Drsná matematika

Martin Panák, Jan Slovák

Pokus o učební text pro začínající studenty informatiky přibližující podstatnou část matematiky v rozsahu čtyř semestrálních přednášek. Prozatím jsou zaznamenány první tři semestry přibližně v odpředneseném rozsahu. Poslední semestr je zapisován průběžně.

Obsah

Předmluva

Tento učební text vzniká průběžně při přípravě přednášek pro předměty Matematika I–IV na Fakultě informatiky MU. Text se snaží prezentovat standardní výklad matematiky s akcentem na smysl a obsah prezentovaných matematických metod. Řešené úlohy pak procvičují základní pojmy, ale zároveň se snažíme dávat co nejlepší příklady užití matematických modelů. Studenti navíc mají řešit a odevzdávat každý týden zadávané příklady. Seminární skupiny pak obdobně standardním „cvičením“ vytváří podporu pro řešení domácích úloh. V tomto textu podáváme formální výklad proložený řešenými příklady.

Ne vše se daří průběžně naplňovat tak, jak bychom si představovali. Samotný teoretický text by měl být podrobnější a lépe formulovaný, řešených příkladů bychom chtěli mít podstatně více a měly by pokrývat celou škálu složitosti, od banálních až po perličky ke skutečnému přemýšlení.

Posluchače bychom rádi naučili:

- přesně formulovat definice základních pojmů a dokazovat jednoduchá matematická tvrzení,
- vnímat obsah i přibližně formulovaných závislostí, vlastností a výhledů použití,
- 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 nechutě). 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 tento postup se 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 „víme“, nechce se nám přemýšlet, pokud „nevíme“, je to ještě horší. Jediný spolehlivý postup pro orientaci v matematice je hledat porozumnění v mnoha pokusech a hledat je při četbě v různých zdrojích. Určitě nepovažujeme tento text za dostatečný jediný zdroj pro každého.

Pro ulehčení vícekolového přístupu ke čtení je text strukturován také pomocí barev, resp. sazby, takto

- normální text je sázen černě
- řešené příklady jsou sázeny barvou
- složitější text, který by měl být čten pozorněji, ale určitě ne přeskakován, je sázen barvou
- náročné pasáže, které mohou (nebo by raději měly být) být při studiu přinejmenším napoprvé přeskakovány jsou sázeny v barvě .

První tři semestry výuky už jednou proběhly a výsledných 9 kapitol máte v rukou. Popišme tedy nyní stručně obsah a také výhled na semestr následující.

1. semestr: Úvodní motivační kapitola se snaží v rozsahu přibližně 4–5 týdnů přednášek ilustrovat několik přístupů k matematickému popisu problémů. Začínáme nejjednoduššími funkcemi (základní *kombinatorické formule*), 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, uspořádní, ekvivalence*). Nenechte se zde uvrhnout do chaotického zmatku příliš 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.

Dalších přibližně 5 týdnů přednášek je věnováno 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. Jednoduché postupy pro práci s *vektory a maticemi* jsou obsahem kapitoly druhé, další kapitola je pak věnována aplikacím maticového počtu v různých lineárních modelech (*systémy lineárních rovnic, lineární procesy, lineární diferenční rovnice, Markovovy procesy, lineární regrese*).

Poslední 2–3 přednášky prvního semestru jsou věnovány použitím maticového počtu v geometrických úlohách a lze se z nich dozvědět něco málo o *afinní, euklidovské a projektivní geometrii.*

2. semestr: Další semestr je věnován tzv. spojitým modelům. Chceme co nejnázorněji ukázat, že základní ideje, jak s funkcemi pracovat, bývají jednoduché. Stručně řečeno, hledáme cesty, jak složitější věci nelineární povahy řešit pomocí jednoduchých lineárních triků a postupů lineární algebry. Složitosti se pojí skoro výhradně se zvládnutím rozumně velké třídy funkcí, pro které mají naše postupy být použitelné.

Prvně proto přišla na řadu kapitola pátá, kde diskutujeme jaké funkce potřebujeme pro nelineární modely. Začínáme s *polynomy a spliny*, pak postupně diskutujeme pojmy *spojitosti*, *limity posloupností a funkcí* a *derivace funkcí* a seznámíme se se všemi základními *elementárními funkcemi* a s *mocninnými řadami.*

Tím je připravena půda pro klasický diferenciální a integrální počet. Ten prezentujeme v kaptole šesté s důrazem na co nejjednodušší pochopení *aproximací*, *integračních procesů* a *limitních procesů.*

Poslední sedmá kapitola se věnuje náznakům aplikací a snaží se co nejvíce připomínat analogie k postupům jednoduché lineární algebry z minulého semestru. Místo lineárních zobrazení mezi konečně rozměrnými vektorovými prostory tak pracujeme s lineárními operacemi mezi nekonečně rozměrnými vektorovými prostory funkcí, definovaných buď integrálními nebo diferenciálními operátory. Zatímco studium diferenciální rovnic ponecháváme do semestru dalšího, zde studujeme nejprve aproximace funkcí s pomocí vzdálenosti definované integrálem (tzv. *Fourierovy řady*) abychom vzápětí mohli ukázat souvislost s některými integrálními transformacemi (*Fourirerova transformace*).

3. semestr: Zde nejprve pokračujeme v našem stručném nastínění analytických metod pro modely s mnoha proměnnými. Nejprve v osmé kapitole rozšíme základní postupy a výsledky týkající se derivací na *funkce více proměnných*, včetně *funkcí*

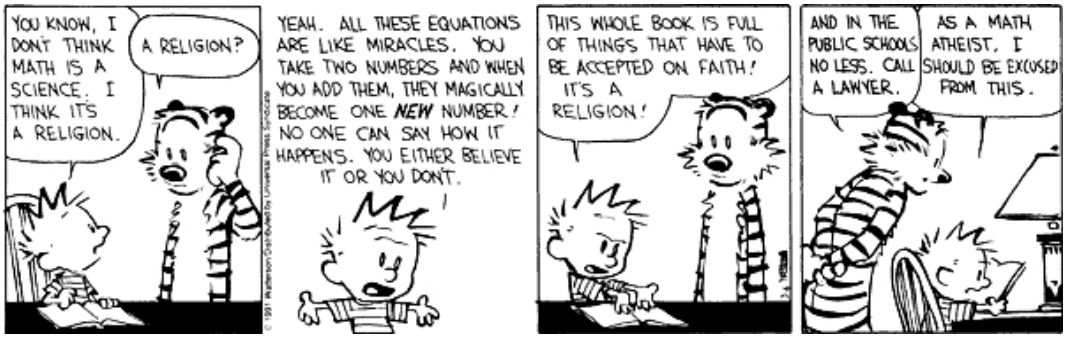
zadaných implicitně a tzv. *vázaných extrémů*. Hned poté rozšíříme teorii integrování o tzv. násobné integrály. Poté se věnujeme stručně modelům zachycujím známou zněnu našich obejktů, tj. *diferenciálním rovnicím*. Závěrem této kapitoly pak uvádíme několik poznámek o odhadech a numerických příbliženích.

Devátá kapitola směřuje zpět do světa diskrétních metod. Zabýváme se v ní základními pojmy poznatky teorie grafů a jejich využitím v praktických problémech (např. prohledávání do šířky a hloubky, *minimální pokrývající kostry*, *toky v sítích*, *hry popisované stromy*). Závěrem uvádíme pár poznámek o vytvořujících funkcích.

4. semestr: V posledním semestru celého cyklu přednášek se hodláme zabývat nejprve obecné algebraickými strukturami s důrazem na teorii grup a náznaky jejích aplikací. Tomuto tématu budeme věnovat 5–6 přednášek.

Konečně, závěrečná jedenáctá kapitola je věnována matematické pravděpodobnosti a statistice v rozsahu 6-7 přednášek. Seznámíme se s pojmy *pravděpodobnostní prostor, hustota pravděpodobnosti, normální rozdělení, střední hodnota, medián, kvantil, rozptyl, příklady diskrétních a spojitých rozdělení* a budeme se náznakem věnovat *statistickému zpracování dat*.

Únor 2007, Martin Panák, Jan Slovák



KAPITOLA 1

Úvod a motivace

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

1. Čísla a funkce

Lidé trpí chorobnou snahou mít jasno „kolik něco je“, případně „za kolik“, „jak dlouho“ apod. Výsledkem takových úvah je většinou nějaké „číslo“, říkejme učeněji „hodnota“. Za číslo se přitom považuje něco, co umíme sčítat a násobit a splňuje to obvyklé zákonitosti, ať už všechny nebo jen některé. Nejjednodušším příkladem jsou tzv. čísla přirozená, budeme je značit $\mathbb{N} = \{1, 2, 3, \dots\}$, často zvláště v informatice brána včetně nuly, a čísla celá $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Kdo si libuje ve formálním přístupu v rámci některé z korektních teorií množin a ví, co to je prázdná množina $\emptyset$, může definovat

e1.1 (1.1) $$0 := \emptyset,\ 1 := \{\emptyset\},\ 2 := \{\emptyset, 1\}, \dots, n+1 := \{0, 1, \dots, n\}.$$

Pak lze snadno formálně definovat sčítání a násobení celých čísel, uspořádání, 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. Např. o číslu a řekneme, že je menší než b tehdy a jen tehdy, když $a \neq b$ a $a \in b$. Nebudeme se tu tím podrobně zabývat a předpokládáme, že čtenář i čísla racionální ($\mathbb{Q}$), reálná ($\mathbb{R}$) a komplexní ($\mathbb{C}$) důvěrně zná.[1] Prakticky budeme připomínat teoretické i praktické souvislosti při dalším výkladu, viz příklad 1.4(1). Podobně bude konstrukce racionálních čísel z přirozených diskutována v 1.47, konstrukci reálných čísel bude vhodné zmínit při studiu limitních procesů později a již dříve budeme z různých algebraických pohledů zkoumat čísla komplexní.

Pro náš další rozlet ale bude teď užitečné vyjmenovat obvyklé vlastnosti, které sčítání a násobení čísel má. 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.

1.1

1.1. Vlastnosti sčítání.

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

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

(KG3) existuje prvek 0 takový, že pro všechny a platí $a + 0 = a$

(KG4) pro všechny a existuje prvek $(-a)$ takový, že platí $a + (-a) = 0$.

[1] Podrobně lze formální základy matematiky nalézt např. ve skriptech Pavla Horáka [**10**].

Vlastnostem (KG1) – (KG4) říkáme vlastnosti *komutativní grupy*. Celá čísla $\mathbb{Z}$ jsou dobrým příkladem komutativní grupy, přirozená čísla nikoliv, protože nesplňují KG4 (a případně neobsahují nulu pokud ji do $\mathbb{N}$ nezahrnujeme).

1.2

1.2. Vlastnosti násobení.

(O1) $$(a \cdot b) \cdot c = a \cdot (b \cdot c), \text{ pro všechny } a, b, c$$

(O2) $$a \cdot b = b \cdot a, \text{ pro všechny } a, b$$

(O3) existuje prvek 1 takový, že pro všechny a platí $1 \cdot a = a$

(O4) $$a \cdot (b + c) = a \cdot b + a \cdot c, \text{ pro všechny } a, b, c.$$

Poslední vlastnosti O4 se říká *distributivita*.

Množiny s operacemi $+$, $\cdot$ a vlastnostmi (KG1)–(KG4), (O1)–(O4) se nazývají *komutativní okruhy*. Potřebujeme však zpravidla ještě další běžnou vlastnost čísel:

(P) pro každý $a \neq 0$ existuje prvek a^{-1} takový, že platí, $a \cdot a^{-1} = 1$.

Když naše objekty splňují navíc i (P), hovoříme o *poli* (často také o *komutativním tělese*). Někdy se ale setkáme se slabší dodatečnou vlastností. Např. okruh celých čísel $\mathbb{Z}$ nesplňuje (P), ale splňuje

(OI) $$a \cdot b = 0 \quad \Rightarrow \quad \text{buď } a = 0 \text{ nebo } b = 0.$$

Hovoříme o *oboru integrity*.

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 latinská písmena ze začátku abecedy.

Kdo chce postupovat co nejpřesněji a formálně, měl by předchozí vlastnosti 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 tady i naše výsledky 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 vždy zdůrazňovat, přestože naše ambice mohou být v rámci daného časového prostoru pro přednášky jen velice skromné.

1.3

1.3. Skalární funkce. Často pracujeme s 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 formulí poskládanou z (prozatím si představme konečně mnoha) známých operací. Pokud je hodnotou skalár, hovoříme o *skalární funkci*. Také může být ale hodnota dána pouze přibližně nebo s jistou pravděpodobností.

Smyslem matematických úvah pak bývá z neformálního popisu závislostí najít explicitní formule pro funkce, které je popisují. Podle typu úlohy a cíle se pak pracuje:

- 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 (hodnoty nezávislé veličiny jsou jednotliví pracovníci x z nějaké množiny, $f(x)$ je jejich roční mzda za dané období), nebo měsíční mzda konkrétního pracovníka v čase (nezávislou hodnotou je čas v měsících, závislou příjem). 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 **1.4. Příklady.** (1) Podívejme se na obyčejné sčítání přirozených čísel jako na operačně definovanou skalární funkci. Definujeme $a + b$ jako výsledek procedury, ve které k a přičítáme 1. Tak jsme vlastně obecně $a + 1$ definovali v rovnicích (1.1). Zároveň odebereme z b nejmenší prvek, dokud není b prázdná. Je evidentní, že takto definované sčítání sice je dáno formulí, tato ale není vhodná pro praktické počítání. Tak tomu bude v našem výkladu často – teoreticky korektní definice pojmu neznamená, že úkony s ním 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) a s většími si poradí počítače (pokud nejsou příliš velká).

(2) Důležitou operačně definovou skalární funkcí na přirozených číslech je *faktoriál*, který definujeme vztahy

$$f(0) = 1,\ f(n+1) = (n+1) \cdot f(n).$$

Píšeme $f(n) = n!$ a definice zjevně znamená $n! = n \cdot (n-1) \cdots 1$. To také není příliš efektivní formule pro velká n, lepší ale těžko hledat.

2. Kombinatorické formule

1.5 **1.5. Permutace, kombinace a variace.** 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. Hovoříme o *permutacích* prvků množiny S. Jestliže si předem prvky v S očíslujeme, tj. ztotožníme si S s množinou $S = \{1, \dots, n\}$ 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:

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

e1.1a (1.2) $$f(n) = n!$$

Dalším jednoduchým příkladem hodnoty určené formulí jsou tzv. *binomická 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. Proto pro počet *kombinací k-tého stupně* z n prvků platí (samozřejmě je $k \leq n$)

e1.2 (1.3) $$c(n,k) = \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1} = \frac{n!}{(n-k)!k!}.$$

Ani toto není pro výpočet moc uspokojivá formule při velikých k i n, protože obsahuje výrazy pro faktoriály.

