a všímat si velikostí $S_g$:

Identita je jediný prvek řádu 1, $|S_{\mathrm{id}}| = 84$. Příspěvek do sumy je 84.

Zrcadlení $g$ jsou všechna řádu 2 a je jich 9. Přitom je zjevně $|S_g| = 4$, celkový příspěvek je proto $4 \cdot 9 = 36$.

Dvě rotace $g$ o úhel $2\pi/3$ nebo $4\pi/3$ mají řád 3 a $|S_g| = 3$. Jejich příspěvek je tedy 6.

Konečně zbývajících rotací (řádu 9 v $D_9$) je 6 a nenechávají na místě žádný prvek, do celkové sumy tedy ničím nepřispívají.

Celkem dostáváme podle formule z Burnsidova lemmatu:

$$N = \frac{1}{|D_9|} \sum_{g \in D_9} |S_g| = \frac{126}{18} = 7.$$

Najděte si příslušných sedm různých náhrdelníků! □

**11.58.** Určete počet obarvení políček tabulky $3 \times 3$ třemi barvami, považujeme-li za stejná obarvení, která na sebe přejdou při nějaké symetrii tabulky (tedy rotací nebo zrcadlením).

**Řešení.** Grupa symetrií tabulky je grupou symetrií čtverce, tedy dihedrální grupa $D_4$. Všech obarvení tabulky, pokud považujeme každé

#### Dělitelnost v okruzích

Obecně říkáme, že $a \in \mathbb{K}$ *dělí* $c \in \mathbb{K}$, jestliže existuje $b$ tak, že $a \cdot b = c$. Skutečnost, že $c \in \mathbb{K}$ je dělitelné $a \in \mathbb{K}$, zapisujeme $a|c$.

Dělitelé jedničky, tj. invertibilní prvky v $\mathbb{K}$, se nazývají *jednotky*. Jednotky v komutativním okruhu vždy tvoří komutativní grupu.

V oboru integrity jsou dělitelé určeni jednoznačně. Skutečně je-li $b = a \cdot c$ a $b \neq 0$, pak $c$ je jednoznačně dáno volbou $a, b$, protože při $b = ac = ac'$ totiž platí $0 = a \cdot (c - c')$ a $a \neq 0$. Z neexistence dělitelů nuly proto vyplývá $c = c'$.

Přímo z definic vyplývají následující tvrzení:

**Lemma.** *Nechť $a, b, c \in \mathbb{K}$. Potom*

*(1) je-li $a|b$ a zároveň $b|c$, pak také $a|c$,*
*(2) je-li $a|b$ a zároveň $a|c$, pak také $a|(\alpha b + \beta c)$ pro všechny $\alpha, \beta \in \mathbb{K}$,*
*(3) $a|0$ pro všechna $a \in \mathbb{K}$ (je totiž $a \cdot 0 = 0$),*
*(4) každý prvek $a \in \mathbb{K}$ je dělitelný všemi jednotkami $e \in \mathbb{K}$ a jejich násobky $a \cdot e$ (jak přímo plyne z existence $e^{-1}$).*

#### Jednoznačný rozklad v oboru integrity

Řekneme, že prvek $a \in \mathbb{K}$ je *nerozložitelný*, jestliže je dělitelný pouze jednotkami $e \in \mathbb{K}$ a jejich násobky $a \cdot e$.

Řekneme, že okruh $\mathbb{K}$ je *obor integrity s jednoznačným rozkladem*, jestliže platí:

- pro každý nenulový prvek $a \in \mathbb{K}$ existují nerozložitelné $a_1, \ldots, a_r \in \mathbb{K}$ takové, že $a = a_1 \cdot a_2 \ldots a_r$,
- jsou-li prvky $a_1, \ldots, a_r$ a $b_1, \ldots, b_s$ nerozložitelné, nejsou mezi nimi žádné jednotky a $a = a_1 a_2 \ldots a_r = b_1 b_2 \ldots b_s$, pak je $r = s$ a ve vhodném přeuspořádání platí $a_j = e_j b_j$ pro vhodné jednotky $e_j$.

Již jsme viděli, že $\mathbb{Z}$ je obor integrity s jednoznačným rozkladem a každé pole (komutativní těleso) je obor integrity s jednoznačným rozkladem (protože každý nenulový prvek v poli je jednotka).

Pro ilustraci si uveďme příklad oboru integrity, který jednoznačný rozklad nemá. Konstrukce je podobná polynomům, jen místo mocnin uvážíme vhodně se skládající odmocniny: Naše $\mathbb{K}$ bude mít prvky tvaru



$$a_0 + \sum_{i=1}^{k} a_i \left( \sqrt[2^{n_i}]{x^{m_i}} \right),$$

kde $a_0, \ldots, a_k \in \mathbb{Z}$, $m_i, n \in \mathbb{Z}_{>0}$. Pak jednotky jsou v $\mathbb{K}$ pouze prvky $\pm 1$, všechny prvky s $a_0 = 0$ jsou rozložitelné, ale např. výraz $x$ nelze vyjádřit jako součin nerozložitelných. Nerozložitelných prvků je v $\mathbb{K}$ prostě příliš málo.

**11.19. Dělení se zbytkem a kořeny polynomu.** Základním nástrojem pro diskusi dělitelnosti, společných dělitelů apod. v okruhu celých čísel $\mathbb{Z}$ byla procedura dělení se zbytkem a Euklidův algoritmus pro hledání největších společných dělitelů. Tyto postupy nyní zobecníme.



**Lemma** (Algoritmus pro dělení se zbytkem)**.** *Nechť $\mathbb{K}$ je komutativní okruh bez dělitelů nuly a $f, g \in \mathbb{K}[x]$ polynomy, $g \neq 0$. Pak*

políčko za jedinečné, je $3^9$. Na těchto obarveních nám tedy působí grupa $G = D_4$. Postupně projdeme všechny symetrie $g$ z $G$ a určíme, kolik takových obarvení zachovávají:

- $g = \mathrm{Id}$: $|S_g| = 3^9$.
- $g$ je rotace o 90° či o 270°(= −90°): Při takové rotaci přejde libovolné rohové pole na sousední rohové pole. Aby se obarvení nezměnilo, musí mít všechna rohová pole stejnou barvu. Obdobně musí mít stejnou barvu středová políčka stran. Středové políčko celé tabulky pak může být libovolné. Celkem existuje $3^3$ různých obarvení, která se nezmění, provedeme-li s tabulkou jednu z uvažovaných rotací.
- $g$ je rotace o 180°: Čtyři dvojice políček středově symetrických podle středu tabulky musí mít stejnou barvu, středové políčko pak může opět být obarveno libovolně. Celkem $|S_g| = 3^5$.
- $g$ je jednou ze čtyř osových symetrií: Políčka, která se při osové symetrii zachovávají (jsou tři), mohou být obarvena libovolně, zbylých šest polí tvoří tři dvojice políček, které se na sebe při osové symetrii zobrazí. Políčka ve dvojici musí tedy mít stejnou barvu. Celkem $|S_g| = 3^6$.

Podle Burnsidova lemmatu je počet hledaných obarvení roven

$$\frac{1}{8}\left(3^9 + 2\cdot 3^3 + 3^5 + 4\cdot 3^6\right) = 2862. \qquad \square$$

**11.59.**

a) Určete všechny rotační symetrie pravidelného osmistěnu.

b) Určete počet obarvení stěn pravidelného osmistěnu třemi barvami, považujeme-li za stejná ta obarvení, která na sebe přejdou při nějaké rotaci osmistěnu.

**Řešení.**

a) Umístíme-li osmistěn do kartézské souřadné soustavy tak, že dvojice protějších vrcholů bude na osách a střed v počátku souřadnic, pak je každá rotační symetrie dána tím, který ze šesti vrcholů bude po jejím provedení na ose $z$ „dole“ a která ze čtyř z něj vedoucích hran z něj půjde „dopředu nahoru“. Grupa má tedy celkem 24 prvků. Jde o rotace o ±90° a o 180° okolo os procházejících protějšími vrcholy, o rotace o 180° podle os procházejících středy protějších hran a konečně o rotace o ±120° okolo os procházejích středy protějších stěn.

b) Obarvení osmistěnu, považujeme-li každou stěnu za jedinečnou, je celkem $3^8$. Pro každou rotační symetrii $g$ spočtěme, kolik zachovává různých obarvení:

*existuje $a \in \mathbb{K}$, $a \neq 0$ a polynomy $q$ a $r$ splňující $af = qg + r$, kde $r = 0$ nebo $\deg r < \deg g$. Je-li navíc $\mathbb{K}$ pole, nebo je aspoň vedoucí koeficient polynomu $g$ roven jedné, potom lze volit $a = 1$ a polynomy $q$ a $r$ jsou v tomto případě určeny jednoznačně.*

Důkaz. Tvrzení dokážeme indukcí vzhledem ke stupni $f$. Je-li $\deg f < \deg g$ nebo $f = 0$, pak volíme $a = 1$, $q = 0$, $r = f$, což vyhovuje všem našim podmínkám. Pro konstantní polynom $g$ klademe $a = g$, $q = f$, $r = 0$.

Předpokládejme tedy, že $\deg f \geq \deg g > 0$ a pišme

$$f = a_0 + \cdots + a_n x^n, \quad g = b_0 + \cdots + b_m x^m.$$

Buď platí $b_m f - a_n x^{n-m} g = 0$ a nebo je $\deg(b_m f - a_n x^{n-m} g) < \deg f$. V prvém případě jsme hotovi, ve druhém pak, podle indukčního předpokladu, existují $a'$, $q'$, $r'$ splňující

$$a'\left(b_m f - a_n x^{n-m} g\right) = q' g + r'$$

a buď $r' = 0$ nebo $\deg r' < \deg g$. Tzn.

$$a' b_m f = \left(q' + a' a_n x^{n-m}\right) g + r'.$$

Přitom je-li $b_m = 1$ nebo $\mathbb{K}$ je pole, pak podle indukčního předpokladu lze volit $a' = 1$ a $q'$, $r'$ jsou tak určeny jednoznačně. V takovém případě ovšem získáme

$$b_m f = \left(q' + a_n x^{n-m}\right) g + r',$$

a je-li $\mathbb{K}$ pole, můžeme rovnost vynásobit $b_m^{-1}$.

Předpokládejme, že $f = q_1 g + r_1$ je jiné řešení. Pak $0 = f - f = (q - q_1)g + (r - r_1)$ a buď je $r = r_1$, nebo $\deg(r - r_1) < \deg g$. V prvém případě odtud ovšem plyne i $q = q_1$, protože $\mathbb{K}[x]$ neobsahuje dělitele nuly. Nechť $ax^s$ je člen nejvyššího stupně v $q - q_1 \neq 0$ (určitě existuje). Potom jeho součin se členem nejvyššího stupně v $g$ musí být nulový (protože nejvyšší stupeň dostaneme tak, že vynásobíme nejvyšší stupně). To ovšem znamená, že $a = 0$. Protože $ax^s$ byl největší nenulový stupeň, nutně dostáváme, že $q - q_1$ žádné nenulové monomy neobsahuje, je tedy určitě nulové. Pak ovšem i $r = r_1$. $\square$

Proceduru dělení se zbytkem můžeme okamžitě využít k diskusi kořenů polynomů. Uvažme tedy polynom $f \in \mathbb{K}[x]$, $\deg f > 0$ a zkusme jej vydělit polynomem $x - b$, $b \in \mathbb{K}$. Protože je vedoucí koeficient jednička, algoritmus pro dělení dává jednoznačný výsledek. Dostáváme tedy jednoznačně zadané polynomy $q$ a $r$ splňující $f = q(x - b) + r$, kde $r = 0$ nebo $\deg r = 0$, tj. $r \in \mathbb{K}$. Tzn., že hodnota polynomu $f$ v $b \in \mathbb{K}$ je rovna právě $f(b) = r$. Z toho plyne, že prvek $b \in \mathbb{K}$ je kořen polynomu $f$ právě, když $(x - b)|f$. Protože po vydělení polynomem stupně jedna vždy klesne stupeň výsledku alespoň o jedničku, dokázali jsme následující tvrzení:

**Důsledek.** *Každý polynom $f \in \mathbb{K}[x]$ má nejvýše $\deg f$ kořenů. Zejména tedy zadávají polynomy nad nekonečným oborem integrity stejná zobrazení $\mathbb{K} \to \mathbb{K}$, právě když jde o stejné polynomy.*

Skutečně dva polynomy nad oborem integrity, které zadávají stejné zobrazení $\mathbb{K} \to \mathbb{K}$, mají rozdíl, jehož kořenem je každý prvek v $\mathbb{K}$. To však znamená, že pokud by jejich rozdíl nebyl nulový polynom, pak $\mathbb{K}$ má nejvýše tolik prvků, kolik je maximum ze stupňů uvažovaných polynomů.

Zatímco reálné polynomy mohou být i úplně bez kořenů, každý komplexní polynom naopak takovýto rozklad připouští. To je obsahem tzv. základní věty algebry, kterou pro úplnost uvádíme

– $g$ je rotace o $\pm 90°$ podle osy procházející protějšími vrcholy. Potom $g$ zachovává $3^2$ obarvení. Takových rotací je celkem 6.
– $g$ je rotace o $180°$ podle osy procházející protějšími vrcholy nebo podle osy procházející středy protějších hran. Potom $g$ zachovává $3^4$ různých obarvení. Takových rotací je celkem $3 + 6 = 9$.
– $g$ je rotace o $\pm 120°$. Potom $g$ zachovává opět $3^4$ různých obarvení. Takových rotací je osm.

Celkem je hledaný počet obarvení roven

$$\tfrac{1}{24}\left(3^8 + 6 \cdot 3^2 + 17 \cdot 3^4\right) = 333. \qquad \square$$

**11.60.** Kolik různých náramků lze sestavit právě z devíti bílých, šesti červených a tří černých korálků? (dva náramky považujeme za stejné, pokud se liší pouze nějakou rotací v prostoru)



**Řešení.** Grupa symetrií náramku je dihedrální grupa $D_{18}$ o 36 prvcích. Ta operuje na množině náramků, kde máme pevně očíslovaná místa na náramku (od jedné do osmnácti), těch je $18!/(9!6!3!) = 4084080$. Symetrie, které zachovávají nenulový počet takovýchto náramků, jsou zjevně pouze rotace o $120°$ a $240°$ a zrcadlení podle osy procházející protějšími vrcholy (takových je devět) a samozřejmě identita. Podle Burnsidova lematu je hledaný počet náramků roven

$$\frac{1}{36}\left(4084080 + 2 \cdot \binom{6}{3}\binom{3}{3} + 9 \cdot \binom{8}{4}\binom{4}{3}\right) = 113590.$$

$\square$

*11.61.* Určete, kolik existuje náramků sestavených z právě šesti stejných bílých, šesti stejných červených a šesti stejných černých korálků, přičemž dva náramky považujeme za stejné, pokud se liší nějakou rotací (v prostoru). $\bigcirc$

s (v podstatě) kompletním důkazem. Díky tomuto výsledku víme, že každý polynom v $\mathbb{C}[x]$ má tolik kořenů, včetně násobnosti, jako je jeho stupeň $\deg f = k$. Proto připouští vždy rozklad tvaru

$$f(x) = b(x - a_1) \cdot (x - a_2) \ldots (x - a_k)$$

s vhodnými komplexními kořeny $a_i$ a vedoucím koeficientem $b$.

**11.20. Věta** (Základní věta algebry)**.** *Pole $\mathbb{C}$ je algebraicky uzavřené, tj. každý polynom stupně alespoň 1 má kořen.*



Důkaz. Předpokládejme, že $f \in \mathbb{C}[z]$ je nenulový polynom, který nemá kořen, tj. $f(z) \neq 0$ pro všechna $z \in \mathbb{C}$. Definujme zobrazení

$$\varphi : \mathbb{C} \to \mathbb{C}, \quad z \mapsto \frac{f(z)}{|f(z)|},$$

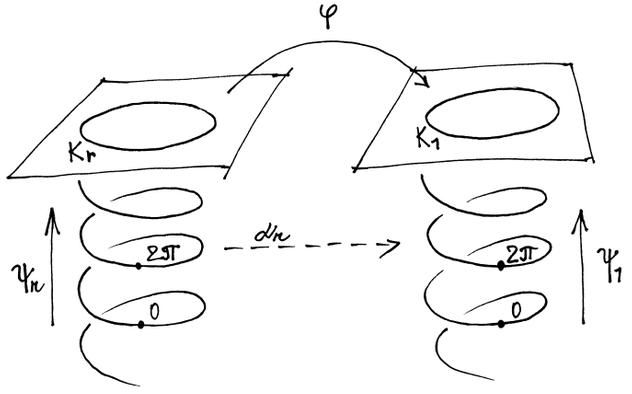
tj. $\varphi$ zobrazí celé $\mathbb{C}$ do jednotkové kružnice $K_1 = \{e^{it}, t \in \mathbb{R}\} \subseteq \mathbb{R}^2 = \mathbb{C}$. Díky našemu předpokladu o nenulovosti $f(z)$ je to skutečně dobře definované zobrazení. Dále definujme zobrazení s hodnotami v kružnici $K_r \subseteq \mathbb{C}$ se středem v nule a poloměrem $r \geq 0$:

$$\psi_r : \mathbb{R} \to K_r, \quad t \mapsto \psi(t) = re^{it}.$$

Pro každé $r \in \langle 0, \infty)$ máme definováno spojité zobrazení $\kappa_r = \varphi \circ \psi_r : \mathbb{R} \to K_1$. Ze spojité závislosti $\kappa$ na parametru $r$ navíc vyplývá existence zobrazení $\alpha_r : \mathbb{R} \to \mathbb{R}$ jednoznačně zadaného podmínkami $0 \leq \alpha_r(0) < 2\pi$ a $\kappa_r(t) = e^{i\alpha_r(t)}$. Získané zobrazení $\alpha_r$ opět spojitě závisí na $r$. Celkem tedy máme spojité zobrazení

$$\alpha : \mathbb{R} \times \langle 0, \infty) \to \mathbb{R}, \quad (t, r) \mapsto \alpha_r(t)$$

a z jeho konstrukce plyne, že pro všechna $r$ je $\frac{1}{2\pi}(\alpha_r(2\pi) - \alpha_r(0)) = n_r \in \mathbb{Z}$. Protože je $\alpha$ spojité, znamená to, že $n_r$ je celočíselná konstanta nezávislá na $r$. Podívejte se na obrázek, odkud kam jdou jednotlivá zobrazení v naší konstrukci!




Pro dokončení důkazu si stačí uvědomit, že pokud $f = a_0 + \cdots + a_d z^d$ a $a_d \neq 0$, pak pro malá $r$ se bude $\alpha_r$ chovat podobně jako konstantní zobrazení, zatímco pro velká $r$ to vyjde stejně, jako kdyby $f = z^d$. Nejprve si spočtěme, jak tedy $n_r$ dopadne při $f = z^d$, pak toto tvrzení upřesníme a důkaz tím bude ukončen.

*11.62.* Určete, kolik existuje náramků sestavených z právě osmi stejných bílých, osmi stejných červených a osmi stejných černých korálků, přičemž dva náramky považujeme za stejné, pokud se liší nějakou rotací (v prostoru). ○

*11.63.* Kolik existuje náramků složených ze tří stejných bílých a šesti stejných černých korálků, považujeme-li dva náramky za stejné, lze-li jeden na druhý převést rotací (v prostoru)? ○

### D. Okruhy

*11.64.* Rozhodněte, zda množina $R$ s operacemi $\oplus, \odot$ tvoří okruh, komutativní okruh, obor integrity či těleso:

i) $R = \mathbb{Z}, a \oplus b = a + b + 3, a \odot b = -3$,
ii) $R = \mathbb{Z}, a \oplus b = a + b - 3, a \odot b = a \cdot b - 1$,
iii) $R = \mathbb{Z}, a \oplus b = a + b - 1, a \odot b = a + b - a \cdot b$,
iv) $R = \mathbb{Q}, a \oplus b = a + b, a \odot b = b$,
v) $R = \mathbb{Q}, a \oplus b = a + b + 1, a \odot b = a + b + a \cdot b$,
vi) $R = \mathbb{Q}, a \oplus b = a + b - 1, a \odot b = a + b + a \cdot b$.

○

**Řešení.**

i) je okruh,
ii) není okruh,
iii) je obor integrity,
iv) není okruh,
v) je těleso,
vi) není okruh. □

**11.65.** Dokažte, že podmnožina komplexních čísel $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ tvoří obor integrity. Jedná se o těleso?

**Řešení.** Libovolný podokruh oboru integrity je nutně opět oborem integrity. V tomto případě uvažujeme o podmnožině tělesa $\mathbb{C}$ (tedy i oboru integrity). Že se jedná o podokruh je zřejmé (opačná čísla ve zkoumané množině leží, součin dvou čísel rovněž). Inverze však existují pouze pro čísla $1, i, -1, -i$ (jedná se o tzv. podgrupu jednotek – invertibilních prvků). Nejedná se tedy o těleso. □

**11.66.** Uvažujme v okruhu reálných $2 \times 2$ matic podokruh matic tvaru $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Dokažte, že tento podokruh je izomorfní $\mathbb{C}$.

**Řešení.** Ukážeme, že izomorfismus je daný zobrazením $\varphi : \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a + ib$. Pro součin prvků v daném podokruhu

Funkce $\mathbb{C} \to \mathbb{C}, z \mapsto z^d, z \mapsto \frac{z^d}{|z^d|}$ se snadno vyjádří pomocí goniometrického tvaru komplexních čísel $z = r(\cos\alpha + i \sin\alpha)$:

$$z^d = r^d (\cos d\alpha + i \sin d\alpha) = r^d \, \mathrm{e}^{i d\alpha},$$
$$\frac{z^d}{|z^d|} = 1(\cos d\alpha + i \sin d\alpha) = \mathrm{e}^{i d\alpha}.$$

Zobrazení $\varphi$ je tedy v tomto případě pouze otočení komplexní roviny, následované středovou projekcí na jednotkovou kružnici.

Pak tedy $\kappa_r(t) = \mathrm{e}^{idt}$, a proto $\alpha_r(t) = dt$ nezávisle na $r$. Odtud pro naši volbu $f = z^d$ vyplývá $n_r = d$. Pokud zvolíme $f = az^d$, $a \neq 0$, nebude to mít na předchozí výsledek žádný vliv (přesvědčte se!).

Zvolme nyní obecný polynom $f = a_0 + \cdots + a_d z^d$, který nemá kořen. Víme tedy, že $a_0 \neq 0$ (pokud by bylo $a = 0$, existoval by kořen). Pro $z \neq 0$ platí

$$\frac{f(z)}{a_d z^d} = 1 + \frac{1}{a_d}(a_0 z^{-d} + \cdots + a_{d-1} z^{-1}),$$

a proto $\lim_{|z|\to\infty} \frac{f(z)}{a_d z^d} = 1$. Když tohle víme, můžeme spočítat

$$\lim_{|z|\to\infty} \left| \frac{f(z)}{|f(z)|} - \frac{a_d z^d}{|a_d z^d|} \right| = \lim_{|z|\to\infty} \left| \frac{f(z)}{a_d z^d} \frac{a_d z^d}{|a_d z^d|} \frac{|a_d z^d|}{|f(z)|} - \frac{a_d z^d}{|a_d z^d|} \right| = 0.$$

Proto $n_r = d$ pro velká $r$.

Podobnou úvahu uděláme i pro malá $r$. Připomeňme si, že $a_0 \neq 0$:

$$\frac{f(z)}{a_0} = 1 + \frac{1}{a_0}(a_1 z + \cdots + a_d z^d),$$

proto $\lim_{|z|\to 0} \frac{f(z)}{a_0} = 1$. Přitom opět platí $\frac{f(z)}{|f(z)|} = \frac{f(z)}{a_0} \frac{a_0}{|a_0|} \frac{|a_0|}{|f(z)|}$. Odtud $\lim_{|z|\to 0} \frac{f(z)}{|f(z)|} = \lim_{|z|\to 0} \frac{a_0}{|a_0|}$, tj. $n_r = 0$ pro malá $r$. Celkem vidíme, že stupeň našeho polynomu je $d = 0$. □

**11.21. Největší společný dělitel polynomů.** Uvažme okruh polynomů $\mathbb{K}[x]$ nad oborem integrity $\mathbb{K}$. Řekneme, že $h$ je *největší společný dělitel* dvou polynomů $f$ a $g \in \mathbb{K}[x]$ jestliže:



- $h | f$ a zároveň $h | g$,
- jestliže $k | f$ a zároveň $k | g$, pak také $k | h$.

Jako přímý důsledek existence algoritmu pro jednoznačné dělení se zbytkem dostáváme následující důležitou *Bezoutovu rovnost* (její důkaz se o dělení se zbytkem opírá úplně stejně jako tomu bylo v kapitole 10 u celých čísel).

**Věta.** *Nechť $\mathbb{K}$ je pole a nechť $f, g \in \mathbb{K}[x]$. Pak existuje největší společný dělitel $h$ polynomů $f$ a $g$. Polynom $h$ je určený jednoznačně až na násobek nenulovým skalárem. Přitom existují polynomy $A, B \in \mathbb{K}[x]$ takové, že $h = Af + Bg$.*

Důkaz. Přímá konstrukce polynomů $h$, $A$ a $B$ se provede tzv. Euklidovým algoritmem. Provádíme postupně dělení se zbytkem ($\mathbb{K}$ je pole, takže to vždy umíme jednoznačně, viz předchozí

dostáváme formuli

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -bc-ad \\ bc+ad & ac-bd \end{pmatrix}$$

a v $\mathbb{C}$ je $(a+ib)(c+id) = ac-bd+i(bc+ad)$. Odtud je vidět, že $\varphi$ je homomorfismus vzhledem k násobení. Protože sčítání je definováno po složkách, je zřejmě $\varphi$ i homomorfismus vzhledem ke sčítání, a jedná se tedy o homomorfismus okruhů. Toto zobrazení je evidentně injektivní i surjektivní a proto izomorfismus. □

**11.67.** Dokažte, že identita je jediný automorfismus pole reálných čísel.

**Řešení.** Mějme nějaký automorfismus $\varphi : \mathbb{R} \to \mathbb{R}$. Základním předpokladem je $\varphi(0) = 0$ a $\varphi(1) = 1$. Protože $\varphi$ je homomorfismus vzhledem ke sčítání, tak pro všechna přirozená $n$ platí $\varphi(n) = \varphi(1+1+\cdots+1) = n\varphi(1) = n$ a $\varphi(-n) = -n$, a protože je homomorfismus vzhledem k násobení, tak pro celá čísla $p, q, q \neq 0$ máme $\varphi(p) = \varphi(q \cdot \frac{p}{q}) = \varphi(p) \cdot \varphi(\frac{p}{q})$. Odtud $\varphi(\frac{p}{q}) = \frac{p}{q}$, tj. $\varphi(r) = r$ pro všechna racionální $r$.

Uvažme kladné $x \in \mathbb{R}$. Pak $\varphi(x) = \varphi\left(\sqrt{x}^2\right) = \varphi\left(\sqrt{x}\right)^2 \geq 0$. Proto pro libovolná $x, y \in \mathbb{R}$, $x < y$ platí $\varphi(x) < \varphi(y)$. Nyní předpokládejme, že $\varphi$ není identické zobrazení, tj. $\varphi(z) \neq z$ pro nějaké $z \in \mathbb{R}$. Bez újmy na obecnosti můžeme předpokládat, že $\varphi(z) < z$. Protože je $\mathbb{Q}$ husté v $\mathbb{R}$, tak existuje nějaké $r \in \mathbb{Q}$, pro které platí $\varphi(z) < r < z$. Víme ovšem, že $\varphi(r) = r$, a proto z $r < z$ plyne $\varphi(r) < \varphi(z)$. Celkem tedy máme $\varphi(z) < \varphi(r) < \varphi(z)$, což je spor. □

**11.68.** Nechť $p$ je prvočíslo a $R$ je okruh s jednotkou obsahující $p^2$ prvků. Dokažte, že $R$ je komutativní.

**Řešení.** Protože $(R, +)$ je konečná komutativní grupa s $p^2$ prvky, je podle 11.8 izomorfní buď $\mathbb{Z}_{p^2}$ nebo $\mathbb{Z}_p \times \mathbb{Z}_p$. V prvním případě je $(R, +)$ cyklická, a proto existuje prvek $x \in R$ takový, že každý prvek $R$ je tvaru $nx$ pro nějaké $1 \leq n \leq p^2$. Protože všechny takové prvky spolu komutují, je celé $R$ komutativní.

V druhém případě musí mít každý prvek řád $p$ (vzhledem ke sčítání). Nechť $x \in R$ je libovolný prvek, který není v aditivní podgrupě generované jednotkou. Pak každý prvek $R$ musí být tvaru $m+nx$, kde $1 \leq m, n \leq p$. I takové prvky spolu zřejmě komutují, a proto je opět celé $R$ komutativní. □

**11.69.** Určete inverze prvků 17, 18 a 19 v $(\mathbb{Z}_{131}^{\times}, \cdot)$, tedy v grupě invertibilních prvků ze $\mathbb{Z}_{131}$ s operací násobení.

lemma):

$$\begin{aligned} f &= q_1 g + r_1, \\ g &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\vdots \\ r_{p-1} &= q_{p+1} r_p + 0. \end{aligned}$$

V tomto postupu neustále klesají stupně $r_i$, proto jistě nastane rovnost z posledního řádku (pro vhodné $p$) a ta říká, že $r_p | r_{p-1}$. Z předposledního řádku pak ale plyne $r_p | r_{p-2}$ a postupně dojdeme až nazpět k prvnímu a druhému řádku, které dají $r_p | g$ a $r_p | f$.

Pokud $h | f$ a $h | g$, pak ze stejných rovností postupně plyne, že $h$ dělí všechny $r_i$, zejména tedy $r_p$, tzn. získali jsme největšího společného dělitele $h = r_p$ polynomů $f$ a $g$.

Nyní můžeme postupně dosazovat z poslední do předchozích rovnic:

$$\begin{aligned} h = r_p &= r_{p-2} - q_p r_{p-1} = \\ &= r_{p-2} - q_p(r_{p-3} - q_{p-1} r_{p-2}) = \\ &= -q_p r_{p-3} + (1 + q_{p-1}) r_{p-2} = \\ &= -q_p r_{p-3} + (1 + q_{p-1} q_p) r_{p-2} = \\ &= -q_p r_{p-3} + (1 + q_p q_{p-1})(r_{p-4} - q_{p-2} r_{p-3}) = \\ &\vdots \\ &= Af + Bg. \end{aligned}$$

□

**11.22. Podílová tělesa.** Když se potýkáme s celočíselnými



výpočty, je často technicky výhodnější pracovat v číslech racionálních a až na konci postupu ověřit, že výsledek musí ve skutečnosti být celočíselný. Takto jsme už postupovali mnohokrát. Při práci s polynomy nám bude podobný postup užitečný také.

Nechť $\mathbb{K}$ je komutativní okruh (s jedničkou) bez dělitelů nuly. Jeho *podílové těleso* definujeme jako třídy ekvivalence dvojic $(a, b) \in \mathbb{K} \times \mathbb{K}$, $b \neq 0$, které zapisujeme $\frac{a}{b}$, a ekvivalence je dána

$$\frac{a}{b} = \frac{a'}{b'} \quad \Leftrightarrow \quad ab' = a'b.$$

Sčítání a násobení definujeme prostřednictvím reprezentantů tříd

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd},$$
$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Snadno se ověří korektnost této definice a všechny axiomy komutativního tělesa. Zejména je $\frac{0}{1}$ neutrální prvek vzhledem ke sčítání, $\frac{1}{1}$ je neutrální prvek vzhledem k násobení a pro $a \neq 0, b \neq 0$ je $\frac{a}{b}\frac{b}{a} = \frac{1}{1}$.

Podílové těleso okruhu $\mathbb{K}[x_1, \ldots, x_r]$ nazýváme *těleso racionálních funkcí* a značíme jej $\mathbb{K}(x_1, \ldots, x_r)$. Všechny algebraické operace s polynomy v softwarových systémech jako je Maple nebo Mathematica jsou prováděny ve skutečnosti nad podílovými tělesy, tj. v tělesech racionálních funkcí, zpravidla s použitím $\mathbb{K} = \mathbb{Q}$.

Zformulujme si teď velice užitečné (i elegantní) tvrzení, jehož důkaz je docela přímočarý, ale vyžaduje poměrně technické dopracování detailů (a odvíjí se na úrovni podílového tělesa racionálních funkcí). Doporučujeme proto pečlivě pročíst následující odstavec

**Řešení.** Nalezneme pomocí Eukleidova algoritmu:

$$131 = 7 \cdot 17 + 12,$$
$$17 = 1 \cdot 12 + 5,$$
$$12 = 2 \cdot 5 + 2,$$
$$5 = 2 \cdot 2 + 1.$$

Je tedy $1 = 5-2\cdot 2 = 5-2(12-2\cdot 5) = 5\cdot 5-2\cdot 12 = 5\cdot(17-12)-2\cdot 12 = 5\cdot 17-7\cdot 12 = 5\cdot 17-7\cdot(131-7\cdot 17) = 54\cdot 17-7\cdot 131$. Inverze k 17 je 54. Obdobně $[18]^{-1} = 51$ a $[19]^{-1} = 69$. □

*11.70.* Nalezněte inverzi prvku $[49]_{\mathbb{Z}_{253}}$ v $\mathbb{Z}_{253}$ ○

*11.71.* Nalezněte inverzi prvku $[37]_{\mathbb{Z}_{208}}$ v $\mathbb{Z}_{208}$. ○

*11.72.* Nalezněte inverzi prvku $[57]_{\mathbb{Z}_{359}}$ v $\mathbb{Z}_{359}$. ○

*11.73.* Nalezněte inverzi prvku $[17]_{\mathbb{Z}_{40}}$ v $\mathbb{Z}_{40}$. ○

## E. Okruhy polynomů

*11.74.* **Eisensteinovo kriterium ireducibility.** Udává, kdy je polynom nad okruhem $\mathbb{Z}$ nerozložitelný nad $\mathbb{Q}$ (což je stejné jako nerozložitelnost nad $\mathbb{Z}$):

Buď

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

polynom nad $\mathbb{Z}$ a dále nechť existuje prvočíslo $p$ tak, že

- $p$ dělí $a_j$, $j = 0, \ldots, n-1$,
- $p$ nedělí $a_n$,
- $p^2$ nedělí $a_0$,

pak je $f(x)$ nerozložitelný nad $\mathbb{Z}$ ($\mathbb{Q}$). Dokažte toto kriterium. ○

**11.75.** Rozložte nad $\mathbb{C}$ a nad $\mathbb{R}$ mnohočlen

$$x^4 + 2x^3 + 3x^2 + 2x + 1.$$

**Řešení.** Příklad lze řešit jak hledáním největšího společného dělitele s derivací, tak jako reciprokou rovnici:

- Spočítejme Eukleidovým algoritmem největšího společného dělitele daného polynomu a jeho derivace $4x^3 + 6x^2 + 6x + 2$. Největší společný dělitel je dán v libovolném okruhu až na násobek jednotky a i v průběhu Eukleidova algoritmu můžeme mezivýsledky násobit jednotkami daného okruhu. V případě okruhu polynomů nad tělesem skalárů a případně pak při prvním čtení přeskočit další tři lemmata důkazu (a pokračovat na straně 668).

**11.23. Věta.** *Je-li $\mathbb{K}$ obor integrity s jednoznačným rozkladem, pak také okruh polynomů $\mathbb{K}[x]$ je obor integrity s jednoznačným rozkladem.*



Důkaz. Myšlenka důkazu je velice jednoduchá. Uvažujme polynom $f \in \mathbb{K}[x]$. Je-li $f$ rozložitelný, pak je $f = f_1 \cdot f_2$, kde žádný z polynomů $f_1, f_2 \in \mathbb{K}[x]$ není jednotka. Předpokládejme na chvíli navíc, že je-li $f$ dělitelný nerozložitelným polynomem $h$, pak jistě $h$ dělí $f_1$ nebo $f_2$.

Pokud tomu tak vždy bude, docílíme postupnou aplikací předchozí úvahy jednoznačného rozkladu. Pokud je totiž $f_1$ dále rozložitelný, opět $f_1 = g_1 \cdot g_2$, kde $g_1, g_2$ nejsou jednotky, a přitom vždy buď oba polynomy $g_1$ a $g_2$ mají menší stupeň než $f$, nebo se sníží počet nerozložitelných faktorů ve vedoucích členech $g_1$ a $g_2$ (např. nad celými čísly $\mathbb{Z}$ je $2x^2 + 2x + 2 = 2(x^2 + x + 1)$). Proto po konečném počtu kroků dojdeme k rozkladu $f = f_1 \ldots f_r$ na nerozložitelné polynomy $f_1, \ldots, f_r$.

Z našeho dodatečného předpokladu také plyne, že každý nerozložitelný polynom $h$ dělící $f$ dělí některý z $f_1, \ldots, f_r$. Proto pro každý další rozklad $f = f_1' f_2' \ldots f_s'$ nutně každý z faktorů $f_i$ dělí některý z $f_j'$ a v takovém případě musí být $f_j' = e f_i$ pro vhodnou jednotku $e$. Postupným krácením takových dvojic odvodíme, že $r = s$ a jednotlivé faktory se liší pouze o násobky jednotek. □

Zbývá tedy dokázat, že je-li $f = f_1 f_2$ dělitelný nerozložitelným polynomem $h$, pak jistě $h$ dělí $f_1$ nebo $f_2$. Toto tvrzení odvodíme v několika následujících odstavcích.

**Důsledek.** *Je-li $\mathbb{K}$ obor integrity s jednoznačným rozkladem, pak také okruh polynomů $\mathbb{K}[x_1, \ldots, x_r]$ je obor integrity s jednoznačným rozkladem.*

Vidíme tedy, že každý polynom nad oborem integrity s jednoznačným rozkladem můžeme rozložit tak, jak to známe s polynomy s reálnými nebo komplexními koeficienty.

Zejména je tomu tedy tak pro polynomy nad jakýmkoliv polem skalárů.

**11.24. Lemma.**



*Nechť $\mathbb{K}$ je obor integrity s jednoznačným rozkladem. Pak platí:*
*(1) Jsou-li $a, b, c \in \mathbb{K}$, $a$ je nerozložitelné a $a|bc$, pak buď $a|b$ nebo $a|c$.*
*(2) Jestliže konstantní polynom $a \in \mathbb{K}[x]$ dělí $f \in \mathbb{K}[x]$ pak $a$ dělí všechny koeficienty polynomu $f$.*
*(3) Je-li $a$ nerozložitelný konstantní polynom v $\mathbb{K}[x]$ a $a|fg$, $f, g \in \mathbb{K}[x]$, pak $a|f$ nebo $a|g$.*

Důkaz. (1) Podle předpokladu $bc = ad$ pro vhodné $d \in \mathbb{K}$ a nechť $d = d_1 \ldots d_r$, $b = b_1 \ldots b_s$, $c = c_1 \ldots c_q$ jsou rozklady na nerozložitelné faktory. To znamená

$$ad_1 \ldots d_r = b_1 \ldots b_s c_1 \ldots c_q.$$

Z jednoznačnosti rozkladu $ad$ plyne $a = eb_j$ nebo $a = ec_i$ pro vhodnou jednotku $e$.

(2) Nechť $f = b_0 + b_1 x + \cdots + b_n x^n$. Protože $a|f$, jistě existuje polynom $g = c_0 + c_1 x + \ldots c_k x^k$ takový, že $f = ag$. Odtud okamžitě plyne $k = n, ac_0 = b_0, \ldots, ac_n = b_n$.

jsou jednotky právě všechny nenulové skaláry. Násobíme tak, abychom se v co největší míře vyhnuli počítání se zlomky.

$$\begin{aligned}
&2x^4+4x^3+6x^2+4x+2 : 2x^3+3x^2+3x+1 = x+\frac{1}{2}\\
&2x^4+3x^3+3x^2+x\\
&\qquad x^3+3x^2+3x+2\\
&\qquad x^3+\frac{3}{2}x^2+\frac{3}{2}x+\frac{1}{2}\\
&\qquad\qquad \frac{3}{2}x^2+\frac{3}{2}x+\frac{3}{2}
\end{aligned}$$

Dále dělíme polynom $2x^3+3x^2+3x+1$ zbytkem $\frac{3}{2}x^2+\frac{3}{2}x+\frac{3}{2}$ (pronásobeným jednotkou $\frac{2}{3}$)

$$\begin{aligned}
&2x^3+3x^2+3x+1 : x^2+x+1 = 2x+1\\
&2x^3+2x^2+2x\\
&\qquad x^2+x+1
\end{aligned}$$

Násobné kořeny původního polynomu jsou právě kořeny největšího společného dělitele tohoto polynomu se svojí derivací, tedy kořeny polynomu $x^2+x+1$. Tento má právě kořeny $-\frac{1}{2}\pm i\sqrt{3}/2$, které jsou dvojnásobnými kořeny původního polynomu. Rozklad polynomu nad $\mathbb{C}$ je tedy rozkladem na součin kořenových činitelů (tak je tomu podle základní věty algebry vždy):

$$\begin{aligned}
x^4+2x^3+3x^2+2x+1 &=\\
&= \left(x+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)^2\cdot\left(x+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^2.
\end{aligned}$$

Rozklad nad $\mathbb{R}$ pak dostaneme vynásobením kořenových závorek odpovídajících komplexně sdruženým kořenům polynomu (tento součin musí být polynom s reálnými koeficienty, ověřte!):

$$x^4+2x^3+3x^2+2x+1 = \left(x^2+x+1\right)^2.$$

- Řešme rovnici

$$x^4+2x^3+3x^2+2x+1=0.$$

Vydělením $x^2$ a substitucí $t=x+\frac{1}{x}$ dostáváme rovnici

$$t^2+2t+1=0$$

s dvojnásobným kořenem $-1$. Dosazením do substituce dostáváme již známou rovnici $x^2+x+1=0$ s výše uvedenými řešeními. □

**Poznámka.** Připomeňme na tomto místě známé tvrzení, že jedinými ireducibilními polynomy nad $\mathbb{R}$ jsou lineární polynomy a kvadratické

(3) Uvažujme $f,g\in\mathbb{K}[x]$ jako výše a předpokládejme, že $a$ nedělí ani $f$ ani $g$. Pak podle předchozího bodu existuje nějaké $i$ tak, že $a$ nedělí $b_i$, a nějaké $j$ tak, že $a$ nedělí $c_j$. Zvolme taková $i,j$ nejmenší možná. Koeficient u $x^{i+j}$ v polynomu $fg$ je $b_0c_{i+j}+b_1c_{i+j-1}+\cdots+b_{i+j}c_0$. Podle naší volby $a$ dělí všechny $b_0c_{i+j},\dots,b_{i-1}c_{j+1},b_{i+1}c_{j-1},\dots,b_{i+j}c_0$. Zároveň ale nedělí $b_ic_j$. Proto nemůže dělit celý koeficient. □

**11.25. Lemma.** *Uvažme podílové těleso $\mathbb{L}$ oboru integrity $\mathbb{K}$ s jednoznačným rozkladem. Je-li polynom $f$ nerozložitelný v $\mathbb{K}[x]$, je nerozložitelný také v $\mathbb{L}[x]$.*

Důkaz. Každý koeficient $a\in\mathbb{K}$ můžeme považovat za prvek $\frac{a}{1}\in\mathbb{L}$. Proto každý nenulový polynom $f\in\mathbb{K}[x]$ můžeme uvažovat jako polynom v $\mathbb{L}[x]$ .

Předpokládejme, že $f=g'h'$ pro vhodné $g',h'\in\mathbb{L}[x]$, kde polynomy $g',h'$ nejsou jednotky v $\mathbb{L}[x]$ (tzn. nejsou to konstantní polynomy, neboť $\mathbb{L}$ je pole). Nechť $a$ je společný násobek jmenovatelů koeficientů v $g'$ a $b$ je společný násobek jmenovatelů koeficientů v $h'$. Pak $bh',ag'\in\mathbb{K}[x]$ a platí $abf=(bh')(ag')$. Nechť $c$ je nerozložitelný faktor v rozkladu $ab$. Pak $c$ dělí $(bh')(ag')$, a proto $c$ dělí polynom $bh'$ nebo polynom $ag'$ (podle předchozího lemmatu). To ale znamená, že $c$ můžeme vykrátit. Po konečném počtu takových krácení zjistíme, že $f=gh$ pro polynomy $g,h\in\mathbb{K}[x]$. Přitom stupeň polynomů se neměnil, proto i $g$ a $h$ nejsou konstantní.

Tím jsme dokázali, že když je $f$ rozložitelné v $\mathbb{L}[x]$, je rozložitelné i v $\mathbb{K}[x]$ a odtud negací vyplývá i požadovaná implikace. □

**11.26. Lemma.** *Nechť $\mathbb{K}$ je obor integrity s jednoznačným rozkladem a $f,g,h\in\mathbb{K}[x]$. Předpokládejme, že $f$ je nerozložitelné a $f|gh$. Pak buď $f|g$ nebo $f|h$.*

Důkaz. Je-li $f$ konstantní polynom (tj. prvek v $\mathbb{K}$), pak jsme tvrzení již dokázali, viz jedno z předchozích lemmat.

Předpokládejme, že $\deg f>0$. Již víme, že $f$ je nerozložitelný také v $\mathbb{L}[x]$, kde $\mathbb{L}$ je podílové těleso okruhu $\mathbb{K}$. Předpokládejme tedy nejdříve, že $\mathbb{K}$ je pole (a je tedy rovno svému podílovému tělesu). Předpokládejme dále, že $f|gh$ a zároveň $f$ nedělí $g$. Ukážeme, že pak jistě $f|h$. Největší společný dělitel polynomů $g$ a $f$ musí být konstantní polynom v $\mathbb{L}$, proto existují $A,B\in\mathbb{L}[x]$ takové, že $1=Af+Bg$. Odtud $h=Afh+Bgh$, a protože $f|gh$, musí platit i $f|h$.

Vraťme se nyní k obecnému případu. Podle předchozího vyplývá z našich předpokladů, že $f|g$ nebo $f|h$ v okruhu polynomů $\mathbb{L}[x]$ nad podílovým tělesem $\mathbb{L}$ okruhu $\mathbb{K}$. Nechť např. $h=kf$ v $\mathbb{L}[x]$ a zvolme $a\in\mathbb{K}$ tak, aby $ak\in\mathbb{K}[x]$. Pak $ah=akf$ a pro každý nerozložitelný faktor $e\in a$ musí platit $e|ak$, protože $f$ je nerozložitelný a nekonstantní. Můžeme proto $e$ krátit. Po konečném počtu takových krácení je z $a$ jednotka, tzn. $h=k'f$ pro vhodné $k'\in\mathbb{K}[x]$. □

Důkaz tohoto lemmatu ukončil celý důkaz věty 11.23.

polynomy se záporným diskriminantem. Toto tvrzení vyplývá i z úvah v předchozím příkladě.

**11.76.** Rozložte polynom $x^5 + 3x^3 + 3$ na ireducibilní složky nad

i) $\mathbb{Q}$,

ii) $\mathbb{Z}_7$.

**Řešení.**

i) Podle Eisensteinova kriteria je daný polynom ireducibilní nad $\mathbb{Z}$ i $\mathbb{Q}$ (použijeme prvočíslo 3).

ii) $(x-1)^2(x^3+2x^2-x+3)$. Např. pomocí Hornerova schematu zjistíme dvojnásobný kořen 1. Po vydělení polynomem $(x-1)^2$ dostáváme polynom $(x^3+2x^2-x+3)$, který již nemá nad $\mathbb{Z}_7$ kořeny. Proto je ireducibilní (kdyby byl rozložitelný, musel by mít jeden faktor stupeň jedna, tedy $(x^3+2x^2-x+3)$ by musel mít kořen). □

**11.77.** Rozložte polynom $x^4 + 1$ nad

- $\mathbb{Z}_3$,
- $\mathbb{C}$,
- $\mathbb{R}$.

**Řešení.**

- $(x^2+x+2)(x^2+2x+2)$
- Kořeny jsou všechy čtvrté odmocniny z $-1$, ty leží v komplexní rovině na jednotkové kružnici a mají argumenty postupně $\pi/4$, $\pi/4+\pi/2$, $\pi/4+\pi$ a $\pi/4+3\pi/2$, jsou to tedy čísla $\pm\sqrt{2}/2 \pm i\sqrt{2}/2$. Rozklad tedy je

$$\left(x-\frac{\sqrt2}{2}-i\frac{\sqrt2}{2}\right)\left(x-\frac{\sqrt2}{2}+i\frac{\sqrt2}{2}\right)\left(x+\frac{\sqrt2}{2}-i\frac{\sqrt2}{2}\right)\left(x-\frac{\sqrt2}{2}+i\frac{\sqrt2}{2}\right).$$

- Vynásobením kořenových činitelů komplexně sdružených kořenů v rozkladu nad $\mathbb{C}$ dostáváme rozklad nad $\mathbb{R}$:

$$\left(x^2-\sqrt2 x+1\right)\left(x^2+\sqrt2 x+1\right)..$$ □

**11.78.** Nalezněte polynom s racionálními koeficienty a s co nejmenším stupněm, jehož kořenem je číslo $\sqrt[2007]{2}$.

**Řešení.** $P(x) = x^{2007} - 2$. Ukažme, že neexistuje polynom menšího stupně s kořenem $\sqrt[2007]{2}$. Buď totiž $Q(x)$ nenulový polynom nejmenšího stupně s kořenem $\sqrt[2007]{2}$. Pak $\operatorname{st} Q(x) \le 2007$. Vydělme $P(x)$ polynomem $Q(x)$ se zbytkem: $P(x) = Q(x)\cdot D(x) + R(x)$, kde $D(x)$ je neúplný podíl po dělení a $R(x)$ zbytek po dělení, $\operatorname{st} R(x) < \operatorname{st} Q(x)$, nebo $R(x) = 0$. Dosazením čísla $\sqrt[2007]{2}$ do poslední rovnice vidíme, že $\sqrt[2007]{2}$ je kořenem i polynomu $R(x)$, z definice polynomu $Q(x)$ musí být tedy $R(x)$ nulový polynom, tedy $Q(x)$ dělí $P(x)$. Polynom $P(x)$ je však ireducibilní (podle Eisensteinova kriteria), jeho jediným netriviálním dělitelem je on sám

### 3. Systémy polynomiálních rovnic



V praktických úlohách se často setkáváme s objekty nebo ději popsanými polynomy, resp. systémy polynomiálních rovnic.

Může jít o hledání příslušnosti bodu k nějakému tělesu, hledání extrémů na algebraicky popsaných podmnožinách mnohorozměrných prostorů, analýzu pohybů součástí nějakého stroje atd.

**11.27. Afinní variety.** Pro jednoduchost (existence kořenů polynomů) budeme pracovat zejména nad polem komplexních čísel, nicméně některé úvahy rozvineme pro obecné pole $\mathbb{K}$.

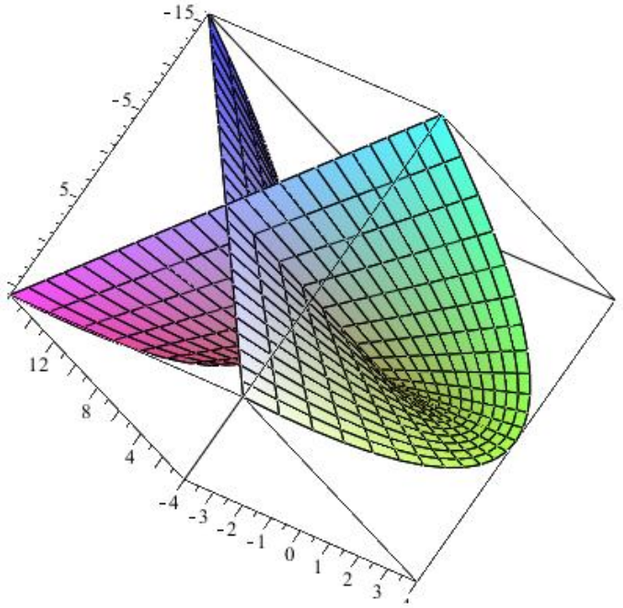
Afinním $n$-rozměrným prostorem nad polem $\mathbb{K}$ rozumíme $\mathbb{K}^n = \underbrace{\mathbb{K}\times\cdots\times\mathbb{K}}_{n}$ se standardní afinní strukturou, viz začátek čtvrté kapitoly.

Jak jsme již viděli, polynom $f = \sum_\alpha a_\alpha x^\alpha \in \mathbb{K}[x_1,\dots,x_n]$ lze přirozeným způsobem chápat jako zobrazení $f\colon \mathbb{K}^n \to \mathbb{K}$ definované

$$f(u_1,\dots,u_n) := \sum_\alpha a_\alpha u^\alpha, \text{ kde } u^\alpha = u_1^{\alpha_1}\cdots u_n^{\alpha_n}.$$

V dimenzi $n = 1$ popisuje rovnost $f(x) = 0$ jen nejvýše konečně mnoho bodů v $\mathbb{K}$. Ve vyšší dimenzi bude rovnost $f(x_1,\dots,x_n)$ popisovat podmnožiny podobné, jako jsou křivky v rovině nebo plochy v trojrozměrném prostoru, mohou ale mít docela složité a samoprotínající se tvary.

Např. množina zadaná rovnicí $(x^2+y^2)^3 - 4x^2y^2 = 0$ vypadá jako čtyřlístek. Pěkný obrázek dvourozměrné plochy dává tzv. Whitneyho deštník $x^2 - y^2 z = 0$, který kromě znázorněné části na obrázku obsahuje také celou přímku $\{x = 0, y = 0\}$.




Obrázek byl vykreslen s pomocí parametrického popisu $x = uv$, $y = v$, $z = u^2$, ze kterého nejspíš snadno uhádneme i implicitní popis $x^2 - y^2 z = 0$.

Další obrázek ukazuje tzv. Enneperovu plochu s parametrizací $x = 3u + 3uv^2 - u^3$, $y = 3v + 3u^2 v - v^3$, $z = 3u^2 - 3v^2$.

(až na násobení jednotkou okruhu polynomů nad $\mathbb{Q}$, tedy racionální konstantou), je tedy $Q(x) = P(x)$ (opět až na pronásobení jednotkou). Například polynom $\frac{1}{3}x^{2007} - \frac{2}{3}$ také splňuje podmínky zadání. Normovaný polynom splňující tyto podmínky je však již jediný a je to polynom $P(x)$. □

**11.79.** Najděte všechny ireducibilní polynomy stupně nejvýše 2 nad $\mathbb{Z}_3$.

**Řešení.** Nerozložitelné jsou z definice všechny lineární mnohočleny. Nerozložitelné polynomy stupně dva dostaneme tak, že z množiny všech polynomů stupně 2 nad $\mathbb{Z}_3$ „vyškrtáme“ rozložitelné polynomy, tedy násobky dvojic lineáních polynomů. Reducibilní polynomy stupně dva jsou tedy: $(x+1)^2 = x^2+2x+1$, $(x+2)^2 = x^2+x+1$, $(x+1)(x+2) = x^2+2, x^2, x(x+1) = x^2+x, x(x+2) = x^2+2x$. Stačí uvažovat pouze normované polynomy, ostatní z nich dostaneme násobením dvojkou (rozmysli). Celkem normované ireducibilní polynomy stupně 2 nad $\mathbb{Z}_3$ jsou $x^2+2x+2, x^2+x+2, x^2+1$. □

**11.80.** Rozhodněte, zda je následující polynom nad $\mathbb{Z}_3$ ireducibilní, případně nalezněte jeho rozklad:

$$x^4 + x^3 + x + 2.$$

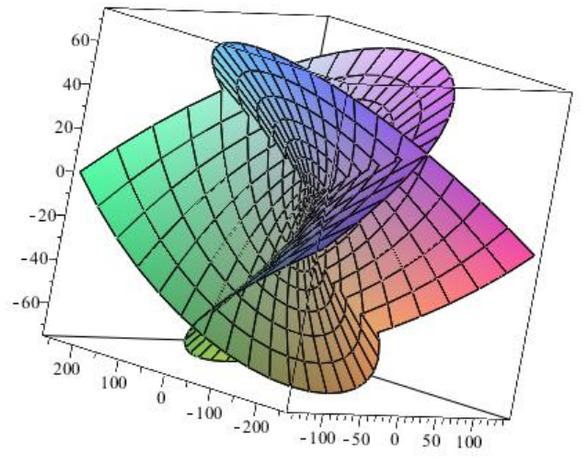
**Řešení.** Dosazením čísel 0, 1, 2 zjistíme, že daný polynom nemá v $\mathbb{Z}_3$ kořen. Je tedy buď ireducibilní nebo je součinem dvou polynomů stupně 2. Vzhledem k tomu, že daný polynom je normovaný, tak je-li součinem nějakých dvou polynomů stupně dva, je součinem i normovaných polynomů stupně dva (po případném pronásobení obou polynomů dvojkou). Hledejme tedy konstanty $a, b, c, d \in \mathbb{Z}_3$ tak, aby

$$\begin{aligned} x^4 + x^3 + x + 2 &= (x^2 + ax + b)(x^2 + cx + d) = \\ &= x^4 + (a+c)x^3 + (ac + b + d)x^2 + \\ &\quad + (ad + bc)x + bd. \end{aligned}$$

Porovnáním koeficientů u jednotlivých mocnin $x$ dostáváme soustavu čtyř rovnic o čtyřech neznámých:

$$\begin{aligned} 1 &= a + c, \\ 0 &= ac + b + d, \\ 1 &= ad + bc, \\ 2 &= bd. \end{aligned}$$

Z poslední rovnice je jedno z čísel $b, d$ rovno jedné, druhé pak dvěma, vzhledem k symetrii soustavy vůči dvojicím $(a, b)$ a $(c, d)$ můžeme zvolit například $b = 1$, $d = 2$. Z druhé rovnice potom $ac = 0$, tedy jedno z čísel $a, c$ je nula, z první rovnice je pak druhé z nich jednička. Ze třetí rovnice $2a + c = 1$, je tedy $a = 0$, $c = 1$. Celkem






Těžko si představit, jak z této parametrizace dopočítat ručně implicitní popis, přesto to budeme umět algoritmicky zvládnout eliminací proměnných $u$ a $v$ z těchto tří rovnic.

Budeme k tomu ale muset vybudovat docela složitou teorii. Začneme jako obvykle formalizací objektů.

### Afinní variety

Nechť $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. *Afinní varietou* v $\mathbb{K}^n$ určenou polynomy $f_1, \ldots, f_n$ nazveme množinu

$$\begin{aligned} &\mathfrak{V}(f_1, \ldots, f_s) = \\ &= \{(a_1, \ldots, a_n) \in \mathbb{K}^n;\ f_i(a_1, \ldots, a_n) = 0, i = 1, \ldots, s\} \end{aligned}$$

Afinní variety jsou například všechny kuželosečky, kvadriky a nadkvadriky singulární i regulární. Mnoho pěkných křivek či ploch můžeme snadno popsat jako afinní variety.

Varieta určená více polynomy je pak průnik variet zadaných jednotlivými polynomy. Tedy například $\mathfrak{V}(x^2+y^2-1, z)$ je kružnice se středem $(0,0,0)$ a poloměrem jedna ležící v rovině $xy$.

Podobně $\mathfrak{V}(xz, yz)$ je sjednocení přímky $x = 0$, $y = 0$ a roviny $z = 0$, protože právě pro body těchto dvou útvarů jsou oba polynomy $xz$, $yz$ nulové.

Vidíme na těchto příkladech, že není lehké se vypořádat s pojmem dimenze. Stačí zmíněná přímka navíc k rovině, aby naše varieta byla třírozměrná, nebo ji ještě budeme považovat za dvojrozměrnou s jistou anomálií?

Následující přímočaré tvrzení si ověřte samostatně:

**Věta.** *Nechť $V = \mathfrak{V}(f_1, \ldots, f_s)$, $W = \mathfrak{V}(g_1, \ldots, g_t) \subseteq \mathbb{K}^n$ jsou afinní variety. Potom i $V \cup W$ a $V \cap W$ jsou afinní variety a platí*

$$\begin{aligned} V \cap W &= \mathfrak{V}(f_1, \ldots, f_s, g_1, \ldots, g_t), \\ V \cup W &= \mathfrak{V}(f_i g_j) \quad \textit{pro } 1 \le i \le s,\ 1 \le j \le t. \end{aligned}$$

V následujících odstavcích se mimo jiné pokusíme zodpovědět otázky, které se v souvislosti s varietami bezprostředně nabízejí.

A. Platí $\mathfrak{V}(f_1, \ldots, f_s) = \emptyset$?

B. Je $\mathfrak{V}(f_1, \ldots, f_s)$ konečná množina?

$$x^4 + x^3 + x + 2 = (x^2 + 1)(x^2 + x + 2).$$ □

**11.81.** Pro libovolné liché prvočíslo $p$ určete všechny kořeny polynomu

$$P(x) = x^{p-2} + x^{p-3} + \cdots + x + 2$$

v tělese $\mathbb{Z}_p$.

**Řešení.** Vzhledem k rovnosti

$$x^{p-1} - 1 = (x - 1)(P(x) - 1)$$

jsou všechna čísla ze $\mathbb{Z}_p$ kromě jedničky kořeny $P(x) - 1$, nemohou tedy být kořeny $P(x) + 1$. Jednička je kořenem triviálně vždy, je to tedy jediný kořen. □

**11.82.** Rozložte polynom $p(x) = x^2 + x + 1$ v $\mathbb{Z}_5[x]$ a $\mathbb{Z}_7[x]$.

**Řešení.** V $\mathbb{Z}_5[x]$ je ireducibilní, v $\mathbb{Z}_7[x]$ je $p(x) = (x - 2)(x - 4)$. □

**11.83.** Rozložte polynom $p(x) = x^6 - x^4 - 5x^2 - 3$ v $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_7[x]$ víte-li o něm, že má vícenásobný kořen.

**Řešení.** Euklidovým algoritmem zjistíme, že největší společný dělitel $p$ a derivace $p'$ je $x^2 + 1$. Dvojnásobným vydělěním polynomu $p(x)$ tímto faktorem zjistíme, že

$$p(x) = (x^2 + 1)^2(x^2 - 3).$$

Tyto faktory jsou zřejmě ireducibilní v okruzích $\mathbb{Q}[x]$ a $\mathbb{Z}[x]$.

V $\mathbb{C}[x]$ můžeme polynom vždy rozložit na lineární činitele, v tomto případě stačí rozložit faktor $x^2 + 1$, ale to je snadné $x^2 + 1 = (x + i)(x - 1)$. Faktor $x^2 - 3$ je roven $(x - \sqrt{3})(x + \sqrt{3})$ dokonce v $\mathbb{R}[x]$. V okruhu $\mathbb{C}[x]$ je tedy

$$p(x) = (x + i)^2(x - i)^2\left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right)$$

a v $\mathbb{R}[x]$ je

$$p(x) = (x^2 + 1)^2\left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right).$$

V $\mathbb{Z}_5[x]$ má polynom $x^2 + 1$ kořeny $\pm 2$ a polynom $x^2 - 3$ nemá žádné, a proto

$$p(x) = (x - 2)^2(x + 2)^2(x^2 - 3).$$

V $\mathbb{Z}_7[x]$ nemá kořen ani jeden z těchto polynomů, a proto rozklad na ireducibilní faktory je totožný s rozkladem v $\mathbb{Q}[x]$ a $\mathbb{Z}[x]$.

$$p(x) = (x^2 + 1)^2(x^2 - 3).$$ □

C. Jak lze chápat pojem dimenze v případě variet?

Všechny tyto problémy lze „rozumně“ řešit pro variety v oboru komplexních čísel (resp. pro všechna algebraicky uzavřená pole), pro čísla reálná je to komplikovanější a prakticky nemožné je to pro obecná pole. Například pro racionální čísla je ověření tvrzení $\mathfrak{V}(x^n + y^n - z^n) = \emptyset$ známo jako tzv. velká Fermatova věta, mnohokrát zmiňovaná v kapitole desáté.

**11.28. Parametrizace.** Pro některé ryze praktické operace s varietami je vhodné používat implicitní reprezentaci (tedy až dosud používané vyjádření). Např. zjištění, zda daný bod patří do variety, resp. do určité části prostoru jí vymezené, je při implicitním popisu docela snadné. Jindy je naopak daleko užitečnější vyjádření parametrické (např. jsme jej již použili při kreslení obrázků).

Varieta $\mathfrak{V}(x + y + z - 1, x + 2y - z - 3)$ je přímka (průnik dvou rovin). Řešíme-li systém

$$\begin{aligned} x &+ y + z - 1 = 0,\\ x &+ 2y - z - 3 = 0, \end{aligned}$$

dostaneme přímo parametrické vyjádření této přímky

$$\begin{aligned} x &= -1 - 3t,\\ y &= 2 - 2t,\\ z &= t. \end{aligned}$$

### Racionální parametrizace

**Definice.** *Racionální parametrickou reprezentací* variety $\mathfrak{V}(f_1, \ldots, f_r) \subseteq \mathbb{K}^n$ rozumíme racionální funkce $r_1, \ldots, r_n \in \mathbb{K}(t_1, \ldots, t_s)$ splňující následující podmínky

- je-li $x_i = r_i(t_1, \ldots, t_s)$ pro $i = 1, 2, \ldots, n$, pak $(x_1, \ldots, x_n) \in \mathfrak{V}(f_1, \ldots, f_r)$ pro libovolná $t_1, \ldots, t_s$;
- $\mathfrak{V}(f_1, \ldots, f_r)$ je minimální afinní varieta obsahující takto dané body $(x_1, \ldots, x_n)$.

Všimněme si, že při parametrizaci nepožadujeme popis všech bodů variety. To je podstatné, jak je vidět i na jednoduchém příkladu parametrizace kružnice v rovině,

$$x = \frac{2t}{1 + t^2},\ y = \frac{-1 + t^2}{1 + t^2},$$

kterou obdržíme tzv. stereografickou projekcí. (Ověřte si detailně!) Všimněme si, že skutečně dostaneme parametrizací všechny body, kromě bodu $(0, 1)$, ze kterého promítáme. Ten totiž není dosažitelný pro žádnou hodnotu parametru $t$. To není způsobeno naší nešikovností, z rozdílných topologických vlastností přímky a kružnice totiž vyplývá, že globální bijektivní racionální parametrizace existovat nemůže.

V této souvislosti se nabízí další otázky.

D. Existuje parametrizace dané variety, resp. lze ji nalézt?

E. Naopak umíme k parametricky zadané varietě najít její implicitní popis?

Obecná odpověď na otázku D je obecně záporná. V podstatě lze tvrdit, že většinu afinních variet parametrizovat nelze, respektive neexistuje algoritmus parametrizace implicitního popisu.

**11.84.** O polynomu $p = x^6 + x^5 + 4x^4 + 2x^3 + 5x^2 + x + 2$ víte, že má vícenásobný kořen $x = i$. Rozložte jej na ireducibilní polynomy v $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_2[x]$, $\mathbb{Z}_5[x]$ a $\mathbb{Z}_7[x]$. Polynom $q = x^2y^2 + y^2 + xy + x^2y + 2y + 1$ vydělte se zbytkem ireducibilními faktory polynomu $p$ v $\mathbb{R}[x]$ a výsledek využijte k vyřešení soustavy polynomiálních rovnic $p = q = 0$ nad $\mathbb{C}$.

**Řešení.** $p = (x^2+1)^2(x^2+x+2)$, v $\mathbb{Z}_2$: $p = x(x+1)^5$, v $\mathbb{Z}_5$: $p = (x-2)^2(x+2)^2(x^2+x+2)$, v $\mathbb{Z}_7$: $p = (x^2+1)^2(x+4)^2$. Pro druhý polynom dostáváme $q = (y^2+y)(x^2+x+2) - y^2(x+1) + 1$ a $q = (y^2+y)(x^2+1) + y(x+1) + 1$. Je-li tedy $x = \alpha$ kořenem $x^2 + x + 2$, tj. $\alpha = -\frac{1}{2} \pm \frac{1}{2}i\sqrt{7}$, pak je $y = \frac{1}{\sqrt{1+\alpha}}$. Pokud $x = \beta$ je kořenem faktoru $x^2 + 1$, tj. $\beta = \pm i$, pak je $y = -\frac{1}{1+\beta}$ □

*11.85.* Rozložte na ireducibilní faktory $\mathbb{R}[x]$ a poté v $\mathbb{C}[x]$ polynom

$$4x^5 - 8x^4 + 9x^3 - 7x^2 + 3x - 1.$$

○

*11.86.* Rozložte na ireducibilní faktory v $\mathbb{R}[x]$ a poté v $\mathbb{C}[x]$ polynom

$$x^5 + 3x^4 + 7x^3 + 9x^2 + 8x + 4.$$

○

*11.87.* Rozložte polynom $x^4 - 4x^3 + 10x^2 - 12x + 9$ nad $\mathbb{R}$ a nad $\mathbb{C}$.

○

*11.88.* Rozhodněte, zda je následující polynom nad $\mathbb{Z}_3$ ireducibilní, případně nalezněte jeho rozklad na ireducibilní faktory:

$$x^5 + x^2 + 2x + 1.$$

○

*11.89.* Rozhodněte, zda je následující polynom nad $\mathbb{Z}_3$ ireducibilní, případně nalezněte jeho rozklad:

$$x^4 + 2x^3 + 2.$$

○

**11.90.** Určete všechny normované ireducibilní polynomy stupně 2 nad $\mathbb{Z}_5$.

**Řešení.** Polynomy určíme vylučovací metodou. Ze všech polynomů stupně dva nad $\mathbb{Z}_5$ vyloučíme všechny, které nejsou ireducibilní, tedy mají kořen.

$x^2 \pm 2, x^2 \pm x + 2, x^2 \pm 2x - 2, x^2 - x \pm 1, x^2 \pm 2x - 1.$ □

Na první pohled je zřejmé, že pro jednu a tutéž varietu existuje více implicitních, případně i parametrických popisů. Nejednoznačnosti implicitního jsou způsobeny reprezentací pomocí několika „generujících" polynomů a zjevně máme velikou volnost v jejich volbě.

**11.29. Ideály.** Abychom se vyhnuli závislosti na jednotlivých zvolených rovnicích zadávajících varietu, budeme chtít uvažovat i všechny důsledky zadaných rovnic. To vede na následující algebraický pojem:



IDEÁLY

**Definice.** Množinu $I \subseteq \mathbb{K}$, kde $\mathbb{K}$ je komutativní okruh, nazveme *ideálem*, platí-li $0 \in I$ a zároveň

$$f, g \in I \implies f + g \in I,$$
$$f \in I, h \in \mathbb{K} \implies f \cdot h \in I.$$

Ideály můžeme *generovat* podmnožinami, budeme používat značení $I = \langle a_1, \ldots, a_n \rangle$. Tím máme na mysli

$$I = \Big\{ \sum_i a_i b_i,\ b_i \in \mathbb{K} \Big\}.$$

Množina generátorů může být také nekonečná. Je-li generátorů jen konečný počet, říkáme, že ideál je *konečně generovaný*.

IDEÁL VARIETY

Pro varietu $V = \mathfrak{V}(f_1, \ldots, f_s)$ klademe

$$\mathfrak{I}(V) := \big\{ f \in \mathbb{K}[x_1, \ldots, x_n];\ f(a_1, \ldots, a_n) = 0, \forall\, (a_1, \ldots, a_n) \in V \big\}.$$

**Lemma.** *Nechť $f_1, \ldots, f_s, g_1, \ldots, g_t \in \mathbb{K}[x_1, \ldots, x_n]$ jsou polynomy. Pak platí*

*(1) jestliže $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, pak $\mathfrak{V}(f_1, \ldots, f_s) = \mathfrak{V}(g_1, \ldots, g_t)$;*

*(2) $\mathfrak{I}(V)$ je ideál a platí $\langle f_1, \ldots, f_s \rangle \subseteq \mathfrak{I}(V)$, kde $V = \mathfrak{V}(f_1, \ldots, f_s)$.*

DŮKAZ. Jestliže nějaký bod $(a_1, \ldots, a_n)$ patří varietě $\mathfrak{V}(f_1, \ldots, f_s)$, v tomto bodě se jistě nuluje i jakýkoliv polynom

$$f = h_1 f_1 + \cdots + h_s f_s,$$

tj. libovolný prvek ideálu $I = \langle f_1, \ldots, f_s \rangle$. Proto se v něm dle předpokladu nulují i všechny polynomy $g_i$. Ověřili jsme tedy

$$\mathfrak{V}(f_1, \ldots, f_s) \subseteq \mathfrak{V}(g_1, \ldots, g_t).$$

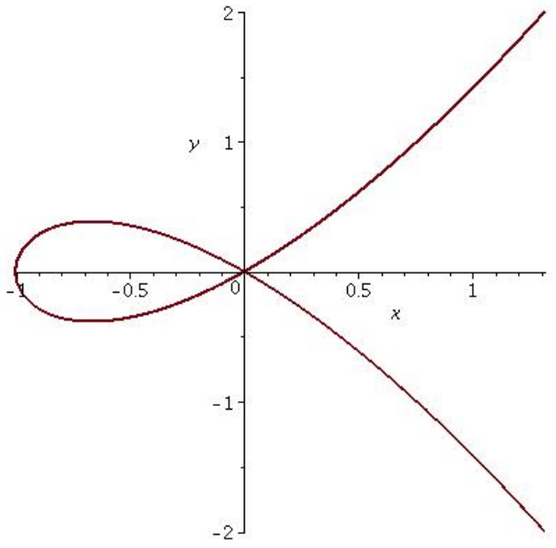
Opačná inkluze se dokáže stejně.

Abychom ověřili druhé tvrzení, zvolme $g, g' \in \mathfrak{I}(V)$, $h \in \mathbb{K}[x_1, \ldots, x_n]$. Pak zjevně pro každý bod $a \in V$

$$(gh)(a) = 0 \Rightarrow gh \in \mathfrak{I}(V),$$
$$(g + g')(a) = 0 \Rightarrow g + g' \in \mathfrak{I}(V).$$

Je tedy $\mathfrak{I}(V)$ ideál v $\mathbb{K}[x_1, \ldots, x_n]$.

Pro libovolný $f = h_1 f_1 + \cdots + h_s f_s \in \langle f_1, \ldots, f_s \rangle$ a bod $a \in V$ je samozřejmě také $f(a) = 0$, což ověřuje i dokazovanou inkluzi. □




OBRÁZEK 1. $\mathfrak{V}(x^3+x^2-y^2)$

### F. Okruh polynomů více proměnných

**11.91.** Určete zbytek polynomu $x^3y+x+yz+yz^4$ vůči bázi $(x^2y+z, y+z)$ a uspořádání $<_{\text{lex}}, <_{\text{grlex}}$.

**Řešení.** □

Pro představu si uveďme příklady některých variet zadaných polynomy.

**11.92. Křivky v afinní rovině $\mathbb{R}^2$.** Každý nenulový polynom $f(x,y)$ ve dvou proměnných zadává „křivku" v $\mathbb{R}^2$ rovnicí $f(x,y)=0$. Jde tedy o množinu nulových bodů jednoho polynomu $f$, budeme ji značit $K=\mathcal{V}(f)$. Odvoďte si, že je-li $f=f_1\dots f_k$, pak $\mathcal{V}(f)=\mathcal{V}(f_1)\cup\dots\cup\mathcal{V}(f_k)$.

Příklady takto zadaných křivek jsou vedeny na následujících obrázcích.

**11.93.** Pomocí Vašeho oblíbeného výpočetního programu zakreslete v rovině křivku zadanou rovnicí $x^3+x^2-y^2=0$.

**Řešení.** Viz obrázek 1. □

**11.94.** Pomocí Vašeho oblíbeného výpočetního programu zakreslete v rovině křivku zadanou rovnicí $2x^4-3x^2y+y^2-2y^3+y^4=0$.

**Řešení.** Viz obrázek 2. □

Křivky se můžeme pokusit zadat rovnicemi $x=f(t)$, $y=g(t)$, kde $f,g\in\mathbb{R}[t]$. Křivka je pak zadaná jako „polynomiální vložení" reálné přímky do roviny.

Nejjednodušší příklady jsou triviální variety – jeden bod a celý afinní prostor:

$$\mathfrak{I}\big(\{(0,0,\dots,0)\}\big)=\langle x_1,\dots,x_n\rangle,$$
$$\mathfrak{I}(\mathbb{K}^n)=\{0\}\quad\text{pro libovolné nekonečné pole }\mathbb{K}.$$

Inkluze opačná k druhé části věty obecně neplatí. Například varieta $\mathfrak{V}(x^2,y^2)$ má jediný bod – $(0,0)$. $\mathfrak{I}(V)$ je potom $\langle x,y\rangle\supset\langle x^2,y^2\rangle$.

Jsou-li $V,W\subseteq\mathbb{K}^n$ variety, pak platí

$$V\subseteq W\implies\mathfrak{I}(V)\supseteq\mathfrak{I}(W).$$

Neboli polynomy, které se nulovaly na nějaké varietě, se nutně musí nulovat i na její podmnožině.

Můžeme hned formulovat další přirozené problémy:

F. Je každý ideál $I\in\mathbb{K}[x_1,\dots,x_n]$ konečně generovaný?
G. Lze algoritmicky zjistit, zda $f\in\langle f_1,\dots,f_s\rangle$?
H. Jaký je přesný vztah mezi $\langle f_1,\dots,f_s\rangle$ a $\mathfrak{I}\big(\mathfrak{V}(f_1,\dots,f_s)\big)$?

**11.30. Dimenze 1.** Podívejme se na polynomy v jedné proměnné $x$

$$f=a_0x^n+a_1x^{n-1}+\dots+a_n,\quad\text{kde } a_0\neq 0.$$

Vedoucí člen polynomu definujeme jako $LT(f):=a_0x^n$ (označení pochází z anglického „leading term"). Zřejmě platí

$$\deg f\le\deg g\iff LT(f)|LT(g).$$

Nechť $\mathbb{K}$ je pole a $g$ nenulový polynomu. Víme, že každý polynom $f\in\mathbb{K}[x]$ lze jednoznačně psát jako

$$f=q\cdot g+r,\quad\text{kde } r=0\text{ nebo }\deg r<\deg g.$$

Jde ve skutečnosti o algoritmický postup, podíl $q$ a zbytek $r$ počítá následující algoritmus:

(1) $q:=0, r:=f$
(2) `while` $r\neq 0\wedge LT(g)|LT(r)$
  (a) $q:=q+LT(r)/LT(g)$
  (b) $r:=r-LT(r)/LT(g)\cdot g$

Pro průchod cyklem platí invariant $f=q\cdot g+r$, algoritmus tedy dává správný výsledek, pokud se zastaví. Stupeň $r$ se každým průchodem zmenšuje, proto k zastavení nutně dojde.

**Důsledek.** *Nechť $\mathbb{K}$ je pole. Pak každý ideál v okruhu polynomů $\mathbb{K}[x]$ je tvaru $\langle f\rangle$.*

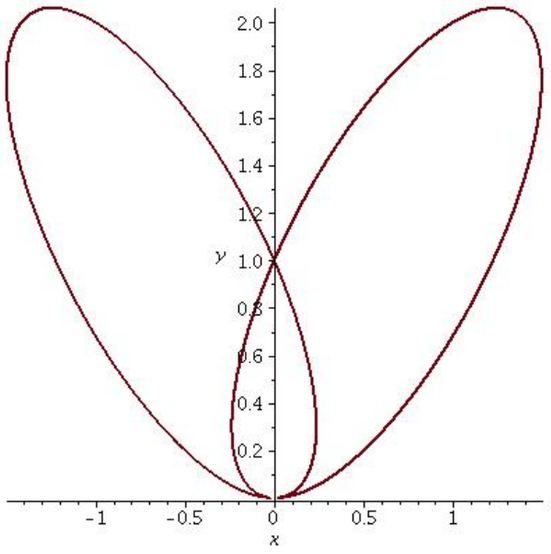
DŮKAZ. Uvažme jakýkoliv ideál $I\subseteq\mathbb{K}[x]$. Je-li $I=\{0\}$, pak je generován nulovým polynomem. Jestliže $I$ obsahuje nenulový polynom $f$, pak jistě obsahuje i polynom $f$ minimálního stupně. Jistě je pak $\langle f\rangle\subseteq I$.

Pro jakýkoliv jiný polynom $g\in I$ spočteme výsledek dělení se zbytkem, tj. $g=qf+r$. Zjevně je tedy $qf\in I$, a proto i $r\in I$. Stupeň $f$ byl ale minimální, takže nutně $r=0$. Je tedy i $g\in I$ a $I=\langle f\rangle$. □

Ideály generované jediným prvkem se nazývají *hlavní ideály*. Okruhům, které mají vlastnost z posledního lemmatu, říkáme *okruh hlavních ideálů*.

Největší společný dělitel $h=GCD(f,g)$ polynomů $f$ a $g$ lze opět spočítat algoritmicky (největší společný dělitel bude v proměnné $h$ v okamžiku zastavení algoritmu):

(1) $h:=f, s:=g$
(2) `while` $s\neq 0$
  (a) $r:=$ zbytek po dělení $h/s$




Obrázek 2. $\mathfrak{V}(2x^4 - 3x^2y + y^2 - 2y^3 + y^4)$

**11.95.** Parametrizujte křivku (varietu) $\mathfrak{V}(x^3 + x^2 - y^2)$.

**Řešení.** Parametrizaci odvodíme výpočtem průniků přímek $y = tx$ s danou křivkou, tj parametrizujeme směrnicí těchto přímek. Technicky to znamená, že za $y$ dosazujeme $tx$ a z rovnice vyjádříme $x$ pomocí $t$:

$$x^3 + x^2 - t^2x^2 = x^2(x + 1 - t) \implies x = t - 1 \vee x = 0.$$

Potom $y = t^2(t - 1)$, nebo pro $x = 0$ je jediným vyhovujícím bodem na křivce $y = 0$. Bod $[0, 0]$ lze získat volbou $t = 1$ z uvedené parametrizace, stačí tedy uvažovat pouze tuto parametrizaci. □

O něco více křivek obdržíme, když budeme v parametrizaci uvažovat podíly polynomů $f = \frac{f_1}{f_2}$, $g = \frac{g_1}{g_2}$. Hovoříme pak o racionální parametrizaci.

**11.96.** Odvoďte parametrizaci kružnice pomocí stereografické projekce (viz obrázek)

(b) $h := s$
(c) $s := r$

Nechť $f = q \cdot g + r$ a $h = GCD(f, g)$. Potom $h|r, g$ a zároveň

$$\forall p \in \mathbb{K}[x]\colon\ p|r, g, \quad \text{tedy } p|f \text{ a } p|h.$$

Odtud $h$ je $GCD(r, g)$. Triviálně $GCD(h, 0) = h$, proto algoritmus počítá správně $GCD(f, g)$. Protože stupně $r$ postupně klesají, algoritmus se nutně zastaví.