Pokud nám ale záleží i na pořadí vybrané k-tice prvků, hovoříme o *variaci k-tého stupně*. Jak jsme si již ověřili, pro počet variací platí

$$v(n,k) = n(n-1)\cdots(n-k+1)$$

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

Binomická čísla dostala svůj název 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

e1.3 (1.4)
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

a všimněme si, že pro odvození jsme potřebovali pouze distributivitu, komutativnost a asociativitu násobení a sčítání. Formule (1.4) 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 $k > n$.

1.6 **1.6. 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

$$\begin{aligned}\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} \\ &= \frac{(k+1)n! + (n-k)n!}{(k+1)!(n-k)!} \\ &= \frac{(n+1)!}{(k+1)!(n-k)!}\end{aligned}$$

což je ale levá strana tohoto tvrzení.

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

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

Prakticky stejně dokážeme i (4). Zjevně platí pro $n = 0$, předpokládejme, že platí pro nějaké n, a spočtěme příslušnou sumu pro $n+1$ s využitím tvrzení (2).

Dostaneme

$$\begin{aligned}\sum_{k=0}^{n+1} k\binom{n+1}{k} &= \sum_{k=-1}^{n}(k+1)\binom{n}{k} + \sum_{k=0}^{n+1} k\binom{n}{k}\\ &= \sum_{k=0}^{n}\binom{n}{k} + \sum_{k=0}^{n} k\binom{n}{k} + \sum_{k=0}^{n} k\binom{n}{k}\\ &= 2^n + n2^{n-1} + n2^{n-1} = (n+1)2^n.\end{aligned}$$

□

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:

$n=0:$				0		1		0		
$n=1:$			0		1		1		0	
$n=2:$		0		1		2		1		0
$n=3:$	0		1		3		3		1		0
$n=4:$	0		1		4		6		4		1		0
$n=5:$		1		5		10		10		5		1	

Všimněme si, že v jednotlivých řádcích máme právě koeficienty u jednotlivých mocnin z výrazu (1.4), např. poslední uvedený řádek říká

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

Uveďme si příklad demonstrující kombinatorické úvahy (berte to jako zahřívací rozcvičku!):

1.7. Příklady.

1.7.1. *Maminka chce Jeníkovy a Mařence rozdělit pět hrušek a šest jablek. Kolika způsoby to může udělat? (hrušky mezi sebou považujeme za nerozlišitelné, stejně tak jablka)*

Řešení. Pět hrušek samostatně může maminka rozdělit šesti způsoby, šest jablek pak samostatně sedmi způsoby. Podle pravidla součinu pak obě ovoce současně může rozdělit 42 způsoby. □

1.7.2. *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 dvojciferných 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. □

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

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

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

□

1.7.4. *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

$$\binom{16}{3}\cdot 4\cdot 13!$$

□

1.7.5. *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 dvě sta možných, na kterých budou např. líce). Celkem je hledaná pravděpodobnost

$$\frac{\binom{200}{100}}{2^{200}}=\frac{\frac{200!}{100!\cdot 100!}}{2^{200}}$$

□

1.8. Poznámka. Všimněme si, že v předchozím příkladu jsme mimochodem kombinatoricky dokázali nerovnost

$$\binom{200}{100}<2^{200},$$

resp. malým zobecněním dokonce pro libovolná $k,n\in\mathbb{N}$, $k\leq n$

$$\binom{n}{k}<2^n.$$

1.8a

1.9. Permutace, kombinace a variace s opakováním. Pořadí n prvků, z nichž mezi některými nerozlišujeme, nazýváme *permutace s opakovaním*. Nechť je mezi n danými prvky p_1 prvků prvního druhu, p_2 prvků druhého druhu, ..., p_k prvků k-tého druhu, $p_1+p_2+\cdots+p_k = n$, potom počet pořadí těchto prvků s opakováním budeme značit $P(p_1,\ldots,p_k)$. Zřejmě platí

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

Volný výběr prvků z n možností, včetně pořadí, nazýváme *variace k-tého stupně s opakováním*, jejich počet budeme značit $V(n,k)$. 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

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

Pokud nás výběr zajímá bez zohlednění pořadí, hovoříme o *kombinacích s opakováním* a pro jejich počet píšeme $C(n,k)$.

Věta. *Počet kombinací s opakováním k-té třídy z n prvků je pro všechny $0 \le k$ a $0 < n$*

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

Důkaz. Důkaz je opřen o trik (jednoduchý, když ho někdo už zná). Nechť $x_1,\ldots,x_k$ je kombinace libovolných prvků z dané množiny

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

na které si zafixujeme uvedené pořadí prvků. Jednotlivé volby x_i přidáme do pořadí $a_1,\ldots$ tam, kde je shodný prvek. Např. pro $S = \{a,b,c,d\}$ a volbu $x_1 = b$, $x_2 = c$, $x_3 = b$ dostaneme $S' = [a,b,b,b,c,c,d]$. Nyní si uvědomme, že pro rozpoznání původní kombinace nám stačí vědět, kolik je prvků v jednotlivých skupinách (je tam vždy právě o jeden prvek více než kolik patří do kombinace). Můžeme si to znázornit

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

protože příslušnost jednotlivých přihrádek k prvkům S je námi pevně zvolena.

Počet $C(n,k)$ je proto roven počtu možných umístění přihrádek $|$, tj. výběr $n-1$ pozic z $n+k-1$ možných. □

Příklady na procvičení:

4.

1.10. Příklady.

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

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

v množině přirozených čísel.

Řešení. Řešení je samozřejmě velice silně závislé na tom, jestli považujeme nulu za přirozené číslo. Rozhodněme se, že ne, ale určeme nejprve počet řešení rovnice v množině celých nezáporných čísel. 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 $\binom{n+k-1}{n}$.

Hledáme-li řešení v oboru přirozených čísel, tak si všimněme, že přirozená čísla $x_1, \dots x_k$ jsou řešením dané rovnice, právě když jsou celá nezáporná čísla $y_i = x_i - 1$, $i = 1, \dots, k$, řešením rovnice

$$y_1 + y_2 + \cdots + y_k = n - k.$$

Těch je podle první části řešení $\binom{n-1}{k-1}$. □

1.10.2. *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 $C(3,5)^2 - 3(C(2,5)^2 - 2) - 3 = \binom{7}{2}^2 - 3(6^2 - 2) - 3 = 336$. □

1.10.3. *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 $6!4!/2$. □

1.10.4. *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

$$6 \cdot P(1,1,2,2) = \frac{6 \cdot 6!}{2 \cdot 2}.$$

□

1.10.5. *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 třetí třídy z pěti prvků (viz odstavec 2.4. učebních textů). 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 $10 = 2 \cdot 5$; 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. □

3. Diferenční rovnice

V předchozích odstavcích jsme viděli formule, které zadávaly hodnotu skalární funkce definované na přirozených číslech (faktoriál) nebo dvojicích čísel (binomická čísla) pomocí předcházejících hodnot. Tomu lze rozumět také tak, že místo hodnoty naší funkce zadáváme její změnu při odpovídající změně nezávislé proměnné. Porovnejte si formule v 1.4 a v 1.6. 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.

1.8

1.11. Lineární 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 dvojicích přirozených čísel. Je zřejmé, že takový vztah, spolu s volbou pro $f(0)$, zadává jednoznačně celou nekonečnou posloupnost hodnot $f(0), f(1), \dots, f(n), \dots$. Jako příklad může sloužit definiční formule pro faktoriál, tj. $n! = n \cdot (n-1)!$. Vidíme, že skutečně vztah pro $f(n+1)$ závisí na n i hodnotě $f(n)$.

Po konstantní závislosti je nejjednodušší tzv. *lineární diferenční rovnice*

e1.4 (1.5) $$f(n+1) = a \cdot f(n) + b,$$

kde a, $b \in \mathbb{N}$. Takovou rovnici umíme snadno řešit. Je-li $b = 0$, pak zjevně

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

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, tj.

e1.5 (1.6) $$f(n+1) = a_n \cdot f(n) + b_n$$

1.9

1.12. Věta. *Obecné řešení diferenční rovnice (1.6) prvního řádu s počáteční podmínkou $f(0) = y_0$ je dáno vztahem*

e1.6 (1.7) $$f(n) = \left(\prod_{i=0}^{n-1} a_i\right) y_0 + \sum_{r=0}^{n-1} \left(\prod_{i=r+1}^{n-1} a_i\right) b_r.$$

Důkaz. Tvrzení dokážeme matematickou indukcí. Pro zjednodušení zápisu užíváme konvenci, že konečný součin s prázdnou množinou součinitelů je roven jedné (podobně jako součet s prázdnou množinou sčítanců je roven nule). To je zapotřebí v samotné formuli v pravém sčítanci pro hodnotu $r = n-1$, kde není žádné vyhovující i.

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

$$\begin{aligned} f(n+1) &= a_n \left(\left(\prod_{i=0}^{n-1} a_i\right) y_0 + \sum_{r=0}^{n-1} \left(\prod_{i=r+1}^{n-1} a_i\right) b_r \right) + b_n \\ &= \left(\prod_{i=0}^{n} a_i\right) y_0 + \sum_{r=0}^{n} \left(\prod_{i=r+1}^{n} a_i\right) b_r, \end{aligned}$$

jak se přímo vidí roznásobením výrazů. □

1.10 **1.13. Důsledek.** *Obecné řešení lineární diferenční rovnice (1.5) s $a \neq 1$ a počáteční podmínkou $f(0) = y_0$ je*

e1.7
$$f(n) = a^n y_0 + \frac{1-a^n}{1-a} b. \tag{1.8}$$

Důkaz. Dosazením konstantních hodnot za a_i a b_i do obecné formule dostáváme zjevně první sčítanec okamžitě. Pro vyčíslení součtu součinů v druhém si je třeba všimnout, že se jedná o výrazy $(1 + a + \cdots + a^{n-1})b$. Sečtením této geometrické řady (připomeňme, že $1 - a^n = (1-a)(1 + a + \cdots + a^{n-1})$) dostaneme právě požadovaný výsledek. □

Uveďme si praktické příklady na řešení diferenčních rovnic prvního řádu:

1.14. Příklady.

1.14.1. Splácení půjčky *Mirek si chce koupit nové auto. Auto 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 bych chtěl auto splatit za tři roky. Jak vysoká bude měsíční splátka?*

Řešení. Označme Mirkovu měsíční splátku S. Po prvním měsíci splatí Mirek S korun, z nichž část půjde na vlastní splátku, část na splacení úroku. Částku, kterou bude Mirek dlužit po uplynutí k měsíců označme d_k. Po prvním měsíci bude Mirek dlužit

$$d_1 = 300000 - S + \frac{0,06}{12} 300000. \tag{1.9}$$

Obecně po uplynutí k-tého měsíce

lr
$$d_k = d_{k-1} - S + \frac{0,06}{12} d_{k-1}. \tag{1.10}$$

Podle vztahu (1.8) je d_k dáno následovně

$$d_k = \left(1 + \frac{0,06}{12}\right)^k 300000 - \left[\left(1 + \frac{0,06}{12}\right)^k - 1\right] \left(\frac{12S}{0,06}\right). \tag{1.11}$$

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

$$S = 300000 \left(\frac{\frac{0,06}{12}}{1 - (1 + \frac{0,06}{12})^{-36}}\right) \doteq 9127. \tag{1.12}$$

□

Všimněme si, že rekurentní vztah (1.10) můžeme použít na náš příklad pouze tak dlouho, dokud budou všechna $y(n)$ kladná, tj. dokud bude Mirek skutečně něco dlužit.

Otázka. *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

$$q^k = \frac{200S}{200S - c},$$

jehož logaritmováním obdržíme

$$k = \frac{\ln 200S - \ln(200S - c)}{\ln g},$$

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

1.14.2. Stavební spoření. *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 rok) 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 $x_1 = 36000 + 3000\left(1 + \frac{11}{12} + \cdots + \frac{1}{12}\right) = 36585$, celkem

$$x_5 = 38115 \left(\frac{(1,03)^4 - 1}{0,03}\right) + (1,03)^4 \cdot 36585 + 1500 \doteq 202136.$$

□

1.15. 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 ...

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

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

Řešení. $y_n = 2(\frac{3}{2})^n - 2$. □

1.11

1.16. Rovnice druhého řádu. Obecně nazýváme *diferenční rovnicí řádu* k vztah

$$f(n+k) = F(n, f(n), \ldots, f(n+k-1)) = 0,$$

kde F je známá skalární funkce v $k+1$ proměnných skalárních veličinách. Celá poslounost hodnot je jednoznačně určena volbou k-tice čísel $f(0), \ldots, f(k-1)$.

Lineární diferenční rovnicí druhého řádu rozumíme

e1.8 (1.13) $$f(n+2) = a \cdot f(n+1) + b \cdot f(n) + c,$$

kde a, b, c jsou známé skalární koeficienty. Dobře známým příkladem s $c = 0$ je např. Fibonacciho posloupnost čísel $y_0, y_1, \ldots$, viz příklad 1.17.1. Zkusme dosadit

do rovnice (1.13) podobné řešení jako u lineárních, tj. $f(n) = \lambda^n$ pro nějaké skalární λ. Dosazením dostáváme

$$\lambda^{n+2} - a\lambda^{n+1} - b\lambda^n = \lambda^n(\lambda^2 - a\lambda - b) = 0$$

a odtud vidíme, že buď je $\lambda = 0$ nebo

$$\lambda_1 = \frac{1}{2}(a + \sqrt{a^2 + 4b}), \quad \lambda_2 = \frac{1}{2}(a - \sqrt{a^2 + 4b}).$$

Protože součet dvou řešení rovnice $f(n+2) - a \cdot f(n+1) - b \cdot f(n) = 0$ je opět řešením téže rovnice a totéž platí pro konstatní násobky řešení, odvodili jsme obecné řešení $f(n) = C_1\lambda_1^n + C_2\lambda_2^n$ a 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. Ukažme alespon na jednom příkladě.

e1.9 (1.14)
$$y_{n+2} = y_{n+1} + \frac{1}{2}y_n$$
$$y_0 = 2, y_1 = 0.$$

V našem případě je tedy $\lambda_{1,2} = \frac{1}{2}(1 \pm \sqrt{3})$ a zjevně $y_0 = C_1 + C_2 = 2$ a $y_1 = \frac{1}{2}C_1(1 + \sqrt{3}) + \frac{1}{2}C_2(1 - \sqrt{3})$ je splněno pro právě jednu volbu těchto konstant. Přímým výpočtem $C_1 = 1 - \frac{1}{3}\sqrt{3}$, $C_2 = 1 + \frac{1}{3}\sqrt{3}$.

Tento příklad je velice poučný z mnoha důvodů. Na první pohled je vidět, že použitá metoda funguje pro obecné lineární diferenční rovnice bez absolutních členů. Řešení tu lze hledat pomocí kořenů tzv. charakteristického polynomu rovnice. Dále si všimněme, 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 utečou do neomezených kladných nebo záporných hodnot.

Ukážeme „populační model“, který je příkladem na rekurentní rovnici druhého řádu:

1.17. Příklady.

1. **1.17.1. 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 splodí 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 neumře a žádný se tam „nepřistěhuje“)?*

Řešení. Po uplynutí prvního měsíce je na louce pořád jeden pár, nicméně samička otěhotní. Po dvou měsích se narodí první potomci, takze na louce budou dva páry. Po uplynutí každého dalšího měsíce se narodí (tedy přibude) tolik zajíců, kolik otěhotnělo zaječic před měsícem, což je přesně tolik, kolik bylo před měsícem párů schopných splodit 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

párů v předchozích dvou měsících. Pro počet párů zajíců na louce tedy dostáváme *homogenní lineární rekuretní formuli*

fib (1.15) $$p_{n+2} = p_{n+1} + p_n, \quad n = 1, \dots,$$

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 dále pro nehomogenní formule). Pro hodnotu n-tého členu můžeme odvodit explicitní formuli. V hledaní formule nám pomůže pozorování, že pro jistá r je funkce r^n řešením rekurentní formule bez počátečních podmínek. Tato r získáme prostě tak, že dosadíme do rekurentního vztahu:

fib (1.16) $$r^{n+2} = r^{n+1} + r^n \quad \text{a po vydělení } r^n \text{ dostaneme}$$

(1.17) $$r^2 = r + 1,$$

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 $a_n = (\frac{1-\sqrt{5}}{2})^n$ a $b_n = (\frac{1+\sqrt{5}}{2})^n$, $n \geq 1$ vyhovují danému vztahu. Zřejmě také jejich libovolná lineární kombinace $c_n = sa_n + tb_n$, $s, t \in \mathbb{R}$. 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

(1.18) $$p_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n(\sqrt{5})}.$$

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 jednoznačně zadána. □

Posloupnost zadaná rekurentní formulí (1.15) se nazývá *Fibonacciho posloupnost*. Tato formule je příkladem homogenní lineární diferenční rovnice. Další příklad ukáže na ekonomickém modelu případ tzv. nehomogenní diferenční rovnice

3. **1.17.2. Zjednodušený model chování národního produktu**

(1.19) $$y_{k+2} - a(1+b)y_{k+1} + aby_k = 1,$$

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

$$x^2 - a(1+b)x + ab = 0, \quad \text{tj. } x^2 - x + \frac{1}{4} = 0,$$

která má dvojnásobný kořen $\frac{1}{2}$. Všechna řešení homogenní rovnice jsou potom tvaru $a(\frac{1}{2})^n + bn(\frac{1}{2}^n)$.

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.

V našem případě (tj. pokud jsou všechny koeficienty i nehommogenní 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

$$y_{k+2} - y_{k+1} + \frac{1}{4}y_k = 1$$

jsou tedy tvaru $4 + a(\frac{1}{2})^n + bn(\frac{1}{2})^n$. 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 danéneho diferenční rovnice „uhodneme“ tvar partikulárního řešení. Tvary partikulárních řešení jsou známy pro celou řadu nehomogenních členů. Např. rovnice

$$y_{n+k} + a_1 y_{n+k-1} + \cdots + a_k y_n = P_m(n), \tag{1.20}$$

s reálnými kořeny charakteristické rovnice má partikulární řešení tvaru $Q_m(n)$, kde $P_m(n)$ a $Q_m(n)$ jsou polynomy stupně m.

Další možnou metodou řešení je tzv. *variace konstant*, kdy nejprve najdeme řešení

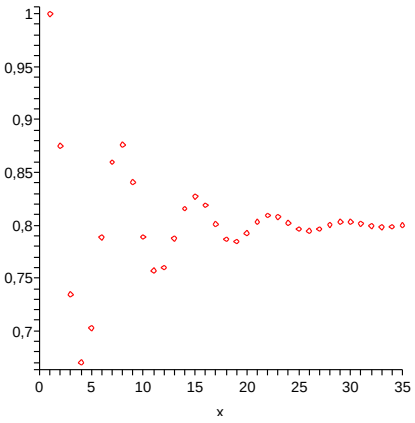
$$y(n) = \sum_{i=1}^{k} c_i f_i(n)$$

zhomogenizované rovnice a po té uvažujeme konstanty c_i jako funkce $c_i(n)$ proměnné n a hledáme partikulární řešení dané rovnice ve tvaru

$$y(n) = \sum_{i=1}^{k} c_i(n) f_i(n).$$

Ukažme si na obrázku hodnoty f_i pro $i \leq 35$ a rovnicí

$$f(n) = \frac{9}{8}f(n-1) - \frac{3}{4}f(n-2) + \frac{1}{2}, \quad f(0) = f(1) = 1$$



1.17.3. *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

$$x_{n+2} = 2x_n.$$

Její charakteristický polynom je $x^2 - 2$, jeho kořeny jsou $\pm\sqrt{2}$. Řešení zhomogenizované rovnice je tedy tvaru

$$a(\sqrt{2})^n + b(-\sqrt{2})^n, \quad \text{pro libovolné } a, b \in \mathbb{R}$$

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 partikulárním řešením je posloupnost $-n - 2$.

Řešení dané nehomogenní diferenční rovnice druhého řádu bez počátečních podmínek jsou tedy tvaru $a(\sqrt{2})^n + b(-\sqrt{2})^n - n - 2$, $a, b \in \mathbb{R}$.

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:

$$\begin{aligned} x_0 : &\quad a(\sqrt{2})^0 + b(-\sqrt{2})^0 - 2 = 1, \quad \text{tedy } a + b = 3 \\ x_1 : &\quad \sqrt{2}a - \sqrt{2}b = 4, \end{aligned}$$

jejichž řešením dostáváme $a = \frac{6+5\sqrt{2}}{4}$, $b = \frac{6-5\sqrt{2}}{4}$. Řešením je posloupnost

$$x_n = \frac{6 + 5\sqrt{2}}{4}(\sqrt{2})^n + \frac{6 - 5\sqrt{2}}{4}(-\sqrt{2})^n - n - 2.$$

□

1.17.4. *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

$$x^4 - x^3 - x + 1 = 0$$

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 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 $x_1 = -\frac{1}{2} + i\sqrt{3} = \cos(120°) + i\sin(120°)$ a $x_2 = -\frac{1}{2} - i\sqrt{3} = \cos(120°) - i\sin(120°)$.

Pro druhou hodnotu neznámé t dostáváme rovnici

$$x + \frac{1}{x} = 2$$

s dvojnásobným kořenem 1. Celkem je tedy bazí hledaného vektorového prostoru posloupností, které jsou řešením dané diferenční rovnice následující čtveřice posloupností: $\{-\frac{1}{2} + i\sqrt{3}\}_{n=1}^{\infty}$, $\{-\frac{1}{2} - i\sqrt{3}\}_{n=1}^{\infty}$,$\{1\}_{n=1}^{\infty}$ (konstantní posloupnost) a $\{n\}_{n=1}^{\infty}$. Hledáme-li však reálnou bazi, musíme nahradit dva generátory (posloupnosti) z této báze s komplexními hodnotami generátory reálnými. Protože tyto generátory odpovídají geometrickým řadám, jejichž libovolné členy jsou komplexně združená 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), $\{n\}_{n=1}^{\infty}$, $\{\cos(n \cdot 120°)\}_{n=1}^{\infty}$, $\{\sin(n \cdot 120°)\}_{n=1}^{\infty}$. □

1.17.5. *Určete explicitní vzorec pro n-tý člen jediné posloupnosti* $\{x_n\}_{n=1}^{\infty}$ *vyhovující následujícím podmínkám:*

$$x_{n+2} = x_{n+1} - x_n, \ , x_1 = 1, \ x_2 = 5.$$

Řešení. $x_n = 2\sqrt{3}\sin(n \cdot 60°) - 4\cos(n \cdot 60°)$. □

1.17.6. *Určete explicitní vzorec pro n-tý člen jediné posloupnosti* $\{x_n\}_{n=1}^{\infty}$ *vyhovující následujícím podmínkám:*

$$-x_{n+3} = 2x_{n+2} + 2x_{n+1} + x_n, \ , x_1 = 1, \ x_2 = 1 \, x_3 = 1.$$

Řešení. $x_n = -3(-1)^n - 2\cos(n \cdot 120°) - 2\sqrt{3}\sin(n \cdot 120°)$. □

1.17.7. *Určete explicitní vzorec pro n-tý člen jediné posloupnosti* $\{x_n\}_{n=1}^{\infty}$ *vyhovující následujícím podmínkám:*

$$-x_{n+3} = 3x_{n+2} + 3x_{n+1} + x_n, \ , x_1 = 1, \ x_2 = 1, \ x_3 = 1.$$

Řešení. $x_n = (-1)^n(-2n^2 + 8n - 7)$. □

1.12

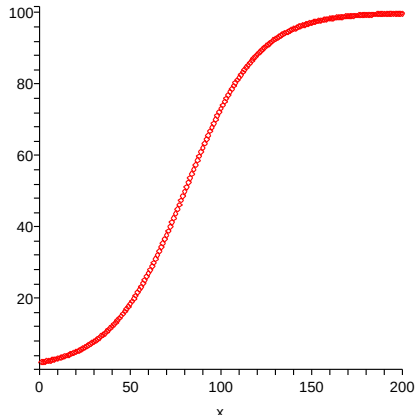
1.18. Nelineární příklad. Vraťme se na chvíli k rovnici prvního řádu, kterou jsme velice primitivně modelovali populační růst závisející přímo úměrně na okamžité velikosti populace p. Realističtější model bude mít takto úměrnou změnu populace $\Delta p(n) = p(n+1) - p(n)$ jen při malých hodnotách p, tj. $\Delta p/p \sim r > 0$. Při určité limitní hodnotě $p = K > 0$ ale naopak už populace neroste a při ještě větších už klesá. Předpokládejme, že právě hodnoty $y_n = \Delta p(n)/p(n)$ závisí na $p(n)$ lineárně. Chceme tedy popsat přímku v rovině proměnných p a y, která prochází body $[0, r]$ a $[K, 0]$. Položíme proto

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

Dosazením za y dostáváme $p(n+1) - p(n) = p(n)(-\frac{r}{K}p(n) + r)$, tj. diferenční rovnici prvního řádu

$$p(n+1) = p(n)(1 - \frac{r}{K}p(n) + r). \tag{1.21}$$

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 počáteční stav jsou právě dva jedinci.



4. Pravděpodobnost

Předchozí sekce naznačila, že hodnoty skalárních funkcí umíme definovat pomocí popisu jejich změn v závislosti na změnách závislé proměnné. Teď se podíváme na další obvyklý případ – sledované hodnoty často nejsou známy ani explicitně formulí, ani implicitně nějakým popisem. Jsou výsledkem nějaké nahodilosti a my se snažíme popsat s jakou *pravděpodobností* nastane ta či ona možnost.

1.19. Co je pravděpodobnost? Nejbanálnějším příkladem může sloužit obvyklé házení kostkou s šesti stranami 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 strana padne s pravděpodobností $\frac{1}{6}$“. Pokud ale si třeba sami nožíkem vyrobíme takovou kostku, 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 se tím náš matematický model skutečnosti stal (pro tento konkrétní případ) nedobrým.

V dalším budeme pracovat s abstraktním matematickým popisem pravděpodobnosti v nejjednoduším 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 matematikové také (nejspíše ve spolupráci s jinými experty). Později se vrátíme k pravděpodobnosti (jakožto teorii popisující chování nahodilých procesů nebo i plně determinovaných dějů, kde ovšem neznáme přesně všechny určující parametry) a matematické statistice (jakožto teorii umožňující posoudit, do jaké míry lze očekávat, že vybraný model je ve shodě s realitou). K tomu ovšem bude již potřebný dosti rozsáhlý matematický aparát, který budeme mezitím několik semestrů budovat.

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

- $\Omega \in \mathcal{A}$, 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,
- jsou-li $A, B \in \mathcal{A}$, pak $A \cup B \in \mathcal{A}$, tj. pro každé dva jevy je jevem i jejich sjednocení.

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 $\mathcal{A}$).

Zjevně je i 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

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

Pro naše házení kostkou je $\Omega = \{1, 2, 3, 4, 5, 6\}$ a jevové pole je tvořeno všemi podmnožinami. 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 Ω se nazývá *jistý jev*, prázdná podmnožina $\emptyset \in \mathcal{A}$ se nazývá *nemožný jev*,
- jednoprvkové podmnožiny $\{\omega\} \in \Omega$ 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 $A \subset B$,
- je-li $A \in \mathcal{A}$, pak se jev $B = \Omega \setminus A$ nazývá *opačný jev k jevu* A, píšeme $B = A^c$.

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

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

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

Funkci P nazýváme *pravděpodobností* na jevovém poli $(\Omega, \mathcal{A})$.

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

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

Dále můžeme matematickou indukcí snadno rozšířit aditivnost na jakýkoliv konečný počet neslučitelných jevů $A_i \subset \Omega$, $i \in I$, tj.

$$P(\cup_{i\in I} A_i) = \sum_{i\in I} P(A_i), \text{ kdykoliv je } A_i \cap A_j = \emptyset,\ i \neq j,\ i, j \in I.$$

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

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

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

1.23. Příklady.

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

$$1 - (1 - \frac{12}{10^5})^{5000} \doteq 0,45.$$

□

1.23.2. Ruleta. *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 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* 2500 *Kč v plusu, tak končí)*

Řešení. Nejprve spočítejme, kolikrát po sobě může Aleš prohrát. Začíná-li s 10 Kč, tak na n vsazení potřebuje

$$10 + 20 + \cdots + 10 \cdot 2^{n-1} = 10(\sum_{i=0}^{n-1} 2^i) = 10(\frac{2^n - 1}{2 - 1}) = 10 \cdot (2^n - 1).$$

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, pravděpodbnost prohry v osmi po sobě následujících (nezávislých) sázkách je tedy $(19/37)^8$. Pravděpodobnost, že vyhraje 10 Kč (při daném postupu) je tedy $1 - (19/37)^8$. Na to, aby vyhrál 2500 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. □

1.23.3. *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).*

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

(1) *v šestém poschodí,*
(2) *ve stejném poschodí,*
(3) *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 1.5 a 1.9)

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

□

1.23.5. *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, na nich jsou pak muži i ženy rozmístěny libovolně). Výsledná pravděpodobnost je tedy

$$p(n) = \frac{2(n!)^2}{(2n)!},\ p(2) \doteq 0,33,\ p(5) \doteq 0,0079,\ p(8) \doteq 0,00016$$

□

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

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 $c(8,2)c(4,3) = \binom{8}{2}\binom{4}{3}$ (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

Řešení.