Největší společný dělitel dvou polynomů tedy existuje. Je určen jednoznačně až na násobek skalárem. Dva různé $GCD$ se totiž musí dělit navzájem a to je u polynomů možné právě v tomto případě.

Největšího společného dělitele více než dvou polynomů definujeme takto: Je-li $s > 2$, potom

$$GCD(f_1, \ldots, f_s) := GCD\big(f_1, GCD(f_2, \ldots, f_s)\big).$$

**Lemma.** *Pro polynomy* $f_1, \ldots, f_s$ *platí* $\langle GCD(f_1, \ldots, f_s)\rangle = \langle f_1, \ldots, f_s\rangle$.

Důkaz. $GCD(f_1, \ldots, f_s)$ dělí všechny polynomy $f_i$. Je tedy hlavní ideál $\langle GCD(f_1, \ldots, f_s)\rangle$ obsažen v ideálu $\langle f_1, \ldots, f_s\rangle$. Naopak z Bezoutovy rovnosti okamžitě plyne inkluze opačná. □

Položili jsme několik otázek. Tady jsou odpovědi pro dimenzi 1:

- Protože $\mathfrak{V}(f_1, \ldots, f_s) = \mathfrak{V}(GCD(f_1, \ldots, f_s))$, problém prázdnosti variety se redukuje na problém existence kořene polynomu.
- Ze stejného důvodu je varieta vždy konečnou množinou izolovaných bodů – kořenů $GCD(f_1, \ldots, f_s)$ s jedinou výjimkou, kdy $GCD(f_1, \ldots, f_s) = 0$; to nastane pouze v případě, že $f_1 = f_2 = \cdots = f_s = 0$. Pak je varietou celá množina $\mathbb{K}$.
- Pojem dimenze v tomto případě postrádá smysl, všechny variety mají coby diskrétní množiny bodů dimenzi nulovou.
- Každý ideál je generovatelný jediným polynomem.
- $f \in \langle f_1, \ldots, f_s\rangle \iff GCD(f_1, \ldots, f_s)|f$.
- Označíme-li $\langle f\rangle := \mathfrak{I}(\mathfrak{V}(f_1, \ldots, f_s))$, pak $f$ a $GCD(f_1, \ldots, f_s)$ se mohou lišit pouze násobností kořenů.

**11.31. Monomiální uspořádání.** Abychom mohli zobecnit dělení polynomů se zbytkem pro polynomy více proměnných, najdeme nejprve dobrý ekvivalent pojmů stupeň polynomu a vedoucí člen polynomu.



Dělením se zbytkem polynomu $f \in \mathbb{K}[x_1, \ldots, x_n]$ polynomy $g_1, \ldots, g_s$ chceme rozumět vyjádření

$$f = a_1g_1 + \cdots + a_sg_s + r,$$

kde žádný člen zbytku $r$ nebude dělitelný některým z vedoucích členů $LT\, g_i$.

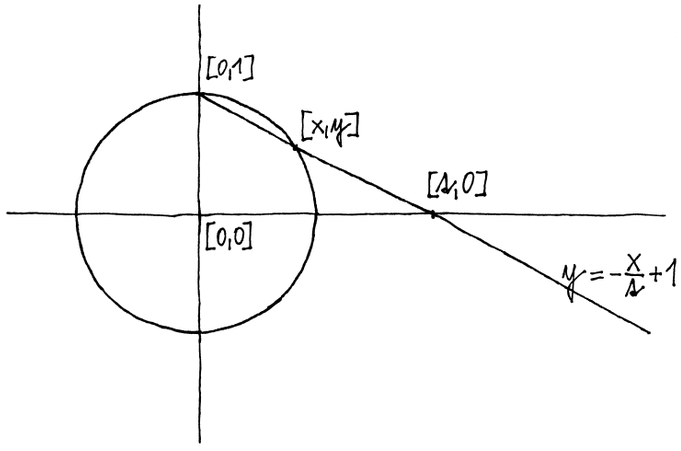
Zkusme to s $f = x^2y + xy^2 + y^2$, $g_1 = xy - 1$ a $g_2 = y^2 - 1$. Prvním dělením získáme

$$f = (x + y) \cdot g_1 + (x + y^2 + y).$$

$LT(y^2 - 1)$ nedělí $x$ (vedoucí člen zbytku), a tak bychom teoreticky nemohli pokračovat dál.

Přesuneme-li však toto $x$ do zbytku, dostáváme teprve výsledek

$$f = (x + y) \cdot g_1 + g_2 + (x + y + 1).$$




**Řešení.** Dosazením rovnice přímky $y = \frac{x}{t} + 1$ do rovnice kružnice, dostáváme rovnici

$$x^2 + \left(\frac{x^2}{t^2} - \frac{2x}{t} + \right) = 1,$$

s řešením $x = 0$ nebo parametrickým vyjádřením

$$x = \frac{2t}{1+t^2},\ y = \frac{t^2-1}{1+t^2},$$

které však nepostihuje bod [0, 1]. □

**Poznámka.** Všimněme si, že tentokrát vložení reálné přímky dá pouze „skoro všechny body“ parametrizované variety, jeden z nich (tj. bod, z kterého promítáme) totiž není dosažitelný pro žádnou hodnotu parametru $t$. To není způsobeno naší nešikovností, z rozdílných topologických vlastností přímky a kružnice totiž vyplývá, že globální parametrizace existovat nemůže.

**Poznámka.** Protože $\mathbb{R}$ není algebraicky uzavřené pole, máme problémy s existencí kořenů polynomů. V důsledku toho se při malé změně koeficientů zadávající rovnice může drasticky změnit výsledná varieta. Nabízí se pracovat s komplexními polynomy v $\mathbb{C}[x, y]$ a jimi zadanými podmnožinami v $\mathbb{C}^2$. To nás nemusí nijak děsit, naopak naše původně reálné křivky jsou obsaženy ve svých „komplexifikacích“ (reálné polynomy prostě chápeme jako komplexní, které mají náhodou reálné koeficienty) a pouze získáváme bohatější nástroje pro popis jejich vlastností (imaginární tečny apod.).

Dále nám chybí „nevlastní body“. Např. při parametrizaci kružnice můžeme chybějící bod popsat jako obraz jediného nevlastního bodu reálné přímky, tj. bodu v „nekonečnu“. Těchto problémů se nejlépe zbavíme tím, že budeme pracovat v tzv. projektivním rozšíření (reálné nebo komplexní) roviny.

Projektivní rozšíření je výhodné používat v celé řadě problémů, jeho využití také uvidíme při definici grupové operace na bodech eliptické křivky, viz ||H||.

Zde již žádný člen zbytku není dělitelný žádným z $LT(g_1)$, $LT(g_2)$.

Jak jsme ale vlastně určovali vedoucí členy?

### Uspořádání monomů

Úplné (lineární) dobré (tj. každá neprázdná podmnožina má nejmenší prvek) uspořádání $<$ na $\mathbb{N}^n$ splňující

$$\forall \alpha, \beta, \gamma \in \mathbb{Z}^n : \alpha < \beta \implies \alpha + \gamma < \beta + \gamma$$

nazveme *monomiálním uspořádáním* na $\mathbb{K}[x_1, \ldots, x_n]$.

Uspořádání na $\mathbb{N}^n$ indukuje uspořádání na monomech, jakmile zvolíme pořadí proměnných $x_1 < x_2 < \ldots x_n$.

Každý polynom lze však přeskládat jako klesající posloupnost monomů (na koeficienty teď nehledíme).

Následující tři definice zavádějí nejběžněji užívaná monomiální uspořádání. Všechna se opírají o předem dané uspořádání jednotlivých proměnných, standardně $x_1 > x_2 > \cdots > x_n$.

**Definice.** *Lexikografické uspořádání* je takové $<_{\text{lex}}$, že pro každé $\alpha, \beta \in \mathbb{N}^n$ platí

$$\alpha >_{\text{lex}} \beta \iff \text{nejlevější nenulový člen v } \alpha - \beta \text{ je kladný.}$$

*Gradované lexikografické uspořádání* je takové $<_{\text{grlex}}$, že pro každé $\alpha, \beta \in \mathbb{N}^n$ platí:

$$\alpha >_{\text{grlex}} \beta \iff \begin{aligned} &|\alpha| > |\beta| \quad \text{nebo} \\ &|\alpha| = |\beta| \quad \text{a zároveň } \alpha >_{\text{lex}} \beta. \end{aligned}$$

*Gradované opačné lexikografické uspořádání* je takové $<_{\text{grevlex}}$, že pro každé $\alpha, \beta \in \mathbb{N}^n$ platí:

$$\alpha >_{\text{grevlex}} \beta \iff \begin{aligned} &|\alpha| > |\beta| \quad \text{nebo} \\ &|\alpha| = |\beta| \quad \text{a zároveň nejpravější} \\ &\qquad\qquad \text{nenulový člen}(\alpha - \beta) < 0. \end{aligned}$$

Tedy $x_1 >_{\text{grevlex}} x_2 >_{\text{grevlex}} \cdots >_{\text{grevlex}} x_n$, ale pokud $x > y > z$, pak $x^2yz^2 >_{\text{grlex}} xy^3z$, ale $x^2yz^2 <_{\text{grevlex}} xy^3z$.

Ověřte si podrobně, že $>_{\text{lex}}, >_{\text{grlex}}, >_{\text{grevlex}}$ jsou skutečně monomiální uspořádání.

**11.32. Dělení se zbytkem.** Nechť $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$ je nenulový polynom v $\mathbb{K}[x_1, \ldots, x_n]$ a $<$ monomiální uspořádání. Pak definujeme:

- *Stupeň* $\text{multideg } f := \max\{\alpha \in \mathbb{N}^n,\ a_\alpha \neq 0\}$,
- *Vedoucí koeficient* $LC\, f := a_{\text{multideg } f}$,
- *Vedoucí monom* $LM\, f := x^{\text{multideg } f}$,
- *Vedoucí člen* $LT\, f := LC\, f \cdot LM\, f$.

Tyto pojmy jsou tedy pro polynomy více proměnných vesměs silně závislé na volbě konkrétního uspořádání.

**Lemma.** *Nechť $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ a uvažme monomiální uspořádání $<$. Pak*

*(1)* $\text{multideg}(f \cdot g) = \text{multideg } f + \text{multideg } g$,

*(2)* $f + g \neq 0 \implies \text{multideg}(f + g) \leq \max\{\text{multideg } f, \text{multideg } g\}$.

Důkaz. Plyne okamžitě přímo z definic. □

**Věta.** *Nechť $<$ je monomiální a $F = (f_1, \ldots, f_s)$ s-tice polynomů v $\mathbb{K}[x_1, \ldots, x_n]$. Pak každý $f \in \mathbb{K}[x_1, \ldots, x_n]$ lze vyjádřit jako*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

**11.97. (Komplexní kružnice).** Uvažme množiny bodů $X^\varepsilon = \mathcal{V}(z_1^2 + z_2^2 - \varepsilon) \subseteq \mathbb{C}^2$ pro libovolné $\varepsilon \in \mathbb{R} \setminus \{0\}$. Příslušné reálné křivky jsou

$$X^\varepsilon_{\mathbb{R}} = X^\varepsilon \cap \mathbb{R}^2 = \begin{cases} \text{kružnice s poloměrem } \sqrt{\varepsilon} & \varepsilon > 0, \\ \emptyset & \varepsilon < 0. \end{cases}$$

Budeme psát $z_j = x_j + iy_j = x_j + \sqrt{-1}y_j$. Je tedy $X^\varepsilon$ zadáno jako podmnožina v $\mathbb{R}^4$ systémem dvou reálných rovnic

$$\begin{aligned} \mathrm{Re}(z_1^2 + z_2^2 - \varepsilon) &= x_1^2 + x_2^2 - y_1^2 - y_2^2 - \varepsilon = 0, \\ \mathrm{Im}(z_1^2 + z_2^2 - \varepsilon) &= 2(x_1y_1 + x_2y_2) = 0. \end{aligned}$$

Lze proto očekávat, že $X^\varepsilon$ bude „dvourozměrná plocha“ v $\mathbb{R}^4$. Zkusíme si ji představit jako plochu v $\mathbb{R}^3$ ve vhodném průmětu $\mathbb{R}^4 \to \mathbb{R}^3$. Zvolme si za tím účelem zobrazení

$$\varphi_+ : (x_1, x_2, y_1, y_2) \mapsto \left( x_1, x_2, \frac{x_1y_2 - x_2y_1}{\sqrt{x_1^2 + x_2^2}} \right)$$

Označme ještě $V$ podmnožinu v $\mathbb{R}^4$ zadanou druhou naší rovnicí, tj.

$$V = \{(x_1, x_2, y_1, y_2);\ x_1y_1 + x_2y_2 = 0, (x_1, x_2) \neq (0, 0)\}.$$

Zúžení zobrazení $\varphi_+$ na $V$ je invertibilní a jeho inverze $\psi_+$ je dána

$$\psi_+ : (u, v, w) \mapsto \left( u, v, -\frac{vw}{\sqrt{u^2 + v^2}}, \frac{uw}{\sqrt{u^2 + v^2}} \right).$$

Všimněme si nyní, že

$$\left( \frac{x_1y_2 - x_2y_1}{\sqrt{x_1^2 + x_2^2}} \right)^2 = y_1^2 + y_2^2$$

a odtud vyplývá

$$\varphi_+(V \cap X^\varepsilon) = H^\varepsilon = \{(u, v, w);\ u^2 + v^2 - w^2 - |\varepsilon| = 0\}.$$

Nyní můžeme složit zkonstruovaná zobrazení

$$\varphi_\varepsilon : X^\varepsilon \to V @> \varphi_+ >> \mathbb{R}^3 \setminus \{(0, 0, 0)\} \supseteq H^\varepsilon$$

a pro každé $\varepsilon > 0$ získáme bijekci $\varphi_\varepsilon : X^\varepsilon \to H^\varepsilon$. Reálná část této variety je „nejužší kružnice“ na jednodílném rotačním hyperboloidu $H^\varepsilon$, viz obrázek.

*kde $a_i, r \in \mathbb{K}[x_1, \ldots, x_n]$ pro všechna $i = 1, 2, \ldots, s$. Navíc $r = 0$ nebo $r$ je lineární kombinací monomů, z nichž žádný není dělitelný kterýmkoli z LT $f_1, \ldots,$ LT $f_s$, a pokud $a_i f_i \neq 0$, pak* multideg $f \geq$ multideg $a_i f_i$ *pro každé $i$.*

*Polynom $r$ nazýváme* zbytkem po dělení $f/F$.

Důkaz. Věta neříká nic o jednoznačnosti výsledku. Následující algoritmus dává jedno možné řešení a je tedy důkazem platnosti věty.

Nadále budeme výsledkem dělení se zbytkem chápat právě tento výstup pevně zvoleného algoritmu.

(1) $a_1 := 0, \ldots, a_s := 0, r := 0, p := f$
(2) `while` $p \neq 0$
  (a) $i := 1$
  (b) $d :=$ *false*
  (c) `while` $i \leq s \wedge \mathrm{not}\, d$
    (i) `if` LT $f_i |$LT $p$
      $a_i := a_i +$ LT $p/$LT $f_i$
      $p := p - (LT\ p/LT\ f_i) \cdot f_i$
      $d :=$ *true*
    (ii) `else` $i := i + 1$
  (d) `if` $\mathrm{not}\, d$
    (i) $r := r +$ LT $p$
    (ii) $p := p -$ LT $p$

Při každém průchodu vnějším cyklem se právě jednou provede právě jeden z příkazů 2(c)i, 2(d)ii, a tedy stupeň $p$ klesne. Proto algoritmus skončí.

Platí invariant $f = a_1 f_1 + \cdots + p + r$ a přitom každý člen každého $a_i$ je podílem LT $p/$LT $f_i$ z nějakého okamžiku. Proto stupeň těchto členů je menší než stupeň $p$ v daném okamžiku a ten je nejvýše roven stupni $f$. Dohromady stupeň každého $a_i f_i$ je menší nebo roven stupni $f$. □

V okruhu $\mathbb{K}[x_1, \ldots, x_n]$ platí pouze implikace

$$f = a_1 f_1 + \cdots + a_s f_s + 0 \implies f \in \langle f_1, \ldots, f_s \rangle.$$

Obrácení obecně pro naše dělení se zbytkem neplatí. Uvažujme $f = xy^2 - x$, $f_1 = xy + 1$, $f_2 = y^2 - 1$. Potom algoritmus dělení dá

$$f = y(xy + 1) + 0(y^2 - 1) + (-x - y),$$

ale přitom evidentně $f = x(y^2 - 1)$, a tedy $f \in \langle f_1, f_2 \rangle$.

**11.33. Monomiální ideály.** Ideál $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ nazýváme *monomiální*, jestliže existuje množina multiindexů $\alpha \subseteq \mathbb{N}^n$ taková, že $I$ je generován právě všemi monomy $x^\alpha$ s $\alpha \in A$.

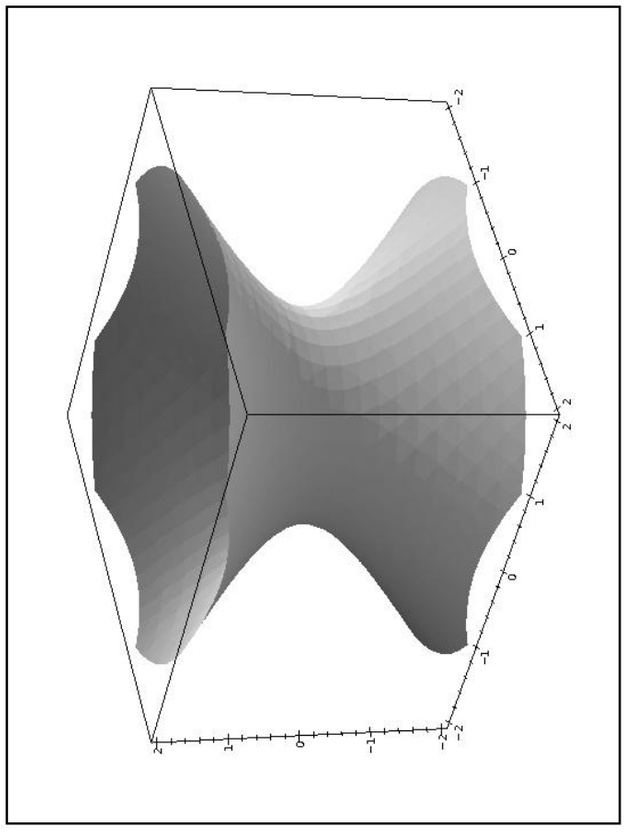


To znamená, že všechny polynomy v $I$ jsou tvaru $\sum_{\alpha \in A} h_\alpha x^\alpha$, kde $h_\alpha \in \mathbb{K}[x_1, \ldots, x_n]$.

Zřejmě pro monomiální ideál $I$ platí, že $x^\beta \in I$, právě když existuje $\alpha \in A$ takové, že $x^\alpha$ dělí $x^\beta$.

**Lemma.** *Nechť $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ je monomiální ideál, $f \in \mathbb{K}[x_1, \ldots, x_n]$ polynom. Pak následující tvrzení jsou ekvivalentní*

*(1) $f \in I$,*
*(2) každý člen polynomu $f$ je prvkem $I$;*
*(3) polynom $f$ je lineární kombinací monomů z $I$ s koeficienty z $\mathbb{K}$.*



Pro $\varepsilon < 0$ můžeme zopakovat předchozí úvahy, pouze v definici $\varphi_+$ přehodíme proměnné $x$ a $y$ a znaménka:

$$\varphi_- : (x_1, x_2, y_1, y_2) \mapsto \left( -y_1, -y_2, \frac{-y_1x_2 + y_2x_1}{\sqrt{y_1^2 + y_2^2}} \right),$$

což přivodí změnu inverze $\psi_-$

$$\psi_+ : (u, v, w) \mapsto \left( -\frac{vw}{\sqrt{u^2+v^2}}, \frac{uw}{\sqrt{u^2+v^2}}, -u, -v \right).$$

Nyní je opět $H^\varepsilon$ jednodílý rotační hyperboloid, ovšem jeho reálná část je $X^\varepsilon_{\mathbb{R}} = \emptyset$.

V komplexním případě můžeme pozorovat, že při spojité změně koeficientů se výsledná varieta většinou v podstatě nemění, až na jisté „kastastrofické“ body, kdy může dojít ke kvalitativnímu skoku. Říká se tomu *princip permanence*. V reálném případě tento princip vůbec neplatí.

**11.98. Projektivní rozšíření přímky a roviny.** Reálný prostor $\mathbb{P}_1(\mathbb{R})$ je definován jako množina všech směrů v $\mathbb{R}^2$, tj. jeho body jsou jednorozměrné podprostory vektorového prostoru $\mathbb{R}^2$.

Důkaz. Implikace (3) $\Longrightarrow$ (2) $\Longrightarrow$ (1) jsou zřejmé. Zbývá ukázat (1) $\Longrightarrow$ (3).

Zapišme si polynom $f = \sum_\alpha a_\alpha x^\alpha$, kde $a_\alpha \in \mathbb{K}$. Z předpokladu $f \in I$ vyplývá, že lze také vyjádřit $f = \sum_{\beta\in A} h_\beta x^\beta$, kde $x^\beta \in I$ a $h_\beta \in \mathbb{K}[x_1, \ldots, x_n]$.

Každý člen $a_\alpha x^\alpha$ se musí rovnat některému členu z druhé rovnosti. Jistě tedy každý člen $a_\alpha x^\alpha$ polynomu $f$ můžeme vyjádřit jako součet výrazů $d\, x^{\beta+\delta}$, kde $d \in \mathbb{K}$, $x^\beta \in I$. Pak ale také $x^\alpha \in I$, a tedy platí (3). □

**Důsledek.** *Dva monomiální ideály splývají právě tehdy, když obsahují stejné monomy.*

**11.34. Věta** (Dicksonovo lemma)**.** *Každý monomiální ideál* $I = \langle x^\alpha,\ \alpha \in A\rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *lze psát ve tvaru* $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s}\rangle$, *kde* $\alpha_1, \ldots, \alpha_s \in A$.

Důkaz. Důkaz provedeme indukcí podle počtu proměnných.



V případě $n = 1$ je $I \subseteq \mathbb{K}[x]$, $I = \langle x^\alpha,\ \alpha \in A \subseteq \mathbb{N}\rangle$. Množina všech exponentů v $A$ má jistě minimum a definujeme $\beta := \min A$. Potom zřejmě $x^\beta$ dělí všechny monomy $x^\alpha$ s $\alpha \in A$ a tedy také $I = \langle x^\beta\rangle$.

Uvažujme nyní $n > 1$ a předpokládejme, že pro menší počty proměnných tvrzení platí. Pro přehlednost si označíme proměnné jako $x_1, \ldots, x_{n-1}, y$ a monomy budeme psát ve tvaru $x^\alpha y^m$, kde $\alpha \in \mathbb{N}^{n-1}$, $m \in \mathbb{N}$. Předpokládejme, že $I \subseteq \mathbb{K}[x_1, \ldots, x_{n-1}, y]$ je monomiální a definujme $J \subseteq \mathbb{K}[x_1, \ldots, x_{n-1}]$ následovně

$$J := \langle x^\alpha,\ \exists m \in \mathbb{N},\ x^\alpha y^m \in I\rangle.$$

Zřejmě je $J$ monomiální ideál v $n-1$ proměnných a tedy podle indukčního předpokladu lze psát $J = \langle x^{\alpha_1}, \ldots, x^{\alpha_s}\rangle$. Dále z definice $J$ vyplývá, že existují taková minimální $m_i \in \mathbb{N}$, že $x^{\alpha_i} y^{m_i} \in I_A$. Označme tedy $m := \max\{m_i\}$ a definujme analogicky systém ideálů $J_k \subseteq \mathbb{K}[x_1, \ldots, x_{n-1}]$ pro $0 \le k \le m-1$

$$J_k := \langle x^\beta;\ x^\beta y^k \in I_A\rangle.$$

Opět všechny $J_k$ splňují indukční předpoklad a tedy je lze vyjádřit

$$J_k = \langle x^{\alpha_{k,1}}, \ldots, x^{\alpha_{k,s_k}}\rangle.$$

Zbývá ukázat, že $I$ je generovaný právě zkonstruovanou konečnou množinou monomů

$$\begin{gathered} x^{\alpha_1} y^m, \ldots, x^{\alpha_s} y^m, \\ x^{\alpha_{0,1}} y^0, \cdots, x^{\alpha_{0,s_0}} y^0, \\ \vdots \\ x^{\alpha_{m-1,1}} y^{m-1}, \ldots, x^{\alpha_{m-1,s_{m-1}}} y^{m-1}. \end{gathered}$$

Uvažujme tedy libovolný monom $x^\alpha y^p \in I$. Nastane jeden ze dvou případů

- $p \ge m$. Potom jistě $x^\alpha \in J_{\text{„}} k = p$, a tedy některý z $x^{\alpha_1} y^m, \ldots, x^{\alpha_s} y^m$ dělí $x^\alpha y^p$.
- $p < m$. Potom analogicky $x^\alpha \in J_k$ a některý z $x^{\alpha_{k,1}} y^k, \ldots, x^{\alpha_{k,s_k}} y^k$ dělí $x^\alpha y^p$.

Podle předchozího lemmatu lze každé $f \in I$ vyjádřit jako lineární kombinaci monomů z $I$, ty jsou již dělitelné některým z našich generátorů, proto $f$ patří do ideálu jimi generovaného. Proto $I$ je jeho podmnožinou. Opačná inkluze je zcela triviální a důkaz Dicksonova lemmatu je hotov. □

Komplexní projektivní prostor $\mathbb{P}_1(\mathbb{C})$ je definován jako množina všech směrů v $\mathbb{C}^2$, jeho body jsou tedy jednorozměrné podprostory komplexního vektorového prostoru $\mathbb{C}^2$.

Analogicky body reálných, resp. komplexních, dvourozměrných projektivních prostorů jsou definovány jako směry v $\mathbb{R}^3$, resp. $\mathbb{C}^3$.

### G. Rozšíření stereografické projekce

Zkusme si nyní rozšířit definici stereografické projekce tak, aby kružnice byla parametrizována body $\mathbb{P}_1(\mathbb{R})$. Podívejme se tedy, jak bude vypadat odpovídající zobrazení $\mathbb{P}_1(\mathbb{R}) \to \mathbb{P}_2(\mathbb{R}^2)$. Body v projektivních rozšířeních budeme zadávat tzv. *homogenními souřadnicemi*, které jsou dány až na společný násobek. Např. body v $\mathbb{P}_2(\mathbb{R})$ budou $(x : y : z)$.

Kružnice v rovině $z = 1$ je dána jako průnik kužele směrů zadaných rovnicí $x^2 + y^2 - z^2 = 0$ s touto rovinou. Inverzi k stereografické projekci (tj. naši parametrizaci kružnice) můžeme nyní zapsat takto:

$$(t : 1) \mapsto \left(\frac{2t}{1+t^2} : \frac{t^2-1}{t^2+1} : 1\right) = \left(2t : t^2 - 1 : t^2 + 1\right).$$

Přitom pro $t \neq 0$ je $(t : 1) = (2t^2 : 2t)$ a původní stereografickou projekci (tj. inverzi předchozího zobrazení) můžeme také zapsat pomocí lineárního předpisu

$$(x : y : z) \mapsto (y + z : x),$$

který rozšiřuje naši parametrizaci i na nevlastní bod $(0 : 1) \mapsto (0 : 1 : 1)$. Zobrazení celého $\mathbb{P}_1(\mathbb{R})$ na kružnici má pak „lineární“ zápis

$$\mathbb{P}_1(\mathbb{R}) \ni (x : y) \mapsto (2x : x - y : x + y) \in \mathbb{P}_2(\mathbb{R}).$$

Podívejme se ještě, jak jednoduché je spočíst přímo vzorec pro stereografickou projekci v projektivních rozšířeních (viz 4.33): Vložíme si $\mathbb{P}_1(\mathbb{R})$ jako body s homogenními souřadnicemi $(t : 0 : 1)$ a mezi lineárními kombinacemi bodů $(0 : 1 : -1)$ (tj. pól, ze kterého promítáme) a $(x : y : z)$ (obecný bod kružnice) musíme najít ten, který má souřadnice $(u : 0 : v)$. Jediná možnost je bod $(x : 0 : z + y)$, což je náš předchozí vztah.

### H. Eliptické křivky

*Singulárním bodem* nadplochy v $P^n$, zadané homogenním polynomem

$$F(x_0, x_1, \ldots, x_n) = 0,$$

rozumíme bod, pro který je $\frac{\partial F}{\partial x_i} = 0$ pro $i = 1, \ldots, n$.

Geometricky se pak v singulárním bodě děje „něco divného“. Podmínka na nulovost všech parciálních derivací znamená v případě

**11.35. Hilbertova věta.** Nyní již máme nachystáno vše potřebné pro diskusi pěkných bází ideálů v okruzích polynomů. Hlavní myšlenkou je maximální využití informací o vedoucích členech prvků v bázi a v celém ideálu.

Je-li $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ nenulový, označíme

$$LT\, I := \{ax^\alpha;\ \exists f \in I:\ LT\, f = ax^\alpha\}.$$

Zřejmě $\langle LT\, I\rangle$ je monomiální ideál, proto podle Dicksonova lemmatu lze psát $\langle LT\, I\rangle = \langle LT\, g_1, \ldots, LT\, g_s\rangle$ pro nějaká vhodná $g_1, \ldots, g_s \in I$.

**Věta.** *Každý ideál $I \in \mathbb{K}[x_1, \ldots, x_n]$ je konečně generovaný.*

Důkaz. Pokud je $I = \{0\}$, je tvrzení triviální. Uvažujme tedy $I \neq \{0\}$. Podle Dicksonova lemmatu a předchozí poznámky existují taková $g_1, \ldots, g_s \in I$, že $\langle LT\, I\rangle = \langle LT\, g_1, \ldots, LT\, g_s\rangle$.

Zřejmě $\langle g_1, \ldots, g_s\rangle \subseteq I$. Vezměme libovolné $f \in I$ a proveďme dělení se zbytkem $s$-ticí $g_1, \ldots, g_s$. Dostáváme

$$f = a_1 g_1 + \cdots + a_s g_s + r,$$

kde žádný člen $r$ není dělitelný $LT\, g_1, \ldots, LT\, g_s$.

Protože $r = f - a_1 g_1 - \cdots - a_s g_s$, platí $r \in I$, a tedy také $LT\, r \in LT\, I$. Zřejmě tedy $LT\, r \in \langle LT\, I\rangle$. Připusťme, že $r \neq 0$. Protože $\langle LT\, I\rangle$ je monomiální, musí být $LT\, r$ dělitelný některým z jeho generátorů, tj. $LT\, g_1, \ldots, LT\, g_s$. To je ovšem spor s výsledkem algoritmu dělení. Proto $r = 0$ a $I$ je generovaný $g_1, \ldots, g_s$. □

#### Gröbnerovy báze ideálů

**11.36. Definice.** Konečná množina generátorů $g_1, \ldots, g_s$ ideálu $I \subseteq k[x_1, \ldots, x_n]$ se nazývá *Gröbnerova báze,* jestliže platí $\langle LT\, I\rangle = \langle LT\, g_1, \ldots, LT\, g_s\rangle$.

Báze použitá v důkazu Hilbertovy věty byla Gröbnerova.

**Důsledek.** *Každý ideál $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ má Gröbnerovu bázi. Přitom každá množina polynomů $g_1, \ldots, g_s \in I$ splňující $\langle LT\, I\rangle = \langle LT\, g_1, \ldots, LT\, g_s\rangle$ je Gröbnerovou bází ideálu $I$.*

Ukažme smysl předchozích obecných výsledků na nejjednodušším případě polynomů stupně jedna s lexikografickým uspořádáním.

Označme generátory $f_i = \sum_j a_{i,j} x_j + a_{i,0}$. Uvažujme matici $A = (a_{i,j})$, kde $i = 1, \ldots, s$ a $j = 0, \ldots, n$ a aplikujme na ni Gaussovu eliminaci. Získáme $B = (b_{i,j})$ ve schodovitém tvaru, z ní navíc vypustíme nulové řádky. Máme novou bázi $g_1, \ldots, g_t$, kde $t \leq s$.

Vzhledem k provedeným úpravám je každé $f_i$ vyjádřitelné jako lineární kombinace $g_1, \ldots, g_t$, a tedy

$$\langle f_1, \ldots, f_s\rangle = \langle g_1, \ldots, g_t\rangle.$$

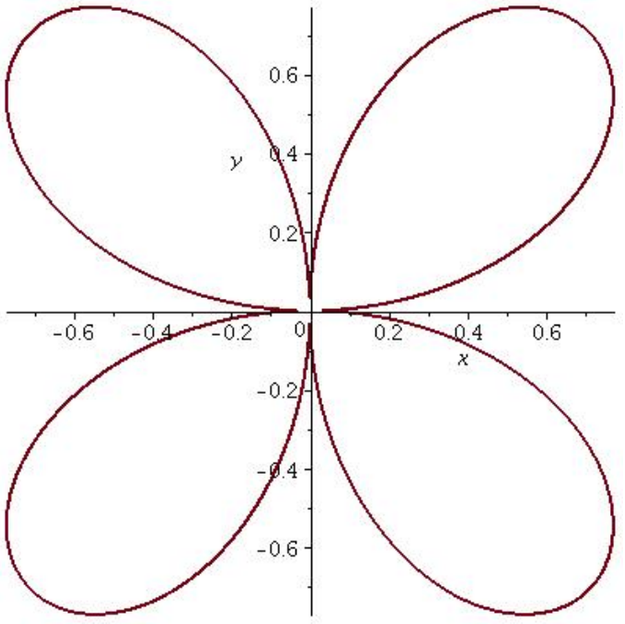
Ověříme si, že takto získané polynomy $g_1, \ldots, g_t$ jsou Gröbnerovou bází.

Bez újmy na obecnosti předpokládejme, že proměnné jsou značeny tak, že $LM\, g_i = x_i$ pro $i = 1, \ldots, t$. Libovolný $f \in I$ lze psát

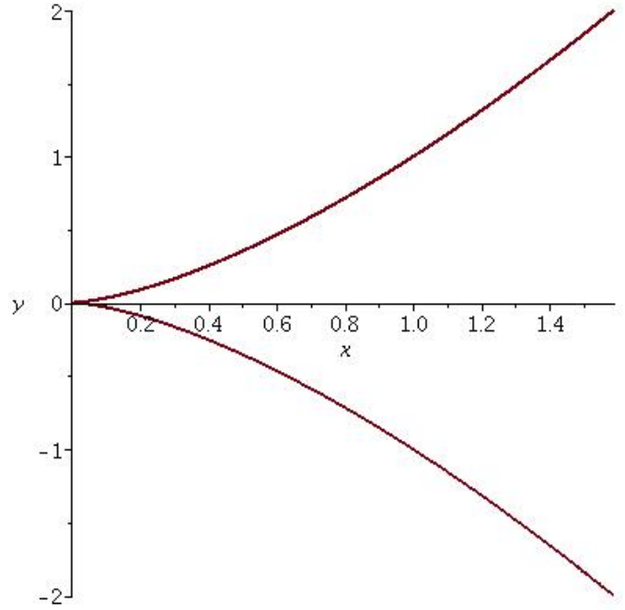
$$f = h_1 f_1 + \cdots + h_s f_s = h'_1 g_1 + \cdots + h'_t g_t.$$

Chceme, aby $LT\, f \in \langle LT\, g_1, \ldots, LT\, g_t\rangle$, tj. $LT\, f$ má být dělitelný některým z $x_1, \ldots, x_t$. Předpokládejme, že $f$ je pouze

křivky v projektivním prostoru $P^2(\mathbb{R})$, že v daném bodě není definována tečna k uvažované křivce. To znamená, že na křivce je tzv. *bod zvratu* (anlicky cusp), nebo se křivka sama protíná. „Pěkná“ singularita je třeba u „čtyřlístku“, tj. varietě dané nulovými body polynomu $(x^2+y^2)^3-4x^2y^2$ v $\mathbb{R}^2$:




Bod zvratu je můžeme pak najít na křivce dané v $\mathbb{R}^2$ rovnicí $x^3-y^2=0$.




*Eliptickou křivkou* $\mathcal{C}$ rozumíme množinu bodů v $\mathbb{K}^2$, kde $\mathbb{K}$ je nějaké těleso, splňující rovnici

$$y^2 = x^3 + ax + b,$$

v proměnných $x_{t+1},\dots,x_n$. Pak ale $h_1' = 0$, protože $x_1$ je vzhledem ke schodovitosti $B$ pouze v $g_1$. Analogickým postupem získáme $h_2' = \cdots = h_t' = 0$, a tedy $f = 0$.

Dokázali jsme sice existenci nadějných zvláštních bází, zatím je ale neumíme algoritmicky konstruovat. K tomu se dostaneme v následujících odstavcích.

**11.37. Věta.** *Nechť $G = \{g_1,\dots,g_t\}$ je Gröbnerova báze ideálu $I \subseteq \mathbb{K}[x_1,\dots,x_n]$ a $f$ je polynom v $\mathbb{K}[x_1,\dots,x_n]$. Pak existuje právě jedno $r = \sum_\alpha a_\alpha x^\alpha \in \mathbb{K}[x_1,\dots,x_n]$ s těmito vlastnostmi:*

*(1) žádný člen $r$ není dělitelný žádným z $LT\,g_1,\dots,LT\,g_t$, tj. $\forall\alpha\forall i:\ LT\,g_i \nmid a_\alpha x^\alpha$;*

*(2) $\exists g \in I:\ f = g + r$.*

Důkaz. Algoritmus pro dělení se zbytkem dá

$$f = a_1g_1 + \cdots + a_tg_t + r,$$

kde $r$ splňuje podmínku (1). Za $g$ si zvolme $a_1g_1+\cdots+a_tg_t$, které samozřejmě patří do $I$.

Zbývá dokázat jednoznačnost. Předpokládejme

$$f = g + r = g' + r',$$

kde $r \neq r'$. Zřejmě platí $r - r' = g' - g \in I$. Protože $G$ je Gröbnerova báze, je $LT(r-r')$ dělitelný některým z $LT\,g_1,\dots,LT\,g_t$. Máme přitom jen dvě možnosti

- $LM\,r \neq LM\,r'$. Pak ten s vyšším stupněm musí být dělitelný některým z vedoucích členů $LT\,g_1,\dots,LT\,g_t$, což je spor s podmínkou (1).
- $LM\,r = LM\,r'$ a zároveň $LC\,r \neq LC\,r'$. Potom ale oba monomy $LM\,r$ a $LM\,r'$ musí být dělitelné některým z $LT\,g_1,\dots,LT\,g_t$, což je opět spor.

Proto tedy $LT\,r = LT\,r'$ a induktivní úvahou odtud plyne $r = r'$. □

Předchozí věta zobecňuje dělení se zbytkem, kde na místě dělitele vystupuje ideál. V případě jedné proměnné nebylo co zobecňovat, protože každý ideál byl generovaný jedním polynomem. Zajímá-li nás pouze zbytek, věta navíc říká, že nezáleží na pořadí polynomů v Gröbnerově bázi. Proto má smysl zavést značení $\overline{f}^G$ pro zbytek po dělení $f/G$, pokud $G = (g_1,\dots,g_s)$ je Gröbnerova báze.

**Důsledek.** *Nechť $G = \{g_1,\dots,g_t\}$ je Gröbnerova báze ideálu $I \subseteq \mathbb{K}[x_1,\dots,x_n]$ a $f$ je polynom v $\mathbb{K}[x_1,\dots,x_n]$. Pak je libovolný polynom $f$ prvkem ideálu $I$, právě když je zbytek po dělení $f/G$ nulový.*

**11.38. Syzygy.** Dalším krokem bude nalezení dostatečné „testovací množiny“ polynomů z daného ideálu, které je třeba prověřit dělením se zbytkem, abychom mohli usoudit, že je uvažovaný systém generátorů již Gröbnerovou bazí.



Pro $\alpha = \text{multideg}\,f$ a $\beta = \text{multideg}\,g$ uvažme

$$\gamma := (\gamma_1,\dots,\gamma_n), \quad \text{kde } \gamma_i = \max\{\alpha_i,\beta_i\}.$$

Monom $x^\gamma$ nazýváme *nejmenším společným násobkem (least common multiple)* monomů $LM\,f$ a $LM\,g$ a zavádíme označení $LCM(LM\,f, LM\,g) := x^\gamma$. Výraz

$$S(f,g) := \frac{x^\gamma}{LT\,f}\cdot f - \frac{x^\gamma}{LT\,g}\cdot g$$

nazýváme $S$-polynomem (nebo také *syzygy*, neboli spřežení) polynomů $f, g$.

kde $a, b \in \mathbb{K}$. Přidává se též podmínka nesingularity, což nad tělesem reálných čísel znamená, že

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

Výraz $\Delta$ nazýváme diskriminantem dané rovnice. Upozorněme, že v definici křivky se na pravé straně definující rovnice objevuje kubický polynom bez kvadratického člene. Tomuto zápisu se říká *Weierstrasův tvar* rovnice eliptické křivky.

**11.99.** Dokažte, že křivka $y^2 = x^3 + ax + b$ v $\mathbb{R}^2$ má singularitu, právě když $4a^3 - 27b^2 = 0$.

**Řešení.** Rovnice křivky v homogenních souřadnicích (viz 4.33) zní $F(x, y, z) = 0$, kde

$$F(x, y, z) = y^2 z - x^3 - axz^2 - bz^3. \tag{11.1}$$

Máme

$$\begin{aligned} \frac{\partial F}{\partial x} &= -3x^2 - az^2, \\ \frac{\partial F}{\partial y} &= 2yz, \\ \frac{\partial F}{\partial z} &= y^2 - 2axz - 3bz^2. \end{aligned}$$

Nechť $[x, y, z]$ je singulárním bodem dané křivky. Pokud by $z = 0$, tak z nulovosti parciálních derivací polynomu $F$ podle $x$, resp. podle $z$, vyplývá $x = 0$, resp. $y = 0$. To je však „aut“, neboť bod $[0, 0, 0]$ není bodem uvažovaného projektivního prostoru $P^2(\mathbb{R})$. Pro singulární bod tedy $z \neq 0$ a proto z $\frac{\partial F}{\partial y} = 0$ dostáváme $y = 0$. Označíme-li $\gamma = \frac{x}{z}$, pak z $-3x^2 - az^2 = 0$ vyplývá $3\gamma^2 = -a$ a z rovnice $y^2 - 2axz - 3bz^2 = 0$ plyne $2a\gamma = -3b$. Vidíme, že rovnost $a = 0$ vynucuje i $b = 0$, tedy rovnost $4a^3 = 27b^2$ je triviálně splněna. Pokud $a \neq 0$ pak vyjádříme $\gamma$ ze dvou získaných rovnic. Z jedné je $\gamma = -\frac{3b}{2a}$, ze druhé pak $\gamma^2 = -\frac{a}{3}$. Celkem

$$\gamma^2 = -\frac{a}{3} = \frac{9b^2}{4a^2} \implies 4a^3 + 27b^2 = 0.$$

Jeden směr implikace je tak dokázán. Obráceně, pokud $4a^3 + 27b^2 = 0$, pak pokud definujeme $\gamma = -\frac{3b}{2a}$, tak bod $[\gamma, 0, 1]$ vyhovuje rovnici eliptické křivky:

$$\begin{aligned} \gamma^2 + a\gamma + b &= \left(-\frac{3b}{2a}\right)\left(-\frac{a}{3}\right) + a\left(-\frac{3b}{2a}\right) + b = \\ &= \frac{b}{2} - \frac{3b}{2} = 0. \end{aligned}$$

Vzhledem k volbě $\gamma$ jsou pak i všechny tři parciální derivace v bodě $[\gamma, 0, 1]$ polynomu $F$ nulové. □

Jedná se o nástroj k eliminaci vedoucích členů, Gaussova eliminace je speciálním případem tohoto postupu pro polynomy stupně jedna. Na rozdíl od ní ale může dojít ke zvýšení stupně, i když původní vedoucí členy odstraní.

Vezměme například $f = x^3y^2 - x^2y^3 + x$, $g = 3x^4y + y^2$, tedy polynomy stupně 5 v $\mathbb{R}[x, y]$ a uspořádání $<_{\text{grlex}}$. Pak $\gamma = (4, 2)$ a

$$S(f, g) = \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g = xf - \frac{1}{3}yg = -x^3y^3 + x^2 - \frac{1}{3}y^3,$$

což je polynom stupně 6.

**Věta.** *Nechť $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ je ideál. Pak je $G = \{g_1, \ldots, g_t\}$ jeho Gröbnerova báze, právě když pro každé $i \neq j$ je zbytek po dělení $S(g_i, g_j)/G$ nulový.*

Důkaz. Důkaz začneme technickým lemmatem, které popisuje, jakým způsobem mohou nastávat krácení při vyjádření polynomů pomocí generátorů. Přesněji řečeno, že je můžeme vždy vyjádřit pomocí S-polynomů.

**Lemma.** *Uvažme polynom $f = \sum_{i=1}^{t} c_i x^{\alpha_i} g_i$, kde $c_1, \ldots, c_t \in \mathbb{K}$ a $\alpha_i + \text{multideg}\, g_i = \delta$ pro nějaké pevné $\delta$ kdykoli $c_i \neq 0$. Pokud* multideg $f < \delta$, *pak existují taková $c_{jk} \in \mathbb{K}$, že*



$$\sum_{i=1}^{t} c_i x^{\alpha_i} g_i = \sum_{j,k=1}^{t} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k),$$

*kde $x^{\gamma_{jk}} = LCM(LM\, g_j, LM\, g_k)$ a každý monom $x^{\delta-\gamma_{jk}} S(g_j, g_k)$ má stupeň menší než $\delta$.*

Důkaz. Označme $d_i := LC\, g_i$ a $p_i = x^{\alpha_i} g_i / d_i$. Určitě platí $c_i d_i = LC(c_i x^{\alpha_i} g_i)$ a $LC\, p_i = 1$. Protože multideg$(c_i x^{\alpha_i} g_i) = \delta$ a zároveň multideg $f < \delta$, musí nutně platit také $\sum_{i=1}^{t} c_i d_i = 0$. Pokusme se teď $f$ vyjádřit jako kombinaci $S$-polynomů:

$$\begin{aligned} f = \sum_{i=1}^{t} c_i d_i p_i &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \\ &+ \cdots + (c_1 d_1 + \cdots + c_{t-1} d_{t-1})(p_{t-1} - p_t) + \\ &+ \underbrace{(c_1 d_1 + \cdots + c_t d_t)}_{0} p_t. \end{aligned}$$

Každý rozdíl $p_j - p_k$ lze vyjádřit v $S$-polynomech

$$\begin{aligned} \frac{x^\delta}{d_j x^{\delta-\alpha_j}} g_j - \frac{x^\delta}{d_k x^{\delta-\alpha_k}} g_k &= x^{\delta-\gamma_{jk}} \left( \frac{x^{\gamma_{jk}}}{LT\, g_j} g_j - \frac{x^{\gamma_{jk}}}{LT\, g_k} g_k \right) = \\ &= x^{\delta-\gamma_{jk}} S(g_j, g_k) \end{aligned}$$

Z obou rovností se už snadno odvodí jednotlivé koeficienty $c_{jk}$. □

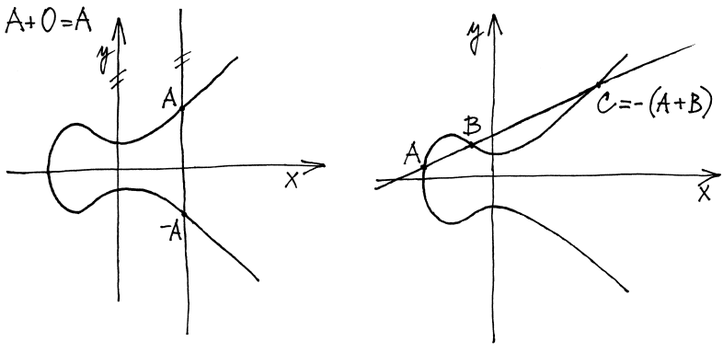
Nyní můžeme přikročit k důkazu věty. Implikace „$\Longrightarrow$“ plyne bezprostředně z důsledku v odstavci 11.37. Musíme dokázat implikaci opačnou.

Uvažme nenulový polynom $f \in I$. Potřebujeme ukázat, že za předpokladu dokazované implikace vždy bude platit $LT\, f \in \langle LT\, g_1, \ldots LT\, g_t \rangle$. Podaří-li se zaručit, že lze náš polynom vyjádřit jako $f = \sum_{i=1}^{t} h_i g_i$ s vlastností

$$\text{multideg}\, f = \max\{\text{multideg}(h_i g_i)\},$$

bude $LT\, f$ nutně dělitelný některým $LT\, g_i$, a tedy $G$ bude skutečně Gröbnerova báze.

Abychom pomocí eliptické křivky snadno zavedli grupovou operaci na jejích bodech, je výhodné křivku uvážit v projektivním rozšíření roviny (viz 4.33) a definujeme bod $O \in \mathcal{C}$ jako směr $(0, 1)$ (což je bod $[0, 1, 0]$ v homogenních souřadnicích). Operaci sčítání pak geometricky definujeme pro dva body $A, B \in \mathcal{C}$ jako bod $-C$, kde $C$ je třetí průsečík přímky $AB$ s eliptickou křivkou. Pokud $A = B$ je výsledek dán dalším průsečíkem tečny k eliptické křivce v bodě $A$.




**11.100.** Dokažte, že předchozí definice definuje korektně operaci na bodech eliptické křivky.

**Řešení.** Průsečíky přímky s eliptickou křivkou dostaneme jako řešení kubické rovnice. Ta pokud má dva reálné kořeny, odpovídající bodům $A$ a $B$, tak má i třetí reálný kořen, tedy přímka $AB$ musí mít nutně ještě jeden průsečík s danou křivkou. V případě tečny odpovídá bod $A$ dvojnásobnému kořenu, další průsečík tedy opět existuje. Co se týče nevlastních bodů (poslední souřadnice v homogenních souřadnicích je nulová, odpovídají směrům v rovině), tak jediným nevlastním bodem ležícím na křivce dané rovnicí (‖11.1‖) je právě pouze bod $O = [0, 1, 0]$. Sčítání s bodem $O$ znamená hledání druhého průsečíku eliptické křivky (mimo bodu $A$) s rovnoběžkou s osou $y$ vedenou bodem $A$. Nevlastní přímka $z = 0$ má pak s křivkou trojnásobný průsečík 0, je tedy $O + O = O$. □

**Poznámka.** Operace je tedy korektně definována. Navíc přímo z definice vyplývá, že je komutativní. Z předchozích úvah vyplývá i to, že $O$ je neutrální prvek operace. Důkaz asociativity není zcela triviální.

**11.101.** Definujte předchozí operaci i algebraicky.

**Řešení.** Pro libovolný bod $A \in \mathcal{C}$ definujeme $A + O = O + A = A$.

Pro bod $A \in \mathcal{C}$, $A = (\alpha, \beta, 1)$ je zřejmě i $B \in \mathcal{C}$ a definujeme $A + B = 0$, tedy $A = -B$.

Označme $m_i := \text{multideg}(h_i g_i)$, $\delta := \max\{m_1, \ldots, m_t\}$. Zřejmě multideg $f \leq \delta$. Nechť jsou polynomy $h_1, \ldots, h_t$ zvoleny tak, že $\delta$ je minimální. Protože pracujeme s monomiálním uspořádáním, které je dobré, takové $\delta$ existuje.

Dokažme tedy, že multideg $f = \delta$. Můžeme psát

$$f = \sum_{m_i=\delta} h_i g_i + \sum_{m_i<\delta} h_i g_i = \\ = \sum_{m_i=\delta} (LT\, h_i) g_i + \sum_{m_i=\delta} (h_i - LT\, h_i) g_i + \sum_{m_i<\delta} h_i g_i .$$

Všechny sčítance druhé a třetí sumy mají jistě stupeň menší než $\delta$. Připustíme-li, že multideg $f < \delta$, potom nutně

$$\text{multideg} \left( \sum_{m_i=\delta} (LT\, h_i) g_i \right) < \delta .$$

Označme nyní $c_i x^{\alpha_i} := LT\, h_i$ a aplikujme naše technické lemma:

$$\sum_{m_i=\delta} (LT\, h_i) g_i = \sum_{m_i=\delta} c_i x^{\alpha_i} g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k).$$

Z předpokladu věty a algoritmu o dělení se zbytkem získáváme

$$S(g_j, g_k) = \sum_{i=1}^{t} p_{ijk} g_i$$

a navíc $\text{multideg}(p_{ijk} g_i) \leq \text{multideg}\, S(g_j, g_k)$. Označíme-li $q_{ijk} := x^{\delta-\gamma_{jk}} p_{ijk}$, dostáváme

$$x^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} q_{ijk} g_i .$$

Podle druhé části lemmatu platí

$$\text{multideg}(q_{ijk} g_i) \leq \text{multideg}\big(x^{\delta-\gamma_{jk}} S(g_j, g_k)\big) < \delta$$

a dosazením dostáváme

$$\sum_{m_i=\delta} (LT\, h_i) g_i = \sum_{j,k} c_{jk} \left( \sum_{i=1}^{t} q_{ijk} g_i \right) = \\ = \sum_{i=1}^{t} \left( \sum_{j,k} c_{jk} q_{ijk} \right) g_i .$$

Přitom platí

$$\text{multideg} \left( \sum_{j,k} c_{jk} q_{ijk} g_i \right) < \delta \quad \text{pro } i = 1, \ldots, t.$$

Dosazením do naší původní rovnosti získáváme vyjádření $f$ jako kombinace $g_1, \ldots, g_t$, kde všechny sčítance jsou stupně menšího než $\delta$. To je spor s minimální volbou $\delta$, a tedy multideg $f = \delta$, odkud $LT\, f \in \langle LT\, g_1, \ldots, LT\, g_t \rangle$ a báze $G$ je Gröbnerova. □

**11.39. Naivní algoritmus pro Gröbnerovy báze.** Právě dokázaná věta nám již poskytuje účinný prostředek pro zjištění, zda nějaká báze je Gröbnerova. Uvažujme například $I = \langle x + y, y - z \rangle$. Jediný $S$-polynom, který připadá v úvahu je



$$S(x + y, y - z) = \frac{xy}{x}(x + y) - \frac{xy}{y}(y - z) = xz + y^2 .$$

Pro bod $A \neq -B$, $A = [\alpha, \beta, 1]$ a bod $B \in \mathcal{C}$, $B = [\gamma, \delta, 1]$ položme

$$\begin{aligned} k &= \begin{cases} \frac{\beta-\delta}{\alpha-\gamma} & \text{pro } A \neq B, \\ [5pt]\frac{3\alpha^2+a}{2\beta} & \text{pro } A = B, \end{cases} \\ \sigma &= k^2 - \alpha - \gamma, \\ \tau &= -\beta + k(\alpha - \sigma). \end{aligned}$$

Potom definujeme $A + B = [\gamma, \tau, 1]$. Na čtenáři necháváme ověření, že se vskutku jedná o stejnou operaci, kterou jsme definovali geometricky. □

## I. Gröbnerovy báze

**11.102.** Je báze $g_1 = x^2$, $g_2 = xy + y^2$ Gröbnerova pro lexikografické uspořádání $x > y$? Pokud ne, najděte ji.

**Řešení.** Vedoucí monomy jsou zřejmě $LT(g_1) = x^2$, $LT(g_2) = xy$, a proto je jejich S-polynom roven

$$S(g_1, g_2) = yg_1 - xg_2 = -xy^2.$$

Podle věty 11.38 je $g_1$, $g_2$ Gröbnerova báze právě tehdy, když je zbytek po dělení tohoto S-polynomu bázovými polynomy nulový. Dělením se zbytkem, viz 11.32, ovšem dostáváme

$$S(g_1, g_2) = yg_1 - xg_2 + yg_2 - y^3.$$

Zbytek $y^3$ ukazuje, že daná báze není Gröbnerova. Abychom ji vytvořili, musíme podle 11.39 právě tento polynom, $g_3 = y^3$, přidat k polynomům $g_1$, $g_2$. Nyní spočítáme

$$S(g_1, g_3) = y^3 g_1 - x^2 g_3 = 0$$

a

$$S(g_2, g_3) = y^2 g_2 - xg_3 = y^4 = yg_3.$$

Odtud vyplývá podle věty 11.38, že $g_1$, $g_2$, $g_3$ už je Gröbnerova báze. □

**11.103.** Je báze $g_1 = xy - 2y$, $g_2 = y^2 - x^2$ Gröbnerova pro lexikografické uspořádání $y > x$? Pokud ne, najděte ji.

**Řešení.** Protože $LT(g_1) = xy$ a $LT(g_2) = y^2$, má příslušný S-polynom má tvar $S(g_1, g_2) = yg_1 - xg_2 = x^3 - 2y^2 = -2g_2 + x^3 - 2x^2$. Vedoucí člen $x^3$ není násobkem vedoucího členu $xy$ ani $y^2$, a proto nejde o Gröbnerovu bázi. Tu dostaneme přidáním polynomu $g_3 = x^3 - 2x^2$. Potom totiž

$$S(g_1, g_3) = x^2 g_1 - yg_3 = 0$$

a

$$\begin{aligned} S(g_2, g_3) &= x^3 g_2 - y^2 g_3 = 2y^2 x^2 - x^5 = \\ &= (4y + 2xy)g_1 - (x^2 + 2x + 4)g_3 + 8g_2. \end{aligned}$$ □

Dělením získáme $xz + y^2 = z(x + y) + y(y - z)$, a tedy daná báze je Gröbnerova.

Následující algoritmus využívá přesně tento postup pro nalezení nějaké Gröbnerovy báze ideálu generovaného $s$-ticí polynomů $F = (f_1, \ldots, f_s)$.

(1) $G := F$, $G' := \emptyset$
(2) `while` $G \neq G'$
  (a) $G' := G$
  (b) $\forall p, q \in G' \colon p \neq q$ `do`
    (i) $s := \overline{S(p, q)}^{G'}$
    (ii) `if` $s \neq 0$
      $G := G \cup \{s\}$

Když se algoritmus zastaví, jistě to bude v $G$ Gröbnerova báze. Musíme tedy už jen ověřit, že se skutečně zastaví. V jeho průběhu ovšem při každém běhu vnitřním cyklem (2), tj. když se přidává nějaký netriviální zbytek po dělení, buď monomiální ideál generovaný $LT\,G$ vzroste nebo zůstane stejný. Dostáváme tedy neklesající řetězec (monomiálních) ideálů $I_1 = LT(F) \subseteq I_2 \subseteq \cdots \subseteq \subseteq I_k \subseteq \cdots$. Označíme-li nyní $I = \cup_{k=1}^{\infty} I_k$, pak jde jistě o ideál a podle Hilbertovy věty musí být konečně generovaný. To ale znamená, že všechny generátory $I$ jsou již v některém z $I_k$ a proto od tohoto $k$ počínaje bude platit $I_k = I_{k+1} = \ldots$.[6]

Stabilizace tohoto řetězce monomiálních ideálů hlavních členů je ale ekvivalentní zastavení algoritmu.

Tento algoritmus ovšem není zdaleka ideální. Lze vymyslet velmi jednoduše vypadající vstupy, pro něž vrací divoké výsledky. Dále výstupní báze se přímo odvíjí od vstupní, a tedy pro tentýž ideál zadaný různými bázemi dá také různé výsledky.

**11.40. Redukce bází.** Viděli jsme, že k rozpoznání, které generátory jsou potřebné pro Gröbnerovu bázi, stačí sledovat jejich vedoucí členy. Prvním krokem v naší diskusi bude prosté vyházení všech prvků, které v tomto smyslu nejsou třeba.



**Lemma.** *Nechť $G$ je Gröbnerova báze ideálu $I$ a $p \in G$ takový, že $LT\,p \in \langle LT(G \setminus \{p\})\rangle$. Pak $G - \{p\}$ je také Gröbnerova báze $I$.*

Důkaz. Z definice Gröbnerovy báze platí $\langle LT\,I\rangle = \langle LT\,G\rangle$. Protože $LT\,p \in \langle LT(G \setminus \{p\})\rangle$, platí $\langle LT(G \setminus \{p\})\rangle = \langle LT\,G\rangle$. Odsud již plyne tvrzení. □

**Definice.** *Minimální Gröbnerovou bází* ideálu $I$ je taková Gröbnerova báze $G$, že pro všechna $p \in G$ platí $LC\,p = 1$ a zároveň $LT\,p \notin \langle LT(G - \{p\})\rangle$.

Například mějme $\mathbb{K}[x, y]$ a $<_{\text{grlex}}$, $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2 y - 2y^2 + x\rangle$. Zmíněný algoritmus dá pět polynomů $F = (f_1, \ldots, f_5)$:

$$F = (x^3 - 2xy, x^2 y - 2y^2 + x, -x^2, -2xy, -2y^2 + x).$$

Přitom platí $LT\,f_1 = x^3 = -x\,LT\,f_3$ a $LT\,f_2 = -\frac{1}{2}x\,LT\,f_4$ a tedy $f_1$ a $f_2$ jsou zbytečné.

Tato redukce nám ale jistě ještě nestačí, protože k redundanci může docházet i na úrovni jednotlivých členů bázových prvků. Např. si můžeme všimnout, že pro každé $a$ je

[6] V angličtině se podmínce stabilizace každého neklesajícího řetězce ideálů říká ACC, „ascending chain condition“. Okruhy, které splňují ACC, se nazývají Noetherovské (na počest Emy Noether). Hilbertovu větu proto také lze formulovat jako tvrzení „okruh polynomů nad noetherovským okruhem je opět noetherovský“.

**11.104.** Eliminujte proměnné v ideálu

$$I = \langle x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - y - z \rangle.$$

**Řešení.** Eliminace proměnných dosáhneme nalezením Gröbnerovy báze vzhledem k lexikografickému monomiálnímu uspořádání. Označme polynomy v ideálu $I$ po řadě $g_1, g_2, g_3$. Redukcí $g_2 = g_1 + 1 - 2x$ dostáváme redukovaný polynom $f_1 = 2x - 1$. Tímto polynomem redukujeme $g_3 = f_1 + 1 - y - z$ na $f_2 = y + z - 1$. Nyní zredukujeme i $g_1$ vydělením $f_1$, $f_2$ a dostaneme

$$g_1 = (\frac{1}{2}x + \frac{1}{4}) f_1 + y^2 + z^2 - 1$$

a

$$y^2 + z^2 - 1 = (y - z + 1) f_2 + 2z^2 - 2z + \frac{1}{4}.$$

Odtud $f_3 = 8z^2 - 8z + 1$. Vidíme, že v tomto případě jsme si vystačili s redukováním polynomů a že žádný jiný polynom přidávat nemusíme. Báze ideálu $I$ s eliminovanými proměnnými je $I = \langle 2x - 1, y + z - 1, 8z^2 - 8z + 1 \rangle$. □

**11.105.** Najděte řešení soustavy polynomiálních rovnic

$$\begin{aligned} x^2 y - z^3 &= 0, \\ 2xy - 4z &= 1, \\ z - y^2 &= 0, \\ x^3 - 4yz &= 0. \end{aligned}$$

**Řešení.** Nejlépe pomocí nějakého výpočetního programu zjistíme, že pro příslušný ideál

$$\langle x^2 y - z^3, 2xy - 4z - 1, z - y^2, x^3 - 4yz \rangle$$

je Gröbnerova báze vzhledem k lexikografickému monomiálnímu uspořádání rovna $\langle 1 \rangle$, a proto soustava nemá žádné řešení. □

**11.106.** Nalezněte Gröbnerovu bázi variety v $\mathbb{R}^3$ danou parametricky pomocí rovnic



$$\begin{aligned} x &= 3u + 3uv^2 - u^3, \\ y &= 3v + 3u^2 v - v^3, \\ z &= 3u^2 - 3v^2. \end{aligned}$$

Jedná se o Enneperovu plochu, jejíž obrázek můžete najít na straně 668.

$\{x^2 + axy,\ xy,\ y^2 - 1/2x\}$ minimální Gröbnerovou bází uvedeného ideálu.

Proto zavádíme následující pojem:

Redukovaná Gröbnerova báze

Polynom $g \in G$ nazveme *redukovaný* pro bázi $G$, pokud žádný z jeho monomů neleží v $\langle LT(G \setminus \{g\}) \rangle$. *Redukovanou Gröbnerovou bází* ideálu $I$ potom nazveme takovou Gröbnerovu bázi $G$, že pro všechna $p \in G$ platí $LC\ p = 1$ a zároveň $p$ je redukovaný pro $G$.

Zjevně je každá redukovaná Gröbnerova báze minimální a navíc platí:

**Tvrzení.** *Je-li polynom $g$ redukovaný pro nějakou minimální Gröbnerovu bázi $G$ ideálu $I$, pak je také redukovaný pro každou minimální Gröbnerovu bázi $G'$ téhož ideálu, která jej obsahuje.*

Důkaz. Tvrzení dokážeme sporem. Uvažme $G = \{g_1, \ldots, g_s\}$, $G' = \{g'_1, \ldots, g'_t\}$ a zvolme člen $m$ polynomu $g$, kde $m \in \langle LT(G' - \{g\}) \rangle$ (tj. $g$ není redukovaný pro $G'$). Potom $m = a_1\, LT\, g'_1 + \cdots + a_t\, LT\, g'_t$ pro nějaké vhodné polynomy $a_1, \ldots, a_t$. Protože $G$ i $G'$ jsou Gröbnerovy báze téhož ideálu, platí $\langle LT\, G \rangle = \langle LT\, G' \rangle$, a tedy každé $LT\, g'_i$ lze vyjádřit jako kombinaci $LT\, g_1, \ldots, LT\, g_s$. Odtud už plyne $m \in \langle LT\, G \rangle$, a protože je $G'$ minimální, je $m \in \langle LT(G \setminus \{g\}) \rangle$, což je spor s předpokládanou redukovaností $g$ pro $G$. □

Nyní již máme vše připraveno pro důkaz hlavního výsledku o existenci a jednoznačnosti redukované Gröbnerovy báze.

**11.41. Věta.** *Nechť $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ je nenulový. Pak pro každé monomiální uspořádání existuje právě jedna redukovaná Gröbnerova báze ideálu $I$. Navíc každou Gröbnerovu bázi lze algoritmicky redukovat.*

Důkaz. Předpokládejme, že $G$ je Gröbnerova báze ideálu $I$. S ohledem na lemma z předchozího odstavce lze předpokládat, že $G$ je i minimální. (Algoritmus minimalizace je zřejmý, stačí testovat pouze dělitelnost vedoucích monomů v jakémkoliv pořadí a vypouštět nadbytečné členy báze.)

Předpokládejme, že polynom $g \in G$ není redukovaný. Při dělení $g/(G \setminus \{g\})$ se tedy $LT\, g$ nutně dostane do zbytku, protože nemá čím být dělitelný (báze je minimální). Tedy $LT(\overline{g}^{G \setminus \{g\}}) = LT\, g$, protože nic jiného už nemůže být vedoucím členem zbytku. Označme

$$g' := \overline{g}^{G \setminus \{g\}}, \quad G' := \big(G \setminus \{g\}\big) \cup \{g'\}.$$

Tento nový systém generátorů $G'$ je opět minimální Gröbnerovou bází ideálu $I$, protože $\langle LT\, G' \rangle = \langle LT\, G \rangle$, tj. také platí $\langle LT\, G' \rangle = \langle LT\, I \rangle$. Polynom $g'$ je zřejmě redukovaný pro $G'$ díky vlastnostem algoritmu pro dělení. Byl-li nějaký $h \neq g$ redukovaný pro $G$, zůstává podle předchozího tvrzení z předchozího odstavce redukovaný i pro $G'$.

Při každé provedené redukci některého z prvků dojde ke snížení celkového počtu členů ve všech polynomech v redukované Gröbnerově bázi. Proto se algoritmus zastaví v okamžiku, kdy už jsou všechny prvky redukované a máme tedy algoritmus konstrukce redukované Gröbnerovy báze.

Zbývá dokázat její jednoznačnost. Předpokládejme dvě redukované Gröbnerovy báze $G, \tilde{G}$ nenulového ideálu $I$. Platí tedy $\langle LT\, G \rangle = \langle LT\, I \rangle = \langle LT\, \tilde{G} \rangle$. Protože tento ideál je monomiální,

**Řešení.** Aplikace eliminační procedury (např. v systému MAPLE za použití `gbasis` s uspořádáním `plex`) dá odpovídající implicitní popis, tj. rovnici s jediným polynomem devátého stupně:

$$-59049z - 104976z^2 - 6561y^2 - 72900z^3 - 18954y^2z -$$
$$- 23328z^4 + 32805z^2x^2 + 14580z^3x^2 + 3645z^4x^2 - 1296y^4z -$$
$$- 16767y^2z^2 - 6156y^2z^3 - 783y^2z^4 + 39366zx^2 + 19683x^2 -$$
$$- 1296y^4 - 2430z^5 + 432z^6 + 108z^7 + 486z^5x^2 - 432y^4z^2 +$$
$$+ 54y^2z^5 + 27z^6x^2 - 48y^4z^3 + 15y^2z^6 - 64y^6 - z^9.$$

□ Jak si ukážeme na následujícím jednoduchém příkladu, Gröbnerovu bázi lze využít i při počítání některých celočíselných optimalizačních úloh.

**11.107.** Jaký je minimální počet bankovek potřebný k zaplacení 77700 Kč? Uvažujte nejprve, že k dispozici máte bankovky v hodnotě 100 Kč, 200 Kč, 500 Kč, 1000 Kč. Potom předpokládejte, že máte i bankovku 2000 Kč a na konec předpokládejte, že nemáte bankovky 2000 Kč, ale máte bankovky v hodnotě 5000 Kč.

**Řešení.** Označme si bankovky po řadě proměnnými $s, d, p, t, D, P$. Platbu bude reprezentovat polynom v těchto proměnných tak, že exponent každé proměnné bude určovat počet použitých příslušných bankovek. Naříklad, pokud zaplatíme pouze ve stokorunách, bude příslušný polynom $q = s^{777}$. Pokud zaplatíme deseti tisícikoruny, deseti pětisetkorunami a stokorunami, pak bude $q = t^{10}p^{10}s^{627}$. V prvním případě bude počet bankovek 777, ve druhém $10 + 10 + 627 = 647$.
Pokud máme pouze bankovky $s, d, p, t$, pak má ideál popisující vztah jednotlivých bankovek tvar

$$I_1 = \langle s^2 - d, s^5 - p, s^{10} - t\rangle.$$

Abychom minimalizovali počet použitých bankovek, spočítáme Gröbnerovu bázi vzhledem ke gradovanému opačnému lexikografickému uspořádání (chceme eliminovat malé bankovky)

$$G_1 = (p^2 - t, s^2 - d, d^3 - sp, sd^2 - p).$$

Nyní vezmeme libovolný polynom reprezentující danou platbu. Redukcí tohoto polynomu vzhledem k bázi $G_1$ dostaneme polynom, jehož stupeň je pro naše monomiálního uspořádání minimální a je jednoduché si rozmyslet, že to je právě polynom reprezentující optimální platbu. Vezměme tedy např. $q = s^{777}$. Redukce vzhledem ke $G_1$ je pak $t^{77}pd$. To znamená, že optimální platba v prvním případě je 77 tisícikorun, jedna pětisetkoruna a jedna dvousetkoruna. Dohromady tedy 79 bankovek.

lze pro něj aplikovat Dicksonovo lemma. S odvoláním na konstrukci báze v jeho důkazu lze tvrdit, že existuje právě jedna monomiální báze monomiálního ideálu tak, že koeficienty jejích členů jsou rovny jedné a žádný z členů této báze nedělí jiný.

Podle definice minimality musí být $LT\,G$ i $LT\,\tilde{G}$ právě takovou bází. Tedy $LT\,G = LT\,\tilde{G}$. Ke každému $g \in G$ tedy existuje právě jedno $\tilde{g} \in \tilde{G}$ takové, že $LT\,g = LT\,\tilde{g}$.

Platí $g - \tilde{g} \in I$. Protože $G$ je Gröbnerova, platí $\overline{g - \tilde{g}}^{\,G} = 0$. Členy $LT\,g, LT\,\tilde{g}$ se odečtou už v $g - \tilde{g}$. Protože obě báze jsou redukované, nemůže být žádný ze zbývajících členů $g - \tilde{g}$ dělitelný kterýmkoli z $LT\,G = LT\,\tilde{G}$. Musí se tedy dostat do zbytku. Platí tedy

$$g - \tilde{g} = \overline{g - \tilde{g}}^{\,G} = 0.$$

Tím je jednoznačnost dokázána. □

**11.42. Poznámky.** Máme již k dispozici několik odpovědí na dříve položené otázky. Umíme totiž účinně rozhodnout o příslušnosti polynomu do daného ideálu pomocí dělení se zbytkem prostřednictvím Gröbnerovy báze. A umíme také pomocí redukovaných Gröbnerových bází rozhodnout, zda jsou dva ideály stejné.



Pro náš problém řešení systémů polynomiálních rovnic to znamená, že pro daný systém polynomiálních rovnic umíme rozhodnout, zda nějaká jiná polynomiální rovnice patří do jimi generovaného ideálu. Umíme také o dvou různých systémech algoritmicky rozhodnout, zda generují stejný ideál svých důsledků.

Při těchto algoritmických konstrukcích bude záležet na zvoleném uspořádání monomů, samotné odpovědi na výše uvedené otázky ale na uspořádání nezávisí.

Jak jsme zmiňovali v úvodu kapitoly, technika Gröbnerových bází je jedním ze základů počítačové algebry. Samozřejmě jsou při implementacích v programových systémech využita různá zlepšení výše uvedeného algoritmu. Např. je možné využít techniky redukcí již během vytváření Gröbnerovy báze v základním algoritmu z odstavce 11.39 apod.



V literatuře lze dohledat také různé varianty pro nekomutativní algebraické objekty (např. při formálních manipulacích s diferenciálními operátory). Algoritmus pro nalezení Gröbnerovy báze lze také interpretovat jako speciální případ Knuth-Bendixova algoritmu pro přepisovací pravidla řešící problém ekvivalentnosti slov v monoidech zadaných generátory a sadou rovností.

Konečně v samotné komutativní algebře je technika Gröbnerových bází použitelná daleko sofistikovaněji. Při průchodu naším algoritmem totiž dostáváme syzygy všech dvojic generátorů konečné báze. Tyto syzygy jsou vlastně bází tzv. podmodulu všech relací mezi $k$ prvky $g_1, \ldots, g_k$ báze, tj. podmnožiny $S$ v prostoru $(\mathbb{K}[x_1, \ldots, x_n])^k$. Na takové podmnožiny opět můžeme rozšířit samotný algoritmus a najít význačné generátory všech relací mezi generátory. Takto můžeme pokračovat, dokud existují nějaké netriviální relace. Lze dokázat, že nejpozději po $n$ takových krocích už žádné netriviální relace nebudou existovat a počty generátorů relací v jednotlivých krocích nám dávají velmi podrobnou informaci o topologických vlastnostech příslušné afinní variety $\mathfrak{V}(g_1, \ldots, g_k)$.

V druhém případě, kdy máme i bankovku $D$, je ideál $I_2 = \langle s^2 - d, s^5 - p, s^{10} - t, s^{20} - D\rangle$ a jeho Gröbnerova báze je

$$G_2 = (t^2 - D, p^2 - t, s^2 - d, d^3 - sp, sd^2 - p).$$

Redukce $q = s^{777}$ vzhledem ke $G_2$ dá $D^{38}tpd$, takže tentokrát zaplatíme 41 bankovkami. Ve třetím případě je $I_3 = \langle s^2 - d, s^5 - p, s^{10} - t, s^{50} - P\rangle$ a

$$G_3 = (t^5 - P, p^2 - t, s^2 - d, d^3 - sp, sd^2 - p),$$

a redukce je proto rovna $P^{15}t^2\,pd$. V tomto případě tedy potřebujeme pouze 19 bankovek.

Tuto jednoduchou úlohu lze samozřejmě vyřešit rychle prostou úvahou. Uvedený postup používající Gröbnerovu bázi ovšem dává univerzální algoritmus. který lze automaticky použít pro vyšší částky a jiné, složitější případy. □

Gröbnerovy báze najdou využití i v robotice. Konkrétně v inverzní kinematice, kde se zjišťuje, jak nastavit jednotlivé klouby robota, aby dosáhl určité pozice. Taková úloha často vede na soustavu nelineárních rovnic, kterou lze vyřešit právě pomocí nalezení Gröbnerovy báze, viz následující příklad.

**11.108.** Uvažujme jednoduchého robota znázorněného na obrázku, který se sestává ze tří rovných částí délky 1, které jsou spojeny nezávislými klouby, které umožňují libovolné úhly $\alpha, \beta, \gamma$. Tímto robotem chceme shora uchopit předmět ležící na zemi ve vzdálenosti $x$. Jak je potřeba nastavit úhly $\alpha, \beta, \gamma$? Načrtněte konfiguraci robota pro $x = 1, 1{,}5a\sqrt{3}$.

**Řešení.** Uvažujeme přirozeně souřadný systém, ve kterém počátek robotické ruky leží v počátku a zem odpovídá ose $x$. Z elementární trigonometrie plyne, že celkový $x$–ový dosah robota při úhlech $\alpha, \beta, \gamma$ bude roven

$$x = \sin\alpha + \sin(\alpha + \beta) + \sin(\alpha + \beta + \gamma).$$

Podobně dosah robota ve svislém směru bude

$$y = \cos\alpha + \cos(\alpha + \beta) + \cos(\alpha + \beta + \gamma).$$

Podmínka uchopení předmětu shora je zřejmě ekvivalentní podmínce $\alpha + \beta + \gamma = \pi$, a proto zadání úlohy vede na soustavu

$$\begin{aligned} \sin\alpha + \sin(\alpha + \beta) &= x,\\ \cos\alpha + \cos(\alpha + \beta) - 1 &= 0. \end{aligned}$$

Abychom z této soustavy udělali soustavu polynomiálních rovnic, zavedeme nové proměnné $s_1 = \sin\alpha$, $c_1 = \cos\alpha$, $s_2 = \sin\beta$, $c_2 = \cos\beta$, které samozřejmě splňují $s_1^2 + c_1^2 = 1$ a $s_2^2 + c_2^2 = 1$. S využitím základních trigonometrických rovnic pro součty v argumentu pak předchozí

**11.43. Eliminace proměnných.** Na závěr této části si uvedeme alespoň jednu aplikaci předchozích algoritmů.



Budeme považovat okruh $\mathbb{K}[x_{p+1}, \ldots, x_n]$ za podokruh $\mathbb{K}[x_1, \ldots, x_n]$. Jedná se o polynomy, v nichž se nevyskytují proměnné $x_1, \ldots, x_p$. Je to skutečně podokruh, ale už ne ideál.

Eliminační ideály

Nechť $I = \langle f_1, \ldots, f_s\rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Pro $p = 1, \ldots, n$ definujeme

$$I_p := I \cap \mathbb{K}[x_{p+1}, \ldots, x_n].$$

Tuto množinu nazveme *$p$-tým eliminačním ideálem.* Všimněme si, že $I_p$ je ideálem pouze v $\mathbb{K}[x_{p+1}, \ldots, x_n]$.

Na úrovni polynomiálních rovnic $I_p$ obsahuje všechny rovnice, které jsou důsledky systému $f_1 = 0, \ldots, f_s = 0$ a ve kterých vystupují pouze proměnné $x_{p+1}, \ldots, x_n$.

**Věta** (Eliminační věta)**.** *Nechť $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ je ideál, $G = \{g_1, \ldots, g_m\}$ jeho Gröbnerova báze vzhledem k $<_{lex}$. Proměnné nechť jsou uspořádány $x_1 >_{lex} x_2 >_{lex} \cdots$. Potom pro každé $p = 0, \ldots, n$ je $G_p := G \cap \mathbb{K}[x_{p+1}, \ldots, x_n]$ Gröbnerovou bází ideálu $I_p$.*

*Jestliže je $G$ minimální, resp. redukovaná, Gröbnerova báze, pak $G_p$ je opět báze minimální, resp. redukovaná.*

Důkaz. Bez újmy na obecnosti můžeme uvažovat $G_p = \{g_1, \ldots, g_r\}$. Protože $G \subseteq I$, je i $G_p \subseteq I_p$. Inkluze $\langle G_p\rangle \subseteq I_p$ platí triviálně. Dokážeme tedy inkluzi opačnou.

Pro libovolný polynom $f \in I_p$ bychom rádi ověřili, že

$$f = h_1 g_1 + \cdots + h_r g_r.$$

Provedeme za tím účelem dělení se zbytkem původní Gröbnerovou bází $G$. Protože je také $f \in I$, platí $\overline{f}^{\,G} = 0$, a tedy

$$f = h_1 g_1 + \cdots + h_r g_r + h_{r+1} g_{r+1} \cdots + h_m g_m.$$

Každý z polynomů $g_{r+1}, \ldots, g_m$ musí obsahovat nějakou z proměnných $x_1, \ldots, x_p$, jinak by byl prvkem $G_p$. Vzhledem k vlastnostem lexikografického uspořádání takovou proměnnou obsahují i $LT\,g_{r+1}, \ldots, LT\,g_m$. Uvědomíme-li si postup algoritmu pro dělení se zbytkem a skutečnost, že v $f$ není žádný monom obsahující některou z $x_1, \ldots, x_p$, musí být $h_{r+1} = \cdots = h_m = 0$. Ověřili jsem proto $f \in \langle G_p\rangle$.

Dokázali jsme nejen požadovanou inkluzi, ale i fakt, že dělení $f/G$ dopadne na $I_p$ stejně jako $f/G_p$. Pro $1 \le i < j \le r$ uvažujme $S$-polynomy $S(g_i, g_j)$. Platí

$$\overline{S(g_i, g_j)}^{\,G_p} = \overline{S(g_i, g_j)}^{\,G} = 0$$

a tedy $G_p$ je Gröbnerova báze ideálu $I_p$.