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

□

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

Řešení. $\frac{2^2\cdot 3^3-1}{10^5-1}$. (v čitateli i jmenovateli odečítáme nulu) □

1.23.8. *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. Například rozdělíme uvažovaný jev na sjednocení tří disjunktních jevů: podle toho, kolikátou vytáhneme červenou kouli. Pravděpodobnosti, že vytáhneme koule přesně ve zvoleném pořadí jsou:

$$\frac{1}{2}\frac{4}{9}\frac{5}{8},\quad \frac{1}{2}\frac{5}{9}\frac{1}{2},\quad \frac{1}{2}\frac{5}{9}\frac{1}{2}.$$

Celkem $\frac{5}{12}$. □

1.23.9. *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. Pravděpodobnost toho, že i-tá vytažená koule bude černá je tedy rovna podílu počtu posloupností pěti červených, pěti bílých a šesti černých koulí, kdy je na i-tém místě černá koule

(těch je tolik, kolik je libovolných posloupností pěti bílých, pěti červených a pěti černých koulí, tedy $P(5,5,5) = \frac{15!}{5!5!5!}$) a počtu všech posloupností složených z pěti bílých, pěti červených a šesti černých koulí, tedy $P(6,5,5) = \frac{16!}{6!5!5!}$. Tedy celkem

$$\frac{\frac{15!}{5!5!5!}}{\frac{16!}{6!5!5!}} = \frac{3}{8}.$$

□

1.24. Příklad. Vraťme se k házení kostkou a zkusme popsat jevy ze základního prostoru Ω 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

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

Ze známé klasické pravděpodobnosti pro jednotlivé hody umíme odvodit pravděpodobnosti našich jevů v Ω. 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 dvěmi 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:

2	3	4	5	6	7	8	9	10	11	12
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.

Obecně je sčítání pravděpodobností složité. Následující věta je přímým promítnutím tzv. kombinatorického *principu inkluze a exkluze* do naší konečné pravděpodobnosti:

1.16 **1.25. Věta.** *Buďte $A_1, \dots, A_k \in \mathcal{A}$ libovolné jevy na základním prostoru Ω s jevovým polem $\mathcal{A}$. Pak platí*

$$\begin{aligned} P(\cup_{i=1}^k A_i) = & \sum_{i=1}^{k} P(A_i) - \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} P(A_i \cap A_j) \\ & + \sum_{i=1}^{k-2} \sum_{j=i+1}^{k-1} \sum_{\ell=j+1}^{k} P(A_i \cap A_j \cap A_\ell) \\ & - \cdots \\ & + (-1)^{k-1} P(A_1 \cap A_2 \cap \cdots \cap A_k). \end{aligned}$$

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

Skutečně, díky aditivní vlastnosti pravděpodobnosti si můžeme představit, že každý jev rozložíme na elementární (tj. jednobodové), jakkoliv ve skutečnosti nemusí jednoprvkové podmnožiny do jevového pole obecně patřit. Pak je pravděpodobnost každého jevu dána součtem pravděpodobností jednotlivých elementárních jevů do něj patřících a tvrzení věty můžeme číst následovně: sečteme všechny pravděpodobnosti výsledků ze všech 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.

Aby se takový postup stal důkazem, je zapotřebí si ujasnit, že skutečně všechny korekce, tak jak jsou napsány, 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“.

Důkaz. Pro $k = 1$ tvrzení zjevně platí a předpokládejme, že platí pro všechny počty množin menší než pevně zvolené $k > 1$. Nyní si uvědomme, že pro libovolné dva jevy platí $P(B) = P(B \cap A) + P(B \setminus A)$. Podobně

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

Toto je ale tvrzení naší věty pro $k = 2$. Nyní můžeme pracovat v indukčním kroku na formuli s $k + 1$ jevy, když sjednocení k jevů bereme jako A ve formuli výše, zatímco zbývající hraje roli B:

$$\begin{aligned} P(\cup_{i=1}^{k+1} A_i) &= P\big(\big(\cup_{i=1}^{k} A_i\big) \cup A_{k+1}\big) \\ &= \sum_{j=1}^{k} \left((-1)^{j+1} \sum_{1 \le i_1 < \cdots < i_j \le k} P(A_{i_1} \cap \cdots \cap A_{i_j}) \right) + P(A_{k+1}) \\ &\quad - P((A_1 \cup \cdots \cup A_k) \cap A_{k+1}). \end{aligned}$$

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

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

a pro tento výraz opět použít indukční předpoklad, tj. formuli ve větě. Zjevně tím právě přidáme všechny dosud chybějící členy. □

1.26. Poznámka. Speciálním případem předchozí věty je situace, kdy všechny konečné podmnožniny základního prostoru jsou jevy a všechny elementární jevy mají stejnou pravděpodobnost. Ve formuli 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. Pak můžeme vyčíst následující tvrzení pro obecnou konečnou množinu M a její podmnožiny $A_1, \ldots, A_k$. Budeme psát $|M|$ pro počet prvků množiny M, tj. pro *mohutnost* množiny M.

$$|M \setminus (\cup_{i=1}^k A_i)| = |M| + \sum_{j=1}^{k} \left((-1)^i \sum_{1 \le i_1 < \cdots < i_j \le k} |A_{i_1} \cap \cdots \cap A_{i_j})| \right). \tag{1.22}$$

Skutečně, $|\cup_{i=1}^k A_i| + |M \setminus (\cup_{i=1}^k A_i)| = |M|$, tzn.

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

a dosazením z naší věty dostáváme právě požadované tvrzení. Říká se mu *princip inkluze a exkluze*.

Uveďme si příklad, jak vypadá využití principu inkluze a exkluze:

1.27. Příklady.

5. **1.27.1. Nepořádná sekretářka** *Sekretářka má rozeslat pět dopisů pěti různým lidem. Dopisy pro různé adresáty vkládá do obálek s adresami náhodně. Jaká je pravděpodobnost, že alespoň jeden člověk dostane dopis určený pro něj?*

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 pěti, tak všechny příznivé jevy (tedy žádný dopis nepřijde do obálky se stejným číslem) odpovídají takovým pořadím pěti prvků, kdy i-tý prvek není na i-tém místě ($i = 1, \ldots, 5$), 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

$$d = 5! - |M_1 \cup \cdots \cup M_5|$$

Počet prvků průniku $|M_{i_1} \cap \cdots \cap M_{i_k}|$, $k = 1, \ldots, 5$ je $(5-k)!$ (pořadí prvků $i_1, \ldots, i_k$ je pevně dáno, ostatních $5-k$ prvků řadíme libovolně). Podle principu inkluze a exkluze je

$$|M_1 \cup \cdots \cup M_5| = \sum_{k=1}^{5} (-1)^{k+1} \binom{5}{k} (5-k)!$$

a tedy pro hledaný počet d dostáváme vztah

$$\begin{aligned} d &= 5! - \sum_{k=1}^{5} (-1)^{k+1} \binom{5}{k} (n-k)! \\ &= \sum_{k=0}^{5} (-1)^k \binom{5}{k} (5-k)! = 5! \sum_{k=0}^{5} \frac{(-1)^k}{k!} \end{aligned}$$

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

$$\sum_{k=0}^{5} \frac{(-1)^k}{k!}$$

a hledaná pravděpodobnost pak

$$1 - \sum_{k=0}^{5} \frac{(-1)^k}{k!} = \frac{19}{30}.$$

□

1.27.2. *Kolika způsoby lze rozestavit n shodných věží na šachovnici $n \times n$ tak, aby bylo každé neobsazené pole ohrožováno některou z věží?*

Řešení. Daná rozestavení jsou sjednocením dvou množin: množiny rozestavení, kdy je alespoň v jednom řádku 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:

$$2n^n - n!.$$

□

1.28. Nezávislé jevy. Uvažme libovolný pravděpodobnostní prostor $(\Omega, \mathcal{A}, P)$ a v něm nějaké jevy $A_1, \dots, A_k$. 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

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

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

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

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

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

$$A_1 \cup \dots \cup A_k = (A_1^c \cap \dots \cap A_k^c)^c$$

a dostáváme:

$$P(A_1 \cup \cdots \cup A_k) = 1 - P(A_1^c \cap \cdots \cap A_k^c) = 1 - (1 - P(A_1)) \dots (1 - P(A_k)).$$

1.29. Podmíněná pravděpodobnost. Obvyklé je také klást dotazy s dodatečnou podmínkou. Např. „jaká je pravděpodobnost, že při hodu dvěmi kostkami padly dvě pětky, je-li součet hodnot deset?“. Formalizovat takové potřeby umíme následovně.

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 nezávislé tehdy a jen tehdy, je-li $P(A) = P(A|H)$. Přímo z definice také vyplývá tzv. „věta o násobení pravděpodobností“ pro jevy $A_1, \dots, A_k$ splňující $P(A_1 \cap \cdots \cap A_k) > 0$:

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

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.

1.30. Příklady.

1.30.1. *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 jev, že ani na jedné kostce nepadne dvojka jako B, jev „padne součet 7“ jako A. Množinu všech možných výsledků budeme značit opět jako Ω. Pak

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

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 nejsou stochasticky nezávislé. □

1.31. 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 Ω se známým obsahem $\operatorname{vol}\Omega$ (symbol „vol“ od anglického „volume“, tj. obsah/objem). Příkladem může sloužit třeba jednotkový čtverec. Náhodné jevy budou reprezentovány podmnožinami $A \subset \Omega$ za jevové pole $\mathcal{A}$ bereme systém podmnožin, u kterých umíme určit jejich obsah. Třeba všechna konečná sjednocení trojúhelníků. Nastoupení nebo nenastoupení jevu je dáno výběrem bodu v Ω, kterým se trefíme nebo netrefíme do množiny reprezentující jev A.

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

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

Uvažme jako příklad problém, kdy náhodně vyberem dvě hodnoty $a < b$ v intervalu $(0, 1) \subset \mathbb{R}$. Všechny hodnoty a i b jsou stejně pravděpodobné a otázka zní „jaká je pravděpodobnost, že interval (a, b) bude mít velikost alespoň jedna polovina?“.

Odpověď je docela jednoduchá: volba čísel a, b je volbou libovolného bodu (a, b) ve vnitřku trojúhelníku Ω s hraničními vrcholy $[0, 0]$, $[0, 1]$, $[1, 1]$ (načrtněte si obrázek!). Potřebujeme znát plochu podmnožiny, která odpovídá bodům s $b > a + \frac{1}{2}$, 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?“.

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 a čtverce poloměru. Pokud zvolíme za Ω jednotkový čtverec a za A průnik Ω 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 vygenerované dvojice (a, b) menší než jedna, tj. $\sqrt{a^2 + b^2} < 1$, pak výsledek bude při velkém počtu pokusů s velikou jistotou dobře aproximovat číslo $\frac{1}{4}\pi$. Numerickým postupům založeným na tomto principu se říká *metody Monte Carlo*.

Obdobné úlohy na geometrickou pravděpodobnost lze bezezbytku formulovat v $\mathbb{R}^3$ a obecněji. Uveďme ale ještě raději jednoduchý příklad v rovině:

1.32. Příklady.

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

Řešení. Náhodné rozdělení tyče na tři díly interpretujeme jako náhodný výběr dvou bodů řezu. Pravděpodobnostní prostor je tedy čtverec 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:

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

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

1.32.2. *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 2h. Jaká je pravděpodobnost, že se po cestě potkají (jezdí po stejné trase). Cesta trvá oběma 2h.*

Řešení. Prostor všech možných jevů je čtverec 10×10, Mirek vyjíždějící v čase x, potká Marka vyjíždějícího v čase y právě když $|x - y| \leq 2$. Tato nerovnost vymezuje v daném čtverci oblast „příznivých jevů“. Obsah zbylé části spočítáme přímo jednodušeji, neboť je sjednocením dvou pravoúhlých rovnoramenných trojúhelníků o

odvěsnách 8, tedy je roven 64, obsah části odpovídající „příznivým jevům“ je tedy 36, celkem je hledaná pravděpodobnost

$$\frac{36}{100} = \frac{9}{25}$$

□

1.32.3. *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 3×3. 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 $11/38$ obsahu čtverce. Tomuto zlomku je tedy rovna i hledaná pravděpodobnost. □

1.32.4. *Jednou denně někdy mezi osmou hodinou ranní a osmou hodinnou 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 12×12, 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 7, tedy je roven 49, obsah části odpovídající „příznivým jevům“ je tedy 95, celkem je hledaná pravděpodobnost

$$\frac{95}{144}.$$

□

1.32.5. Extreme games. *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 rychostí 72 km/h a jsou dlouhé 100metrů, cesta trvá 30min, vlaky se míjejí někde na trase. Hazardér Jarda 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 mpžností je tedy úsečka $\langle 0, 1800 s \rangle$, prostor „příznivých“ možností je úsečka délky $7,5$ ležící někde uvnitř předchozí úsečky. Pravděpodobnost uražení hlavy je tedy $7,5/1800$. □

5. Geometrie v rovině

Na konci minulé kapitoly jsme intuitivně používali elementární pojmy z geometrie reálné roviny. Budeme teď podrobněji zkoumat jak se vypořádávat s potřebou popisovat „polohu v rovině“, resp. dávat do souvislostí polohy různých bodů roviny.

1.23

1.33. Afinní rovina a vektorový prostor $\mathbb{R}^2$. Zkusme si množinu $A = \mathbb{R}^2$ 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 ví, co to znamená posunout se v libovolném násobku nějakého směru. Časem 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 $[0, 1]$“. Do všech ostatních se pak dostane tak, že poskočí „a–krát ve směru $[1, 0]$“, pak „b–krát ve směru $[0, 1]$“ 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 $[0, 1]$ a pak teprve v tom druhém.

To, co jsme popsali, se nazývá volba *(afinního) souřadného systému v rovině*, bod O je jeho *počátkem*, posunutí $E_1 - O$ ztotožňujeme s dvojicí $[1, 0]$, podobně u E_2 a obecně každý bod P roviny je ztotožněn s dvojicí čísel $[a, b] = P - O$.

Všimněme si, že zároveň volbou pevného počátku O jsou ztotožněny jednotlivé body P roviny se směry posuvu $v = P - O$ a že všechny takové posuvy umíme skládat (budeme říkat „sčítat“) a také jednotlivé směry násobit v poměru každého reálného čísla (budeme říkat „násobit skalárem“). Takovéto operace sčítání a násobení splňují hodně vlastností skalárů, viz 1.1 a 1.2, zkuste si promyslet které. Uvidíme brzy, že se jedná o standarní příklad (dvourozměrného reálného) vektorového prostoru. Budeme proto už teď místo o směrech posuvu mluvit o *vektorech* a od bodů je budeme rozlišovat tím, že budou dány dvojicemi souřadnic v kulatých závorkách místo hranatých.

1.24

1.34. Přímky v rovině. Když se náš pozorovatel umí posouvat o libovolný násobek pevného vektoru, pak také ví, co je to *přímka*. Je to podmnožina $p \subset A$ v rovině taková, že existují bod O a 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 $v = (\alpha, \beta)$:

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

Jednoduchým výpočtem dostaneme (vyloučíme t z parametrického vyjádření pro x a y, když pro určitost předpokládáme, že třeba $\alpha \neq 0$)

$$-\beta x + \alpha y + (\beta x_0 - \alpha y_0) = 0.$$

To je obecná rovnice přímky

e1.12 (1.23) $$ax + by = c,$$

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

e1.13 (1.24) $$a\alpha + b\beta = 0.$$

Výraz nalevo v rovnici přímky (1.23) 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, pro které body bude tato konstanta nula.

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

e1.14
$$\begin{aligned} ax + by &= r \\ cx + dy &= s. \end{aligned} \tag{1.25}$$

Opět můžeme levou stranu vnímat jako přiřazení, které každé dvojici souřadnic $[x(P), y(P)]$ bodů v rovině přiřadí vektor hodnot dvou skalárních funkcí F_1 a F_2 daných levými stranami jednotlivých rovnic (1.25). 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 zadaného vektoru $w = (r, s)$.

1.25
1.35. Lineární zobrazení a matice. Přiřazení F, se kterým jsme pracovali při popisu průniku přímek, zjevně respektuje operace sčítání a násobení s vektory a skaláry:

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

pro všechny $a, b \in \mathbb{R}$, $v, w \in \mathbb{R}^2$. Říkáme, že F je *lineární zobrazení* z $\mathbb{R}^2$ do $\mathbb{R}^2$, a píšeme $F : \mathbb{R}^2 \to \mathbb{R}^2$. Obdobně, v rovnici 1.23 pro přímku šlo o lineární zobrazení $F : \mathbb{R}^2 \to \mathbb{R}$ a jeho předepsanou hodnotu c.

Stručně budeme zapisovat taková zobrazení pomocí *matic* a jejich násobení, které definujeme takto:

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

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 obrdržíme jako výsledek opět matice. Snadno ověříme tzv. asociativitu násobení (zkuste propočítat!):

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

Stejně snadno je vidět i distributivita $A \cdot (B + C) = A \cdot B + A \cdot C$, neplatí však komutativita a existují „dělitelé nuly“. Např.

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

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 $\mathbb{R}$. Samozřejmě, 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 pomocí vztahu

e1.15
$$ad - bc = 0 \tag{1.26}$$

tj. vyjádření, kdy jsou nalevo v rovnicích (1.25) stejné výrazy až na skalární násobek. V takovém případě bud nebude v průniku žádný bod (rovnoběžné různé přímky) nebo tam budou všechny body přímky (stejné přímky). Ověřte!

Výrazu nalevo v (1.26) říkáme *determinant* matice A a píšeme pro něj $\det A = ad - bc$, případně

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

Jestliže k výsledku lineárního zobrazení ještě dovolíme přičíst pevný vektor $T = (x(T), y(T))$, tj. naše zobrazení bude

$$v = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \cdot v + T = \begin{pmatrix} ax + by + x(T) \\ cx + dy + y(T) \end{pmatrix},$$

máme popsána právě všechna tzv. *afinní zobrazení roviny* do sebe. Známými příklady jsou všechny afinní podobnosti. Lineární zobrazení pak odpovídají těm afinním zobrazením, které zachovávají pevný bod O.

Co se stane, když náš pozorovatel z odstavce 1.33 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 bude právě změna realizovaná pomocí afinního zobrazení. Časem budeme vidět obecné důvody, proč tomu tak je ve všech dimenzích.

1.26

1.36. Euklidovská rovina. Přidejme nyní schopnost našeho pozorovatele vidět vzdálenosti. Okamžitě pak můžeme definovat pojmy jako jsou úhel a otočení v rovině.

Jednoduše si to můžeme představit takto: rozhodne se 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 větu. Odtud vyjde známý vzorec pro velikost vektoru $v = (a, b)$

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

Jiný možný postup by byl, kdyby pozorovatel vyšel z pojmu vzdálenost (a věděl co znamená „kolmý“ třeba díky Euklidově větě), zvolil první z vektorů velikosti jedna, zvolil si orientaci (třeba proti směru hodinových ručiček) a vybral jednotkový kolmý směr (jednoznačně určí z požadavku platnosti Euklidovy věty třeba pomocí pravoúhlého trojúhelníku se stranami o velikostech 3, 4 a 5).

Úhel φ dvou vektorů v, w v rovině pak zpravidla popisujeme s využitím tzv. goniometrické funkce $\cos\varphi$. Používaný vzorec pro funkci cos je dán hodnotou reálné první souřadnice jednotkového vektoru, jehož úhel s vektorem $(1, 0)$ je φ. 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 $v = (x(v), y(v))$, $w = (x(w), y(w))$ takto:

$$\cos\varphi = \frac{x(v) \cdot x(w) + y(v) \cdot y(w)}{\|v\| \cdot \|w\|}.$$

Dobrým příkladem lineárního zobrazení, které zachovává velikosti, je rotace o předem daný úhel ψ. Je dáno formulí s maticí R_ψ:

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

Specielně, aplikací na jednotkový vektor $(1, 0)$ dostáváme skutečně právě očekávaný výsledek $(\cos\psi, \sin\psi)$.

Pokud bychom chtěli zapsat rotaci kolem jiného bodu $P = O + w$, snadno napíšeme formuli pomocí translací:

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

Dalším příkladem 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 translací. Hledejme tedy matici Z_ψ zrcadlení vzhledem k přímce s jednotkovým směrovým vektorem v svírajícím úhel ψ s vektorem $(1, 0)$. Např.

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

a obecně můžeme psát (otočíme do „nulové“ polohy, odzrcadlíme a vrátíme zpět)

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

Můžeme proto (díky asociativitě násobení matic) spočíst:

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

Povšimněme si také, že

$$Z_\psi \cdot Z_0 = \begin{pmatrix} \cos 2\psi & \sin 2\psi \\ \sin 2\psi & -\cos 2\psi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos 2\psi & -\sin 2\psi \\ \sin 2\psi & \cos 2\psi \end{pmatrix}.$$

To lze zformulovat jako

Tvrzení. *Otočení o úhel ψ 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), dokázali jsme právě standardní formule pro goniometrické funkce dvojnásobného úhlu.

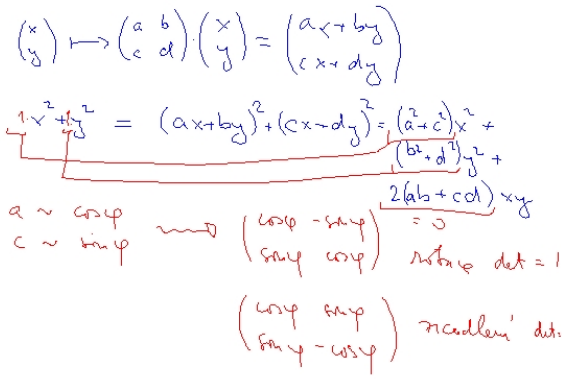
Hlubší je následující rekapitulace předchozích úvah:

1.27 **1.37. Věta.** *Lineární zobrazení euklidovské roviny je složeno ze 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 přitom právě tehdy, když je determinant matice R roven jedné, což odpovídá sudému počtu zrcadlení. Při lichém počtu zdrcadlení je determinant roven -1.

Promyslete si podrobněji úplný důkaz. Na tabuli vypadal jeho náznak takto:



1.28

1.38. Obsah trojúhelníka. Závěrem našeho malého výletu do geometrie se zaměřme na pojem obsah. Trojúhelník je vymezen dvojicí vektorů v a w, které přiloženy do počátku O zadají zbylé dva vrcholy. Chtěli bychom tedy najít formuli (skalární funkci vol), která dvěma vektorům přiřadí číslo rovné obsahu $\operatorname{vol}\Delta(v,w)$ takto definovaného trojúhelníku $\Delta(v,w)$.

Ze zadání je vidět, že by mělo platit (nakreslete si a uvažujte plochu jako součin základny krát výšky podělené dvěma – výška součtu bude jistě součtem výšek…)

$$\operatorname{vol}\Delta(v+v',w) = \operatorname{vol}\Delta(v,w) + \operatorname{vol}\Delta(v',w)$$
$$\operatorname{vol}\Delta(av,w) = a\operatorname{vol}\Delta(v,w)$$

a přidejme 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.

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 souřadných vektorů $v = (1,0)$ a $w = (0,1)$ a evidentně tedy každá možnost pro $\operatorname{vol}\Delta$ je jednoznačně určena už vyčíslením na této jediné dvojici argumentů (v,w). Jsou si tedy všechny možnosti rovny až na skalární násobek. Ten umíme určit požadavkem

$$\operatorname{vol}\Delta((1,0),(1,0)) = \frac{1}{2},$$

tj. volíme *orientaci* a *měřítko*.

Vidíme tedy, že determinant zadává plochu rovnoběžnostěnu určeného sloupci matice A (a plocha trojúhelníku je tedy poloviční).

1.29

1.39. Viditelnost v rovině. Předchozí popis hodnot pro orientovaný objem nám dává do rukou elegantní nástroj pro určování viditelnosti orientovaných úseček. Orientovanou úsečkou rozumíme dva body v rovině $\mathbb{R}^2$ s určením pořadím. Můžeme

si ji představovat jako šipku od prvého k druhému bodu. Taková orientovaná úsečka nám rozděluje rovinu na dvě poloroviny, říkejme jim „levou“ a „pravou“.

Jestliže uvažujeme obvyklou orientaci „proti směru hodinových ručiček“ pro hranici mnohoúhelníku, pak pozorovatel nalevo od orientované úsečky (tj. uvnitř takového mnohoúhelníka) tuto vidí a naopak pozorovatel napravo ji nevidí. Má tedy smysl ptát se, jestli je orientovaná úsečka $[A, B]$ v rovině viditelná z bodu C.

Spočtěme orientovanou plochu příslušného trojúhelníku zadaného vektory $A-C$ a $B-C$. Pokud jsme s bodem C nalevo od úsečky, pak při naší orientaci bude vektor $A-C$ dříve než ten druhý a proto výsledná plocha (tj. hodnota determinantu) bude kladná. To odpovídá situaci, kdy úsečku vidíme. Naopak, při opačné poloze bude výsledkem záporná hodnota determinantu a podle zjistíme, že úsečku nevidíme.

Uvedený jednoduchý postup je často využíván pro testování polohy při standardních úlohách v 2D grafice.

Závěrem této části si uveďme několik standardních příkladů:

1.40. Příklady.

1.40.1. *Je dána přímka*

$$p: \ [2,0] + t(3,2).$$

Určete její obecnou rovnici a nalezněte průnik s přímkou

$$q: \ [-1,2] + s(1,3).$$

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 na úsečce 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 úsečky q dostáváme souřadnice průsečíku P:

$$P = [-\frac{19}{7}, -\frac{22}{7}]$$

. □

1.40.2. *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 zrcadlením 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 polopřímky dané odraženým paprskem ($t=-2$). Odražený paprsek tedy přímku q neprotne. □

1.40.3. *Z bodu* $[-2,0]$ *vyrazila v pravé poledne konstantní rychlostí* $1ms^{-1}$ *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:

$$\begin{aligned} p &: [-2,0]+r(3,2)\\ q &: [5,-2]+s(-1,1), \end{aligned}$$

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 v bodě $[-2,0]$, druhá v bodě $[5,-2]$. Za čas t sekund urazí první t jednotek délky ve směru $(3,2)$ druhá pak $2t$ jednotek délky ve směru $(-1,1)$. Odpovídající parametrizace jsou tedy

$$p : [-2,0]+\frac{t}{\sqrt{13}}(3,2) \tag{1.27}$$

$$q : [5,-2]+\sqrt{2}t(-1,1), \tag{1.28}$$

(1.29)

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 a tedy v době, kdy dorazí do průsečíku P počátek první úsečky, bude již druhá úsečka pryč a úsečky se tak nesrazí. □

1.40.4. Viditelnost stran trojúhelníka. *Je dán trojúhelník s vrcholy* $[5,6]$*,* $[7,8]$*,* $[5,8]$*. Určete, které jeho strany je vidět z bodu* $[0,1]$*.*

Řešení. Uspořádáme vrcholy v kladném smyslu, tedy proti směru hodinových ručiček: $[5,6]$, $[7,8]$, $[5,8]$. Pomocí příslušných determinantů určíme, je-li bod $[0,1]$ „nalevo“ či „napravo“ od jednotlivých stran trojúhelníka uvažovaných jako orientované úsečky,

$$\begin{vmatrix} 7 & 5\\ 7 & 7 \end{vmatrix}>0 \qquad \begin{vmatrix} 5 & 5\\ 7 & 5 \end{vmatrix}<0 \qquad \begin{vmatrix} 5 & 7\\ 5 & 7 \end{vmatrix}=0$$

Z nulovosti posledního determinantu vidíme, že body $[0,1]$, $[5,6]$ a $[7,8]$ leží na přímce, stranu $[5,6][7,8]$ tedy nevidíme. Stranu danou vrcholy $[5,8]$ a $[7,8]$ pak narozdíl od strany $[5,6][5,8]$ nevidíme. □

1.40.5. *Určete, které strany čtyřúhelníka s vrcholy* $[95,99]$*,* $[130,106]$*,* $[40,60]$*,* $[130,120]$*. jsou viditelné z bodu* $[2,0]$*.*

Řešení. Nejprve je třeba určit strany čtyřúhelníka („správné“ pořadí vrcholů): $[95,99][40,60][130,106][130,120]$. Po spočítání příslušných determinantů (viz přednáška) zjistíme, že jsou vidět pouze strana $[40,60][130,106]$. □

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

1.40.7. *Určete obsah čtyřúhelníka $ABCD$ s vrcholy $A = [1, 0]$, $B = [11, 13]$, $C = [2, 5]$ a $D = [-2, -5]$.*

Řešení. Rozdělíme na dva trojúhelníky ABC a ACD. Jejich obsahy pak spočítáme pomocí patřičných determinantů, viz 1.38

$$S = \frac{1}{2}\begin{vmatrix} 1 & 5 \\ 10 & 13 \end{vmatrix} + \frac{1}{2}\begin{vmatrix} 1 & 5 \\ -3 & -5 \end{vmatrix} = \frac{47}{2}.$$

□

1.40.8. *Buď dán pravidelný šestiúhelník $ABCDEF$ (vrcholy jsou označeny v kladném smyslu) se středem v bodě $[1, 0]$ 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:

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

□

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

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

1.40.10. *Napište souřadnice vrcholů trojúhelníka, který vznikne otočením rovnostranného trojúhelníka jehož dva vrcholy jsou $[1, 1]$ a $[2, 3]$ (třetí pak v polorovině dané přímkou $[1, 1][2, 3]$ a bodem $[0, 0]$) o $60°$ v kladném smyslu kolem bodu $[0, 0]$.*

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

1.40.11. *Určete obsah trojúhelníka $A_2A_3A_{11}$, kde $A_0A_1 \dots A_{11}$ 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: $A_2 = \cos(\pi/3) + i\sin(\pi/3) = 1/2 + i\sqrt{3}/2$, $A_3 = \cos(\pi/2) + i\sin(\pi/2) = i$, $A_{11} =$

$\cos(-\pi/6) + i\sin(-\pi/6) = \sqrt{3}/2 - i/2$. Podle vzorce pro obsah trojúhelníka je potom hledaný obsah S roven

$$S = \frac{1}{2}\left|\begin{matrix} A_2 - A_{11} \\ A_3 - A_{11} \end{matrix}\right| = \frac{1}{2}\left|\begin{matrix} \frac{1}{2} - \frac{\sqrt{3}}{2} & \frac{1}{2} + \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} + \frac{3}{2} & \end{matrix}\right| = \frac{3-\sqrt{3}}{4}.$$

□

1.40.12. 4. *Určete odchylku (nebo její cosinus) úhlopříček A_3A_7 a A_5A_{10} pravidelného dvanáctiúhelníka*
$A_0A_1A_2A_3A_4A_5A_6A_7A_8A_9A_{10}A_{11}$.