Tvrzení o minimalitě nebo redukovanosti báze je zřejmé z definic těchto pojmů. □

Jediná vlastnost lexikografického uspořádání, kterou jsme použili v důkazu, je tvrzení, že pokud se některé proměnné objevují v polynomu $f$, pak se objevují v jeho vedoucím členu. To je ovšem podstatně slabší požadavek, než definice lexikografického uspořádání. Proto lze při skutečných implementacích používat jakékoliv uspořádání, které bude zajišťovat tuto vlastnost. Dosáhne se tak většinou efektivnějších výpočtů, protože čisté lexikografické

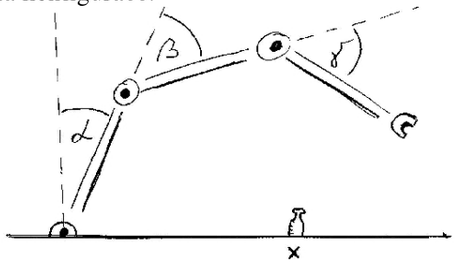
soustavu převedeme na ekvivalentní polynomiální soustavu

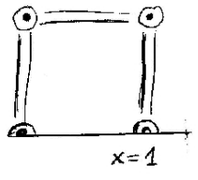
$$\begin{aligned} s_1 + s_1c_2 + c_1s_2 - x &= 0,\\ c_1 + c_1c_2 - s_1s_2 - 1 &= 0,\\ s_1^2 + c_1^2 - 1 &= 0,\\ s_2^2 + c_2^2 - 1 &= 0. \end{aligned}$$

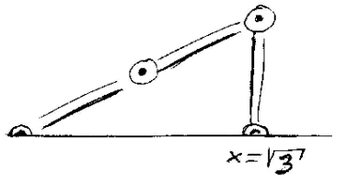
Každý výpočetní program pak v okamžiku najde Gröbnerovu bázi příslušného ideálu. Pro gradované opačné lexikografické uspořádání $s_1 > c_1 > s_2 > c_2$ dostaneme bázi

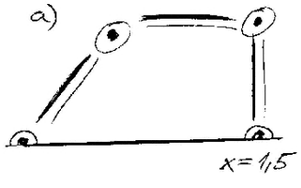
$$(2c_2 + 1 - x^2, 2c_1(1 + x^2) - 2s_2x - 1 - x^2, 2s_1(1 + x^2) +$$
$$+2s_2 - x - x^3, 4s_2^2 - 3 - 2x^2 + x^4),$$

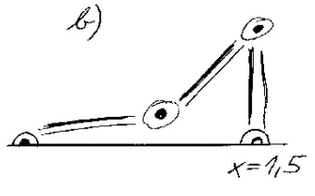
a odtud už je snadné dopočítat hodnoty proměnných v závislosti na parametru $x$. Ihned například vidíme $c_2 = \frac{x^2-1}{2}$, tj. $\beta = \arccos(\frac{x^2-1}{2})$. Především je tedy jasné, že úloha nemá řešení pro $|x| > \sqrt{3}$. Konkrétně, pro $|x| < \sqrt{3}$ má 2 různá řešení a pro $|x| = \sqrt{3}$ jedno řešení ($\alpha = \frac{\pi}{3}$, $\beta = 0$, $\gamma = \frac{2\pi}{3}$ pro kladné $x$, $\alpha = -\frac{\pi}{3}$, $\beta = 0$, $\gamma = \frac{4\pi}{3}$ pro záporné). Pro $x = 1$ dopočítáme řešení $\alpha = 0$, $\beta = \frac{\pi}{2}$, $\gamma = \frac{\pi}{2}$ a degenerované řešení $\alpha = \frac{\pi}{2}$, $\beta = -\frac{\pi}{2}$, $\gamma = \pi$. Podobně dopadne případ $x = -1$. Je dobré si uvědomit, že pro $|x| < 1$ bude vždy jedno řešení odpovídat konfiguraci robota, při které dojde k překřížení některých částí. Pro tyto hodnoty parametru $x$ tedy bude existovat jediná uskutečnitelná konfigurace.




uspořádání zpravidla vede k nepříjemnému nárůstu stupňů polynomů.

**11.44. Implicitní popis parametrizovaných variet.** Z předchozí věty lze docela snadno odvodit algoritmus pro nalezení implicitního popisu variet zadaných pomocí polynomiální parametrizace. Nebudeme se věnovat detailní diskusi, protože nemáme k dispozici všechny nástroje pro práci s nejmenšími varietami obsahujícími body zadané parametrizací. Zůstaneme proto na úrovni poznámek.

Jestliže je naše parametrizace variety dána polynomiálními vztahy

$$x_1 = f_1(u_1, \ldots, u_k), \ldots, x_n = f_n(u_1, \ldots, u_k),$$

spočteme redukovanou Gröbnerovu bázi ideálu

$$\langle x_1 - f_1, \ldots, x_n - f_n \rangle$$

v lexikografickém uspořádání, kde $u_i > x_j$ pro všechna $i, j$. Z této báze dostaneme redukovanou Gröbnerovu bázi eliminačního ideálu $I_k$ a to je přesně hledaný ideál a jeho implicitní popis.

Ve skutečnosti nám pro výpočet stačí takové uspořádání, které zaručí převahu všech $u_i$ nad $x_j$, aby se algoritmem pro výpočet Gröbnerovy báze eliminovala $u_i$, jinak může být uspořádání libovolné. Máme tak naději dosáhnout efektivnějšího výpočtu než s čistým lexikografickým uspořádáním.

Když je naše parametrizace racionální, tj.

$$x_i = \frac{f_i(t_1, \ldots, t_m)}{g_i(t_1, \ldots, t_m)},$$

asi nás hned napadne dosadit do předchozí věty ideál $\langle x_1g_1 - f_1, \ldots, x_ng_n - f_n \rangle$. To ale většinou nefunguje dobře. Například uvažujme

$$x = \frac{u^2}{v}, \quad y = \frac{v^2}{u}, \quad z = u.$$

Dostali bychom $I = \langle vx - u^2, uy - v^2, z - u \rangle$ a po eliminaci $I_2 = \langle z(x^2y - z^3) \rangle$. Správný výsledek je ale jenom $\mathfrak{V}(x^2y - z^3)$, tedy náš postup přidal navíc celou rovinu.

Problém je v tom, že zahrnujeme i celou varietu nulových bodů jmenovatelů v parametrizacích jednotlivých proměnných $W = \mathfrak{V}(g_1, \ldots, g_n)$. Raději tedy parametrizaci $F$ chápejme jako zobrazení $F : (\mathbb{K}^k - W) \to \mathbb{K}^n$. Pro implicitizaci pak použijeme ideál

$$I = \langle g_1x_1 - f_j, \ldots, g_nx_n - f_n, 1 - g_1 \cdots g_ny \rangle \subseteq$$
$$\subseteq \mathbb{K}[y, t_1, \ldots, t_m, x_1, \ldots, x_n],$$

kde si navíc pomáháme dodatečnou proměnnou $y$. Potom lze ukázat, že $V(I_{k+1})$ je minimální afinní varieta obsahující $F(\mathbb{K}^m - W)$.

### 4. Uspořádané množiny a Booleovská algebra



Z vlastností čísel nebo symetrií objektů abstrahovali podstatné axiomy a dostali jsme daleko šířeji použitelné nástroje pro úvahy v lineární algebře, při diskusi grup symetrií a jejich akcí, studium okruhů polynomů atd. Nyní budeme postupovat obdobně a okamžitě uvidíme, že jen docela drobnou změnou základních vlastností dostaneme na první pohled úplně jiné objekty. To, co zůstane podobné, je algebraická práce se symboly zastupujícími velice rozmanité objekty a tím pádem i docela univerzální použitelnost výsledků.

Za východisko si vezmeme základní operace s množinami, tj. jejich sjednocení, průnik a vztahy inkluze. Naším prvním cílem

□

Gröbnerovy báze lze využít i v softwarovém inženýrství při hledání invariantů cyklů, které jsou potřeba k ověřování správnosti algoritmů, viz následující příklad.

**11.109.** Ověřte správnost následujícího algoritmu pro výpočet součinu dvou celých čísel $a, b$.

```
(x, y, z) := (a, b, 0);
while not (y = 0) do
 if y mod 2 = 0
 then (x, y, z) := (2*x, y/2, z)
 else (x, y, z) := (2*x, (y-1)/2, x+z)
 end if
end while
return z
```

**Řešení.** Označíme-li si jako $X, Y, Z$ počáteční hodnoty proměnných $x, y, z$, pak z definice je polynom $p$ invariantem cyklu právě tehdy, když v každém kroku platí $p(x, y, z, X, Y, Z) = 0$. Takový polynom můžeme najít pomocí Gröbnerovy báze následujícím způsobem.
Označme $f_1$, $f_2$ přiřazení ve dvou větvích algoritmu, tj.

$$f_1(x, y, z) = (2x, \frac{1}{2}y, z) \text{ a } f_2(x, y, z) = (2x, \frac{y-1}{2}, x + z).$$

Pro $n$ iterací prvního okamžitě spočítáme explicitní vztah $f_1^n(x, y, z) = (2^n x, \frac{1}{2^n}y, z)$. Abychom převedli tuto iterovanou funkci na polynomialní zobrazení, zavedeme nové proměnné $u := 2^n$, $v := \frac{1}{2^n}$. Potom je $f_1^n$ dána polynomiální funkcí

$$F_1 : \quad x \mapsto ux \quad y \mapsto vy \quad z \mapsto z,$$

kde nové proměnné splňují $uv = 1$. Invariantní polynom pak zřejmě musí ležet v ideálu

$$I_1 = \langle ux - X, vy - Y, z - Z, uv - 1\rangle.$$

Abychom takový polynom našli, stačí odtud eliminovat proměnné $u$ a $v$, což můžeme dobře udělat právě pomocí Gröbnerovy báze vzhledem ke gradovanému opačnému lexikografickému uspořádání s $u > v > x > y > z$. Ta je rovna

$$(xy - XY, z - Z, x - vX, y - uY).$$

Odtud $F_1(xy - XY) = xy - XY$ a $F_1(z - Z) = z - Z$ a všechny další polynomy invariantní vyhledem k libovolnému počtu $n$ aplikací $f_1$ jsou dány polynomem v (polynomech) $xy - XY$ a $z - Z$.
Podobnou úvahu teď provedeme pro $f_2$. Pro $n$ iterací odvodíme vztah

$$f_2^n(x, y, z) = (2^n x, \frac{1}{2^n}(y + 1) - 1, (2^n - 1)x + z),$$

bude uvést tyto operace do souvislosti s výrokovou logikou (tj. formalizovanými postupy pro vyjadřování výroků a vyhodnocování jejich pravdivosti).

**11.45. Množinová algebra.** S každou množinou $M$ máme k dispozici také množinu $K = 2^M$ všech jejích podmnožin a na ní operace $\vee : K \times K \to K$ sjednocení množin a $\wedge : K \times K \to K$ průniku množin. To jsou dvě *binární operace*, které jsme dosud značili $\cup$ a $\cap$.

Dále máme ke každé množině $A \in K$ také její množinu doplňkovou $A' = K \setminus A$, což je další *unární operace*.

Konečně máme „největší objekt“, tj. celou množinu $M$, který je neutrální vůči operaci $\wedge$ a který proto budeme v této souvislosti označovat jako 1. Obdobně se chová prázdná množina $\emptyset \in K$ vůči operaci $\vee$. Tu budeme v této souvislosti značit jako 0.

Na množině $K$ všech podmnožin v $M$ můžeme velmi snadno ověřit pro všechny prvky $A, B, C$ následující vlastnosti (již jsme definovali význačné prvky $0 = \emptyset$ a $1 = M$ a unární operaci vzetí doplňku $A'$ k podmnožině $A$):

(1) $A \wedge (B \wedge C) = (A \wedge B) \wedge C$,
(2) $A \vee (B \vee C) = (A \vee B) \vee C$,
(3) $A \wedge B = B \wedge A$, $A \vee B = B \vee A$,
(4) $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$,
(5) $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$,
(6) existuje $0 \in K$ tak, že $A \vee 0 = A$,
(7) existuje $1 \in K$ tak, že $A \wedge 1 = A$,
(8) $A \wedge A' = 0$, $\quad A \vee A' = 1$.

Porovnejme si tyto vlastnosti s vlastnostmi okruhů:



První dvě z nich, tj. (1) a (2) říkají, že obě operace $\wedge$ a $\vee$ jsou asociativní. Vlastnost (3) konstatuje komutativitu obou operací.

Až potud je tedy vše jako u číselných oborů a operací sčítání a násobení. Zásadní změnou jsou ale další dvě vlastnosti (4) a (5), protože ty vyžadují jak distributivitu operace $\vee$ vůči průniku $\wedge$, tak naopak. To pochopitelně u sčítání a násobení čísel nejde — máme tam pouze distributivitu sčítání vůči násobení, ale ne naopak.

Poslední tři vlastnosti (6) – (8) konstatují existenci neutrálních prvků vůči oběma operacím, ale také existenci obdoby k „inverzím“ ke všem prvkům (ale všimněme si, že průnikem s komplementem chceme dostat neutrální prvek ke sjednocení a naopak, tedy odlišně od vzetí inverzí v okruzích). Jistě nás nepřekvapí, když za chvíli uvidíme, že takto silně provázané vlastnosti dvou různých operací nemůže mít příliš mnoho objektů.

### Booleovské algebry

**Definice.** Množině $K$ spolu s dvěma binárními operacemi $\wedge$ a $\vee$ a jednou unární operací $'$ splňující vlastnosti (1)–(8) říkáme *Booleovská algebra*. Operaci $\wedge$ budeme říkat *infimum* (případně *průnik*, anglicky často také *meet*), operaci $\vee$ budeme říkat *supremum* (případně *sjednocení*, anglicky také *join*). Prvku $A'$ se říká *doplněk* k prvku $A$.

a po zavedení proměnných $u$ a $v$ dostaneme ekvivalentní polynomiální funkci

$$F_2: \quad x \mapsto ux \quad y \mapsto v(y+1)-1 \quad z \mapsto (u-1)x+z.$$

Invariantní polynom pro $F_2$ pak získáme stejně jako v předchozím případě pomocí Gröbnerovy báze příslušného ideálu. Nás ale zajímají polynomy, které jsou invariantní jak pro $F_1$, tak i pro $F_2$. Ty zřejmě musí ležet v ideálu

$$I_2 = \langle F_2(xy - XY),\, F_2(z-Z),\, uv-1\rangle.$$

Dosazením za $F_2$ dostaneme

$$I_2 = \langle uxv(y+1) - ux - XY,\, (u-1)x + z - Z,\, uv-1\rangle$$

a pomocí Gröbnerovy báze tohoto ideálu eliminujeme proměnné $u$ a $v$ a najdeme polynom $xy - XY + z - Z$, který je invariantní jak pro $F_1$, tak pro $F_2$ a je to tedy invariant daného cyklu. Vzhledem k počátečním podmínkám $X = a$, $Y = b$, $Z = 0$ vidíme, že během celého programu platí $xy - ab + z = 0$. Na konci cyklu bude platit $y = 0$, a proto bude výsledek opravdu $z = ab$. □

Nyní ukážeme několik příkladů, ve kterých využijeme Gröbnerovy báze k řešení různých polynomiálních soustav. V těchto příkladech nebude primárním cílem najít Gröbnerovu bázi, ale vyřešit danou soustavu.

**11.110.** Pomocí Gröbnerovy báze vyřešte polynomiální soustavu

$$x^3 - 2xy = 0,$$
$$x^2 y + x - 2y^2 = 0.$$

**Řešení.** Označme $f_1 := x^3 - 2xy$, $f_2 := x^2 y + x - 2y^2$. Báze $(f_1, f_2)$ není Gröbnerova, protože například $LM(yf_1 - xf_2) = x^2 \notin (x^3, x^2 y) = (LM(f_1), LM(f_2))$. Musíme tedy k bázi přidat právě polynom

$$yf_1 - xf_2 = -x^2.$$

Vzniklou bázi pak můžeme redukovat tím, že polynomy $f_1, f_2$ vydělíme $x^2$. Tak dostaneme bázi

$$\left(xy,\, x - 2y^2,\, x^2\right).$$

První polynom ovšem můžeme vydělit druhým se zbytkem $2y^3$ a třetí druhým se zbytkem $4y^4$. Dostáváme tak bázi

$$\left(x - 2y^2,\, y^3\right)$$

a ta už je Gröbnerova: podle naivního algoritmu (viz 11.39) stačí pouze ověřit, že polynom

$$S\left(x - 2y^2, y^3\right) = y^3\left(x - 2y^2\right) - xy^3 = -2y^5$$

Všimněme si, že axiomy Booleovské algebry jsou zcela symetrické vůči záměně operací $\wedge$ a $\vee$, společně se záměnou prvků 0 a 1. Důsledkem tohoto faktu je, že jakékoliv tvrzení, které odvodíme z axiomů, má také platné *duální tvrzení*, které vznikne z prvého právě záměnou všech výskytů $\wedge$ za $\vee$ a naopak a stejně tak všech výskytů 0 a 1. Hovoříme o *principu duality*.

**11.46. Vlastnosti Booleovských algeber.** Jako obvykle si hned odvodíme několik elementárních důsledků axiomů. Zejména si povšimněme, že tak dokážeme u speciálního případu Booleovské algebry všech podmnožin v dané množině $M$ elementární vlastnosti známé z množinové algebry. Např. je doplněk k $A \in K$ určen svými vlastnostmi jednoznačně. V obecném pohledu však toto pozorování říká, že máme-li dáno $(K, \wedge, \vee)$, může existovat nejvýše jedna unární operace $'$, se kterou dostaneme Booleovskou algebru $(K, \wedge, \vee, ')$.

Skutečně pokud $B, C \in K$ splňují vlastnosti $A'$ (tj. poslední axiom (8) v definici výše), platí

$$B = B \vee 0 = B \vee (A \wedge C) =$$
$$= (B \vee A) \wedge (B \vee C) = 1 \wedge (B \vee C) = B \vee C$$

a stejně také spočteme

$$C = C \vee B.$$

Je tedy nutně $B = C$. Všimněme si, že použitím tohoto výsledku na prvky 1 a 0, společně s jejich definicí, okamžitě dostáváme jednoznačnost pro tyto výjimečné prvky v libovolné Booleovské algebře (promyslete si podrobně!).

Vlastnosti v následujícím tvrzení mají svá zavedená jména v množinové algebře: vlastnosti (2) se říká *absorpční zákony*, vlastnosti (3) popisují *idempotentnost* operací $\wedge$ a $\vee$ a rovnosti (4) jsou známy jako *De Morganova pravidla*.



**Tvrzení.** *V každé Booleovské algebře $(K, \wedge, \vee, ')$ platí pro všechny prvky v $K$:*

*(1)* $A \wedge 0 = 0, \quad A \vee 1 = 1,$
*(2)* $A \wedge (A \vee B) = A, \quad A \vee (A \wedge B) = A,$
*(3)* $A \wedge A = A, \quad A \vee A = A,$
*(4)* $(A \wedge B)' = A' \vee B', \quad (A \vee B)' = A' \wedge B',$
*(5)* $(A')' = A.$

Důkaz. Podle principu duality potřebujeme z každého z duálních tvrzení na jednotlivých řádcích dokázat pouze jedno. Počítejme s využitím axiomů:

Začneme s vlastností (3)

$$A = A \wedge 1 = A \wedge (A \vee A') = (A \wedge A) \vee 0 = A \wedge A.$$

Nyní už umíme snadno (1)

$$A \wedge 0 = A \wedge (A \wedge A') = (A \wedge A) \wedge A' = A \wedge A' = 0$$

a pak je snadné i (2)

$$A \wedge (A \vee B) = (A \vee 0) \wedge (A \vee B) =$$
$$= A \vee (0 \wedge B) = A \vee 0 = A.$$

K důkazu De Morganových pravidel stačí ověřit, že $A' \vee B'$ má vlastnosti doplňku k $A \wedge B$, pak to totiž bude doplněk dle úvahy výše. S využitím (1) spočteme

$$(A \wedge B) \wedge (A' \vee B') = ((A \wedge B) \wedge A') \vee ((A \wedge B) \wedge B') =$$
$$= (0 \wedge B) \vee (A \wedge 0) = 0.$$

dává zbytek nula vůči bázi $\left(x-2y^2, y^3\right)$, dokonce v libovolném uspořádání na polynomech. Řešením soustavy je zřejmě bod $(0,0)$. □

**11.111.** Je dána soustava polynomiálních rovnic

$$\begin{aligned} x^2yz^2 + x^2y^2 + yz - xyz^2 - z^2 &= 0,\\ x^2y + z &= 0,\\ xyz + z + 1 &= 0. \end{aligned}$$

Seřaďte monomy polynomů podle lexikografického uspořádání s $x > y > z$, pak vydělte první polynom druhým a třetím a výsledek využijte k vyřešení soustavy v oboru reálných čísel.

**Řešení.**

$$\begin{aligned} x^2y^2 + x^2yz^2 - xyz^2 + yz - z^2 &= \left(y+z^2\right)\left(x^2y+z\right) -\\ &\quad - y(xyz+z+1) - z^3 + z. \end{aligned}$$

Odtud $z = 0, \pm 1$. Potom např.

$$\begin{aligned} 0 &= z\left(x^2y+z\right) - x(xyz+z+1) =\\ &= z^2 - zx - x. \end{aligned}$$

Odtud $x = \frac{z^2}{z+1}$ a z třetí rovnice $y = -\frac{(1+z)^2}{z^3}$. Vyhovuje jediný reálný bod $\left(\frac{1}{2}, -4, 1\right)$. □

**11.112.** Pomocí Gröbnerovy báze vyřešte polynomiální soustavu

$$\begin{aligned} x^2 + y + z &= 1,\\ x + y^2 + z &= 1,\\ x + y + z^2 &= 1. \end{aligned}$$

**Řešení.** Označme $f_1 := x + y + z^2 - 1$. Zbytek po dělení polynomu $x + y^2 + z - 1$ polynomem $f_1$ je

$$f_2 = y^2 - y - z^2 + z.$$

Zbytek po dělení polynomu $x^2 + y + z - 1$ polynomem $f_1$ je $y^2 + 2yz^2 - y + z^4 - 2z^2 + z$ a dalším dělením polynomem $f_2$ dostaneme zbytek

$$f_3 = 2yz^2 + z^4 - z^2.$$

Báze $(f_1, f_2, f_3)$ ještě není Gröbnerova. Tu zkonstruujeme volbou $g_1 := f_1$, $g_2 := f_2$ a místo $f_3$ vezmeme $S$-polynom

$$2z^2 f_2 - y f_3 = -yz^4 - yz^2 - 2z^4 + 2z^3.$$

Potom dělením polynomem $f_3$ dostaneme zbytek

$$\begin{aligned} g_4 &= z^6 - 4z^4 + 4z^3 - z^2 =\\ &= z^2(z-1)^2\left(z^2+2z-1\right). \end{aligned}$$

Obdobně, s použitím (2) dostáváme

$$\begin{aligned} (A \wedge B) \vee (A' \wedge B') &= (A \vee (A' \vee B')) \vee (B \vee (A' \vee B')) =\\ &= (1 \vee B') \wedge (1 \vee A') = 1. \end{aligned}$$

Konečně přímo z definice je $A' \wedge A = 0$ a $A' \vee A = 1$, má proto $A$ požadované vlastnosti doplňku k $A'$ a je tedy $A = (A')'$. □

**11.47. Příklady Booleovských algeber.** Nejmenší zajímavá algebra je množina všech podmnožin jednoprvkové množiny $M$. Ta má právě dva prvky $0 = \emptyset$ a $1 = M$. Operace $\wedge$ a $\vee$ v tomto případě splývají s násobením a sčítáním v okruhu zbytkových tříd $\mathbb{Z}_2$, proto budeme nadále hovořit o Booleovské algebře $\mathbb{Z}_2$.



Podobně jako u vektorových prostorů a okruhů můžeme algebraickou strukturu Booleovské algebry přenášet na prostory funkcí, jejichž obor hodnot Booleovskou algebrou je. Skutečně pro množinu všech funkcí $S = \{f : M \to K\}$ z množiny $M$ do Booleovské algebry $(K, \wedge, \vee, ')$ definujeme potřebné operace a vybrané prvky 0 a 1 na $S$ jako funkce v argumentu $x \in M$ takto:

$$\begin{aligned} (f_1 \wedge f_2)(x) &= (f_1(x)) \wedge (f_2(x)) \in K,\\ (f_1 \vee f_2)(x) &= (f_1(x)) \vee (f_2(x)) \in K,\\ (1)(x) &= 1 \in K,\ (0)(x) = 0 \in K,\\ (f)'(x) &= (f(x))' \in K. \end{aligned}$$

Ověření, že tyto nové operace skutečně zadávají Booleovskou algebru je zcela přímočaré a jednoduché.

Připomeňme, že všechny podmnožiny dané množiny $M$ lze interpretovat jako zobrazení $M \to \mathbb{Z}_2$, když na jedničku zobrazíme právě body vybrané podmnožiny. Pak skutečně můžeme sjednocení a průnik definovat výše uvedeným způsobem — např. o každém bodu $x \in M$ rozhodujeme u $(A \wedge B)(x)$, zda patří do $A$ a zda patří do $B$ a vezmeme sjednocení výsledků v $\mathbb{Z}_2$, tj. výsledek bude 1, právě když $x$ padne do sjednocení.

**11.48. Výroková logika.** V předchozích odstavcích jsme použili symboliku, kterou je často rozumné interpretovat tak, že z prvků $A, B, \ldots \in K$ tvoříme „slova“ pomocí operací $\vee, \wedge, '$ a závorek vyjasňujících v jakém pořadí a na jaké argumenty jsou operace aplikovány. Samotné axiomy Booleovských algeber a jejich důsledky pak říkají, že velice často různá slova dávají stejnou hodnotu výsledku v $K$.



V případě množiny všech podmnožin $K = 2^M$ je to zřejmé – prostě jde o rovnost podmnožin. Nyní uvedeme stručně jinou podobnou souvislost.

Budeme pracovat opět se slovy jako výše, interpretujeme je ale jako tvrzení složené z elementárních výroků $A, B, \ldots$ a logických operací AND (binární operace $\wedge$), OR (binární operace $\vee$) a negace NOT (unární operace $'$). Taková slova nazýváme *výroky* a přiřazujeme jim pravdivostní hodnotu v závislosti na pravdivostní hodnotě jednotlivých elementárních argumentů. Pravdivostní hodnotu přitom bereme jako prvek z triviální Booleovy algebry $\mathbb{Z}_2$, tedy buď 0 nebo 1. Pravdivostní hodnota výroku je plně určena přiřazením hodnot pro nejjednodušší výroky $A \wedge B$, $A \vee B$ a $A'$, tj. $A \wedge B$ je pravdivé, pouze když jsou oba výroky $A$ a $B$ pravdivé, $A \vee B$ je nepravdivé, pouze když jsou oba výroky nepravdivé, a $A'$ má opačnou hodnotu než $A$.

Výrok obsahující $n$ elementárních výroků tedy představuje funkci $(\mathbb{Z}_2)^n \to \mathbb{Z}_2$ a dva výroky nazýváme logicky ekvivalentní,

Báze $(g_1, g_2, g_3)$ už je Gröbnerova a proto můžeme úlohu vyřešit zpětnou eliminací. Z $g_4 = 0$ máme $z = 0,\ 1,\ -1 \pm \sqrt{2}$. Dosazením do $g_2 = 0$ a $g_1 = 0$ dostaneme řešení $(1, 0, 0), (0, 1, 0), (0, 0, 1), \big(-1 + \sqrt{2}, -1 + \sqrt{2}, -1 + \sqrt{2}\big), \big(-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2}\big)$. □

**11.113.** Vyřešte v $\mathbb{R}$ soustavu polynomiálních rovnic



$$\begin{aligned} &x^2 - 2xz - 4,\\ &x^2y^2z + yz^3,\\ &2xy^2 - 3z^3. \end{aligned}$$

**Řešení.** Báze vhodná pro eliminaci proměnných je Gröbnerova báze pro lexikografické monomiální uspořádání s $x > y > z$. Použitím programu Maple tak najdeme bázi

$$\begin{aligned} 144z^5 + 35z^7 + 12z^9,\\ 23z^6 + 12z^8 + 44yz^4,\\ yz^3 + 3z^5 + 4zy^2, 9z^4 + 4y^3,\\ -8y^2 - 6z^4 + 3xz^3, 2xy^2 - 3z^3,\\ x^2 - 2xz - 4. \end{aligned}$$

Protože pro diskriminant prvního polynomu báze (vyděleného $z^5$) platí $35^2 - 4.144.7 < 0$, musí být $z = 0$. Dosazením do dalších polynomů pak hned dostáváme $y = 0, x = \pm 2$. □

**11.114.** Vyřešte v $\mathbb{R}$ soustavu polynomiálních rovnic

$$\begin{aligned} xy + yz - 1,\\ yz + zw - 1,\\ zw + wx - 1,\\ wx + xy - 1. \end{aligned}$$

**Řešení.** V tomto případě se hodí uvažovat gradované lexikografické uspořádání $w > x > y > z$. Algoritmem 11.39 nebo opět pomocí výpočetních programů najdeme příslušnou Gröbnerovu bázi

$$(x - z, w - y, 2yz - 1).$$

Řešením je pak množina bodů $(\frac{1}{2t}, t, \frac{1}{2t}, t)$ pro libovolné $0 \neq t \in \mathbb{R}$. □

**11.115.** Vyřešte v $\mathbb{R}$ soustavu polynomiálních rovnic

$$\begin{aligned} x^2 + yz + x,\\ z^2 + xy + z,\\ y^2 + xz + y. \end{aligned}$$

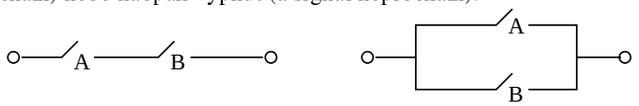
**Řešení.** Podle algoritmu 11.39 nebo raději s pomocí programu Maple nalezneme Gröbnerovu bázi pro lexikografické monomiální jestliže zadávají stejnou funkci. V předchozím příkladu jsme již ověřili, že na množině tříd logicky ekvivalentních výroků je dána struktura Booleovy algebry. Nutně tedy pro výrokovou logiku bude v tomto smyslu platné vše, co dokážeme pro obecné Booleovy algebry.

Stručně si proberme, jak vypadají obvyklé další jednoduché výroky ve výrokové logice jakožto prvky Booleovy algebry (tj. reprezentujeme vždy naším výrazem třídu výroků ekvivalentních):

Implikaci $A \Rightarrow B$ dostaneme jako $A' \vee B$, ekvivalenci $A \Leftrightarrow B$ odpovídá $(A \wedge B) \vee (A' \wedge B')$. Dále vylučovací OR, neboli XOR, je dáno jako $(A \wedge B') \vee (A' \wedge B)$, negace $NOR$ operace $OR$ je vyjádřena jako $A' \wedge B'$ a negace NAND operace AND je dána jako $A' \vee B'$. Konečně tautologie je dána pomocí libovolného elementárního výroku jako $A \vee A'$.

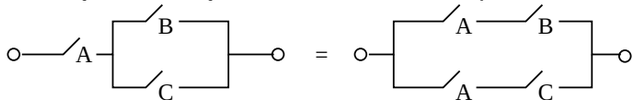
Všimněme si také, že $XOR$ odpovídá v množinové algebře symetrickému rozdílu množin.

**11.49. Přepínače jako Booleova algebra.** Přepínač je pro nás černá skříňka, která má jen dva stavy, buď je zapnut (a signál prochází) nebo naopak vypnut (a signál neprochází).




Jeden nebo více přepínačů zapojujeme do sítě sériově nebo paralelně. Sériové zapojení je popsáno pomocí binární operace $\wedge$, paralelní je naopak $\vee$. Unární operace $A'$ zadává přepínač, který je vždy v opačné poloze než $A$. Každé konečné slovo vytvořené pomocí přepínačů $A, B, \ldots$ a operací $\wedge, \vee$ a $'$ umíme převést na obrázek, který bude představovat systém přepínačů propojených dráty a zcela obdobně jako v minulém odstavci nám každá volba poloh jednotlivých přepínačů zadá hodnotu „zapnuto/vypnuto“ pro celý systém.

Opět se snadno krok po kroku ověří platnost základních axiomů Booleových algeber pro náš systém. Na následujícím obrázku je ilustrován jeden z axiomů distributivity.




Propojení bez přepínače odpovídá prvku 1, koncové body bez propojení (nebo sériové zapojení $A$ a $A'$) dává prvek 0. Nakreslete si obrázky pro všechny axiomy Booleovské algebry a ověřte si je!

**11.50. Dělitelé.** Dalším přirozeným příkladem Booleovské algebry může být systém dělitelů přirozeného čísla nebo polynomu.



Začněme trochu obecněji a zvolme pevně takové přirozené číslo $p \in \mathbb{N}$ nebo polynom $p \in \mathbb{K}[x_1, \ldots, x_s]$ nad oborem integrity $\mathbb{K}$ s jednoznačným rozkladem. Za nosnou množinu $D_p$ bereme množinu všech dělitelů $q$ našeho $p$. Pro dva takové dělitele definujeme $q \wedge r$ jako největší společný dělitel prvků $q$ a $r$, $q \vee r$ je nejmenší společný násobek. Dále definujeme význačný prvek $1 \in D_p$ jako naše číslo nebo polynom $p$ a neutrálním prvkem 0 vůči supremu na $D_p$ je jednička v $\mathbb{N}$, resp. $1 \in \mathbb{K} \subseteq \mathbb{K}[x_1, \ldots, x_s]$. Unární operaci $'$ definujeme pomocí dělení: $q' = p/q$.

**Lemma.** *Množina $D_p$ spolu s výše uvedenými operacemi $\wedge, \vee$ a $'$ je Booleovská algebra, právě když rozklad $p$ na nerozložitelné faktory neobsahuje žádné kvadráty (tj. v jednoznačném*

uspořádání s $x > y > z$ složenou ze šesti polynomů:

$$z^2 + 3z^3 + 2z^4,$$
$$z^2 + z^3 + 2yz^2 + 2yz^3,$$
$$y - yz - z - z^2 - 2yz^2 + y^2,$$
$$yz + z + z^2 + 2yz^2 + xz,$$
$$z^2 + xy + z,\ x^2 + yz + x.$$

První polynom v této bázi má kořeny $z = 0, -1, -\frac{1}{2}$. Rozborem jednotlivých případů zjistíme, že řešením soustavy jsou právě body $(0,0,0)$, $(-1,0,0)$, $(0,-1,0)$, $(0,0,-1)$ a $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2})$. □

### J. Booleovy algebry a svazy

**11.116.** Nalezněte (úplnou) disjunktivní normální formu výrazu

$$\big(B' \Rightarrow C\big) \wedge [(A \vee C) \wedge B]'.$$

**Řešení.**



Obsahuje-li formule relativně málo proměnných (v našem případě tři), je nejvýhodnější sestavit pravdivostní tabulku daného výrazu a z ní úplnou disjunktivní normální formu odečíst. Tabulka bude obsahovat $2^3 = 8$ řádků. Označme ještě zkoumanou formuli písmenem $\varphi$.

| $A$ | $B$ | $C$ | $B' \Rightarrow C$ | $[(A \vee C) \wedge B]'$ | $\varphi$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 0 |

Výsledná úplná disjunktivní normální forma je dána disjunkcí formulí odpovídajícím řádkům, které mají v posledním sloupečku jedničku (daná formule je pro danou volbu základních proměnných pravdivá). Řádku pak odpovídá konjunkce daných proměnných (je-li hodnota proměnné 1), případně jejich negací (je-li hodnota 0). V našem případě píšeme disjunkci konjunkcí odpovídajících druhému, třetímu a šestému řádku, tedy formuli

$$(A' \wedge B' \wedge C) \vee (A' \wedge B \wedge C') \vee (A \wedge B' \wedge C).$$

Formuli můžeme také přepisovat pomocí rozepsání logické spojky $\Rightarrow$ pomocí spojek $\wedge$ a $\vee$, de Morganových pravidel a distributivních zákonů:

*rozkladu $p = q_1 \dots q_n$ na nerozložitelné faktory jsou všechna $q_i$ po dvou různá).*

Důkaz. Ověření axiomů je vcelku snadné, projdeme jeden po druhém a budeme zkoumat, kdy je zapotřebí našeho požadavku na nepřítomnost kvadrátů v rozkladu.

Největší společný dělitel konečného počtu čísel nebo polynomů nezávisí na pořadí, ve kterém jej počítáme. Stejně tak pro nejmenší společný násobek. To odpovídá axiomům (1) a (2) v 11.45. Komutativita, tj. axiom (3), je zcela zřejmá.

Pro tři libovolné prvky $a$, $b$ a $c$ můžeme bez újmy na obecnosti psát jejich rozklad ve tvaru $a = q_1^{p_1} \dots q_s^{p_s}$, $b = q_1^{m_1} \dots q_s^{m_s}$ a $c = q_1^{k_1} \dots q_s^{k_s}$, kde připouštíme i mocniny 0 a všechny prvky $q_j$ jsou po dvou nesoudělné. Prvek $a \wedge b \in D_p$ je tedy prvek s rozkladem, ve kterém se objeví všechna společná $q_i$ v mocnině, která bude minimem z mocnin v $a$ a $b$. Naopak $a \vee b$ bude mít rozklad, ve kterém se objeví všechny členy z rozkladů $a$ a $b$ a to s mocninou, která bude tou větší z mocnin příslušného faktoru v $a$ a $b$. Z této úvahy nyní snadno plynou distributivní zákony (4) a (5) z 11.45.

Problém nemáme ani s existencí prvků 0 a 1, které jsme přímo definovali a zjevně splňují axiomy (6) a (7). Případná existence kvadrátů v rozkladech ale znemožní určení doplňku. Např. v $D_{12} = \{1,2,3,4,6,12\}$ nelze $6 \wedge 6' = 1$ dosáhnout, protože má 6 netriviálního společného dělitele se všemi ostatními prvky v $D_{12}$ mimo jedničku, ta ovšem nesplňuje $6 \vee 1 = 12$.

Pokud ovšem nejsou v rozkladu čísla nebo polynomu $p$ kvadráty, definujeme doplněk pomocí dělení jako $q' = p/q$ a snadno ověříme potřebné vlastnosti z axiomů (6)–(8). □

**11.51. Částečná uspořádání.** K Booleovským algebrám teď



půjdeme z jiné strany. Základní strukturou pro nás bude pojem *uspořádání*. Vzpomeňme na definici uspořádání jakožto reflexivní, antisymetrické a tranzitivní relace $\leq$ na množině $K$. Taková relace obecně neříká o každé dvojici $a, b \in K$, jestli je $a \leq b$ nebo $b \leq a$ (takové uspořádání se nazývá *úplné uspořádání* nebo dobré uspořádání). Často v našem případě obecného uspořádání proto hovoříme také o *částečném uspořádání* a množina $(K, \leq)$ vybavená částečným uspořádáním se nazývá *uspořádaná množina*[7].

Takové uspořádání je zejména vždy na množině $K = 2^M$ všech podmnožin množiny $M$ prostřednictvím inkluze podmnožin. Pomocí naší relace infima na $K$ je můžeme definovat jako $A \subseteq B$, právě když $A \wedge B = A$. Ekvivalentně $A \subseteq B$, právě když $A \vee B = B$.

**Lemma.** *Je-li $(K, \wedge, \vee, ')$ Booleova algebra, pak relace $\leq$ definovaná vztahem $A \leq B$, právě když $A \wedge B = A$, je částečné uspořádání. Navíc pro všechny prvky $A, B, C \in K$ platí:*

*(1)* $A \wedge B \leq A$,
*(2)* $A \leq A \vee B$,
*(3) jestliže $A \leq C$ a zároveň $B \leq C$, pak také $A \vee B \leq C$,*
*(4) $A \leq B$, právě když $A \wedge B' = 0$,*
*(5)* $0 \leq A$ *a* $A \leq 1$.

Důkaz. Všechny dokazované vlastnosti a vztahy jsou výsledkem jednoduchého výpočtu v Booleovské algebře $K$. Začněme s vlastnostmi uspořádání pro $\leq$. Reflexivita je přímým důsledkem

[7] I v české literatuře se také používá název *poset* z anglického „partially ordered set“, který zdůrazňuje, že jde o částečné uspořádání, tj. ne každá dvojice prvků je srovnatelná

$$
\begin{aligned}
&\big(B' \Rightarrow C\big) \wedge [(A \vee C) \wedge B]' \iff \\
\iff &(B \vee C) \wedge \big[(A \vee C)' \vee B'\big] \iff \\
\iff &(B \vee C) \wedge \big[\big(A' \wedge C'\big) \vee B'\big] \iff \\
\iff &\big[(B \vee C) \wedge \big(A' \wedge C'\big)\big] \vee \big[(B \vee C) \wedge B'\big] \iff \\
\iff &\big[\big(B \wedge A' \wedge C'\big) \vee \big(C \wedge A' \wedge C'\big)\big] \vee \big[\big(B \wedge B'\big) \vee \big(C \wedge B'\big)\big] \iff \\
\iff &\big(B \wedge A' \wedge C'\big) \vee \big(C \wedge B'\big),
\end{aligned}
$$

což již je (neúplná) disjunktivní normální forma dané formule. Tato formule je zjevně ekvivalentní úplné disjunktivní normální formě dané formule, kterou jsme odvodili z tabulky (slovo „úplná“ znamená, že se ve formuli objevují pouze konjunkce všech tří proměnných či jejich negací). □

*11.117.* Nalezněte disjuktivní normální formu výrazu

$$((A \wedge B) \vee C)' \wedge (A' \vee (B \wedge C' \wedge D))$$

○

V logice známe několik logických spojek: $\wedge$, $\vee$, $\Longrightarrow$, $\equiv$. A také operátor $'$. Libovolnou výrokovou formuli užívajících těchto spojek lze pravdivostně ekvivalentně zapsat použitím pouze některých z nich, například spojkou $\vee$ a operátorem $'$. Existují i spojky NAND a NOR ($A \,\mathrm{NAND}\, B = (A \wedge B)'$, $A \,\mathrm{NOR}\, B = (A \vee B)'$). Tyto spojky mají tu vlastnost, že pomocí pouze jedné znich lze pravdivostně ekvivalentně zapsat libovolnou výrokovou formuli (čtenář si rozmyslí, že uvedené základní spojky i operátor $'$ lze pomocí jak spojky NAND, tak pouze pomocí spojky NOR ekvivalentně vyjádřit). Tyto spojky lze implementovat v elektrických obvodech pomocí tzv. „brán“.

*11.118.* Vyjádřete výrokovou formuli $(A \Rightarrow B)$ pomocí obvodu obsahujícího pouze hradlo NAND. ○

**11.119.** Zjednodušte výraz

$$((A \wedge B) \vee (A \Rightarrow B)) \wedge ((B' \Rightarrow C) \vee (B \wedge C')).$$

**Řešení.** Přepsáním do Booleovy algebry dostáváme

$$(a \cdot b + a' + b) \cdot (b + c + b \cdot c') = \cdots = a' \cdot c + b.$$

To znamená, že výše uvedená formule je ekvivalentní výroku $(A' \wedge C) \vee B$. □

idempotence: $A \wedge A = A$, tj. $A \leq A$. Podobně komutativita pro $\wedge$ zaručuje antisymetrii $\leq$, protože z $A \wedge B = A$ a zároveň $B \wedge A = B$ vyplývá

$$A = A \wedge B = B \wedge A = B.$$

Konečně z platnosti $A \wedge B = A$ a $B \wedge C = B$ vyvodíme

$$A \wedge C = (A \wedge B) \wedge C = A \wedge (B \wedge C) = A \wedge B = A,$$

což ověřuje tranzitivitu relace $\leq$.

Dále počítáme $(A \wedge B) \wedge A = (A \wedge A) \wedge B = A \wedge B$, takže $A \wedge B \leq A$.

Ze vztahu $A \wedge (A \vee B) = A$, viz 11.46(2), plyne $A \leq A \vee B$, což dokazuje tvrzení (2).

Distributivita společně s předpokladem (3) dává

$$(A \vee B) \wedge C = (A \wedge C) \vee (B \wedge C) = A \vee B,$$

takže skutečně platí (3).

Tvrzení (5) plyne přímo z axiomů pro význačné prvky 1 a 0.

Zbývá nám tvrzení (4). Jestliže $A \leq B$, pak $A \wedge B' = A \wedge B \wedge B' = 0$. Naopak je-li $A \wedge B' = 0$, pak $A = A \wedge 1 = A \wedge (B \vee B') = (A \wedge B) \vee (A \wedge B') = (A \wedge B) \vee 0 = A \wedge B$. Odtud $A \leq B$ a důkaz je ukončen. □

Všimněme si, že stejně jako v případě algebry podmnožin je v Booleovských algebrách $A \wedge B = A$, právě když je $A \vee B = B$. Skutečně je-li $A \wedge B = A$, pak z absorpčních zákonů plyne $A \vee B = (A \wedge B) \vee B = B$ a naopak. Můžeme proto pro definici částečného uspořádání stejně dobře používat také operaci $\vee$.

**11.52. Svazy.** Viděli jsme, že každá Booleova algebra zadává uspořádanou množinu $(K, \leq)$. Zdaleka ne každá uspořádaná množina ovšem vzniká takovýmto způsobem. Např. triviální částečné uspořádání, kdy $A \leq A$ pro všechny $A$ a všechny dvojice různých prvků jsou nesrovnatelné, samozřejmě z Booleovy algebry vzniknout nemůže, pokud je v $K$ více než jeden prvek (viděli jsme, že největší a nejmenší prvek v Booleově algebře je totiž srovnatelný s každým prvkem). Zkusme se zamyslet, do jaké míry lze z uspořádání budovat operace $\wedge$ a $\vee$.



Pracujme s pevně zvolenou uspořádanou množinou $(K, \leq)$. O prvku $C \in K$ řekneme, že je *dolní závorou* pro nějakou množinu prvků $L \subseteq K$, je-li $C \leq A$ pro všechny $A \in L$. Prvek $C \in K$ je *infimem množiny* $L \subseteq K$, jestliže je dolní závorou a pro každou jinou dolní závoru $D$ téže množiny platí $D \leq C$. Jde tedy o největší dolní závoru dané množiny.

Obdobně definujeme *horní závoru* a *supremum* podmnožiny $L$ záměnou $\leq$ za $\geq$ v posledním odstavci.

Konečné uspořádané množiny se přehledně zobrazují pomocí orientovaných grafů. Prvky $K$ jsou představovány uzly a hranou jsou spojeny právě prvky v relaci s orientací od většího k menšímu. *Hasseho diagram* uspořádané množiny je zakreslení takového grafu v rovině tak, že větší prvky jsou zobrazeny vždy výš než menší (a orientace hran je tedy dána takto implicitně). Zvláště u malého počtu prvků množiny $K$ je to velmi přehledný způsob, jak diskutovat různé příklady, viz příklady ve vedlejším sloupci.

**11.120.** Anna, Bára, Kateřina a Dana chtějí jet na výlet. Rozhodněte, která z děvčat pojedou, mají-li být dodrženy tyto zásady: Pojede aspoň jedna z dvojice Bára/Dana, nejvýše jedna z dvojice Anna/Kateřina, aspoň jedna z dvojice Anna/Dana a nejvýše jedna z dvojice Bára/Kateřina. Dále je jisté, že Bára nepojede bez Anny a že Kateřina pojede, pojede-li Dana.

**Řešení.** Přepsáním do Booleovy algebry, úpravou a přepsáním zpět dostaneme, že na výlet pojede buď právě Anna s Bárou nebo právě Kateřina s Danou. □

**11.121.** Pomocí přepisu do Booleovy algebry vyřešte následující úlohu: Při vyšetřování vraždy bylo zajištěno pět podezřelých Kalina, Nováček, Obrátil, Pražák a Ryvola. V době činu byl na místě Obrátil nebo Pražák, ale nejvýše jeden z dvojice Kalina, Nováček a aspoň jeden z dvojice Kalina, Obrátil. Podezřelý Ryvola tam mohl být jen v přítomnosti Pražáka, ale pokud tam Ryvola byl, nechyběl ani Obrátil. Lze vyloučit spolupráci Nováčka s Pražákem, zato Nováček a Obrátil tvoří nerozlučnou dvojici. Kdo z podezřelých vraždu spáchal?

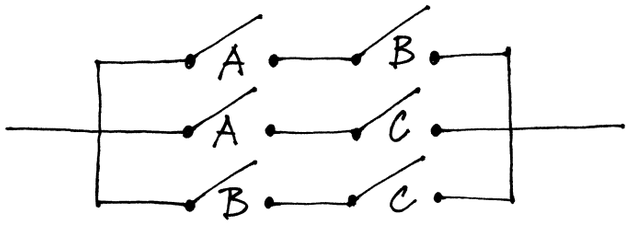
**Řešení.** Přepisem do Booleovské algebry, podle prvních písmen jména, dostáváme

$$(o+p)(k'+n')(k+o)(p+r')(r'+o)(n'+p')(no+n'o')$$

a s využitím $x^2 = x, xx' = 0, x+x' = 1$ dostaneme úpravou předchozího výrazu $r'p'nok'+r'pn'o'k$. Vinni jsou teda buď Nováček a Obrátil nebo Kalina s Pražákem. □

**11.122.** Volební skříňka pro tři voliče je skříňka, která zpracuje hlasy tří voličů a jejím výstupem je výsledek „ano“, pokud byla pro většina z voličů. Navrhňete takovou skříňku složenou z přepínačových obvodů.

**Řešení.**




□

### Svazy

**Definice.** *Svaz* je uspořádaná množina $(K, \leq)$, ve kterém každá dvouprvková množina $\{A, B\}$ má supremum $A \vee B$ a infimum $A \wedge B$. Hovoříme přitom o *úplném svazu*, jestliže existuje supremum a infimum každé podmnožiny v $K$.

Na svazu $(K, \leq)$ tedy máme definovány binární operace $\wedge$ a $\vee$ a přímo z definice je zjevná asociativita a komutativita těchto operací (dokažte si podrobně!).

Všimněme si také, že jakýkoliv prvek v $K$ je horní závorou pro prázdnou množinu, proto supremum prázdné množiny musí být menší než všechny prvky v $K$. Obdobně infimum prázdné množiny musí být větší než jakýkoliv prvek v $K$. Zejména tedy úplný svaz má vždy *největší* a *nejmenší prvek*.

Protože jsou binární operace $\wedge$ a $\vee$ asociativní a komutativní, jistě existují v každém svazu suprema a infima všech konečných neprázdných množin. V případě konečných uspořádaných množinů $(K, \leq)$ jde proto o úplný svaz tehdy a jen tehdy, když v něm existuje jediný největší prvek $1 \in K$ a jediný nejmenší prvek $0 \in K$.

O svazu říkáme, že je *distributivní*, jestliže operace $\wedge$ a $\vee$ splňují axiomy distributivity (4) a (5) z odstavce 11.46 na straně 687. Snadno lze ale nakreslit Hasseho diagram svazu, který není distributivní, viz obrázek níže.

Nyní už můžeme snadno definovat Booleovskou algebru v jazyce svazů: Booleovská algebra je distributivní svaz s největším prvkem 1 a nejmenším prvkem 0 takový, že v něm existují ke všem prvkům komplementy (tj. prvky splňující vlastnost 11.45(8)).

Ověřili jsme již, že v takovém případě jsou komplementy definovány jednoznačně (viz úvahy na začátku odstavce 11.46), takže je naše alternativní definice Booleovské algebry korektní.

Všimněme si také, že při diskusi dělitelů daného čísla nebo polynomu $p$ jsme narazili na distributivní svazy $D_p$, které jsou Booleovskou algebrou právě tehdy, když rozklad $p$ neobsahuje kvadráty, viz Lemma 11.50.

**11.53. Homomorfismy.** Jak jsme již viděli u mnoha matematických struktur, o objektech se dozvídáme informace pomocí tzv. homomorfismů, tj. zobrazení, které zachovávají příslušné operace. Obzvlášť jednoduché je to u uspořádaných množin:

### Izotonní zobrazení

Homomorfismem uspořádaných množin $(K, \leq_K)$ a $(L, \leq_L)$ rozumíme takové zobrazení $f : K \to L$, že z $A \leq_K B$ vždy vyplývá také $f(A) \leq_L f(B)$. Hovoříme přitom také o *izotonních zobrazeních*.

V případě svazů a Booleovských algeber definujeme homomorfismy podobně jako u okruhů:

### Homomorfismy svazů a algeber

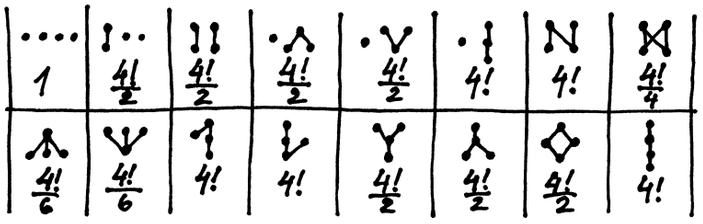
Zobrazení $f : (K, \wedge, \vee, ') \to (L, \wedge, \vee, ')$ se nazývá *homomorfismus Booleovských algeber*, jestliže pro všechny $A, B \in K$ platí

(1) $f(A \wedge B) = f(A) \wedge f(B)$,
(2) $f(A \vee B) = f(A) \vee f(B)$,
(3) $f(A') = f(A)'$.

*11.123.* Nalezněte konečnou podmnožinu množiny kladných celých čísel takovou, že pokud ji uvážíme jako uspořádanou množinu, kde relace uspořádání je dána relací dělitelnosti, tak se nebude jednat o svaz. ○

**11.124.** Určete počet relací uspořádání na čtyřprvkové množině. Pro každý z neizomorfních typů uspořádání (každý typ je dán Hasseovým diagramem) určete, zda se jedná o svaz. Vyskytuje se mezi uspořádáními Booleova algebra?

**Řešení.** Postupně projdeme všechny možné Hasseovy diagramy uspořádání na nějaké čtyřprvkové množině $M$ a spočítáme, kolik různých uspořádání (tj. podmnožin množiny $M \times M$) má daný Hasseův diagram, viz obr.:




Celkem tedy je 219 uspořádání na čtyřprvkové množině.

Uvědomme si, že podmínka existence suprema a infima libovolných dvou prvků ve svazu, implikuje indukcí existenci suprema a infima libovolné neprázdné konečné množiny prvků svazu. U konečných svazů to mimo jiné znamená, že (neprázdný) konečný svaz musí mít největší a nejmenší prvek.

Pouze na základě tohoto kriteria vidíme, že možnými svazy jsou pouze uspořádání na posledních dvou obrázcích. Tomu tak skutečně je, předposlední uspořádání je dokonce Booleovou algebrou. □

*11.125.* Určete počet relací uspořádání množiny $\{1, 2, 3, 4, 5\}$ takových, že právě dvě disjunktní dvojice prvků jsou nesrovnatelné. ○

**11.126.** Nakreslete Hasseho diagram svazu dělitelů čísla 36. Je tento svaz distributivní? Jedná se o Booleovu algebru?

**Řešení.** Svaz je distibutivní (neobsahuje, a ani žádné jeho dělení ne, jako podgraf tvz. „Diamant“, ani „Pětiúhelník“).

Homomorfismus $f$ je izomorfismus Booleovských algeber, jestliže je $f$ bijektivní.

Podobně definujeme homomorfismy svazů jako zobrazení, která splňují vlastnosti (1) a (2).

Snadno se ověří, že bijektivnost $f$ již zaručí, že $f^{-1}$ je opět homomorfismem.

Z definice uspořádání na Booleových algebrách nebo svazech je zřejmé, že každý homomorfismus $f : K \to L$ bude také splňovat $f(A) \leq f(B)$ pro všechny prvky $A \leq B$ v $K$, půjde tedy vždy o izotonní zobrazení.

Jakkoliv umíme rekonstruovat operace suprema a infima z uspořádání, pokud toto vzniklo z Booleovy algebry, není pravda, že by každý homomorfismus uspořádaných množin byl automaticky homomorfismem příslušných algeber nebo svazů.

**11.54. Věty o pevném bodě.** Mnoho praktických úloh spočívá v diskusi existence a vlastností pevných bodů zobrazení $f : K \to K$ na nějaké množině $K$, tj. prvků $x \in K$ s vlastností $f(x) = x$. Naše úvahy o infimech a supremech umožňují překvapivě snadno odvodit velice silná tvrzení tohoto typu. Dokážeme si jednu takovou klasickou větu, kterou odvodili Knaster a Tarski (ve speciálním případě Booleovské algebry podmnožin dané množiny již koncem dvacátých let 20. století, obecné tvrzení pak publikoval Tarski v r. 1955):

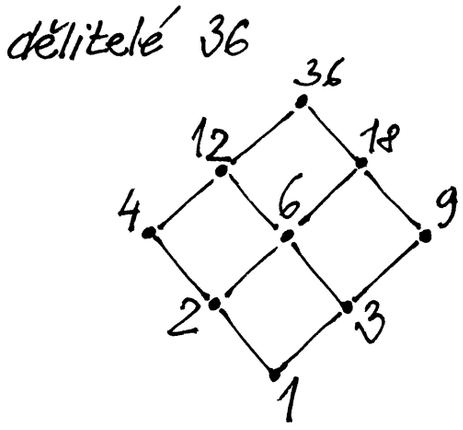


**Věta** (Tarského věta)**.** *Uvažujme libovolný úplný svaz $(K, \wedge, \vee)$ a libovolné izotonní zobrazení $f : K \to K$. Pak $f$ má pevný bod a množina všech pevných bodů $f$ je (s uspořádáním zděděným z $K$) opět úplný svaz.*

Důkaz. Označme $M = \{x \in K; x \leq f(x)\}$. Protože v $K$ existuje minimální prvek, je jistě $M$ neprázdná a protože $f$ zachovává uspořádání, je $f(M) \subseteq M$. Označme dále $z_1 = \sup M$. Pak jistě pro $x \in M$ platí $x \leq z_1$, tedy také $f(x) \leq f(z_1)$. Přitom zároveň víme $x \leq f(x)$, takže $f(z_1)$ je horní závorou pro $M$. Pak ovšem nutně $z_1 \leq f(z_1)$, takže i $z_1 \in M$ a proto $f(z_1) \leq z_1$. Dokázali jsme tedy $f(z_1) = z_1$ a pevný bod je nalezen.

Trochu složitější je dokázat dovětek, že množina $Z \subseteq K$ všech pevných bodů zobrazení $f$ je úplný svaz. Zřejmě jsme již našli její největší prvek $z_1 = \max Z$ a úplně stejným postupem s použitím infima a vlastnosti $f(x) \leq x$ místo definice $M$ a jejího suprema bychom našli také nejmenší bod $z_0 = \min Z$.

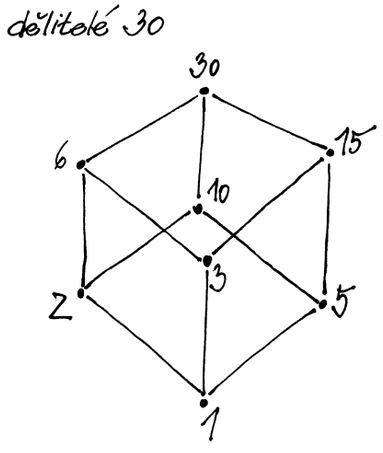
Uvažme nyní libovolnou neprázdnou množinu $Q \subseteq Z$ a označme $y = \sup Q$. Toto supremum sice nemusí ležet v $Z$, ukážeme ale, že bude přesto v $Z$ existovat supremum i ve zděděném uspořádání $\leq_Z$ z uspořádání v $K$. Za tím účelem si označme $R = \{x \in K; y \leq x\}$, tj. množinu všech prvků v $K$ větších než naše $y$. Přímo z definic je zřejmé, že tato množina $R$ je spolu s uspořádáním zděděným z $K$ opět úplný svaz a zúžení zobrazení $f$ na $R$ bude opět izotonní zobrazení $f_{|R} : R \to R$. Podle výše dokázaného tedy bude mít $f_{|R}$ nejmenší pevný bod $\bar{y}$. Samozřejmě je $\bar{y} \in Z$ a snadno nahlédneme, že ve skutečnosti je $\bar{y}$ supremem námi zvolené množiny $Q$ vůči zděděnému uspořádání na $Z$. Přitom je možné, že $\bar{y} > y$. Obdobným postupem se zaměněnými relacemi a volbou infima najdeme i infimum libovolné neprázdné podmnožiny v $Z$. Největší a nejmenší prvek jsme již našli dříve a důkaz je ukončen. □




□

**11.127.** Nakreslete Hasseho diagram svazu dělitelů čísla 30. Je tento svaz distributivní? Jedná se o Booleovu algebru?

**Řešení.** Tento svaz je Booleovou algebrou o osmi prvcích. Všechny Booleovy algebry o $2^n$ prvcích, pro pevné $n$, jsou si izomorfní (viz 11.58). V tomto případě se jedná o „krychli". Graf Booleovy algebry o osmi prvcích lze totiž nakreslit jako průmět krychle do roviny.




□

**11.128.** Rozhodněte, zda každý svaz na tříprvkové množině je *řetězec* (řetězec je uspořádaná množina, ve které je každý prvek srovnatelný s každým).

**Řešení.** Jak již jsme si všimli v příkladu ‖11.124‖, neprázdný konečný svaz musí mít svůj největší a nejmenší prvek. Tedy jeden ze tří prvků je největší (tj. srovnatelný s oběma dalšími), druhý nejmenší (tedy opět srovnatelný s oběma dalšími) a třetí je tudíž srovnatelný také s oběma ostatními (největším i nejmenším). □

**Poznámka.** V literatuře lze najít mnoho variant vět o pevných bodech v různých souvislostech. Jednou z velmi užitečných je tzv. *Kleeneho věta*, jejíž tvrzení můžeme vyčíst z právě dokázané věty následujícím způsobem.

Jestliže (ve značení Tarského věty) uvážíme spočetnou podmnožinu v $K$ tvořenou tzv. *Kleeneho řetězcem*

$$0 \le f(0) \le f(f(0)) \le \dots,$$

pak supremum $z$ této podmnožiny zjevně nemůže být větší než kterýkoliv pevný bod zobrazení $f$. Skutečně pokud je $y$ pevný bod zobrazení $f$, pak ze vztahu $0 \le y$ dostaneme $f(0) \le f(y) = y$ atd. Pokud má $f$ navíc vlastnost *spojitosti*, tzn. že „dostatečně" zachovává suprema, můžeme dovodit že $f(z)$ bude opět supremem téhož řetězce a tedy pevný bod. Musí to proto být nejmenší pevný bod. Toto tvrzení se nazývá *Kleeneho věta o pevném bodě* a má četná použití v teorii rekurzí, při diskusi zastavení algoritmů atd.

Nebudeme zde zacházet do podrobností kolem spojitosti zobrazení mezi uspořádanými množinami.

**11.55. Normální tvary výrazů.** Vrátíme se závěrem zpět k diskusi Booleovských algeber s konečným počtem prvků a ukážeme si jejich úplnou klasifikaci.



Při diskusi výrokové logiky jsme se potýkali s problémem, co vlastně jsou prvky příslušné Booleovy algebry. Formálně vzato jsme je definovali jako třídy ekvivalentních výroků. Jinak řečeno, pracovali jsme s hodnotovými funkcemi pro výroky s daným počtem argumentů. Vůbec jsme přitom neřešili obtížný problém, jak rozpoznat stejné výroky v tomto smyslu. Také jsme neřešili, jestli všechny formálně možné hodnotové funkce $(\mathbb{Z}_2)^n \to \mathbb{Z}_2$ lze zadat pomocí základních logických operací.

Zcela obdobně se můžeme tázat, jak poznat, zda dva systémy přepínačů mají stejnou funkci. Obdobně jako u výroků zde pro systém s $n$ přepínači pracujeme s funkcemi $(\mathbb{Z}_2)^n \to \mathbb{Z}_2$ a zjevně existuje právě $2^{2^n}$ různých takových přepínacích funkcí. Na těchto funkcích umíme přirozeným způsobem zadat strukturu Booleovy algebry (využíváme, že hodnoty, tj. $\mathbb{Z}_2$, jsou Booleovou algebrou).

Odpovíme nyní na výše uvedené otázky tak, že pro libovolný prvek obecné Booleovy algebry sestrojíme jeho tzv. normální tvar, tj. napíšeme jej pomocí dobře vybrané skupiny nejjednodušších prvků a operace $\vee$. Porovnáním normálních tvarů dvou prvků pak už snadno poznáme, zda jsou stejné či nikoliv. Nejprve si tedy vybereme obzvlášť jednoduché prvky Booleovských algeber:

Atomy v Booleovské algebře

Prvek $A \in K$ nazveme *atom* v Booleově algebře $K$, jestliže pro všechny $B \in K$ platí $A \wedge B = A$ nebo $A \wedge B = 0$.

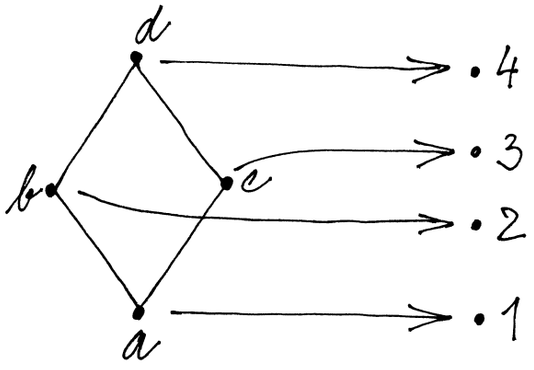
Jinak řečeno, $A$ je atom, když pro všechny ostatní prvky $B \le A$ implikuje $B = 0$ nebo $B = A$.

Velmi jednoduché je to v Booleovské algebře všech podmnožin dané konečné množiny $M$. Zjevně budou atomy právě všechny jednoprvkové podmnožiny $A = \{x\}$ v množině $M$. Skutečně pro každou podmnožinu $B$ budeme mít buď $A \wedge B = A$, pokud $x \in B$, nebo $A \wedge B = 0$, pokud $x \notin B$.

Podívejme se ještě, jak vypadají atomy v Booleově algebře funkcí přepínačového systému s $n$ přepínači $A_1, \dots, A_n$. Snadno ověříme, že zde je $2^n$ atomů, které jsou tvaru $A_1^{\sigma_1} \wedge \dots \wedge A_n^{\sigma_n}$, kde buď $A_i^{\sigma_i} = A_i$ nebo $A_i^{\sigma_i} = A_i'$.

**11.129.** Udejte příklad izotonního zobrazení dvou svazů, které není svazovým homomorfismem.

**Řešení.** Opět se vrátíme k příkladu ‖11.124‖ a uvážíme zobrazení dle obrázku:




□

**11.130.** Rozhohněte, zda libovolný svazový homomorfismus mezi konečnými svazy zobrazí nejmenší prvek jednoho svazu na nejmenší prvek druhého svazu.

**Řešení.** Ne. Libovolné konstantní zobrazení mezi dvěma svazy je svazovým homomorfismem. Pokud konstantní hodnotou nebude zrovna nejmenší prvek druhého svazu, pak se jedná o homomorfismus, který vyvrací tvrzení ze zadání příkladu. □

**11.131.** Rozhodněte, zda každý řetězec, který má největší a nejmenší prvek je úplným svazem.

**Řešení.** Ne. Uvážme například množinu celých čísel bez nuly, kterou uspořádáme následovně: libovolné kladné číslo bude větší než záporné, pořadí kladných čísel mezi sebou však „obrátíme“ a totéž uděláme se zápornými čísly. Potom bude číslo 1 největším číslem daného řetězce a číslo $-1$ nejmenším. Množina kladných celých čísel však nebude mít v této uspořádané množině infimum.

Formálně definujeme na $\mathbb{Z} \setminus \{0\}$ uspořádání $\prec$ následovně:

$$a \prec b \iff [(\operatorname{sgn}(a) \cdot \operatorname{sgn}(b) = 1 \wedge b > a) \vee (\operatorname{sgn}(a) > \operatorname{sgn}(b))].$$

Skutečně pro dvě funkce $\varphi$ a $\psi$ je jejich infimem funkce $\varphi \wedge \psi$, jejíž hodnoty jsou dány součinem jejich hodnot v $\mathbb{Z}_2$. Platí tedy $\varphi \leq \psi$, jestliže $\varphi$ má hodnotu $1 \in \mathbb{Z}_2$ všude tam, kde má $\psi$ hodnotu $1 \in \mathbb{Z}_2$. Odtud už plyne, že v naší Booleově algebře hodnotových funkcí je funkce $\varphi$ atomem, právě když z $2^n$ hodnot $\varphi$ na jednotlivých možnostech hodnot jednotlivých argumentů má právě jednou hodnotu $1 \in \mathbb{Z}_2$. Všechny takové funkce ovšem lze vytvořit právě uvedeným způsobem.

A nyní můžeme zformulovat slibovanou větu o *normálním disjunktivním tvaru.*

**Věta.** *Každý prvek $B$ v konečné Booleově algebře $(K, \wedge, \vee, ')$ lze zapsat jako supremum atomů*

$$B = A_1 \vee \cdots \vee A_k.$$

*Tato formule je navíc jednoznačná až na pořadí atomů.*

Důkaz nám zabere několik odstavců, ale základní idea je docela jednoduchá:



Uvažme všechny atomy $A_1, A_2, \ldots, A_k$ v $K$, které jsou menší nebo rovny $B$. Z vlastností uspořádání na množině $K$ (viz 11.51(3)) je okamžitě vidět, že také

$$Y = A_1 \vee \cdots \vee A_k \leq B.$$

Hlavním naším krokem v důkazu bude ověřit, že $B \wedge Y' = 0$, což podle 11.51(4) zaručuje $B \leq Y$. Tím bude dokázána rovnost $B = Y$.

**11.56. Tři pomocná tvrzení.** Postupně si odvodíme několik technických vlastností atomů a pak teprve dokončíme důkaz věty o normálním disjunktivním tvaru. Pokračujeme v symbolice používané v minulém odstavci.

**Tvrzení.** *(1) Jestliže jsou $Y, X_1, \ldots, X_\ell$ atomy v $K$, pak $Y \leq X_1 \vee \ldots \vee X_\ell$ tehdy a jen tehdy, když $Y = X_i$ pro nějaké $i = 1, \ldots, \ell$.*
*(2) Pro každý prvek $Y \neq 0$ v $K$ existuje atom $X$, pro který je $X \leq Y$.*
*(3) Jestliže jsou $X_1, \ldots, X_r$ všechny atomy v $K$, pak $Y = 0$, právě když $Y \wedge X_i = 0$ pro všechna $i = 1, \ldots, r$.*

Důkaz. (1) Jestliže platí nerovnost v tvrzení, pak

$$Y \wedge (X_1 \vee \cdots \vee X_\ell) = Y.$$

Díky distributivitě můžeme rovnost přepsat jako

$$(Y \wedge X_1) \vee \cdots \vee (Y \wedge X_\ell) = Y,$$

přitom ale je pro všechna $i$ buď $Y \wedge X_i = 0$ nebo $Y \wedge X_i = X_i$. Pokud by tedy byly všechny tyto průniku 0, bylo by i $Y = 0$. Musí být tedy nějaké $i$, pro které je $Y \wedge X_i = X_i$. Prvek $Y$ je přitom také atom, takže jsme dokázali požadovanou rovnost $Y = X_i$.

Opačná implikace je zřejmá.

(2) Pokud je $Y$ samo atomem, pak stačí zvolit $X = Y$. Jestliže $Y$ není atom, pak z definice vyplývá, že musí existovat nenulový prvek $Z_1$, pro který je $Z_1 \leq Y$. Jestliže ani $Z_1$ není atom, pak ze stejných důvodů najdeme $Z_2 \leq Z_1$ a postupně tak sestrojíme posloupnost různých prvků

$$\ldots Z_k \leq Z_{k-1} \leq \cdots \leq Z_1 \leq Y,$$

která nemůže být nekonečná, protože celá Booleovská algebra $K$ je konečná. Proto musí skončit nějakým atomem $Z_k$.




□

**11.132.** Udejte příklad nekonečného řetězce, který je úplným svazem.

**Řešení.** Například množina reálných čísel spolu s prvky $-\infty, \infty$. Svazová supréma a infíma jsou definovány souhlasně s těmito pojmy v množině reálných čísel. Dále je $-\infty$ infimum množin, které nejsou zdola ohraničené, podobně $\infty$ je supremum množin, které nejsou shora ohraničené. Prvek $-\infty$ je nejmenším a $\infty$ největším v daném svazu. □

**11.133.** Rozhodněte, zda je množina konvexních podmnožin $\mathbb{R}^3$ svazem (s vhodnými operacemi suprema a infima). Pokud ano, je tento svaz úplný, distributivní?.

**Řešení.** Jedná se o svaz. Infimem dvou množin je jejich průnik (průnikem dvou konvexních množin je opět konvexní množina), supremem pak konvexní obal jejich sjednocení. Je zřejmé, že axiomy svazu jsou pro takto definované operace vskutku splněny (rozmysli). Průnik libovolného systému množin i konvexní obal jeho sjednocení je vždy definován, jedná se tedy o úplný svaz.

Svaz však není distributivní. Uvažme například tři jednotkové koule $K_1$, $K_2$ a $K_3$ se středy v bodech $[3,0,0]$, $[-3,0,0]$, resp. $[0,0,0]$. Pak

$$K_1 \wedge (K_2 \vee K_3) = \emptyset \neq (K_1 \wedge K_2) \vee (K_1 \wedge K_3).$$

□

**11.134.** Rozhodněte, zda je množina vektorových podprostorů prostoru $\mathbb{R}^3$ s vhodnými operacemi svazem. Je tento svaz úplný, distributivní?

**Řešení.** Jedná se o svaz, operacemi jsou dány průnikem a součtem vektorových prostorů (je snadné ověřit, že tyto operace splňují axiomy svazu).

Tento svaz je úplný (infimum je dané průnikem, není co řešit; supremum součtem vektorových prostorů, to je buď jedno-, dvou- či třídimenzionální vektorový prostor).

(3) Předpokládejme nejprve, že $Y \wedge X_i = 0$ pro všechny indexy $i$. Pokud by ale bylo $Y \neq 0$, pak podle předchozího bodu musí existovat atom $X_j$, pro který $X_j \wedge Y = X_j$, což je spor.

Opačná implikace je triviální. □

**11.57. Důkaz věty o normálním tvaru.** Pokračujme v naší úvaze o přepsání prvku $B$ pomocí výrazu

$$Y = A_1 \vee \cdots \vee A_k \leq B,$$

kde $A_i$ jsou všechny atomy v $K$ menší nebo rovny $B$. Spočteme

$$B \wedge Y' = B \wedge (A_1 \vee \cdots \vee A_k)' = B \wedge A_1' \wedge \cdots \wedge A_k'.$$

Jestliže je $A = A_i$ atom obsažený ve sjednocení $Y$, pak tedy $B \wedge Y' \wedge A = 0$. Pokud ale je $A$ atom, který ve výrazu $Y$ nevystupuje, dostáváme také $B \wedge Y' \wedge A = 0$, neboť $Y$ obsahuje právě všechny atomy menší než $B$, a proto $B \wedge A = 0$.

Dokázali jsme tedy, že $B \wedge Y'$ má nulový průnik se všemi atomy, a proto je to nulový prvek podle našeho třetího pomocného tvrzení výše. Proto tedy $B \leq Y$. Z definice $Y$ ale víme $Y \leq B$ a antisymetrie uspořádání tedy zaručuje $B = Y$, jak jsme chtěli dokázat.

Zbývá jednoznačnost výrazu až na pořadí. Předpokládejme tedy, že jsme zapsali $B$ dvěma způsoby v požadovaném tvaru

$$B = A_1 \vee \cdots \vee A_k = \tilde{A}_1 \vee \cdots \vee \tilde{A}_\ell.$$

Nyní každé $A_i$ splňuje $A_i \leq B$, a proto je podle prvního pomocného tvrzení výše nutně rovno jednomu z $\tilde{A}_j$. Opakováním tohoto argumentu dostáváme požadovanou jednoznačnost a důkaz je ukončen.

**11.58. Klasifikace.** 
Na závěr našich úvah ještě dokážeme, že ve skutečnosti byly všechny naše příklady konečných Booleovských algeber izomorfní. Zejména tedy uvidíme, že každou z $2^{2^n}$ hodnotových funkcí pro $n$ elementárních výroků umíme zapsat vhodným výrokem, stejně jako každou z $2^{2^n}$ různých přepínacích funkcí umíme zadat pomocí vhodně sestavených $n$ přepínačů. V obou případech se bude diskutovaná algebra chovat stejně jako Booleovská algebra všech podmnožin v množině s $2^n$ prvky.

Navíc jsme se naučili každý takový výraz napsat v jednoznačném normálním tvaru, takže umíme algoritmicky určit, zda budou např. dva přepínačové systémy vykazovat stejné chování, aniž bychom porovnali hodnoty při všech $2^n$ možných vstupech.

**Věta.** *Každá konečná Booleova algebra je izomorfní Booleovské algebře $K = 2^M$, kde $M$ je množina atomů v $K$.*

Důkaz. Myšlenka důkazu je zcela přímočará. Při každém izomorfismu konečné Booleovské algebry $(K, \wedge, \vee, ')$ musí atomy být zobrazeny na atomy. Najděme si tedy množinu $M$ všech atomů v $K$ a uvažme Booleovu algebru $(2^M, \cap, \cup, ')$ všech podmnožin v $M$. Tím máme i zadánu přirozenou korespondenci mezi atomy v $K$ a $2^M$.

Použijeme nyní disjunktivní normální formu k rozšíření zobrazení na celé $K$. Každý prvek $X \in K$ lze psát jednoznačně, až na pořadí atomů $A_i$, ve tvaru

$$X = A_1 \vee \cdots \vee A_k$$

a definujeme tedy funkci $f : K \to 2^M$ vztahem

$$f(X) = f(A_1) \cup \cdots \cup f(A_k) = \{A_1, \ldots, A_k\},$$

Svaz není distributivní (stačí uvážit tři různoběžky). □

### K. Kódy

**11.135.** Uvažujme (5, 3) kód nad $\mathbb{Z}_2$ generovaný polynomem $x^2 + x + 1$. Vypište všechna kódová slova, najděte generující matici a matici kontroly parity.

**Řešení.** $p(x) = x^2 + x + 1$. Kódová slova jsou právě násobky generujícího polynomu:

$$0\cdot p,\ 1\cdot p,\ x\cdot p,\ (x+1)\cdot p,\ x^2\cdot p,\ (x^2+1)\cdot p,\ (x^2+x)\cdot p,\ (x^2+x+1)\cdot p$$

neboli

$$0, x^2 + x + 1, x^3 + x^2 + x, x^3 + 1, x^4 + x^3 + x^2, x^4 + x^3 + x + 1, x^4 + x, x^4 + x^2 + 1$$

neboli

$$00000, 11100, 01110, 10010, 00111, 11011, 01001, 10101.$$

Bázové vektory vynásobené $x^{5-3} = x^2$ dávají mod $(p)$:

$$\begin{aligned} x^2 &\equiv x + 1,\\ x^3 &= x.x^2 \equiv x(x + 1) = x^2 + x \equiv 1,\\ x^4 &\equiv x. \end{aligned}$$

To znamená, že bázové vektory se zakódují následovně

$$\begin{aligned} 1 &\mapsto x^2 + x + 1, & & & 100 &\mapsto 11100,\\ x &\mapsto x^3 + 1, & & \text{tj.} & 010 &\mapsto 10010,\\ x^2 &\mapsto x^4 + x, & & & 001 &\mapsto 01001, \end{aligned}$$

a proto je generující matice

$$G = \begin{pmatrix} 1 & 1 & 0\\ 1 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1 \end{pmatrix}$$

a matice kontroly parity

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0\\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$ □

*11.136.* Určete generující matici a matici kontroly parity (7, 4) kódu nad $\mathbb{Z}_2$ generovaným polynomem $x^3 + x + 1$. ○

tj. jako sjednocení jednoprvkových podmnožin $A_i \subseteq M$ obsažených ve výrazu.

Z jednoznačnosti normálního tvaru vyplývá, že $f$ je nutně bijekcí. Zbývá dokázat, že jde o homomorfismus Booleovských algeber.

Jsou-li $X$ a $Y$ dva prvky v $K$, pak v normální formě jejich suprema jsou právě atomy, které vystupují v $X$ nebo v $Y$, zatímco v infimu jsou to atomy vystupující v obou výrazech současně. To ale právě ověřuje, že $f$ zachovává operace $\wedge$ a $\vee$. Pro doplňky si všimněme, že atom $A$ vystupuje v normální formě $X'$, právě když $X \wedge A = 0$. Odtud již vidíme, že i komplementy $f$ zachovává a důkaz je ukončen. □

Pro nekonečné Booleovské algebry obecně neplatí, že by byly izomorfní Booleovské algebře všech podmnožin nějaké vhodné množiny $M$. Platí však, že je izomorfní Booleově podalgebře vhodné podmnožiny všech množin nějaké množiny $M$. Tomuto výsledku se říká *Stoneova věta o reprezentaci*.

### 5. Kódování

Často potřebujeme přenášet informace a přitom zajišťovat jejich správnost. Někdy stačí zajistit, abychom poznali, zda je informace nezměněná, a při chybě si vyžádáme informaci znovu, jindy potřebujeme zajistit, aby chyby byly i opraveny bez nového přenášení zprávy. To vše je úkol kódování a v dalších odstavcích se tomuto úkolu budeme věnovat.

Pokud navíc chceme, aby zprávu mohl číst pouze adresát, potřebujeme i tzv. šifrování. Tomu jsme se krátce věnovali na konci minulé kapitoly.

**11.59. Kódy.** Při přenosu informace zpravidla dochází k její deformaci. Budeme pro jednoduchost pracovat s modelem, kdy jednotlivé částečky informace jsou buď nuly nebo jedničky (tj. prvky v $\mathbb{Z}_2$), říkáme jim *bity*, a přenášíme konečná slova o $k$ bitech pro nějaké pevně zvolené $k \in \mathbb{N}$. Obdobné postupy jsou možné nad libovolnými konečnými poli, my ale zůstaneme u nejjednoduššího případu $\mathbb{Z}_2$.



Přenosové chyby chceme rozpoznávat, případně i opravovat, a za tím účelem přidáváme ke $k$-bitovému slovu dodatečných $n - k$ bitů informace pro pevně zvolené $n > k$. Hovoříme o $(n, k)$-*kódech*.

Všech slov o $k$ bitech je $2^k$ a každé z nich má jednoznačně určovat jedno *kódové slovo* z $2^n$ možných. Máme tedy u $(n, k)$-kódů ještě

$$2^n - 2^k = 2^k(2^{n-k} - 1)$$

slov, které jsou chybové. Lze tedy tušit, že pro veliké $k$ nám i malý počet přidaných bitů dává hodně redundantní informace.

Úplně jednoduchým příkladem je *kód kontrolující paritu*. Kódové slovo o $k + 1$ bitech je určené tak, aby přidáním prvního bitu ke $k$–bitovému slovu byl zaručen sudý počet jedniček ve slově. Jde tedy o $(k + 1, k)$–kód.

Pokud při přenosu dojde k lichému počtu chyb, s použitím tohoto jednoduchého kódu na to přijdeme. Dvě různá kódová slova se při tomto kódu vždy liší alespoň ve dvou pozicích, chybové slovo se ale od alespoň dvou různých kódových slov liší pouze v pozici jedné. Nemůžeme proto umět chyby opravovat, ani kdybychom věděli, že při přenosu došlo k právě jedné chybě.