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

Úlohu lze řešit čistě metodami syntetické geometrie: označíme ještě S střed dvanáctiúhelníka 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 dopňkem výše zmíněných úhlů do 180°, tedy je rovna 105°. Hledaná odchylka je tedy 75°. □

1.40.13. *Najděte matice A takové, že*

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

Námět na přemýšlení: jaké geometrické zobrazení v rovině zadává matice A^2?

Řešení. A^2 je matice rotace o 60°, takže

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

tedy matice rotace o 30°, resp. 210°. □

K dalšímu procvičení nejen geometrických úvah mohou posloužit následující příklady:

1.41. Příklady.

1.41.1. Kružnice dělící rovinu. *Na kolik maximálně částí dělí rovinu k kružnic?*

Řešení. Pro maximální počet p_k oblastí, na které dělí rovinu kružnice odvodíme rekurentní vzorec

$$p_{k+1} = p_k + 2k$$

$(k+1)$. kružnice totiž protíná k předchozích maximálně v $2k$ průsečících (a tato situace skutečně může nastat). Navíc zřejmě $p_1 = 1$. Pro počet p_k tedy dostáváme

$$p_k = p_{k-1} + 2(k-1) = p_{k_2} + 2(k-2) + 2(k-1) = \cdots = p_1 + \sum_{i=1}^{k-1} 2i = 2 + (k-1)k.$$

□

1.41.2. *Na kolik maximálně částí dělí trojrozměrný prostor n koulí?*

Řešení. 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 $p_n = \frac{n}{3}(n^2 - 3n + 8)$. □

1.41.3. *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

$$x_n = n(n-1) + 2.$$

□

1.41.4. 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.

Řešení. Obdržíme například rozepsáním obou stran do souřadnic: $u = (u_1, u_2)$, $v = (v_1, v_2)$. Pak

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

□

1.42. Konstrukce lichoúhelníka.

1.42.1. *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 domácí úloha) Označíme-li vrcholy hledaného $(2n+1)$-úhelníka po řadě A_1, $A_2, \ldots, A_{2n+1}$ a středy stran (od středu A_1A_2) postupně S_1, $S_2, \ldots S_{2n+1}$, tak provedeme-li středové souměrnosti po řadě podle těchto středů, tak bod A_1 je zjevně pevným bodem výsledné středové symetrie, 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 získáme zobrazováním bodu A_1 ve středových souměrnostech podle $S_1, \ldots, S_{2n+1}$. □

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.

1.30

1.43. Relace mezi množinami. *Binární relací* mezi množinami A a B rozumíme 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

$$D \subset A, \quad D = \{a \in A; \exists b \in B, (a, b) \in R\}.$$

Podobně *oborem hodnot relace* je podmnožina

$$I \subset B, \quad I = \{b \in B; \exists a \in A, (a, b) \in R\}.$$

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 funcí zavedli. Píšeme

$$f : D \subset A \to I \subset B, f(a) = b$$

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*
- *injektivní zobrazení*, jestliže je $D = A$ a pro každé $b \in I$ existuje právě jeden *vzor* $a \in A$, $f(a) = b$.

Vyjádření zobrazení $f : A \to B$ jakožto relace

$$f \subset A \times B, \quad f = \{(a, f(a)); a \in A\}$$

známe také pod názvem *graf zobrazení f*.

1.31

1.44. Skládání relací a funkcí. U zobrazení je jasná koncepce, jak se skládají. Máme-li zobrazení $f : A \to B$ a $g : B \to C$, pak jejich *složení* $g \circ f$ je definováno

$$(g \circ f)(a) = g(f(a)).$$

Ve značení používaném pro relace totéž můžeme zapsat jako

$$\begin{aligned} f \subset A \times B, &\quad f = \{(a, f(a)); a \in A\} \\ g \subset B \times C, &\quad g = \{(b, g(b)); b \in B\} \\ g \circ f \subset A \times C, &\quad g \circ f = \{(a, g(f(a))); a \in A\}. \end{aligned}$$

Zcela obdobně definujeme *skládání relací*, v předchozích vztazích jen doplníme existenční kvantifikátory, tj. musíme uvažovat všechny „vzory“ a všechny „obrazy“.Uvažme relace $R \subset A \times B$, $S \subset B \times C$. Potom

$$S \circ R \subset A \times C, \quad S \circ R = \{(a, c); \exists b \in B, (a, b) \in R, (b, c) \in S\}.$$

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.

Pro každou relaci $R \subset A \times B$ 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 invezní 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 obrazení, u obecných relací tomu tak být nemusí.

1.32

1.45. Relace na množině. V případě $A = B$ hovoříme o relaci na množině A. Říkáme, že R je:

- *reflexivní*, pokud $\mathrm{id}_A \subset R$ (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 $R^{-1} \cap R \subset \mathrm{id}_A$ (tj. pokud $(a,b) \in R$ a zároveň $(b,a) \in R$, pak $a = b$),
- *tranzitivní*, pokud $R \circ R \subset R$, 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.

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 $A \to B$) a na ní relací $X \subset Z$ danou vlastností „být podmnožinou“. Evidentně jsou splněny všechny tři vlastnosti pro uspořádání: skutečně, je–li $X \subset Y$ a zároveň $Y \subset X$ musí být nutně množiny X a Y stejné. Je–li $X \subset Y \subset Z$ je také $X \subset Z$ a také reflexivita je zřejmá.

Říkáme, že uspořádání je *úplné*, když pro každé dva prvky 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 $X \subset Y$ ani $Y \subset X$.

Připomeňme rekurentní definici přirozených čísel $\mathbb{N} = \{0,1,2,3,\dots\}$, kde

$$0 = \emptyset, \quad n+1 = \{0,1,2,\dots,n\}.$$

Definujeme relaci $m < n$ právě, když $m \in n$. Evidentně jde o úplné úspořádání. Např. $2 \leq 4$, protože

$$2 = \{\emptyset, \{\emptyset\}\} \subset \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} = 4.$$

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.

1.33

1.46. Rozklad podle ekvivalence. Každá ekvivalence R na množině A zadává zároveň *rozklad* množiny A na podmnožiny vzájemně ekvivalentních prvků, tzv. *třídy ekvivalance*. Klademe pro libovolné $a \in A$

$$R_a = \{b \in A; (a,b) \in A\}.$$

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 podmnožina 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 suktečně rozloží na jednotlivé třídy.

Můžeme také třídám rozkladu rozumět tak, že třídu $[a]$ vnímáme jako prvek a „až na ekvivalenci“.

1.34

1.47. Příklad – 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.

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:

$$(a,b) \sim (a',b') \quad \Longleftrightarrow \quad a-b = a'-b' \quad \Longleftrightarrow \quad a+b' = a'+b.$$

Všimněme si, že zatímco výrazy v prostřední rovnosti v přirozených číslech neumíme, výrazy v pravo 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.

$$[(a,b)] + [(c,d)] = [(a+c, b+d)],$$

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 přklad 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 1.1 a 1.2. Pro násobení je neutrálním prvkem jednička, ale pro všechna čísla a různá od nuly a jedničky neumíme najít číslo a^{-1} s vlastností $a\cdot a^{-1} = 1$, tzn. chybí nám inverzní prvky. Zároveň si povšimněte, že platí vlastnost oboru integrity (OI), viz 1.2, 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 $\mathbb{N}$. Na množině uspořádaných dvojic (p,q), $q \neq 0$, celých čísel definujeme relaci $\sim$ tak, jak očekáváme, že se mají chovat podíly p/q:

$$(p,q) \sim (p',q') \quad \Longleftrightarrow \quad p/q = p'/q' \quad \Longleftrightarrow \quad p\cdot q' - p'\cdot q.$$

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.

1.48. Příklad – zbytkové třídy. Jiným dobrým a jednoduchým příkladem jsou tzv. zbytkové třídy celých čísel. Pro pevně zvolené přirozené číslo k definujeme equivalenci $\sim_k$ 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 definovat násobení a sčítání. Zkuste si ověřit, že výsledná množina „skalárů“ je komutativním tělesem (tj. splňuje i vlastnost (P) z 1.2) právě když je k prvočíslo.

Závěrem si ještě procvičme spolu s relacemi ještě i kombinatoriku:

1.49. Ekvivalence ano či ne.

1.49.1. *Rozhodněte, zda následující relace na množině M jsou relace ekvivalence:*

(1) $M = \{f : \mathbb{R} \to \mathbb{R}\}$, $(f \sim g) \iff f(0) = g(0)$.
(2) $M = \{f : \mathbb{R} \to \mathbb{R}\}$, $(f \sim g) \iff f(0) = g(1)$.
(3) *M je množina přímek v rovině, dvě přímky jsou v relaci, jestliže se neprotínají.*
(4) *M je množina přímek v rovině, dvě přímky jsou v relaci, jestliže jsou rovnoběžné.*
(5) $M = \mathbb{N}$, $(m \sim n) \iff S(m) + S(n) = 20$, *kde $S(n)$ značí ciferný součet čísla n.*

Řešení.

(1) Ano. Ověříme tři vlastnosti ekvivalence:
  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 $f(0) = h(0)$.
(2) Ne. Definovaná relace není reflexivní, např pro funkci sin máme $\sin(0) \neq \sin(1)$
(3) Ne. Relace opět není reflexivní (každá přímka protíná sama sebe)
(4) Ano. Třídy ekvivalence pak tvoří množinu neorientovaných směrů v rovině.
(5) Ne. Relace není reflexivní. $S(1) + S(1) = 2$.

□

1.49.2. *Počet injektivních zobrazení mezi množinami*
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 $v(3, 4) = 4 \cdot 3 \cdot 2 = 24$. □

1.49.3. *Počet surjektivních zobrazení mezi danými množinami*
Určete počet surjektivních zobrazení množiny $\{1, 2, 3, 4\}$ na množinu $\{1, 2, 3\}$

Řešení. Počet zjistíme obecným principem „inkluze a exkluze“. Od počtu všech zobrazení odečteme ta, která nejsou surjektivní, t.j. ta, jejichž obor hodnot je buď jednoprvkovou nebo dvouprvkovou množinou. 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 $\binom{3}{2}(2^4 - 2)$ ($\binom{3}{2}$ způsoby můžeme vybrat definiční obor 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

$$3^4 - \binom{3}{2}(2^4 - 2) - 3 = 36. \tag{1.30}$$

□

1.49.4. *Počet relací ekvivalence na množině*
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. □

Závěrem ještě jeden příklad ukazující, že „divné“ skaláry se chovají divně:

1.49.5. *Nenulový mnohočlen s nulovými hodnotami*
Najděte nenulový mnohočlen 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 livovolné prvočíslo p a číslo a s ním nesoudělné platí:

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p). \tag{1.31}$$

Hledaný polynom je tedy například polynom $x^7 - x$ (polynom $x^6 - 1$ by neměl nulovou hodnotu v čísle 0). □

KAPITOLA 2

Elementární lineární algebra

neumíte ještě počítat se skaláry?
– zkusme to rovnou s maticemi...

1. Vektory a matice

2.1

2.1. Vektory nad skaláry. Symbolem $\mathbb{K}$ budeme nadále značit nějakou množinu skalárů. Prozatím budeme *vektorem* rozumět uspořádanou n-tici skalárů, kde pevně zvolené $n \in \mathbb{N}$ budeme nazývat *dimenzí*. Sčítání vektorů definujeme po složkách (skaláry samozřejmě sčítat umíme) a násobení vektoru $u = (a_1, \dots, a_n)$ skalárem b definujeme tak, že každý prvek n-tice u vynásobíme skalárem b (skaláry v $\mathbb{K}$ násobit umíme), tj.

$$u + v = (a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$
$$b \cdot u = b \cdot (a_1, \dots, a_n) = (b \cdot a_1, \dots, b \cdot a_n).$$

Zpravidla požadujeme, aby skaláry byly z nějakého pole[1], viz 1.1.

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 pro nulový prvek stejný symbol jako pro nulový prvek skalárů. Podobně budeme pro sčítání a násobení používat stále stejný symbol (plus a buď tečku nebo prosté zřetězení znaků). Navíc nebudeme 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 proměných, komponent a v součtech).

Pro všechny vektory v, $w \in \mathbb{K}^n$ a skaláry a, $b \in \mathbb{K}$ platí

(V1) $$a \cdot (v + w) = a \cdot v + a \cdot w$$

(V2) $$(a + b) \cdot v = a \cdot v + b \cdot v$$

(V3) $$a \cdot (b \cdot v) = (a \cdot b) \cdot v$$

(V4) $$1 \cdot v = v$$

Pro kterékoliv pole skalárů $\mathbb{K}$ se snadno ověří právě sformulované vlastnosti (V1)–(V4) pro $\mathbb{K}^n$, protože při ověřování vždy používáme pouze vlastnosti skalárů uvedené v 1.1 a 1.2. Budeme takto pracovat např. s $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{C}^n$, $(\mathbb{Z}_k)^n$, $n = 1, 2, 3, \dots$.

[1] Čtenář, který se ještě nesmířil s abstrakcí okruhů a polí, nechť přemýšlí v rámci číselných oborů. Potom okruhy skalárů zahrnují i celá čísla $\mathbb{Z}$ a všechny zbytkové třídy, zatímco mezi poli jsou pouze $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ a zbytkové třídy $\mathbb{Z}_k$ s prvočíselným k.

Všimněme si také, že k ověření vlastností (V1)–(V4) potřebujeme pro použité skaláry pouze vlastnosti okruhu. Vlastnost (P) však bude přesto podstatná později.

2.2

2.2. Matice nad skaláry. Maticí typu m/n nad skaláry $\mathbb{K}$ rozumíme obdélníkové schéma

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

kde $a_{ij} \in \mathbb{K}$ pro všechny $1 \leq i \leq m,\ 1 \leq j \leq n$. Matici A s prvky a_{ij} značíme také $A = (a_{ij})$.

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 $A : \{1, \dots, m\} \times \{1, \dots, n\} \to \mathbb{K}$. Matice typu $1/n$ nebo $n/1$ jsou vlastně právě vektory v $\mathbb{K}^n$. I obecné matice lze však chápat jako vektory v $\mathbb{K}^{m \cdot n}$, prostě zapomeneme na řádkování. Zejména tedy je definováno sčítání matic a násobení matic skaláry:

$$A + B = (a_{ij} + b_{ij}),$$

kde $A = (a_{ij})$, $B = (b_{ij})$,

$$a \cdot A = (a.a_{ij}),$$

kde $A = (a_{ij})$, $a \in \mathbb{K}$. Dále pak 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:

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

2.3. Příklad. Matice lze vhodně využít pro zápis lineárních rovnic. Uvažme následující systém m rovnic v n proměnných:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= y_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= y_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= y_m. \end{aligned}$$

Posloupnost $x_1, \dots, x_n$ lze chápat jako vektor proměnných, tj. sloupec v matici typu $n/1$, a podobně s hodnotami $y_1, \dots, y_n$. Systém rovnic lze pak formálně psát ve tvaru $A \cdot x = y$:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Původní rovnice nyní obdržíme tak, že vždy bereme řádky z A a sčítáme součiny odpovídajících komponent, tj. $a_{i1}x_1+\cdots+a_{in}x_n$. Tím získáme i-tý prvek výsledného vektoru.

V rovině, tj. pro vektory dimenze 2, jsme už zavedli takovýto počet a viděli jsme, že s ním lze pracovat velice efektivně (viz 1.35). Nyní budeme postupovat obecněji a zavedeme i na maticích operace násobení.

2.4

2.4. Součin matic. Pro libovolnou matici $A = (a_{ij})$ typu m/n nad okruhem skalárů $\mathbb{K}$ a libovolnou matici $B = (b_{jk})$ typu n/q nad $\mathbb{K}$ definujeme jejich součin $C = A \cdot B = (c_{ik})$ jako matici typu m/q s prvky

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}, \text{ pro libovolné } 1 \leq i \leq m,\ 1 \leq k \leq q.$$

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

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*. Na množině čtvercových matic nad $\mathbb{K}$ dimenze n je součin matic definován pro každé dvě matice, je tam tedy definována operace násobení:

Tvrzení. *Pro libovolný okruh skalárů je na množině všech čtvercových matic dimenze n definována operace násobení. Splňuje vlastnosti 1.2(O1) a (O3) vzhledem k jednotkové matici $E = (\delta_{ij})$. Dále spolu se sčítáním matic vyhovuje 1.2(O4). Obecně však neplatí 1.2(O2) ani (OI), zejména tedy neplatí 1.2(P).*

Důkaz. Asociativita násobení – (O1): Protože skaláry jsou asociativní, distributivní i komutativní, můžeme spočíst

$$A = (a_{ij}) \text{ typu } m/n, \quad B = (b_{jk}) \text{ typu } n/p, \quad C = (c_{kl}) \text{ typu } p/q$$

$$A \cdot B = (\sum_j a_{ij}.b_{jk}), \quad B \cdot C = (\sum_k b_{jk}.c_{kl})$$

$$(A \cdot B) \cdot C = (\sum_k (\sum_j a_{ij}.b_{jk}).c_{kl}) = \sum_{j,k} a_{ij}.b_{jk}.c_{kl}$$

$$A \cdot (B \cdot C) = (\sum_j a_{ij}.(\sum_k b_{jk}.c_{kl})) = \sum_{j,k} a_{ij}.b_{jk}.c_{kl}$$

Jednotkový prvek – (O3):

$$A \cdot E = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \\ 0 & 0 & \cdots & 1 \end{pmatrix} = A = E \cdot A$$

(O4) - distributivita: 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

$$A \cdot (B + C) = (\sum_j a_{ij}(b_{jk} + c_{jk}) = ((\sum_j a_{ij}b_{jk}) + (\sum_j a_{ij}c_{jk})) = A \cdot B + A \cdot C$$

$$(B + C) \cdot D = (\sum_k (b_{jk} + c_{jk})d_{kl}) = ((\sum_k b_{jk}d_{kl}) + (\sum_k c_{jk}d_{kl})) = B \cdot D + C \cdot D$$

Není komutativní: - jak jsme již viděli v 1.35, 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 a 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!) □

V důkazu jsme vlastně pracovali s maticemi obecnějšího typu, dokázali jsme tedy příslušné vlastnosti obecněji:

Tvrzení. *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 tato násobení definována. Jednotková matice je neutrálním prvkem pro násobení zleva i zprava.*

2.6

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 měli umět s maticemi, máme ale problém, jak poznat, zda taková 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 je samozřejmé, že obě matice musí mít tutéž dimenzi n. Matici, k níž existuje matice inverzní, říkáme *invertibilní matice*.

Pokud A^{-1} a B^{-1} existují, pak existuje i $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$. Je totiž (díky právě dokázané asociativitě násobení) $(B^{-1} \cdot A^{-1}) \cdot (A.B) = B^{-1} \cdot (A^{-1} \cdot A) \cdot B = E$ a $(A \cdot B) \cdot (B^{-1} \cdot A^{-1}) = A \cdot (B \cdot B^{-1}) \cdot A^{-1} = E$.

Protože s maticemi umíme počítat zrovna jako se skaláry, jen mají složitější chování, můžeme formálně snadno řešit systémy lineárních rovnic: Jestliže vyjádříme soustavu n rovnic pro n neznámých součinem matic

$$A \cdot x = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$$

a existuje matice inverzní k matici A, pak lze násobit zleva A^{-1} a dostaneme $A^{-1} \cdot y = A^{-1} \cdot A \cdot x = E \cdot x = x$, tj. 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.

2.7

2.7. Ekvivalentní úpravy matic. Z hlediska řešení systémů rovnic

$$A \cdot x = b$$

je jistě přirozené považovat za ekvivalentní matice A a vektory b, které zadávají systémy rovnic se stejným řešením. Uvedeme si jednoduché manipulace s řádky rovnic a stejným způsobem pak můžeme upravovat i vektor napravo. Když se nám podaří vlevo dostat systém s jednotkovou maticí, bude napravo řešení původního systému. Takovým operacím říkáme *řádkové elementární transformace*. Jsou to:

- záměna dvou řádků
- vynásobení vybraného řádku nenulovým skalárem
- přičtení řádku k jinému řádku.

Je zjevné, že odpovídající operace na úrovni rovnic v systému nemohou změnit množinu všech jeho řešení. Později bude vidět, že sloupcové transformace odpovídají řešení téhož systému ale v transformovaných souřadnicích

Analogicky, *sloupcové elementární 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 algoritmiclký a většinou se mu říká *Gausova 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 $a_{ij} = 0$ a všechny předchozí prvky na i-tém řádku jsou také nulové, 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

$$\begin{pmatrix} 0 & \dots & 0 & a_{1j} & \dots & \dots & \dots & a_{1m} \\ 0 & \dots & 0 & 0 & \dots & a_{2k} & \dots & a_{2m} \\ \vdots & & & & & & & \\ 0 & \dots & \dots & \dots & \dots & 0 & a_{lp} & \dots \\ \vdots & & & & & & & \end{pmatrix}$$

a matice může, ale nemusí, končit několika nulovými řádky. K převodu libovolné matice můžeme použít jednoduchý algoritmus:

(1) Záměnou řádků docílíme, že v prvním řádku bude v prvním nenulovém sloupci nenulový prvek, nechť je to j-tý sloupec.
(2) Pro $i = 2, \dots$, 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 zbytek řádků a sloupců v získané matici dospějeme po konečném počtu kroků k požadovanému tvaru.

□

Uvedený postup je skutečně právě obvyklá eliminace proměnných v systémech lineárních rovnic. Pro řešení systémů rovnic má ale uvedený postup rozumný smysl jen, když mezi skaláry neexistují dělitelé nuly. Pokud tvoří skaláry pole, pak můžeme navíc ze schodovitého tvaru snadno spočíst řešení (případně ověřit jeho neexistenci), promyslete si pečlivě rozdíl mezi $\mathbb{K} = \mathbb{Z}$, $\mathbb{K} = \mathbb{R}$ a případně $\mathbb{Z}_2$ nebo $\mathbb{Z}_3$.

2.8 **2.8. Poznámka.** 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)

$$\begin{pmatrix} 1 & 0 & \dots & & & & \\ 0 & \ddots & & & & & \\ \vdots & & 0 & \dots & 1 & & \\ & & \vdots & \ddots & \vdots & & \\ & & 1 & \dots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

(2) Vynásobení i-tého řádku (resp. sloupce) skalárem a:

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \leftarrow i$$

(3) Sečtení i-tého řádku (resp. sloupce) s j-tým:

$$i \rightarrow \begin{pmatrix} 1 & 0 & & & & & \\ 0 & \ddots & & & & & \\ & & \ddots & & & & \\ & & & \ddots & & & \\ & & 1 & & \ddots & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$
$$\uparrow$$
$$j$$

Toto prostinké pozorování je ve skutečnosti velice podstatné, protože součin invertibilních matic je invertibilní a všechny elementární transformace jsou nad polem skalárů invertibilní. Pro libovolnou matici A tedy dostaneme násobením vhodnou invertibilní maticí $P = P_k \cdots P_1$ zleva (postupné násobení k maticemi zleva) její ekvivalentní řádkový schodovitý tvar $A' = P \cdot A$.

Jestliže obecně aplikujeme tentýž eliminační postup na sloupce, dostaneme z každé matice B její sloucový schodovitý tvar B' vynásobením vhodnou invertibilní maticí $Q = Q_1 \cdots Q_\ell$. Pokud ale začneme s maticí $B = A'$ v řádkově schodovitém

tvaru, eliminuje takový postup pouze všechny dosud nenulové prvky mimo diagonálu matice a závěrem lze ještě i tyto elementárními operacemi změnit na jedničky. Celkem jsme tedy ověřili důležitý výsledek, ke kterému se budeme mnohokrát vracet:

2.9

2.9. Věta. *Pro každou matici A typu m/n nad polem skalárů $\mathbb{K}$ existují čtvercové invertibilní matice P dimenze m a Q dimenze n takové, že matice $P \cdot A$ je v řádkově schodovitém tvaru a*

$$P \cdot A \cdot Q = \begin{pmatrix} 1 & \dots & 0 & \dots & \dots & \dots & 0 \\ \vdots & \ddots & & & & & \\ 0 & \dots & 1 & 0 & \dots & \dots & 0 \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \end{pmatrix}.$$

2.10

2.10. Algoritmus pro výpočet inverzní matice. V předchozích úvahách jsme se dostali prakticky k úplnému algoritmu pro výpočet inverzní matice. Během jednoduchého níže uvedeného postupu buď zjistíme, že inverze neexistuje, nebo bude inverze spočtena. I nadále pracujeme nad polem skalárů.

Ekvivalentní řádkové transformace se čtvercovou maticí A dimenze n vedou k matici P' takové, že $P' \cdot A$ bude v řádkově schodovitém tvaru. Přitom může (ale nemusí) být jeden nebo více posledních řádků nulových. Jestliže má existovat inverzní matice k A, pak existuje i inverzní matice k $P' \cdot A$. Jestliže však je poslední řádek v $P \cdot A$ nulový, bude nulový i poslední řádek v $P \cdot A \cdot B$ pro jakoukoliv matici B dimenze n. Existence takového nulového řádku 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 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 A.

Prakticky tedy můžeme postupovat tak, že 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 $\mathbb{K}$. Tytéž úpravy postupně prováděné s E vedou právě k matici $P = P'' \cdot P'$ z předchozích úvah, tedy z ní získáme právě hledanou inverzi. Pokud tento algoritmus narazí na vynulování celého řádku v původní matici, znamená to, že matice inverzní neexistuje.

2.10a

2.11. Závislost řádků a sloupců a hodnost matice. 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 2.23, bude ale užitečné pochopit podstatu už nyní. Lineární kombinací řádků (nebo sloupců)

matice $A = (a_{ij})$ typu m/n rozumíme výraz $a_1 u_{i_1} + \cdots + a_k u_{i_k}$, kde a_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 *lineárně závislé*. V opačném případě, tj. když jedinou možnost jak získat nulový řádek je vynásobení výhradně nulovými skaláry, jsou *lineárně nezávislé*. Obdobně definujeme lineárně závislé a nezávislé sloupce matice.

Předchozí výsledky o Gausově eliminaci můžeme vnímat takovým způsobem, že počet výsledných nenulových „schodů“ v řádkově nebo sloupcově schodovitém tvaru je vždy roven témuž přirozenému číslu a to počtu lineárně nezávislých řádků matice a témuž počtu lineárně nezávislých sloupců matice. Tomuto číslu říkáme *hodnost matice*, značíme $h(A)$. Zapamatujme si výsledné tvrzení:

Věta. *Nechť A je matice typu m/n nad polem skalárů $\mathbb{K}$. Matice A má stejný počet $h(A)$ lináně nezávislých řádků a lineárně nezávislých sloupců. Zejména je hodnost vždy nejvýše rovna menšímu z rozměrů matice A.*

Algoristmus pro výpočet inverzních matic také říká, že čtvercová matice A dimenze m má inverzi právě, když je její hodnost rovna počtu řádků m.

Ukažme si ještě užití matic pro běžné geometrické transformace, podobně jako v našich úvahách o geometrii roviny (viz 1.36):

2.12. Matice rotací podle souřadnicových os.

2.12.1. *Napište matici zobrazení rotací o úhel φ postupně kolem 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 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 musíme dávat pozor na znaménko. Je totiž rotace kolem osy y v kladném smyslu, tedy taková rotace, že pokud se díváme proti směru osy y, tak se svět točí proti směru hodinových ručiček, je rotací 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. □

2.13. Matice rotace kolem dané osy.

2.13.1. *Napište matici zobrazení rotace v kladném smyslu o úhel* $60°$ *kolem přímky dané počátkem a vektorem* $(1,1,0)$ *v* $\mathbb{R}^3$.

Řešení. Daná otáčení je složením následujících tří zobrazení:

- rotace o $45°$ v záporném smyslu podle osy z (osa rotace $(1,1,0)$ přejde do osy x)
- rotace o $60°$ v kladném smyslu podle osy x.
- rotace o $45°$ v kladném smyslu podle osy z (osa x přejde zpět na osu danou vektorem $(1,1,0)$).

Matice výsledné rotace tedy bude součinem matic odpovídajících těmto třem zobrazením, přičemž pořadí matic je dáno pořadím provádění jednotlivých zobrazení, prvnímu zobrazení odpovídá v součinu matice nejvíce napravo. Celkem tedy dostáváme pro hledanou matici A vztah:

$$A = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} & \frac{\sqrt{6}}{4} \\ \frac{1}{4} & \frac{3}{4} & -\frac{\sqrt{6}}{4} \\ -\frac{\sqrt{6}}{4} & \frac{\sqrt{6}}{4} & \frac{1}{2} \end{pmatrix}$$

□

2. Determinanty

V páté části první kapitoly jsme viděli, že pro čtvercové matice dimenze n 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 1.35 a formule (1.26). Determinant byl užitečný i jinak, viz 1.37 a 1.38, kde jsme si volnou úvahou odvodili, že obsah rovnoběžníka 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.

2.10c

2.14. Definice determinantu.

Připomeňme, že bijektivní zobrazení množiny X na sebe se nazývá *permutace množiny* X, viz 1.5. Je-li $X = \{1, 2, \dots, n\}$, lze permutace zapsat pomocí výsledného pořadí ve formě tabulky:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Prvek $x \in X$ se nazývá samodružným bodem permutace σ, je-li $\sigma(x) = x$. Permutace σ taková, že existují právě dva různé prvky $x, y \in X$ s $\sigma(x) = y$ a $\sigma(z) = z$ pro všechna ostatní $z \in X$ se nazývá *transpozice*, značíme ji (x, y).