**11.137.** Sedmibitovou zprávu $a_0a_1\dots a_6$, chápanou jako $a_0+a_1x+\cdots+a_6x^6$, kódujeme polynomiálním kódem generovaným polynomem $x^4+x+1$.

i) Zakódujte zprávu 1100011.

ii) Obdrželi jste kód 10111010001. Jaká byla posílaná zpráva, když budete předpokládat, že došlo k chybě na maximálně jednom bitu?

iii) Jaká byla zpráva v ii), pokud předpokládáme, že došlo k chybě právě na dvou bitech?

**Řešení.** i)

$$\begin{aligned} x^4 &\equiv x+1,\\ x^5 &\equiv x^2+x,\\ x^9 &\equiv x^3+x,\\ x^{10} &\equiv x^2+x+1, \end{aligned}$$

odkud

$$\begin{aligned} 1+x+x^5+x^6 \mapsto \quad & x^4+x^5+x^9+x^{10}+x+1+x^2+x+\\ & x^3+x+x^2+x+1=\\ = \quad & x^3+x^4+x^5+x^9+x^{10}. \end{aligned}$$

Kód je tedy 00011100011.

ii) $1+x^2+x^3+x^4+x^6+x^{10}$ dává po dělení $x^4+x+1$ zbytek $x^2+1\equiv x^8$. Došlo tedy k chybě na devátém bitu a původní zpráva byla 1010101.

iii) Chyba mohla nastat na prvním a třetím bitu ($x^2+1$), na pátém a šestém ($x^4+x^5\equiv x^2+1$), nebo na druhém a jedenáctém ($x^{10}+x\equiv x^2+1$). V prvním případě byla zpráva 1010001 ve druhém 0110001 a ve třetím 1010000. □

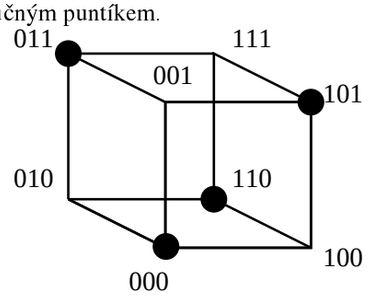
**11.138.** Sedmibitovou zprávu $a_0a_1\dots a_6$, chápanou jako $a_0+a_1x+\cdots+a_6x^6$, kódujeme polynomiálním kódem generovaným polynomem $x^4+x^3+1$.

i) Zakódujte zprávu 1101011.

ii) Obdrželi jste kód 01001011101. Jaká byla posílaná zpráva, když budete předpokládat, že došlo k chybě na maximálně jednom bitu?

iii) Jaká byla zpráva v ii), pokud předpokládáme, že došlo k chybě právě na dvou bitech?

Přehledně jsou všechna možná slova o dvou bitech s jedním přidaným paritním bitem vidět na obrázku níže. Kódová slova jsou zvýrazněna tučným puntíkem.




Navíc kódem kontrolujícím pouze paritu neumíme detekovat tak obvyklé chyby, jako je záměna dvou sousedních hodnot ve slově.

**11.60. Vzdálenost slov.** Na obrázku ilustrujícím (3, 2)–kód kontrolující paritu je vidět, že ve skutečnosti každé chybné slovo je „stejně" daleko od tří kódových slov – jsou to ta, která se liší v právě jednom bitu. Ostatní jsou dál. Abstraktně můžeme takové pozorování zachytit definicí vzdálenosti:



VZDÁLENOST SLOV

*Hammingova vzdálenost* dvou slov je rovna počtu bitů, ve kterých se liší.

Pokud uvažujeme slova $x$, $y$, $z$ a první dvě se liší v $r$ bitech, zatímco $y$ a $z$ se liší v $s$ bitech, pak se nutně $x$ a $z$ liší v nejvýše $r+s$ bitech, je tedy splněna trojúhelníková nerovnost pro vzdálenosti.

Aby kód mohl odhalovat chyby v $r$ bitech, musí být minimální vzdálenost mezi kódovými slovy alespoň $r+1$. Pokud budeme chtít i opravit nepřesně přenesené slovo s $r$ chybami, pak nutně musí existovat jen jediné kódové slovo, které má od přijatého chybného slova vzdálenost nejvýše $r$. Ověřili jsme tedy jednoduchá tvrzení:

**Věta.** *(1) Kód spolehlivě odhaluje nejvýše $r$ chyb ve slově, právě když je minimální Hammingova vzdálenost kódových slov $r+1$.*

*(2) Kód spolehlivě odhaluje i opravuje nejvýše $r$ chyb, právě když je minimální Hammingova vzdálenost kódových slov $2r+1$.*

**11.61. Konstrukce polynomiálních kódů.** K praktickému použití potřebujeme efektivně konstruovat kódová slova tak, abychom je mezi všemi slovy snadno rozpoznali. Kontrolu parity jsme už viděli, další triviální možnost je prosté opakování bitů. Např. (3, 1)–kód bere jednotlivé bity a posílá je třikrát po sobě.



Docela systematickou cestou ke konstrukci kódů je využití dělitelnosti polynomů. Zpráva $b_0b_1\dots b_{k-1}$ je reprezentována jako polynom nad polem $\mathbb{Z}_2$

$$m(x)=b_0+b_1x+\cdots+b_{k-1}x^{k-1}.$$

POLYNOMIÁLNÍ KÓD

Nechť $p(x)=a_0+\cdots+a_{n-k}x^{n-k}\in\mathbb{Z}_2[x]$ je polynom s koeficienty $a_0=1$, $a_{n-k}=1$. *Polynomiální kód generovaný polynomem $p(x)$* je $(n,k)$–kód, jehož slova jsou polynomy stupně menšího než $n$ dělitelné $p(x)$.

**Řešení.** i)

$$\begin{aligned} x^4 &\equiv x^3+1,\\ x^5 &\equiv x^3+x+1,\\ x^7 &\equiv x^2+x+1,\\ x^9 &\equiv x^2+1,\\ x^{10} &\equiv x^3+x, \end{aligned}$$

dostáváme tak

$$\begin{aligned} &1+x+x^3+x^5+x^6 \sim x^4+x^5+x^7+x^9+x^{10}\\ &\equiv x^3+1+x^3+x+1+x^2+x+1+x^2+1+x^3+x=\\ &\equiv x^3+x \sim x^4+x^5+x^7+x^9+x^{10}+x^3+x. \end{aligned}$$

Kód je tedy $\underbrace{0101}_{\text{kontrola}}\ \underbrace{1101011}_{\text{zpráva}}$.

ii) $x+x^4+x^6+x^7+x^8+x^{10}$ dává po dělení $x^4+x^3+1$ zbytek $x^2+x+1\equiv x^7$. Došlo tedy k chybě na osmém bitu a původní zpráva byla 1010101.

iii) Buď nastala chyba na druhém a desátém bitu ($x+x^9\equiv x^2+x+1$), nebo na čtvrtém a sedmém ($x^3+x^6\equiv x^2+x+1$), nebo pátém a devátém ($x^4+x^8\equiv x^2+x+1$). V prvním případě byla zpráva 00001011111, ve druhém 01011001101, ve třetím 01000011001. □

**11.139.** Uvažme $(15,11)$ kód generovaný polynomem $1+x^3+x^4$. Přijali jsme kód 011101110111001. Určete původní 11-bitovou zprávu, předpokládáme-li, že při přenosu došlo k chybě na jednom bitu.

**Řešení.** Řetězec je kódové slovo právě tehdy, když je dělitelný generujícím polynomem, tj. v našem případě $1+x^3+x^4$. Přijatý řetězec odpovídá polynomu $x+x^2+x^3+x^5+x^6+x^7+x^9+x^{10}+x^{11}+x^{14}$. Tento polynom dává po dělení $1+x^3+x^4$ zbytek $x+1$. To znamená, že při přenosu došlo k chybě. Předpokládáme-li, že chyba je jen na jednom bitu, musí existovat mocnina $x$, která je rovna tomuto zbytku modulo $1+x^3+x^4$. Proto počítáme $x^4\equiv x^3+1, x^5\equiv x^3+x+1,\ldots, x^{12}\equiv x+1$. Chyba tedy nastala na třináctém bitu a originální zpráva byla 01110111101.

Můžeme si příklad i víc rozebrat. Když si spočítáme všechny mocniny $x$, dostaneme

$$\begin{aligned} x^4 &\equiv x^3+1,\\ x^5 &\equiv x^3+x+1,\\ x^6 &\equiv x^3+x^2+x+1,\\ x^7 &\equiv x^2+x+1,\\ x^8 &\equiv x^3+x^2+x, \end{aligned}$$

Zpráva $m(x)$ je zakódována jako $v(x)=r(x)+x^{n-k}m(x)$, kde $r(x)$ je zbytek po dělení polynomu $x^{n-k}m(x)$ polynomem $p(x)$.

Z definice kódového slova $v(x)$ pro přenášené slovo $m(x)$ čteme:

$$\begin{aligned} v(x) &= r(x)+x^{n-k}m(x)=\\ &= r(x)+q(x)p(x)+r(x)=q(x)p(x), \end{aligned}$$

protože nad $\mathbb{Z}_2$ je součet dvou stejných polynomů vždy nulový. Budou tedy skutečně všechna kódová slova dělitelná $p(x)$.

Naopak je-li $v(x)$ dělitelné $p(x)$, můžeme číst poslední výpočet z opačné strany a vidíme, že jde skutečně o kódové slovo vzniklé uvedeným postupem.

Z definice je také vidět, že kódové slovo vznikne přidáním $n-k$ bitů na začátek slova. Původní zpráva je tedy obsažena přímo v polynomu $v(x)$, takže dekódování správného slova je velmi snadné.

Uveďme si dva jednoduché příklady, které už známe. Všimněme si nejprve, že $1+x$ dělí polynom $v(x)$ tehdy a jen tehdy, když $v(1)=0$. To nastane právě tehdy, když je ve $v(x)$ sudý počet nenulových koeficientů. Polynom $p(x)=1+x$ proto generuje $(n,n-1)$–kód kontroly parity pro všechna $n\geq 3$.

Obdobně se snadno ověří, že polynom $p(x)=1+x+\ldots+x^{n-1}$ generuje $(n,1)$–kód $n$–násobného opakování bitů. Skutečně dělením polynomu $b_0x^{n-1}$ polynomem $p$ dostaneme zbytek $b_0(1+\cdots+x^{n-2})$ a tedy příslušné kódové slovo je $b_0p(x)$.

**11.62. Detekce chyb.** Označme si $e(x)$ *vektor chyb*, které vznikou při přenosu. Místo posílaného slova $v\in(\mathbb{Z}_2)^n$ tedy dopadne přenos příjmem polynomu



$$u(x)=v(x)+e(x).$$

Chyba je rozpoznatelná, pouze když generátor kódu $p(x)$ nedělí $e(x)$. Máme proto zájem o polynomy $p(x)$ v $\mathbb{Z}_2[x]$, které nevystupují jako dělitelé zbytečně často.

**Definice.** Ireducibilní polynom $p(x)\in\mathbb{Z}_2[x]$ stupně $m$ se nazývá *primitivní*, jestliže $p(x)$ dělí polynom $(1+x^k)$ pro $k=2^m-1$, ale nedělí jej pro žádná menší $k$.

**Věta.** *Je-li $p(x)$ primitivní polynom stupně $m$, pak pro všechna $n\leq 2^m-1$ odhaluje příslušný $(n,n-m)$–kód všechny jednoduché a dvojité chyby.*

Důkaz. Jestliže nastane právě jedna chyba, pak $e(x)=x^i$ pro vhodné $0\leq i<n$. Protože je $p(x)$ ireducibilní polynom, nemůže mít kořen v $\mathbb{Z}_2$. Zejména tedy nemůže dělit beze zbytku $x^i$, protože rozklad $x^i$ je jednoznačný. Tedy je každá jednotlivá chyba rozpoznatelná.

Jestliže nastanou chyby právě dvě, pak

$$e(x)=x^i+x^j=x^i\left(1+x^{j-i}\right)$$

pro jistá $0\leq i<j<n$. Již víme, že $p(x)$ nedělí beze zbytku žádné $x^i$, a protože je primitivní, nedělí beze zbytku ani $1+x^{j-i}$, pokud je $j-i<2^m-1$. Zároveň je $p(x)$ ireducibilní, nedělí proto ani součin $e(x)=x^i(1+x^{j-i})$, a důkaz je ukončen. □

**11.63. Důsledek.** *Je-li $q(x)$ primitivní polynom stupně $m$, pak pro všechna $n\leq 2^m-1$ rozpoznává $(n,n-m-1)$–kód generovaný*

$$
\begin{aligned}
x^9 &\equiv x^2 + 1,\\
x^{10} &\equiv x^3 + x,\\
x^{11} &\equiv x^3 + x^2 + 1,\\
x^{12} &\equiv x + 1,\\
x^{13} &\equiv x^2 + x,\\
x^{14} &\equiv x^3 + x^2
\end{aligned}
$$

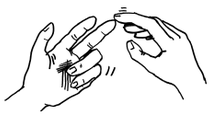
a generující matice je tedy

$$
G = \begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0\\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0\\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1\\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
$$

Můžeme si ověřit, že vynásobením 01110111101 dostaneme kódové slovo 011101110111101, které se liší od přijatého řetězce 011101110111001 právě na tom třináctém bitu. □

A nyní začneme efektivně využívat kontrolní matici.

**11.140.** Určete generující matici a matici kontroly parity $(7, 2)$ kódu



(tj. dva bity jsou informační a pět kontrolních) generovaného polynomem $x^5 + x^4 + x^2 + 1$. Dekódujte přijaté slovo 0010111 (tj. udejte dvoubitovou zprávu, která byla poslána), za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

**Řešení.** Generující matice kódu je

$$
G = \begin{pmatrix}
1 & 1\\
0 & 1\\
1 & 1\\
0 & 1\\
1 & 1\\
1 & 0\\
0 & 1
\end{pmatrix}.
$$

*polynomem $p(x) = q(x)(1 + x)$ všechny dvojité chyby a všechna slova s lichým počtem chyb.*

Důkaz. Kódová slova generovaná zvoleným polynomem $p(x)$ jsou dělitelná jak $x + 1$, tak primitivním polynomem $p_1(x)$. Jak jsme již ověřili, faktor $x + 1$ má za důsledek kontrolu parity, tj. všechna kódová slova mají sudý počet nenulových komponent. Tím umíme odhalit výskyt lichého počtu chyb. Jak jsme již také viděli v předchozí větě, druhý faktor umí odhalit dvojnásobné chyby. □

Následující tabulka ilustruje sílu výsledků předchozích dvou tvrzení pro několik primitivních polynomů v nízkých stupních. Např. poslední řádek nám říká, že přidáním pouhých 10 kontrolních bitů ke slovu o délce 1013 bitů budeme umět pomocí polynomu $(x + 1)p(x)$ odhalit jednotlivé, dvojité, trojité a všechny liché počty výskytů chyb v přenosu. Jde přitom o přenášení dosti velkých čísel, v desítkové soustavě by měly přes tři sta cifer.

| primitivní polynom $p(x)$ | kontrolní bity | délka slova |
|---:|---:|---:|
| $1 + x$ | 1 | 1 |
| $1 + x + x^2$ | 2 | 3 |
| $1 + x + x^3$ | 3 | 7 |
| $1 + x + x^4$ | 4 | 15 |
| $1 + x^2 + x^5$ | 5 | 31 |
| $1 + x + x^6$ | 6 | 63 |
| $1 + x^3 + x^7$ | 7 | 127 |
| $1 + x^2 + x^3 + x^4 + x^8$ | 8 | 255 |
| $1 + x^4 + x^9$ | 9 | 511 |
| $1 + x^3 + x^{10}$ | 10 | 1023 |

Nástroje pro konstrukci primitivních polynomů dává teorie konečných polí. Souvisí s tzv. primitivními prvky v Galoisových polích $G(2^m)$. Ze stejné teorie lze také dovodit příjemnou realizaci dělení se zbytkem, tj. ověřování, zda je přijaté slovo kódové, pomocí zpožďovacích registrů. Jde o jednoduchý obvod s tolika prvky, kolik je stupeň polynomu.[8]

**11.64. Lineární kódy.** Polynomiální kódy lze efektivně popisovat také pomocí elementárního maticového počtu. Budeme přitom pracovat s vektorovými prostory nad $\mathbb{Z}_2$, takže musíme být opatrní při využívání výsledků elementární lineární algebry, protože jsme v ní často využívali vlastnost, že $v = -v$ zaručuje $v = 0$. To nyní samozřejmě neplatí.



Základní definice vektorových prostorů, existence bází a popis lineárních zobrazení pomocí matic ale zůstávají v platnosti. Bude užitečné připomenout si při čtení následujících odstavců obecnou teorii a ujistit se o její použitelnosti.

Vyjdeme z obecnější definice kódů, která požaduje lineární závislost kódového slova na původní informaci:

Lineární kódy

Injektivní lineární zobrazení $g : (\mathbb{Z}_2)^k \to (\mathbb{Z}_2)^n$ je *lineární kód*. Matice $G$ typu $k/n$ reprezentující toto zobrazení ve standardních bázích se nazývá generující *matice kódu*.

[8] Více o této krásné teorii a jejích souvislostech s kódy se lze dočíst např. v knize Gilbert, W., Nicholson, K., Modern Algebra and its applications, John Wiley & Sons, 2nd edition, 2003, 330+xvii pp., ISBN 0-471-41451-4.

Generující matice je tvaru $G = \begin{pmatrix} P \\ \mathbb{I}_k \end{pmatrix}$, kde $P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$. Matice kontroly je tvaru $\begin{pmatrix} \mathbb{I}_{n-k} & P \end{pmatrix}$, tedy v našem případě je

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Přijaté slovo vynásobíme kontrolní maticí a dostáváme tak syndrom (chybu) slova:

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Syndrom příslušný přijatému slovu je tedy 01111. Nyní určíme všechna slova příslušná tomuto syndromu. Dostaneme je tak, že k přijatému slovu přičteme postupně všechna platná kódová slova. Platná kódová slova jsou čtyři, odpovídající čtyřem možným zprávám, které můžeme poslat. Získáme je vynásobením možných zpráv (00, 01, 10, 11) generující maticí. Dostáváme tak slova

$$0000000,\ 1111101,\ 1010110,\ 0101011.$$

Prostor slov odpovídajících danému syndromu je afinní prostor se zaměřením daným vektorovým prostorem všech platných kódových slov (viz 11.66). Dostáváme tak slova

$$0010111,\ 1101010,\ 1000001,\ 0111100.$$

Nejmenší možný počet chyb při přenosu je roven minimálnímu počtu jedniček v kódových slovech s daným syndromem. V našem případě ze čtyř kódových slov má nejméně jedniček slovo 1000001, které je tedy takzvaným vedoucím reprezentantem třídy slov se syndromem 01111. Nejmenší možný počet chyb ve slově se syndromem 01111 jsou dvě. Původně přenášené slovo pak získáme odečtením (což je v $\mathbb{Z}_2$ ekvivalentní přičtení) přijatého slova a vedoucího reprezentanta třídy s daným syndromem. V našem případě

$$0010111 - 1000001 = 1010110.$$

Pro každé slovo $v$ je příslušným kódovým slovem delší vektor

$$u = G \cdot v.$$

**Věta.** *Každý polynomiální $(n, k)$–kód je lineární kód.*

Důkaz. Použijeme elementární vlastnosti dělení polynomů se zbytkem. Použijme naše přiřazení polynomu $v(x) = r(x) + x^{n-k} m(x)$ původní polynomiální zprávě $m(x)$ na součet dvou různých zpráv $m(x) = m_1(x) + m_2(x)$. Zbytek po dělení $x^{n-k}(m_1(x) + m_2(x))$ je díky jednoznačnosti dělení dán jako součet zbytků $r_1(x) + r_2(x)$ pro jednotlivé zprávy. Dostaneme tedy

$$v(x) = r_1(x) + r_2(x) + x^{n-k}(m_1(x) + m_2(x)),$$

což je požadovaná aditivita. Protože jediným nenulovým skalárem je v $\mathbb{Z}_2$ jednička, dokázali jsme požadovanou linearitu zobrazení slova $m(x)$ na delší slovo $v(x)$. Toto zobrazení je navíc injektivní, protože původní slovo $m(x)$ je prostě zkopírováno za přidané bity. □

Např. uvažujme polynomiální $(6, 3)$–kód využívající polynomu $p(x) = 1 + x + x^3$ pro kódování slov se třemi bity. Vyčíslením na jednotlivých bázových prvcích $m_i(x) = x^{i-1}$, $i = 1, 2, 3$ dostáváme

$$v_0 = (1 + x) + x^3,$$
$$v_1 = (x + x^2) + x^4,$$
$$v_2 = (1 + x + x^2) + x^5$$

a tedy matice odpovídající tomuto $(6, 3)$–kódu je

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Protože je u polynomiálních kódů vždy původní slovo zkopírováno za přidané kontrolní bity, musí mít každý lineární kód vzniklý z polynomiálního matici s jednotkovým blokem $\mathbb{I}_k$ řádu $k$ zabírajícím posledních $k$ řádků matice, doplněným maticí $P$ s $n - k$ řádky a $k$ sloupci.

**11.65. Věta.** *Je-li $g : (\mathbb{Z}_2)^k \to (\mathbb{Z}_2)^n$ lineární kód s (blokově zapsanou) maticí*

$$G = \begin{pmatrix} P \\ \mathbb{I}_k \end{pmatrix},$$

*potom zobrazení $h : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^{n-k}$ s maticí*

$$H = \begin{pmatrix} \mathbb{I}_{n-k} & P \end{pmatrix}$$

*má následující vlastnosti*

*(1)* $\operatorname{Ker} h = \operatorname{Im} g$,
*(2) přijaté slovo $u$ je kódové slovo, právě když je $H \cdot u = 0$.*

Důkaz. Složení $h \circ g : (\mathbb{Z}_2)^k \to (\mathbb{Z}_2)^{n-k}$ je dáno součinem matic (počítáme nad $\mathbb{Z}_2$)

$$H \cdot G = \begin{pmatrix} \mathbb{I}_{n-k} & P \end{pmatrix} \cdot \begin{pmatrix} P \\ \mathbb{I}_k \end{pmatrix} = P + P = 0.$$

Za předpokladu nejmenšího možného počtu chyb při přenosu bylo tedy odesláno slovo 1010110, informační bity jsou pouze poslední dva, tedy slovo 10. □

*11.141.* Uvažujme (7, 3) lineární kód generovaný polynomem $x^4 + x^3 + x + 1$. Napište jeho generující a kontrolní matice. Metodou vedoucích reprezentantů dékodujte přijatou zprávu 1110010, za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb. ○

**11.142.** V lineárním (7, 4)-kódu (tj. délka vlastní zprávy jsou 4) nad $\mathbb{Z}_2$ zadaném maticí

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

byla přijata zpráva 1010001. Dekódujte ji (tj. nalezněte odesílanou zprávu) za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

**Řešení.** Je možných $2^4$, tedy 16 posílaných zpráv. Všechna platná kódová slova pak dostaneme pronásobením možných zpráv (0000, 0001, ..., 1111) generující maticí kódu. Dostáváme tak slova:

| | | | |
|---|---|---|---|
| 0110001, | 1010010, | 1100100, | 0111000 |
| 1100011, | 1010101, | 0001001, | 1011100 |
| 1101010, | 0110110, | 0001110, | 1101101 |
| 1011011, | 0000111, | 0111111, | 0000000. |

Nyní sestavíme matici kontroly parity daného kódu:

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

(z generující matice jsme vzali blok, který netvoří jednotkovou matici, a před něj napíšeme čtvercový blok tvořený jednotkovou maticí tak aby „pasoval“). Pokud vynásobíme vektor obdržené zprávy $z^T = (1010001)$ maticí $H$ dostáváme syndrom zprávy $s = Hz = (110)^T$. Jedno ze slov s tímto syndromem je slovo 1100000 (syndrom doplníme nulami do správné délky). Všechna slova se syndromem 110 dostaneme přičtením tohoto slova ke všem kódovým slovům. Získáváme tak slova

| | | | |
|---|---|---|---|
| 1010001, | 0110010, | 0000100, | 1011000, |
| 0000011, | 0110101, | 1101001, | 0111100, |
| 0001010, | 1010110, | 1101110, | 0001101, |
| 0111011, | 1100111, | 1011111, | 1100000 |

Z těchto slov se syndromem 110 obsahuje pouze slovo 0000100 pouze jednu jedničku, jedná se tedy o vedoucího reprezentanta třídy

Dokázali jsme tedy $\operatorname{Im} g \subseteq \operatorname{Ker} h$. Protože je prvních $n-k$ sloupců v $H$ tvořeno bázovými vektory v $(\mathbb{Z}_2)^{n-k}$, má obraz $\operatorname{Im} h$ maximální dimenzi $n-k$ a tedy má tento obraz $2^{n-k}$ různých vektorů. Vektorové prostory nad $\mathbb{Z}_2$ jsou konečné komutativní grupy, proto můžeme použít vztah mezi mohutnostmi podgrup a faktorgrup z odstavce 11.10 a dostáváme

$$|\operatorname{Ker} h| \cdot |\operatorname{Im} h| = |(\mathbb{Z}_2)^n| = 2^n.$$

Proto je počet vektorů v $\operatorname{Ker} h$ roven $2^n \cdot 2^{k-n} = 2^k$. K dokončení důkazu prvního tvrzení si nyní stačí povšimnout, že obraz $\operatorname{Im} f$ má také $2^k$ prvků.

Druhé tvrzení je samozřejmým důsledkem prvního tvrzení. □

Matici $H$ z věty se říká *matice kontroly parity* příslušného $(n, k)$–kódu.

Např. matice $H = (1\ 1\ 1)$ je zjevně takovou maticí pro (3, 2) kód přidávající jeden paritní bit k slovu o dvou bitech. Skutečně ji snadno dostaneme z matice

$$G = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

zadávající tento kód.

Pro výše uvedený (6, 3)–kód to bude matice

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

**11.66. Samoopravné kódy.** Jak jsme viděli, přenos zprávy $u$ dává výsledek

$$v = u + e.$$

To je ale nad $\mathbb{Z}_2$ ekvivalentní $e = u + v$.

Pokud tedy známe vektorový podprostor $V \subseteq (\mathbb{Z}_2)^n$ správných kódových slov, víme u každého výsledku, že správné slovo (s opravenými případnými chybami) je ve třídě rozkladu $v + V$ ve faktorovém vektorovém prostoru $(\mathbb{Z}_2)^n/V$.



Zobrazení $h : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^{n-k}$ zadané maticí kontroly parity má $V$ za jádro, proto indukuje injektivní lineární zobrazení $h : (\mathbb{Z}_2)^n/V \to (\mathbb{Z}_2)^{n-k}$. Jeho hodnoty jsou jednoznačně určeny hodnotami $H \cdot u$.

SYNDROMY SLOV

Hodnota $H \cdot u$, kde $H$ je matice kontroly parity pro lineární kód, se nazývá *syndrom* slova $u$ v tomto kódu.

Samozřejmým důsledkem konstrukce je následující:

**Věta.** *Dvě slova jsou ve stejné třídě rozkladu $u + V$, právě když sdílí syndrom.*

Samoopravné kódy nyní můžeme konstruovat tak, že pro každý syndrom určíme prvek v příslušné třídě, který je nejvhodnějším slovem. Budeme patrně vybírat tak, abychom s co největší pravděpodobností opravili jednu, případně více chyb.

Zkusme si to na příkladu (6, 3), pro který už máme spočteny matice $G$ a $H$. Sestavíme tabulku všech syndromů a jim odpovídajících kódových slov.

slov se syndromem 110. Odečtením vedoucího reprezentanta od obdržené zprávy dostáváme zprávu, která byla odeslána, došlo-li k nejmenšímu možnému počtu chyb (v tomto případě k jedné), tedy zprávu (101)0101, z níž jsou poslední čtyři bity informační. Poslaná informace byla 0101. □

**11.143.** V lineárním (7, 4)-kódu (tj. délka vlastní zprávy je 4) nad $\mathbb{Z}_2$ zadaném maticí

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

byla přijata zpráva 1101001. Dekódujte ji (tj. nalezněte odesílanou zprávu) za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

**Řešení.** Syndrom 101, vedoucí reprezentant 0001000, poslaná zpráva (110)0001 □

**11.144.** V lineárním (7, 4)-kódu (tj. délka vlastní zprávy jsou 4) nad $\mathbb{Z}_2$ zadaném maticí

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

byla přijata zpráva 0000011. Dekódujte ji (tj. nalezněte odesílanou zprávu) za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

**Řešení.** Syndrom 011, vedoucí reprezentant 0000100, poslaná zpráva (000)0111. □

**11.145.** V lineárním (7, 4)-kódu (tj. délka vlastní zprávy jsou 4) nad $\mathbb{Z}_2$ zadaném maticí

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

byla přijata zpráva 0001100. Dekódujte ji (tj. nalezněte odesílanou zprávu) za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Syndrom 000 mají právě všechna kódová slova. Všechna možná slova s daným syndromem pak dostaneme přičtením syndromu (doplněného nulami na délku kódového slova) ke všem kódovým slovům.

V následujících dvou tabulkách jsou v prvním řádku příslušné syndromy, na dalším řádku pak uvádíme ten z vektorů v příslušné třídě, který má nejméně jedniček. Skoro ve všech případech jde o jedinou jedničku, jen v posledním sloupci máme jedničky dvě a zvolili jsme si jako význačný prvek ten, který má jedničky vedle sebe (třeba protože věříme, že násobné chyby s větší pravděpodobností nastávají těsně po sobě)

| 000 | 100 | 010 | 001 |
|---|---|---|---|
| **000000** | **100000** | **010000** | **001000** |
| 110100 | 010100 | 100100 | 111100 |
| 011010 | 111010 | 001010 | 010010 |
| 111001 | 011001 | 101001 | 110001 |
| 101110 | 001110 | 111110 | 100110 |
| 001101 | 101101 | 011101 | 000101 |
| 100011 | 000011 | 110011 | 101011 |
| 010111 | 110111 | 000111 | 011111 |

| 110 | 011 | 111 | 101 |
|---|---|---|---|
| **000100** | **000010** | **000001** | **000110** |
| 110000 | 110110 | 110101 | 110010 |
| 011110 | 011000 | 011011 | 011100 |
| 111101 | 111011 | 111000 | 111111 |
| 101010 | 101100 | 101111 | 101000 |
| 001001 | 001111 | 001100 | 001011 |
| 100111 | 100001 | 100010 | 100101 |
| 010011 | 010101 | 010110 | 010001 |

Počínaje druhým sloupcem první tabulky, je každý sloupec tabulky afinním prostorem, jehož zaměřením je vektorový prostor daný prvním sloupcem první tabulky. Je tomu tak, protože daný kód je lineární, všechna kódová slova tedy tvoří vektorový prostor a jednotlivé třídy ve faktorovém prostoru jsou afinní podprostory.

Zejména je tedy rozdíl každých dvou slov ve stejném sloupci nějakým kódovým slovem. Tučně vyznačená slova představují tzv. vedoucí reprezentanty třídy (afinního prostoru) odpovídajícího danému syndromu. Jsou to slova s nejmenším počtem jedniček v sloupci. Udávají tak nejmenší počet bitových změn, které musíme v libovolném slovu na sloupci provést, abychom dostali kódové slovo.

Např. pokud dostaneme kódové slovo 111101, má syndrom 110. Vedoucím reprezentantem ve třídě tohoto syndromu je slovo 000100 a jeho odečtením od obdrženého kódového slova dostaneme platné kódové slovo 111001. Je to platné kódové slovo s nejmenší Hammingovou vzdáleností od obdrženého slova. Odeslaná zpráva tedy patrně byla 001.

**Řešení.** Syndrom 110, vedoucí reprezentant 0000010, poslaná zpráva (000)1110. □

**11.146.** Máme množinu čtyř slov, která chceme přenášet binárním kódem, který by uměl opravovat jednoduché chyby. Jakou nejmenší délku kódového slova můžeme použít, požadujeme-li, aby všechna kódová slova měla stejnou délku? Proč?



**Řešení.** Označme hledanou délku jako $n$. Minimální Hammingova vzdálenost dvou kódových slov musí být alespoň tři. To znamená, že pokud ve dvou kódových slovech změníme jeden bit, nemůžeme dostat stejná slova. Množina slov, které dostaneme z jednoho kódového slova změnou nejvýše jednoho bitu, čítá (včetně původního slova) $n+1$ slov. Pro různá kódová slova musíme dostat disjunktní množiny. Celkem tedy takto dostáváme $4(n+1)$ různých slov délky $n$. Slov délky $n$ je ovšem $2^n$, požadujeme tedy $4(n+1) \leq 2^n$. Tato nerovnost je splňena až pro $n \geq 5$. Kódová slova musí tedy mít délku minimálně 5. Hledaná kódová slova délky 5 s minimální Hammingovou vzdáleností 3 jsou například: 00111, 01001, 10100, 11010. □

**11.147.** Kolik minimálně bitů musí mít kódové slovo kódu (uvažujeme pouze kódy se stejnou délkou kódových slov), který má čtyři informační bity a opravuje až dvojnásobné chyby?



**Řešení.** Provedeme analogickou úvahu jako v předchozím příkladě. Má-li kód opravovat dvojnásobné chyby, tak Hammingova vzdálenost libovolných dvou slov musí být alespoň pět. To znamená, že pokud v libovolných dvou kódových slovech změníme libovolný bit, či dva bity, tak nikdy nedostaneme ta stejná slova nebo slovo kódové. Označíme-li $n$ délku kódového slova tak dostáváme nerovnost

$$2^4 \left(1 + n + \binom{n}{2}\right) \leq 2^n.$$

Nejmenší $n$, které nerovnost splňuje je $n = 10$, kódové slovo tedy musí mít alespoň osm bitů. Není složité takový kód vymyslet, necháváme na čtenáři. □

### Řešení cvičení

*11.3.* i) Není ani grupoid (operace není na dané množině uzavřená), ii) nekomutativní monoid, iii) komutativní grupa, iv) nekomutativní grupa, v) grupa, vi) pologrupa (1 není neutrální prvek kvůli prvku 0).

*11.4.*

i) $G$ tvoří komutativní monoid,
ii) $G$ tvoří komutativní grupu,
iii) $G$ tvoří komutativní grupu.

*11.5.*

i) Daná množina s operací tvoří komutativní pologrupu, která není monoidem.
ii) Daná množina s operací tvoří nekomutativní grupoid, který není pologrupou.
iii) Daná množina tvoří nekomutativní grupoid, který není pologrupou.
iv) Daná množina tvoří nekomutativní pologrupu, která nemá neutrální prvek.
v) Daná množina tvoří komutativní monoid, který není grupou.
vi) Daná množina tvoří komutativní monoid, který není grupou.
vii) Daná množina tvoří nekomutativní grupu.

*11.8.* Jedná se o nekomutativní grupu.

*11.9.*

i) $(1, 3, 5, 7, 2, 4, 6)$
ii) $(1, 3, 2) \circ (4, 6, 5)$, $(1, 4, 2, 5, 3, 6)$, $(1, 5, 2, 6, 3, 4)$, $(1, 6, 2, 4, 3, 5)$
iii) Neexistuje

*11.12.* Žádná taková neexistuje, díky paritě.

*11.22.*

i) Ano
ii) Ne
iii) Ano
iv) Ne
v) Ano
vi) Ano
vii) Ne
viii) Ne

*11.23.*

i) Ano
ii) Ne

*11.24.* $m = 10$.

*11.35.* Tvrzení není pravdivé. Uvažte například $\mathbb{S}_n/\mathbb{A}_n \sim Z_2$, $n \geq 3$.

*11.40.* Čtyřprvková podgrupa, přibude pouze zrcadlení podle roviny kolmé k uvažované rovině obsahující osu rotace (je izomorfní Kleinově grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$). Není normální.

*11.50.*

i) Je izomorfismus
ii) Je homomorfismus, který není surjektivní ani injektivní.
iii) Není homomorfismus

*11.51.* V řešení uvádíme právě vlastnosti, které daný předpis má. Vyjímku tvoří fakt, že všechny předpisy zadávají zobrazení, což neuvádíme.

i) je surjektivní homomorfismus,
ii) je surjektivní homomorfismus,
iii) je homomorfismus,
iv) není ani homomorfismus,
v) Je homomorfismus,
vi) Je homomorfismus.

*11.52*.

i) Je surjektivní homomorfismus, který není injektivní.
ii) Není homomorfismus.
iii) Není homomorfismus.

*11.53*.

i) Je to injektivní, nesurjektivní homomorfismus.
ii) Není ani zobrazení („obraz“ neleží v $\mathbb{A}_4$).

*11.54*.

i) Je injektivní homomorfismus.
ii) Není homomorfismus.
iii) Není homomorfismus.
iv) Není homomorfismus.

*11.55*.

i) Je homomorfismus.
ii) Předpis nezadává zobrazení.
iii) Je surjekivní homomorfismus.

*11.61*. $\frac{1}{36}\left(\frac{18!}{(6!)^3}+2\cdot 3!+2\cdot\frac{6!}{(2!)^3}+\frac{9!}{(3!)^3}+18\frac{9!}{(3!)^3}\right)=477368.$

*11.62*. $\frac{1}{48}\left(\frac{24!}{(8!)^3}+\frac{12!}{(4!)^3}+2\frac{6!}{2^3}+4\cdot 3!+24\frac{12!}{(4!)^3}\right)=197216213.$

*11.63*. 7.
*11.70*. 31.
*11.71*. 45.
*11.72*. 63.
*11.73*. 33.
*11.74*. Předpokládejte opak, totiž že polynom je součinem dvou polynomů s celočíselnými koeficienty. Indukcí dokažte, že jeden z těchto mnohočlenů má všechny koeficienty dělitelné prvočíslem $p$ (začněte u absolutního členu). Pak by však byl i vedoucí koeficient $f(x)$ dělitelný $p$.

*11.85*. Nad $\mathbb{R}$: $(x-1)(2x^2-x+1)^2$, nad $\mathbb{C}$: $(x-1)\left(x-\frac{1\pm i\sqrt{7}}{4}\right)^2$.

*11.86*. Nad $\mathbb{R}$: $(x+1)(x^2+x+2)^2$, nad $\mathbb{C}$: $(x+1)\left(x+\frac{1\pm i\sqrt{7}}{4}\right)^2$.

*11.87*. Nad $\mathbb{R}$: $(x^2-3x+2)^2$, nad $\mathbb{C}$: $\left(x-1+\sqrt{2}i\right)^2\left(x-1-\sqrt{2}i\right)^2$.

*11.88*. $x^5+x^2+2x+1=(x^2+1)(x^3+2x+1)$.

*11.89*. $x^4+2x^3+2$ je ireducibilní. Nemá kořeny a není součinem dvou polynomů stupně 2 (nutno početně ověřit!).

*11.117*. $A'\wedge C'$.
*11.118*. ($A$ NAND($B$ NAND $B$)).
*11.123*. Např. {1, 2, 3, 12, 18}.
*11.125*. Tři různé Hasseovy diagramy vyhovujících uspořádání. Celkem $5!+5!+5!/4=270$.

*11.136.*

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

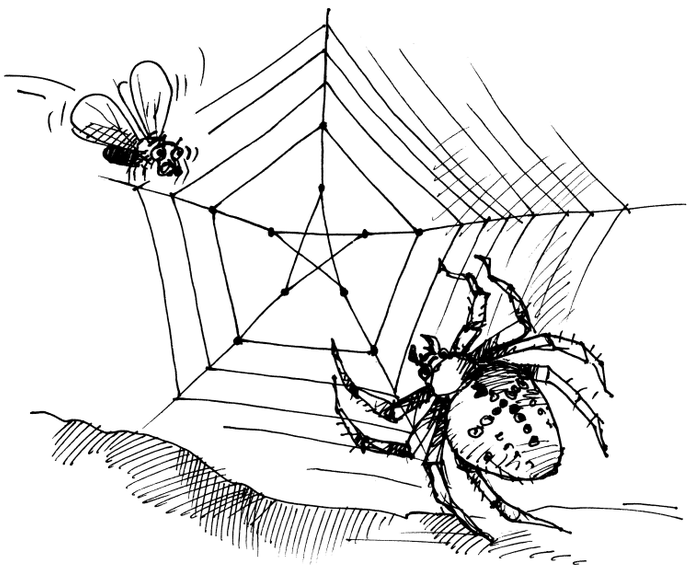
1

*11.141.* Nelze jednoznačně rozhodnout. V úvahu připadají zprávy 010, 110, 111.

KAPITOLA 12

# Kombinatorické metody, grafy a algoritmy

*že tak často myslíme raději v obrázcích?*
*– ano, ale spočíst zvládneme jen diskrétní věci ...*



## A. Základní pojmy

Jednou z pohnutek vzniku teorie grafů byla vizualizace jistých problémů obsahujících relace. Lidský mozek rád uvažuje o věcech, které si umí představit. A tak se nám líbí znázornění binární relace jakožto grafu, kde vrcholy odpovídají prvkům a hrany (čáry mezi nimi) pak tomu, že dané dva prvky jsou v relaci. Případně můžeme zakódovat relaci složitěji, třeba jako v Hasseho diagramu (viz 11.52). O uspořádáních prakticky uvažujeme výhradně jako o Hasseho diagramech. Do grafů lze také převést například relaci přátelství či známosti mezi lidmi. To dává vzniknout celé řadě „rekreačních“ problémů.

**12.1.** Na vysokoškolských kolejích se každý večer pořádají párty. Jeden student vždycky pozve všechny své známé bydlících na koleji a vzájemně je představí (pokud už se neznají). Předpokládejme, že každý obyvatel koleje už uspořádal alespoň jednu párty a někteří dva

V této kapitole se vrátíme k problémům, ve kterých jde o vzájemné vztahy nebo vlastnosti konečných množin objektů. Tzv. kombinatorické úlohy jsme naznačili již v druhé části první kapitoly a zavedly nás také k rekurencím v části následující. Čtenář si jistě ulehčí další práci připomenutím odstavců 1.7–1.13.

Podobně jako teorie čísel je kombinatorika oblastí matematiky, kde můžeme problémy i jejich řešení často velice snadno formulovat. O to těžší, a z hlediska používaných metod i komplexnější, bývá jejich řešení.

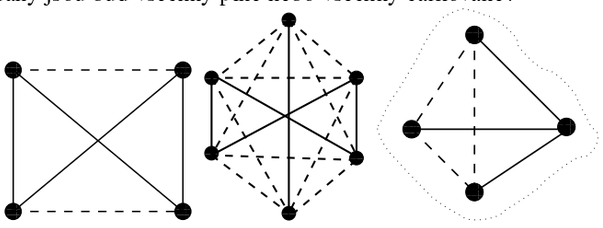
## 1. Grafy a algoritmy

**12.1. Dva ilustrační příklady.** Na večírku se někteří návštěvníci



po dvojicích znají a jiné dvojice se naopak neznají. Kolik lidí musíme pozvat, abychom zaručili, že se alespoň tři hosté buď navzájem po dvou znají nebo po dvou neznají?

Situace, jako je tato, si umíme dobře představit pomocí obrázku. Puntíky nám představí jednotlivé hosty, plnou čarou spojíme ty dvojice, které se znají, čárkovanou ty ostatní. Naše tvrzení pak zní: při jakém počtu puntíků vždy najdeme trojúhelník, jehož strany jsou buď všechny plné nebo všechny čárkované?



Na levém obrázku se čtyřmi puntíky takový trojúhelník není, uprostřed je. Snadno ověříme, že jej najdeme vždy, když počet hostů bude alespoň šest. (Máme-li večírek s $n$ hosty, bude z každého puntíku vycházet $n-1$ čar. Při $n > 5$ budou jistě buď aspoň tři plné nebo aspoň tři čárkované. Situace je znázorněna na pravém obrázku. V zobrazeném kousku celé situace se sledovaný host se třemi jinými zná, zbylé puntíky jsou spojeny čárkovaně – to by znamenalo, že máme trojúhelník hostů, kteří se neznají. Pokud by se ale jedna dvojice z nich znala, vznikl by naopak trojúhelník hostů, kteří se znají.)

V druhém příkladu předpokládejme, že máme krabičku, která požírá jeden bit za druhým, a má svítit buď modře nebo červeně podle toho, zda byl poslední bit nula nebo jednička. Opět si schéma můžeme pěkně znázornit:

studenti se pořád ještě neznají. Ukažte, že nebudou seznámeni na následující párty.

**Řešení.** Ukážeme graf známostí mezi studenty na počátku (vrcholy odpovídají studentům, hrany odpovídají známostem). Ukážeme, že pokud nějací dva studenti leží ve stejné komponentě souvislosti tohoto grafu (existuje řetězec známých počínající jedním studentem a končících druhým), viz 12.12, pak už budou nutně seznámeni poté, co každý uspořádá alespoň jednu párty. Uvažme totiž nejkratší cestu (řetězec známostí) mezi studenty, kteří leží ve stejné komponentě souvislosti grafu. Vždy, když uspořádá párty někdo ležící na této cestě, tak zkrátí délku nejkratší cesty o jedna (pořadatel z cesty vypadne). Protože párty uspořádá každý ze studentů na cestě (známostí), tak budou seznámeni i dva studenti na konci. Pokud tedy nějací dva studenti nebyli seznámeni ani poté, co již každý uspořádal aspoň jednu párty, znamená to, že leží v jiných komponentách souvislosti grafu známostí a tímto způsobem nebudou seznámeni nikdy, zejména ne na příští párty. □

Základní pojmy z teorie grafů si procvičíme zejména na jednoduchých kombinatorických úlohách.

**12.2.** Určete, kolik hran mají grafy $K_6$, $K_{5,6}$, $C_8$.

**Řešení.** Úplný graf na 6 vrcholech $K_6$ má $\binom{6}{2} = 15$ hran, úplný bipartitní graf $K_{5,6}$ (viz 12.3) má $5 \cdot 6 = 30$ hran a konečně kružnice $C_8$ má 8 hran. □

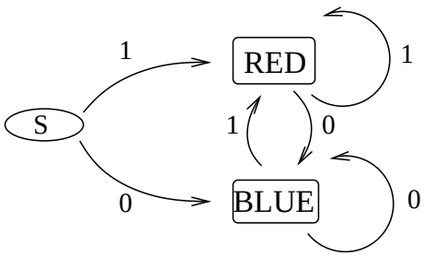
**12.3. Skóre grafu.** Ověřte, zda daná posloupnost je skóre (viz 12.7) nějakého grafu. Pokud ano, nějaký graf s tímto skóre nakreslete.

i) (1, 2, 3, 4, 5, 6, 7, 8, 9),
ii) (1, 1, 1, 2, 2, 3, 4, 5, 5).

**Řešení.** Nejprve bývá vhodné ověřit nutnou podmínku z (12.1). V prvním případě je $1 + \cdots + 9 = \frac{1}{2} \cdot 9 \cdot 10 = 45$, a podmínka tedy není splněna. Proto první posloupnost neodpovídá žádnému grafu.

Ve druhém případě je součet požadovaných stupňů roven 24 a nutná podmínka je splněna. Dále budeme postupovat podle věty Havla a Hakimiho z odstavce 12.7.

$$(1, 1, 1, \underline{2}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \mathbf{5}) \longleftrightarrow (1, 1, 1, \underline{1}, \underline{1}, \underline{2}, \underline{3}, \mathbf{4}) \longleftrightarrow$$
$$\longleftrightarrow (1, 1, 1, 0, 0, 1, 2) \longleftrightarrow (0, 0, 1, 1, \underline{1}, \underline{1}, \mathbf{2}) \longleftrightarrow$$
$$\longleftrightarrow (0, 0, 1, 1, 0, 0) \longleftrightarrow (0, 0, 0, 0, \underline{1}, \mathbf{1}) \longleftrightarrow$$
$$\longleftrightarrow (0, 0, 0, 0, 0).$$




Třetí vrchol, ze kterého pouze vychází dvě šipky, naznačuje start před prvním zaslaným bitem.

V obou příkladech máme společné schéma. Máme nějakou konečnou množinu objektů, kterou si znázorňujeme jako vrcholy, a jejich vlastnosti, které znázorňujeme spojnicemi mezi nimi. Už dávno víme, že takové situace umíme popisovat pomocí tzv. relací, viz text začínající odstavcem 1.36 v šesté části první kapitoly. Třeba čtenáře neodstraší ukázka, jak se jednoduchým věcem dá složitě říkat: V našem prvním příkladu pracujeme na stejné množině hostů se dvěma komplementárními symetrickými a antireflexními relacemi, ve druhém pak jde o příklad dvou antisymetrických relací na třech prvcích.

**12.2. Základní pojmy grafů.** My teď ale můžeme na relace pozapomenout a budeme pracovat s terminologií odpovídající našim obrázkům. Nenechte se zmást novým významem slova *graf*, pro který jsme již měli význam u funkcí. Ve skutečnosti není věcná podobnost až tak vzdálená.



### Grafy a orientované grafy

**Definice.** *Grafem* (též *neorientovaným grafem*) $G = (V, E)$ rozumíme množinu $V$ jeho *vrcholů* spolu s podmnožinou $E$ množiny $\binom{V}{2}$ všech dvouprvkových podmnožin ve $V$.

Prvkům $E$ říkáme *hrany grafu*. Vrcholům hrany $e = \{v, w\}$, $v \neq w$, říkáme *hraniční (krajní) vrcholy* hrany $e$. O hranách, které mají daný vrchol $v$ za hraniční, říkáme, že z vrcholu $v$ *vycházejí*.

*Orientovaným grafem* $G = (V, E)$ rozumíme množinu $V$ jeho vrcholů spolu s podmnožinou $E \subseteq V \times V$. Prvnímu z vrcholů definujících hranu $e = (v, w)$ říkáme *počáteční vrchol hrany*, druhému pak *koncový vrchol*. Hrana $e$ *vychází* ze svého počátečního vrcholu a *vchází* do koncového. U orientovaných hran mohou být koncový a počáteční vrchol totožný, hovoříme pak o *smyčce*.

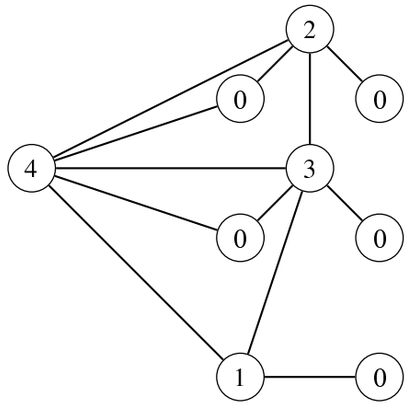
*Sousední hrany grafu* jsou ty, které sdílí hraniční vrchol, u *sousedních hran orientovaného grafu* musí být tento vrchol pro jednu hranu koncový a pro druhou počáteční. Naopak sousední vrcholy jsou ty, které jsou hraničními pro tutéž hranu.

Ke každému orientovanému grafu $G = (V, E)$ přiřazujeme jeho *symetrizaci*. Je to (neorientovaný) graf se stejnými vrcholy jako má $G$, přičemž $e = \{v, w\}$ je hranou, právě když alespoň jedna z hran $e' = (v, w)$ nebo $e'' = (w, v)$ patří do $E$.

Grafy jsou mimořádně dobrým jazykem pro přemýšlení o postupech a odvozování vztahů týkajících se konečných množin objektů. Jsou také pěkným příkladem kompromisu mezi přirozeným sklonem k „přemýšlení v obrázcích“ a přesným matematickým vyjadřováním.

Obecný jazyk teorie grafů nám v konkrétních úlohách umožňuje přidávat informace o vrcholech nebo hranách. Můžeme tak např. „obarvit“ vrcholy podle příslušnosti objektů k několika

Nebylo samozřejmě nezbytné provádět postup až do konce, mohli jsme skončit již ve chvíli, kdy máme posloupnost, které je zřejmě skórem nějakého grafu. Daná posloupnost je tedy skóre grafu, který zkonstruujeme postupem od konce (vždy je ale třeba dávat pozor, abychom přidávali hrany k vrcholům těch stupňů, které mají být spojeny s nově přidávaným vrcholem – v tomto místě je taky obecně možnost získat neizomorfní grafy se stejným skóre). Příkladem jednoho z možných výsledků je graf (čísla ve vrcholech udávají, v kterém kroku byl vrchol přidán)




□

**12.4.** Určete, kolik existuje navzájem neizomorfních úplných bipartitních grafů majících 1001 hran.

**Řešení.** Úplný bipartitní graf $K_{m,n}$ má $m \cdot n$ hran, úlohu lze tedy přeformulovat do tvaru: kolika způsoby je možné rozložit číslo 1001 na součin dvou čísel? Protože $1001 = 7 \cdot 11 \cdot 13$, dostáváme $1001 = 1 \cdot 1001 = 7 \cdot (11 \cdot 13) = 11 \cdot (7 \cdot 13) = 13 \cdot (7 \cdot 11)$. Máme tedy čtyři neizomorfní úplné bipartitní grafy:

$$K_{1,1001},\ K_{7,143},\ K_{11,91} \text{ a } K_{13,77}.$$ □

**12.5.** Určete, kolik existuje homomorfismů grafů (viz 12.4)

a) z $P_2$ do $K_5$,
b) z $K_3$ do $K_5$.

**Řešení.** Jediné omezení plynoucí z požadavku na homomorfismus je, že se vrcholy, mezi kterými vede hrana, nesmí zobrazit na tentýž vrchol.

a) $5 \cdot 4 \cdot 4 = 80$.
b) $5 \cdot 4 \cdot 3 = 60$. □

**12.6. Počet sledů.** Pomocí matice sousednosti (viz 12.8) určete počet sledů délky 4 z vrcholu 1 do vrcholu 2 v následujícím grafu:

disjunktním skupinám nebo můžeme označit hrany několika různými hodnotami apod. Existence hrany mezi vrcholy různých barev může naznačit „konflikt“. Např. když modré a červené vrcholy představují příslušnost k dvěma zájmovým skupinám osob, zatímco hrany označují plánované sousedství u obědové tabule, pak hrana mezi vrcholy různých barev může znamenat skutečný potenciální konflikt. Náš první příklad v předchozím odstavci můžeme tedy chápat jako graf s obarvenými hranami. Dokázané tvrzení v této řeči zní:

*V grafu $K_n = \left(V, \binom{V}{2}\right)$ s $n \geq 6$ vrcholy a se všemi možnými hranami, které jsou obarveny dvěma barvami, je vždy alespoň jeden trojúhelník z hran o stejné barvě.*

Orientovaný graf ve druhém příkladu výše, s označenými hranami hodnotami nula nebo jedna, představuje jednoduchý *konečný automat*. Tento název odráží představu, že graf popisuje proces, který se vždy nachází ve stavu popsaném některým z vrcholů, a další stav nastane po kroku odpovídajícím jedné z hran, které z vrcholu vychází. Teorií konečných automatů se zde ale nebudeme podrobněji zabývat.

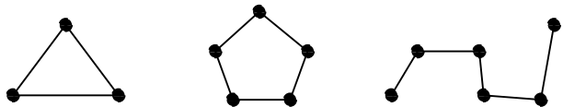
**12.3. Příklady užitečných grafů.** Nejjednodušším grafem je



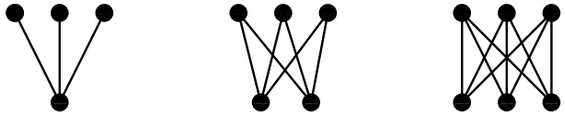
graf bez hran, pro ten si ale ani nebudeme zavádět zvláštní označení.

Opačný extrém je naopak užitečný a grafu se všemi možnými hranami říkáme *úplný graf*. Značíme jej symbolem $K_n$, kde $n$ je počet vrcholů grafu. Graf $K_4$ a $K_6$ jsme již viděli v úvodním odstavci, $K_3$ je *trojúhelník*, $K_2$ je *úsečka*.

Dalším důležitým grafem je *cesta*, tj. graf, kde existuje uspořádání vrcholů $(v_0, \ldots, v_n)$ takové, že $E = \{e_1, \ldots, e_n\}$, kde $e_i = \{v_{i-1}, v_i\}$ pro všechna $i = 1, \ldots, n$. Hovoříme o *cestě délky* $n$ a značíme ji $P_n$. Pokud cestu upravíme tak, že poslední a první vrchol splývají (pro $n \geq 3$), dostaneme *kružnici délky* $n$ a značíme $C_n$. Na dalším obrázku vidíme $K_3 = C_3$, $C_5$ a $P_5$.

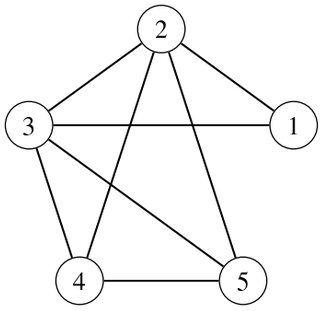


Dalším příkladem je tzv. *úplný bipartitní graf*, který vznikne tak, že vrcholy obarvíme dvěma barvami a pak přidáme všechny hrany, které spojí vrcholy různých barev. Značíme jej $K_{m,n}$, kde $m$ a $n$ jsou počty vrcholů s jednotlivými barvami. Na obrázku je vidět $K_{1,3}$, $K_{2,3}$ a $K_{3,3}$.



Dobrým příkladem grafu je také tzv. *hyperkostka* $H_n$ v dimenzi $n$, která vznikne tak, že vrcholy jsou všechna čísla $0, \ldots, 2^n - 1$. Hrany spojí právě ta čísla, která se v zápisu ve dvojkové soustavě liší v právě jednom bitu. Na obrázku níže je $H_4$ a popis vrcholů je naznačen.

Všimněme si, že přímo z definice vyplývá, že hyperkostku v dané dimenzi vždy dostaneme tak, že vhodně spojíme hranami




**Řešení.** Matice sousednosti zadaného grafu je

$$A_G = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

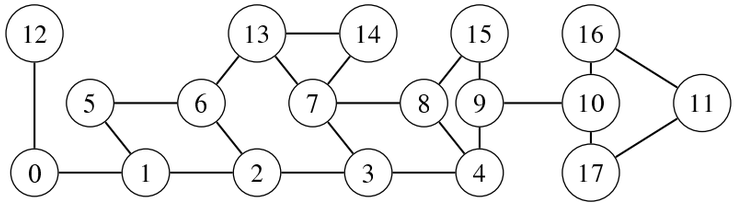
Počet sledů délky 4 z vrcholu 1 do 2 dostaneme jako prvek na pozici [1, 2] v matici $A_G^4$. Protože

$$A_G^2 = \begin{pmatrix} 2 & 1 & 1 & 2 & 2 \\ 1 & 4 & 3 & 2 & 2 \\ 1 & 3 & 4 & 2 & 2 \\ 2 & 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 2 & 3 \end{pmatrix},$$

je $(A_G^4)_{1,2} = (2, 1, 1, 2, 2) \cdot (1, 4, 3, 2, 2)^T = 17$. Dostali jsme tak 17 sledů délky 4 mezi vrcholy 1 a 2. □

*12.7. Mostem* v grafu rozumíme hranu, po jejímž odebrání se zvýší počet souvislých komponent grafu. *Artikulací* je vrchol se stejnou vlastností, tj. odebereme-li jej (samozřejmě spolu s incidentními hranami), dojde ke zvýšení počtu souvislých komponent.

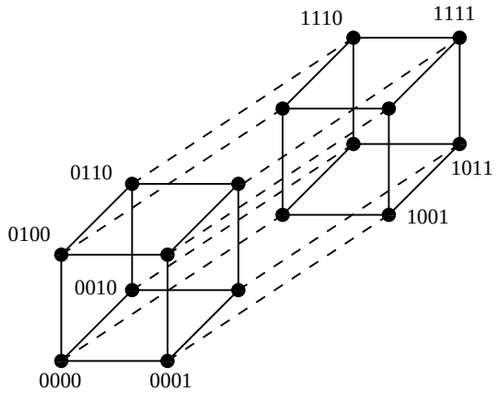
V grafu na obrázku najděte všechny mosty a artikulace.



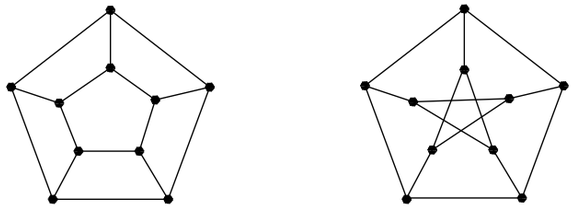

○

**12.8.** Dokažte, že hamiltonovský graf (viz 12.18) musí být vrcholově 2-souvislý. Udejte příklad grafu, který je vrcholově 2-souvislý a přesto v něm neexistuje hamiltonovská kružnice.

**Řešení.** V hamiltonovském grafu vedou mezi libovolnými dvěma vrcholy dvě neprotínající se cesty („oblouky“ hamiltonovské kružnice). Odstraněním jednoho vrcholu se tedy zjevně neporuší souvislost grafu (odstraněný vrchol může ležet pouze na jedné ze dvou cest). Příkladem dvě hyperkostky o jednu dimenzi menší. Na obrázku je to naznačeno tak, že příslušné hrany mezi dvěma disjunktními kopiemi $H_3$ jsou čárkované. Samozřejmě ale můžeme takto rozložit $H_4$ mnoha různými způsoby.




Poslední dva příklady jsou tzv. *cyklický žebřík* $CL_n$ s $2n$ vrcholy, který je vytvořen propojením dvou kopií kružnice $C_n$ tak, že hrany spojí odpovídající vrcholy dle pořadí, a tzv. *Petersenův graf*, který je sice docela podobný $CL_5$, ale ve skutečnosti je to nejjednodušší „vyvraceč nesprávných úvah“ – graf, na němž se vyplatí testovat tvrzení, než je začneme dokazovat.



**12.4. Morfismy grafů a podgrafy.** Jako vždy u matematických pojmů, klíčovou roli hrají i u grafů zobrazení mezi množinami vrcholů a hran, která zachovávají uvažovanou strukturu. Ve skutečnosti stačí sledovat jen zobrazení mezi vrcholy.



### Morfismy grafů

**Definice.** Pro grafy $G = (V, E)$ a $G' = (V', E')$ nazveme *morfismem* (též *homomorfismem*) $f : G \to G'$ takové zobrazení $f_V : V \to V'$ mezi množinami vrcholů, že je-li $e = \{v, w\}$ hrana v $E$, pak $e' = \{f_V(v), f_V(w)\}$ musí být hranou v $E'$.

V dalším textu nebudeme ve značení odlišovat morfismus $f$ a zobrazení $f_V$. Zároveň pak takové zobrazení $f_V$ určuje i zobrazení $f_E : E \to E'$, $f_E(e) = e'$, kde $e$ a $e'$ jsou jako výše.

Pro orientované grafy je definice shodná, jen pracujeme s uspořádanými dvojicemi $e = (v, w)$ v roli hran.

Všimněme si, že u grafů tato definice znamená, že pokud $f(v) = f(w)$ pro dva různé vrcholy ve $V$, pak mezi nimi nesměla být hrana. U orientovaných grafů je taková hrana přípustná, pokud je na společném obrazu smyčka.

Speciálním případem je morfismus libovolného grafu $G$ do úplného grafu $K_m$. Takový morfismus je ekvivalentní vybranému obarvení vrcholů grafu $G$ pomocí $m$ různých jmen vrcholů $K_m$ tak, že stejně obarvené vrcholy nejsou spojeny hranou. Hovoříme v tomto případě o *barvení grafu* pomocí $m$ barev.

grafu, který je vrcholově 2-souvislý a přesto v něm neexistuje hamiltonovská kružnice, je například Petersenův graf (viz úvodní obrázek ke kapitole). □

**12.9.** Určete, kolik existuje v grafu $K_5$ různých kružnic (viz 12.3).

**Řešení.** Spočítáme postupně délky kružnic délek tři, čtyři a pět. Kružnice délky tři je jednoznačně dána třemi vrcholy na ní. Tři vrcholy můžeme vybrat $\binom{5}{3}$ způsoby. Kružnice délky 4 je dána svými vrcholy (ty můžeme vybrat $\binom{5}{4}$ způsoby) a dvojicí sousedů jednoho pevně zvoleného vrcholu na kružnici (tu je možné vybrat $\binom{3}{2}$ způsoby ze zbývajících tří vrcholů). Konečně kružnice délky pět je dána opět dvojicí sousedů jednoho pevně zvoleného vrcholu a navíc ještě dalším vrcholem (ze dvou zbylých), sousedícím s jedním vybraným vrcholem ze dvou sousedů. Celkem tak máme

$$\binom{5}{3}+\binom{5}{4}\cdot\binom{3}{2}+\binom{5}{5}\cdot\binom{4}{2}\cdot\binom{2}{1}=37$$

možností. □

**12.10.** Určete počet podgrafů (viz 12.4) grafu $K_5$.

**Řešení.** Počet podgrafů spočítáme postupně podle počtu $v$ jejich vrcholů:

- $v=0$. Jde o prázdný graf. Ten je pouze jediný.
- $v=1$. Jeden vrchol můžeme vybrat pěti způsoby, celkem tedy máme 5 grafů.
- $v=2$. Dva vrcholy můžeme vybrat $\binom{5}{2}$ způsoby, mezi vybranými vrcholy pak buď vede nebo nevede hrana. Celkem je tedy $\binom{5}{2}\cdot 2$ takových grafů.
- $v=3$. Tři vrcholy můžeme vybrat $\binom{5}{3}$ způsoby, mezi každými dvěma vybranými vrcholy buď vede, nebo nevede hrana, celkem $\binom{5}{3}\cdot 2^{\binom{3}{2}}$ grafů.
- $v=4$. Zde napočítáme $\binom{5}{4}\cdot 2^{\binom{4}{2}}$ grafů.
- $v=5$. V tomto případě máme $\binom{5}{5}\cdot 2^{\binom{5}{2}}$ grafů.

Celkem jsme našli 1550 podgrafů grafu $K_5$. □

**12.11.** Určete počet cest mezi dvěma různými pevně vybranými vrcholy v grafu $K_7$.

**Řešení.** Spočítáme cesty postupně podle jejich délky. Cesta délky jedna je jedna (hrana spojující dva vybrané vrcholy). Cest délek dva je pět (vybíráme jeden z pěti zbylých vrcholů, přes který cesta půjde). Cest délek tři je $5\cdot 4$ (vybíráme dva vrcholy, přes které cesta půjde, včetně jejich pořadí), obdobně cest délky čtyři je $5\cdot 4\cdot 3$, cest délky pět je $5\cdot 4\cdot 3\cdot 2$ a konečně cest délky šest je taktéž $5!$. Delší cesty v $K_7$ nejsou. Celkem máme $1+5+5\cdot 4+5\cdot 4\cdot 3+5!+5!=326$ cest. □

A na závěr tohoto oddílu ještě jedna zábavná úloha.

V případě, že je morfismus $f: G\to G'$ bijekcí na vrcholech takovou, že i $f^{-1}$ je morfismem, hovoříme o *izomorfismu* grafů. Izomorfní grafy se liší pouze různým pojmenováním vrcholů.

Každý morfismus orientovaných grafů je také morfismem jejich symetrizací. Naopak to samozřejmě obecně neplatí.

Jednoduchými a mimořádně užitečnými příklady morfismů grafů jsou pojmy *cesta*, *sled* a *kružnice* v grafu:

### Cesty, sledy a kružnice v grafech

*Sled délky* $n$ v grafu $G$ je jakýkoliv morfismus $s: P_n\to G$ (tj. v obrazu se mohou opakovat vrcholy i hrany).

*Tah* je speciální případ sledu, v němž se mohou opakovat vrcholy, ale nikoliv hrany.

*Cestou délky* $n$ v grafu $G$ rozumíme morfismus $p: P_n\to G$ takový, že $p$ je injektivní zobrazení (tj. všechny obrazy vrcholů $v_0,\dots,v_n$ z $P_n$ jsou různé).

*Kružnice* délky $n$ v grafu $G$ je morfismus $c: C_n\to G$ takový, že $c$ je injektivní zobrazení vrcholů.

Budeme přitom často pro zjednodušení zápisu našich úvah ztotožňovat morfismus a jeho obraz. Obvykle budeme sledy konkrétně zapisovat ve tvaru $(v_0,e_1,v_1,\dots,e_n,v_n)$, kde $e_i=\{v_{i-1},v_i\}$ pro $i=1,\dots,n$.

Sled si můžeme představit jako dráhu „přičinlivého ale tápajícího“ poutníka z vrcholu $f(v_0)$ do vrcholu $f(v_n)$. Poutník se totiž v žádném vrcholu (neorientovaného) grafu nezastaví. Skutečně v $P_n$ existuje vždy mezi následujícími vrcholy $v_{i-1}$ a $v_i$ hrana, zatímco smyčky v neorientovaných grafech nepřipouštíme. Klidně se ale po cestě grafem vrací do vrcholů nebo i dokonce po hranách, kterými dříve šel. Poutník „na tahu“ je již o něco moudřejší a cesta je naopak průchod grafem z počátečního vrcholu $f(v_0)$ do koncového $f(v_n)$ bez zbytečných oklik.

**12.5. Podgrafy.** Obrazy cest, sledů i kružnic jsou příklady tzv. *podgrafů*, ne však stejným způsobem. Definujme nejprve obecně, co je to podgraf. K souvislosti s morfismy se vrátíme vzápětí.



### Podgrafy

**Definice.** Graf $G'=(V',E')$ je podgrafem v grafu $G=(V,E)$, jestliže $V'\subseteq V$, $E'\subseteq E$.

Jestliže si v grafu $G=(V,E)$ vybereme nějakou podmnožinu vrcholů $V'\subseteq V$, pak největším podgrafem s těmito vrcholy je tzv. *indukovaný podgraf*. Je to graf $G'=(V',E')$, kde $e\in E$ patří i do $E'$, právě když oba krajní vrcholy hrany $e$ patří do $V'$. Jde tedy o případ, kdy množina hran $E'$ je dána jako průnik $E\cap\binom{V'}{2}$.

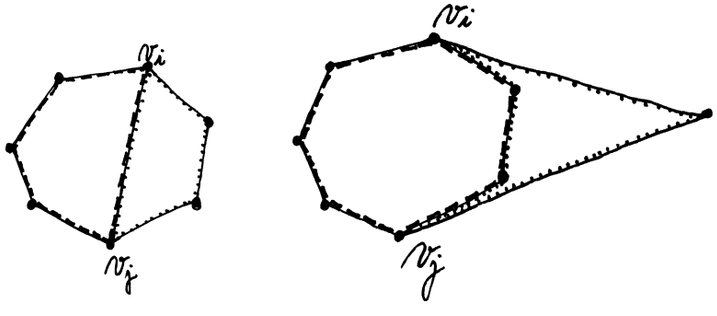
Dalším zvláštním případem je tzv. *faktor* grafu – je to podgraf $G'=(V,E')$, který má stejnou množinu vrcholů jako $G$, ale jeho množina hran $E'$ je libovolnou podmnožinou. *Klika* je pak takový podgraf grafu $G$, který je izomorfní nějakému úplnému grafu.

Každý podgraf tedy můžeme sestrojit postupným použitím těchto dvou případů – napřed zvolíme $V'\subseteq V$ a pak v indukovaném podgrafu na $V'$ vybereme cílovou množinu hran $E'$.

Snadno je vidět, že každý obraz homomorfismu (tj. obraz jak vrcholů, tak hran) tvoří podgraf.

**12.12.** V jisté zemi jsou města spojená cestami. Každé město je přímo spojeno právě se třemi jinými. Dokažte, že existuje město, ze kterého lze podniknout okružní cestu, při které použijeme počet cest, který není dělitelný třemi.

**Řešení.** Formulujme tuto úlohu v řeči teorie grafů: v grafu, ve kterém je stupeň každého vrcholu roven třem, existuje kružnice, jejíž délka není dělitelná třemi. Dokážeme indukcí dokonce silnější tvrzení: v grafu, ve kterém je stupeň každého vrcholu roven alespoň třem, existuje kružnice, jejíž délka není dělitelná třemi. Toto tvrzení lze na rozdíl od původního dokázat, neboť v indukčním kroku máme k dispozici silnější předpoklady, než by tomu bylo u tvrzení původního. Indukci povedeme vzhledem k počtu $k$ vrcholů grafu. Pro $k = 4$ je tvrzení jednoduché. Mějme tedy graf, ve kterém jsou stupně všech vrcholů rovny třem. Indukční předpoklad zní, že libovolném grafu, ve kterém jsou stupně všech vrcholů rovny třem a má menší počet vrcholů menší než daný graf tvrzení platí. V grafu zřejmě existuje kružnice (čtenář jistě nebude mít problémy si toto tvrzení dokázat). Pokud její délka není dělitelná třemi, jsme hotovi. Předpokládejme tedy pro spor, že $C = v_1 v_2 \dots v_{3n}$. Každý z vrcholů této cesty musí být v daném grafu spojen ještě s minimálně jedním dalším vrcholem, než jsou jeho sousedé na kružnici. Pokud by v uvedené cestě byl nějaký vrchol $v_i$ spojen s nějakým vrcholem $v_j$ ($j > i + 1$), pak by cesty $v_1 v_2 \dots v_i v_j v_{j+1} \dots v_{3n}$ a $v_i v_{i+1} \dots v_j$ měly součet délek roven $3n+2$, tedy délka alespoň jedné z nich by nebyla dělitelná třemi. Podobně, pokud by nějaké vrcholy $v_i$ a $v_j$, $1 \le i < j \le 3n$ byly spojeny se stejným vrcholem mimo kružnici.




V tomto novém grafu vedou opět minimálně tři hrany z každého vrcholu (včetně $V$) a můžeme na něj tedy použít indukční předpoklad. V novém grafu tedy máme kružnici $w_1 w_2 \dots w_k$, kde $3 \nmid k$. Pokud v ní není obsažen vrchol $V$, tak jde o kružnici v původním grafu. Pokud je, tak analogicky jako v předchozích případech uvážíme dvě kružnice, součet jejichž délek je $3n + 2k$ a tudíž délka minimálně jedné z nich není dělitelná třemi. V každém případě dostáváme spor, čímž je indukční krok a tím i celý důkaz ukončen. □

**12.6. Kolik je vlastně neizomorfních grafů?** Snadno si budeme umět načrtnout až na izomorfismus všechny grafy na málo vrcholech (třeba třech nebo čtyřech). Obecně jde ale o nesmírně složitý kombinatorický problém a i rozhodnutí o konkrétních dvou daných grafech, zda jsou izomorfní, je obecně mimořádně obtížné.

**Poznámka.** Rozhodnout, zda jsou dva dané grafy izomorfní (tzv. *Graph isomorphism problem*), je úkol, který je poměrně zvláštním příslušníkem třídy **NP**-problémů[1] – není o něm známo ani, je-li **NP**-úplný, ani je-li polynomiální složitosti. Naproti tomu, o tzv. *Subgraph isomorphism problem* je známo, že je **NP**-úplný.

Odpovědět přesně i jen na otázku v záhlaví odstavce je děsně těžké. Odhadnout, že je neizomorfních grafů „moc“, je ale poměrně snadné. Všech možných grafů na $n$ vrcholech je totiž tolik, kolik je všech podmnožin v množině hran. Všech podmnožin v množině o mohutnosti $k$ je $2^k$. Izomorfních grafů s danými $n$ vrcholy nemůže být víc, než kolik je bijekcí na $n$ vrcholech, a těch je $n!$. Neizomorfních grafů tedy nemůže být méně než

$$k(n) = \frac{2^{\binom{n}{2}}}{n!}.$$

Jestliže si tuto funkci zlogaritmujeme při základu 2, dostaneme (používáme zjevný vztah $n! \le n^n$)

$$\log_2 k(n) = \binom{n}{2} - \log_2 n! \ge \frac{n^2}{2}\left(1 - \frac{1}{n} - \frac{2\log_2 n}{n}\right).$$

Pro velká $n$ tedy zjevně dostáváme

$$\log_2 k(n) = \frac{1}{2}n^2 - O(n \log_2 n),$$

viz terminologii pro asymptotické odhady z odstavce 6.17 na straně 340.

**12.7. Stupně vrcholů a skóre grafu.** Relativně snadné může být ověření, že dva dané grafy izomorfní nejsou. Izomorfní grafy se totiž od sebe liší pouze přejmenováním vrcholů. Proto musí mít stejné všechny číselné nebo jiné charakteristiky, které se přečíslováním vrcholů nemění. Jednoduché údaje tohoto typu můžeme dostat např. sledováním počtů hran vycházejících z jednotlivých vrcholů.

STUPNĚ VRCHOLŮ A SKÓRE GRAFU

Pro vrchol $v \in V$ v grafu $G = (V, E)$ říkáme, že jeho *stupeň* je $k$, jestliže v $E$ existuje $k$ hran, jejichž hraničním vrcholem $v$ je. Píšeme v takovém případě

$$\deg v = k.$$

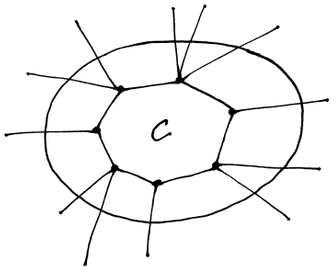
*Skóre grafu* $G$ s vrcholy $V = (v_1, \dots, v_n)$ je posloupnost

$$(\deg v_1, \deg v_2, \dots, \deg v_n).$$

U orientovaných grafů rozlišujeme *vstupní stupeň* $\deg_+ v$ vrcholu $v$ a *výstupní stupeň* $\deg_- v$. Říkáme, že orientovaný graf je *vyvážený*, když pro všechny vrcholy platí $\deg_- v = \deg_+ v$.

[1] Wikipedia, *NP (complexity)*, `http://en.wikipedia.org/wiki/NP_(complexity)` (as of Aug. 7, 2013, 13:44 GMT).

Předpokládejme tak, že každý z vrcholů kružnice je spojen s nějakými vrcholy mimo $C$, přičemž žádné dva nejsou spojeny se stejným vrcholem. Za tohoto předpokladu je korektní uvážit graf, který vznikne z původního grafu nahrazením všech vrcholů $v_1, v_2, \ldots, v_{3n}$ jediným vrcholem $V$.




### B. Základní algoritmy

Začněme s algoritmy prohledávání do šířky a do hloubky, které slouží jako základ pro složitější algoritmy. Jejich konkrétní implementace může být různá, proto odpovědi na následující příklady nejsou jednoznačné.

**12.13.** Uvažme graf o šesti vrcholech 1, 2,..., 6. Vrcholy jsou spojeny hranou, právě když je součet jejich čísel lichý. Popište práci algoritmu prohledávání do šířky na tomto grafu. Kterou hranu tohoto grafu projde algoritmus jako poslední, bude-li počátečním vrcholem vrchol 5 a hrany ze zpracovávaného vrcholu uvažujeme postupně podle hodnoty druhého koncového vrcholu hrany (od nejmenšího)?

**Řešení.** Z vrcholu 5 algoritmus postupně projde hrany (5, 2), (5, 4), (5, 6) a detekuje tím postupně vrcholy 2, 4, 6 (fronta detekovaných vrcholů je 2, 4, 6). Prvním detekovaným vrcholem je vrchol 2, algoritmus tedy pokračuje s ním, vrchol 5 se stává zpracovaným a vrchol 2 se stává aktivním. Z něj vedou hrany (2, 5) (již prošlá) a nové hrany (2, 1), (2, 3) a s nimi se detekují postupně vrcholy 1 a 3. Algoritmus prošel všechny hrany z vrcholu 2, ten se tedy stává zpracovaným (fronta detekovaných nezpracovaných vrcholů je tedy 4, 6, 1, 3) a první z detekovaných vrcholů, který ještě není zpracovaný, se stává aktivním. Tím je vrchol 4. Objevíme nové hrany (4, 1) a (4, 3), nedetekujeme přitom žádné nové vrcholy. Vrchol 4 se stává zpracovaným a na řadě je ve frontě vrchol 6. Tak objevíme hrany (6, 1) a (6, 3). Pokud zná algoritmus počet hran v grafu, končí. Jinak projde ještě vrcholy 1 a 3 a zjistí, že z nich už žádné nové hrany nevedou, a skončí. Poslední objevenou hranou je hrana (3, 6). □

**12.14.** Uvažme graf o šesti vrcholech 1, 2,..., 6. Vrcholy jsou spojeny hranou, právě když je jejich součet lichý. Popište práci algoritmu prohledávání do hloubky na tomto grafu. Kterou hranu tohoto grafu projde tento algoritmus jako poslední, bude-li počátečním vrcholem

Je zřejmé, že pro izomorfní grafy se jejich skóre může lišit pouze permutací hodnot. Pokud tedy porovnáme skóre grafů setříděné podle velikosti hodnot, pak různá skóre zaručují neizomorfnost grafu. Naopak ale snadno najdeme příklad grafů se stejným skóre, které izomorfní být nemohou, např. $G = C_3 \cup C_3$ má skóre $(2, 2, 2, 2, 2, 2)$ stejně jako $C_6$. Zjevně ale izomorfní nejsou, protože v $C_6$ existuje cesta délky 5, která v druhém grafu být nemůže.

Podíváme se na kritéria, jaká skóre mohou vůbec grafy mít. Protože každá hrana vychází ze dvou vrcholů, musí být v celkovém součtu skóre započtena každá hrana dvakrát (v angličtině bývá tato podmínka z pochopitelných důvodů zmiňována jako *handshake lemma*). Proto platí

$$\sum_{v \in V} \deg v = 2|E|. \tag{12.1}$$

Zejména tedy musí být součet všech hodnot skóre sudý.



Následující věta[2] Havla a Hakimiho je naší první úvahou o operacích nad grafy. Protože je důkaz konstruktivní, jde vlastně o návod, jak pro dané skóre buď najít příklad takového grafu, nebo zjistit, že takový graf neexistuje.

**Věta** (Algoritmus na sestrojení grafu s daným skóre)**.** *Pro libovolná přirozená čísla $0 \le d_1 \le \cdots \le d_n$ existuje graf $G$ na $n$ vrcholech s těmito hodnotami skóre tehdy a jen tehdy, když existuje graf se skóre*

$$(d_1, d_2, \ldots, d_{n-d_n} - 1, d_{n-d_n+1} - 1, \ldots, d_{n-1} - 1)$$

*na $n-1$ vrcholech.*

Důkaz. Na jednu stranu je implikace jednoduchá: Pokud existuje graf $G'$ o $n-1$ vrcholech se skóre uvedeným ve větě, pak můžeme přidat ke grafu $G'$ nový vrchol $v_n$ a spojit jej hranou s posledními $d_n$ vrcholy grafu $G'$. Tím dostaneme požadovaný graf $G$ s předepsaným skóre.

Naopak je to o něco těžší. Postup nám zároveň ukáže, jak málo skóre určuje graf, z něhož vzniklo. Ukážeme, že při pevně zadaném skóre $(d_1, \ldots, d_n)$ s $0 \le d_1 \le \cdots \le d_n$ vždy existuje graf, jehož vrchol $v_n$ je spojen hranou právě s posledními $d_n$ vrcholy $v_{n-d_n}, \ldots, v_{n-1}$.

Idea je jednoduchá – pokud některý z posledních $d_n$ vrcholů $v_k$ není hranou spojen s $v_n$, musí být $v_n$ spojen s některým z vrcholů dřívějších. Pak bychom měli umět prohodit koncové vrcholy dvou hran tak, aby $v_n$ a $v_k$ spojeny byly a skóre se nezměnilo.



Technicky to lze provést takto: Uvažme všechny grafy $G$ s daným skóre a označme si pro každý takový graf číslo $\nu(G)$, které je největším indexem vrcholu, který není spojen hranou s vrcholem $v_n$. Nechť $G$ je nyní pevně zvolený graf s $\nu(G)$ nejmenším možným. Pak buďje $\nu(G) = n - d_n - 1$, a získali jsme tak požadovaný graf, nebo je $\nu(G) \ge n - d_n$.

Pokud by platil druhý případ, musel by být $v_n$ spojen hranou s některým $v_i$, $i < \nu(G)$. Protože je $\deg v_{\nu(G)} \ge \deg v_i$, nutně existuje nějaký vrchol $v_\ell$, do kterého vede hrana z $v_{\nu(G)}$, ale nikoliv z vrcholu $v_i$. Nyní záměnou hrany $\{v_\ell, v_{\nu(G)}\}$ za $\{v_\ell, v_i\}$ a zároveň hrany $\{v_i, v_n\}$ za hranu $\{v_{\nu(G)}, v_n\}$ dostáváme graf $G'$ s týmž skóre, ale menším $\nu(G')$, což je spor s naší volbou. Namalujte si obrázek!

[2] Dokázaná nezávisle Václavem Havlem v roce 1955 v *Časopise pro pěstování matematiky* a S.L. Hakimim v roce 1962.

vrchol 5 a hrany ze zpracovávaného vrcholu procházíme podle hodnoty druhého koncového vrcholu hrany (od nejmenšího)?

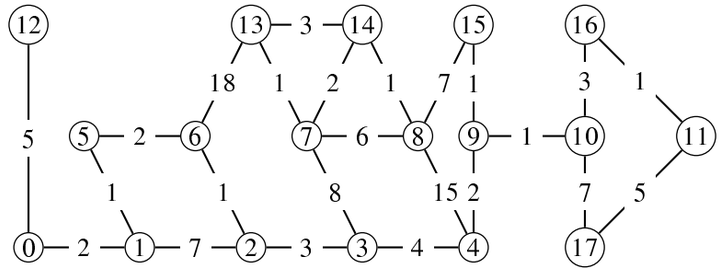
**Řešení.** Algoritmus nejprve objeví hrany vedoucí z vrcholu 5 a to dle zadání v posloupnosti (5, 2), (5, 4), (5, 6). Vrcholy jsou tedy aktivovány v pořadí 2, 4, 6. Vrchol 5 se stává zpracovaným a zásobník detekovaných vrcholů je 6, 4, 2. Pokračujeme s naposledy detekovaným vrcholem, tj. vrcholem 6. Objevíme hrany (6, 1), (6, 3), vrchol 6 je zpracovaný, zásobník detekovaných vrcholů je tedy 3, 1, 4, 2. Pokračujeme s vrcholem 3. Objevíme hrany (3, 2), (3, 4), zásobník vrcholů bude 4, 2, 1, 4, 2. s vrcholem 4, objevíme hranu (4, 1), zásobník vrcholů bude 1, 2, 1, 2, pokračujeme s vrcholem 1, objevíme poslední hranu (1, 2). (Pozn.: do zásobníku zapisujeme vždy pouze ještě nezpracované vrcholy.) □

**Poznámka.** Pokud bychom volili opačnou prioritu hran tak bychom dostali následující posloupnost postupně prohledávaných hran: (5, 2), (2, 1), (1, 4), (4, 3), (3, 2), (3, 6), (6, 1), (6, 5), (4, 5). Intuitivně si prohledávání do hloubky můžeme představit také tak, že algoritmus zpracovává v každém vrcholu pouze první dosud neprozkoumanou hranu.

*12.15.* Označme vrcholy v grafu $K_6$ postupně čísly 1, 2,..., 6. Napište posloupnost hran grafu $K_6$ tak, jak je bude procházet algoritmus „prohledávání do hloubky“, bude-li počátečním vrcholem vrchol 3 a hrany ze zpracovávaného vrcholu budeme procházet postupně podle velikosti druhého koncového vrcholu hrany (od nejmenšího). ○

*12.16.* Označme vrcholy v grafu $K_6$ postupně čísly 1, 2,...6. Napište posloupnost hran grafu $K_6$ tak, jak je bude procházet algoritmus „prohledávání do šířky“, bude-li počátečním vrcholem vrchol 3 a hrany ze zpracovávaného vrcholu budeme procházet postupně podle velikosti druhého koncového vrcholu hrany (od nejmenšího). ○

*12.17.* Užijte Dijkstrův algoritmus k nalezení nejkratších cest z vrcholu číslo 9 do všech ostatních vrcholů.




○

**12.18.** Udejte příklad

Nutně tedy platí první z možností, tj. náš graf vznikl přidáním posledního vrcholu a jeho spojením s posledními $d_n$ vrcholy hranou. □

Všimněme si, že skutečně věta dává přesný postup, jak zkonstruovat graf se zadaným skóre. Pokud by takový graf neexistoval, algoritmus to po cestě pozná. Postup je takový, že od zadaného vzestupně uspořádaného skóre postupně odprava od hodnot stupňů vrcholů odečítáme tolikrát jedničku, kolik je největší hodnota $d_n$. Uspořádáme znovu podle získaného skóre a postupujeme stejně, dokud buď neumíme přímo graf se zadaným skóre napsat, nebo naopak nevidíme, že takový neexistuje. Jestliže graf v některém z kroků sestrojíme, zpětným postupem přidáváme vždy jeden nový vrchol a hrany podle toho, jak jsme odečítali jedničky. Zkuste si několik jednoduchých příkladů sami. Uvědomme si ale, že algoritmus sestrojuje pouze jeden z mnoha grafů, které mohou k danému skóre existovat!

**12.8. Algoritmy a reprezentace grafů.** Jak jsme již naznačovali,



grafy jsou jazykem, ve kterém často formulujeme algoritmy. Samotný pojem (grafového) algoritmu můžeme (pro naše potřeby) formalizovat jako postup, kdy v nějakém orientovaném grafu přecházíme z vrcholu do vrcholu podél orientovaných hran a přitom zpracováváme informace, které jsou určeny a ovlivněny výsledkem předchozích operací, vrcholem, ve kterém se zrovna nacházíme, a hranou, kterou jsme do vrcholu vstoupili. Při zpracování informace se zároveň rozhodujeme, kterými výstupními hranami budeme pokračovat a v jakém pořadí.

Pokud je graf neorientovaný, můžeme všechny hrany považovat za dvojice hran orientované opačnými směry.

Případně také můžeme při chodu algoritmu samotný graf upravovat, tj. přidávat či odebírat vrcholy a hrany.

Abychom mohli dobře takové algoritmy realizovat (většinou s pomocí počítače), je třeba umět uvažovaný graf efektivně zadat. Jednou z možností je tzv. *hranový seznam* (Edge List). Orientovaný nebo neorientovaný graf $G = (V, E)$ si v něm reprezentujeme jako dva seznamy $V$ a $E$ propojené ukazateli tak, že každý vrchol ukazuje na všechny z něj vycházející a do něj vcházející hrany a každá hrana ukazuje na svůj počáteční a koncový vrchol. Je vidět, že paměť potřebná na uchování grafu je v tomto případě $O(|V|+|E|)$, protože na každou hranu ukazujeme právě dvakrát a na každý vrchol ukazujeme tolikrát, kolik je jeho stupeň a součet stupňů je také roven dvojnásobku počtu hran. Až na konstantní násobek jde tedy stále o optimální způsob uchovávání grafu v paměti.

Zcela jiný způsob je zadání tzv. *matice sousednosti* grafu. Uvažme (neorientovaný) graf $G = (V, E)$, zvolme uspořádání jeho vrcholů $V = (v_1, \ldots, v_n)$ a definujme matici $A_G = (a_{ij})$ nad $\mathbb{Z}_2$ (tj. zaplněnou jen nulami a jedničkami) takto:

$$a_{ij} = \begin{cases} 1 & \text{jestliže je hrana } e_{ij} = \{v_i, v_j\} \text{ v } E, \\ 0 & \text{jestliže není hrana } e_{ij} = \{v_i, v_j\} \text{ v } E. \end{cases}$$

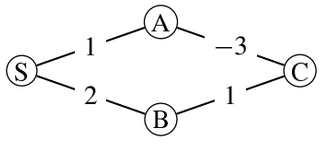
Popřemýšlejte samostatně, jak vypadají matice grafů z příkladů na začátku této kapitoly.

Při nejjednodušším způsobu uchovávání matic v poli je zadání grafu pomocí matice sousednosti velice neefektivní metoda. Potřebuje totiž vždy $O(n^2)$ místa v paměti. Pokud je ale v grafu

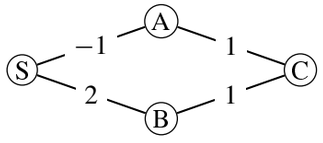
i) grafu s alespoň 4 vrcholy, který neobsahuje cyklus záporné délky a na němž dá Dijkstrův algoritmus chybný výsledek,

ii) grafu s alespoň 4 vrcholy, který obsahuje (alespoň jednu) zápornou hranu a přesto na něm dá Dijkstrův algoritmus správný výsledek.

**Řešení.** V obou případech je třeba si rozmyslet fungování Dijkstrova algoritmu. Pak už je snadné uvést požadované příklady (přitom je zřejmě mnoho dalších možností). V prvním případě je takovým grafem (s počátečním vrcholem $S$) například




Dijkstrův algoritmus začínající v $S$ jako první navštíví vrchol $A$ a za nejkratší označí cestu délky 1, přitom zřejmě existuje cesta $(S, B, C, A)$ délky 0. Podobně v druhém případě vyhovuje například graf




□

**Bellmanův-Fordův algoritmus.** Tento algoritmus pracuje na stejném principu jako Dijkstrův; místo postupu po jednotlivých vrcholech je ale zpracovává „naráz“ – cyklus *relaxace* (tedy porovnání zda současná ohodnocení vrcholů není možné zlepšit využitím dané hrany) probíhá $(|V|-1)$-krát přes všechny hrany. Jeho výhodou je, že připouští záporně ohodnocené hrany a detekuje záporné cykly (pokud provedeme relaxační cyklus navíc ještě jednou a dojde ke změně, musí být v grafu záporný cyklus). Cenou za to ale je (obvykle) vyšší časová náročnost.

**12.19.** Užijte Bellmanův-Fordův algoritmus k nalezení nejkratších cest z vrcholu $S$ do všech ostatních vrcholů. Hrany procházejte v pořadí dle čísla počátečního (příp. koncového) vrcholu (počáteční vrchol má nejmenší číslo). Změňte ohodnocení hrany $(8, 6)$ z 18 na $-18$, algoritmus proveďte s tímto novým grafem a ukažte, jak se detekují záporné cykly.

málo hran, dostáváme tzv. řídkou matici se skoro všemi prvky nulovými. Existuje řada postupů, jak takové řídké matice uchovávat v paměti efektivněji.

Mělo by nás zajímat, jak se v obou způsobech zadání grafu zpracují základní operace nad grafem, kterými rozumíme:

- *odebrání hrany*,
- *přidání hrany*,
- *přidání vrcholu*,
- *odebrání vrcholu*,
- *dělení hrany nově přidaným vrcholem.*

Na první pohled je patrné, že při realizaci matice jako pole nul a jedniček umíme první dvě operace v konstantním čase $O(1)$, zatímco ostatní v lineárním čase $O(n)$.

U hranového seznamu bude hodně záležet na implementaci datových struktur. V principu by ale operace měly být všechny v čase úměrném počtu měněných údajů v okamžiku, kdy již najdeme položku, kterou máme v seznamech měnit. Např. při odebrání vrcholu musíme také odebrat i všechny s ním sousedící hrany.

Maticová reprezentace je užitečná minimálně v teoretických úvahách s využitím maticového počtu:

**12.9. Věta.** *Nechť $G = (V, E)$ je graf s uspořádanými vrcholy $V = (v_1, \dots, v_n)$ a maticí sousednosti $A_G$. Označme $A_G^k = (a_{ij}^{(k)})$ prvky $k$-té mocniny matice $A_G = (a_{ij})$.*

*Pak $a_{ij}^{(k)}$ je počet sledů délky $k$ mezi vrcholy $v_i$ a $v_j$.*

Důkaz. Celý důkaz povedeme indukcí přes délku sledů. Tvrzení pro případ $k = 1$ je pouze jiným vyjádřením definice matice sousednosti. Předpokládejme tedy dále, že věta platí pro nějaké $k$ a zkoumejme, kolik je sledů délky $k+1$ mezi vrcholy $v_i$ a $v_j$ pro nějaké pevné indexy $i$ a $j$. Jistě každý takový sled obdržíme pomocí jedné hrany z $v_i$ do nějakého vrcholu $v_\ell$ a nějakého sledu délky $k$ mezi $v_\ell$ a $v_j$. Různé volby přitom dávají vždy různé výsledky. Proto označíme-li $a_{\ell j}^{(k)}$ počet různých sledů délky $k$ z $v_\ell$ do $v_j$, pak námi hledaný počet sledů délky $k+1$ bude

$$a_{ij}^{(k+1)} = \sum_{\ell=1}^{n} a_{i\ell} \cdot a_{\ell j}^{(k)}.$$

To je ale právě vztah pro násobení matice $A_G$ s mocninou $A_G^k$. Dokázali jsme, že naše čísla $a_{ij}^{(k+1)}$ jsou právě prvky matice $A_G^{k+1}$. □

**Důsledek.** *Jsou-li $G = (V, E)$ a $A_G$ jako v předchozí větě, pak lze všechny dvojice vrcholů $G$ spojit cestou, právě když má matice $(A + \mathbb{E}_n)^{n-1}$ samé nenulové členy (zde $\mathbb{E}_n$ označuje jednotkovou matici s $n$ řádky a sloupci).*

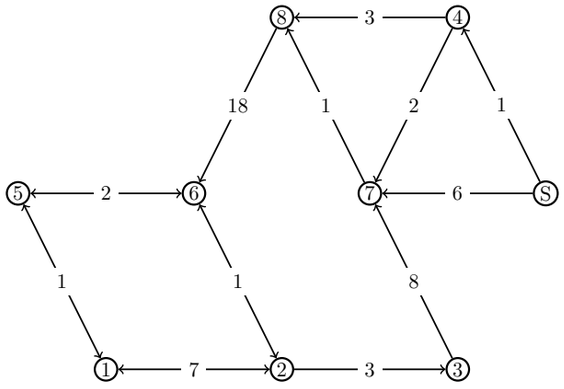
Důkaz. Díky distributivitě násobení matic a skutečnosti, že jednotková matice $\mathbb{E}_n$ komutuje s každou jinou maticí stejného rozměru, dostaneme roznásobením

$$(A + \mathbb{E}_n)^{n-1} = A^{n-1} + \binom{n-1}{1} A^{n-2} + \cdots + \binom{n-1}{n-2} A + \mathbb{E}_n.$$

Výsledná matice má za členy čísla (ve značení jako v minulé větě)

$$a_{ij}^{(n-1)} + \cdots + \binom{n-1}{\ell} a_{ij}^{(n-1-\ell)} + \cdots + (n-1)a_{ij} + \delta_{ij},$$

kde $\delta_{ii} = 1$ pro všechna $i$ a $\delta_{ij} = 0$ pro $i \neq j$.




**Řešení.** Hrany podle pokynů procházíme v pořadí: (S,4), (S,7), (1,2), (1,5), (2,1), (2,3), (2,6), (3,7), (4,7), (4,8), (5,1), (5,6), (6,2), (6,5), (7,8), (8,6). Ohodnocení vrcholů (v závorce jsou uvedeny případné vyšší hodnoty dosažené dříve během téhož průchodu):

| | $S$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | $\infty$ | $\infty$ | $\infty$ | 1 | $\infty$ | 22 | 3(6) | 4 |
| 2 | 0 | $\infty$ | 23 | $\infty$ | 1 | 24 | 22 | 3 | 4 |
| 3 | 0 | 25(30) | 23 | 26 | 1 | 24 | 22 | 3 | 3 |
| 4 | 0 | 25 | 23 | 26 | 1 | 24 | 22 | 3 | 3 |

Protože při čtvrtém průchodu již nedošlo ke změně, můžeme běh algoritmu v tuto chvíli ukončit.

V pozměněném grafu vypadá průchod takto (pro názornost nebudeme vypisovat hodnoty u vrcholů, které mezi průchody nedoznaly změn):

| | $S$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | $\infty$ | $\infty$ | $\infty$ | 1 | $\infty$ | $-14$ | 3(6) | 4 |
| 2 | | | $-13$ | | | $-12$ | | | |
| 3 | | $-11(-6)$ | | $-10$ | | | $-19$ | $-2$ | $-1$ |
| 4 | | | $-18$ | | | $-17$ | | | |
| 5 | | $-16$ | | $-15$ | | | $-24$ | $-7$ | $-6$ |
| 6 | | | $-23$ | | | $-22$ | | | |
| 7 | | $-21$ | | $-20$ | | | $-29$ | $-12$ | $-11$ |
| 8 | | | $-28$ | | | $-27$ | | | |
| 9 | | $-26$ | | $-25$ | | | $-34$ | $-17$ | $-16$ |

Graf má 9 vrcholů a protože při devátém průchodu ještě došlo ke změně, algoritmus detekoval záporný cyklus. Běh algoritmu jsme samozřejmě mohli ukončit již dříve, pokud bychom si všimli charakteru změn mezi jednotlivými kroky, z něhož je patrné, že u vrcholů 1, 2, 3, 5, 6, 7, 8 dochází k neohraničenému (a opakovanému) zmenšování ohodnocení. Algoritmus je samozřejmě možné naprogramovat tak, že produkuje strom nejkratších cest a v případě detekce záporného cyklu i vrcholy na tomto cyklu ležící. □

**Cesty mezi všemi dvojicemi vrcholů.** Často potřebujeme znát nejkratší cesty mezi všemi dvojicemi vrcholů – i k tomu lze sice

Toto číslo evidentně zadává součet počtů sledů délek $0, \ldots, n-1$ mezi vrcholy $v_i$ a $v_j$ vynásobených kladnými konstantami. Bude proto nenulové právě tehdy, jestliže mezi těmito vrcholy existuje nějaká cesta. □
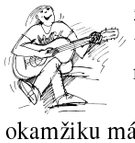
**12.10. Poznámka.** Ještě si všimněme vlivu permutace našeho uspořádání vrcholů $V$ na matici sousednosti grafu. Není obtížné si uvědomit, že permutace vrcholů grafu $G$ má za následek jednu a tutéž permutaci řádků i sloupců matice $A_G$. Každou takovou permutaci můžeme zadat právě jednou tzv. permutační maticí, tj. maticí z nul a jedniček, která má v každém řádku a každém sloupci právě jednu jedničku a jinak nuly. Je-li $P$ taková permutační matice, pak nová matice sousednosti izomorfního grafu $G'$ bude

$$A_{G'} = P \cdot A_G \cdot P^T,$$

kde transponovaná matice $P^T$ je zároveň maticí inverzní (zjevně jsou permutační matice ortogonální) a tečkou označujeme násobení matic. Každou permutaci umíme napsat jako složení transpozic a proto příslušnou permutační matici dostaneme jako součin příslušných matic pro transpozice.

Tyto úvahy lze v případě potřeby dále rozvíjet a přemýšlet o souvislostech matic sousednosti a matic lineárních zobrazení mezi vektorovými prostory.

**12.11. Prohledávání v grafu.** Mnoho užitečných algoritmů je založeno na postupném prohledávání všech vrcholů v grafu. Zpravidla máme zadaný počáteční vrchol nebo si jej na začátku procesu zvolíme.



V průběhu procesu vyhledávání pak v každém okamžiku máme vrcholy

- *již zpracované* – ty, které jsme již při běhu algoritmu procházeli a definitivně zpracovali;
- *aktivní* – ty vrcholy, které jsou detekovány a připraveny pro zpracovávání;
- *spící* – ty vrcholy, na které teprve dojde.

Zároveň si udržujeme přehled o již zpracovaných hranách. V každém okamžiku musí být množiny vrcholů a/nebo hran v těchto skupinách disjunktním rozdělením množin $V$ a $E$ vrcholů a hran grafu $G$ a některý z aktivních vrcholů je aktuálně zpracováván. Sledujme nejprve princip obecně na příkladě prohledávání vrcholů. V dalších odstavcích pak budeme postup používat pro algoritmy řešící konkrétní úlohy.

Na počátku průběhu takového algoritmu tedy máme jeden aktivní vrchol a všechny ostatní vrcholy jsou spící. V prvním kroku projdeme všechny hrany vycházející z aktivního vrcholu a jejich příslušným koncovým vrcholům, které jsou spící, změníme statut na aktivní. V dalších krocích vždy u zpracovávaného vrcholu probíráme ty z něho vycházející hrany, které dosud nebyly probrány a jejich koncové vrcholy přidáváme mezi aktivní. Tento postup aplikujeme stejně u orientovaných i neorientovaných grafů, jen se drobně mění význam adjektiv koncový a počáteční u vrcholů.

V konkrétních úlohách se také můžeme omezovat na některé z hran, které vychází z aktuálního vrcholu. Na principu to ale nic podstatného nemění.

Pro realizaci algoritmů je nutné se rozhodnout, v jakém pořadí zpracováváme aktivní vrcholy a v jakém pořadí zpracováváme hrany z nich vycházející. V zásadě přichází v úvahu dvě možnosti zpracovávání vrcholů:

použít předchozí algoritmy, aplikované postupně na všechny vrcholy v roli počátečního vrcholu, ale lze to provést ještě efektivněji. Jednou z možností je využít podobnosti s násobením matic, z čehož vychází *Floydův-Warshallův algoritmus* (nejznámější algoritmus typu *all pairs shortest paths*), který:

- v čase $O(n^3)$ vypočte vzdálenosti mezi všemi vrcholy;
- vychází z matice $U_0 = A = (a_{ij})$ délek hran (přičemž klade $u_{ii} = 0$ pro všechny vrcholy $i$) a postupně počítá matice $U_0, U_1, \ldots, U_{|V|}$, kde $u_k(i,j)$ je délka nejkratší cesty z $i$ do $j$, kde cesta prochází pouze vrcholy z $\{1, 2, \ldots, k\}$;
- při výpočtu matic vychází ze vztahu

$$u_k(i,j) = \min\{u_{k-1}(i,j), u_{k-1}(i,k) + u_{k-1}(k,j)\}.$$

Jinými slovy: u nejkratší cesty z $i$ do $j$, během níž máme povoleno navštívit pouze vrcholy očíslované $1, \ldots, k$, se můžeme ptát, jestli využívá vrchol $k$. Pokud ano, pak je tato cesta složením nejkratší cesty z $i$ do $k$ s nejkratší cestou z $k$ do $j$ (které využívají jen vrcholy $1, \ldots, k-1$). V opačném případě je tato hledaná cesta stejná jako nejkratší cesta z $i$ do $j$, která využívá jen vrcholy $1, \ldots, k-1$. Zřejmě pro $k = |V|$ dostaneme nejkratší cesty mezi všemi dvojicemi vrcholů (bez dalšího omezení). Budeme si navíc udržovat pro každý vrchol jeho nejbližšího předchůdce na cestě z vrcholu $i$ (tedy tzv. matici předchůdců) a aktualizovat podle následujícího předpisu:

- Inicializace:

$$(P_0)_{ij} = i \text{ pro } i \neq j \text{ a } a_{ij} < \infty,$$

- V $k$-tém kroku aktualizujeme

$$(P_k)_{ij} = \begin{cases} (P_{k-1})_{kj}, & \text{pokud vrchol } k \text{ přinesl vylepšení,} \\ (P_{k-1})_{ij}, & \text{jinak.} \end{cases}$$

Pak můžeme po ukončení výpočtu snadno zkonstruovat nejkratší cestu mezi libovolnými dvěma vrcholy tak, že při určování cesty z $u$ do $v$ z matice $P = P_n = (p_{ij})$ odvozujeme tuto cestu (v obráceném pořadí) podle předpisu $v, w = p_{uv}, p_{uw}, \ldots$.

**12.20.** Floydův a Warshallův algoritmus použijte na orientovaný graf na obrázku. Jednotlivé mezivýpočty zapisujte do matic. Uveďte, jak se v průběhu výpočtu detekují cykly záporné délky. Udržujte si všechny informace potřebné pro konstrukci minimálních cest.

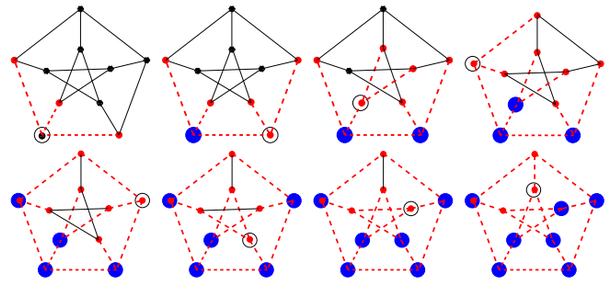
(1) vrcholy vybíráme pro další zpracování ve stejném pořadí, jako se stávaly aktivními (fronta),
(2) dalším vrcholem vybraným pro zpracování je poslední zaktivněný vrchol (zásobník).

V prvním případě hovoříme o *prohledávání do šířky*, ve druhém o *prohledávání do hloubky*.

Na první pohled je zřejmá role volby vhodných datových struktur pro uchovávání údajů o grafu. Hranový seznam umožňuje projít všechny hrany vycházející z právě zpracovávaného vrcholu v čase lineárně úměrném jejich počtu. Každou hranu přitom diskutujeme nejvýše dvakrát, protože má právě dva konce. Zjevně tedy platí:

**Věta.** *Celkový čas realizace vyhledávání do šířky i do hloubky je $O((n+m)K)$, kde $n$ je počet vrcholů v grafu, $m$ je počet hran v grafu a $K$ je čas potřebný na zpracování jedné hrany, resp. jednoho vrcholu.*

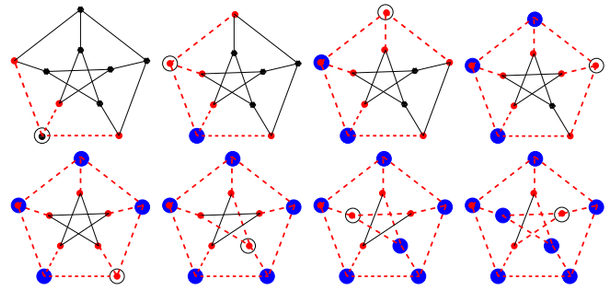
Následující obrázky slouží pro ilustraci prohledávání do šířky:



Je na nich zachyceno prvních osm kroků prohledávání do šířky Petersenova grafu.

Jemně zakroužkovaný vrchol je ten právě zpracovávaný, velké šedé puntíky jsou již zpracované vrcholy, čárkované šedé hrany jsou již zpracované a drobné šedé vrcholy jsou ty aktivní (poznají se také podle toho, že do nich již vede některá zpracovaná hrana). Hrany na obrázku zpracováváme v pořadí orientace proti směru hodinových ručiček, přičemž za „první“ bereme směr „kolmo dolů“.

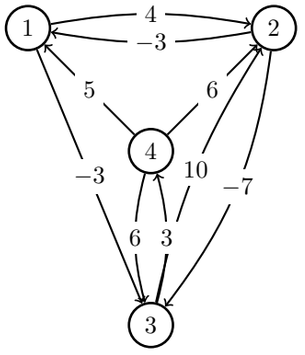
Totéž je na dalších obrázcích postupem „do hloubky“. Všimněte si, že první krok je stejný jako v předchozím případě.



**12.12. Souvislé komponenty grafu.** Každý graf $G = (V, E)$ se přirozeně rozpadá na disjunktní podgrafy $G_i$ takové, že vrcholy $v \in G_i$ a $w \in G_j$ jsou spojeny nějakou cestou, právě když $i = j$.



Tento postup si můžeme formalizovat takto: Nechť je $G = (V, E)$ neorientovaný graf. Na množině vrcholů grafu $G$ zavedeme relaci $\sim$ tak, že $v \sim w$, právě když existuje cesta z $v$ do $w$. Promyslete si, že tato relace je dobře definovaná a že se jedná o ekvivalenci. Každá třída $[v]$ této ekvivalence definuje indukovaný podgraf $G_{[v]} \subseteq G$ a disjunktní sjednocení těchto podgrafů je ve skutečnosti původní graf $G$. Skutečně podle




**Řešení.** Postupujeme podle algoritmu a dostáváme matice délek nejkratších cest spolu s maticemi předchůdců:

$$U_0 = \begin{pmatrix} 0 & 4 & -3 & \infty \\ -3 & 0 & -7 & \infty \\ \infty & 10 & 0 & 3 \\ 5 & 6 & 6 & 0 \end{pmatrix}, \quad P_0 = \begin{pmatrix} - & 1 & 1 & - \\ 2 & - & 2 & - \\ - & 3 & - & 3 \\ 4 & 4 & 4 & - \end{pmatrix};$$

$$U_1 = \begin{pmatrix} 0 & 4 & -3 & \infty \\ -3 & 0 & -7 & \infty \\ \infty & 10 & 0 & 3 \\ 5 & 6 & \mathbf{2} & 0 \end{pmatrix}, \quad P_1 = \begin{pmatrix} - & 1 & 1 & - \\ 2 & - & 2 & - \\ - & 3 & - & 3 \\ 4 & 4 & 1 & - \end{pmatrix};$$

$$U_2 = \begin{pmatrix} 0 & 4 & -3 & \infty \\ -3 & 0 & -7 & \infty \\ \mathbf{7} & 10 & 0 & 3 \\ \mathbf{3} & 6 & \mathbf{-1} & 0 \end{pmatrix}, \quad P_2 = \begin{pmatrix} - & 1 & 1 & - \\ 2 & - & 2 & - \\ 2 & 3 & - & 3 \\ 2 & 4 & 2 & - \end{pmatrix};$$

$$U_3 = \begin{pmatrix} 0 & 4 & -3 & \mathbf{0} \\ -3 & 0 & -7 & \mathbf{-4} \\ 7 & 10 & 0 & 3 \\ 3 & 6 & -1 & 0 \end{pmatrix}, \quad P_3 = \begin{pmatrix} - & 1 & 1 & 3 \\ 2 & - & 2 & 3 \\ 2 & 3 & - & 3 \\ 2 & 4 & 2 & - \end{pmatrix};$$

$$U_4 = \begin{pmatrix} 0 & 4 & -3 & 0 \\ -3 & 0 & -7 & -4 \\ \mathbf{6} & \mathbf{9} & 0 & 3 \\ 3 & 6 & -1 & 0 \end{pmatrix}, \quad P_4 = \begin{pmatrix} - & 1 & 1 & 3 \\ 2 & - & 2 & 3 \\ 2 & 4 & - & 3 \\ 2 & 4 & 2 & - \end{pmatrix}.$$

Protože se v matici $U_4$ na diagonále neobjevilo záporné číslo, graf neobsahuje záporný cyklus. Hledáme-li např. nejkratší cestu z 3 do 1, pak předchůdcem 1 na této cestě je $P_4[3, 1] = 2$ a předchůdcem 2 pak $P_4[3, 2] = 4$, proto je tato cesta 3, 4, 2, 1 a její délka je $U_4[3, 1] = 6$. □

**Hamiltonovské grafy.** Rozhodnutí, zda je zadaný graf hamiltonovský, je tzv. NP-úplný problém, je tedy dobré mít k dispozici nějaké jednodušší nutné nebo postačující podmínky pro tuto vlastnost.

Mezi známé postačující podmínky patří Diracova, Oreho a Bondy-Chvátalova věta.

**Dirac:** Má-li v grafu $G$ s $n \geq 3$ vrcholy každý vrchol stupeň alespoň $n/2$, je $G$ hamiltonovský.

definice naší ekvivalence, žádná hrana původního grafu nemůže propojovat vrcholy z různých komponent. Podgrafům $G_{[v]}$ říkáme *souvislé komponenty grafu* $G$.

Říkáme, že je graf $G = (V, E)$ *souvislý*, jestliže má jedinou souvislou komponentu.

Je-li graf $G$ orientovaný, pak většinou definujeme souvislost obdobně jako pro neorientované grafy, pouze u definice relace výslovně požadujeme, aby cesta existovala jak z vrcholu $v$ do vrcholu $w$, tak z vrcholu $w$ do vrcholu $v$. Nicméně je užitečný také pojem *slabé souvislosti*, kdy pouze požadujeme, aby symetrizace daného grafu byla souvislá.



Jako skutečně jednoduchý příklad prohledávání v grafu si můžeme uvést algoritmus na vyhledání všech souvislých komponent v grafu. Jedinou informací, kterou musíme zpracovávat při prohledávání do šířky nebo hloubky, je, kterou komponentu aktuálně procházíme.

Samotné prohledávání, tak jak jsme jej prezentovali, projde právě všechny vrcholy jedné komponenty. Začneme tedy se všemi vrcholy spícími a vezmeme kterýkoliv z nich. Kdykoliv při běhu algoritmu skončíme s prázdnou množinou aktivních vrcholů ke zpracování, máme nachystánu jednu celou komponentu na výstup. Stačí pak vzít jakýkoliv další dosud spící vrchol a pokračovat dále. Teprve až nebudou ani žádné spící vrcholy, ukončíme algoritmus.

**12.13. Vícenásobně souvislé grafy.** Pojem souvislosti potřebujeme i v silnějších podobách, kdy máme zaručenu určitou redundanci v množství cest mezi vrcholy.

**Definice.** Řekneme, že (neorientovaný) graf $G = (V, E)$ je

- *vrcholově k–souvislý*, jestliže má alespoň $k+1$ vrcholů a bude souvislý i po odebrání libovolné podmnožiny $k - 1$ vrcholů;
- *hranově k–souvislý*, jestliže bude souvislý po odebrání libovolné podmnožiny $k - 1$ hran.

V případě $k = 1$ definice jen opakuje souvislost grafu $G$ (neboť dodatečná podmínka je prázdná). Silnější souvislost grafu je žádoucí např. u síťových aplikací, kdy klient požaduje značnou redundanci poskytovaných služeb v případě výpadku některých linek (tj. hran) nebo uzlů (tj. vrcholů).

Obecně platí tvrzení tzv. *Mengerovy věty*[3]. Říká, že pro každé dva vrcholy $v$ a $w$ je v grafu $G = (V, E)$ počet hranově různých cest z $v$ do $w$ roven minimálnímu počtu hran, které je třeba odstranit, aby se $v$ a $w$ ocitly v různých komponentách vzniklého grafu. Stejně tak je počet vrcholově různých cest z $v$ do $w$ roven počtu vrcholů, které je třeba odstranit, aby byly vrcholy $v$ a $w$ v různých komponentách.

K této tématice se ještě vrátíme v odstavci 12.36. Podrobněji se ale hned podíváme aspoň na nejjednodušší zajímavý případ. To jsou takové souvislé grafy o alespoň třech vrcholech, kdy vynecháním libovolného vrcholu nenarušíme jejich souvislost.

**Věta.** *Pro graf $G = (V, E)$ s alespoň třemi vrcholy jsou následující podmínky ekvivalentní:*

- *$G$ je (vrcholově) 2–souvislý;*
- *každé dva vrcholy $v$ a $w$ v grafu $G$ leží na společné kružnici;*
- *graf $G$ je možné vytvořit z trojúhelníka $K_3$ pomocí postupného přidávání hran a dělení hran.*

[3] Karl Menger je dokázal již v roce 1927, tedy dříve než vznikl obor teorie grafů.

**Ore:** Má-li v grafu $G$ s $n \geq 4$ vrcholy každá dvojice nesousedních vrcholů součet stupňů alespoň $n$, je $G$ hamiltonovský.

*Uzávěrem grafu* $G$ budeme pro naše současné účely rozumět graf $cl(G)$, který dostaneme z $G$ přidáním všech hran $u$, $v$ takových, že $u$, $v$ nejsou sousední a pro něž platí $\deg(u) + \deg(v) \geq n$.

**Bondy, Chvátal:** Graf $G$ je hamiltonovský, právě když je $cl(G)$ hamiltonovský.

**12.21.** Dokažte tvrzení Bondyho a Chvátala.

**Řešení.** Zřejmě stačí dokázat, že pokud je $G$ hamiltonovský po přidání hrany $\{u, v\}$ takové, že $u$, $v$ nejsou sousední a $\deg(u) + \deg(v) \geq n$, pak je hamiltonovský i bez této hrany. Předpokládejme, že $G + \{u, v\}$ je hamiltonovský a $G$ nikoliv. Pak existuje hamiltonovská cesta v $G$ z $u$ do $v$. Pro každý vrchol sousedící s $u$ platí, že jeho předchůdce na této cestě nemůže sousedit s $v$ (jinak bychom měli hamiltonovskou kružnici v $G$). Tedy $\deg(u) + \deg(v) \leq n - 1$. □

**12.22.**

i) Dokažte, že z Bondy-Chvátalovy věty plyne Oreho a z ní Diracova.

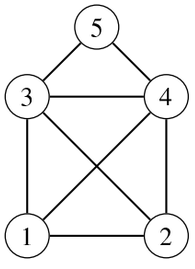
ii) Udejte příklad hamiltonovského grafu, který splňuje podmínku Oreho věty, ale ne věty Diracovy.

iii) Udejte příklad hamiltonovského grafu, jehož uzávěr není úplný graf.

**Řešení.**

i) Pokud graf $G$ splňuje předpoklady Oreho věty, pak jeho uzávěrem je úplný graf, který je zřejmě hamiltonovský a podle Bondyho a Chvátala je i původní graf hamiltonovský. Dále, pokud graf $G$ splňuje předpoklady Diracovy věty, pak zřejmě splňuje i předpoklady Oreho věty a je tedy hamiltonovský.

ii) Takovým příkladem je například




Vrchol 5 má totiž stupeň 2, což je méně než $\frac{5}{2}$. Součet stupňů libovolné dvojice (dokonce všech, nejen nesousedních) vrcholů je přitom alespoň 5.

iii) Takovým příkladem hamiltonovského grafu jsou kružnice $C_n$, $n > 4$, pro něž je $cl(C_n) = C_n$.

Důkaz. Dokážeme nejprve ekvivalenci prvních dvou tvrzení. Na jednu stranu je implikace zřejmá: Jestliže každé dva vrcholy sdílejí kružnici, pak jsou mezi nimi vždy alespoň dvě různé cesty a tedy odebráním vrcholu nemůžeme pokazit souvislost.

Opačná implikace je o něco složitější. Budeme postupovat in-



dukcí podle minimální délky cesty spojující vrcholy $v$ a $w$. Předpokládejme nejprve, že vrcholy sdílí hranu $e$, tj. minimální cesta má délku 1. Kdyby odebráním této hrany $e$ vznikly dvě komponenty, pak by nutně muselo dojít k rozpadu $G$ na alespoň dvě komponenty i po odebrání buď vrcholu $v$ nebo vrcholu $w$. Je proto i graf bez této hrany $e$ souvislý a je v něm proto cesta mezi $v$ a $w$. Spolu s hranou $e$ tato cesta vytváří kružnici.

Nechť nyní v rámci indukčního předpokladu umíme takovou sdílenou kružnici sestrojit pro všechny vrcholy spojitelné cestou délky nejvýše $k$ a uvažujme vrcholy $v$ a $w$ a je spojující nejkratší cestu

$$(v = v_0, e_1, v_1, \ldots, v_{k+1} = w)$$

délky $k + 1$. Pak $v_1$ a $w$ umíme spojit cestou o délce nejvýše $k$, a proto leží na společné kružnici. Označme si $P_1$ a $P_2$ příslušné dvě různé cesty mezi $v_1$ a $w$. Graf $G \setminus \{v_1\}$ je ale také souvislý, existuje tedy cesta $P$ z $v$ do $w$, která neprochází vrcholem $v_1$ a tato nutně musí někdy poprvé narazit na jednu z cest $P_1$ a $P_2$. Předpokládejme, že se tak stane ve vrcholu $z$ na cestě $P_1$. Pak je (uzavřená) cesta, která vznikne složením části cesty $P$ z $v$ do $z$, části cesty $P_1$ ze $z$ do $w$ a opačnou cestou k $P_2$ z $w$ do $v$ hledanou kružnicí (nakreslete si obrázek!).

Máme tedy dokázánu ekvivalenci prvních dvou podmínek. Nyní se budeme věnovat ekvivalenci první a třetí podmínky.

Je zřejmé, že dělením hrany nebo přidáním hrany ve vrcholově 2-souvislém grafu $G = (V, E)$ vlastnost 2–souvislosti nepokazíme. Jedna implikace tedy je ověřená.

Zbývá tedy dokázat, že pokud je graf 2-souvislý, pak je ho možné vytvořit z $K_3$ přidáváním a dělením hran. V $G$ jistě díky 2-souvislosti existuje kružnice, a tu je možné z $K_3$ získat dělením hran. Uvažme nyní podgraf $G' = (V', E')$ určený touto kružnicí a uvažme hranu $e = \{v, w\}$, která nepatří do $E'$, ale alespoň jeden z vrcholů do $V'$ patří. Pokud by tam patřily oba, můžeme prostě přidat ke grafu $G'$ novou hranu $e$, čímž získáme podgraf $(V', E' \cup \{e\})$ v grafu $G$ obsahující více vrcholů a hran než graf $G'$. Uvažme tedy zbývající možnost, že $v \in V'$ a $w \notin V'$. Díky 2–souvislosti grafu $G$ bude tento graf souvislý i po odebrání vrcholu $v$ a bude v něm tedy existovat nejkratší cesta $P$ spojující vrchol $w$ s některým vrcholem (označme jej $v'$) v $G'$ (mimo odebraný vrchol $v$) a neobsahující tedy žádný jiný vrchol z $V'$. Přidáním celé této cesty ke grafu $G'$ společně s hranou $e$ (což uděláme tak, že přidáme hranu $\{v, v'\}$ a nadělíme ji na potřebný počet „nových“ vrcholů a hran) dostaneme nový podgraf splňující naše předpoklady a obsahující více vrcholů a hran než právě uvažovaný graf $G'$. Po konečném počtu těchto kroků tedy z trojúhelníka $K_3$ zkonstruujeme celý graf $G$, jak je požadováno. □

**12.14. Metrika na grafech.** V posledním důkazu jsme využili

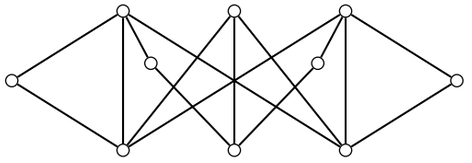


pojem „délka cesty“. Ukážeme si nyní, že takto skutečně lze matematicky vybudovat pojem vzdálenosti na grafu.

□

**Rovinné grafy.**

**12.23.** Rozhodněte, zda je graf na obrázku rovinný.



**Řešení.** Daný graf rovinný není díky Kuratowského větě (viz strana 731), protože má podgraf, který je dělením $K_{3,3}$. □

*12.24.* Rozhodněte, zda existuje graf mající skóre

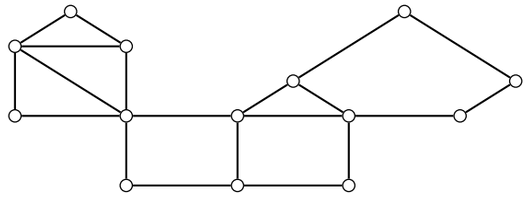
$$(6, 6, 6, 7, 7, 7, 7, 8, 8, 8).$$

Pokud ano, existuje i rovinný graf daného skóre? ○

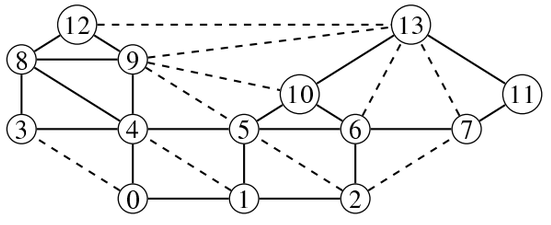
**12.25.** Kolik minimálně hran může mít šestistěn?

**Řešení.** V libovolném mnohostěnu je každá stěna ohraničena minimálně třemi hranami. Každá hrana přitom leží ve dvou stěnách. Označíme-li $s$ počet stěn a $h$ počet hran mnohostěnu dostáváme tak odhad $3s \leq 2h$ (viz také 12.26). Pro šestistěn dává tento odhad $18 \leq 2h$, neboli $h \geq 9$. Šestistěn s devíti hranami skutečně existuje, dostaneme jej například „slepením“ dvou stejně velikých pravidelných čtyřstěnů stěnou k sobě. Minimální možný počet hran šestistěnu je tedy devět. □

**12.26.** Rozhodněte, zda je daný rovinný graf maximální. Doplňte co nejvíce hran při zachování rovinnosti.



**Řešení.** Graf má 14 vrcholů a 20 hran, proto $3|V|-6-|E| = 16$. Graf tedy není maximální a přidat lze při zachování rovinnosti 16 hran.




Přidali jsme 10 (čárkovaných) hran, dalších 6 hran spojující vrcholy „vnějšího“ devítiúhelníku jsme z důvodu přehlednosti nezobrazovali. □

Na každém (neorientovaném) grafu definujeme *vzdálenost vrcholů* $v$ a $w$ jako číslo $d_G(v, w)$, které je rovno počtu hran v nejkratší možné cestě z $v$ do $w$. Pokud cesta neexistuje, píšeme $d_G(v, w) = \infty$.

Budeme v dalším uvažovat pouze souvislé grafy $G$. Pak pro takto zadanou funkci $d_G : V \times V \to \mathbb{N}$ platí obvyklé tři vlastnosti vzdálenosti (doporučujeme srovnat s úvahami v druhé části sedmé kapitoly, od odstavce 7.12 na straně 408):

- $d_G(v, w) \geq 0$ a přitom $d_G(v, w) = 0$, právě když $v = w$;
- vzdálenost je symetrická, tj. $d_G(v, w) = d_G(w, v)$;
- platí trojúhelníková nerovnost, tj. pro každou trojici vrcholů $v, w, z$ platí

$$d_G(v, z) \leq d_G(v, w) + d_G(w, z).$$

Říkáme, že $d_G$ je *metrika na grafu* $G$.

Kromě těchto tří standardních vlastností splňuje metrika na grafu evidentně ještě

- $d_G(v, w)$ má vždy nezáporné celočíselné hodnoty;
- je-li $d_G(v, w) > 1$, pak existuje nějaký vrchol $z$ různý od $v$ a $w$ takový, že $d_G(v, w) = d_G(v, z) + d_G(z, w)$.



Lze dokázat, že pro každou funkci $d_G$ s výše uvedenými pěti vlastnostmi na $V \times V$ (pro konečnou množinu $V$) je možné nadefinovat hrany $E$ tak, aby $G = (V, E)$ byl graf s metrikou $d_G$. Zkuste si ukázat jako cvičení! (Je vcelku jasné, jak zkonstruovat příslušný graf. Je třeba „jen“ dokázat, že pak skutečně bude zadaná funkce $d_G$ výše zavedenou metrikou na tomto grafu.)

**12.15. Dijkstrův algoritmus nejkratších cest.** Dá se tušit, že



nejkratší cestu v grafu, která vychází z daného vrcholu $v$ a končí v jiném vrcholu $w$ budeme umět hledat pomocí prohledávání grafu do šířky. Při tomto typu prohledávání totiž postupně diskutujeme vrcholy, do kterých se umíme dostat z výchozího vrcholu po jediné hraně, poté projdeme všechny, které mají vzdálenost nejvýše 2 atd. Na této jednoduché úvaze je založen jeden z nejpoužívanějších grafových algoritmů – tzv. *Dijkstrův algoritmus*.

Tento algoritmus hledá nejkratší cesty i v praktické podobě, kdy jednotlivé hrany $e$ jsou *ohodnoceny* velikostmi, tj. kladnými reálnými čísly $w(e)$. Kromě aplikace na hledání vzdáleností v silničních nebo jiných sítích to mohou být také výnosy či náklady, toky v sítích atd.

Vstupem algoritmu je graf $G = (V, E)$ s ohodnocením hran a počáteční vrchol $v_0$. Výstupem je ohodnocení vrcholů čísly $d_w(v)$, která udávají nejmenší možný součet ohodnocení hran podél cest z vrcholu $v_0$ do vrcholu $v$. Postup dobře funguje v orientovaných i neorientovaných grafech.

Pro konečný chod algoritmu a jeho výsledek je skutečně pod-



statné, že všechna naše ohodnocení jsou kladná – viz příklad ‖12.18‖.

Dijkstrův algoritmus vyžaduje jen drobnou modifikaci obecného prohledávání do šířky:

- U každého vrcholu $v$ budeme po celý chod algoritmu udržovat číselnou hodnotu $d(v)$, která bude horním odhadem skutečné vzdálenosti vrcholu $v$ od vrcholu $v_0$.
- Množina již zpracovaných vrcholů bude v každém okamžiku obsahovat ty vrcholy, u kterých již nejkratší cestu známe, tj. $d(v) = d_w(v)$.

*12.27.* Každé z následujících tvrzení dokažte nebo ukažte vhodný protipříklad.

i) Každý graf s méně než 9 hranami je rovinný.
ii) Graf, který není rovinný, není hamiltonovský.
iii) Graf, který není rovinný, je hamiltonovský.
iv) Graf, který není rovinný, není eulerovský (viz 12.17).
v) Graf, který není rovinný, je eulerovský.
vi) Každý hamiltonovský graf je rovinný.
vii) Žádný hamiltonovský graf není rovinný.
viii) Každý eulerovský graf je rovinný.
ix) Žádný eulerovský graf není rovinný.

○

- Do množiny aktivních (právě zpracovávaných) vrcholů $W$ zařadíme vždy právě ty vrcholy $y$ z množiny spících vrcholů $Z$, pro které je $d(y) = \min\{d(z);\ z \in Z\}$.

Předpokládáme, že graf $G$ má alespoň dva vrcholy. Formálněji lze Dijkstrův algoritmus popsat takto:

(1) *Iniciační krok:* Nastavíme hodnoty u všech $v \in V$:

$$d(v) = \begin{cases} 0 & \text{pro } v = v_0, \\ \infty & \text{pro } v \neq v_0. \end{cases}$$

Nastavíme $Z = V$, $W = \emptyset$.

(2) *Test cyklu:* Jestliže ohodnocení všech vrcholů $y \in Z$ je rovno $\infty$, algoritmus končí, v opačném případě pokračujeme dalším krokem. (Algoritmus tedy zejména končí, pokud je $Z = \emptyset$.)

(3) *Aktualizace stavu vrcholů:*
- Najdeme množinu $N$ všech vrcholů $v \in Z$, pro které $d(v)$ nabývá nejmenší možné hodnoty

$$\delta = \min\{d(y);\ y \in Z\};$$

- posledně zpracované aktivní vrcholy $W$ přesuneme do množiny zpracovaných a za nové aktivní vrcholy zvolíme $W = N$ a odebereme je ze spících, tj. množina spících bude nadále $Z \setminus N$.

(4) *Tělo hlavního cyklu:* Pro všechny hrany v množině $E_{WZ}$ všech hran vycházejících z některého aktivního vrcholu $v$ a končících ve spícím vrcholu $y$ opakujeme:
- vybereme dosud nezpracovanou hranu $e \in E_{WZ}$;
- pokud je $d(v) + w(e) < d(y)$, nahradíme $d(y)$ touto menší hodnotou.

Pokračujeme testem v kroku 2.

**12.16. Věta.** *Pro všechny vrcholy $v$ v souvislé komponentě vrcholu $v_0$ v grafu $G$ najde Dijkstrův algoritmus vzdálenosti $d_w(v)$. Vrcholy ostatních souvislých komponent zůstanou ohodnoceny $d(v) = \infty$.*

*Algoritmus lze implementovat tak, že ukončí svoji práci v čase $O(n \log n + m)$, kde $n$ je počet vrcholů a $m$ je počet hran v $G$.*

Důkaz. Napřed ukážeme správnost algoritmu, tj. budeme muset ověřit, že

- algoritmus po konečném počtu kroků skončí;
- výstup v okamžiku ukončení bude mít požadované vlastnosti.

Formulace testu cyklu zaručuje, že při každém jeho průchodu se zmenší počet spících vrcholů alespoň o jeden, protože $N$ bude vždy neprázdná. Nutně tedy algoritmus po konečném počtu kroků skončí.

Po průchodu iniciačním cyklem zjevně platí

$$d(v) \geq d_w(v) \tag{12.2}$$

pro všechny vrcholy grafu. Předpokládejme tedy, že tato nerovnost platí při vstupu do hlavního cyklu algoritmu a ověříme, že platí i po výstupu z cyklu. Skutečně pokud v kroku 4 měníme $d(y)$, pak je to proto, že jsme našli vrchol $v$ s vlastností

$$d_w(y) \leq d_w(v) + w(\{v, y\}) \leq d(v) + w(\{v, y\}) = d(y),$$

kde napravo již máme nově změněnou hodnotu.

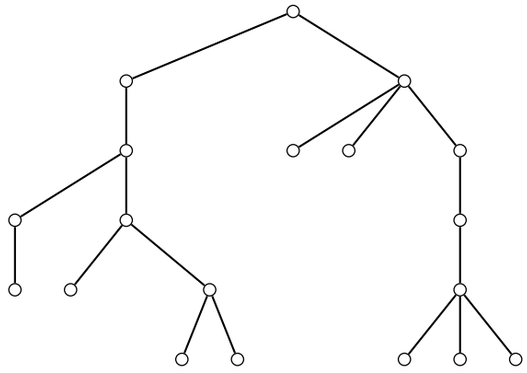
Rovnost (12.2) bude proto jistě platit i v okamžiku ukončení algoritmu a zbývá nám ověřit, že na konci algoritmu bude platit i nerovnost opačná. Za tímto účelem si promysleme, co se vlastně děje v krocích 3 a 4 v algoritmu.

**Stromy.**

**12.28.** Určete kód grafu na obrázku jako

i) pěstěného stromu,

ii) stromu.



**Řešení.**

i) Postupem popsaným v 12.22 dostaneme kód pěstěného stromu

0 0 0 0 0 1 1 0 0 1 0 0 1 0 1 1 1 1 1 0 0 1 0 1 0 0 0 0 1 0 1 0 1 1 1 1 1 1 1.

V grafu naznačený kořen je skutečně vhodným kandidátem, protože jde o jediný prvek centra tohoto stromu.

ii) Při jednoznačné konstrukci pěstěného stromu řadíme potomky lexikograficky vzestupně, proto je hledaným kódem stromu

0 0 0 0 0 0 1 0 1 0 1 1 1 1 0 1 0 1 1 0 0 0 0 0 1 0 1 1 0 1 1 0 0 0 1 1 1 1 1. □

*12.29.* Rozhodněte, zda existují stromy s následujícími kódy. V případě, že ano, potom daný strom nakreslete.

- 00011001111001,
- 0000011001001011111001010000101011111 1.

○

**Huffmanovo kódování.** Pracujeme s pěstěnými binárními stromy, kde máme navíc každou hranu *obarvenou* některým symbolem z dané výstupní abecedy $A$ (často $A = \{0, 1\}$). Kódovými slovy $C$ jsou slova nad abecedou $A$, na která převádíme symboly vstupní abecedy. Našim úkolem je reprezentovat daný text pomocí vhodných kódových slov nad výstupní abecedou.

Je snadno vidět, že je užitečné chtít, aby seznam kódových slov byl *bezprefixový* (v opačném případě může nastat problém s dekódováním).

Ke konstrukci binárních prefixových kódů (tj. nad abecedou $A = \{0, 1\}$) využijeme binárních stromů. Označíme-li hrany



Označme si $0 = d_0 < \cdots < d_k$ všechny existující různé konečné vzdálenosti $d_w(v)$ vrcholů grafu $G$ od počátečního vrcholu $v_0$. Tím máme zároveň rozdělenu množinu vrcholů grafu $G$ na disjunktní podmnožiny $V_i$ vrcholů se vzdáleností právě $d_i$. Při prvním průchodu hlavním cyklem máme $N = V_0 = \{v_0\}$, číslo $\delta$ bude právě $d_1$ a množinu spících vrcholů změníme na $V \setminus V_0$.

Předpokládejme, že by tomu takto bylo až do $j$-tého průchodu včetně, tj. při vstupu do cyklu by platilo $N = V_j$, $\delta = d_j$ a $\bigcup_{i=0}^{j} V_i = V \setminus N$. Uvažme nějaký vrchol $y \in V_{j+1}$, tj. $d_w(y) = d_{j+1} < \infty$ a existuje cesta $(v_0, e_1, v_1, \ldots, v_\ell, e_{\ell+1}, y)$ celkové délky $d_{j+1}$. Pak ovšem jistě

$$d_w(v_\ell) \leq d_{j+1} - w(\{v_\ell, y\}) < d_{j+1}. \tag{12.3}$$

Podle našeho předpokladu tedy již dříve (v některém z předchozích průchodů hlavním cyklem) byl vrchol $v_\ell$ aktivní a tedy již v tom průchodu bylo jeho ohodnocení rovno $d_w(v_\ell) = d(v_\ell) = d_i$ pro některé $i \leq j$. Proto po stávajícím průchodu hlavním cyklem bude výsledkem nastavení

$$d(y) = d_w(v_\ell) + w(\{v_\ell, y\}) = d_{j+1}$$

a toto v dalších průchodech již nikdy nebude měněno. V nerovnosti (12.2) tedy ve skutečnosti nastává po ukončení chodu algoritmu rovnost.

Naše analýza průchodu hlavním cyklem nám zároveň umožňuje odhadnout čas potřebný na chod algoritmu (tj. počet elementárních operací s grafem a dalšími objekty s ním spojenými). Je totiž vidět, že hlavním cyklem projdeme tolikrát, kolik v grafu existuje různých vzdáleností $d_i$. Každý vrchol při jeho zpracování v kroku 3 budeme uvažovat právě jednou a budeme muset přitom umět setřídit dosud spící vrcholy. To dává odhad $O(n \log n)$ na tuto část algoritmu, pokud budeme používat pro uchovávání grafu seznam hran a vrcholů obohacený o ohodnocení hran a spící vrcholy budeme uchovávat ve vhodné datové struktuře umožňující vyhledání množiny $N$ aktivních vrcholů v čase $O(\log n + |N|)$. To lze dosáhnout datovou strukturou, které se říká halda (heap). Každá hrana bude právě jednou zpracovávána v kroku 4, protože vrcholy jsou aktivní pouze při jednom průchodu cyklem. □

Všimněme si, že pro nerovnost (12.3), která byla podstatná pro analýzu algoritmu, je nutný předpoklad o nezáporných vahách všech hran.



V praktickém použití bývají přidávána různá heuristická vylepšení. Např. není nutné dopočítávat celý algoritmus, pokud nás zajímá pouze nejkratší cesta mezi dvěma vrcholy. V okamžiku, kdy totiž je vrchol vyřazován z aktivních, víme, že jeho vzdálenost je již spočtena správně.

Také není nutné na začátku algoritmus iniciovat s nekonečnou hodnotou. Samozřejmě by to při programování ani nešlo, můžeme však postupovat ještě daleko lépe než jen přiřadit dostatečně velikou konstantu. Například při počítání nejkratší cesty po silniční síti můžeme jako iniciaci volit předem známe vzdušné vzdálenosti bodů. Pak totiž známe předem odhady vzdáleností $d_w^0(v)$ vrcholů $v$ a $v_0$ takové, že pro všechny hrany $e = \{v, y\}$ platí

$$|d_w^0(v) - |d_w^0(y)| \leq w(e)$$

a tato nerovnost nám stačí pro důkaz správnosti algoritmu.

vycházející z každého uzlu 0, resp. 1, a označíme-li navíc listy stromu symboly vstupní abecedy, dostaneme prefixový kód nad $A$ pro tyto symboly zřetězením označení hran na cestě z kořene do příslušného listu.

Takto vytvořený kód je zřejmě *prefixový*. Uděláme-li tuto konstrukci navíc tak, abychom odrazili četnost symbolů vstupní abecedy v kódovaném textu, dosáhneme tak dokonce *bezztrátové komprese dat*.

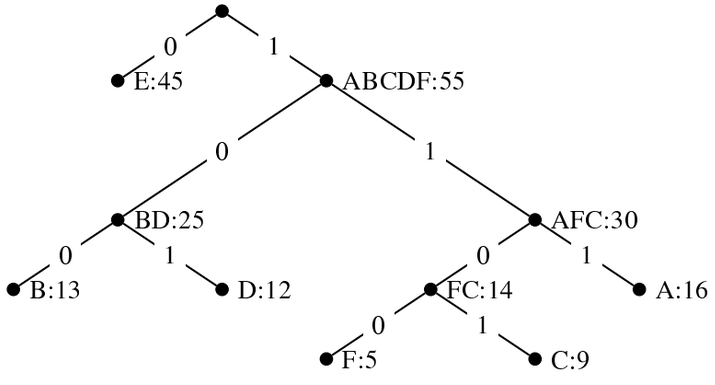
Nechť $M$ je seznam četností symbolů vstupní abecedy v textu. Algoritmus postupně zkonstruuje optimální binární strom (tzv. *minimum-weight binary tree*) a přiřazení symbolů listům.

- Vyber dvě nejmenší četnosti $w_1, w_2$ z $M$. Vyrob strom se dvěma listy označenými příslušnými symboly a kořenem označeným $w_1 + w_2$ , odeber z $M$ hodnoty $w_1, w_2$ a nahraď je hodnotou $w_1 + w_2$.
- Tento krok opakuj; pouze v případě, že vybraná hodnota z $M$ je součtem, pak nevyráběj nový list, ale „připoj“ příslušný již existující podstrom.
- Kód každého symbolu urči cestou od kořene (např. vlevo=„0“, vpravo=„1“).

**12.30.** Nalezněte Huffmanův kód pro vstupní abecedu s frekvencemi `['A':16,'B':13,'C':9,'D':12,'E':45,'F':5]`.

**Řešení.** Pokud bychom každému písmenu abecedy naivně přiřadili 3bitový kód, pak na zprávu délky 100 spotřebujeme 300 bitů.

Ukážeme, že Huffmanův kód to zvládne úsporněji. Sestrojíme strom podle algoritmu.




Dostali jsme tak kódy $A: 111, B: 100, C: 1101, D: 101, E: 0, F: 1100$ a po vynásobení délek kódů frekvencemi získáme očekávanou délku kódu stoznakové zprávy rovnou

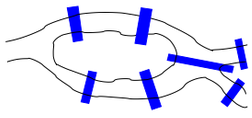
$$3 \cdot 16 + 3 \cdot 13 + 4 \cdot 9 + 3 \cdot 12 + 1 \cdot 45 + 4 \cdot 5 = 224. \qquad \square$$

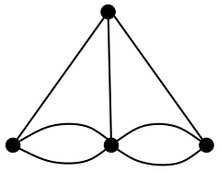
**12.17. Eulerovy sledy.** Každý si asi pamatujeme na hříčky typu „nakreslete obrázek jedním tahem“. V řeči grafů to zachytíme takto:

**Definice.** Sled, který projde všechny hrany grafu právě jednou a začíná a končí ve stejném vrcholu, se nazývá *eulerovský tah* (též *eulerovský sled*) a souvislým grafům, které takový sled připouští, říkáme *eulerovské*.



Eulerovský tah samozřejmě projde zároveň každý vrchol grafu alespoň jednou, může ale vrcholy procházet i vícekrát. Nakreslit graf jedním tahem, který začíná a končí v jednom vrcholu, tedy znamená najít eulerovský tah. Terminologie odkazuje na klasický příběh o sedmi mostech ve městě Královec (Königsberg, tj. Kaliningrad), které se měly projít na procházce každý právě jednou, a důkaz nemožnosti takové procházky pochází od Leonharda Eulera z roku 1736.





Situace je znázorněna na obrázku, kde je nalevo neumělý náčrt řeky s ostrovy a mosty, napravo odpovídající (multi)graf. Vrcholy tohoto grafu odpovídají „souvislé pevnině“, hrany mostům. Pokud by nám vadily násobné hrany mezi vrcholy (což jsme zatím formálně nepřipouštěli), stačí do hran za každý most přidat ještě jeden vrchol, tj. rozdělit hrany pomocí nových vrcholů. Kupodivu je obecné řešení takového problému dosti snadné, jak ukazuje následující věta. Samozřejmě také ukazuje, že se Euler zamýšleným způsobem procházet skutečně nemohl.

**Věta.** *Graf $G$ je eulerovský tehdy a jen tehdy, když je souvislý a všechny vrcholy v $G$ mají sudé stupně.*

Důkaz. Je-li graf eulerovský, nutně musíme při procházení všech hran každý vrchol stejněkrát opustit jako do něj vstoupit. Proto nutně musí být stupeň každého vrcholu sudý. Kdo chce důkaz této implikace vidět více formálně, může uvážit sled, který začne a skončí ve vrcholu $v_0$ a projde všechny hrany. Každý vrchol bude jedenkrát nebo vícekrát na této cestě a jeho stupeň bude roven dvojnásobku počtu výskytů.

Předpokládejme naopak, že graf $G$ má všechny vrcholy jen sudých stupňů, a uvažme nejdelší možný sled $(v_0, e_1, \ldots, v_k)$ v $G$ bez opakujících se hran. Předpokládejme na okamžik, že $v_k \neq v_0$. To znamená, že do $v_0$ vchází nebo vychází v tomto sledu jen lichý počet hran, a tedy jistě existuje nějaká hrana vycházející z $v_0$, která v tomto sledu není. To by ale znamenalo, že jej umíme prodloužit, aniž bychom opakovali hranu, což je spor. Nutně proto musí být v našem sledu $v_0 = v_k$.

Definujme nyní podgraf $G' = (V', E')$ v grafu $G$ tak, že do něj dáme právě všechny vrcholy a hrany v našem pevně zvoleném sledu. Pokud $V' \neq V$, pak díky souvislosti grafu $G$ nutně existuje hrana $e = \{v, w\}$ taková, že $v \in V'$ a $w \notin V'$. Pak ovšem můžeme náš pevně zvolený sled začít a skončit ve vrcholu $v$ a následně pokračovat hranou $e$, což je opět spor s jeho největší možnou délkou. Proto nutně $V' = V$. Zbývá tedy už jen ukázat, že také $E' = E$.

## C. Minimální kostra

**12.31.** Kolik existuje různých koster (viz 12.29) grafu $K_5$? Kolik různých jich existuje až na izomorfismus?

**Řešení.** Existují tři navzájem neizomorfní kostry (se skóre $(1,2,2,2,1)$, $(1,2,3,1,1)$, $(4,1,1,1,1)$). Příslušné třídy isomorfních grafů mají postupně $5 \cdot \binom{4}{2} \cdot 2$, $5 \cdot 4 \cdot 3$ a 5 prvků, celkem $125 = 5^3$ různých koster, což souhlasí s obecným Cayleyho vzorcem pro počet koster úplného grafu (viz 12.47). □

**12.32.** Označme vrcholy v grafu $K_6$ postupně čísly $1, 2, \ldots 6$ a každou hranu $\{i, j\}$ ohodnoťme číslem $[(i + j) \bmod 3] + 1$. Kolik existuje různých minimálních koster v tomto grafu?

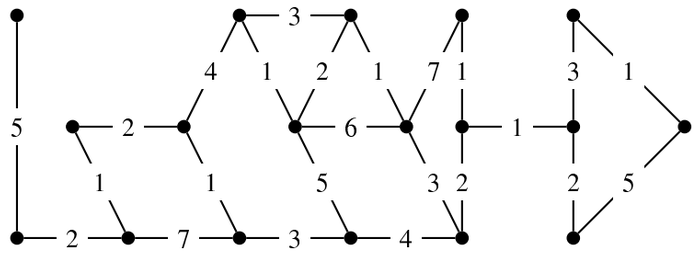
**Řešení.** Hrany s ohodnocením jedna tvoří kružnici 12451 délky čtyři a hranu 36. Jde tedy o nesouvislý podgraf daného grafu. Není tedy možné vybrat kostru daného grafu pouze z hran s ohodnocením jedna. Minimální kostra bude mít tedy součet ohodnocení hran v ní minimálně $4 \cdot 1 + 2 = 6$. Kostru s touto hodnotou skutečně můžeme vybrat. Z hran s ohodnocením 1 můžeme vypustit libovolnou hranu ze zmiňované kružnice a nezávisle přidáme nějakou hranu s ohodnocením dvě, která spojuje v podgrafu hran s ohodnocením jedna komponentu 1245 s komponentou 36. Takové hrany jsou celkem čtyři. Celkem má daný graf $4 \cdot 4 = 16$ různých minimálních koster. □

**12.33.** Najděte minimální kostru grafu na obrázku pomocí

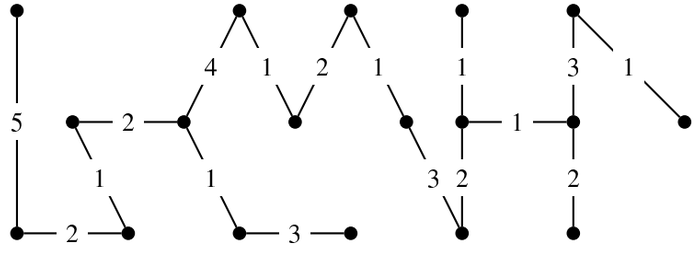
i) Kruskalova,

ii) Jarníkova (Primova) algoritmu.

Vysvětlete, proč není možné přímo použít Borůvkův algoritmus.




**Řešení.** Řešením je kostra




Předpokládejme tedy, že hrana $e = \{v, w\} \notin E'$. Opět stejně jako výše můžeme náš sled začít a skončit ve $v$ a poté pokračovat hranou $e$, což by opět byl spor. □

**Důsledek.** *Graf lze nakreslit jedním tahem, právě když má všechny stupně vrcholů sudé nebo má právě dva vrcholy lichého stupně.*

Důkaz. Nechť $G$ je graf s právě dvěma vrcholy lichého stupně. Uvažme graf $G'$, který vznikne z $G$ přidáním jednoho nového vrcholu $w$ a dvou hran, které spojují $w$ s dvěma vrcholy lichého stupně. Tento graf už bude eulerovský a eulerovský sled v $G'$ vede na požadovaný výsledek.

Naopak pokud jde graf $G$ nakreslit jedním tahem, který končí v různých vrcholech, bude nutně náš graf $G'$ eulerovský, a proto má $G$ požadované stupně vrcholů. □

Situace pro orientované grafy je velmi podobná.

**Definice.** Orientovaný graf nazveme *vyvážený*, jestliže pro každý jeho vrchol $v$ platí $\deg_+(v) = \deg_-(v)$.

**Důsledek.** *Orientovaný graf $G$ je eulerovský právě když je vyvážený a jeho symetrizace je souvislý graf (tj. graf $G$ je slabě souvislý).*

Důkaz. Analogický jako v neorientovaném případě. □

**12.18. Hamiltonovy kružnice.** Obdobný požadavek na průchod grafem, ovšem tak, abychom prošli právě jednou každým vrcholem (tj. zároveň nejvýše jednou každou hranou), vede naopak na obtížné problémy. Takový průchod grafem je realizován kružnicí, která obsahuje všechny vrcholy grafu $G$. Hovoříme o *hamiltonovských kružnicích* v grafu $G$. Graf se nazývá hamiltonovský, jestliže má hamiltonovskou kružnici. Zatímco (zdánlivě podobně složitý) problém nalezení eulerovského tahu je triviální, zjistit, zda je daný graf hamiltonovský, je **NP-úplný problém**.

Samozřejmě máme k dispozici algoritmické řešení metodou „hrubé síly“, kdy pro daný graf s $n$ vrcholy vygenerujeme všech $n!$ možných posloupností, ve kterých lze projít všech $n$ vrcholů, a pro každou z nich prověříme, zda je cestou v grafu $G$. To je pochopitelně nepoužitelný postup i pro nepříliš veliká $n$.

Jde o velice živou oblast výzkumu. Např. v roce 2010 publikoval A. Björklund algoritmus založený na náhodnostní metodě Monte Carlo, který počítá množství Hamiltonových kružnic v grafu $G$ s $n$ vrcholy v čase $O(1{,}567^n)$.[4]

**12.19. Stromy.** Často potřebujeme při řešení praktických problémů místo posilování redundancí (jako u počítačových nebo rozvodných sítí) naopak minimalizovat počet hran grafu při zachování jeho souvislosti. To je samozřejmě vždy možné, dokud je v grafu alespoň jedna kružnice.

[4] Björklund, Andreas (2010), "Determinant sums for undirected Hamiltonicity", Proc. 51st IEEE Symposium on Foundations of Computer Science (FOCS '10), pp. 173-182, arXiv:1008.0541, doi:10.1109/FOCS.2010.24.

Borůvkův algoritmus není možné použít, protože ohodnocení hran není prosté, to se dá ale v praxi celkem snadno napravit jemnými modifikacemi ohodnocení. □

*12.34.* Uvažme následující postup pro určování minimální cesty mezi dvěma vrcholy v ohodnoceném neorientovaném grafu: nejprve nalezneme minimální kostru grafu, za minimální cestu pak prohlásíme jedinou cestu spojující dva dané vrcholy v minimální kostře. Dokažte, že je tento postup správný, nebo uveďte protipříklad. ○

*12.35.* Máme dánu následující tabulku vzdáleností světových metropolí: Londýna, Mexico City, New Yorku, Paříže, Pekingu a Tokia:

$$\begin{pmatrix} & L & MC & NY & P & Pe & T \\ L & & 5558 & 3469 & 214 & 5074 & 5959 \\ MC & & & 2090 & 5725 & 7753 & 7035 \\ NY & & & & 3636 & 6844 & 6757 \\ P & & & & & 5120 & 6053 \\ Pe & & & & & & 1307 \end{pmatrix}$$

Jaká je nejmenší délka kabelu, kterým je možné propojit tato města? (předpokládáme, že délka kabelu potřebného k propojení daných dvou měst je právě vzdálenost v tabulce). ○

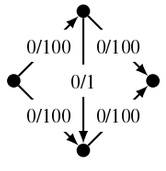
*12.36.* Najděte minimální kostru pomocí maticové verze Jarník-Primova algoritmu v grafu zadaném maticí ohodnocení hran

$$\begin{pmatrix} - & 12 & - & 16 & - & - & - & 13 \\ 12 & - & 16 & - & - & - & 14 & - \\ - & 16 & - & 12 & - & 14 & - & - \\ 16 & - & 12 & - & 13 & - & - & - \\ - & - & - & 13 & - & 14 & - & 15 \\ - & - & 14 & - & 14 & - & 15 & - \\ - & 14 & - & - & - & 15 & - & 14 \\ 13 & - & - & - & 15 & - & 14 & - \end{pmatrix}$$

○

## D. Toky v sítích

**12.37. Příklad špatného chování Ford-Fulkersonova algoritmu.** Ford-Fulkersonův algoritmus má složitost v nejhorším případě $O(E \cdot |f|)$, kde $|f|$ je hodnota maximálního toku. Na síti




si ukážeme jeho nevhodné chování, které je dáno tím, že tento algoritmus prohledává do hloubky (tučněji jsou znázorňovány hrany, podél nichž tok sytíme).

### Lesy, stromy, listy

Souvislý graf, ve kterém není žádná kružnice, se nazývá *strom*. Graf neobsahující kružnice nazýváme *les* (nepožadujeme přitom souvislost grafu). Můžeme tedy formulovat dobře zapamatovatelnou matematickou větu: „Strom je souvislý les.“[5]

Obecně v grafech nazýváme vrcholy stupně jedna *listy* (případně také *koncové vrcholy*).

Následující lemma ukazuje, že každý strom lze vybudovat postupně z jediného vrcholu přidáváním listů:

**Lemma.** *Každý strom s alespoň dvěma vrcholy obsahuje alespoň dva listy.*

*Pro libovolný graf $G$ s listem $v$ jsou následující tvrzení ekvivalentní:*

- *$G$ je strom;*
- *$G \setminus v$ je strom.*

Důkaz. Dokažme nejprve první tvrzení. Opět použijeme cestu nejdelší možné délky v grafu $G$. Nechť $P = (v_0, \ldots, v_k)$ je taková cesta. Pokud by $v_0$ nebyl list, pak by z něj vedla hrana $e$ s druhým koncovým vrcholem $v$, který nemůže být vrcholem v $P$, protože to bychom získali kružnici. Pak by ale bylo možné prodloužit $P$ o tuto hranu, což také nejde. Ze sporu tedy plyne, že $v_0$ je list a totéž platí o $v_k$.

Předpokládejme nyní, že $v$ je list stromu $G$. Uvážíme-li libovolné dva jiné vrcholy $w$, $z$ v grafu $G$, nutně mezi nimi existuje cesta a žádný vrchol uvnitř této cesty nemůže mít stupeň jedna. Proto tato cesta zůstane i v $G \setminus v$ a dokázali jsme, že po odebrání $v$ zůstane graf souvislý. Samozřejmě v něm nemůže být kružnice, když ze stromu vznikl odebráním vrcholu.

Je-li naopak $G \setminus v$ strom, nemůžeme přidání vrcholu stupně 1 vytvořit kružnici a také souvislost výsledného grafu je zřejmá. □

Ve skutečnosti lze stromy popsat mnoha ekvivalentními a prakticky užitečnými vlastnostmi. Některé z nich jsou v následující větě:

**12.20. Věta.** *Pro každý graf $G = (V, E)$ jsou následující podmínky ekvivalentní:*

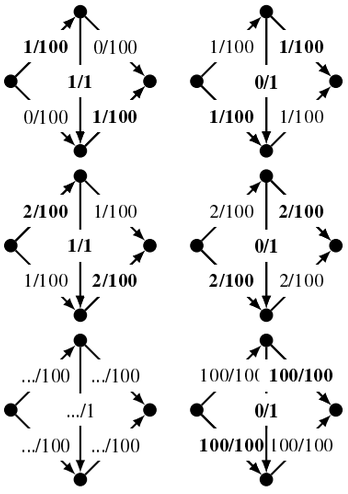
*(1) $G$ je strom.*
*(2) Pro každé dva vrcholy $v$, $w$ grafu $G$ existuje právě jedna cesta z vrcholu $v$ do $w$.*
*(3) Graf $G$ je souvislý, ale vyjmutím libovolné hrany vznikne nesouvislý graf.*
*(4) Graf $G$ neobsahuje kružnici, avšak každým přidáním hrany do grafu $G$ kružnice vznikne.*
*(5) $G$ je souvislý graf a mezi velikostí množin jeho vrcholů a hran platí vztah*

$$|V| = |E| + 1.$$

Důkaz. Větu bylo ve skutečnosti obtížnější zformulovat než dokázat. Ukážeme nejprve, že pro stromy platí vlastnosti 2–5. Podle předchozího lemmatu má každý strom o alespoň dvou vrcholech list $v$ a jeho odebráním dostaneme opět strom. Stačí tedy dokázat, že platí-li 2–5 pro nějaký strom, platí také po přidání nového listu. To je ale vesměs zřejmé.

[5] Obdobně: pařezy nelze považovat za stromy, protože obsahují kružnice.

**Řešení.** Postupujeme striktně prohledáváním do hloubky (přičemž vrcholy prozkoumáváme v pořadí nejprve zleva doprava a poté shora dolů):




Vidíme, že k nalezení maximálního toku jsme potřebovali 200 průchodů hledáním nenasycené cesty. □

**12.38.** Určete hodnotu maximálního toku a najděte minimální řez v síti dané maticí kapacit $A$, kde vrchol 1 je zdroj a vrchol 8 stok.

$$A = \begin{pmatrix} - & 16 & 24 & 12 & - & - & - & - \\ - & - & - & - & 30 & - & - & - \\ - & - & - & - & 9 & 6 & 12 & - \\ - & - & - & - & - & - & 21 & - \\ - & - & - & - & - & 9 & - & 15 \\ - & - & - & - & - & - & - & 9 \\ - & - & - & - & - & - & - & 18 \\ - & - & - & - & - & - & - & - \end{pmatrix}$$

**Řešení.** Postupně nacházíme zlepšující polocesty:

1–2–5–8 s rezervou 15.

1–2–5–6–8 s rezervou 1.

1–3–5–6–8 s rezervou 8.

1–4–7–8 s rezervou 12.

1–3–7–8 s rezervou 6.

Celkový nalezený tok má hodnotu 42. Že je opravdu maximální, vidíme z toho, že máme řez tvořený hranami (5, 8), (6, 8) a (7, 8) velikosti rovněž 42 (jedná se tedy o minimální řez). □

**12.39.** Na obrázku je uveden tok v dané síti (čísla $f/c$ udávají současný tok a kapacitu dané hrany). Zjistěte, je-li uvedený tok maximální, pokud ano, své tvrzení zdůvodněte. Pokud maximálním tokem není, maximální tok najděte a svůj postup podrobně popište. Uveďte některý minimální řez v dané síti.

Pro důkazy opačných implikací opět nemusíme dělat mnoho. V případě vlastností 2 a 3 pracujeme se souvislým grafem a přímo jejich formulace vylučují existenci kružnice. V případě čtvrté vlastnosti naopak stačí ověřit souvislost $G$. Libovolné dva vrcholy $v$ a $w$ v $G$ jsou ovšem buď spojeny hranou nebo přidáním této hrany vznikne kružnice, tj. i bez ní existuje mezi nimi cesta.

Poslední implikaci zvládneme indukcí vzhledem k počtu vrcholů. Předpokládejme, že souvislé grafy o $n$ vrcholech a $n-1$ hranách jsou stromy. Graf o $n+1$ vrcholech a $n$ hranách má celkový součet stupňů vrcholů $2n$ a tedy musí obsahovat alespoň jeden list. Pak ovšem díky indukčnímu předpokladu tento graf vznikl přidáním listu ke stromu, a je tedy také stromem. □

**12.21. Kořenové stromy, binární stromy a haldy.** Stromy využíváme pro organizaci dat tak, abychom v datech uměli buď rychle vyhledávat nebo v nich udržovat pořádek, nejčastěji obojí.



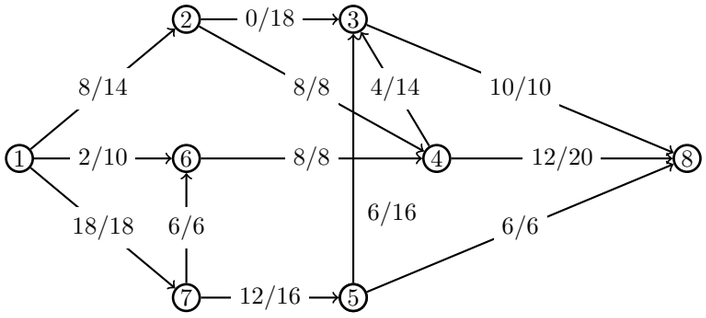
Protože ve stromu není žádná kružnice, volba jednoho vrcholu $v_r$ zadává orientaci všech hran. Skutečně do každého vrcholu vede z $v_r$ právě jedna cesta a orientaci hran bereme podél ní. Přitom není možné, že by pro různé cílové vrcholy probíhaly příslušné cesty jednu hranu v různých směrech – to by opět vedlo na kružnici.

Situace se tedy po výběru jednoho vrcholu začíná více podobat skutečnému stromu v přírodě – jeden jeho vrchol je výjimečný tím, že roste ze země. Stromy s jedním vybraným „počátečním" vrcholem nazýváme *kořenové stromy*, význačný vrchol $v_r$ pak *kořen stromu*.

V kořenovém stromu je dobře definován pojem *následník* a *předchůdce* vrcholu takto: vrchol $w$ je následník $v$ a naopak $v$ je předchůdce $w$ právě tehdy, když existuje cesta z kořene stromu do $w$, která prochází $v$ a $v \neq w$. *Přímý následník* a *přímý předchůdce* vrcholu jsou pak následníci a předchůdci přímo spojení hranou. Často o nich mluvíme také jako o *synech* a *otcích* (patrně v narážce na genealogické stromy).

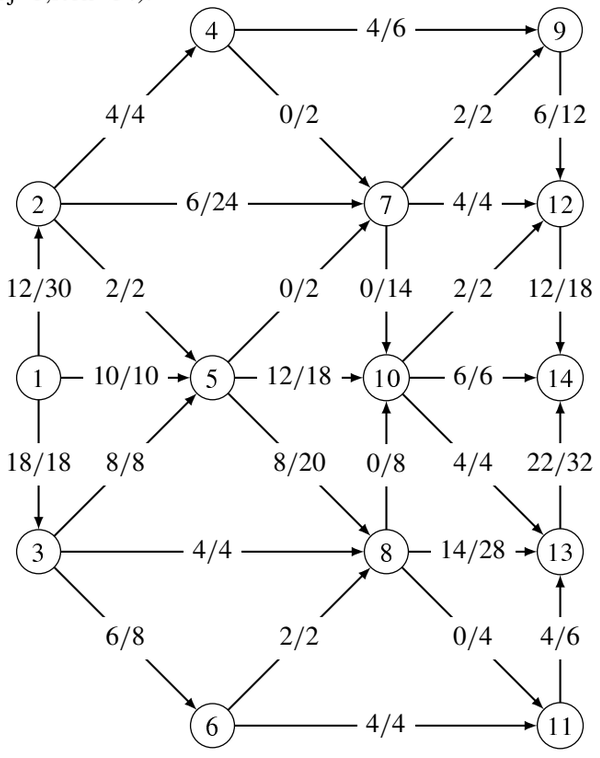
K vyhledávání se nejčastěji používají tzv. *binární stromy*, které jsou speciálním případem kořenového stromu, kdy každý otec má nejvýše dva následníky (někdy se ale pod stejným označením binární strom předpokládá, že všechny vrcholy kromě listů mají právě dva následníky). Pokud máme s vrcholy spojeny klíče v nějaké úplně uspořádané množině (např. reálná čísla), hledání vrcholu s daným klíčem je realizováno jako hledání cesty od kořene stromu a v každém vrcholu se podle velikosti rozhodujeme, do kterého ze synů budeme pokračovat (resp. zastavíme hledání, pokud jsme již v hledaném vrcholu). Abychom mohli tuto cestu jednoznačně krok po kroku určovat, požadujeme, aby jeden syn společně se všemi jeho následníky měli menší klíče než druhý syn a všichni jeho následníci.

Pro efektivní vyhledávání se snažíme o tzv. *vyvážené binární stromy*, ve kterých se délky cest z kořene do listů liší maximálně o jedničku. Nejdále od vyváženého stromu na $n$ vrcholech je tedy cesta $P_n$ (která formálně může být považována za binární strom), zatímco dokonale vyvážený strom, kde kromě listů má každý otec právě dva syny, je možné sestrojit pouze pro hodnoty $n = 2^k - 1$, $k = 1, 2, \ldots$. Ve vyvážených stromech dohledání vrcholu podle klíče bude vždy vyžadovat pouze $O(\log_2 n)$ kroků. Hovoříme v této souvislosti také často o *binárních vyhledávacích stromech*. Jako cvičení si rozvažte, jak lze účinně vykonávat základní operace




**Řešení.** V síti existuje zlepšující (polo)cesta 1–2–3–4–8 s rezervou 4, po jejím nasycení dostaneme tok velikosti 32. Protože máme řez téže velikosti (3, 8), (5, 8), (2, 4), (6, 4), našli jsme maximální tok. □

**12.40.** Nalezněte maximální tok a minimální řez v síti na obrázku (zdroj=1,stok=14).




**Řešení.** Cesty sytíme v pořadí

$$1 \xrightarrow{18} 2 \xrightarrow{18} 7 \xrightarrow{14} 10 \xleftarrow{12} 5 \xrightarrow{12} 8 \xrightarrow{4} 11 \xrightarrow{2} 13 \xrightarrow{10} 14 \qquad \text{r.2}$$

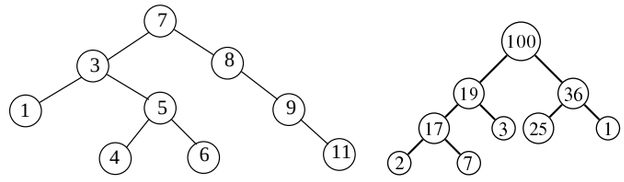
$$1 \xrightarrow{16} 2 \xrightarrow{16} 7 \xrightarrow{12} 10 \xleftarrow{10} 5 \xrightarrow{10} 8 \xrightarrow{14} 13 \xrightarrow{8} 14 \qquad \text{r.8}$$

Našli jsme tedy tok velikosti 50, který je maximální, protože neexistuje další rezervní cesta, a prostřednictvím dosažitelných vrcholů najdeme rovněž řez kapacity 50, ten tvoří hrany

[2, 4] : 4, [7, 9] : 2, [7, 12] : 4, [10, 12] : 2, [10, 14] : 6, [13, 14] : 32. □

s grafy (přidávání a odebírání vrcholů se zadanými klíči včetně vyvážení) nad binárními vyhledávacími stromy.

Mimořádně užitečným příkladem využití struktury binárních stromů je datová struktura halda. Jde opět o vyvážené binární stromy s vrcholy opatřenými klíči a požadujeme, aby podél všech cest od kořene k listům ve stromu klíče klesaly (tzv. maximální halda) nebo naopak stoupaly (tzv. minimální halda). Díky tomuto uspořádání umíme v konstantním čase odebírat z haldy podmnožiny buď maximálních nebo minimálních prvků a skutečné náklady na takovou operaci spočívají v obnovení struktury haldy po odebrání kořene. Jako cvičení si ukažte, že je to možné zvládnout v logaritmickém čase.




Na obrázku nalevo je binární vyhledávací strom, napravo je příklad maximální haldy.

**12.22. Izomorfismy stromů.** Stromům, jejich různým variantám a použití je věnována obsáhlá literatura. My se zde už pouze na chvíli zamyslíme nad (v obecnosti obtížným) problémem hledání izomorfismu grafů pro speciální třídu stromů. Budeme postupovat tak, že napřed zesílíme strukturu, kterou mají naše izomorfismy zachovávat a nakonec ukážeme, že postup je použitelný i pro úplně obecné stromy.



Pro přehled nad strukturou kořenových stromů je kromě vztahů otec–syn ještě užitečné mít syny uspořádány v pořadí (třeba v představě odleva doprava nebo podle postupného růstu atd.). Hovoříme o *pěstěných stromech* $T = (V, E, v_r, \nu)$, kde $\nu$ je částečné uspořádání na hranách takové, že srovnatelné jsou vždy právě hrany směřující od jednoho otce k synům.

Homomorfismem kořenových stromů $T = (V, E, v_r)$ a $T' = (V', E', v'_r)$ rozumíme takový morfismus grafů $\varphi : T \to T'$, který převádí $v_r$ na $v'_r$. Obdobně pro izomorfismy. Pro pěstěné stromy navíc požadujeme, aby zobrazení hran zachovávalo částečná uspořádání $\nu$ a $\nu'$.

Pro pěstěné stromy $T = (V, E, v_r, \nu)$ zavedeme jejich (jak uvidíme) jednoznačný popis pomocí slov z nul a jedniček. Obrazně si můžeme představit, že strom kreslíme a každý přírůstek naznačíme dvěma tahy, které si označíme 0 (dolů) a 1 (nahoru). Začneme od listů, kterým takto všem přiřadíme slovo 01. Celý strom pak budeme popisovat zřetězováním částí slov tak, že máli otec $v$ syny uspořádány jako posloupnost $v_1, \ldots, v_\ell$, a jsou-li již jednotliví synové označeni slovy $W_1, \ldots, W_\ell$, pak pro otce použijeme slovo

$$0W_1 \ldots W_\ell 1.$$

Strom na levém obrázku výše tedy zapíšeme postupně takto (přidáváme postupně vrcholy podle vzdálenosti od kořene, syny máme uspořádány zleva doprava):

$$01,\ 01,\ 01 \mapsto 01,\ 001011,\ 0011 \mapsto$$
$$\mapsto 0010010111,\ 000111 \mapsto 000100101110001111.$$

Hovoříme o *kódu pěstěného stromu*. Ověřte si, že skutečně kreslením cest dolů a nahoru (třeba si můžeme představit, že dolů

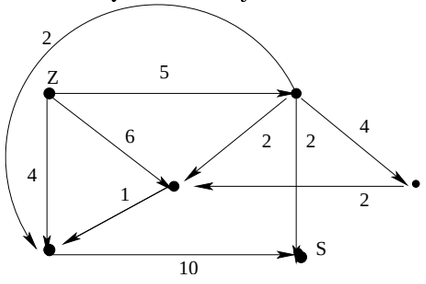
*12.41.* Pomocí Ford-Fulkersonova algoritmu (prohledávání do hloubky, vrcholy volte vzestupně podle čísel) nalezněte maximální tok v síti na množině vrcholů $\{1, 2, \ldots, 9\}$ se zdrojem 1 a stokem 9. Nalezněte minimální řez v této síti. Jednotlivé kroky svého postupu podrobně popište. Hrany $e \in E$ , dolní omezení, resp. horní omezení na tok danou hranou ($d(e)$, resp. $h(e)$) a současný tok na dané hraně $f(e)$ jsou uvedeny v tabulce:

| $e$ | $d(e)$ | $h(e)$ | $f(e)$ |
|---|---|---|---|
| (1,2) | 0 | 6 | 0 |
| (1,3) | 0 | 6 | 0 |
| (1,6) | 0 | 4 | 0 |
| (2,3) | 0 | 2 | 0 |
| (2,4) | 0 | 3 | 0 |
| (3,4) | 0 | 4 | 0 |
| (3,5) | 0 | 4 | 0 |
| (4,5) | 3 | 5 | 4 |
| (4,8) | 0 | 3 | 0 |

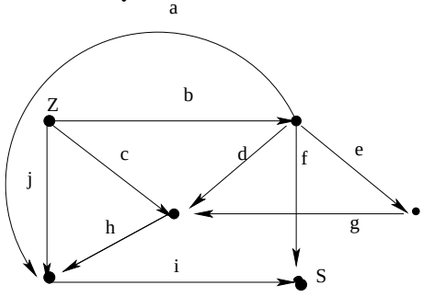
| $e$ | $d(e)$ | $h(e)$ | $f(e)$ |
|---|---|---|---|
| (5,1) | 0 | 3 | 0 |
| (5,6) | 0 | 6 | 0 |
| (5,7) | 0 | 5 | 4 |
| (5,8) | 0 | 5 | 0 |
| (6,9) | 0 | 5 | 0 |
| (7,4) | 1 | 6 | 4 |
| (7,9) | 0 | 3 | 0 |
| (8,9) | 0 | 9 | 0 |

○

**12.42.** *Řezem* v síti $(V, E, z, s, w)$ můžeme také rozumět množinu hran $C \subset S$ takovou, že v síti $(V, E \setminus C, z, s, w)$ neexistuje žádná cesta ze zdroje $z$ do stoku (cíle, spotřebiče) $s$, ale pokud z C odebereme libovolnou hranu $e$, tak už nová množina tuto vlastnost mít nebude, tedy v $(V, E \setminus C \cup e, z, s, w)$ existuje cesta ze $z$ do $s$. Určete všechny tyto řezy (a jejich hodnoty) v následující síti:




**Řešení.** Označíme-li hrany dle obrázku




pak jsou řezy následující: {f,i},{f,h,j,a},{f,j,c,a,d,e},{f,j,c,a,d,g}, {b,j,c},{b,j,h},{b,i}. Jejich kapacity jsou pak postupně 12, 9, 20, 18, 15, 10, 15. □

*12.43.* Najděte maximální tok v síti z předchozího příkladu. ○

malujeme levý obrubník cesty a nahoru pravý) získáme skutečně původní strom s jednou hranou směřující shora do kořene navíc.

**Věta.** *Dva pěstěné stromy jsou izomorfní, právě když mají přiřazen stejný kód.*

Důkaz. Z konstrukce je zřejmé, že izomorfní stromy budou mít stejný kód, zbývá tedy pouze dokázat, že různé kódy vedou na neizomorfní stromy.

Dokážeme to indukcí podle délky kódu (tj. počtu nul a jedniček). Ten je roven dvojnásobku počtu hran zvýšenému o jedničku, tj. dvojnásobku počtu vrcholů, jde tedy vlastně o indukci vzhledem k počtu vrcholů stromu $T$. Nejkratší možný kód odpovídá nejmenšímu stromu s jedním vrcholem. Předpokládejme, že věta platí pro stromy o nejvýše $n$ vrcholech, tj. pro kódy o délce nejvýše $k = 2n$, a uvažme kód tvaru $0W1$, kde $W$ je slovo o délce $2n$. Jistě je ve $W$ jednoznačně určena nejmenší levá část $W_1$, která obsahuje stejně nul a jedniček (při kreslení stromu to znamená první okamžik, kdy se vrátíme do kořenového vrcholu stromu odpovídajícího $0W1$). Stejně najdeme $W_2$ jako další úsek obsahující stejně nul a jedniček atd., až celé slovo $W$ vyjádříme jako $W = W_1 W_2 \ldots W_\ell$. Podle indukčního předpokladu odpovídají všem kódům $W_i$ jednoznačně pěstěné stromy (až na izomorfismy), a pořadí jejich kořenů, jakožto synů kořenu našeho stromu $T$, je dáno jednoznačně pořadím v kódu. Nutně proto je i pěstěný strom $T$ jednoznačně určený kódem $0W1$ až na izomorfismus. □



Nyní můžeme docela snadno využít klasifikaci pěstěných stromů pomocí kódů k popisu všech stromů. U kořenových stromů potřebujeme určit pořadí jejich synů jednoznačně až na izomorfismus. Na pořadí synů ovšem nezáleží právě tehdy, když jsou podgrafy určené jejich následníky izomorfní.

Můžeme proto využít obdobu (v jistém smyslu rekurzivní) konstrukce kódu pro pěstěné stromy a postupovat obdobně s využitím lexikografického uspořádání synů podle jejich kódů. Tzn. že kód $W_1 > W_2$, jestliže buď ve $W_1$ narazíme při čtení zleva dříve na jedničku než ve $W_2$ nebo je $W_2$ počátečním úsekem slova $W_1$. Kořenový strom budeme tedy popisovat zřetězováním částí slov tak, že má-li otec $v$ syny již označeny kódy $W_1, \ldots, W_\ell$, pak pro otce použijeme slovo

$$0W_1 \ldots W_\ell 1,$$

kde pořadí $W_1, \ldots, W_\ell$ je zvoleno tak, aby $W_1 \leq W_2 \leq \cdots \leq W_\ell$.

Pokud není určen kořen ve stromě, můžeme se jej pokusit určit tak, aby byl „přibližně uprostřed stromu“. To lze realizovat tak, že všechny jednotlivé vrcholy stromu označíme hodnotou tzv. *výstřednosti* (též *excentricity*). Definujeme výstřednost $\mathrm{ex}_T(v)$ vrcholu $v$ v grafu $T$ jako největší možnou vzdálenost z $v$ do nějakého vrcholu $w$ v $T$, kterou lze dosáhnout. Tento pojem má smysl pro všechny grafy, u stromu ale díky nepřítomnosti kružnic platí, že minimální hodnoty excentricity vždy dosahuje buď právě jeden vrchol nebo právě dva vrcholy.

**Lemma.** *Buď $C(T)$ množina vrcholů stromu $T$, jejichž výstřednost nabývá minimální hodnoty ($C(T)$ se nazývá střed/centrum grafu, minimální hodnota pak poloměr grafu). Pak $C(T)$ má jeden vrchol, nebo dva vrcholy spojené hranou v $T$.*

Další příklady na hledání maximálních toků a minimálních řezů naleznete na straně 757.

### E. Klasická pravděpodobnost a kombinatorika

V této části si zopakujeme postupy, které jsme se naučili již v první kapitole.

**12.44.** Hodíme $n$ kostkami. Jaká je pravděpodobnost, že mezi čísly, která padnou, nebudou hodnoty 1, 3 a 6?

**Řešení.** Úlohu můžeme přeformulovat tak, že $n$-krát po sobě hodíme 1 kostkou. Pravděpodobnost, že při prvním hodu nepadne 1, 3 nebo 6, je $1/2$. Pravděpodobnost, že při prvním a druhém hodu nepadne 1, 3 ani 6, je zjevně $1/4$ (výsledek prvního hodu neovlivňuje výsledek druhého). Vzhledem k tomu, že jev určený výsledkem nějakého hodu a jakýkoli jev určený výsledkem jiného hodu jsou vždy (stochasticky) nezávislé, hledaná pravděpodobnost je $1/2^n$. □

**12.45.** Z deseti karet, z nichž právě jedna je eso, namátkou vybereme kartu a vrátíme ji zpět. Kolikrát takový výběr musíme provést, aby pravděpodobnost, že aspoň jednou vybereme eso, byla větší než 0,9?

**Řešení.** Označme $A_i$ jev „při $i$-tém výběru bylo vytaženo eso“. Jednotlivé jevy $A_i$ jsou (stochasticky) nezávislé, proto víme, že

$$P\left(\bigcup_{i=1}^{n} A_i\right) = 1 - (1 - P(A_1)) \cdot (1 - P(A_2)) \cdots (1 - P(A_n))$$

pro každé $n \in \mathbb{N}$. Připomeňme, že hledáme $n \in \mathbb{N}$ takové, aby platilo

$$P\left(\bigcup_{i=1}^{n} A_i\right) = 1 - (1 - P(A_1)) \cdot (1 - P(A_2)) \cdots (1 - P(A_n)) > 0{,}9.$$

Zřejmě je $P(A_i) = 1/10$ pro libovolné $i \in \mathbb{N}$. Proto stačí vyřešit nerovnici

$$1 - \left(\tfrac{9}{10}\right)^n > 0{,}9,$$

ze které lze vyjádřit

$$n > \frac{\log_a 0{,}1}{\log_a 0{,}9}, \quad \text{kde } a > 1.$$

Vyčíslením potom zjistíme, že daný pokus musíme provést alespoň dvaadvacetkrát. □

**12.46.** Z balíčku 32 karet náhodně vybereme šestkrát po sobě po jedné kartě, a to bez vracení. Spočtěte pravděpodobnost, že první král bude vybrán až při šestém výběru.

**Řešení.** Podle věty o násobení pravděpodobností je výsledek

$$\tfrac{28}{32} \cdot \tfrac{27}{31} \cdot \tfrac{26}{30} \cdot \tfrac{25}{29} \cdot \tfrac{24}{28} \cdot \tfrac{4}{27} \doteq 0{,}0723.$$ □

Důkaz. Snadno indukcí s využitím triviálního faktu, že nejvzdálenějším vrcholem od každého vrcholu $v$ je nutně list. Centrum $T$ tedy splývá s centrem stromu $T'$, který vznikne z $T$ vypuštěním listů a příslušných hran. □

Nyní tedy můžeme přiřadit jednoznačný kód, až na izomorfismus, i každému stromu. Pokud je v centru $T$ jediný vrchol, použijeme jej jako kořen, v opačném případě vytvoříme stejným způsobem kód pro dva stromy vzniklé z $T$ odebráním hrany (bez vrcholů) spojující vrcholy centra, tyto kódy lexikograficky porovnáme a za kód stromu $T$ prohlásíme kód kořenového stromu $(T, x)$, kde $x$ je ten z vrcholů, jehož komponenta měla lexikograficky menší kód.

**Důsledek.** *Dva stromy $T$ a $T'$ jsou izomorfní, právě když mají společný kód.*

Z uvedených úvah lze snadno nahlédnout, že algoritmus na testování izomorfismu stromů lze implementovat v lineárním čase vzhledem k počtu vrcholů.

Stromy jsou velice speciální třída grafů a většinou je používáme v různých podobách s dodatečnými požadavky. Vrátíme se k nim později v souvislosti s praktickými aplikacemi. Předtím se ještě zastavíme u jiné třídy mimořádně užitečných grafů.

**12.23. Rovinné grafy.** Velice často se setkáváme s grafy, které

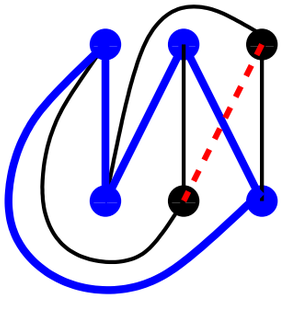


jsou nakresleny v rovině tak, že se jejich hrany „neprotínají“. To znamená, že každý vrchol grafu je ztotožněn s nějakým bodem v rovině a hrany mezi vrcholy $v$ a $w$ odpovídají spojitým křivkám $c : [0, 1] \to \mathbb{R}^2$ spojujícím vrcholy $c(0) = v$ a $c(1) = w$. Navíc ještě předpokládáme, že se jednotlivé dvojice hran protínají nejvýše v koncových vrcholech. Hovoříme o *rovinném grafu* $G$.

Otázka, jestli daný graf připouští realizaci jako rovinný graf, vyvstává velice často v aplikacích. Jednoduchý příklad je následující:

Tři dodavatelé vody, elektřiny a plynu mají každý své jedno přípojné místo v blízkosti tří v řadě stojících rodinných domků. Všichni dodavatelé je chtějí všechny napojit tak, aby se jejich sítě nekřížily (třeba se jim nechce kopat příliš hluboko . . . ). Je to možné zvládnout? Odpověď zní: „není“.

V tomto případě se to zdá být jasné. Jde o úplný bipartitní graf $K_{3,3}$, kde tři vrcholy představují přípojná místa, další tři pak domky. Hrany jsou linie sítí. Všechny hrany umíme zvládnout, jedna poslední ale už nejde, viz obrázek, na kterém neumíme čárkovanou hranu nakreslit bez křížení:



Pro skutečný důkaz ovšem potřebujeme skutečné matematické nástroje. V tomto případě nebudeme úplnou diskusi provádět, alespoň ji ale naznačíme.

**12.47.** Mějme balíček 32 karet. Vytáhneme-li dvakrát po jedné kartě, určete pravděpodobnost, že druhá tažená karta bude eso, když první kartu vrátíme, a také tehdy, když ji do balíčku nevrátíme (druhou kartu potom vybíráme z balíčku 31 karet).

**Řešení.** Pokud kartu do balíčku vrátíme, zjevně opakujeme pokus, který má 32 možných (stejně pravděpodobných) výsledků, přičemž právě 4 z nich vyhovují námi uvažovanému jevu. Vidíme, že v tomto případě je hledaná pravděpodobnost 1/8. Ve druhém případě, kdy první kartu do balíčku nevrátíme, je ovšem hledaná pravděpodobnost stejná. Postačuje např. uvážit, že při vytažení postupně všech karet je pravděpodobnost vytažení esa jako první karty totožná s pravděpodobností, že druhá vytažená karta bude eso. Pochopitelně bylo možné využít toho, že máme zavedenu podmíněnou pravděpodobnost. Tak bychom mohli obdržet

$$\frac{4}{32}\cdot\frac{3}{31}+\frac{28}{32}\cdot\frac{4}{31}=\frac{1}{8}.$$ □

*12.48.* **Kombinatorické identity.** Kombinatorickou úvahou (zejména nikoliv indukcí) si odvoďte následující důležité kombinatorické vztahy:

Aritmetická řada
$$\sum_{k=0}^{n} k=\frac{n(n+1)}{2}=\binom{n+1}{2}$$

Geometrická řada
$$\sum_{k=0}^{n} x^k=\frac{x^{n+1}-1}{x-1}$$

Binomická věta
$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$$

Horní binomická řada[1]
$$\sum_{k=0}^{n}\binom{k}{m}=\binom{n+1}{m+1}$$

Vandermondova konvoluce
$$\binom{m+n}{r}=\sum_{k=0}^{r}\binom{m}{k}\binom{n}{r-k}.$$

○

**12.49. Poker varianty Texas hold'em.** Nyní spočítejme několik jednoduchých úloh týkajících se populární karetní hry Texas hold'em, jejíž pravidla zde nebudeme uvádět (pokud je čtenář nezná, snadno je dohledá na internetu). Jaká je pravděpodobnost, že:

i) Jako startovní kombinaci dostanu dvojici stejných symbolů?
ii) Ve své startovní dvojici karet budu mít eso?
iii) Na konci budu mít jednu z šesti nejlepších kombinací karet?
iv) Vyhraji, pokud držím v ruce eso a trojku (libovolné barvy), na flopu je eso a dvě dvojky a na turnu je třetí dvojka a

[1] Též hokejková identita.



Můžeme se opřít o docela pracně dokazatelný topologický výsledek (tzv. *Jordanova věta*), že každá spojitá uzavřená křivka v rovině, která sama sebe neprotíná (tj. „pokřivená kružnice"), rozděluje rovinu na dvě části. Jinými slovy, každá jiná spojitá křivka, spojující jeden bod uvnitř takové křivky a jeden vně, musí nutně naši křivku protínat. Poznamenejme, že pokud hrany realizujeme po částech lineárními křivkami (tj. každá hrana je dána složením na sebe navazujících konečně mnoha úseček), pak je důkaz Jordanovy věty vcelku snadný.

Protože jsou v grafu $K_{3,3}$ jednotlivé vrcholy v každé z trojic vrcholů nespojených hranami (tj. v každé paritě) stejné až na volbu pořadí, můžeme naši tlustší šedou kružnici považovat za obecný případ kružnice se čtyřmi body a diskutovat umístění zbylých dvou vrcholů. Aby byl graf rovinný, musely by být oba buď uvnitř naší kružnice nebo vně. Obě možnosti jsou opět rovnocenné, nechť jsou tedy uvnitř. Nyní diskutujme jejich polohu vůči vhodné kružnici se dvěma šedými silnějšími a dvěma černými tenkými hranami (tj. přes tři šedé a jeden černý vrchol) a vůči ní diskutujme pozici zbývajícího černého vrcholu. Dojdeme k nemožnosti umístit poslední hranu bez křížení.

Zcela obdobně lze ukázat, že úplný graf $K_5$ také není rovinný (viz též odstavec 12.26). Obecně se dá dokázat silná *Kuratowského věta*:

**12.24. Věta.** *Graf $G$ je rovinný právě tehdy, když žádný jeho podgraf není izomorfní dělení grafu $K_{3,3}$ nebo grafu $K_5$.*

Jedna implikace této věty je zřejmá – dělením rovinného grafu vzniká vždy opět rovinný graf a jestliže podgraf nelze v rovině nakreslit bez křížení, totéž musí platit i pro celý graf $G$. Opačný směr důkazu je naopak velice složitý a nebudeme se jím zde zabývat.

Problematice rovinných grafů je věnováno ve výzkumu i v aplikacích hodně pozornosti, my se zde omezíme pouze na vybrané ilustrace.

Zmiňme alespoň na okraj, že existují algoritmy, které testují rovinatost grafu na $n$ vrcholech v čase $O(n)$, což určitě nejde přímou aplikací Kuratowského věty.

**12.25. Stěny v rovinných grafech.** Uvažme rovinný graf $G$, včetně jeho realizace v $\mathbb{R}^2$ a nechť $S$ je množina všech bodů $x\in\mathbb{R}^2$, které nepatří žádné hraně, ani nejsou vrcholem. Množina $\mathbb{R}^2\setminus G$ se rozpadne na disjunktní souvislé podmnožiny $S_i$, kterým říkáme *stěny rovinného grafu* $G$. Jedna stěna je výjimečná – ta, jejíž doplněk obsahuje všechny vrcholy grafu. Budeme jí říkat neohraničená stěna $S_0$. Množinu všech stěn budeme označovat $S=\{S_0,S_1,\ldots,S_k\}$ a rovinný graf $G=(V,E,S)$.



Jako nejjednodušší příklad si můžeme rozebrat stromy. Každý strom je zjevně rovinný graf, jak je vidět například z možnosti realizovat jej postupným přidáváním listů k jedinému vrcholu. Samozřejmě také můžeme použít Kuratowského větu – když není v $G$ žádná kružnice, nemůže obsahovat jakékoliv dělení grafů $K_{3,3}$ nebo $K_5$. Protože strom $G$ neobsahuje žádnou kružnici, dostáváme pouze jedinou stěnu $S_0$ a to tu neohraničenou. Protože víme, jaký je poměr mezi počty vrcholů a hran pro všechny stromy, dostáváme vztah

$$|V|-|E|+|S|=2.$$

**12.26. Eulerův vztah.** Vztah mezi počty hran, stěn a vrcholů lze odvodit pro všechny rovinné grafy. Jde o tzv. Eulerův vztah.

všechny tyto čtyři karty mají různou barvu (poslední karta river ještě není otočena)?

**Řešení.**

i) Počet různých symbolů je 13 a jsou vždy čtyři (pro každou barvu jeden). Proto je počet dvojic se stejnými symboly $13\binom{4}{2} = 78$. Počet všech možných dvojic je $\binom{13\cdot 4}{2} = 1326$. Pravděpodobnost stejných symbolů je tedy $\frac{1}{17} \doteq 0{,}06$.

ii) Jedna karta je eso, to jsou čtyři možnosti a druhá je libovolná, to je 51 možností. Dvojice s oběma esy, kterých je $\binom{4}{2} = 6$ jsme ale takto započítali dvakrát. Dostáváme tedy $4 \cdot 51 - 6 = 198$ dvojic a pravděpodobnost je $\frac{198}{1326} \doteq 0{,}15$.

iii) Spočítáme pravděpodobnosti jednotlivých nejlepších kombinací:

ROYAL FLUSH: Takové kombinace jsou zřejmě jen čtyři - pro každou barvu jedna. Všech kombinací pěti karet je $\binom{52}{5} = 2598960$. Pravděpodobnost je tak rovna přibližně $1{,}5 \cdot 10^{-6}$, tedy je hodně malá.

STRAIGHT FLUSH: Postupka, která končí nejvyšší kartou v rozmezí 5 až K, tj. 9 možností pro každou barvu. Dostáváme $\frac{36}{2598960} \doteq 1{,}4 \cdot 10^{-5}$.

POKER: Čtyři stejné symboly - 13 možností (pro každý symbol jedna). Pátá karta může být libovolná, to znamená 48 možností. Odtud: $\frac{624}{2598960} \doteq 2{,}4 \cdot 10^{-4}$.

FULL HOUSE: Tři stejné symboly $13\binom{4}{3} = 52$ možností a k tomu dva stejné symboly je $12\binom{4}{2} = 72$ možností. Pravděpodobnost je $\frac{3744}{2598960} \doteq 1{,}4 \cdot 10^{-3}$.

FLUSH: Všech pět karet stejné barvy znamená $4\binom{13}{5} = 5148$ možností a pravděpodobnost je pak $\frac{5148}{2598960} \doteq 2 \cdot 10^{-3}$.

STRAIGHT: Nejvyšší karta postupky je v rozmezí 5 až A, tj. 10 možností. Barva každé karty je pak libovolná, tj. dohromady $10 \cdot 4^5 = 10240$ možností. Zde jsme ale započítali jak straight flush, tak i royal flush. Ty je potřeba odečíst a výsledná pravděpodobnost pak je $\frac{10200}{2598960} \doteq 3,9 \cdot 10^{-3}$.

Celkově pro zjištění pravděpodobnosti nějaké z šesti nejlepších kombinací tedy dostáváme pravděpodobnost přibližně $3{,}9 \cdot 10^{-3} + 2 \cdot 10^{-3} + 1{,}4 \cdot 10^{-3} + 0{,}24 \cdot 10^{-3} = 7{,}54 \cdot 10^{-3}$, tj. asi 0,75%.

V Texas hold'em hraji vždy s pěti nejlepšími kartami ze sedmi. Počet příznivých kombinací z pěti karet jsme spočítali a k tomu dvě zbylé mohou být libovolné – to je $\binom{52-5}{2}$ kombinací. Dělit budeme počtem všech kombinací ze sedmi karet, tj. $\binom{52}{7}$. Pravděpodobnost dané kombinace pro Texas hold'em

Všimněme si, že z něho zejména vyplývá, že počet stěn v rovinném grafu nezávisí na způsobu, jak jeho rovinnou realizaci vybereme:

**Věta.** *Nechť $G = (V, E, S)$ je souvislý rovinný graf. Pak platí*

$$|V| - |E| + |S| = 2.$$

Důkaz. Budeme postupovat indukcí přes počet hran. Graf s jedinou hranou vztah splňuje.

Mějme dále graf $G$, pro nějž platí $|E| > 1$. Pokud $G$ neobsahuje kružnici, tj. jde o strom, tvrzení jsme již dokázali v 12.20(5), neboť každý strom má pouze jedinou stěnu $S_0$.

Předpokládejme dále, že nějaká hrana $e$ v grafu $G$ je obsažena v kružnici. Pak je i graf $G' = G \setminus e$ souvislý a podle indukčního předpokladu splňuje $G'$ Eulerův vztah, což znamená, že

$$|V| - (|E| - 1) + (|S| - 1) = 2,$$

protože s odebráním jedné hrany dojde nutně i k propojení právě dvou stěn grafu $G$ do jedné stěny v $G'$. Odtud ihned dostáváme platnost Eulerova vztahu i pro graf $G$. □

**Důsledek.**
- *Je-li $G = (V, E, S)$ rovinný graf s $n \geq 3$ vrcholy a $e$ hranami, pak platí*

$$e \leq 3n - 6,$$

*přičemž rovnost nastává, právě když jde o maximální rovinný graf (tj. nemůžeme už přidat žádnou hranu, aniž by $G$ přestal být rovinným grafem).*
- *Pokud navíc uvažovaný graf neobsahuje trojúhelník (tj. $K_3$ jako podgraf), platí dokonce $e \leq 2n - 4$.*

Důkaz. Jistě můžeme do daného grafu přidávat hrany tak dlouho, dokud se nestane maximálním. Pokud pro tento maximální graf $G$ bude platit rovnost z našeho tvrzení, pak samozřejmě bude platit i dokazovaná nerovnost pro graf původní.

Stejně tak, pokud by $G$ nebyl souvislý, jistě bychom mohli spojit hranou jeho komponenty, a nebyl by tedy maximální. I kdyby byl souvislý, ale ne 2-souvislý, pak by jistě existoval vrchol $v \in V$ takový, že po jeho odejmutí by se graf $G$ rozpadl do několika komponent $G_1, \ldots, G_k$, $k \geq 2$. Pak ovšem jistě bude možné přidat nějakou hranu mezi těmito komponentami, aniž bychom v původním grafu $G$ narušili jeho rovinnost (nakreslete si obrázek!). Můžeme tedy rovnou předpokládat, že je náš původní graf $G$ maximální rovinný 2–souvislý graf.

Jak jsme ukázali ve větě 12.13, každý 2–souvislý graf vzniká postupně z trojúhelníka $K_3$ dělením hran a přidáváním hran. Induktivně tak snadno ukážeme, že každá stěna rovinného grafu je nutně ohraničená kružnicí (což se jeví intuitivně jako zřejmé).

Pokud by ale nějaká stěna v našem maximálním rovinném grafu $G$ nebyla ohraničená trojúhelníkem, mohli bychom rozdělit tuto stěnu hranou (v geometrii bychom řekli úhlopříčkou), a jistě by tedy nemohl být $G$ maximální. Víme tedy, že hranice všech stěn v $G$ jsou trojúhelníky $K_3$. Odtud tedy vyplývá, že $3|S| = 2|E|$.

Nyní už stačí dosadit do Eulerova vzorce za počet stěn

$$|S| = \frac{2}{3}|E|.$$

Druhé tvrzení je analogické, pouze s tím rozdílem, že stěny v maximálním rovinném grafu nyní budou ohraničeny čtyřúhelníky, odkud vyplyne $4|S| = 2|E|$. □

tedy dostaneme z pravděpodobnosti pro klasický poker vynásobením koeficientem $\frac{\binom{52}{5}\binom{47}{2}}{\binom{52}{7}} = 21$.

Uvědomme si, že takto nedostaneme přesnou hodnotu pravděpodobnosti, protože jsme některé příznivé kombinace započítali vícekrát. Například v pětici karet máme full house a mezi těmi dvěma libovolnými kartami máme čtvrtý symbol k těm třem stejným. Máme tedy vlastně poker a tuto kombinaci počítáme dvakrát. Nicméně se výsledek nebude lišit o moc a pravděpodobnost vynikající kombinace u Texas hold'em bude zhruba dvacetkrát vyšší než u klasického pokeru. To je asi i jeden z důvodů, proč se prosadila tato herní varianta pokeru.

iv) Evidentně je situace hodně dobrá, proto bude lepší spočítat nepříznivé situace, kdy bude mít lepší kombinaci soupeř. Já mám v tuto chvíli full house ze dvou es a tří dvojek. Jediná kombinace, která by mě mohla porazit v tuto chvíli, je buď full house ze tří es a dvou dvojek nebo dvojkový poker. To znamená, že soupeř by určitě musel držet eso nebo poslední dvojku. Pokud drží dvojku a libovolnou jinou kartu, pak určitě vyhraje bez ohledu na kartu na riveru. Kolik je možností pro tuto kartu ke dvojce? $3+4+\cdots+4+2=45$ (jednu trojku a dvě esa už mít v ruce nemůže). Všech zbylých kombinací je $\binom{46}{2} = 1035$ a pravděpodobnost takové prohry je tak 0,043. Pokud drží v ruce eso, pak se může stát následující. Pokud drží (zbylá) dvě esa, tak opět vyhraje, pokud na riveru nepřijde dvojka - pak nastane remíza. Pravděpodobnost (podmíněná) mé prohry je tedy $\frac{1}{1035}\cdot\frac{43}{44} \doteq 10^{-3}$. Pokud drží soupeř v ruce eso a nějakou jinou kartu, než 2 a A, tak následuje remíza bez ohledu na river. Celková pravděpodobnost výhry nebo remízy je tak skoro 96 %. □

*12.50.* Osm karet, čtyři esa a čtyři krále rozdělíme po dvou mezi čtyři hráče. Jaká je pravděpodobnost, že někdo dostane alespoň dvě esa? Výsledek vyjádřete ve tvaru podílu dvou dvojciferných čísel. ○

*12.51.* Aleš má dvě speciální hrací kostky, na jedné padá vždy šestka, na druhé padá pouze čtyřka, pětka, či šestka, každé číslo se třetinovou pravděpodobností. Jaká je pravděpodobnost, že mu při hodu těmito dvěma kostkami padne vyšší součet než Martinovi, který hází se dvěma poctivými kostkami. Výsledek vyjádřete ve tvaru podílu dvou dvouciferných čísel. ○

**12.52.** Kolika způsoby lze rozestavit $n$ shodných věží na šachovnici $n\times n$ tak, aby bylo každé neobsazené pole ohrožováno některou z věží?

Z důsledku snadno dostaneme (bez Kuratowského věty), že $K_5$ a $K_{3,3}$ nejsou rovinné: v prvním případě je totiž $|V| = 5$ a $|E| = 10 > 3|V| - 6$, ve druhém pak, protože $K_{3,3}$ neobsahuje trojúhelník, máme $|V| = 6$, $|E| = 9 > 2|V| - 4$.

**12.27. Konvexní mnohostěny v prostoru.** Rovinné grafy si



můžeme dobře představit jako namalované na povrchu koule místo v rovině. Sféra vznikne z roviny tak, že přidáme jeden bod „v nekonečnu". Opět můžeme stejným způsobem hovořit o stěnách a pro takovýto graf pak jsou všechny jeho stěny rovnocenné (i stěna $S_0$ je ohraničená).

Naopak každý konvexní mnohostěn $P \subseteq \mathbb{R}^3$ si můžeme představit jako graf nakreslený na povrchu koule (můžeme si představit, že hrany a vrcholy daného mnohostěnu promítneme na dostatečně velkou sféru z libovolného bodu uvnitř $P$). Vypuštěním jednoho bodu uvnitř jedné ze stěn (ta se stane neohraničenou stěnou $S_0$) pak obdržíme rovinný graf jako výše tak, že „proděravělou sféru natáhneme do roviny".

Rovinné grafy, které vzniknou z konvexních mnohostěnů, jsou zjevně 2–souvislé, protože každé dva vrcholy v konvexním mnohostěnu leží na společné kružnici. Navíc v nich platí, že každá stěna kromě $S_0$ je vnitřkem nějaké kružnice a $S_0$ je vnějškem nějaké kružnice (při kreslení na sféře jsou všechny stěny vnitřek nějaké kružnice). Názorné se zdá i to, že ve skutečnosti budou grafy vznikající z konvexních mnohostěnů dokonce 3–souvislé.

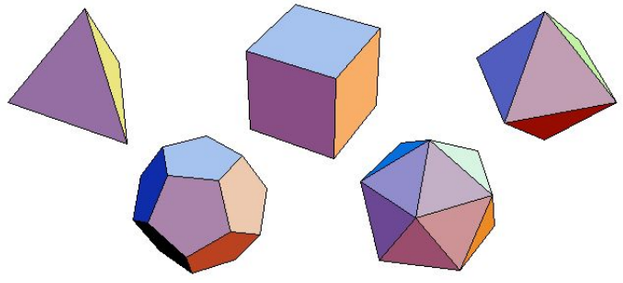
To není náhoda, platí totiž (dosti náročná) tzv. *Steinitzova věta* (kterou nebudeme dokazovat):

**Věta.** *Libovolný vrcholově* 3*–souvislý rovinný graf* $G$ *vzniká z konvexního mnohostěnu v* $\mathbb{R}^3$.

**12.28. Platónská tělesa.** Jako ilustraci kombinatorické práce



s grafy odvodíme klasifikaci tzv. pravidelných mnohostěnů, tj. mnohostěnů poskládaných ze stejných pravidelných mnohoúhelníků tak, že se jich v každém vrcholu dotýká stejný počet. Již v dobách antického myslitele Platóna se vědělo, že jich je pouze pět:



Přeložíme si požadavek pravidelnosti do vlastností příslušného grafu: chceme, aby každý vrchol měl stejný stupeň $d \geq 3$ a zároveň aby na hranici každé stěny byl stejný počet $k \geq 3$ vrcholů. Označme $n$ počet vrcholů, $e$ počet hran a $s$ počet stěn.

Máme k dispozici jednak vztah provazující stupně vrcholů s počtem hran:

$$dn = 2e.$$

Podobně počítáme počet hran, které ohraničují jednotlivé stěny, a bereme v úvahu, že každá je hranicí dvou stěn, tj.

$$2e = ks.$$

**Řešení.** Daná rozestavení jsou sjednocením dvou množin: množiny rozestavení, kdy je v každém řádku alespoň jedna věž (tedy v každém řádku právě jedna; tato množina má $n^n$ prvků – v každém řádku vybereme nezávisle jedno pole pro věž) a množiny rozestavení, kdy je v každém sloupci alespoň (tedy právě) jedna věž (stejnou úvahou jako u první množiny má tato množina rovněž $n^n$ prvků). Průnik těchto množin pak má $n!$ prvků (místa pro věže vybíráme postupně od prvního řádku – tam máme $n$ možností, ve druhém pak již pouze $n-1$ možností – jeden sloupec je již obsazen, ...). Podle principu inkluze a exkluze je počet hledaných rozestavení:

$$2n^n - n!.$$ □

**12.53.** Pětkrát jsme hodili mincí. Pokud padl líc, dali jsme do klobouku bílou kuličku. Když padl rub, dali jsme do téhož klobouku kuličku černou. Vyjádřete pravděpodobnost, že v klobouku je více černých kuliček než bílých, je-li v klobouku alespoň jedna černá kulička.

**Řešení.** Zaveďme jevy

$A$ – v klobouku je víc černých kuliček než bílých,

$H$ – v klobouku je aspoň jedna černá kulička.

Chceme stanovit $P(A|H)$. Uvědomme si, že pravděpodobnost $P\left(H^C\right)$ opačného jevu k jevu $H$ je $2^{-5}$ a že pravděpodobnost jevu $A$ je stejná jako pravděpodobnost $P\left(A^C\right)$ jevu opačného (v klobouku je víc bílých kuliček). Nutně tedy $P(H) = 1 - 2^{-5}$, $P(A) = 1/2$. Dále je $P(A \cap H) = P(A)$, neboť jev $H$ obsahuje jev $A$ (jev $A$ má za důsledek jev $H$). Celkem jsme obdrželi

$$P(A|H) = \frac{P(A \cap H)}{P(H)} = \frac{\frac{1}{2}}{1 - \left(\frac{1}{2}\right)^5} = \frac{16}{31}.$$ □

### F. Pokročilejší kombinatorické úlohy

V první kapitole jsme se seznámili se základními kombinatorickými postupy. I když využijeme pouze těchto postupů, jsme schopni vyřešit relativně komplikované úlohy.

**12.54.** Na kružnici stojí $n$ pevností ($n \geq 3$), očíslovaných po řadě



čísly $1,\ldots,n$. V jeden okamžik každá vystřelí na jednu ze dvou sousedních (pevnosti 1 a $n$ rovněž považujeme za sousední). Označme $P(n)$ počet možných výsledků střelby (za výsledek střelby považujeme množinu čísel právě těch pevností, které byly při střelbě zasaženy, nerozlišujeme přitom mezi jedním a dvěma zásahy). Dokažte, že čísla $P(n)$ a $P(n+1)$ jsou nesoudělná.

Eulerův vztah pak říká

$$2 = n - e + s = \frac{2e}{d} - e + \frac{2e}{k}.$$

Úpravou odtud dostáváme pro naše konstanty $d$ a $k$ vztah

$$\frac{1}{d} - \frac{1}{2} + \frac{1}{k} = \frac{1}{e}.$$

Protože nejen $d$ a $k$, ale také $e$ a $n$ musí být kladná přirozená čísla (tj. zejména je $\frac{1}{e} > 0$), dostáváme z této rovnosti velice silné omezení možností. Zejména levá strana nabývá maximální hodnotu pro $d = 3$. Dosadíme-li tuto hodnotu $d = 3$, obdržíme drobnou úpravou nerovnost

$$-\frac{1}{6} + \frac{1}{k} = \frac{1}{e} > 0.$$

Odtud vyplývá $k \in \{3, 4, 5\}$ pro obecné $d$. V původní rovnosti jsou ale role $k$ a $d$ symetrické, musí tedy i $d \in \{3, 4, 5\}$. Prověřením několika zbývajících možností dostáváme následující výčet všech řešení:

| $d$ | $k$ | $n$ | $e$ | $s$ |
|---|---|---|---|---|
| 3 | 3 | 4 | 6 | 4 |
| 3 | 4 | 8 | 12 | 6 |
| 4 | 3 | 6 | 12 | 8 |
| 3 | 5 | 20 | 30 | 12 |
| 5 | 3 | 12 | 30 | 20 |

Zbývá ukázat, že všechny odpovídající pravidelné mnohostěny skutečně existují. Již jsme je viděli na obrázcích výše, to ale není matematický důkaz. U prvních tří jistě nejsou pochybnosti. Uveďme si pěknou geometrickou konstrukci dvanáctistěnu (malujte si přitom obrázek!).



Začneme s krychlí a na všech jejích stěnách budeme současně a stejným způsobem stavět „stany áčka“. Horní vodorovné tyčky přitom nachystáme na úrovni ploch stěn krychle tak, aby byly pro sousední stěny vždy na sebe kolmé, a jejich délku zvolíme tak, aby lichoběžníky bočních stěn stanu měly tři stejně dlouhé strany. Nyní budeme zdvihat současně a stejně všechny stany při zachovávání poměrů tří stran lichoběžníků. Jistě nastane právě jednou okamžik, ve kterém budou sousední lichoběžníkové a trojúhelníkové stěny koplanární (tj. budou v jedné rovině). Tak vznikne pravidelný dvanáctistěn.

Jako cvičení si zkuste sestrojit dvacetistěn!

### 2. Příklady využití grafových technik

V této části se zaměříme na několik příkladů využití nástrojů grafů a na nich založených algoritmů.

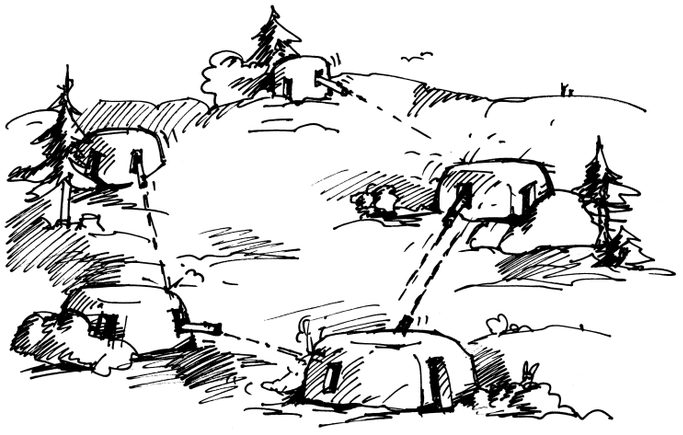
**12.29. Kostra grafu.** V praktických aplikacích často zadává graf



všechny možnosti propojení mezi objekty, příkladem může být třeba silniční nebo vodovodní nebo elektrická síť. Pokud nám stačí zajistit propojitelnost každých dvou vrcholů při minimálním počtu hran, hledáme vlastně v grafu $G$ podgraf $T$ na všech vrcholech grafu $G$, který je stromem.

**Definice.** Libovolný strom $T = (V, E')$ v grafu $G = (V, E)$, $E' \subseteq E$ se nazývá *kostra* grafu $G$.

Evidentně může kostra v grafu existovat, pouze pokud je graf $G$ souvislý. Jako formální důkaz, že platí i opak, uvedeme přímo algoritmus, jak kostru grafu sestrojit.



**Řešení.** Označíme-li zasažené pevnosti černým kolečkem a nezasažené bílým, úloha určit $P(n)$ je ekvivalentní úloze určit počet všech možných obarvení $n$ koleček, umístěných na kružnici, černou a bílou barvou tak, aby nebyla žádná dvě bílá kolečka „ob jedno“. Pro lichá $n$ je tento počet roven počtu $K(n)$ obarvení černou a bílou barvou tak, aby žádná dvě bílá kolečka nestála vedle sebe (přečíslujeme pevnosti tak, že začneme u kolečka 1 a číslujeme popořadě vzestupně po lichých číslech a poté vzestupně po sudých). V případě sudého $n$ je tento počet roven $K(n/2)^2$, kvadrátu počtu obarvení $n/2$ koleček na obvodu kruhu tak, aby žádná dvě bílá nestála vedle sebe (barvíme nezávisle kolečka na lichých a na sudých pozicích).

Pro $K(n)$ poměrně snadno odvodíme rekurentní formuli $K(n) = K(n-1) + K(n-2)$. (Zas tak úplně jednoduché to není, ponecháváme čtenáři jako cvičení.) Navíc snadno spočteme, že $K(2) = 3, K(3) = 4, K(4) = 7$, tedy $K(2) = F(4) - F(0)$, $K(3) = F(5) - F(1)$, $K(4) = F(6) - F(2)$ a indukcí snadno dokážeme $K(n) = F(n+2) - F(n-2)$, kde $F(n)$ značí $n$-tý člen Fibonacciho posloupnosti (kde $F(0) = 0$, $F(1) = F(2) = 1$). Navíc protože $(K(2), K(3)) = 1$, máme pro $n \geq 3$ obdobně jako u Fibonacciho posloupnosti

$$\begin{aligned}(K(n), K(n-1)) &= (K(n) - K(n-1), K(n-1)) = \\ &= (K(n-2), K(n-1)) = \cdots = 1.\end{aligned}$$

Ukážeme nyní, že pro každé sudé $n = 2a$ je $P(n) = K(a)^2$ nesoudělné jak s $P(n+1) = K(2a+1)$, tak s $P(n-1) = K(2a-1)$. K tomu stačí následující: pro $a \geq 2$ je totiž

$$\begin{aligned}&(K(a), K(2a+1)) = (K(a), F(2)K(2a) + F(1)K(2a-1)) = \\ &= (K(a), F(3)K(2a-1) + F(2)K(2a-2) = \cdots = \\ &= (K(a), F(a+1)K(a+1) + F(a)K(a)) = \\ &= (K(a), F(a+1)) = (F(a+2) - F(a-2), F(a+1)) =\end{aligned}$$

**Algoritmus 1.** Seřadíme zcela libovolně všechny hrany $e_1, \ldots, e_m$ v $E$ do pořadí a postupně budujeme množiny hran $E'_i$ tak, že v $(i+1)$-ním kroku přidáme hranu $e_i$ k $E'_i$, jestliže tím nevznikne v grafu $G_i = (V, E_i \cup \{e_i\})$ kružnice, a ponecháme $E_i$ beze změny v případě opačném. Algoritmus skončí, buď pokud má již graf $G_i$ pro nějaké $i$ právě $n-1$ hran nebo pokud již platí $i = m$. Pokud zastavujeme z druhého důvodu, byl původní graf nesouvislý a kostra neexistuje.

**Lemma.** *Výsledkem předchozího algoritmu je vždy les $T$. Jestliže algoritmus skončí s $k \leq n-1$ hranami, má původní graf $n-k$ komponent. Zejména je tedy $T$ kostrou, právě když algoritmus skončí po vložení $n-1$ hran.*

Důkaz. Podle pravidla v algoritmu, výsledný podgraf $T$ v $G$ nikdy neobsahuje kružnice. Je tedy lesem. Jestliže je výsledný počet hran $n-1$, jde o strom, viz Věta 12.20.

Zbývá pouze ukázat, že souvislé komponenty grafu $T$ mají stejné množiny vrcholů jako souvislé komponenty původního grafu $G$. Každá cesta v $T$ je i cestou v $G$, musí tedy všechny vrcholy z jednoho stromu v $T$ ležet všechny v jedné komponentě $G$. Pokud by ale existovala v $G$ cesta z $v$ do $w$ taková, že její koncové vrcholy leží v různých stromech v $T$, pak na ní existuje poslední vrchol $v_i$ v komponentě určené vrcholem $v$ (zejména tedy $v_{i+1}$ v této komponentě neleží). Příslušná hrana $\{v_i, v_{i+1}\}$ musela někdy při chodu algoritmu ale vytvářet kružnici, protože jinak by se bývala ocitla mezi hranami v $T$. Protože se během algoritmu hrany neodebírají, musí tedy existovat cesta mezi $v_i$ a $v_{i+1}$ v $T$. To je ovšem spor s našimi předpoklady, a proto $v$ a $w$ nemohou ležet v různých stromech v $T$. Počet komponent v $T$ je tedy dán tím, že počet vrcholů a hran ve stromech se liší o 1, proto s každou komponentou se tento rozdíl o 1 zvětší. Máme-li tedy v našem lese $n$ vrcholů a $k$ hran, nutně má $n-k$ komponent. □

**Poznámka.** Jako vždy bychom se měli zabývat otázkou, jak složitý je uvedený algoritmus. Kružnice přidáním nové hrany vznikne tehdy a jen tehdy, jestli její koncové vrcholy leží ve stejné souvislé komponentě budovaného lesu $T$. Stačí nám proto průběžně udržovat znalost souvislých komponent.

K realizaci algoritmu proto potřebujeme (v abstraktní podobě) umět pro již zadané třídy ekvivalence na dané množině (v našem případě jsou to vrcholy) slučovat dvě třídy ekvivalence do jedné a nalézat pro daný prvek, do které třídy patří. Pro sjednocení jistě potřebujeme $O(k)$ času, kde $k$ je počet prvků slučovaných tříd a jistě můžeme použít ohraničení počtu $k$ celkovým počtem vrcholů $n$. Můžeme si ale pamatovat spolu se třídami i počty jejich prvků a průběžně pro každý vrchol uchovávat informaci, do které třídy patří. Sjednocení dvou tříd tedy představuje přeznačení jména u všech prvků jedné z nich. Jestliže při přeznačování příslušnosti vrcholů k třídám budeme vždy přeznačovat tu menší z nich, pak celkový počet operací potřebných v našem algoritmu bude $O(n \log n + m)$.

**Algoritmus 2.** Kostru můžeme ale hledat také jinak a rychleji: Budeme v grafu $G = (V, E)$ s $n$ vrcholy a $m$ hranami postupně budovat strom $T$. Začneme v libovolně zvoleném vrcholu $v$ a s prázdnou množinou hran, tj. $T_0 = (\{v\}, \emptyset)$. V $i$-tém kroku hledáme mezi hranami, které dosud nejsou v $T_{i-1}$, ty, které mají v $T_{i-1}$ jeden

$$
\begin{aligned}
&= (F(a+2) - F(a+1) - F(a-2), F(a+1)) = \\
&= (F(a) - F(a-2), F(a+1)) = \\
&= (F(a-1), F(a+1)) = (F(a-1), F(a)) = 1.
\end{aligned}
$$

$$
\begin{aligned}
&(K(a), K(2a-1)) = \\
&= (K(a), F(2)K(2a-2) + F(1)K(2a-3)) = \\
&= (K(a), F(3)K(2a-3) + F(2)K(2a-4)) = \\
&= \cdots = (K(a), F(a)K(a) + F(a-1)K(a-1)) = \\
&= (K(a), F(a-1)) = (F(a+2) - F(a-2), F(a-1)) = \\
&= (F(a+2) - F(a), F(a-1)) = \\
&= (F(a+2) - F(a+1), F(a-1)) = (F(a), F(a-1)) = 1.
\end{aligned}
$$

Tím je tvrzení dokázáno. □

### G. Pravděpodobnost v kombinatorice

Klasická pravděpodobnost velice úzce souvisí s kombinatorikou, jak jsme již viděli v první kapitole. Uveďme další, trochu zamotanější příklad.

Kombinatorika je schována i v následující „pravděpodobnostní“ úloze.

**12.55.** 
Ve vězení je 100 vězňů, očíslovaných 1 až 100. Nejvyšší žalářník do uzavřené místnosti umístil 100 truhel (také očíslovaných 1 až 100) a do truhel náhodně vložil 100 papírků s čísly 1 až 100, přičemž do každé truhly vložil papírek s jiným číslem. Rozhodl se s vězni hrát následující hru: Do místnosti vstoupí vždy jeden vězeň a má za úkol otevřít 50 truhel. Poté odchází jinými dveřmi a nemá možnost se domlouvat s ostatními vězni. Místností takto projdou postupně všichni vězni. Žalářník všem slíbil svobodu, jestliže každý z nich při otevírání truhel najde svoje číslo. Jestliže jen jediný z nich svoje číslo nenajde, budou všichni popraveni. Než vězni začnou hru hrát, mohou se domluvit na nějaké strategii. Existuje strategie, která vězňům zajistí „rozumnou“ šanci na výhru?

**Řešení.** Je zřejmé, že v případě náhodného otevírání truhel, kde jsou volby jednotlivých vězňů nezávislé, je šance každého vězně na nalezení jeho čísla 1/2, tedy celková šance na výhru je $1/2^{100}$. Proto je nutné najít strategii, u které jsou šance na úspěch jednotlivých vězňů co nejvíce závislé. Abychom našli vhodnou strategii, musíme si nejdříve uvědomit, že každý vězeň otevírá truhly po jedné. Přitom nemá žádné informace od ostatních vězňů, stejně tak neví nic o rozmístění čísel v truhlách. Jakmile však otevře nějakou truhlu, zná číslo, které v ní je uložené. Tato skutečnost společně s myšlenkou, že by měl vězeň koncový vrchol, ale druhý koncový vrchol do $T_{i-1}$ nepatří. První takovou hranu přidáme i s druhým koncovým vrcholem a získáme tak $T_i$. Algoritmus skončí, až taková hrana neexistuje.

Evidentně je výsledný graf $T$ souvislý a podle počtu vrcholů a hran je to strom. Ukážeme, že vrcholy $T$ splývají s vrcholy souvislé komponenty grafu $G$. Předpokládejme proto, že do nějakého vrcholu $w$ vede z $v$ cesta. Pokud by $w$ nebyl vrchol v $T$, pak zcela stejně jako v důkazu předchozího lemmatu na ní najdeme poslední vrchol $v_i$, který ještě do $T$ patří. Další hrana cesty by ale v okamžiku ukončení algoritmu připadala v úvahu pro přidání do $T$, což je spor.

Tento algoritmus tedy v čase $O(n+m)$ nalezne kostru souvislé komponenty zvoleného počátečního vrcholu $v$.

**12.30. Minimální kostra.** 
Každá kostra daného grafu $G$ má stejný počet hran, protože je to obecnou vlastností stromů. Tak, jak jsme ale již dříve hledali nejkratší cesty v grafech s ohodnocenými hranami, budeme v případě koster jistě chtít umět najít kostry s minimálním součtem ohodnocení použitých hran.

**Definice.** Nechť $G = (V, E, w)$ je souvislý graf s hranami ohodnocenými nezápornými vahami $w(e)$. Jeho *minimální kostra* $T$ je taková kostra grafu $G$, která má mezi všemi jeho kostrami minimální součet ohodnocení hran kostry.

O praktičnosti takové úlohy můžete přemýšlet třeba v souvislosti s rozvodnými sítěmi elektřiny, plynu, vody apod.

Kupodivu je docela jednoduché minimální kostru najít (za uvedeného předpokladu, že jsou všechna ohodnocení $w(e)$ hran v grafu $G$ nezáporná). Následujícímu postupu se říká *Kruskalův algoritmus*:

- setřídíme všech $m$ hran v $E$ tak, aby $w(e_1) \le w(e_2) \le \cdots \le w(e_m)$;
- v tomto pořadí aplikujeme na hrany postup z Algoritmu 1 pro kostru v předchozím odstavci.

Jde o typický příklad takzvaného „hladového přístupu“, kdy se k maximalizaci zisku (nebo minimalizaci nákladů) snažíme dostat výběrem momentálně nejvýhodnějšího kroku. Často tento přístup zklame, protože nízké náklady na začátku procesu mohou zavinit vysoké na jeho konci. Hladové algoritmy jsou proto často základem velmi užitečných heuristických přístupů, jen málokdy dávají optimální řešení. V našem případě ale skutečně dostaneme vždy minimální kostru:

**Věta.** *Kruskalův algoritmus správně řeší problém minimální kostry pro každý souvislý graf $G$ s nezáporným ohodnocením hran. Algoritmus pracuje v čase $O(m \log m)$, kde $m$ je počet hran v $G$.*

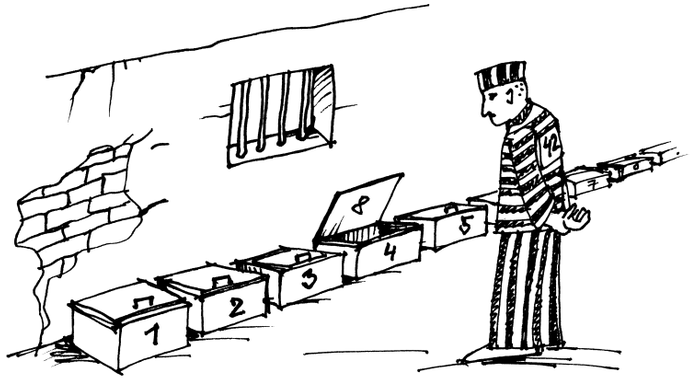
Důkaz. Označme $T = (V, E(T))$ kostru vygenerovanou Kruskalovým algoritmem a nechť $\tilde{T} = (V, E(\tilde{T}))$ je jakákoliv minimální kostra. Z minimality zřejmě $\sum_{e\in E(\tilde{T})} w(e) \le \sum_{e\in E(T)} w(e)$, naším cílem bude ukázat, že rovněž platí



$$\sum_{e\in E(T)} w(e) \le \sum_{e\in E(\tilde{T})} w(e).$$

Pokud $E(T) = E(\tilde{T})$, pak není co dokazovat. Předpokládejme tedy, že existuje hrana $e \in E(T)$ taková, že $e \notin E(\tilde{T})$. Zvolme si takovou hranu $e$ s minimálním ohodnocením $w(e)$.

otevření další truhly podmínit číslem v truhle předchozí, nabízí jednoduchou strategii. Každý vězeň nejprve otevře truhlu se svým číslem. Je-li v ní papírek s jeho číslem, uspěl, a může otevřít další truhly náhodně. Jestliže je v ní jiné číslo, jako další truhlu si zvolí truhlu s právě tímto číslem. Takto pokračuje dokud buď nenajde svoje číslo nebo neotevře 50 truhel. Každá truhla tedy jednoznačně odkazuje na nějakou další truhlu, nazvěme tedy tuto strategii *odkazovací strategie*.




**Pravděpodobnost úspěchu.** Žalářníkovo umístění papírků s čísly do truhel je permutace. Abychom našli pravděpodobnost úspěchu odkazovací strategie, musíme zjistit, pro které permutace bude fungovat. Připomeňme si, že každá permutace se dá zapsat jako spojení uzavřených disjunktních cyklů. Kdyby vězeň dodržující odkazovací strategii mohl otevřít libovolné množství truhel, pak by na své číslo narazil vždy až jako na poslední v cyklu, neboť začíná truhlou se svým číslem, na kterou odkazuje právě papírek s jeho číslem. Z toho plyne, že máme-li $n$ vězňů, pak permutace, pro něž tato strategie nezafunguje, jsou ty permutace, které obsahují nějaký cyklus délky větší než $n/2$, protože žádný vězeň, jehož číslo je obsaženo v tomto cyklu, jej nenajde včas. Musíme tedy spočítat, kolik takových permutací existuje. Obecně pravděpodobnost, že v permutaci délky $n$ bude cyklus délky $r > n/2$ (kratší cykly by se mohly opakovat vícekrát, delší může být vždy maximálně jeden, což nám zjednodušuje výpočet), je následující: Musíme vybrat, kterých $r$ prvků v cyklu bude, uspořádat je v cyklickém pořadí a pak zvolit libovolnou permutaci pro zbylých $n-r$ prvků. Získáváme tedy číslo:

$$\binom{n}{r}(r-1)!\,(n-r)! = \frac{n!}{r}$$

Pravděpodobnost, že se tato permutace vyskytne mezi jednou z celkových možných $n!$ permutací je $1/r$. Pro naši hru se 100 vězni je tedy pravděpodobnost výhry:

Přidáním $e$ do $\tilde{T}$ vznikne v $\tilde{T}$ kružnice $ee_1e_2\cdots e_k$ a alespoň jedna její hrana $e_i$ není v $E(T)$. Vzhledem ke způsobu výběru hrany $e$ by za předpokladu $w(e_i) < w(e)$ byla hrana $e_i$ mezi diskutovanými hranami v Kruskalově algoritmu po vytvoření jistého podstromu $T' \subseteq T \cap \tilde{T}$ a zjevně by její případné přidání k postupně budovanému stromu $T$ nezpůsobilo kružnici. Kdyby tedy platilo $w(e_i) < w(e)$, musela by být v Kruskalově algoritmu hrana $e_i$ vybrána. Proto platí $w(e_i) \geq w(e)$.

Nyní ovšem můžeme v minimální kostře $\tilde{T}$ vyměnit hranu $e_i$ a hranu $e$ (zřejmě půjde díky volbě $e_i$ opět o kostru), aniž bychom zvýšili součet ohodnocení, tj. opět získáme minimální kostru $\tilde{T}$. Ta se ale liší od $T$ již v méně hranách než předtím. Po konečném počtu kroků takto změníme $\tilde{T}$ na $T$, aniž bychom navýšili celkové ocenění hran. □

**12.31. Další algoritmy pro minimální kostru.** I druhý z našich algoritmů pro kostru grafu v předchozím odstavci vede na minimální kostru, pokud v každém okamžiku volíme ze všech možných hran $e_i = \{v_i, v_{i+1}\}$, $v_i \in V_i$, $v_{i+1} \in V \setminus V_i$ tu, která má minimální ohodnocení. Výsledný postup se zpravidla nazývá *Primův algoritmus* podle jeho práce z r. 1957. Ve skutečnosti byl ale popsán českým matematikem Jarníkem již v roce 1930. Raději mu proto říkejme *Jarníkův algoritmus*. Jarník přitom reagoval na ještě dřívější algoritmus brněnského matematika O. Borůvky z r. 1926.

**Věta.** *Jarníkův algoritmus najde minimální kostru pro každý souvislý graf s libovolným ohodnocením hran.*

**Poznámka.** *Borůvkův algoritmus* je docela podobný, konstruuje ale postupně stále co nejvíce souvislých komponent zaráz. Začneme tedy s jednoprvkovými komponentami v grafu $T_0 = (V, \emptyset)$ a pak postupně vždy každou komponentu propojíme nejkratší možnou hranou s komponentou jinou. Opět lze dokázat, že (za předpokladu, že váhy jsou po dvou různé) takto obdržíme minimální kostru. V pseudokódu by šel tento algoritmus zapsat následovně:

(1) *Inicializace*. Vytvoř graf $S$ složený z vrcholů grafu $G$ s prázdnou množinou hran;
(2) *Hlavní cyklus*. Dokud má $S$ více než jednu komponentu, opakuj:
- pro každý strom $T$ v $S$ najdi nejmenší hranu spojující $T$ s $G \setminus T$, tuto hranu přidej do $E$,
- všechny hrany z $E$ přidej do $S$.

Všimněme si, že Borůvkův algoritmus umožňuje realizaci pomocí paralelizovaných výpočtů, a je proto skutečně v různých praktických modifikacích využíván.

Důkazy správnosti obou algoritmů lze snadno dohledat v literatuře.

**12.32. Problém obchodního cestujícího.** Z naší krátké exkurze do grafových problémů a algoritmů by mohl vzniknout dojem, že je v zásadě možné nalézat hezké a jednoduché algoritmy řešící uvažované problémy. To bylo ale způsobeno tím, že jsme si dosud vybírali pouze problémy jednoduché. V drtivé většině případů je tomu naopak, když teoretické výsledky ukazují, že algoritmus fungující alespoň v polynomiálním čase zřejmě neexistuje a používají se takové, které dávají výsledky rozumně dobré, nikoliv však nutně optimální.



Jedním z nejsledovanějších takových kombinatorických problémů je úloha, kdy máme najít v grafu s ohodnocenými hranami

$$1 - \sum_{k=51}^{100} \frac{1}{k} \approx 0{,}311828$$

Jak vidíme, získali jsme velice dobrou šanci na úspěch (ve srovnání s $1/2^{100}$). Pro zajímavost se nyní podívejme, jak se tato pravděpodobnost chová obecně pro rostoucí počet vězňů. Obecně máme pravděpodobnost, že bude při $n$ vězních permutace obsahovat cyklus délky $r > n/2$ rovnu:

$$p = \sum_{k=1+\frac{n}{2}}^{n} \frac{1}{k}$$

Připomeneme, že $\sum_{k=1}^{n} \frac{1}{k} \to \ln(n) + \gamma$ pro $n \to \infty$, kde $\gamma$ je Eulerova konstanta. Máme tedy:

$$p = \sum_{k=1}^{n} \frac{1}{k} - \sum_{k=1}^{\frac{n}{2}} \frac{1}{k} \to \ln(n) + \gamma - \ln\left(\frac{n}{2}\right) - \gamma = \ln 2, \text{ pro } n \to \infty.$$

Odtud tedy máme, že pravděpodobnost úspěchu vězňů je pro velká $n$ rovna $1 - p \simeq 1 - \ln 2 = 0{,}30685\ldots$. V další části si ukážeme, že odkazovací strategie je nejlepší možnou strategií.

**Optimalita strategie.** Pro důkaz optimality odkazovací strategie budeme nejprve muset zavést úpravu pravidel první hry, označme ji hra A a srovnat ji se druhou hrou, označme ji hra B.

Upravíme pravidla hry A následujícím způsobem: Každý vězeň bude otevírat truhly tak dlouho, dokud nenalezne papírek se svým číslem. Vězni vyhrají, pokud žádný z nich neotevře více než 50 truhel. Tato úprava očividně nezmění šance vězňů na výhru, pomůže nám však při důkazu optimality.

Nyní uvažme druhou hru (hru B) s následujícími pravidly: Do místnosti s truhlami jde nejdříve vězeň číslo 1 a otevírá truhly (podle jakékoli strategie), dokud nenalezne papírek se svým číslem, všechny truhly ale zanechá otevřené. Jako další je do místnosti pozván vězeň s nejmenším číslem, které ještě nebylo otevřeno a opět otevírá truhly, dokud nenajde své číslo. Takto hra pokračuje, dokud nejsou otevřeny všechny truhly. Ve hře B vězni vyhrávají, jestliže žádný z nich neotevřel více než 50 (obecně $n/2$) truhel.

Předpokládejme, že žalářník si zapisuje čísla z papírků v tom pořadí, v jakém jsou objevována v truhlách v průběhu hry B podle zvolené strategie vězňů. Dostane tak permutaci čísel 1 až 100, ze které vidí, zda vězni uspěli či ne (podle počtu čísel mezi následujícími čísly). Ať v této hře zvolí vězni jakoukoli strategii, je šance na nalezení nějakého dalšího čísla vždy stejná. Existuje 100! permutací, které odpovídají minimální hamiltonovskou kružnici, tzn. kružnici s minimálním součtem vah použitých hran mezi všemi možnými hamiltonovskými kružnicemi.

Praktické vyjádření ne vždy na první pohled prozradí, že jde právě o tento problém. Setkáváme se s ním například při

- plánování dodávek zboží nebo služeb,
- organizaci poštovní služby (rozvoz pošty, výběr pošty ze schránek),
- plánování údržby sítí (např. bankomatů),
- obsluha požadavků z fronty (např. při paralelních požadavcích na čtení z hard disku),
- plánování postupného měření jednotlivých částí celku (např. při studiu struktury krystalu proteinu pomocí rentgenu, kdy náklady jsou soustředěny zejména na posuvy a zaostření pro jednotlivá měření),
- plánování dělení materiálů (např. dělení tapet při jejich lepení na použité pásy tak, aby navazoval vzorek, a došlo přitom k co nejmenším ztrátám).

I v případě hledání minimální hamiltonovské kružnice můžeme uplatnit hladový (anglicky „greedy“) přístup. Algoritmus začne v libovolném vrcholu $v_1$, který se stane aktivním, a všechny ostatní si označí za spící. Postupuje pak v krocích tak, že vždy najde ten dosud neumístěný vrchol ze spících, do kterého vede z aktivního vrcholu nejméně ohodnocená hrana. Aktivní vrchol označí jako zpracovaný a tento nový vrchol se stane aktivním. Algoritmus skončí buď neúspěchem, když nenajde žádnou hranu z aktivního vrcholu do spícího vrcholu, ale hamiltonovská kružnice ještě nebyla nalezena, nebo využitím všech vrcholů. Pokud ve druhém případě existuje hrana z posledního přidaného vrcholu $v_n$ do $v_1$, získáme hamiltonovskou kružnici.

Je zjevné, že tento algoritmus jen velice zřídka vyprodukuje skutečně minimální hamiltonovskou kružnici. Na úplném grafu zato vždy alespoň nějakou najde.

**12.33. Toky v sítích.** Další skupina aplikací jazyka teorie grafů se



týká přesunu nějakého měřitelného materiálu v pevně zadané síti. Vrcholy v orientovaném grafu představují body, mezi kterými lze podél hran přenášet předem známá množství, která jsou zadána formou ohodnocení hran. Některé vybrané vrcholy představují *zdroj sítě*, jiné výstup ze sítě. Podle analogie potrubní sítě pro přenos kapaliny říkáme výstupním vrcholům *stok sítě*. Síť je tedy pro nás orientovaný graf s ohodnocenými hranami a vybranými vrcholy, kterým říkáme zdroje a stoky.

Je zřejmé, že se můžeme bez újmy na obecnosti omezit na orientované grafy s jedním zdrojem a jedním stokem. V obecném případě totiž vždy můžeme přidat jeden stok a jeden zdroj navíc a spojit je vhodně orientovanými hranami s všemi zadanými zdroji a stoky tak, že ohodnocení přidaných hran bude zároveň zadávat maximální kapacity jednotlivých zdrojů a stoků. Situace je naznačena na obrázku, kde černými vrcholy nalevo jsou zobrazeny všechny zadané zdroje, zatímco černé vrcholy napravo jsou všechny zadané stoky. Nalevo je jeden přidaný (virtuální) zdroj jako bílý vrchol a napravo jeden stok. Označení hran není v obrázku uvedeno.

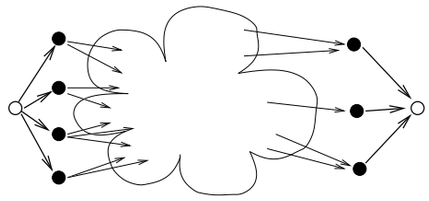
nějakým zvoleným strategiím, ať už náhodným nebo jakkoli sofistikovaným, neboť jsou to jen zápisy pořadí, v jakém byla jednotlivá čísla odhalena.

Pro výpočet pravděpodobnosti výhry vězňů ve hře B si nejprve všimněme, že libovolné pořadí může být zapsáno seskupením cyklů, kde každý cyklus odpovídá otevřeným truhlám jednoho vězně. Pro představu, mějme hru s 8 vězni. Žalářník si zapsal permutaci $(2, 5, 7, 1, 6, 8, 3, 4)$, odtud vidíme, že vězni vyhráli, protože vězeň číslo 1 otevřel truhly s čísly $(2, 5, 7, 1)$, následoval vězeň 3 a otevřel truhly s čísly $(6, 8, 3)$ a nakonec vězeň číslo 4 otevřel pouze truhlu s číslem (4). V tomto případě tedy můžeme psát: $(2, 5, 7, 1, 6, 8, 3, 4) \to (2, 5, 7, 1)(6, 8, 3)(4)$. Navíc ukážeme, že každá takováto permutace vychází z unikátního seřazení čísel 1 až 8. Máme-li libovolnou permutaci zapsanou v cyklické notaci, nejprve jednotlivé cykly přepíšeme tak, aby jejich nejmenší prvek byl poslední a poté celé cykly seřadíme tak, aby byly seřazeny vzestupně podle posledních prvků. Máme například:

$$(7, 5, 8)(2, 4)(1, 6, 3) \to (6, 3, 1)(4, 2)(8, 7, 5) \to$$
$$\to (6, 3, 1, 4, 2, 8, 7, 5).$$

Sestrojili jsme tedy bijekci mezi pořadími otevřených čísel, pro která vězni vyhrají a mezi permutacemi čísel 1 až 8, které neobsahují cyklus větší než 4. Z toho plyne, že pravděpodobnost výhry vězňů ve hře B je stejná, jako pravděpodobnost, že permutace neobsahuje žádný cyklus délky větší než 4 (obecně $n/2$). To přesně odpovídá pravděpodobnosti výhry vězňů v původní hře za využití odkazovací strategie. Z tohoto vyplývá nejdůležitější závěr pro hru A. Vězni mohou totiž jakoukoli strategii ze hry A aplikovat na hru B následujícím způsobem: $i$-tý hráč postupuje stejně, jako ve hře A s tím rozdílem, že je-li nějaká truhla již otevřená, zachová se, jakoby byla zavřená, nevyužije tedy všechny své tahy, ale další krok založí na čísle napsaném na papírku otevřené truhly. Odtud tedy jakákoli strategie, která je úspěšná pro nějaké seřazení papírků ve hře A, musí být nutně úspěšná pro stejné seřazení i ve hře B. Kdyby existovala lepší strategie ve hře A, mohli bychom ji aplikovat na hru B a získat větší šanci na úspěch i v ní, to je však nemožné, protože všechny strategie ve hře B vedou ke stejné pravděpodobnosti úspěchu. Větší šanci na úspěch, než použitím odkazovací strategie, tedy získat nemůžeme. □

**12.56.** V soutěži je $m$ soutěžících a $n$ rozhodčích, kde $n \geq 3$ je liché celé číslo. Každý soutěžící je od každého rozhodčího hodnocen jako úspěšný nebo neúspěšný. Předpokládejme, že libovolní dva rozhodčí



### Sítě a toky

Síť je orientovaný graf $G = (V, E)$ s vybraným jedním vrcholem $z$, nazvaným *zdroj*, a jiným vybraným vrcholem $s$, nazvaným *stok*, spolu s nezáporným ohodnocením hran $w : E \to \mathbb{R}$, které představuje *kapacitní omezení*. *Tokem* v síti $S = (V, E, z, s, w)$ rozumíme ohodnocení hran $f : E \to \mathbb{R}$ takové, že součet hodnot u vstupních hran u každého vrcholu $v$, kromě zdroje a stoku, je stejný jako součet u výstupních hran z téhož vrcholu, tj.

$$\sum_{e \in IN(v)} f(e) = \sum_{e \in OUT(v)} f(e).$$

Toto pravidlo se často (s odkazem na fyzikální terminologii) nazývá Kirchhoffův zákon.

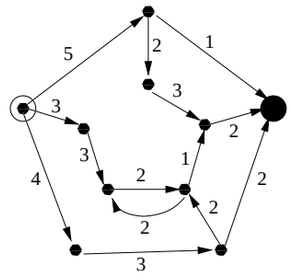
*Velikost toku* $f$ je dána celkovou balancí hodnot u zdroje

$$|f| = \sum_{e \in OUT(z)} f(e) - \sum_{e \in IN(z)} f(e).$$

Z definice je zřejmé, že velikost toku můžeme stejně dobře vypočíst jako hodnotu

$$|f| = \sum_{e \in IN(s)} f(e) - \sum_{e \in OUT(s)} f(e).$$

Na obrázku máme nakreslenu jednoduchou síť se zvýrazněným bílým zdrojem a černým stokem. Součtem maximálních kapacit hran vstupujících do stoku vidíme, že maximální možný tok v této síti je 5.




**12.34. Problém maximálního toku v síti.** Naší úlohou bude pro zadanou síť na grafu $G$ určit maximální možný tok. Na konci minulého odstavce jsme pohledem na obrázek zjistili, že maximální tok v této síti nemůže přesáhnout číslo 5. Podstatné na naší úvaze bylo, že jsme sečetli hodnoty maximálních kapacit u množiny hran, přes které musí jít každá cesta ze $z$ do $s$. Zároveň umíme snadno najít tok, který toto maximum skutečně realizuje (protože je naše síť tak jednoduchá). Tuto rozvahu můžeme zformalizovat takto:

### Řez v síti

*Řezem v síti* $S = (V, E, z, s, w)$ rozumíme takovou množinu hran $C \subseteq E$, že po jejím odebrání nebude v grafu $G = (V, E \setminus C)$

se shodnou v ohodnocení nejvýše $k$ soutěžících. Dokažte, že:

$$\frac{k}{m} \geq \frac{n-1}{2n}.$$

Podívejme se na dva možné přístupy k řešení této úlohy.

**Řešení.** Spočítejme počet $N$ trojic (rozhodčí, rozhodčí, soutěžící), ve kterých jsou rozhodčí různí a hodnotí soutěžícího stejně. Existuje celkem $\binom{n}{2}$ dvojic rozhodčích a každá dvojice hodnotí nejvýše $k$ soutěžících stejným hodnocením, tedy platí $N \leq k\binom{n}{2}$.

Nyní uvažme pevně zvoleného soutěžícího X a spočtěme počet rozhodčích, kteří soutěžícího X hodnotili stejně. Řekněme, že $x$ rozhodčích hodnotilo X jako úspěšného. Potom existuje $\binom{x}{2}$ dvojic, které hodnotily X úspěšně a $\binom{n-x}{2}$, které hodnotily X neúspěšně. Celkově tedy

$$\binom{x}{2} + \binom{n-x}{2} = \frac{x(x-1)}{2} + \frac{(n-x)(n-x-1)}{2}$$

dvojic hodnotí soutěžícího X stejně. Máme:

$$\frac{x(x-1)}{2} + \frac{(n-x)(n-x-1)}{2} = \frac{2x^2 - 2nx + n^2 - n}{2} =$$
$$= \left(x - \frac{n}{2}\right)^2 + \frac{n^2}{4} - \frac{n}{2} \geq \frac{n^2}{4} - \frac{n}{2} = \frac{(n-1)^2}{4} - \frac{1}{4}.$$

Jelikož je $n$ liché, je výraz $(n-1)^2/4$ celé číslo, tedy počet dvojic hodnotících soutěžícího X stejně je nejméně $(n-1)^2/4$. Odtud tedy $N \geq m(n-1)^2/4$. Spojením těchto dvou nerovností tedy získáváme

$$\frac{k}{m} \geq \frac{n-1}{2n}.$$

**Alternativní řešení - pravděpodobnostní metoda.** Zvolme náhodně dva rozhodčí. Nechť $X$ je náhodná veličina, která udává počet případů, kdy se tento pár rozhodčích shoduje v hodnocení. Budeme dokazovat obměnu původního tvrzení, tedy je-li $\frac{k}{m} < \frac{n-1}{2n}$, pak je $X$ větší než $k$ s pravděpodobností větší než nula, což budeme psát $\mathrm{P}(X > k) > 0$.

Mějme náhodné veličiny $X_i$ pro $i = 1, 2, \ldots, m$ nabývající hodnot 0, 1 podle toho, zda $i$-tý soutěžící dostal od obou rozhodčích stejné hodnocení. Nechť $X_i = 1$, když se rozhodčí shodnou a $X_i = 0$ naopak. Odtud pak máme:

$$X = X_1 + X_2 + \cdots + X_m$$

S použitím linearity střední hodnoty získáváme:

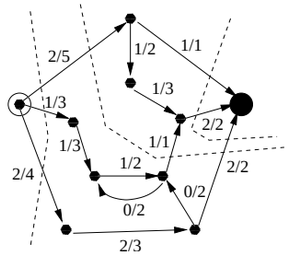
$$E[X] = E[X_1] + E[X_2] + \cdots + E[X_m].$$

Nyní spočteme $E[X_i] = \sum_{x_i \in \{0,1\}} x_i \cdot \mathrm{P}(X_i = x_i)$. Jelikož $X_i$ nabývá pouze hodnot 0 a 1, máme přímo $E[X_i] = \mathrm{P}(X_i = 1)$. Podívejme se na pravděpodobnost $\mathrm{P}(X_i = 1)$, tedy pravděpodobnost, že soutěžící $i$ dostane od obou rozhodčích shodné hodnocení. Existuje $\binom{n}{2}$ možných dvojic rozhodčích. Označme $t_i$ počet rozhodčích, kteří ohodnotí $i$-tého žádná cesta ze zdroje $z$ do stoku $s$. Číslo

$$|C| = \sum_{e \in C} w(e)$$

nazýváme *kapacita řezu C*.

Evidentně platí, že nikdy nemůžeme najít větší tok, než je kapacita kteréhokoliv z řezů. Na dalším obrázku máme zobrazen tok sítí s hodnotou 5 a čárkovanými lomenými čarami jsou naznačeny řezy kapacit 12, 8 a 5.




Ukážeme zde tzv. *Fordův-Fulkersonův algoritmus*[6], který pomocí postupných konstrukcí vhodných cest najde řez s minimální možnou kapacitou a zároveň najde tok, který tuto hodnotu realizuje. Tím dokážeme následující větu:

**Věta.** *Maximální velikost toku v dané síti $S = (V, E, z, s, w)$ je rovna minimální kapacitě řezu v této síti.*

Myšlenka algoritmu je vcelku prostá – prohledáváme cesty mezi vrcholy grafu a snažíme se je „nasytit" co největším tokem. Zavedeme si za tímto účelem následující terminologii. O neorientované cestě v síti $S = (V, E, z, s, w)$ z vrcholu $v$ do vrcholu $w$ řekneme, že je *nenasycená*, jestliže pro všechny hrany této cesty orientované ve směru z $v$ do $w$ platí $f(e) < w(e)$ a pro hrany orientované opačně platí $f(e) > 0$ (někdy též z pochopitelných důvodů – tok budeme nasycovat v „protisměru" hovoříme o *polocestě*, příp. o tzv. zlepšující polocestě). Za *rezervu kapacity* hrany $e$ pak označujeme číslo $w(e) - f(e)$ pro případ hrany orientované ve směru z $v$ do $w$ a číslo $f(e)$ při orientaci opačné. Pro zvolenou cestu bereme za její rezervu kapacity minimální rezervu kapacity jejích hran.

### Fordův-Fulkersonův algoritmus

Vstupem algoritmu je síť $S = (V, E, z, s, w)$ a výstupem maximální možný tok $f : E \to \mathbb{R}$. Pro zjednodušení úvah budeme předpokládat, že všechny kapacity hran jsou dány racionálními čísly.

- *Iniciace:* Zadáme $f(e) = 0$ pro všechny hrany $e \in E$ a prohledáváním do hloubky z vrcholu $z$ najdeme množinu vrcholů $U \subseteq V$, do kterých existuje nenasycená cesta.
- *Hlavní cyklus:* Dokud $s \in U$, opakujeme
  - zvolíme nenasycenou cestu $P$ ze zdroje $z$ do $s$ a zvětšíme tok $f$ u všech hran této cesty o její minimální rezervu;
  - obnovíme $U$.
- Výstupem je (maximální) tok $f$ a minimální řez $C$ tvořený všemi hranami vycházejícími z $U$ a končícími ve $V \setminus U$.

[6] Ford, L. R.; Fulkerson, D. R. (1956). "Maximal flow through a network". Canadian Journal of Mathematics 8: 399–404.

soutěžícího kladně a $n - t_i$ počet rozhodčích, kteří ohodnotí $i$-tého soutěžícího záporně. Počet dvojic úspěšných hodnocení je pak $\binom{t_i}{2}$ a počet dvojic neúspěšných hodnocení je $\binom{n-t_i}{2}$, z toho plyne, že počet shodných hodnocení soutěžícího $i$ je $\binom{t_i}{2} + \binom{n-t_i}{2}$. A tedy:

$$E[X_i] = \mathrm{P}(X_i = 1) = \frac{\binom{t_i}{2} + \binom{n-t_i}{2}}{\binom{n}{2}}.$$

Odtud získáváme:

$$E[X] = \sum_{i=1}^{m} \frac{\binom{t_i}{2} + \binom{n-t_i}{2}}{\binom{n}{2}}.$$

Ukážeme, že pro lichá $n$ platí nerovnost $\binom{t_i}{2} + \binom{n-t_i}{2} \geq \frac{(n-1)^2}{4}$. Upravením nerovnosti získáme

$$(n - 2t_i)^2 \geq 1 \;\Leftrightarrow\; t_i \leq \frac{n-1}{2} \;\text{ nebo }\; t_i \geq \frac{n+1}{2},$$

což zřejmě platí, neboť $\frac{n-1}{2}$ a $\frac{n+1}{2}$ jsou dvě po sobě jdoucí čísla.

S použitím nerovnosti $\binom{t_i}{2} + \binom{n-t_i}{2} \geq \frac{(n-1)^2}{4}$ získáváme:

$$E[X] \geq m \frac{\left(\frac{n-1}{2}\right)^2}{\frac{n(n-1)}{2}} = \frac{m(n-1)}{2n}.$$

Díky předpokladu $\frac{m(n-1)}{2n} > k$ nyní máme $E[X] > k$, tedy $\mathrm{P}(X > k) > 0$ a jsme s důkazem hotovi. □

Dále ukážeme využití pravděpodobnostní metody při řešení zajímavého problému.

**12.57.** Buď $S$ konečná množina bodů v rovině taková, že žádné tři z nich neleží v přímce. Nechť pro libovolný konvexní mnohoúhelník $P$, jehož vrcholy jsou v $S$, značí $a(P)$ počet vrcholů $P$ a $b(P)$ počet bodů z $S$, které neleží v $P$. Dokažte, že pro libovolné reálné číslo $x$ platí

$$\sum_{P} x^{a(P)} (1-x)^{b(P)} = 1,$$

kde sčítáme přes všechny konvexní mnohoúhelníky s vrcholy v $S$.

(Úsečku, resp. bod, resp. prázdnou množinu považujeme za konvexní mnohoúhelníky se dvěma, resp. jedním, resp. žádným vrcholem.)

**Řešení.** Nejprve dokážeme uvedenou rovnost pro $x \in [0,1]$. Obarvěme vrchol z množiny $S$ s pravděpodobností $x$ na bílo a s pravděpodobností $1-x$ na černo (neboli uvažme náhodný výběr velikosti $|S|$ s binomickým rozdělením pravděpodobnosti $\mathrm{Bi}(n,x)$) a řekněme, že zdar odpovídá bílé barvě, nezdar černé). Všimněme si, že při libovolném obarvení bude vždy existovat mnohoúhelník takový, že všechny jeho vrcholy jsou bílé a všechny body mimo něj jsou černé (jde o hranici konvexního obalu bíle obarvených bodů). Z předchozí úvahy víme, že pravděpodobnost, že v tomto náhodném výběru bude

**Důkaz správnosti algoritmu.** Jak jsme viděli, velikost každého toku je nejvýše rovna kapacitě kteréhokoliv řezu. Stačí nám tedy ukázat, že v okamžiku zastavení algoritmu jsme vygenerovali řez i tok se stejnou hodnotou.

Algoritmus se zastaví při prvním případu, kdy neexistuje nenasycená cesta ze zdroje $z$ do stoku $s$. To znamená, že $U$ neobsahuje $s$ a pro všechny hrany $e$ z $U$ do zbytku je $f(e) = w(e)$, jinak bychom museli koncový vrchol $e$ přidat k $U$.

Zároveň ze stejného důvodu všechny hrany $e$, které začínají v komplementu $V \setminus U$ a končí v $U$, musí mít tok $f(e) = 0$.

Pro velikost toku celé sítě jistě platí

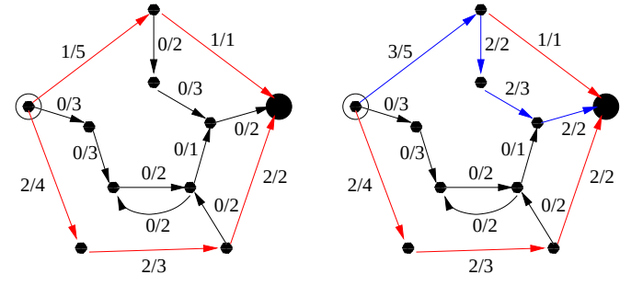
$$|f| = \sum_{\text{hrany z } U \text{ do } V\setminus U} f(e) \;-\; \sum_{\text{hrany z } V\setminus U \text{ do } U} f(e).$$

Tento výraz je ovšem v okamžiku zastavení roven

$$\sum_{\text{hrany z } U \text{ do } V\setminus U} f(e) \;=\; \sum_{\text{hrany z } U \text{ do } V\setminus U} w(e) = |C|,$$

což jsme chtěli dokázat.

Zbývá ovšem ukázat, že algoritmus skutečně zastaví. Protože předpokládáme, že ocenění hran je dáno racionálními čísly, můžeme (celočíselnou změnou měřítka) rovnou předpokládat, že jsou všechna ocenění maximálních kapacit celočíselná. Je zřejmé, že pro celočíselné hodnoty ohodnocení hran dostáváme během chodu algoritmu stále celočíselné toky. Při každém průchodu hlavním cyklem ovšem tok zvyšujeme. Protože ale každý řez dává omezení možného toku shora, musí se algoritmus po konečném počtu kroků zastavit.




Chod algoritmu je ilustrován na obrázku. Vlevo jsou vyšeděny dvě nejkratší nenasycené cesty ze zdroje do stoku (horní má dvě hrany, spodní tři). Napravo je pak nasycena další cesta v pořadí (v nejhornější jdeme první možnou odbočkou) a je také šedá. Je nyní zjevné, že nemůže existovat další nenasycená cesta ze zdroje do stoku. Proto algoritmus v tomto okamžiku skončí.

**12.35. Poznámky k algoritmu.** Naše úloha připouští i další podmínky. Můžeme např. požadovat dodržení maximální kapacity průtoku přes jednotlivé vrcholy. Nebo můžeme chtít dodržet nejen maximální, ale také minimální toky přes jednotlivé hrany či vrcholy.



Přidání kapacit vrcholů je jednoduché – prostě vrcholy zdvojíme a dvojčata označující vstup do vrcholu a výstup z vrcholu spojíme právě jednou hranou s příslušnou kapacitou.

Omezení minimálními průtoky lze zahrnout do iniciace našeho algoritmu. Je ovšem zapotřebí otestovat, jestli takový tok vůbec existuje. V literatuře lze najít řadu dalších nuancí, nebudeme se jim zde věnovat.

Všimněme si však, že se náš algoritmus nemusí nutně zastavit, pokud připustíme iracionální maximální kapacity hran. Dokonce

realizován konvexní mnohoúhelník, jehož všechny vrcholy budou bílé a všechny vrcholy vně něj černé, je rovna jedné. Spočítejme však tuto pravděpodobnost i jiným způsobem. Jev, že nějaký mnohoúhelník bude mít požadovanou vlastnost, je totiž sjednocením $k$ disjunktních jevů, kde $k$ je počet konvexních mnohoúhelníků, totiž že daný konkrétní mnohoúhelník bude mít uvažovanou vlastnost (rozmyslete si, že zkoumanou vlastnost nemohou mít dva různé konvexní mnohoúhelníky). Pro každý konkrétní mnohoúhelník $P$ je pravděpodobnost toho, že jeho vrcholy budou obarveny na bílo a všechny body ležící vně něj rovna $x^{a(P)}(1-x)^{b(P)}$, kde $a(P)$ je počet vrcholů $P$ a $b(P)$ je počet bodů ležících vně něj. Pravděpodobnost sjednocení disjunktních jevů je pak rovna součtu pravděpodobností jednotlivých jevů, tedy

$$\sum_P x^{a(P)}(1-x)^{b(P)} = 1.$$

Tím je rovnost dokázána pro čísla z intervalu $[0, 1]$. Toto však můžeme interpretovat tak, že libovolné číslo z intervalu $[0, 1]$ je kořenem polynomu $\sum_P x^{a(P)}(1-x)^{b(P)} - 1$. Jak ale víme, nenulový polynom nad (nekonečným) tělesem reálných čísel může mít pouze konečně mnoho kořenů (viz 11.19). Polynom $\sum_P x^{a(P)}(1-x)^{b(P)} - 1$ je tedy nulový polynom a rovnost $\sum_P x^{a(P)}(1-x)^{b(P)} = 1$ platí pro libovolné reálné číslo $x$. □

**Poznámka.** Daná rovnost platí, i pokud čísla $a(P)$ a $b(P)$ definujeme jinak: definice $a(P)$ zůstává, $b(P)$ však bude značit počet bodů z $S$, které nejsou vrcholy $P$. Bylo by tedy $a(P)+b(P) = |S|$. Daná rovnost by potom byla důsledkem binomické věty pro dvojčlen $(x+(1-x))^{|S|}$.

**12.58.** Soutěž $n$ hráčů nazýváme $(n, k)$ turnajem, jestliže se hraje v $k$ kolech a navíc splňuje následující podmínky:

i) každý hráč hraje v každém kole a libovolní dva hráči se střetnou nejvýše jednou,

ii) jestliže se hráč $A$ utká s hráčem $B$ v $i$-tém kole, hráč $C$ se v $i$-tém kole utká s hráčem $D$ a hráč $A$ se utká s hráčem $C$ v $j$-tém kole, pak se hráč $B$ v $j$-tém kole utká s hráčem $D$.

Určete všechny dvojice $(n, k)$, pro které existuje $(n, k)$ turnaj.

**Řešení.** Vyhovují všechny dvojice $(n, k)$, kde $2^{\lceil \log_2(k+1) \rceil}$ dělí číslo $n$. Nejprve ukažme, že všechny takové dvojice vyhovují: sestrojíme turnaj $(2^t, k)$, kde $k \leq 2^t - 1$ (obecný případ $2^t \mid n$ z tohoto následně snadno odvodíme). Tohoto turnaje se tedy účastní $2^t$ hráčů. Každému hráči přiřaďme (jedinečnou) posloupnost délky $t$ složenou z nul a jedniček (těchto posloupností je $2^t$, toto přiřazení je tedy možné). V $i$-tém kole necháme hrát hráče $\alpha$ s hráčem $\alpha \oplus \omega(i)$, kde $\omega(i)$ je binární rozvoj čísla $i$, případně doplněný do délky $t$ nulami na začátku (uvedená dvě nemusí dosahované toky ani konvergovat k optimálnímu řešení. V každém případě je ale stále v pořádku ta část důkazu z předchozího odstavce, která ověřila, že v případě zastavení algoritmu je dosažen maximální možný tok.

V případě celočíselných ohodnocení lze dobu chodu algoritmu odhadnout výrazem $O(f|E|)$, kde $f$ je maximální tok v síti a $|E|$ je počet hran (uvědomme si, že v nejhorším budeme v každém kroku zvětšovat dosažený tok o jedničku).

V důkazu správnosti algoritmu jsme explicitně nevyužili zvolený způsob prohledávání grafu při hledání nenasycené cesty. Jinou variantou k Fordově–Fulkersonově algoritmu je tedy volba prohledávání do šířky. Tuto variantu využívá tzv. Edmondsův–Karpův algoritmus, který má zaručené zastavení v čase $O(|V||E|^2)$.[7] Moderními, výrazně efektivnějšími algoritmy, jsou pak Diničův algoritmus, který zjednodušuje hledání nenasycené cesty konstrukcí tzv. *úrovňového grafu*, kdy *zlepšující hrany* uvažujeme pouze tehdy, pokud vedou mezi vrcholy různých vzdáleností od zdroje. Složitost tohoto algoritmu je $O(|V|^2|E|)$, což je u hustých grafů významné vylepšení oproti složitosti algoritmu Edmondse-Karpa.

**12.36. Další úlohy na toky v sítích.** Hezkým využitím toků v sítích je řešení úlohy *bipartitního párování*. Úlohou je v bipartitním grafu najít maximální párování, tedy maximální podmnožinu hran takovou, aby žádné dvě hrany nesdílely vrchol.

Jde o abstraktní variantu docela obvyklé úlohy – třeba spárování kluků a holek k tanci v tanečních, kdybychom měli předem známé možnosti, ze kterých vybíráme.

Tento problém snadno převedeme na hledání maximálního toku. Přidáme si uměle navíc ke grafu zdroj, který propojíme hranami jdoucími do všech vrcholů v jedné skupině v bipartitním grafu, zatímco ze všech vrcholů ve druhé skupině vedeme hranu do přidaného stoku. Všechny hrany opatříme maximální kapacitou 1 a hledáme maximální tok. Za páry pak bereme hrany s nenulovým tokem.



Jiným významným využitím toků je důkaz tzv. Mengerovy věty (uvedli jsme ji jako tvrzení v 12.12). Můžeme se na ně dívat takto: V orientovaném grafu ohodnotíme všechny hrany $e$ maximální kapacitou 1 a totéž pro všechny vrcholy. Dále si zvolíme libovolnou dvojici vrcholů $v$ a $w$, které považujeme za zdroj a stok. Jestliže nás pak zajímá tok tímto grafem, dostaneme právě počet zcela různých cest z $v$ do $w$ (hrany i vrcholy jsou různé kromě začátku a konce). Každý řez přitom odděluje $v$ a $w$ do různých souvislých komponent zbylého grafu. Ze skutečnosti, že kapacita minimálního řezu je rovna hodnotě toku v síti, nyní vyplývá požadované tvrzení.

**12.37. Stromy her.** Obrátíme teď naši pozornost k velice rozšířeným užitím stromových struktur při analýzách možných strategií nebo postupů. Zcela jistě se s nimi setkáme v teorii umělé inteligence a v části teorie her. Své místo ale mají také v ekonomii a mnoha dalších oblastech lidských činností.



[7] Edmonds, Jack; Karp, Richard M. (1972). "Theoretical improvements in algorithmic efficiency for network flow problems". Journal of the ACM (Association for Computing Machinery) 19 (2): 248–264. doi:10.1145/321694.321699.

binární čísla $\alpha$ a $\omega(i)$ sčítáme pomocí operace $\oplus$, což je tzv. binární XOR, neboli sčítání číslic modulo 2).Tento rozvrh zápasů je korektní, neboť potom každý hráč hraje v každém kole, různí hráči mají různé oponenty (pro $\alpha \neq \beta$ je $\alpha+\omega(i) \neq \beta+\omega(i)$) a oponent hráče $\alpha$ hraje skutečně podle tohoto rozpisu s hráčem $\alpha$ (neboť $(\alpha+\omega(i))+\omega(i) = \alpha$). Navíc je také splněna podmínka ze zadání: pokud v $i$-tém kole hraje hráč $\alpha$ s hráčem $\beta$ a hráč $\gamma$ s hráčem $\delta$, tedy pokud $\beta = \alpha + \omega(i)$ a $\delta = \gamma + \omega(i)$, tak je-li v $j$-tém kole soupeřem hráče $\alpha$ hráč $\gamma$, tedy $\gamma = \alpha + \omega(j)$, pak také $\beta + \omega(j) = (\alpha + \omega(i)) + \omega(j) = (\alpha + \omega(j)) + \omega(i) = \gamma + \omega(i) = \delta$, tedy hráči $\beta$ a $\delta$ se střetnou v $j$-tém kole. Libovolný $(2^t \cdot s, k)$, kde $s$ je liché, pak dostaneme jako $s$ paralelně hraných $(2^t, k)$ turnajů.

Nyní ukážeme, že podmínka $2^{\lceil \log_2(k+1) \rceil} \mid n$ je i nutná. Uvažme graf $G_i$, jehož vrcholy jednoznačně odpovídají hráčům v turnaji a hrany odehraným zápasům do $i$-tého kola včetně. Nejprve uvažme hráče $A$ a $B$, kteří spolu hrají v $(i+1)$. kole. Ukážeme, že pak $|\Gamma| = |\Delta|$, kde $\Gamma$ je komponenta hráče $A$ v grafu $G_i$ a $\Delta$ komponenta hráče $B$ v $G_i$ a to tak, že dokážeme, že libovolný hráč z $\Gamma$ se utká s některým hráčem z $\Delta$ v $(i+1)$. kole. Nechť tedy $C \in \Gamma$, tj. v $G_i$ existuje cesta $A = X_1, X_2, \ldots, X_m = C$ taková, že $X_j$ hrál s $X_{j+1}$, $j = 1, \ldots, m-1$, v některém z prvních $i$ kol. Uvažme posloupnost $Y_1, Y_2, \ldots Y_m$, kde $Y_k$ je soupeř $X_k$ v (i+1). kole, $k = 1, \ldots, m$ (tedy $Y_1 = B$). Potom pro libovolné $1 \leq m-1$ se v $(i+1)$. kole utkal hráč $X_j$ s hráčem $Y_j$, hráč $X_{j+1}$ s hráčem $Y_{j+1}$ (podle definice posloupnosti $Y_1, \ldots, Y_i$) a v jistém $r$-tém kole ($1 \leq r \leq i$) se utkali hráči $X_j$ a $X_{j+1}$ (podle definice posloupnosti $X_1, \ldots, X_i$) Podle druhé podmínky ze zadání to však znamená, že hráč $Y_j$ se utkal s hráčem $Y_{j+1}$ rovněž v $r$-tém kole, tedy $Y_jY_{j+1}$ je hrana v $G_i$ pro libovolné $1 \leq j \leq m-1$, tudíž $Y_1, Y_2, \ldots Y_m$ je cestou v $G_i$, takže $B = Y_1$ a $Y_m$ leží ve stejné komponentě, tedy v $\Delta$. Ze symetrie předcházející úvahy vyplývá, že také libovolný hráč z $\Delta$ hrál v $(i+1)$. kole s nějakým hráčem z $\Gamma$, a protože každý hráč hrál v daném kole právě jednou, je $|\Gamma| = |\Delta|$. Z definice komponent je komponenta hráče $A$ v grafu $G_{i+1}$ rovna $\Gamma \cup \Delta$. Potom opět z definice komponent buď $\Gamma = \Delta$ (v tom případě bude komponenta hráče $A$ v grafu $G_{i+1}$ rovna $\Gamma$), nebo $\Gamma \cap \Delta = \emptyset$ (v tomto případě bude komponenta hráče $A$ v grafu $G_{i+1}$ rovna $\Gamma \cup \Delta$). Celkem zůstane velikost komponenty hráče $A$ stejná, nebo se zvětší na dvojnásobek. Uvažme nyní posloupnost komponent $\Gamma_1, \Gamma_2, \ldots, \Gamma_k$ hráče $A$ v grafech $G_1, G_2, \ldots G_k$. Máme $|\Gamma_1| = 2$ (v prvním kole měl hráč $A$ jednoho protivníka) a pro $1 \leq i \leq k-1$ máme z předchozího, že buď $|\Gamma_i| = |\Gamma_{i+1}|$, nebo $2|\Gamma_i| = |\Gamma_{i+1}|$. Je tedy počet vrcholů (hráčů) v každé z uvedených komponent mocninou čísla 2, tedy $|\Gamma_k| = 2^l$, pro nějaké $l$ a $\Gamma_k \geq k+1$ (hráč $A$ hrál v $k$ kolech s různými hráči), tedy

Budeme v této souvislosti hovořit o *hrách*. V matematickém smyslu se teorie her zabývá modely, ve kterých jeden nebo více partnerů činí kroky podle předem známých pravidel a většinou také ve předem známém pořadí. Většinou se možné kroky nebo úkony ohodnocují nějakými výnosy nebo ztrátami pro daného partnera. Smyslem je pak nalezení *strategie hráče*, tj. algoritmického postupu, podle kterého může hráč maximalizovat výnos, případně minimalizovat ztrátu.

Budeme se zabývat tzv. extenzivním popisem her. To je takový popis, kdy máme k dispozici úplnou a konečnou analýzu všech možných stavů hry a výsledná analýza zadává skutečně přesnou rozvahu o výnosech či ztrátách za předpokladu nejlepšího možného chování zúčastněných partnerů. *Strom hry* je kořenový strom, který má za vrcholy všechny možné stavy hry, a tyto vrcholy budou označeny podle toho, který z hráčů je zrovna na tahu. Hrany budou všechny možné tahy daného hráče v daném stavu. Takový úplný popis pomocí stromu můžeme konstruovat pro běžné hry jako jsou piškvorky, šachy, apod.

Jako jednoduchý příklad uveďme jednoduchou variantu hry *Nim*.[8]

Na stole leží na jedné hromádce $k$ sirek, kde $k > 1$ je přirozené číslo, a hráči postupně odebírají každý jednu nebo dvě sirky. V normální variantě hry vyhraje ten, kdo jako poslední má co vzít. Ve variantě hry „na žebráka“ naopak prohrává ten, kdo vzal všechny zbývající sirky. Strom takové hry, včetně všech potřebných informací můžeme sestrojit následovně:

- Stavu s $\ell$ sirkami na stole a s prvním hráčem na tahu odpovídá podstrom s kořenem označeným $F_\ell$, stavu s týmž počtem sirek a druhým hráčem na tahu odpovídá podstrom s kořenem $S_\ell$.
- Vrchol $F_\ell$ má levého syna $S_{\ell-1}$ a pravého syna $S_{\ell-2}$, u vrcholu $S_\ell$ jsou to obdobně synové $F_{\ell-1}$ a $F_{\ell-2}$.
- Listy jsou vždy buď $F_0$ nebo $S_0$ (při normálním režimu hry; při hře na žebráka by to byly stavy $F_1$ a $S_1$, ve kterých příslušný hráč prohrál).

Každý průběh hrou začínající v kořenu $F_k$ odpovídá právě jednomu listu výsledného stromu. Je tedy vidět, že celkový počet $p(k)$ možných her pro $F_k$ je roven

$$p(k) = p(k-1) + p(k-2)$$

pro $k \geq 3$ a snadno vidíme, že $p(1) = 1$ a $p(2) = 2$. Takovou diferenční rovnici jsme už řešili. Jejím řešením jsou tzv. Fibonacciova čísla a umíme pro ně najít explicitní formuli, viz odstavec o vytvořujících funkcích nebo část o diferenčních rovnicích ve čtvrté kapitole. Známe proto i formuli pro počet možných průběhů her. Počet možných stavů hry je přitom roven počtu všech vrcholů ve stromu. Hra přitom vždy skončí výhrou buď prvního nebo druhého hráče. U podobných her může kromě toho hra končit také remízou.

**12.38. Analýza hry.** Připravená stromová struktura nám teď snadno umožní analyzovat hru tak, abychom mohli sestavit skutečně algoritmickou strategii pro každého hráče. Je k tomu jednoduchý rekurzivní postup pro ohodnocení kořene podstromu. Budeme označovat jako $W$ vrcholy, ve kterých (při optimální strategii obou) vítězí první hráč, a $L$ v případě opačném, případně ještě můžeme značit jako $T$ vrcholy stromu odpovídající remíze (z anglického „win“



[8] Název zavedl patrně Charles Bouton ve své analýze těchto her z roku 1901. Prý pochází z německého „Nimm!“, což česky znamená „Ber!“.

$2^l \geq k+1$, neboli $2^l$ je alespoň $2^{\lceil \log_2(k+1) \rceil}$, takže počet hráčů v každé komponentě je dělitelný $2^{\lceil \log_2(k+1) \rceil}$, tudíž je tímto číslem dělitelné i číslo $n$. □

### H. Kombinatorické hry

**12.59.** Uvažme hru dvou hráčů. Na stole jsou čtyři hromádky sirek, o 9, 10, 11 a 14 sirkách. V tahu je nutné provést následující akcí: z jedné libovolně zvolené hromádky odebrat libovolný nenulový počet sirek. Hráči se střídají na tazích a kdo nemůže táhnout prohrál. Existuje výherní strategie za některého z hráčů? (prvního či druhého)

**Řešení.** Uvědomme si, že se jedná o součet čtyř her: každá z nich odpovídá hře s jednou hromádkou, ze které můžeme odebírat libovolný počet sirek (operace součtu her je asociativní, takže můžeme mluvit o součtu libovolného počtu her – aniž bychom určili pořadí sčítání). Zcela jednoduše zjistíme, že hodnota Sprague-Grundyovy funkce (dále jen *SG*-hodnota) počáteční pozice těchto her je rovna počtu sirek v hromádce (Indukcí: nechť mám na hromádce $n$ sirek a *SG* hodnota hry s $k$ sirkami pro $k < n$ je $k$. Z počáteční pozice se lze vhodným tahem dostat do libovolné jiné pozice, podle indukčního předpokladu jsou *SG* hodnoty ostatních stavů ve hře rovny počtu sirek, tedy *SG*-hodnoty ostatních stavů prochází podle indukčního předpokladu všechna čísla od nuly do $n-1$ a z definice *SG* funkce je tak *SG*-hodnota počáteční pozice právě $n$. Podle věty z odstavce 12.39 je hodnota počáteční pozice v naší hře rovna součtu počátečních pozic v jednotlivých sčítaných hrách, tedy

$$9 \oplus 10 \oplus 11 \oplus 14 = 6,$$

protože je hodnota nenulová, existuje výherní strategie za prvního hráče: táhne vždy do stavu s hodnotou nula — podle definice *SG* taková pozice vždy existuje. Například první tah by byl z hromádky o čtrnácti sirkách vzít šest sirek (vybíráme z hromádky, která má *SG* hodnotu takovou, že na prvním místě zleva v jejím binárním zápisu, kde se vyskytuje jednička v *SG* hodnotě aktuální pozice, má rovněž jedničku — změníme tuto jedničku na nulu a ostatní pozice upravíme do sudé parity). □

**12.60.** Uvažme následující hru dvou hráčů: na stole je jedna hromádka sirek. V tahu hráč buď odebere libovolný počet sirek z jedné libovolně vybrané hromádky, nebo nějakou hromádku rozdělí na dvě neprázdné hromádky. Hráči se střídají na tazích a kdo nemůže táhnout, prohrál. Určete *SG*-hodnotu počáteční pozice této hry začínající s hromádkou o $n$ sirkách.

a „lose“ z pohledu prvého hráče, znak $T$ odpovídá anglickému „tie“). Postup je tento:

(1) Listy označíme buď $W$ nebo $L$, případně $T$, podle pravidel hry (u normálního průběhu naší varianty Nim to tedy bude $W$ pro $S_0$ a $L$ pro $F_0$).
(2) Vrchol $F_\ell$ označíme $W$, jestliže existuje syn, který je $W$. Pokud takový syn neexistuje, ale mezi syny existuje vrchol s označením $T$, bude i označovaný vrchol $T$. Ve zbývajícím případě, kdy jsou všichni synové $L$, bude i tento vrchol $L$.
(3) Vrchol $S_\ell$ označíme $L$, jestliže existuje syn označený $L$. Pokud takový syn neexistuje, ale mezi syny existuje vrchol s označením $T$, bude i označovaný vrchol $T$. Ve zbývajícím případě, kdy jsou všichni synové $W$, bude i tento vrchol $W$.

Voláním této procedury na kořen stromu obdržíme ohodnocení všech vrcholů a tím také i strategii pro každého z hráčů:

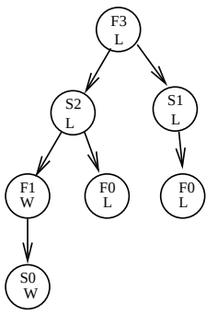
- První hráč se snaží v každém svém kroku přesunout do vrcholu označeném $W$, pokud to ale nejde, hledá alespoň $T$.
- Druhý hráč se snaží v každém svém kroku dostat hru do vrcholu označeného $L$, pokud to nejde, hledá alespoň $T$.

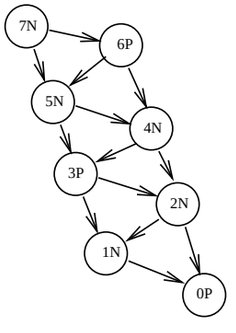
Hloubka rekurze je dána hloubkou stromu. Např. u našeho Nim s $k$ sirkami je to právě $k$.

Získaná analýza ještě není příliš užitečná. Pro její užití v uvedené formě totiž potřebujeme mít k dispozici celý strom hry a to je obecně skutečně velice mnoho dat (u minipiškvorek na hřišti $3 \times 3$ má příslušný strom jednotlivé desítky tisíc vrcholů). Zpravidla se v takovéto podobě používá analýza pomocí stromové struktury tehdy, když zkoumáme pouze malý úsek celého stromu pomocí vhodných heuristických metod a tento kousek si naopak dynamicky utváříme během hry. To je fascinující oblast moderní teorie umělé inteligence, my se jí zde ale nebudeme věnovat.



Pro naše potřeby úplné formální analýzy ale umíme najít kompaktnější vyjádření stromové struktury grafu. Pokud si nakreslíme náš strom pro hru Nim, okamžitě vidíme, že se nám mnohokráte opakují pořád ty stejné situace hry v různých listech, a to podle toho, jaká byla historie hry. Ve skutečnosti jsou ale strategie určeny pouze počtem zbývajících sirek a tím, kdo je na tahu. Můžeme proto stejnou hru popsat pomocí grafu, který bude mít za vrcholy počty zbývajících sirek a celá strategie bude zadána určením, jestli v dané situaci vyhrává ten, kdo je na tahu nebo naopak ten, kdo táhl předtím. K popisu možných tahů budeme používat orientované hrany.



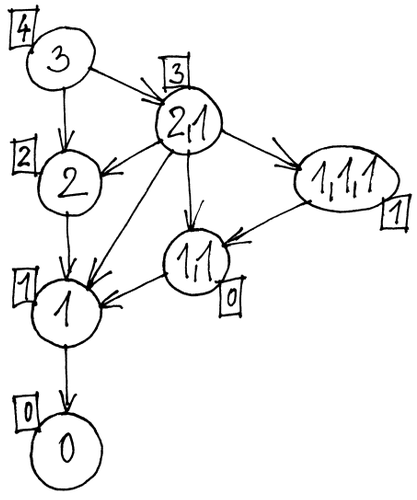




Příklad pro naši hru Nim je na obrázku. Nalevo je úplný strom pro hru se třemi sirkami, napravo je orientovaný graf zobrazující hru se sedmi sirkami. Úplný strom pro hru se sedmi sirkami by měl již 21 listů a počet listů roste exponenciálně s počtem sirek.

**Řešení.** Indukcí dokážeme pro kladná celá $k$ následující předpis:

$$\begin{aligned} g(4k+1) &= g(4k+1) \\ g(4k+2) &= g(4k+2) \\ g(4k+3) &= g(4k+4) \\ g(4k+4) &= g(4k+3) \end{aligned}$$

Zjevně $g(0) = 0$ (na obrázku jsme odvodili hodnotu $SG$ funkce pro pozice s jednou hromádkou o jedné, dvou a třech sirkách; je zřejmé, že obecně bychom tuto hodnotu těžko odvozovali).




Dále budeme postupovat tak, že nejprve budeme předpokládat, že uvedený předpis platí pro všechna čísla menší než $4k+1$, dokážeme, že platí i pro $4k+1$. $SG$-hodnota dané pozice ve hře je dána podle definice jako nejmenší přirozené číslo takové, že neexistuje tah do pozice s touto $SG$-hodnotou. Navíc je Sprague-Grundyho funkce touto vlastností a tím, že koncové pozice mají hodnotu nula, určena jednoznačně. Stačí tedy dokázat, že pro každé číslo $l < 4k+1$ vede z dané pozice tah do pozice s $SG$-hodnotou $l$ a že neexistuje tah do pozice s $SG$-hodnotou $4k+1$. Je zřejmé, že vedou tahy do pozic s hodnotami nižšími než $4k+1$. Všechny tyto hodnoty (i když ne popořadě) mají totiž pozice s jednou hromádkou s menším počtem sirek a do těchto pozic vede tah. Nyní ukážeme, že nelze udělat tah do pozice s $SG$-hodnotou $4k+1$: tahy vedoucí mimo pozice s jednou hromádkou (tam $SG$-hodnotu $4k+1$ nenajdeme) jsou tahy do pozic se dvěma neprázdnými hromádkami, jejichž součet sirek je $4k+1$. Podíváme se na zbytky možných počtů sirek v jednotlivých hromádkách po dělení čtyřmi. Jsou dvě možnosti: v jedné hromádce je počet sirek dělitelný čtyřmi, v druhé dává zbytek jedna, nebo v jedné hromádce dává zbytek dva, ve druhé tři. V prvním případě je $SG$ hodnota jednotlivých

Orientovaný acyklický graf na pravé straně obrázku má pro každý počet sirek právě jeden vrchol a ten zároveň nese označení, zda při jeho průchodu celkově vyhraje ten, kdo je zrovna na řadě (písmeno $N$ od „next“), nebo ten druhý (písmeno $P$ od slova „previous“). Celkově je v něm vždy jen $k+1$ vrcholů pro hru s $k$ sirkami. Zároveň v sobě graf uschovává kompletní strategii: pokud z vrcholu, ve kterém se hráč nachází, vychází hrana končící ve vrcholu s označením $P$, hráč použije tento tah.

Naopak každý acyklický orientovaný graf můžeme považovat za popis hry. Výchozími situacemi jsou v ní ty vrcholy, do kterých nevedou žádné hrany (jeden nebo více), hra končí v listech (opět jeden nebo více). Strategii hry obdržíme opět jednoduchou rekurzivně volanou procedurou (pro zjednodušení nyní uvádíme pouze případy her bez remíz):

- Listy označíme písmenem $P$ (skutečně prohrává ten, kdo je na tahu a nachází se v listu).
- Vrchol grafu označíme jako $N$, pokud z něj vede hrana do vrcholu označeného jako $P$. V opačném případě označíme vrchol jako $P$.

V našem speciálním případě hry Nim je tedy situace obzvláště jednoduchá. Z uvedené strategie vyplývá, že hráč, který je na tahu, prohrává, pokud je počet sirek dělitelný třemi, a vyhrává ve zbylých dvou případech zbytků 1 a 2.

Hry, které umíme reprezentovat výše uvedeným způsobem pomocí acyklického orientovaného grafu, nazýváme *nestranné*. Jde právě o takové hry, ve kterých

- v každé herní situaci mají oba hráči stejné možnosti tahů;
- hra má konečný celkový počet herních situací;
- hra má tzv. nulový součet, tj. lze její výsledek formulovat pomocí výhry jednoho (a tím prohry druhého) hráče, resp. remízy.

Příkladem nestranné hry jsou např. piškvorky na předem známém rozměru použité čtverečkové sítě. Zde sice hráči používají různé symboly, podstatné ale je, že je mohou umístit do kteréhokoliv dosud neobsazeného pole. Naopak šachy nestrannou hrou v tomto smyslu nejsou, protože možné tahy jednotlivých hráčů jsou v každé situaci silně závislé od množství figurek, které ještě mají k dispozici.

**12.39. Součet kombinatorických her.** Klasická hra Nim se hrává poněkud složitěji. Hráči mají před sebou tři hromádky sirek (nebo jiných objektů), každou o daném počtu $k$. Ten, kdo je na řadě, může brát libovolný počet sirek, ale pouze z jedné hromádky. Při normální hře vyhrává ten, kdo bere naposled (při hře na žebráka takový hráč naopak prohrává). Pokud bychom takto hráli s jednou hromádkou, je to jednoduché. První hráč shrábne vše a druhý prohrál. Se třemi to ovšem tak snadno nepůjde. Zároveň nejspíš budeme zvědaví, zda bude znalost analýzy možností pro jednu hromádku nějak užitečná pro kombinovanou složitější hru.



Zavedeme si k tomu účelu nový koncept, tzv. *součet nestranných her*. Věcně to bude tak, že situace ve hře kombinované ze dvou současných her budou uspořádané dvojice jednotlivých možných situací. Tahem pak rozumíme využití možného tahu v jedné z her (a druhá zůstane nezměněna). Půjde tedy o operaci, která dvěma našim acyklickým grafům přiřadí nový acyklický graf. Pro dva acyklické grafy $G_1 = (V_1, E_1)$ a $G_2 = (V_2, E_2)$ je jejich

hromádek dle indukčního předpokladu $4a-1$ a $4b$ (počty sirek v hromádkách jsou nenulové a menší než $4k+1$, takže indukční předpoklad můžeme použít) a pokud si uvědomíme že hra se dvěma hromádkami je součtem her s jednou hromádkou, pak víme, že *SG* hodnota pozice se dvěma hromádkami je rovna nim-součtu *SG* hodnot jednotlivých hromádek v této hře. V prvním případě dostaneme nim-součtem čísel dávajících zbytek tři a nula číslo dávající zbytek tři po dělení čtyřmi (uvažte poslední dva bity čísel), obdobně pro hromádky o $4a+2$ a $4b+3$ sirkách je nim-součet jejich *SG* hodnot ($4a+2$ a $4b+4$) dokonce sudý. V žádném případě není tvaru $4k+1$. Tím je dokázán indukční krok pro přirozená čísla tvaru $4k+1$.

Pro přirozená čísla tvaru $4k+2$ je důkaz indukčního kroku naprosto analogický. Pro čísla tvaru $4k+3$ je trošičku zajímavější: *SG*-hodnoty pozic s jednou hromádkou, do kterých vede tah, tedy těch s menším počtem sirek, vyčerpávají podle indukčního předpokladu pouze čísla do $4k+2$. *SG*-hodnotu $4k+3$ má však pozice se dvěma hromádkami, jedna s jednou sirkou, druhá s $4k+2$ sirkami. Podle indukčního předpokladu jsou *SG* hodnoty hromádky s jednou sirkou jedna a hromádky s $4k+2$ sirkami rovny jedné a $4k+2$ a nim-součet těchto čísel je $4k+3$. Do pozice s *SG*-hodnotou $4k+4$ pak žádný tah nevede: v úvahu připadají pouze pozice se dvěma hromádkami o celkovém počtu $4k+3$ sirek. Možné zbytky po dělení čtyřmi počtů sirek v jednotlivých hromádkách jsou buď 0 a 3, nebo 1 a 2. Podle indukčního předpokladu jsou pak zbytky *SG* hodnot buď 3 a 0, nebo 1 a 2, takže *SG*-hodnota pozice o dvou hromádkách bude dávat vždy zbytek 3 po dělení čtyřmi, tedy nebude tvaru $4k+4$. Indukční krok je tedy dokázán i pro přirozená čísla tvaru $4k+3$. Analogicky se dokáže i pro čísla tvaru $4k+4$. □

## I. Vytvořující funkce

**12.61.** Kolika způsoby je možné koupit 12 balíčků kávy, mají-li v prodejně kávu pěti druhů?

Dále tuto úlohu řešte s následujícími modifikacemi:

i) od každé kávy je třeba koupit aspoň 2 balíčky;
ii) od každé kávy má být koupen sudý počet balíčků;
iii) jedné z káv (např. arabské) jsou k dispozici pouze 3 balíčky.

**Řešení.** Základní úloha je klasickým příkladem kombinatorické úlohy na kombinace pěti druhů s opakováním – odpovědí je $\binom{12+5-1}{5-1} = \binom{16}{4}$. Stejně tak i modifikace úlohy je možné s trochou invence vyřešit kombinatorickou úvahou – my zde ale ukážeme, jak tyto úlohy (takřka bez přemýšlení) vyřešit s pomocí vytvořujících funkcí.

součtem $G_1 + G_2$ graf $G = (V, E)$, kde $V = V_1 \times V_2$ a $E = \{(v_1v_2, w_1v_2);\ (v_1, w_1) \in E_1\} \cup \{(v_1v_2, v_1w_2);\ (v_2, w_2) \in E_2\}$.



V případě jedné hry jsme si vystačili s postupným označováním vrcholů grafu od listů písmeny *N* a *P* podle toho, jestli je nebo není (pomocí orientovaných hran) „vidět“ nějaké $P$. V součtu her se ovšem pohybujeme po jednotlivých hranách složitěji, budeme proto potřebovat jemnější nástroj, jak si vyjadřovat dosažitelnost vrcholů značených jako $P$ z dalších vrcholů.

Dobře k tomu poslouží tzv. *Spragueova–Grundyova funkce* $g : V \to \mathbb{N}$, kterou definujeme na acyklickém orientovaném grafu $G = (V, E)$ rekurzivně takto:[9]

(1) všechny listy $v$ označíme $g(v) = 0$;
(2) pro vrchol $v \in V$ definujeme

$$g(v) = \min\{a \in \mathbb{N};\ \text{neexistuje hrana } (v, w) \text{ s } g(w) = a\}.$$

Při definici jsme použili funkci, které se říkává *minimální vyloučená hodnota*. Definujeme ji pro podmnožiny $S$ přirozených čísel $\mathbb{N} = \{0, 1, \dots\}$ vztahem

$$\operatorname{mex} S = \min \mathbb{N} \setminus S.$$

Naše funkce $g(v)$ je právě $\operatorname{mex} S$ pro množinu $S$ všech hodnot $g(w)$, které jsou podél hran vidět z vrcholu $v$.

Poznamenejme, že uvedená definice je korektní, neboť výše definovaný předpis zřejmě definuje jednoznačně funkci přiřazující každé pozici kombinatorické přirozené číslo.

Na přirozených číslech budeme potřebovat ještě jednu operaci. Je to binární operace

$$(a, b) \mapsto a \oplus b,$$

kterou dostaneme tak, že vyjádříme čísla $a$ a $b$ ve dvojkové soustavě a vzniklé vektory $a$ a $b$ ve vektorovém prostoru $(\mathbb{Z}_2)^k$ nad $\mathbb{Z}_2$ sečteme ($k$ je dostatečně velké). Výsledkem je vyjádření pro $a \oplus b$ a to opět ve dvojkové soustavě. Sčítání vektorů ve $(\mathbb{Z}_2)^k$ je známá operace XOR na jednotlivých bitech.

Nyní již můžeme zformulovat hlavní výsledek, tzv. *Spragueovu–Grundyovu větu*:

**12.40. Věta.** *V orientovaném acyklickém grafu $G = (V, E)$ je vrchol $v \in V$ pozicí $P$, právě když je hodnota Spragueovy–Grundyho funkce $g(v) = 0$.*

*Uvažme orientované acyklické grafy $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ a jejich Spragueovy–Grundyovy funkce $g_1$, $g_2$. Potom jejich součet $G = (V, E) = G_1 + G_2$ má Spragueovu–Grundyovu funkci $g$ dánu vztahem*

$$g(v_1v_2) = g_1(v_1) \oplus g_2(v_2).$$

Důkaz. První tvrzení věty je zřejmé přímo z definice Spragueovy-Grundyovy funkce $g$.



Důkaz druhé části je složitější. Nechť $(v_1v_2)$ je pozice hry $G_1 + G_2$ a uvažme libovolné $a \in \mathbb{N}_0$, které splňuje $a < g_1(v_1) \oplus g_2(v_2)$. Ukážeme, že existuje stav $x_1x_2$ hry $G_1 + G_2$ takový, že $g(x_1) \oplus g(x_2) = a$ a $(v_1v_2, x_1x_2) \in E$ a že zároveň pro žádnou hranu $(v_1v_2, y_1y_2) \in E$ neplatí

$$g_1(y_1) \oplus g_2(y_2) = g_1(v_1) \oplus g_2(v_2).$$

[9] Naznačujeme nyní teorii, kterou rozvinuli v tzv. kombinatorické teorii her nezávisle na sobě R. P. Sprague v roce 1935 a P. M. Grundy v roce 1939.

Hledaný počet odpovídá koeficientu u $x^{12}$ v rozvoji funkce

$$(1+x+x^2+\ldots)^5 = \\ = (1+x+\ldots)(1+x+\ldots)\cdots(1+x+\ldots)$$

do mocninné řady. Počet kávy prvního druhu udává to, který člen z první závorky použijeme do součinu, druhého druhu pak člen z druhé závorky, atd. (Všimněte si, že jsme přitom nijak zvlášť nepřemýšleli nad tím, že káv žádného druhu nemůže být více než 12 – ukazuje se, že s nekonečnými řadami se zde pracuje obvykle snáz než s konečnými polynomy.)

Protože

$$\frac{1}{1-x} = 1+x+x^2+\ldots$$

(viz 12.42), je naší uvažovanou funkcí funkce $(1-x)^{-5}$. Úkolem je tedy rozvinout $(1-x)^{-5}$ do mocninné řady – podle zobecněné binomické věty z 12.42 je koeficientem u $x^k$ číslo $\binom{k+5-1}{5-1}$, v našem případě tedy $\binom{16}{4}$. Všimněte si, že jsme s využitím vytvořujících funkcí zodpověděli otázku nejen pro 12 káv, ale pro libovolný zadaný počet.

Modifikace řešíme analogicky:

i) Vytvořující funkcí je

$$(x^2+x^3+\ldots)^5 = \left(\frac{x^2}{1-x}\right)^5 = \frac{x^{10}}{(1-x)^5},$$

proto je koeficient u $x^{12}$ roven $\binom{2+5-1}{5-1}$.

ii) Sudému počtu káv všech druhů odpovídá vytvořující funkce

$$(1+x^2+x^4+\ldots)^5 = \frac{1}{(1-x^2)^5}.$$

Koeficient u $x^{12}$ lze získat různými způsoby, nejsnáze asi pomocí substituce $y = x^2$ a hledání koeficientu u $y^6$ (což vlastně odpovídá tomu, že v obchodě slepí balíčky po dvou k sobě), odkud dostaneme odpověď $\binom{6+5-1}{5-1}$.

iii) V tomto případě je vytvořující funkce rovna

$$(1+x+x^2+x^3)(1+x+x^2+\ldots)^4,$$

a hledaný výsledek je tedy roven
$\binom{12+4-1}{4-1} + \binom{11+4-1}{4-1} + \binom{10+4-1}{4-1} + \binom{9+4-1}{4-1}$. □

**12.62.** Kolika způsoby můžeme pomocí mincí (1, 2, 5, 10, 20 a 50 Kč) zaplatit platbu 100 Kč?

**Řešení.** Hledáme přirozená čísla $a_1, a_2, a_5, a_{10}, a_{20}$ a $a_{50}$ taková, že $a_i$ je násobkem $i$ pro všechna $i \in \{1, 2, 5, 10, 20, 50\}$ a zároveň $a_1+a_2+a_5+a_{10}+a_{20}+a_{50} = 100$. Je vidět, že požadovaný počet lze získat Tím ověříme právě rekurzivní definici Spragueovy–Grundyovy funkce a věta bude dokázána.

Nejprve budeme hledat vrchol $x_1x_2$ s danou hodnotou $a < g_1(v_1) \oplus g_2(v_2)$ Spragueovy–Grundyovy funkce.

Uvažme číslo $b := a \oplus g_1(v_1) \oplus g_2(v_2)$. Nechť binární zápis tohoto čísla má $k$ cifer. Potom na $k$-tém místě (od konce) v binárním rozvoji čísla $g_1(v_1) \oplus g_2(v_2)$ musí být cifra 1. Skutečně pokud mají $a$ a $g_1(v_1) \oplus g_2(v_2)$ různý počet cifer, je tvrzení zřejmé, a pokud mají $g_1(v_1)$ a $a$ stejný počet cifer, tak právě jedno z čísel $a$ a $g_1(v_1) \oplus g_2(v_2)$ musí mít na $k$-tém místě od konce cifru 1. Nemůže to být přitom číslo $a$, protože ve vyšších řádech si obě čísla musejí být rovna a číslo $a$ je menší.

Tedy právě jedno z čísel $g_1(v_1)$ a $g_2(v_2)$ má na $k$-tém místě cifru 1. Bez újmy na obecnosti předpokládejme, že to je $g_1(v_1)$. Uvažme dále číslo $c := g_1(v_1) \oplus b$. Toto číslo je v binárním zápisu nejvýše $k-1$ ciferné, protože obě sčítaná čísla mají v $k$-tém řádu cifru 1. Je tedy jistě menší než $g_1(v_1)$. Potom ale dle definice hodnoty funkce $g_1(v_1)$ existuje stav $w_1$ hry $G_1$ takový, že $(v_1, w_1) \in E_1$ a $g_1(w_1) = c$. Nyní však $(v_1v_2, w_1v_2) \in E$ a

$$g_1(w_1) \oplus g_2(v_2) = c \oplus g_2(v_2) = g_1(v_1) \oplus b \oplus g_2(v_2) = \\ = g_1(v_1) \oplus a \oplus g_1(v_1) \oplus g_2(v_2) \oplus g_2(v_2) = a.$$

Tím jsme naplnili první část našeho záměru.

Dále uvažme v $G$ libovolnou hranu $(v_1v_2, y_1y_2) \in E$, kde $(v_1, y_1) \in E_1$, a proto $v_2 = y_2$, a předpokládejme $g_1(y_1) \oplus g_2(y_2) = g_1(v_1) \oplus g_2(v_2)$. Pak ovšem $g_1(y_1) \oplus g_2(v_2) = g_1(v_1) \oplus g_2(v_2)$ (jde o operaci ve vektorovém prostoru, můžeme tedy krátit). Pak ale také $g_1(y_1) = g_1(v_1)$, což je ve sporu s vlastnostmi Spragueovy-Grundyovy funkce $g_1$ hry $G_1$. Dokázali jsme tedy i druhou část a věta je dokázána. □

Z věty okamžitě dostáváme srozumitelný a prakticky užitečný výsledek:

**Důsledek.** *Vrchol $v_1v_2$ v součtu grafů je P–pozice, právě když $g_1(v_1) = g_2(v_2)$.*

**Poznámka.** V tomto textu nemůžeme jít do podrobností, obecně lze ale dokázat, že každý konečný acyklický orientovaný graf je izomorfní s konečným součtem vhodně zobecněných her Nim. Naší analýzou jednoduché hry a konstrukcí funkce $g$ jsme tedy v podstatě (alespoň implicitně) zvládli analýzu všech nestranných her.

### 3. Kombinatorické výpočty

**12.41. Vytvořující funkce.** Docela často jsou v kombinatorických úvahách užitečné výsledky dosahované ve „spojitých metodách“, tj. zejména klasické matematické analýze. Tomu můžeme rozumět i naopak – v podstatě byly všechny výsledky v analýze dosaženy vhodným přeložením problému na kombinatorickou úlohu (za příklad může sloužit třeba převedení problému integrace racionálních funkcí lomených na rozklad těchto funkcí na tzv. parciální zlomky). Není proto divu, že tyto již zvládnuté postupy můžeme dobře využívat přímo.

V závěru naší procházky po aplikacích kombinatorických postupů se proto podíváme alespoň na jednu oblast, kde se nám hodí znalosti ze spojitých metod. Začněme jednoduchým příkladem: *Máme v peněžence 4 korunové mince, 5 dvoukorunových a 3 pětikorunové. Z automatu, který nevrací, chceme Colu za 22 Kč. Kolika*

jako koeficient u $x^{100}$ v součinu

$$(1+x+x^2+\dots)(1+x^2+x^4+\dots)(1+x^5+x^{10}+\dots)\cdot$$
$$\cdot(1+x^{10}+x^{20}+\dots)(1+x^{20}+x^{40}+\dots)\cdot$$
$$\cdot(1+x^{50}+x^{100}+\dots)=$$
$$=\frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^5}\cdot\frac{1}{1-x^{10}}\cdot\frac{1}{1-x^{20}}\cdot\frac{1}{1-x^{50}}.$$

Konkrétní výsledek můžeme získat například s pomocí softwaru SAGE (názvy použitých příkazů jsou jistě dostatečně výmluvné):

```
sage: f=1/(1- x)*1/(1-x^2)*1/(1-x^5)\
        *1/(1- x^10)*1/(1-x^20)*1/(1-x^50)
sage: r=taylor(f,x,0,100)
sage: r.coeff(x,100)

4562
```

□

**12.63.** Rozviňte do mocninné řady funkci

i) $\frac{x}{x+2}$,

ii) $\frac{x^2+x+1}{2x^3-3x^2+1}$.

**Řešení.**

i)
$$\frac{x}{x+2}=\frac{x}{2-(-x)}=\frac{x/2}{1-(-x/2)}=$$
$$=\frac{x}{2}-\frac{x^2}{4}+\frac{x^3}{8}-\dots+=\sum_{n=1}^{\infty}(-1)^{n-1}\frac{x^n}{2^n}.$$

ii) Provedeme rozklad na parciální zlomky
$$\frac{x^2+x+1}{2x^3-3x^2+1}=\frac{x^2+x+1}{(x-1)^2(2x+1)}=$$
$$=\frac{A}{2x+1}+\frac{B}{x-1}+\frac{C}{(x-1)^2},$$
kdy zjistíme, že $A=B=\frac{1}{3}$ a $C=1$, proto
$$\frac{x^2+x+1}{2x^3+3x^2+1}=\frac{1/3}{1+2x}-\frac{1/3}{1-x}+\frac{1}{(1-x)^2}=$$
$$=\sum_{n=0}^{\infty}\left[\frac{1}{3}\left((-2)^n-1\right)+(n+1)\right]x^n.$$

□

*12.64.* Určete vytvořující funkci posloupností

i) $(1,2,3,4,5,\dots)$,

ii) $(1,4,9,16,\dots)$,

iii) $(1,1,2,2,4,4,8,8,\dots)$,

iv) $(9,0,0,2\cdot16,0,0,4\cdot25,0,0,8\cdot36,\dots)$,

*způsoby to umíme, aniž bychom ztratili přeplatek?* Hledáme zjevně čísla $i$, $j$ a $k$ taková, že $i+j+k=22$ a zároveň

$$i\in\{0,1,2,3,4\},\ j\in\{0,2,4,6,8,10\},\ k\in\{0,5,10,15\}.$$

Uvažme součin polynomů (třeba nad reálnými čísly)

$$(x^0+x^1+x^2+x^3+x^4)(x^0+x^2+x^4+x^6+x^8+x^{10})\cdot$$
$$\cdot(x^0+x^5+x^{10}+x^{15}).$$

Mělo by být zřejmé, že hledaný počet řešení je právě koeficient u $x^{22}$ ve výsledném polynomu. Skutečně tak dostáváme čtyři možnosti $3\cdot5+3\cdot2+1\cdot1$, $3\cdot5+2\cdot2+3\cdot1$, $2\cdot5+5\cdot2+2\cdot1$ a $2\cdot5+4\cdot2+4\cdot1$.

Tento prostinký příklad zasluhuje větší pozornost, než by se mohlo na první pohled zdát. Jednotlivé polynomy svými koeficienty vyjadřovaly posloupnost hodnot, kterých jsme uměli dosahovat: Jestliže budeme (pro jistotu, abychom nemuseli předem dělat odhady velikostí) pracovat s nekonečnými posloupnostmi, pak pomocí jednotlivých korun umíme dosáhnout hodnot $0,1,2,\dots$ s četnostmi

$$(1,1,1,1,1,0,0,\dots)$$

(pokračují samé nuly), u dvoukorun a pětikorun to budou posloupnosti četností

$$(1,0,1,0,1,0,1,0,1,0,1,0,0,\dots),$$
$$(1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1,0,0,\dots).$$

Ke každé takové posloupnosti s konečně mnoha nenulovými členy můžeme přiřadit polynom a shodou okolností řešení naší úlohy bylo možné odečíst ze součinu těchto polynomů. Takový postup můžeme používat obecně pro práci s posloupnostmi, když nahradíme polynomy mocninnými řadami.

**Definice.** *Vytvořující funkce* (v.f.p.) pro nekonečnou posloupnost $a=(a_0,a_1,a_2,\dots)$ je (formální) mocninná řada

$$a(x)=a_0+a_1x+a_2x^2+\dots=\sum_{i=0}^{\infty}a_ix^i.$$

Vytvořující funkce v praxi využíváme:

- k nalezení **explicitní formule** pro $n$-tý člen posloupnosti;
- často vytvořující funkce vycházejí z rekurentních vztahů, občas ale díky nim odvodíme rekurentní vztahy nové;
- výpočet průměrů či jiných statistických závislostí (např. průměrná složitost algoritmu);
- důkaz různých identit;
- často je nalezení přesného vztahu příliš obtížné, ale mnohdy stačí vztah přibližný nebo alespoň asymptotické chování.

Některým jednoduchým operacím s posloupnostmi odpovídají jednoduché operace nad mocninnými řadami (jak se snadno přesvědčíme provedením příslušné operace s mocninnými řadami):

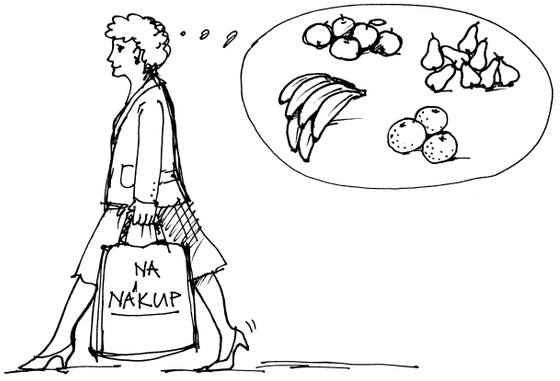
- Sčítání $(a_i+b_i)$ posloupností člen po členu odpovídá součet $a(x)+b(x)$ příslušných vytvořujících funkcí.
- Vynásobení $(\alpha\cdot a_i)$ všech členů posloupnosti stejným skalárem $\alpha$ odpovídá vynásobení $\alpha\cdot a(x)$ příslušné vytvořující funkce.
- Vynásobení vytvořující funkce $a(x)$ monomem $x^k$ odpovídá posunutí posloupnosti doprava o $k$ míst a její doplnění nulami zleva.

v) $(9, 1, -9, 32, 1, -32, 100, 1, -100, \dots, )$.

○

**12.65.** Určete kolika způsoby je možné naplnit tašku $n$ kusy uvedených druhů ovoce, přičemž jednotlivé kusy téhož druhu nerozlišujeme, nemusí být využity všechny druhy a navíc:

- jablek může být libovolný počet,
- banánů musí být sudý počet,
- hrušek musí být násobek 4,
- pomeranče mohou být nejvýše 3 a
- pomelo může být pouze jedno (nebo žádné).




**Řešení.** Vytvořující funkcí pro posloupnost $(a_n)$, kde $a_n$ je hledaný počet způsobů, jak naplnit tašku $n$ kusy ovoce, je

$$\begin{aligned}&(1+x+x^2+\cdots)(1+x^2+x^4\cdots)(1+x^4+x^8+\cdots)\cdot\\&\cdot(1+x+x^2+x^3)(1+x)=\\&=\frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^4}\cdot\frac{1-x^4}{1-x}\cdot(1+x)=\\&=\frac{1}{(1-x)^3}.\end{aligned}$$

Podle zobecněné binomické věty je $(1-x)^{-3}=\sum_{n=0}^{\infty}\binom{n+2}{2}x^n$, proto pro hledaný počet způsobů platí $a_n=\binom{n+2}{2}$. □

**12.66.** S využitím binomické věty znovu odvoďte níže uvedené kombinatorické vztahy.

- $\sum_{k=0}^{n}\binom{n}{k}=2^n$,
- $\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$,
- $\sum_{k=0}^{n}k\binom{n}{k}=n2^{n-1}$.

**Řešení.** Dosadíme-li do binomické věty

$$(1+x)^n=\binom{n}{0}+\binom{n}{1}x+\binom{n}{2}x^2+\cdots+\binom{n}{n}x^n$$

- Pro posunutí posloupnosti doleva o $k$ míst (tj. vynechání prvních $k$ míst posloupnosti) nejprve od $a(x)$ odečteme polynom $b_k(x)$ odpovídající posloupnosti $(a_0, \dots, a_{k-1}, 0, \dots)$ a poté podělíme vytvořující funkci výrazem $x^k$.
- Dosazením polynomu $f(x)$ za $x$ vytvoříme specifické kombinace členů původní posloupnosti. Jednoduše je vyjádříme pro $f(x)=\alpha x$, což odpovídá vynásobení $k$–tého členu posloupnosti skalárem $\alpha^k$. Dosazení $f(x)=x^n$ nám do posloupnosti mezi každé dva členy vloží $n-1$ nul.

První dvě pravidla říkají, že přiřazení vytvořující funkce posloupnosti je homomorfismus vektorových prostorů nad zvoleným tělesem.

Dalšími důležitými operacemi, které se při práci s vytvořujícími funkcemi často objevují, jsou:

- Derivování podle $x$: funkce $a'(x)$ vytvořuje posloupnost $(a_1, 2a_2, 3a_3, \dots)$, člen s indexem $k$ je $(k+1)a_{k+1}$ (tj. mocninnou řadu derivujeme člen po členu).
- Integrování: funkce $\int_0^x a(t)\,\mathrm{d}t$ vytvořuje posloupnost $(0, a_0, \frac{1}{2}a_1, \frac{1}{3}a_2, \frac{1}{4}a_3, \dots)$, pro $k \geq 1$ je člen s indexem $k$ roven $\frac{1}{k}a_{k-1}$ (zřejmě je derivací příslušné mocninné řady člen po členu původní funkce $a(x)$).
- Násobení řad: součin $a(x)b(x)$ je vytvořující funkcí posloupnosti $(c_0, c_1, c_2, \dots)$, kde

$$c_k=\sum_{i+j=k}a_ib_j,$$

tj. členy v součinu až po $c_k$ jsou stejné jako v součinu $(a_0+a_1x+a_2x^2+\cdots+a_kx^k)(b_0+b_1x+b_2x^2+\cdots b_kx^k)$. Posloupnost $(c_n)$ bývá také nazývána *konvolucí* posloupností $(a_n)$, $(b_n)$.

**12.42. Příklady vytvořujících funkcí.** Uvedeme několik jednoduchých příkladů vytvořujících funkcí. Řadu z nich jsme viděli při práci s mocninnými řadami ve třetí části šesté kapitoly. Snad si všichni vzpomenou na vytvořující funkci zadanou geometrickou řadou:

$$a(x)=\frac{1}{1-x}=1+x+x^2+\dots,$$

která tedy odpovídá konstantní posloupnosti $(1, 1, 1, \dots)$.

Ze šesté kapitoly víme, že stejně zapsaná mocninná řada konverguje pro $x \in (-1, 1)$ a její součet je roven funkci $1/(1-x)$. Stejně tak obráceně, rozvineme-li tuto funkci do Taylorovy řady v bodě 0, dostaneme zřejmě původní řadu. Takovéto „zakódování“ posloupnosti čísel do funkce a zpět je klíčovým obratem v teorii vytvořujících funkcí.

Obecně pro každou posloupnost $a_i$ s členy velikosti $|a_n| = O(n^k)$ s konstantním exponentem $k$ konverguje její vytvořující funkce na nějakém okolí nuly (viz 5.51 a 6.45). Můžeme s nimi pak opravdu na konvergenčním intervalu zacházet jako s funkcemi, zejména je umíme sčítat, násobit, skládat, derivovat a integrovat.

čísla $x = 1$, resp. $x = -1$, dostaneme první dvě identity. Třetí pak získáme, když se na obě strany v binomické větě podíváme „spojitýma očima“ a využijeme vlastnosti derivací. □

**12.67.** V krabici je 30 červených, 40 modrých a 50 bílých míčků, míčky stejné barvy přitom nelze rozeznat. Kolika způsoby je možné vybrat soubor 70 míčků?

**Řešení.** Hledaný počet je roven koeficientu u $x^{70}$ v součinu

$$(1+x+x^2+\cdots+x^{30})(1+x+x^2+\cdots+x^{40})(1+x+x^2+\cdots+x^{50}).$$

Tento součin upravíme na tvar $(1-x)^{-3}(1-x^{31})(1-x^{41})(1-x^{51})$, odkud pomocí zobecněné binomické věty dostaneme

$$\left(\binom{2}{2}+\binom{3}{2}x+\binom{4}{2}x^2+\cdots\right)(1-x^{31}-x^{41}-x^{51}+x^{72}+\ldots)$$

a tedy koeficientem u $x^{70}$ je zřejmě $\binom{70+2}{2}-\binom{70+2-31}{2}-\binom{70+2-41}{2}-\binom{70+2-51}{2}=1061$. □

**12.68.** Dokažte, že

$$\sum_{k=1}^{n} H_k = (n+1)(H_{n+1}-1).$$

**Řešení.** Potřebnou konvoluci získáme součinem řad $\frac{1}{1-x}$ a $\frac{1}{1-x}\ln\frac{1}{1-x}$. Odtud

$$[x^n]\tfrac{1}{(1-x)^2}\ln\tfrac{1}{1-x}=\sum_{k=1}^{n}\tfrac{1}{k}(n+1-k),$$

odkud již snadnou úpravou dostaneme požadované. □

**12.69.** Vyřešte rekurenci

$$a_0 = a_1 = 1,$$
$$a_n = a_{n-1} + 2a_{n-2} + (-1)^n.$$

**Řešení.** Jako vždy neuškodí vypsání prvních několika členů posloupnosti (teď ale ani moc nepomůže, snad jen pro kontrolu správnosti výsledku).[1]

Krok 1: $a_n = a_{n-1} + 2a_{n-2} + (-1)^n[n \geq 0] + [n = 1]$.

Krok 2: $A(x) = xA(x) + 2x^2A(x) + \frac{1}{1+x} + x$.

Krok 3:

$$A(x) = \frac{1+x+x^2}{(1-2x)(1+x)^2}.$$

Krok 4: $a_n = \frac{7}{9}2^n + \left(\frac{1}{3}n + \frac{2}{9}\right)(-1)^n$. □

[1] Na rozdíl od tvrzení v *Concrete mathematics* je již možné tuto posloupnost nalézt v *The On-Line Encyclopedia of Integer Sequences*.

Uveďme nyní několik základních mocninných řad a jejich součtů, s nimiž budeme velmi často pracovat:

$$\frac{1}{1-x} = \sum_{n\geq 0} x^n,$$
$$\ln\frac{1}{1-x} = \sum_{n\geq 1}\frac{x^n}{n},$$
$$e^x = \sum_{n\geq 0}\frac{x^n}{n!},$$
$$\sin x = \sum_{n\geq 0}(-1)^n\frac{x^{2n+1}}{(2n+1)!},$$
$$\cos x = \sum_{n\geq 0}(-1)^n\frac{x^{2n}}{(2n)!},$$
$$(1+x)^r = \sum_{k\geq 0}\binom{r}{k}x^k.$$

Poslední vzorec $(1+x)^r = \sum_{k\geq 0}\binom{r}{k}x^k$ je tzv. *zobecněná binomická věta*, kde pro $r \in \mathbb{R}$ je binomický koeficient definován vztahem

$$\binom{r}{k} = \frac{r(r-1)(r-2)\cdots(r-k+1)}{k!}.$$

Speciálně klademe $\binom{r}{0} = 1$.

Pro $n \in \mathbb{N}$ z uvedeného vztahu snadno dostaneme, že funkci $\frac{1}{(1-x)^n}$ lze rozvinout do řady

$$\binom{0+n-1}{n-1}+\binom{1+n-1}{n-1}x+\cdots+\binom{k+n-1}{n-1}x^k+\cdots$$

Tento vztah bude dále rovněž užitečný, protože často vyvstane potřeba rozvíjet do mocninných řad právě racionální funkce tohoto tvaru (např. při rozkladu na parciální zlomky v případě, kdy má jmenovatel násobné kořeny).

**Příklad.** Ukažme si důležitý příklad využívající konvoluci posloupností:

$$\frac{1}{1-x}a(x) \quad \text{je v.f.p.} \quad (a_0, a_0+a_1, a_0+a_1+a_2, \ldots).$$

Odtud např. dostáváme, že

$$\frac{1}{1-x}\ln\frac{1}{1-x} \quad \text{je v.f.p. harmonických čísel} \quad H_n.$$

Protože $\frac{1}{1-x} = \sum_{n\geq 0}x^n$, dostáváme konvolucí posloupnosti $(1, 1, \ldots)$ se sebou vztahy

$$\frac{1}{(1-x)^2} = \sum_{n\geq 0}(n+1)x^n, \quad \frac{1}{(1-x)^3} = \sum_{n\geq 0}\binom{n+2}{2}x^n,$$

což je vztah, který sice máme dokázán již z dřívějška (dokonce dvakrát – jednou díky zobecněné binomické větě a podruhé díky derivaci řady), ale další odvození jistě neuškodilo.

**12.43. Diferenční rovnice s konstantními koeficienty.** Hezkým a poučným příkladem na užití vytvořujících funkcí je úplná diskuse řešení lineárních diferenčních rovnic s konstantními koeficienty. Zabývali jsme se jimi již v třetí části první kapitoly, viz např. 1.12. Tam jsme ale přímo odvodili vzorec pro rovnice prvního řádu, odůvodnili jednoznačnost a existenci řešení, ale řešení

**12.70. Quicksort – analýza průměrného případu.** Naším cílem bude nyní určit očekávaný počet porovnání během algoritmu `Quicksort` pro seřazení nějaké (konečné) posloupnosti prvků.

Ukázka jednoduché implementace typu *divide and conquer*:

```
if L == []: return []
return qsort([x for x in L[1:] if x<L[0]])
     + L[0:1]
     + qsort([x for x in L[1:] if x>=L[0]])
```

Sestavit rekurentní vztah pro počet porovnání není příliš náročné (budeme předpokládat rovnoměrné rozdělení pravděpodobnosti všech možných pořadí dané posloupnosti), algoritmus má následující parametry:

i) Počet porovnání při rozdělení (*divide*): $n-1$.

ii) Předpoklad náhodnosti: pravděpodobnost toho, že prvek $L[0]$ je $k$-tý největší, je $\frac{1}{n}$.

iii) Velikost tříděných polí ve fázi *conquer*: $k-1$ a $n-k$.

Pro střední hodnotu počtu porovnání tak dostáváme rekurentní vztah:

$$C_n = n - 1 + \sum_{k=1}^{n} \frac{1}{n} \left(C_{k-1} + C_{n-k}\right).$$

Tuto rekurenci je možné vyřešit (s použitím jistých triků, které se však lze do jisté míry naučit) i bez využití vytvořujících funkcí.

$$C_n = n - 1 + \frac{2}{n} \sum_{k=1}^{n} C_{k-1} \qquad \textit{symetrie obou sum}$$

$$nC_n = n(n-1) + 2\sum_{k=1}^{n} C_{k-1} \qquad \textit{vynásob } n$$

$$(n-1)C_{n-1} = (n-1)(n-2) + 2\sum_{k=1}^{n-1} C_{k-1} \qquad \textit{tentýž výraz pro } C_{n-1}$$

$$nC_n = (n+1)C_{n-1} + 2(n-1) \qquad \textit{odečteno a upraveno}$$

Tím jsme již dostali podstatně jednodušší rekurenci

$$nC_n = (n+1)C_{n-1} + 2(n-1),$$

která ovšem na rozdíl od většiny předchozích příkladů není rovnicí s konstantními koeficienty.

Rovněž si lze všimnout, že jsme již rekurenci zjednodušili natolik, že je možné iterativně hodnoty $C_n$ dopočítat. Přesto je často žádoucí tyto hodnoty konkrétně (nebo alespoň přibližně) vyjádřit explicitně jako funkci $n$.

Nejprve si pomůžeme drobným trikem, kdy vydělíme obě strany výrazem $n(n+1)$ :

$$\frac{C_n}{n+1} = \frac{C_{n-1}}{n} + \frac{2(n-1)}{n(n+1)}$$

samo jsme pak v podstatě „uhádli“. Nyní můžeme řešení skutečně odvodit.

Zkusme nejprve dobře známý příklad Fibonacciovy posloupnosti zadané rekurencí

$$F_{n+2} = F_n + F_{n+1},\ F_0 = 0,\ F_1 = 1$$

a pišme $F(x)$ pro vytvořující funkci této posloupnosti. Definiční rovnost můžeme vyjádřit pomocí $F(x)$, když použijeme naše operace pro posuv členů posloupnosti. Víme totiž, že $xF(x)$ odpovídá posloupnosti $(0, F_0, F_1, F_2, \dots)$ a $x^2F(x)$ posloupnosti $(0, 0, F_0, F_1, \dots)$. Proto vytvořující funkce $xF(x) + x^2F(x) - F(x)$ odpovídá posloupnosti

$$(-F_0, F_0 - F_1, 0, 0, \dots, 0, \dots).$$

Obdrželi jsme tedy rovnici pro vytvořující funkci $F(x)$:

$$(1 - x - x^2)F(x) = x.$$

Abychom lépe viděli odpovídající posloupnost, můžeme ještě výsledný výraz upravit na součet jednodušších. Víme totiž, že lineární kombinace vytvořujících funkcí odpovídá stejným kombinacím posloupností. Racionální funkce lomené jsme se naučili rozkládat na tzv. parciální zlomky, viz 6.23. Tímto postupem vyjádříme

$$F(x) = \frac{x}{1 - x - x^2} = \frac{A}{x - x_1} + \frac{B}{x - x_2} = \\ = \frac{a}{1 - \lambda_1 x} + \frac{b}{1 - \lambda_2 x},$$

kde $A$, $B$ jsou vhodné (obecně) komplexní konstanty a $x_1$, $x_2$ jsou kořeny polynomu ve jmenovateli. Konstanty $a, b, \lambda_1$ a $\lambda_2$ získáme jednoduchou úpravou jednotlivých zlomků. Výsledkem je obecné řešení pro naši vytvořující funkci

$$F(x) = \sum_{n=0}^{\infty} (a\lambda_1^n + b\lambda_2^n)x^n$$

a tím i obecné řešení naší rekurence. Srovnejte tento postup s výsledkem v 3.10.

Pro obecné lineární diferenční rovnice řádu $k$ je účinný stejný postup. Je-li

$$F_{n+k} = a_0F_n + \cdots + a_{k-1}F_{n+k-1},$$

pak vytvořující funkce pro výslednou posloupnost je

$$F(x) = \frac{x^{k-1}}{1 - a_0x^{k-1} - \cdots - a_{k-1}x}.$$

Rozkladem na parciální zlomky dostaneme obecný výsledek, který jsme zmiňovali již v odstavci 3.12.

Mocninné řady jsou velmi silným nástrojem pro řešení rekurencí. Tím je míněno vyjádření členu $a_n$ jako funkci $n$. Často se s pomocí řad podaří vyřešit na první pohled velmi složité rekurence.

### Postup pro řešení rekurencí

Obvyklý (takřka mechanický) postup pro řešení rekurencí se skládá ze 4 kroků:

(1) Zapíšeme jedinou rovnicí závislost $a_n$ na ostatních členech posloupnosti. Tato *univerzální formule* musí platit pro všechna $n \in \mathbb{N}_0$ (předpokládajíce $a_{-1} = a_{-2} = \cdots = 0$).

Nyní tento vztah „rozbalíme“ (*telescope*, příp. si pomůžeme substitucí $B_n = C_n/(n+1)$):

$$\frac{C_n}{n+1} = \frac{2(n-1)}{n(n+1)} + \frac{2(n-2)}{(n-1)n} + \cdots + \frac{2\cdot 1}{2\cdot 3} + \frac{C_1}{2}.$$

Odtud

$$\frac{C_n}{n+1} = 2\sum_{k=1}^{n-1} \frac{k}{(k+1)(k+2)}.$$

Výraz sečteme např. pomocí rozkladu na parciální zlomky $\frac{k}{(k+1)(k+2)} = \frac{2}{k+2} - \frac{1}{k+1}$ a dostaneme

$$\frac{C_n}{n+1} = 2\left(H_{n+1} - 2 + \frac{1}{n+1}\right),$$

odkud

$$C_n = 2(n+1)H_{n+1} - 4(n+1) + 2$$

($H_n = \sum_{k=1}^{n} \frac{1}{k}$ je součet prvních $n$ členů harmonické řady). Přitom je možné odhadnout $H_n \sim \int_1^n \frac{\mathrm{d}x}{x} + \gamma$, odkud

$$C_n \sim 2(n+1)(\ln(n+1) + \gamma - 2) + 2.$$

Vyřešme nyní rekurenci pro očekávaný počet porovnání v průběhu algoritmu Quicksort

$$nC_n = n(n-1) + 2\sum_{k=1}^{n} C_{k-1}, \quad C_0 = C_1 = 0$$

pomocí uvedeného postupu.

- $\sum_{n\geq 0} nC_n x^n = \sum_{n\geq 0} n(n-1)x^n + 2\sum_{n\geq 0}\sum_{k=1}^{n} C_{k-1}x^n$
- $xC'(x) = \frac{2x^2}{(1-x)^3} + 2\frac{xC(x)}{1-x}$
- Vyřešením této lineární diferenciální rovnice prvního řádu (vynásobíme integračním faktorem $e^{\int -\frac{2}{1-x}\,\mathrm{d}x} = (1-x)^2$, odkud $[(1-x)^2C(x)]' = \frac{2x}{1-x}$) dostaneme

$$C(x) = \frac{2}{(1-x)^2}\left(\ln\frac{1}{1-x} - x\right),$$

odkud konečně $C_n = 2(n+1)(H_{n+1} - 1) - 2n$.

*12.71.* S využitím vytvořující funkce pro Fibonacciho posloupnost $F(x) = x/(1-x-x^2)$ určete vytvořující funkci „poloviční“ Fibonacciho posloupnosti $(F_0, F_2, F_4, \ldots)$. ◯

**12.72.** *Vějířem* řádu $n$ nazveme graf na $n+1$ vrcholech $0, 1, \ldots, n$, který má následujících $2n-1$ hran: vrchol 0 je spojen hranou s každým ze zbylých vrcholů a každý vrchol $k$ je spojen hranou s vrcholem $k+1$ (pro $1 \leq k < n$). Kolik koster má takový graf?

**Řešení.** Označíme-li $v_n$ hledaný počet koster, je zřejmě $v_1 = 1$ a protože je vějířem řádu 2 trojúhelník $K_3$, platí $v_2 = 3$. Ukážeme dále, že

(2) Obě strany rovnice vynásobíme $x^n$ a sečteme přes všechna $n \in \mathbb{N}_0$. Na jedné straně tak dostaneme $\sum_n a_n x^n$, což je vytvořující funkce $A(x)$. Pravou stranu vztahu je pak třeba upravit na výraz rovněž obsahující $A(x)$.
(3) Zjištěná rovnice se vyřeší vzhledem k $A(x)$.
(4) Výsledné $A(x)$ se rozvine do mocninné řady, přičemž koeficient u $x^n$ udává $a_n$, tj. $a_n = [x^n]A(x)$ .

**Příklad.** Vyřešme uvedeným postupem rekurenci

$$a_0 = 0, a_1 = 1,$$
$$a_n = 5a_{n-1} - 6a_{n-2}.$$

**Řešení**. V jednotlivých krocích postupu dostáváme:
Krok 1: $a_n = 5a_{n-1} - 6a_{n-2} + [n=1]$.
Krok 2: $A(x) = 5xA(x) - 6x^2A(x) + x$.
Krok 3:

$$A(x) = \frac{x}{1-5x+6x^2} = \frac{1}{1-3x} - \frac{1}{1-2x}.$$

Krok 4: $a_n = 3^n - 2^n$. □

**12.44. Pěstované binární stromy a Catalanova čísla.**  S využitím vytvořujících funkcí určíme formuli pro počet $b_n$ neizomorfních pěstovaných binárních stromů na $n$ vrcholech, které je pro naše účely možné definovat jako kořen s uspořádanou dvojicí [*levý binární podstrom, pravý binární podstrom*].

Prozkoumáním případů pro malá $n$ vidíme, že

$$b_0 = 1, b_1 = 1, b_2 = 2, b_3 = 5.$$

Snadno nahlédneme, že pro $n \geq 1$ vyhovuje $b_n$ rekurentní formuli

$$b_n = b_0b_{n-1} + b_1b_{n-2} + \cdots + b_{n-1}b_0$$

a vidíme, že jde vlastně o konvoluci posloupností. Vztah upravíme, aby platil pro všechna $n \in N_0$:

$$b_n = \sum_{0\leq k<n} b_k b_{n-k-1} + [n=0].$$

Tím máme hotov krok 1.

V kroku 2 vynásobíme obě strany $x^n$ a sečteme. Je-li $B(x)$ odpovídající vytvořující funkce, pak:

$$B(x) = \sum_n b_n x^n = \sum_{n,k} b_k b_{n-k-1}x^n + \sum_{n,k}[n=0]x^n =$$
$$= \sum_k b_k x^k \left(\sum_n b_{n-k-1}x^{n-k}\right) + 1 =$$
$$= \sum_k b_k x^k\,(xB(x)) + 1 = B(x)\cdot xB(x) + 1.$$

Pozorný čtenář si jistě povšiml, že ve výše uvedeném výpočtu jsme nahradili konvoluci $b_n = b_0b_{n-1} + b_1b_{n-2} + \cdots + b_{n-1}b_0$ vztahem

$$b_n = b_0b_{n-1} + \cdots + b_{n-1}b_0 + b_nb_{-1} + b_{n+1}b_{-2} + \cdots .$$

Díky naší konvenci to ale není problém a velmi to usnadňuje práci se sumami (s nekonečnými součty se zde pracuje podstatně snadněji než neustále hlídat meze).

pro $n > 1$ platí rekurence[2]

$$v_n = v_{n-1} + \sum_{k=0}^{n-1} v_k + 1, \quad v_0 = 0.$$

Pro nějakou kostru vějíře řádu $n$ označme $k \in \{1, \ldots, n-1\}$ největší takové, že v kostře leží všechny hrany cesty $(0, 1, 2, 3, \ldots, k)$. V takové kostře určitě nemohou být hrany $\{0, 2\}, \ldots, \{0, k\}, \{k, k+1\}$, proto je všech takových koster s daným $k$ stejně jako koster na vějíři řádu $n-k$ s vrcholy $0, k+1, k+2, \ldots, n$, tedy $v_{n-k}$. Dále ještě musíme započítat jednu kostru pro $k = n$ a ty kostry, v nichž neleží hrana $\{0, 1\}$ (a tedy nutně obsahují hranu $\{1, 2\}$) – ty dostaneme z vějířů řádu $n-1$ na vrcholech $0, 2, \ldots, n$. Dostali jsme tedy skutečně požadovanou rekurenci $v_n = v_{n-1} + v_{n-1} + v_{n-2} + \cdots + v_0 + 1$.

Nyní tedy máme obecný vztah

$$v_n = v_{n-1} + \sum_{k=0}^{n-1} v_k + 1 - [n = 0],$$

odkud pro vytvořující funkci $V(x)$ této posloupnosti dostáváme obvyklým postupem

$$\begin{aligned} V(x) &= x \cdot V(x) + \sum_{n=0}^{\infty} \sum_{k<n} v_k x^n + \frac{1}{1-x} - 1 = \\ &= x \cdot V(x) + \sum_{k=0}^{\infty} \sum_{n>k} v_k x^n + \frac{x}{1-x} = \\ &= \left( \sum_{k=0}^{\infty} v_k x^k \right) \cdot \sum_{n>k} x^{n-k} + \frac{x}{1-x} = \\ &= \left( \sum_{k=0}^{\infty} v_k x^k \right) \cdot \frac{x}{1-x} + \frac{x}{1-x} = V(x) \cdot \frac{x}{1-x} + \frac{x}{1-x}. \end{aligned}$$

Řešením rovnice $V(x) = xV(x) + \frac{x}{1-x} V(x) + \frac{x}{1-x}$ je

$$V(x) = \frac{x}{1 - 3x + x^2},$$

odkud buď standardním postupem (přes rozklad této racionální funkce na parciální zlomky) nebo s využitím předchozí úlohy přímo dostaneme, že $v_n = F_{2n}$. □

**Rekurzivně propojené posloupnosti.** Někdy dokážeme rozumně vyjádřit hledaný počet způsobů či jevů jen pomocí více vzájemně provázaných posloupností.

[2]Pokud bychom z tohoto rekurentního vztahu počítali dále numerické hodnoty $v_n$, zjistili bychom, že $v_3 = 8$, $v_4 = 21$ a mohli bychom vyslovit hypotézu o provázanosti této posloupnosti s Fibonacciovou posloupností ve tvaru $v_n = F_{2n}$, kterou je možné snadno dokázat indukcí.

V kroku 3 řešíme kvadratickou rovnici $B(x) = xB(x)^2 + 1$ pro $B(x)$ :

$$B(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Znaménko + ale nepřichází v úvahu, protože pak by pro $x \to 0_+$ měla $B(x)$ limitu $\infty$, zatímco vytvořující funkce pro naši posloupnost musí mít v 0 hodnotu $b_0 = 1$.

Zbývá už pouze krok 4, tedy rozvinout $B(x)$ do mocninné řady. Rozvoj získáme pomocí zobecněné binomické věty

$$(1-4x)^{1/2} = \sum_{k\geq 0} \binom{1/2}{k} (-4x)^k = 1 + \sum_{k\geq 1} \frac{1}{2k} \binom{-1/2}{k-1} (-4x)^k$$

a po vydělení $1 - \sqrt{1-4x}$ výrazem $2x$ dostaneme

$$\begin{aligned} B(x) &= \sum_{k\geq 1} \frac{1}{k} \binom{-1/2}{k-1} (-4x)^{k-1} = \\ &= \sum_{n\geq 0} \binom{-1/2}{n} \frac{(-4x)^n}{n+1} = \sum_{n\geq 0} \binom{2n}{n} \frac{x^n}{n+1}. \end{aligned}$$

Dokázali jsme, že počet binárních pěstovaných stromů na $n$ vrcholech je roven $b_n = \frac{1}{n+1}\binom{2n}{n}$ – tato významná posloupnost se nazývá posloupnost *Catalanových čísel*. Kromě toho, že Catalanova čísla vyjadřují počet binárních pěstovaných stromů, vystupují rovněž jako:

- počet slov délky $2n$ obsahujících $n$ znaků $X$ a $Y$ takových, že žádný prefix slova neobsahuje více $Y$ než $X$
- podobně takové fronty u pokladny (5koruny a 10koruny), že nezásobená pokladna může vždy vrátit (zároveň odtud ihned dostaneme pravděpodobnost, že náhodná fronta celá „projde“)
- počet korektně ozávorkovaných výrazů složených z levých a pravých závorek
- počet *monotónních* cest z $[0, 0]$ do $[n, n]$ podél stran jednotkových čtverců, které nepřekročí diagonálu
- počet různých triangulací konvexního $(n+2)$-úhelníku.

**12.45. Exponenciální vytvořující funkce.** Někdy mívá vytvořující funkce posloupnosti $(a_n)$ komplikované vlastnosti, přičemž posloupnost $(a_n/n!)$ má vytvořující funkci daleko jednodušší. V takových případech raději pracujeme s tzv. *exponenciálními vytvořujícími funkcemi* (e.v.f.)

$$\widehat{A}(x) = \sum_{n\geq 0} a_n \frac{x^n}{n!}.$$

Jméno vychází z toho, že vytvořující funkcí *základní* posloupnosti $(1, 1, 1, 1, \ldots)$ je $e^x$.

Základními rozvoji používanými v souvislosti s exponenciálními vytvořujícími funkcemi jsou

$$\begin{aligned} e^x &\overset{\text{e.v.f.}}{\longleftrightarrow} (1, 1, 1, \ldots), \\ \frac{1}{1-x} &\overset{\text{e.v.f.}}{\longleftrightarrow} (1, 1, 2, 6, 24, \ldots) \\ \ln \frac{1}{1-x} &\overset{\text{e.v.f.}}{\longleftrightarrow} (0, 1, 1, 2, 6, 24, \ldots) \end{aligned}$$

**12.73.** Určete, kolika způsoby lze pokrýt (nerozlišenými) kostkami domina obdélník $3 \times n$ (a vyčíslete tuto hodnotu pro obdélník $3 \times 20$)?

**Řešení.** Snadno zjistíme, že $c_1 = 0, c_2 = 3, c_3 = 0$, dále klademe $c_0 = 1$ (nejde jen o konvenci, má to svou logiku).

Najdeme rekurzivní vztah – diskusí chování „na kraji“ zjistíme, že $c_n = 2r_{n-1} + c_{n-2}$, $r_n = c_{n-1} + r_{n-2}$, $r_0 = 0, r_1 = 1$, kde $r_n$ je počet pokrytí obdélníku $3 \times n$, ze kterého jsme odstranili levý horní roh.

Hodnoty $c_n$ a $r_n$ pro několik malých $n$ jsou:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $c_n$ | 1 | 0 | 3 | 0 | 11 | 0 | 41 | 0 |
| $r_n$ | 0 | 1 | 0 | 4 | 0 | 15 | 0 | 56 |

- Krok 1: $c_n = 2r_{n-1} + c_{n-2} + [n = 0], \quad r_n = c_{n-1} + r_{n-2}$.
- Krok 2:

$$C(x) = 2xR(x) + x^2C(x) + 1, \quad R(x) = xC(x) + x^2R(x).$$

- Krok 3:

$$C(x) = \frac{1 - x^2}{1 - 4x^2 + x^4}, \qquad R(x) = \frac{x}{1 - 4x^2 + x^4}.$$

- Krok 4: Vidíme, že obě funkce jsou funkcemi $x^2$, ušetříme si práci tím, že uvážíme funkci $D(z) = 1/(1 - 4z + z^2)$, pak totiž $C(x) = (1 - x^2)D(x^2)$, tj. $[x^{2n}]C(x) = [x^{2n}](1 - x^2)D(x^2) = [x^n](1 - x)D(x)$, a tedy $c_{2n} = d_n - d_{n-1}$.

Kořeny $1 - 4x + x^2$ jsou $2 + \sqrt{3}$ a $2 - \sqrt{3}$ a již standardním způsobem obdržíme

$$c_{2n} = \frac{(2 + \sqrt{3})^n}{3 - \sqrt{3}} + \frac{(2 - \sqrt{3})^n}{3 + \sqrt{3}}.$$

Podobně jako u Fibonacciho posloupnosti je druhý sčítanec pro velká $n$ zanedbatelný a pro všechna $n$ leží mezi 0 a 1, proto

$$c_{2n} = \left\lceil \frac{(2 + \sqrt{3})^n}{3 - \sqrt{3}} \right\rceil.$$

Např. $c_{20} = 413403$. □

**12.74.** Pomocí vytvořující funkce určete počet jedniček v náhodném binárním řetězci.

**Řešení.** Označme $B$ množinu řetězců, pro řetězec $b \in B$ $|b|$ počet jeho bitů a $j(b)$ počet jedniček. Vytvořující funkce má tvar

$$B(x) = \sum_{b \in B} x^{|b|} = \sum_{n \geq 0} 2^n x^n = \frac{1}{1 - 2x}.$$

Vytvořující funkce pro počet jedniček je

$$C(x) = \sum_{b \in B} j(b) x^{|b|}.$$

**12.46. Operace s exponenciálními vytvořujícími funkcemi.** Zdůrazněme, že exponenciální vytvořující funkce se od obyčejných liší i standardními operacemi.

- Vynásobením $x$ získáme funkci posloupnosti $(na_{n-1})$.
- Derivací získáme funkci odpovídající posunutí doleva.
- Integrací získáme funkci odpovídající posunutí doprava.
- Součinem dvou funkcí $\widehat{F}(x)$ a $\widehat{G}(x)$ získáme funkci $\widehat{H}(x)$, která odpovídá posloupnosti $h_n = \sum_k \binom{n}{k} f_k g_{n-k}$, tzv. *binomické konvoluci* $f_n$ a $g_n$.

**Příklad.** Řešme rekurenci danou vztahy $g_0 = 0$, $g_1 = 1$ a předpisem

$$g_n = -2ng_{n-1} + \sum_{k \geq 0} \binom{n}{k} g_k g_{n-k}.$$

**Řešení**. Vzhledem k rekurentnímu vztahu, který obsahuje binomickou konvoluci posloupností, se zdá vhodné využít *exponenciálních vytvořujících funkcí*. Označme $\widehat{G}(x)$ příslušnou exponenciální mocninnou řadu. Budeme postupovat v obvyklých čtyřech krocích.

Krok 1: $g_n = -2ng_{n-1} + \sum_{k \geq 0} \binom{n}{k} g_k g_{n-k} + [n = 1]$.

Krok 2: $\widehat{G}(x) = -2x\widehat{G}'(x) + \widehat{G}(x)^2 + x$.

Krok 3: Řešením kvadratické rovnice dostaneme

$$\widehat{G}(x) = 1/2(1 + 2x \pm \sqrt{1 + 4x^2}).$$

Dosazením $x = 0$ vidíme, že odpovídá znaménko $-$, proto je řešením funkce

$$\widehat{G}(x) = \frac{1 + 2x - \sqrt{1 + 4x^2}}{2}.$$

Krok 4: Pomocí zobecněné binomické věty rozvineme $\widehat{G}(x)$ do mocninné řady. S využitím dříve dokázaného vztahu

$$\binom{-1/2}{k} = \left(-\frac{1}{4}\right)^k \cdot \binom{2k}{k},$$

a protože

$$\binom{1/2}{k} = \frac{1}{2k} \cdot \binom{-1/2}{k - 1},$$

postupně dostaneme

$$\sqrt{1 + 4x^2} = 1 + \sum_{k \geq 1} \frac{1}{k} \cdot (-1)^{k-1} \cdot 2 \cdot \binom{2k - 2}{k - 1} \cdot x^{2k}.$$

Odtud, protože platí

$$\sum_{n \geq 0} g_n \frac{x^n}{n!} = \widehat{G}(x) = \frac{1 + 2x - \sqrt{1 + 4x^2}}{2},$$

máme $g_{2k+1} = 0$ a

$$g_{2k} = (-1)^k \cdot \frac{1}{k} \binom{2k - 2}{k - 1} \cdot (2k)! = (-1)^k \cdot (2k)! \cdot C_{k-1},$$

kde $C_n$ je $n$-té Catalanovo číslo. □

**12.47. Cayleyho formule.** Cayleyho formule je vztah z kombinatorické teorie grafů, který udává, že počet stromů (tj. grafů, v nichž jsou libovolné dva vrcholy spojené právě jednou cestou) na $n$ vrcholech je $\kappa(K_n) = n^{n-2}$. Dokážeme tento výsledek pomocí exponenciálních vytvořujících funkcí.

Označme pro jednoduchost $t_n = \kappa(K_n)$. Lze snadno spočítat, že $t_1 = t_2 = 1, t_3 = 3, t_4 = 16$. (Např. víme, že v případě stromů na 4 vrcholech musíme z $\binom{6}{3} = 20$ potenciálních grafů s právě

Řetězec $b$ dostaneme z o jeden bit kratšího $b'$ přidáním jedné nuly nebo jedničky, tj. $j(b)$ je součtem $j(b')$ jedniček a $j(b')+1$ jedniček. Takže

$$C(x) = \sum_{b'\in B}(1+2j(b'))x^{|b'|+1} = \sum_{b'\in B} x^{|b'|+1} + 2\sum_{b'\in B} j(b')x^{|b'|+1} = \\ = xB(x) + 2xC(x).$$

Odtud

$$C(x) = \frac{x}{(1-2x)^2} = x(1-2x)^{-2}$$

a $n$-tý koeficient je $c_n = 2^{n-1}\binom{-2}{n-1} = n2^{n-1}$. Toto číslo udává počet jedniček v bitech délky $n$. Těch je $b_n = 2^n$. V jednom řetězci je tedy $\frac{c_n}{b_n} = \frac{n}{2}$ jedniček. To je samozřejmě očekávaný výsledek. □

**12.75.** Najděte vytvořující funkci a explicitní vyjádření pro $n$-tý člen posloupnosti $\{a_n\}$ definované rekurentním vztahem

$$a_0 = 1, a_1 = 2$$
$$a_n = 4a_{n-1} - 3a_{n-2} + 1 \text{ pro } n \geq 2.$$

**Řešení.** Univerzální formule platná pro všechna $n \in \mathbb{Z}$ je

$$a_n = 4a_{n-1} - 3a_{n-2} + 1 - 3[n=1].$$

Vynásobením $x^n$ a sečtením přes všechna $n$ dostaneme rovnici pro vytvořující funkci $A(x) = \sum_{n=0}^{\infty} a_n x^n$, ze které vyjádříme

$$A(x) = \frac{3x^2-3x+1}{(1-x)^2(1-3x)} = \frac{3}{4}\cdot\frac{1}{1-x} - \frac{1}{2}\cdot\frac{1}{(1-x)^2} + \frac{3}{4}\cdot\frac{1}{1-3x}.$$

Takže člen u $x^n$ je

$$a_n = \frac{3}{4}(-1)^k\binom{-1}{n} - \frac{1}{2}(-1)^n\binom{-2}{n} + \frac{3}{4}(-3)^n\binom{-1}{n} = \\ = \frac{3}{4} - \frac{1}{2}(n+1) + \frac{3}{4}3^n = d\tfrac{1-2n+3^{n+1}}{4}.$$ □

**12.76.** Pomocí vytvořující funkce vyřešte následující rekurenci:

$$a_0 = 1, a_1 = 2$$
$$a_n = 5a_{n-1} - 4a_{n-2} \quad n \geq 2$$

**Řešení.** Univerzální formule má tvar

$$a_n = 5a_{n-1} - 4a_{n-2} - 3[n=1] + [n=0]$$

Vynásobením obou stran $x^n$ a sečtením přes všechna $n$ dostaneme

$$A(x) = 5xA(x) - 4x^2A(x) - 3x + 1$$

Odtud

$$A(x) = \frac{1-3x}{(1-4x)(1-x)} = \frac{2}{3}\cdot\frac{1}{1-x} + \frac{1}{3}\cdot\frac{1}{1-4x}$$

a

$$a_n = \frac{2}{3}\tbinom{-1}{n} + \frac{2}{3}\tbinom{-1}{n}(-4)^n = \frac{4^n+2}{3}.$$ □

třemi hranami odebrat ty možnosti, kde tyto hrany tvoří trojúhelník. Těch je ale $\binom{4}{3} = 4$).

Rekurentní vztah získáme tak, že zafixujeme jeden vrchol $v$ a možné případy rozdělíme podle počtu komponent v grafu, který dostaneme z koster $K_n$ tak, že odstraníme vrchol $v$ a hrany s ním incidentní. Pak pro $n > 1$ platí

$$t_n = \sum_{m>0}\frac{1}{m!}\sum_{k_1+\cdots+k_m=n-1}\binom{n-1}{k_1,\ldots,k_m}k_1\cdots k_m\cdot t_{k_1}\cdots t_{k_m}.$$

Například pro $n = 4$ tak máme $t_4 = 3t_3 + 6t_1t_2 + t_1^3$.

Ošklivě vypadající rekurenci zjednodušíme substitucí $u_n = nt_n$ (uvědomte si přitom, že $u_n$ udává počet tzv. kořenových stromů).

Pro $n > 1$ jsme tak dostali

$$\frac{u_n}{n!} = \sum_{m>0}\frac{1}{m!}\sum_{k_1+\cdots+k_m=n-1}\frac{u_{k_1}}{k_1!}\cdots\frac{u_{k_m}}{k_m!}$$

a je vidět, že vnitřní suma je koeficient u $x^{n-1}$ v $m$-té mocnině řady $\widehat{U}(x) = \sum u_n\frac{x^n}{n!}$. Proto je

$$\frac{u_n}{n!} = [x^{n-1}]\sum_{m\geq 0}\frac{1}{m!}\widehat{U}(x)^m,$$

a tedy

$$\widehat{U}(x) = x\,\mathrm{e}^{\widehat{U}(x)}.$$

Pro dokončení výpočtu budeme potřebovat silnější tvrzení, které uvedeme bez důkazu. Tzv. *zobecněnou exponenciální mocninnou řadou* $\mathcal{E}_t(x)$ nazýváme řadu

$$\mathcal{E}_t(x) = \sum_{k\geq 0}(tk+1)^{k-1}\frac{x^k}{k!}.$$

Snadno je vidět, že $\mathcal{E}_0 = \mathrm{e}^x$, dále označujeme $\mathcal{E}(x) = \mathcal{E}_1(x)$.

**Tvrzení.** *Pro zobecněnou exponenciální řadu platí* $\ln\mathcal{E}_t(x) = x\cdot\mathcal{E}_t(x)$, *tj. speciálně*

$$\mathcal{E}(x) = \mathrm{e}^{x\mathcal{E}(x)}.$$

Srovnáním tohoto vztahu s výše uvedeným $\widehat{U}(x) = x\,\mathrm{e}^{\widehat{U}(x)}$ vidíme, že $\widehat{U}(x) = x\mathcal{E}(x)$. Proto

$$t_n = \frac{u_n}{n} = \frac{n!}{n}[x^n]\widehat{U}(x) = (n-1)![x^{n-1}]\mathcal{E}(x) = n^{n-2}.$$

**12.48. Alternativní závěr výpočtu.** Pokud vám přišel předchozí závěr výpočtu příliš umělý, zkusme to ještě jednou s využitím tzv. Lagrangeovy inverzní formule.

**Věta.** *Pokud vytvořující funkce* $g(x) = \sum_{n\geq 1} g_n x^n$ *splňuje vztah*

$$x = f(g(x)),$$

*kde* $f(0) = 0$, $f'(0) \neq 0$, *pak*

$$g_n = \frac{1}{n}[u^{n-1}]\left(\frac{u}{f(u)}\right)^n.$$

Řešíme rovnici $\widehat{U}(x) = x\,\mathrm{e}^{\widehat{U}(x)}$, tj. $\widehat{U}(x)$ splňuje vztah $x = f(\widehat{U}(x))$, kde $f(u) = \frac{u}{e^u}$. Odtud z Lagrangeovy formule

$$[x^n]\widehat{U}(x) = \frac{1}{n}[u^{n-1}]\left(\frac{u}{u/e^u}\right)^n = \frac{1}{n}\frac{n^{n-1}}{(n-1)!} = \frac{n^{n-1}}{n!}$$

Protože $\frac{u_n}{n!} = [x^n]\widehat{U}(x)$, dostáváme odtud

$$t_n = \tfrac{u_n}{n} = n^{n-2}.$$

**12.77.** Bankomat vydává bankovky v hodnotě 200, 500 a 1 000 korun. Kolika způsoby mohu vybrat 7 000 korun? Ukažte řešení pomocí vytvořující funkce.

**Řešení.** Úlohu můžeme přeformulovat jako hledání počtu celočíselných řešení

$$2a + 5b + 10c = 70; \quad a, b, c \geq 0.$$

To je také rovno koeficientu u $x^{70}$ v funkce

$$G(x) = (1 + x^2 + x^4 + \cdots)(1 + x^5 + x^{10} + \cdots)(1 + x^{10} + x^{20} + \cdots)$$

Tato funkce je rovna

$$G(x) = \frac{1}{1 - x^2} \frac{1}{1 - x^5} \frac{1}{1 - x^{10}}$$

a protože

$$\frac{1 - x^{10}}{1 - x^5} = 1 + x^5 \text{ a } \frac{1 - x^{10}}{1 - x^2} = 1 + x^2 + x^4 + x^6 + x^8,$$

můžeme ji upravit do tvaru

$$G(x) = \frac{(1 + x^2 + x^4 + x^6 + x^8)(1 + x^5)}{(1 - x^{10})^3}.$$

Podle binomické věty máme

$$(1 - x^{10})^{-3} = \sum_{k=0}^{\infty} (-1)^k \binom{-3}{k} x^{10k},$$

proto je $G(x)$ rovna

$$(1 + x^2 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{13}) \sum_{k=0}^{\infty} (-1)^k \binom{-3}{k} x^{10k}$$

Mocninu $x^{70}$ dostaneme jediným způsobem a to jako $7 \cdot 10 + 0$, tj. koeficient u $x^{70}$ je roven

$$[x^{70}]G(x) = -\binom{-3}{7} = \binom{3+7-1}{7} = \frac{9 \cdot 8}{2} = 36. \qquad \square$$

## J. Doplňující příklady k celé kapitole

*12.78.* Určete, kolik hran musíme přidat do

i) kružnice $C_n$ o $n$ vrcholech,

ii) úplného bipartitního grafu $K_{m,n}$,

abychom dostali úplný graf. ○

*12.79.* Označme vrcholy v grafu $K_6$ postupně čísly $1, 2, \ldots 6$ a každou hranu $\{i, j\}$ ohodnoťme číslem $[(i + j) \bmod 3] + 1$. Kolik existuje různých maximálních koster v tomto grafu? ○

*12.80.* Označme vrcholy v grafu $K_7$ postupně čísly $1, 2, \ldots 7$ a každou hranu $\{i, j\}$ ohodnoťme číslem $[(i + j) \bmod 3] + 1$. Kolik existuje různých minimálních koster v tomto grafu? ○

*12.81.* Označme vrcholy v grafu $K_5$ postupně čísly 1, 2,...5 a každou hranu $i, j$, $i = 1, \ldots, 5$ ohodnoťme číslem 1, pokud je $(i + j)$ liché, číslem 2, pokud je $(i + j)$ sudé. Kolik existuje různých maximálních koster v tomto grafu? ○

*12.82.* Označme vrcholy v grafu $K_5$ postupně čísly 1, 2,...5 a každou hranu $\{i, j\}$, $i = 1, \ldots, 5$ ohodnoťme číslem 1, pokud je $(i + j)$ liché, číslem 2, pokud je $(i + j)$ sudé. Kolik existuje různých minimálních koster v tomto grafu? ○

*12.83.* Označme vrcholy v grafu $K_6$ postupně čísly 1, 2,...6 a každou hranu $i, j$, $i = 1, \ldots, 6$ ohodnoťme číslem 1, pokud je $(i + j)$ dává zbytek 1 po dělení třemi, číslem 2, pokud je $(i + j)$ dává zbytek 2 po dělení třemi a konečně číslem 3, pokud je $(i + j)$ dělitelné třemi. Kolik existuje různých minimálních koster v tomto grafu? ○

*12.84.* Označme vrcholy v grafu $K_6$ postupně čísly 1, 2,...6 a každou hranu $i, j$, $i = 1, \ldots, 6$ ohodnoťme číslem 1, pokud je $(i + j)$ dává zbytek 1 po dělení třemi, číslem 2, pokud je $(i + j)$ dává zbytek 2 po dělení třemi a konečně číslem 3, pokud je $(i + j)$ dělitelné třemi. Kolik existuje různých maximálních koster v tomto grafu? ○

*12.85.* **Icosian Game –** nalezněte hamiltonovskou kružnici v grafu tvořeném vrcholy a hranami pravidelného dodekaedru (dvanáctistěnu). ○

**Řešení.** Viz Wikipedia[3]. □

*12.86.* Existuje hamiltonovská kružnice v Petersenově grafu? ○

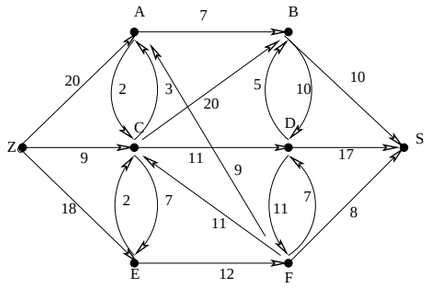
**Řešení.** Neexistuje (přitom ale po odebrání libovolného vrcholu již graf hamiltonovský bude). Ukáže se to např. tak, že se popíší všechny 3-regulární grafy na 10 vrcholech, které jsou hamiltonovské a v každém se nalezne kružnice kratší než 5. □

*12.87.* Je-li $G = (V, E)$ hamiltonovský a $\emptyset \neq W \subsetneq V$, pak $G \setminus W$ má nejvýše $|W|$ komponent souvislosti.

Ukažte na konkrétním příkladu grafu, že opak obecně neplatí. ○

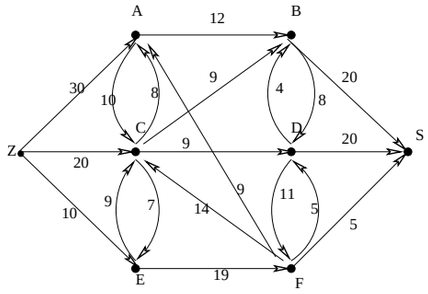
*12.88.* Určete maximální tok a jemu odpovídající minimální řez v následujícím ohodnoceném orientovaném grafu:

[3] Wikipedia, *Icosian game*, `http://en.wikipedia.org/wiki/Icosian_game` (as of Aug. 8, 2013, 13:24 GMT).



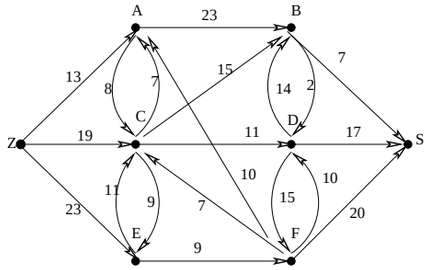

○

*12.89.* Určete maximální tok a jemu odpovídající minimální řez v následujícím ohodnoceném orientovaném grafu:



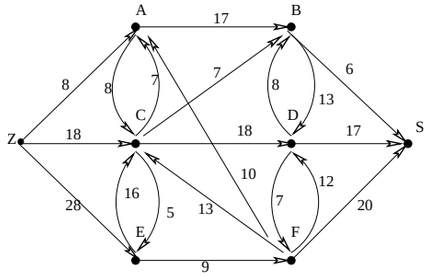

○

*12.90.* Určete maximální tok a jemu odpovídající minimální řez v následujícím ohodnoceném orientovaném grafu:




○

*12.91.* Určete maximální tok a jemu odpovídající minimální řez v následujícím ohodnoceném orientovaném grafu:



○

*12.92.* Určete vytvořující funkce následujících posloupností

i) $(1; 2; 1; 4; 1; 8; 1; 16; \dots)$

ii) $(1; 1; 0; 1; 1; 0; 1; 1; \dots)$

iii) $(1; -1; 2; -2; 3; -3; 4; -4; \dots)$

○

**Řešení.**

i) $(1; 2; 1; 4; 1; 8; 1; 16; \dots) = (1; 0; 1; 0; \dots) + (0; 2; 0; 4; 0; 8; \dots)$. Určíme tedy vytvořující funkce jednotlivých posloupností. První dostaneme z posloupnosti (1, 1, 1, 1, 1). Její vytvořující funkce je $\frac{1}{1-x}$. Nuly vnoříme nahrazením $x^2$ za $x$. Podobně druhou vytvořující funkci dostaneme z posloupnosti $(1; 2; 4; 8; 16; \dots)$. Nejprve vynásobíme dvěma, vložíme nuly a pak vynásobením $x$ dostaneme nulu na začátku.

ii) $(1; 1; 0; 1; 1; 0; 1; 1; \dots) = (1; 0; 0; 1; 0; 0; 1 \dots) + (0; 1; 0; 0; 1; 0; 0; 1 \dots)$.

i) $\frac{1}{1-x^2} + \frac{2x}{1-2x^2}$

ii) $\frac{1+x}{1-x^3}$

iii) $\frac{1}{(1-x^2)^2} + \frac{-x}{(1-x^2)^2}$

□

*12.93.* Určete koeficient u $x^{17}$ v $(x^3 + x^4 + x^5 + \dots)^3$ ○

**Řešení.** $(x^3 + x^4 + x^5 + ...)^3 = \frac{x^9}{(1-x)^3} = x^9 \cdot \frac{1}{(1-x)^3}$. Zajímá nás tedy koeficient u $x^8$ v $\frac{1}{(1-x)^3}$. Ten je roven $\binom{10}{2}$, tedy 45. □

*12.94.* Jaká je pravděpodobnost, že při hodu 12 hracími kostkami padne součet 30?
*Nápověda: Vyjádřete počet všech možností, kdy padne součet 30. Uvažujte* $(x+x^2+x^3+x^4+x^5+x^6)^{12}$.

○

**Řešení.** Výsledná pravděpodobnost bude podílem počtů příznivých a všech možností. Počet všech možností je $6^{12}$. Spočítejme nyní počet příznivých možností. Uvažujme výraz $(x + x^2 + x^3 + x^4 + x^5 + x^6)^{12}$. Počet příznivých možností je potom koeficient u $x^{30}$. Upravujme:

$$(x+x^2+x^3+x^4+x^5+x^6)^{12} = \left(\frac{x(1-x^6)}{1-x}\right)^{12} = x^{12} \cdot \left(\frac{1-x^6}{1-x}\right)^{12}$$

Zajímá nás tedy koeficient u $x^{18}$ u

$$\left(\frac{1-x^6}{1-x}\right)^{12} = (1 - 12x^6 + 66x^{12} - 220x^{18}) \cdot \frac{1}{1-x}^{12}.$$

Ze zobecněné binomické věty pak dostáváme počet příznivých možností

$$\binom{29}{11} - 12 \cdot \binom{23}{11} + 66 \cdot \binom{17}{11} - 220 \cdot \binom{11}{11}.$$

□

*12.95.* Sadař má vysadit 25 nových stromků, přičemž má k dispozici pouze 4 druhy. Sadařova manželka si však klade omezující podmínky: nejvýše jeden ořešák, nejvýše 10 jabloní, alespoň 6 třešní a alespoň 8 slivoní Kolik existuje různých způsobů výběru druhů stromů?

*Nápověda: Zajímá nás koeficient u $x^{25}$ ve výrazu*

$$(1+x)(1+x+\cdots+x^{10})(x^6+x^7+\dots)(x^8+x^9+\dots).$$

○

**Řešení.**

$$(1+x)(1+x+\cdots+x^{10})(x^6+x^7+\dots)(x^8+x^9+\dots) = \frac{x^{14}(1-x^2)(1-x^{11})}{(1-x)^4}.$$

Zajímá nás tedy koeficient u $x^{11}$ ve $(1-x^2-x^{11}\dots)\cdot\frac{1}{(1-x)^4}$, tím je $\binom{14}{3}-\binom{12}{3}-\binom{3}{3}$. □

*12.96.* Vyjádřete obecný člen posloupností určených následujícími rekurencemi:

i) $a_1=3, a_2=5, a_{n+2}=4a_{n+1}-3a_n$ pro $n=1,2,3\dots$.

ii) $a_0=0, a_1=1, a_{n+2}=2a_{n+1}-4a_n$ pro $n=0,1,2,3\dots$.

○

**Řešení.**

i) $a_n=2+3^{n-1}$.

ii) $a_n=\frac{1}{2}\sqrt{-3}\cdot((1+\sqrt{-3})^n-(1-\sqrt{-3})^n)$.

□

*12.97.* Řešte rekurenci, kde v posloupnosti $(a_0,a_1,a_2,\dots)$ je následující člen aritmetickým průměrem předchozích dvou. ○

**Řešení.** $a_n=k\left(-\frac{1}{2}\right)^n+l$. □

*12.98.* Řešte rekurenci $a_{n+2}=\sqrt{a_{n+1}a_n}$ s počátečními podmínkami $a_0=2, a_1=8$.

*Nápověda: Utvořte novou posloupnost $b_n=\log_2 a_n$.* ○

*12.99.* Vyřešíme rekurenci danou vztahem

$$a_n=\sum_{k\geq 0}\binom{n}{k}\frac{a_k}{2^k}, a_0=1.$$

*Nápověda: Vynásobte obě strany $\frac{x^n}{n!}$ a sečtěte. Přitom $\widehat{A}(X)$ je exponenciální vytvořující funkce posloupnosti $(a_n)$.* ○

*12.100.* Spočtěte počet triangulací konvexního $n$-úhelníku.

*Nápověda: Vyberme libovolnou úhlopříčku jdoucí pevným vrcholem. Ta nám mnohoúhelnk rozdělí na dva.* ○

**Řešení.** $t_n=C_{n-2}$, kde $C_n$ značí Catalanovo číslo. □

*12.101.* Určete počet procházek ve čtvercové síti o rozměrech $n\times n$ z levého dolního rohu $A$ do pravého horního rohu $B$, které vedou pouze doprava a nahoru takových, že mají právě jeden bod na diagonále $AB$ (nepočítaje $A$ a $B$).

*Nápověda: Catalanova čísla.* ○

*12.102.* Dokažte, že pro Fibonacciho čísla platí:

i) $F_2+F_4+\cdots+F_{2n}=F_{2n+1}-1$

ii) $F_1+F_3+\cdots+F_{2n-1}=F_{2n}$

○

*12.103.* Označme $H_n$ minimální počet kroků potřebných k přemístění věže o $n$ kotoučích z jednoho kolíku na druhý u hlavolamu Hanojská věž. Odvoďte rekurentní formuli pro výpočet $H_n$ a určete její obecné řešení. ○

**Řešení.** $H_{n+1} = 2H_n + 1$, $H_n = 2^n - 1$. □

A na závěr knihy jeden příklad z praxe.

**12.104.** Volejbalový tým (s liberem, tj. celkem sedm osob) sedí po zápase v hospodě a popíjí zasloužené pivo. Hospodský má k dispozici pouze sedm kríglů.[4] Jaká je pravděpodobnost, že příště

i) právě jeden volejbalista nebude pít ze stejného kríglu,

ii) nikdo nebude pít ze stejného kríglu,

iii) právě tři budou pít ze stejného kríglu.

**Řešení.**

i) Pokud šest lidí dostane ten svůj, tak zákonitě i ten sedmý, pravděpodobnost je tedy nulová.

ii) Nechť $M$ je množina všech pořadí sedmi hráčů a jev $A_i$ je pořadí, kdy $i$-tý hráč dostane svůj krígl. Chceme spočítat $|M - \cup_i A_i|$. Dostáváme $7! \sum_{k=0}^{7} \frac{(-1)^k}{k!} = 1854$. A pravděpodobnost je $\frac{1854}{5040} = \frac{103}{280} \doteq 0{,}37$.

iii) Pro výběr těch tří, kteří dostanou svůj krígl, je $\binom{7}{3} = 35$ možností. Zbylí čtyři musí dostat jiné než svoje. To je opět vzorec z minulého bodu, konkrétně jde o $4! \sum_{k=0}^{4} \frac{(-1)^k}{k!} = 9$ možností. Máme tedy dohromady $9 \cdot 35 = 315$ možností a pravděpodobnost je $\frac{315}{5040} = \frac{1}{16}$.



□

[4] Krígl je specifická nádoba, ze které se pije pivo v hospodě.

## Řešení cvičení

*12.7.* Artikulací jsou vrcholy 0, 1, 9, 10. Mosty tvoří hrany (0, 1), (0, 12), (9, 10).
*12.15.* (3, 1), (3, 2), (3, 4), (3, 5), (3, 6), (6, 1), (6, 2), (6, 4), (6, 5), (5, 1), (5, 2), (5, 4), (4, 1), (4, 2), (2, 1).
*12.16.* (3, 1), (3, 2), (3, 4), (3, 5), (3, 6), (1, 2), (1, 4), (1, 5), (1, 6), (2, 4), (2, 5), ... (5, 6).
*12.24.* Postupem podle Havla a Hakimiho se snadno ukáže, že takový graf existuje. Rovinný ale nikoliv: $|V| = 10$, $|E| = 35$ a aby byl rovinný, muselo by platit $3|V| - 6 \geq |E|$, tj. $24 \geq 35$.
*12.27.*

i) Ano. Plyne ihned z Kuratowského věty ($K_5$ má 10 hran, $K_{3,3}$ 9 hran).
ii) Ne. Protipříkladem je $K_5$ i $K_{3,3}$.
iii) Ne. Mnoho protipříkladů (např. $K_{3,3}$ s přidaným vrcholem a do něj vedoucí hranou).
iv) Ne. Protipříkladem je $K_5$.
v) Ne. Protipříkladem je $K_{3,3}$.
vi) Totéž jako (ii).
vii) Ne. Protipříkladem je $C_n$.
viii) Ne. Protipříkladem je $K_5$.
ix) Ne. Protipříkladem je $C_n$.

*12.29.* V prvním případě ne (existuje vlastní prefix kódu se stejným počtem nul a jedniček), v druhém případě strom existuje.
*12.34.* Postup není správný. Stačí uvážit například kružnici s hranami ohodnocenými až na jednu jedničkami, zbývající hrana ohodnocená dvojkou.
*12.35.* Aplikací libovolného algoritmu na hledání minimální kostry zjistíme, že hledaná délka je 12154. (v kostře jsou hrany LPe, LP, LNY, PeT, MCNY).
*12.41.* Najdeme maximální tok velikosti 15 a rovněž řez [1, 6], [1, 3], [2, 4], [2, 3] téže kapacity.
*12.43.* Z teorie a předchozího příkladu víme, že kapacita minimálního řezu je 9. Maximální tok $f$ není zadán jednoznačně. Můžeme volit například $f(a) = 2$, $f(b) = 4$, $f(c) = 1$, $f(h) = 1$, $f(j) = 4$, $f(f) = 2$, $f(i) = 7$, $f(v) = 0$ pro všechny ostatní hrany $v$ daného grafu.
*12.50.*

$$1 - \frac{4! \cdot 4!}{\frac{8!}{2^4}} = \frac{27}{35}$$

.
*12.51.* $\frac{49}{54}$.
*12.64.*

i) Z příkladu v části 12.42 víme, že vytvořující funkcí posloupnosti $(1, 2, 3, 4, \ldots)$ je funkce $\frac{1}{(1-x)^2}$.
ii) Protože je (i podle předchozí úlohy)

$$\frac{x}{(1-x)^2} \overset{\text{v.f.p.}}{\longleftrightarrow} (0, 1, 2, 3, \ldots),$$

máme pro derivaci této funkce

$$\left(\frac{x}{(1-x)^2}\right)' = \frac{1+x}{(1-x)^3} \overset{\text{v.f.p.}}{\longleftrightarrow} (1 \cdot 1, 2 \cdot 2, 3 \cdot 3, \ldots).$$

Podotkněme, že tuto úlohu bylo možné řešit i se znalostí toho, že $\frac{1}{(1-x)^3} \overset{\text{v.f.p.}}{\longleftrightarrow} \binom{n+2}{n}$.

iii) Máme

$$\frac{1}{1-x} \overset{\text{v.f.p.}}{\longleftrightarrow} (1,1,1,1\dots),$$
$$\frac{1}{1-2x} \overset{\text{v.f.p.}}{\longleftrightarrow} (1,2,4,8,\dots),$$
$$\frac{1}{1-2x^2} \overset{\text{v.f.p.}}{\longleftrightarrow} (1,0,2,0,4,0,\dots),$$
$$\frac{x}{1-2x^2} \overset{\text{v.f.p.}}{\longleftrightarrow} (0,1,0,2,0,4,\dots),$$

odkud dostáváme výsledek

$$\frac{1+x}{1-2x^2} \overset{\text{v.f.p.}}{\longleftrightarrow} (1,1,2,2,4,4,8,8,\dots).$$

iv) Z předchozího víme, že $f(x) = \frac{1+x}{(1-x)^3} \overset{\text{v.f.p.}}{\longleftrightarrow} (1^2, 2^2, 3^2, \dots)$, proto

$$\frac{f(x)-(1+4x)}{x^2} \overset{\text{v.f.p.}}{\longleftrightarrow} (3^2, 4^2, 5^2, \dots).$$

Substitucí $2x^3$ za $x$ dostaneme

$$\frac{f(2x^3)-(1+8x^3)}{4x^6} \overset{\text{v.f.p.}}{\longleftrightarrow} (9,0,0,2\cdot 16,0,0,4\cdot 25,\dots).$$

v) Pokud označíme $F(x)$ výsledek předchozí úlohy, pak je výsledkem

$$F(x) - x^2 F(x) + \tfrac{x}{1-x^3}.$$

*12.71.* $x/(1-3x+x^2)$

*12.78.*

i) Úplný graf na $n$ vrcholech má $\frac{n(n-1)}{2}$ hran, kružnice na $n$ vrcholech má $n$ hran. Musíme tedy ke kružnici přidat $\frac{n(n-1)}{2} - n$ hran.

ii) Podobně jako výše dostaneme výsledek $\frac{(m+n)(m+n-1)}{2} - m \cdot n$.

*12.79.* Hrany s ohodnocením tři tvoří kružnici 23562 délky čtyři a hranu 14. Jde tedy o nesouvislý podgraf daného grafu. Není tedy možné vybrat kostru daného grafu pouze z hran s ohodnocením tři. Maximální kostra bude mít tedy součet ohodnocení hran v ní nejvýše $4 \cdot 3 + 2 = 14$. Kostru s touto hodnotou skutečně můžeme vybrat. Z hran s ohodnocením 3 můžeme vypustit libovolnou hranu ze zmiňované kružnice a nezávisle přidáme nějakou hranu s ohodnocením dvě, která spojuje v podgrafu hran s ohodnocením tři komponentu 2356 s komponentou 14. Takové hrany jsou celkem čtyři. Celkem má daný graf $4 \cdot 4 = 16$ různých maximálních koster.

*12.80.* Nejlevnější hrany s ohodnocením jedna tvoří podgraf obshahující všechny vrcholy a mající dvě komponenty, které mohou být propojeny nějakou hranou s druhým nejmenším ohodnocením. Minimální kostra má tedy součet ohodnocení jejch hran minimálně $6 \cdot 1 + 2 = 8$. Kostry s touto hodnotou skutečně existují, je totiž šest hran hodnoty 2, které propojují zmiňované dvě komponenty. Konkrétně jde o komponentu $\{1,2,4,5,7\}$ a $\{3,6\}$. V první komponentě existují právě tři kružnice a to délky 4, přičemž každá ze šesti hran této komponenty leží právě ve dvou kružnicích. Abychom z dané komponenty získali strom, musíme dvě hrany vypustit, to můžeme udělat $6 \cdot 4/2$ způsoby. Celkem dostáváme $12 \cdot 6 = 72$ různých minimálních koster.

*12.81.* 18.

*12.82.* 12.

*12.83.* 16.

*12.84.* 16.

*12.88.* Min. řez je dán množinou $\{Z, A, E\}$. Hodnota je 32.

*12.89.* Min. řez odpovídá množině $(B, D, S)$. Hodnota je 40.

*12.90.* Řez je dán množinou $\{F, S, D\}$, hodnota je 29.

*12.91.* Min. řez je dán množinou $\{F, S\}$, jeho hodnota je 39.

# Rejstřík


abelovská grupa, 642
$k$-tý absolutní moment, 561
absolutní hodnota, 248
absorpčníproces, 146
absorpční zákony, 687
adjungovaná matice, 153
adjungované zobrazení, 152
afinní
  kombinace bodů, 198
  obal, 195
  podprostor, 195
  repér, 195
  souřadnice v rovině, 28
  soustava souřadnic, 195
  varieta, 669
  zobrazení, 32, 201
  poměr bodů, 202
akce grupy $G$ na množině, 654
$\sigma$–algebra, 533
algebraický doplněk, 83
algebraická násobnost, 110, 157
algoritmus
  Borůvkův, 736
  Dijkstrův, 720
  ElGamal, 636
  Euklidův, 591
  Floydův-Warshallův, 716
  Fordův-Fulkersonův, 739
  Jarníkův, 736
  Kruskalův, 735
  Lagrangeův, 217
  Primův, 736
alternativní hypotéza, 579
analýza citlivosti, 579
analytický tvar, 213
aposteriorní, 577
apriorní, 577
aritmetické reprezentanty, 221
aritmetický průměr, 275, 527
artikulace, 710
asociativita, 8
asociativní operace, 642
asymptota bez směrnice, 336
asymptota se směrnicí, 335
asymptotický odhad, 343
asymptoty, 335
atom, 694
axiomy čísel, 8

báze, 28
  standardní, 92
  báze vektorového prostoru, 89
barvení grafu, 710
Bayesův vzorec, 537
bayesovská statistika, 571
Bellovo číslo, 43
Bernoulliova nerovnost, 276
Beta funkce, 581
Bezoutova věta, 591
binární
  operace, 641
  relace, 39
  strom, 726
  vyhledávací strom, 726
binomická čísla, 12
binomický rozvoj, 12
binomické kongruence, 616
binormála křivky, 341
bipartitní graf, 709
bipartitní párování, 741
bit, 697
bod nespojitosti, 355
bod zvratu, 677
bodový euklidovský prostor, 203
bodový odhad, 574
body v obecné poloze, 198, 223
Booleovská algebra, 686
bootstrap, 586
Borelovské množiny, 539

Carmichaelova čísla, 625
Casoratián, 132
částečné uspořádání, 690
částečný součet, 279

cauchyovská posloupnost, 249, 410
$k$-tý centrální moment, 561
cesta, 709, 711
charakteristická funkce množiny, 358
charakteristická rovnice, 132, 511
charakteristický polynom, 134
charakteristický polynom matice, 104
charakteristický polynom zobrazení, 104
charakteristika, 511
chyba druhého druhu, 579
chyba prvního druhu, 579
člen determinantu, 78
čtvercová matice, 70
cyklická grupa, 647, 650
cyklické zobrazení, 157
cyklický žebřík, 710
cyklus, 80, 644

délka křivky, 359
důsledek jevu, 20, 534
dělitelnost, 661
Darbouxův integrál, 352
De Morganova pravidla, 687
decily, 556
definiční obor funkce, 10
definiční obor relace, 39
dekonvoluce, 430
derivace, 242, 264
  jednostranná, 265
  nevlastní, 265
  parciální druhého řádu, 446
  parciální $k$-tého řádu, 447
  vlastní, 265
  ve směru vektoru, 442
determinant, 31
determinant matice, 78
diferenční rovnice
  lineární, 15
  prvního řádu, 15
diference
  dopředná, 343
  druhého řádu, 343
  středová, 343
  zpětná, 343
diferenciál funkce, 337, 443
diferenciál zobrazení, 454
diferenciální rovnice
  Bernoulliho typu, 494
  homogenní, 493
  Riccatiho typu, 494
diferenční rovnice
  homogenní lineární řádu $k$, 131
dihedrální grupa, 646

dimenze, 67, 89, 194
dimenze matice, 70
diofantické rovnice, 623
Diracova funkce $\delta$, 430
Dirichletův součin, 602
Dirichletova podmínka, 421
Dirichletovo jádro, 424
discrete logarithm problem, 636
diskrétní grupa symetrií, 647
diskrétní logaritmus, 607
diskrétní náhodná veličina, 542
distribuční funkce, 540
distributivita, 8, 656
distributivní svaz, 692
divergentní posloupnost, 256
dokonalé číslo, 596
dolní a horní kvartil, 528
dolní Riemannův integrál, 355
dolní Riemannův součet, 352
dolní závora, 247, 691
doplněk, 686
doplněk minoru, 83
dosažená hladina testu, 580
druhá derivace, 327
duální báze, 97
duální projektivní prostor, 224
duální prostor, 97
duální tvrzení, 687
duální zobrazení, 152
dvojpoměr čtveřice bodů , 224
dělení se zbytkem, 589
dělitelnost, 589

ekvivalence, 600
elementární řádkové transformace, 73
elementární sloupcové transformace, 73
elementární jevy, 534
eliptická křivka , 677
entropie, 532
Euklidův algoritmus, 591
euklidovská rovina, 33
euklidovská transformace, 216
euklidovské podprostory, 203
Eulerova aproximace, 497
Eulerovo číslo e, 277
eulerovské grafy, 723
eulerovský sled, 723
eulerovský tah, 723
exaktnost, 654
excentricita, 728
exponenciální vytvořující funkce, 752
exponenta matice, 509

faktor, 711
faktoriál, 10
faktorová grupa, 653
faktorový vektorový prostor, 159
Fermatova čísla, 630
forma
  $k$-lineárních, 101
  antisymetrická bilineární, 101
  bilineární, 101
  symetrická bilineární, 101
Fourierův ortogonální systém, 403
Fourierova řada, 405
Fourierova kosinusová transformace, 431
Fourierova sinusová transformace, 431
Fourierova transformace, 427
Fourierovy koeficienty, 403
Fourierovy koeficienty funkce, 405
frekvenční statistika, 571
Frenetův repér, 341
Frenetovy–Serretovy vzorce, 341
Fresnelovy sinové a kosinové integrály, 357
fundamentální systém řešení, 126, 132
funkce
  analytická, 332
  cyklometrická, 287
  diferencovatelná, 265
  diferencovatelná v bodě, 443
  $(k+1)$–krát diferencovatelná, 327
  dvakrát diferencovatelná, 327
  exponenciální, 263
  Heavisideova, 246
  hladká, 327
  hyperbolická, 288
  klesající na intervalu, 267
  klesající v bodu, 267
  komplexní funkce reálné proměnné, 237
  konkávní, 334
  konvexní, 334
  lipschitzovsky spojitá, 458
  logaritmická se základem $a$, 264
  mocninná, 263,
  periodická, 287,404
  po částech spojitá, 355
  racionální, 262
  reálné proměnné, 237
  rostoucí na intervalu, 266
  rostoucí v bodě, 266
  ryze racionální lomená, 348
  skalární, 10
  spojitá v bodě, 259
  spojitá zprava, resp. zleva, 260
  stejnoměrně spojitá, 355
  třídy $C^k$, 447
  třídy $C^k(A)$, 327
funkce náhodné veličiny, 552

gaussián, 332
Gaussova eliminace, 73
Gaussova křivka, 549
generátory, 88
generování afinního podprostoru, 195
geometrická řada, 284
geometrická násobnost, 110, 157
geometrické body, 221
geometrický průměr, 276, 527
geometrická báze, 223
Gibbsův jev, 407
goniometrické funkce, 285
gradient funkce, 463
graf, 708
graf zobrazení, 40
Gramův–Schmidtův ortogonalizační proces, 99
Gramův determinant, 209
grupa, 642
  komutativní, 8
grupa permutací, 643
grupoid, 641

hamiltonovská kružnice, 724
Hammingova vzdálenost, 698
harmonický průměr, 275
Hasseho diagram, 691
hermiteovské matice, 153
Hermiteův interpolační polynom, 244
Hessián funkce, 448
  negativně definitní, 452
  negativně semidefinitní, 452
  positivně definitní, 452
  positivně semidefinitní, 452
histogram, 526
hladina testu, 579
hlavní ideál, 672
hlavní normála, 341
hlavních minorech, 83
hodnost kvadratické formy, 213
hodnost matice, 77
$p$–hodnota testu, 580
homogenní úloha, 125
homogenní lineární diferenční rovnice, 131
homogenní lineární rekurence, 131
homogenní souřadnice, 220, 221
homomorfismus Booleovských algeber, 692
homotetie, 102
horní Riemannův integrál, 355
horní Riemannův součet, 352
horní závora, 247, 691

hra, 742
hrana grafu, 708
hraniční bod, 253, 419
hraniční vrcholy, 708
hranice simplexu, 198
hranový seznam, 714
hranově $k$–souvislý graf, 718
hromadné body podmnožiny, 411
hromadný bod množiny, 251
hustota pravděpodobnosti, 543
hyperkostka, 709
hypotéza, 579

idempotentnost, 687
identita
  Besselova, 403
imaginární složka, 8
imerze, 479
implicitní popis, 196
indefinitní Hessián, 452
index, 607
indukovaný podgraf, 711
infimum, 247, 686
infimum množiny, 691
inflexní bod, 335
integrál formy, 483
integrální křivka, 505
integrální věta o střední hodnotě, 355, 359
integrál
  Newtonův, 345
  Riemannův, 350
interpolační polynom, 239
intervalový odhad, 574
invariantní podprostor, 105
inverze v permutaci $\sigma$, 79
inverzní Fourierova transformace, 428
inverzní funkce, 269
inverzní pravděpodobnosti, 537
inverzní prvek, 8, 642
izolovaný bod, 419, 253
izometrie, 415
izomorfismus, 93, 649, 711
izotonní zobrazení, 692
izotropní podgrupa, 655

jádro, 93, 649
jádro integrálního operátoru $L$, 427
Jacobiho matice zobrazení, 454
Jacobiho symbol, 622
jednotka, 642
jednotková matice, 34
jednotkový prvek, 8
jednotky, 661
jednovýběrový t-test, 585
jevové pole, 19, 533
jevy, 19, 533
  elementární, 20
  jisté, 20, 534
  náhodné, 19
  nastoupení alespoň jednoho, 20
  nemožné, 20
  neslučitelné, 20
  opačné, 20
  společné nastoupení, 20
  stochasticky nezávislé, 23
join, 686
Jordanova míra, 359, 473
Jordanův blok, 157
Jordanův rozklad, 157

kalibr, 373
kanonický analytický tvar, 214
kapacita řezu, 739
kapacitní omezení, 738
kartézská souřadná soustava, 203
kartézský součin, 39
kladný směr rotace, 34
kladná matice, 141
klasická pravděpodobnost, 535
Kleeneho řetězec, 694
klika, 711
koeficient šikmosti náhodné veličiny, 564
koeficient špičatosti, 564
koeficienty polynomu, 238, 658
kód kontrolující paritu, 697
kód pěstěného stromu, 727
kódové slovo, 697
kolineace, 222
kolmé, 98
kolmý, 154
kolmou projekci, 99
kombinační čísla, 12
kombinace, 12
  s opakováním, 14
komplexně sdružené číslo, 8
komplexní čísla, 8
komplexní Fourierovy koeficienty, 405
komutativita, 8
komutativní grupa, 642
komutativní okruh, 8, 656
komutativní pologrupa, 642
komutativním těleso, 8
koncové vrcholy, 725
koncový vrchol hrany, 708
konečný automat, 709
konečně rozměrný prostor, 89

kongruence modulo $m$, 600
kongruence o jedné neznámé, 610
konjugace, 248
kontrahující zobrazení, 418
kontrakce, 495
konvergence, 249
konvergence podle distribuční funkce, 566
konvergence podle pravděpodobnosti, 558
konvergence posloupnosti, 256
konverguje, 411
konvexní, 199
konvexní mnohostěny, 199
konvexní obal, 199
konvoluce, 748
konvoluce funkcí, 426
konzistentní odhad, 575
korelační koeficient, 560
korelace veličin, 560
kořen polynomu, 239, 658
kořen stromu, 726
kořenové stromy, 726
kořenový prostor, 159
kořenový vektore, 158
kostra, 733
krátká exaktní posloupnost grup, 653
krabicový diagram, 524, 530
kritické body, 329
kritický bod řádu $k$, 334
kritický obor, 579
kritická hodnota na úrovni $\alpha$, 557
kritérium
  Leibnizovo, 283
  Sylvestrovo kritérium, 219
  Weierstrassovo, 367
křivost, 338
křivost křivky, 341
Kroneckerovo delta, 70
kružnice, 709, 711
kubický interpolační splajn, 245
kumulativní četnosti, 526
kumulativní třídní četnosti, 526
kvadratická regrese, 580
kvadratická forma, 213
  indefinitní, 218
  negativně definitní, 218
  negativně semidefinitní, 218
  pozitivně definitní, 218
  pozitivně semidefinitní, 218
kvadrika, 212
$\alpha$–kvantil, 527
kvantilové koeficienty šikmosti, 530
kvantilová funkce, 556
kvartilové rozpětí výběru, 528
kód
  $(n, k)$-kódy, 697
  lineární, 700
  polynomiální , 698
křivka parametrizovaná délkou, 341

L'Hospitalovo pravidlo, 273
Lagrangeův interpolační polynom, 240
Laplaceova transformace, 432
Laplaceův rozvoj, 84
Legendreův symbol, 617
Legendreovy polynomy, 400
Leibnizovo pravidlo, 268
les, 725
Leslieho model růstu, 139
levá jednotka, 642
levé třídy rozkladu, 651
levá inverze, 642
limes superior, 282
limita, 249, 255, 411
  nevlastní, 255
  vlastní, 255
  zleva, 256
  zprava, 256
lineární algebra, 27
lineární forma, 97, 479
lineární funkcionál, 425
lineární kombinace, 76, 87
lineární kombinace vektorů, 28
lineární model, 582
lineární omezení, 127
lineární zobrazení, 30, 93
lineárním přiblížení, 243
lineární nezávislost, 87
list, 725
logaritmický řád velikosti, 513
logaritmická věrohodnostní funkce, 576
lokálně konečné pokrytí, 484
lokální parametrizace variety, 480
Lucasův test, 631
Ludolfovo číslo, 286

Möbiova funkce, 601
Möbiova inverzní formule, 601
měřítko, 38
marginální rozložení, 550
Markovův řetězec, 144
Markovův proces, 144
matematická indukce, 13
matice, 30
  algebraicky adjungovaná, 85
  antisymetrická, 80
  invertibilní, 72

inverzní, 72
jednotková, 70
kladná, 141
nulová , 69
opačná, 69
přechodu, 96
primitivní, 141
regulární čtvercová, 72
schodovitý tvar, 73
symetrická, 80
zobrazení, 95
matice kódu, 700
matice kontroly parity, 702
matice sousednosti, 714
matice transponovaná, 80
maximum funkce, 451
medián, 527, 556
meet, 686
Mersenneho prvočíslo, 596
metoda
hlavních komponent, 532
Lagrangeových multiplikátorů, 466
nejmenších čtverců, 582
Monte Carlo, 27
metrický prostor, 410
metrika, 410
metrika na grafu, 720
mezní sklon ke spotřebě, 132
minimální kostra, 735
minimální vyloučená hodnota, 745
minimum funkce, 451
minor, 83
doplňkový minor, 83
vedoucí hlavní, 83
množina řešení kongruence, 610
množina
řídká, 415
hustá, 415
kompaktní, 252, 420
neohraničená, 252, 420
neomezená, 420
ohraničená, 420
omezená, 418, 420
otevřená, 252, 411
uzavřená, 251, 411
možné výsledky, 533
mocninná řada, 283
mocninná řada se středem v $x_0$, 288
mocninný zbytek, 616
mocninný průměr stupně $r$, 275
modul nad okruhem, 68
modus, 528
$k$-tý moment, 561
momentová vytvořující funkce, 562
monoid, 642
monomiální uspořádání, 675
monom, 659
morfismus, 710
most, 710
multiindex, 659
multiplikativní funkce, 602
měřítko, 525
intervalové, 526
nominální, 525
ordinální, 526
poměrové, 526

náhodné jevy, 534
náhodný vektor, 540
náhodný výběr, 572
následník, 726
násobek, 589
nadrovina, 198
náhodná veličina, 540
nastoupení alespoň jednoho z jevů, 534
nehomogenní lineární diferenční rovnice, 136
nejmenší prvek, 692
nejmenší společný násobek, 590
největší prvek, 692
největší společný dělitel, 590, 664
nekomutativní okruh, 656
nekonečná řada čísel, 279
nekonečné body, 221
nekonečně rozměrný prostor, 89
nemožný jev, 534
nenasycená hrana, 739
neorientovaný graf, 708
nerovnost
Bernoulliova, 276
Besselova, 149, 402
Cauchyova, 149
Gronwallova, 501
Hölderova pro integrály, 414
Hölderova, 412
Minkowského, 413
Parsevalova, 402
trojúhelníková, 149
nerozložitelný prvek, 661
neslučitelné jevy, 534
nesoudělnost, 593
nestranné hry, 744
nestranný odhad, 575
neurčitý integrál, 344
neutrální prvek, 8
nevlastní body, 221
nevlastní hromadné body, 255

nevlastní integrál 1. druhu, 356
nevlastní integrál 2. druhu, 356
Newtonův integrál, 345
Neymanovo–Pearsonovo lemma, 580
nilpotentní, 157
Nim, 742
normální disjunktivní tvar, 695
normální matice, 156
normální podgrupa, 653
normální zobrazení, 155
normálový prostor, 465
normálový vektor, 463
norma, 141, 149, 410
norma dělení, 350
normovaný, 98
normovaný vektor, 146
normovaný vektorový prostor, 410
normovaná veličina, 557
nulová hypotéza, 579
nulová křivost, 337
nulová míra, 372

obecná Fourierova řada, 408
obor hodnot funkce, 10
obor hodnot relace, 40
obor integrity, 8, 656
obor integrity s jednoznačným rozkladem, 661
obraz, 93
obsah, 37
odchylka vektorů, 205
odchylka podprostorů, 205
ohodnoceny graf, 720
ohraničená množina, 252
ohraničený problém, 129
$\delta$-okolí, 252
okolí bodu, 252
okruh hlavních ideálů, 672
omezený prostor, 420
opačný jev k jevu, 534
orbita akce, 655
orientace, 38, 208
orientace variety, 483
orientovaná varieta s hranicí, 487
Orientovaný (bodový) euklidovský prostor, 208
orientovaný grafem, 708
orientovaný vektorový prostor, 208
orientovaná varieta, 483
ortogonálně diagonalizovatelná, 155
ortogonální, 98, 146
ortogonální báze, 98
ortogonální doplněk, 99, 147
ortogonální grupa, 151
ortogonální matice, 108, 151
ortogonální systém funkcí, 401
ortogonální zobrazení, 107
ortonormální báze, 98, 147, 400
ortonormálním systému funkcí, 401
osa kolineace, 225
oskulační kružnice, 338
ostrý extrém, 451
otec, 726
otevřené $\varepsilon$–okolí, 411
otevřené pokrytí, 253, 419
otevřený interval, 252

párový t-test, 585
pěstěný strom, 727
předchůdce, 726
přirozený logaritmus, 264
přímý předchůdce, 726
přímka, 29
parametrický popis, 196
parciální derivace funkce, 442
parita, 645
parita permutace, 79
partikulární řešení, 126
Pascalův trojúhelník, 13
percentil, 528, 556
permutace, 11
  lichá, 79
  sudá, 79
  s opakováním, 14
permutace množiny $X$, 78
Perronova-Frobeniova teorie, 141
Petersenův graf, 710
Petrohradský paradox, 554
Picardova aproximace, 496
po dvou nesoudělná, 593
počáteční hodnoty, 490
počáteční vrchol hrany, 708
počátek afinní souřadné soustavy, 195
počátek souřadnic, 28
počet řešení kongruence, 610
Pocklington-Lehmerův test, 631
podgraf, 711
podgrupa, 642
podgrupa generovaná množinou, 642
podmodel, 583
podmíněná pravděpodobnost, 536
podprostor generovaný, 88
podílové těleso, 665
polární báze, 217
pole, 8, 657
polocesta, 739
pologrupa, 642
poloměr konvergence, 283

poloosa kuželosečky, 215
polopřímky, 199
poloprostory, 199
polynomiální řád velikosti, 513
popisná statistika, 523
populace, 572
poset, 690
posunutí, 28, 194
povrch, objem rotačního tělesa, 361
pozitivně definitní, 156
pozitivně semidefinitní, 156
průměr, 527
průměr množiny, 252, 418
průměrná odchylka, 529
průnik, 686
přímý následník, 726
pravděpodobnost, 534
  klasická, 21
  podmíněná , 25
pravděpodobnostní funkce, 542
pravděpodobnostní prostor, 20, 534
pravidlo
  lichoběžníkové, 370
  Simpsonovo, 370
pravá inverze, 642
pravá jednotka, 642
příčka, 200
primitivní funkce, 344
primitivní kořen, 606
primitivní matice, 141
primitivní polynom, 699
přímý součet, 89
princip duality, 687
princip inkluze a exkluze, 21, 23
přípustný vektor $x$, 129
přirozený splajn, 245
problém lineárního programování, 127
prohledávání do šířky, 717
prohledávání do hloubky, 717
projekce, 99
projektivizace vektorového prostoru, 221
projektivní kvadrika, 226
projektivní rovina $\mathcal{P}_2$, 220
projektivní transformace, 222
projektivní zobrazení, 222
prvky řádu $k$, 644
první kvartil, 556
prvočíslo, 593
pseudoinverzní matice, 169
pseudoprvočíslo, 627

Rabinův kryptosystém, 634
racionální parametrická reprezentace, 670
řád čísla modulo $m$, 605
řád prvku, 650
řád velikosti, 513
řada
  alternující, 283
  diverguje, 280
  Fourierova, 403
  funkcí, 283
  geometrická, 284
  konverguje absolutně, 280
  Laurentova se středem v $x_0$, 368
  mocninná, 283
  osciluje, 280
řádky matice, 69
reálná složka, 8
reálné funkce reálné proměnné, 237
reciproká rovnici, 135
redukovaná soustava zbytků, 604
regresní přímka, 585
regulární kolineace, 222
rekurence
  homogenní lineární, 131
relace
  antisymetrická, 41
  ekvivalence, 41
  inverzní , 41
  reflexivní, 41
  symetrická, 41
  tranzitivní, 41
  uspořádání, 41
reprezentant
  třídy ekvivalence, 42
řešení diferenciální rovnice, 490
řešitelný problém, 129
řetězec, 693
řez v síti, 738
rezerva kapacity, 739
reziduální rozptyl, 582
reziduální součet čtverců, 582
Riemannův integrál, 350
Riemannův součet, 350
Riemannův–Stieltjesův integrální součet, 371
riemannovská míra, 358
riemannovsky měřitelná množina, 358, 469, 472
rotace vektorového pole, 489
rovinný graf, 729
rovnoběžnostěn, 200
rovnomocně spojitá množina funkcí, 421
rovnost
  Bezoutova, 664
  Parsevalova, 149
rozdělení (pravděpodobnosti) náhodného vektoru, 540
rozdělení pravděpodobnosti náhodné veličiny, 540

rozdělení
  $\chi^2$ s $n$ stupni volnosti, 568
  $\chi^2$ s jedním stupněm volnosti, 567
  alternativní, 544
  Beta, 581
  binomické, 544
  degenerované, 543
  exponenciální, 548
  F-rozdělení, 569
  Fisherovo-Snedecorovo s $k$ a $m$ stupni volnosti, 569
  gama, 548
  geometrické, 544
  mnohoměrné normální, 569
  normální, 549
  Poissonovo, 545
  rovnoměrné, 547
  Studentovo t-rozdělení s $n$ stupni volnosti, 569
rozklad
  $LU$–rozklad, 165
  QR rozklad, 168
rozklad jednotky podřízený lokálně konečnému pokrytí, 485
rozklad na parciální zlomky, 348
rozklad na třídy, 42
rozpětí výběru, 528
rozptyl, 528
rozsah souboru, 526
rozvoj determinantu, 83
RSA, 633
RSS, 582
ryzí okolí, 255

samoadjungovaná matice, 153
samodružný bod, 225
samodružná nadrovina kolineace, 225
Sarrusovo pravidlo, 79
schodovitý tvar matice, 73
sdružená hustotou, 550
sdružená pravděpodobnostní funkce, 550
$\sigma$–algebře Borelovsky měřitelných množin na $\mathbb{R}^k$, 540
signatura kvadratické formy, 218
simplex, 198, 199
singulární bod, 676
singulární hodnoty matice, 167
sinusintegrál, 357
sjednocení, 686
skóre grafu, 712
skalární součin, 69, 98, 146
skaláry, 9
skládání relací, 40
slabě souvislý graf, 724
slabá souvislosti, 718
sled, 711
sled délky $n$, 711
složené číslo, 593
složení, 40
sloupce matice, 69
směrodatná odchylka, 528
směrodatná odchylka náhodné veličiny, 557
směrová derivace, 442
smyčka, 708
současné nastoupení jevů, 534
součet nestranných her, 744
součet podprostorů, 89
součin grup, 650
souřadnice vektoru, 92
soubor hodnot, 525, 526
soukromý klíč, 634, 636
sousední hrany grafu, 708
sousední hrany orientovaného grafu, 708
souvislé komponenty grafu, 718
souvislý graf, 718
spektrální poloměr, 110
spektrální poloměr matice, 141
spektrum lineárního zobrazení, 110, 157
spojitá náhodná veličina, 543
spojitá zobrazení, 412
spojitost, 694
společné nastoupení jevů, 534
společný dělitel, 590
Sprague–Grundyova funkce, 745
srovnatelné prvky, 42
stěna simplexu, 198
stěny rovinného grafu, 730
střed kolineace, 225
střed kuželosečky, 215
střední hodnota, 359
Střední hodnota náhodného vektoru, 553
střední hodnota veličiny, 553
střední kvadratická odchylka, 528
stažení formy , 480
stacionární bod, 466
stacionární bod funkce, 451
stacionární body, 329
standardizovaná veličina, 557
standardní afinní prostor, 193
standardní maximalizační problém, 127
standardní minimalizační problém, 127
standardní unitární prostor, 147
statistické
  jednotky, 525
  soubory, 525
  znaky, 525
statistika, 524
stejnoměrná spojitost, 353
stejnoměrně Cauchyovská, 365

stejnoměrná konvergence, 364
štěpení posloupnosti, 654
stochastická matice, 145
stochasticky nezávislé, 550, 535
stok, 738
stok sítě, 737
stopa matice, 104
stopa zobrazení, 104
strategie hráče, 742
strom, 725
strom hry, 742
stupeň polynomu, 658, 674
stupeň vrcholu, 712
stupeň nilpotentnosti, 157
stupeň polynomu, 238
subdeterminant, 83
submatice, 83
  doplňková, 83
  hlavní, 83
  vedoucí hlavní, 83
supremum, 247, 686
supremum množiny, 691
svědek prvočíselnosti, 631
svaz, 692
symetrická zobrazení, 153
symetrické matice, 153
symetrizace, 708
syn, 726
syndrom, 702
systém diferenciálních rovnic
  autonomní, 502

těleso, 657
těleso racionálních funkcí, 665
třetí kvartil, 556
třídní četnosti, 526
třídy ekvivalence, 42
tah, 711
Taylorův polynom $k$–tého stupně, 330
Taylorův rozvoj se zbytkem, 329
tečná nadrovina, 446
tečná rovina, 446
tečný prostor, 465, 479
tečný vektor, 441, 478
tečna, 243
tečna ke křivce $c$, 442
test, 579
test dobré shody, 585
tok, 738
tok vektorového pole, 505
topologie, 252, 412
  komplexní roviny, 252
  metrických prostorů, 412
  reálné přímky, 252
torze křivky, 341
totálně omezený prostor, 420
transformace, 454
transpozice, 78, 644
tranzitivní akce, 655
trojúhelník, 198, 709
trs nadrovin procházejí bodem, 225
typy měřítek, 525

účelová funkce, 127
úhly, 199
unitární grupa, 151
unitární isomorfismus, 147
unitární matice, 151
unitární prostor, 146
unitární zobrazení, 147
univerzální formule, 750
úplná soustava rovnic, 505
úplné metrické prostory, 411
úplný graf, 709
úplný ortogonální systém, 403
úplném svazu, 692
úplná soustava zbytků, 604
úplné uspořádání, 690
úplný splajn, 245
určitý integrál, 345
úrovňová množina, 463
úsečka, 198, 709
uspořádání, 41, 690
uspořádaná množina, 690
uspořádané pole, 246
uspořádaný soubor hodnot, 526
uzávěr, 251
uzavřený interval, 251

výběrový kvantil, 528
výběrový rozptyl, 528
výběrový soubor, 572
výběrová statistika, 575
výběrový rozptyl, 572
výrok, 688
výstřednost stromu, 728
výstupní stupeň , 712
věrohodnostní funkce, 576
Vandermondův determinant, 240
variační koeficient, 529
variace, 12, 372
  s opakováním, 14
varianční matice, 561
vcházející hrany, 708
veřejný klíč, 634, 636
vedoucí člen, 674

vedoucí koeficient, 674
vedoucí monom, 674
vektor chyb, 699
vektor omezení, 127
vektorová funkce jedné reálné proměnné, 339
vektorové pole, 478, 505
vektorové pole podél křivky, 478
vektorový podprostor, 88
vektorový prostor, 86
vektorový součin, 210
vektory, 27, 67
  nulové, 27
  lineárně závislé, 76
velikost multiindexu, 659
velikost toku, 738
velikost vektoru, 146
veličiny
  stochasticky nezávislé, 24
vlastní čísla matice, 104
vlastní čísla zobrazení, 103
vlastní vektory zobrazení, 103
vnější diferenciál, 486
vnější diferenciální $k$–forma, 480
vnější součin vektorů, 210
vnitřek množiny, 411
vnitřním bod, 419
vnitřním bodem množiny, 253
vrchol grafu, 708
vrcholově $k$–souvislý graf, 718
vstupní stupeň , 712
vycházející hrany, 708
vychýlení odhadu $T$, 575
vytvořující funkce, 747
vyvážený vrchol, 712
vyvážený binární strom, 726
vzájemně kolmé, 154
vzdálenost, 420
vzdálenost bodu od množiny, 251
vzdálenost bodů, 203
vzdálenost vrcholů, 720
vzor množiny v zobrazení, 40
vzorkovací interval, 432
vícerozměrný interval, 468
věta
  Abelova, 368
  Arzelova-Ascoliho, 420
  Bernoulliova, 558
  Bezoutova, 591
  Cauchyova, 82
  Cauchyova o střední hodnotě, 273
  Frobeniova, 126
  Gaussova–Ostrogradského, 489
  Greenova, 488
  Jacobiho, 219
  Jordanova, 730
  klasická Stokesova, 489
  Kleeneho, 694
  kosinová, 205
  Kuratowského, 730
  Lagrangeova, 652
  Lagrangeova o střední hodnotě, 272
  malá Fermatova, 652
  Mengerova, 718
  o setrvačnosti, 217
  Rolleova, 272
  Spragueova–Grundyova, 745
  Steinitzova, 732
  Steinitzova o výměně, 91
  Stoneova o reprezentaci, 697
  Tarského o pevném bodě, 694
  základní věta algebry, 328
  základní věta aritmetiky, 594
  zobecněná binomická věta, 749

wavelety, 409

základní prostor, 19, 533
zákon kvadratické reciprocity, 619
zúplnění metrického prostoru, 415
zaměření, 194
zdroj, 738
zdroj sítě, 737
zobecněná exponenciální mocninná řada, 754
zobrazení
  identické , 41
  injektivní, 40
  surjektivní , 40
  z množiny $A$ do množiny $B$, 40
zobrazení
  diferencovatelné, 454
  do, 40
  na, 40
  třídy $C^k$ , 454
zrcadlení vzhledem k přímce, 35

**Matematika drsně a svižně**
**Jan Slovák, Martin Panák, Michal Bulant**
**a kolektiv**

Vydala Masarykova univerzita v roce 2013
1. vydání, 2013
Náklad 500 výtisků
Sazba nejen systémem LaTeX Tomáš Janoušek
Tisk: Tiskárna Knopp, Černčice 24, 549 01 Nové Město nad Metují

ISBN 978-80-210-6307-5
ISBN 978-80-210-6308-2 (online : pdf)
DOI: 10.5817/CZ.MUNI.O210-6308-2013