V dimenzi dva 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 sečteme:

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

Obecně, nechť $A = (a_{ij})$ je čtvercová matice dimenze n nad $\mathbb{K}$. *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 Σ_n je množina všech možných permutací na $\{1, \ldots, n\}$ a znaménko sgn pro každou permutaci 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* $|A|$.

Jednoduché příklady už umíme: je-li $n = 1$, pak $|a_{11}| = a_{11} \in \mathbb{K}$, a pro $n = 2$ je

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = +a_{11}a_{22} - a_{12}a_{21}.$$

Podobně pro $n = 3$ se dá uhodnout (chceme linearitu v každém sloupci a antisymetrii)

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = + a_{11}a_{22}a_{33} - a_{13}a_{22}a_{31} + a_{13}a_{21}a_{32} \\ - a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} - a_{12}a_{21}a_{33}.$$

Tomuto vzorci se říká *Saarusovo pravidlo*.

Jak tedy najít správná znaménka? Říkáme, že dvojice prvků $a, b \in X = \{1, \ldots, n\}$ tvoří *inverzi v permutaci* σ, je-li $a < b$ a $\sigma(a) > \sigma(b)$. Permutace σ se nazývá *sudá* (resp. *lichá*), obsahuje-li sudý (resp. lichý) počet inverzí.

Parita permutace σ je $(-1)^{\text{počet inverzí}}$ a značíme ji právě $\operatorname{sgn}(\sigma)$. Tolik definice, chceme ale vědět, jak s paritou počítat. Z následujícího tvrzení už je jasně vidět, že Saarusovo pravidlo skutečně počítá determinant v dimenzi 3.

Tvrzení. *Na množině $X = \{1, 2, \ldots, n\}$ je právě $n!$ různých permutací. Tyto lze seřadit do posloupnosti tak, že každé dvě po sobě jdoucí se liší právě jednou transpozicí. Lze při tom začít libovolnou permutací a 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 $n!$ zaručeně různých permutací, tzn. všechny, právě předepsaným způsobem. Všimněte si, že důležitou částí postupu je možnost začít s libovolnou z permutací.

Zbývá poslední dovětek o paritách. Uvažme pořadí $(a_1, \ldots, a_i, a_{i+1}, \ldots, n)$, ve kterém je r inverzí. Pak zjevně je v pořadí $(a_1, \ldots, a_{i+1}, a_i \ldots, n)$ 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. □

Zjistili jsme, že provedení libovolné transpozice změní paritu permutace a že každé pořadí čísel $\{1, 2, \dots, n\}$ lze získat postupnými transpozicemi sousedních prvků. Důsledkem tohoto popisu je, že na každé množině $X = \{1, \dots, n\}$, $n > 1$, 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

$$\operatorname{sgn}(\sigma \circ \eta) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\eta), \quad \operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma).$$

2.15. Rozklad permutace na transpozice.

2.15.1. *Napište permutaci*

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

jako složení transpozicí. Je tato permutace sudá nebo lichá?

Řešení. Transpozici prvků i a j, budeme značit jako (i, j). Danou permutaci můžeme rozložit nejprve na nezávislé cykly, ty potom na transpozice. V našem případě je daná transpozice složením dvou cyklů: $(1, 2, 3)$ a $(4, 5)$ (rozklad dostaneme tak, že si vybereme jeden prvek a ten opakovaně zobrazujeme pomocí dané permutace, dokud nedostaneme na počátku zvolený prvek; „cesta“ prvku tvoří cyklus; z prvků, které jsme ještě neprošli vybereme opět další a opět ho opakovaně zobrazujeme pomocí dané permutace; opakujeme tak dlouho, dokud neprobereme všechny prvky množiny, na které permutace působí). V našem případě se prvek 1 zobrazuje na 3, prvek 3 na prvek 2, prvek 2 zpět na 1, dostáváme tedy cyklus $(1, 3, 2)$. První prvek, který jsme ještě neprošli je číslo 4: 4 se zobrazuje na 5, 5 zpět na 4; dostáváme transpozici, neboli cyklus délky dva. Máme tedy

$$P = (1, 3, 2) \circ (4, 5).$$

Cyklus $(1, 3, 2)$ ještě rozložíme na transpozice: $(1, 3, 2) = (1, 3) \circ (3, 2)$. Celkem tedy

$$P = (1, 3) \circ (3, 2) \circ (4, 5).$$

Parita počtu transpozicí v rozkladu je dána jednoznačně a udává sudost či lichost permutace. Naše permutace je tedy lichá. □

2.12

2.16. Jednoduché vlastnosti determinantu. Pro každou matici $A = (a_{ij})$ typu m/n na skaláry z $\mathbb{K}$ definujeme *matici transponovanou* k A. Jde o matici $A^T = (a'_{ij})$ s prvky $a'_{ij} = a_{ji}$ typu n/m.

Čtvercová matice A s vlastností $A = A^T$ se nazývá *symetrická*. Jestliže platí $A = -A^T$, pak se A nazývá antisymetrická.

Věta. *Pro každou čtvercovou matici A platí*

(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 $|A| = -|B|$,*
(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 odpovídá člen

$$\operatorname{sgn}(\sigma)a_{\sigma(1)1} \cdot a_{\sigma(2)2} \cdots a_{\sigma(n)n} = \operatorname{sgn}(\sigma)a_{1\sigma^{-1}(1)} \cdot a_{2\sigma^{-1}(2)} \cdots a_{n\sigma^{-1}(n)},$$

přičemž musíme ověřit, že je tento člen opatřen správným znaménkem. Parita σ a σ^{-1} je ale stejná, jde tedy opravdu o člen $|A^T|$ a první tvrzení je dokázáno.

(2) Plyne přímo z definice determinantu, protože všechny jeho členy budou nulové.

(3) Ve všech členech $|A|$ dojde 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 zmněnila hodnota determinantu. Vzhledem k tvrzení (4) lze ale přičíst i skalární násobek libovolného jiného řádku. □

2.13 **2.17. Poznámka.** Všimněme si 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.

Vlastnosti (3)–(5) říkají, že determinant jako zobrazení, které n vektorům dimenze n (řádkům nebo sloupcům matice) přiřadí skalár je antisymetrické zobrazení lineární v každém svém argumentu, přesně jak jsme podle analogie z dimenze 2 požadovali.

Pro matici v řádkovém nebo sloupcovém schodovitém tvaru je jediným nenulovým členem determinantu ten, který odpovídá identické permutaci. Vidíme tedy, že determinant takové matice 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. 2.7.

2.14 **2.18. Další vlastnosti determinantu.** Časem uvidíme, že skutečně stejně jako v dimenzi dva je determinant matice roven orientovanému objemu rovnoběžnostěnu určeného jejími sloupci. Uvidíme časem 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*:

Věta. *Nechť $A = (a_{ij})$, $B = (b_{ij})$ jsou čtvercové matice dimenze n nad okruhem skalárů $\mathbb{K}$. Pak $|A \cdot B| = |A| \cdot |B|$.*

My tuto větu odvodíme ryze algebraicky už proto, že předchozí odvolávka na geometrický argument těžko může fungovat pro jakékoliv skaláry. Základním nástrojem je tzv. *rozvoj determinantu* podle jednoho nebo více řádků či sloupců. Budeme potřebovat něco málo technické přípravy. Čtenář, který by snad tolik abstrakce neztrávil může tyto pasáže přeskočit a vstřebat pouze znění Laplaceovy věty a jejich důsledků.

Nechť $A = (a_{ij})$ je matice typu m/n a $1 \leq i_1 < \ldots < i_k \leq m$, $1 \leq j_1 < \ldots < j_l \leq n$ jsou pevně zvolená přirozená čísla. Pak matici

$$M = \begin{pmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \ldots & a_{i_1 j_\ell} \\ \vdots & & & \vdots \\ a_{i_k j_1} & a_{i_k j_2} & \ldots & a_{i_k j_\ell} \end{pmatrix}$$

typu k/ℓ 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 *hlavní submatice*, jejich determinanty *hlavní minory* matice A. Při speciální volbě $k = \ell = 1,\ m = n$ hovoříme o *algebraickém doplňku* A_{ij} prvku a_{ij} matice A.

Pokud je $|M|$ hlavní minor matice A, pak přímo z definice determinantu je vidět, že součin $|M|$ s jeho algebraickým doplňkem je členem determinantu.

Nechť je obecná submatice M určena 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 $(j_1 - 1) + \cdots + (j_k - k)$ výměn sousedních sloupců v A převedeme 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 2.16 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. *Nechť A je 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 $|A|$.*

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, přitom lze pro každý z členů zvolit matici A takovou, že pouze tento člen bude nenulový.

Ukážeme si, že uvažované součiny $|M| \cdot |M^*|$ obsahují právě $n!$ různých členů z $|A|$, bude tvrzení věty dokázáno. Ze zvolených k řádků lze vybrat $\binom{n}{k}$ minorů M a podle předchozího lematu 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 jme bezezbytku dokázali tzv. *Laplaceovu větu*:

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.*

2.15

2.19. Důsledky Laplaceovy věty. Předchozí 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 i-tého sloupce:

$$|A| = \sum_{j=1}^{n} a_{ij} A_{ij} = \sum_{j=1}^{n} a_{ji} A_{ji}$$

kde A_{ij} označuje algebraický doplněk k prvku (minoru stupně 1) a_{ij}. Při praktickém počítání determinantů bývá výhodné kombinovat Laplaceův rozvoj s přímou metodou přičítání lineárních kombinací řádků či sloupců.

2.20. Příklady.

2.20.1. *Spočítejte determinant matice*

$$\begin{pmatrix} 1 & 3 & 5 & 6 \\ 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

Řešení. Začneme rozvíjet podle prvního sloupce, kde máme nejvíce (jednu) nul. Postupně dostáváme

$$\begin{vmatrix} 1 & 3 & 5 & 6 \\ 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 2 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{vmatrix} - 1 \cdot \begin{vmatrix} 3 & 5 & 6 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{vmatrix} + 1 \cdot \begin{vmatrix} 3 & 5 & 6 \\ 2 & 2 & 2 \\ 1 & 2 & 1 \end{vmatrix}$$

$$\overset{\text{Podle Saarusova pravidla}}{=} -2 - 2 + 6 = 2.$$

□

2.20.2. *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:

$$D = -a \cdot a \begin{vmatrix} 1 & 1 \\ a & 1 \end{vmatrix} = -a^2(a^2 - 1)$$

Celkem dostáváme následující podmínku pro a: $a^4 - a^2 + 1 = 0$. Substitucí $t = a^2$, pak máme $t^2 - t + 1$ s kořeny $t_1 = \frac{1+i\sqrt{3}}{2} = \cos(\pi/3) + i\sin(\pi/3)$, $t_1 = \frac{1-i\sqrt{3}}{2} = \cos(\pi/3) - i\sin(\pi/3) = \cos(-\pi/3) + i\sin(-\pi/3)$, odkud snadno určíme čtyři možné hodnoty parametru a: $\cos(\pi/6)+i\sin(\pi/6) = \sqrt{3}/2+i/2$, $\cos(7\pi/6)+i\sin(7\pi/6) = -\sqrt{3}/2 - i/2$, $\cos(-\pi/6) + i\sin(-\pi/6) = \sqrt{3}/2 - i/2$, $\cos(5\pi/6) + i\sin(5\pi/6) = -\sqrt{3}/2 + i/2$. □

Výpočet determinantů bude standardním krokem v mnoha dalších úlohách, proto ponecháme i procvičování na tyto praktičtější příležitosti.

2.21. Důkaz Cauchyovy věty. Jde o trikovou ale elementární aplikaci Laplaceovy věty. Použijeme prostě dvakrát Laplaceův rozvoj na vhodné matice:

Uvažme nejprve matici H dimenze $2n$ (používáme tzv. blokovou symboliku, tj. píšeme matici jakoby složenou z matic)

$$H = \begin{pmatrix} A & 0 \\ -E & B \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} & 0 & \dots & 0 \\ -1 & & 0 & b_{11} & \dots & b_{1n} \\ & \ddots & & \vdots & & \vdots \\ 0 & & -1 & b_{n1} & \dots & b_{nn} \end{pmatrix}$$

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 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

$$|K| = (-1)^{n+1+\cdots+2n}|A \cdot B| = (-1)^{2n\cdot(n+1)} \cdot |A \cdot B| = |A \cdot B|.$$

2.16

2.22. 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 platí $|A|^{-1} = |A^{-1}|$.

My však kombinací Laplaceovy věty a Cauchyho věty umíme víc. 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. Nazýváme ji *algebraicky adjungovaná matice* k matici A.

Věta. *Pro každou čtvercovou matici A nad okruhem skalárů $\mathbb{K}$ platí*

$$AA^* = A^*A = |A| \cdot E.$$

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 $|A| \in \mathbb{K}$. Předpokládejme naopak, že $|A|$ je invertibilní skalár. Spočteme přímým výpočtem $A \cdot A^* = (c_{ij})$:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} a^*_{kj} = \sum_{k=1}^{n} a_{ik} A_{jk}.$$

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 $A \cdot A^* = |A| \cdot E$, ale již v 2.10 jsme odvodili, že z rovnosti $A \cdot B = E$ plyne i $B \cdot A = E$. (Pokud tomu někdo dá přednost, může zopakovat předešlý výpočet pro $A^* \cdot A$.) □

3. Vektorové prostory a lineární zobrazení

Vraťme se teď na chvilku k systémům m lineárních rovnic pro n proměnných z 2.3 a předpokládejme navíc, že jde o rovnice tvaru $A \cdot x = 0$, 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 okamžitě 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 „dimenze“ tohoto prostoru určitě nemá být n (pokud matice systému není nulová). Případy dvou rovnic pro dvě neznámé jsme potkali při řešení geometrických problémů v rovině v 1.34 a pro dvě závislé rovnice byl množinou všech řešení „jednorozměrný“ prostor – přímka. U dvou nezávislých rovnic to byl průsečík dvou přímek, tj. „nularozměrný“ prostor.

Už v 1.16, jsme ale potkali ještě zajímavější příklad prostoru všech řešení homogenní lineární diferenční rovnice (druhého řádu). Opět jsme dvě řešení mohli libovolně kombinovat pomocí sčítání a násobení skaláry a dostali jsme tak všechna možná řešení. Tyto „vektory“ ovšem jsou nekonečné posloupnosti čísel, přestože intuitivně očekáváme, že dimenze celého prostoru řešení by měla být dvě.

Potřebujeme proto obecnější definici vektorového prostoru a jeho dimenze:

2.17

2.23. Abstraktní vektorové prostory. *Vektorovým prostorem V* nad polem skalárů $\mathbb{K}$ rozumíme množinu spolu s operací sčítání, pro kterou platí axiomy 1.1(KG1)–(KG4), a s násobením skaláry, pro které platí axiomy 2.1(V1)–(V4).

Připoměňme 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, 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, ℓ budou nejčastěji označovat indexy výrazů.

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)

Tvrzení. *Nechť V je vektorový prostor nad polem skalárů $\mathbb{K}$, dále uvažme $a, b, a_i \in \mathbb{K}$, 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 $u = 1 \cdot u = (p^{-1} \cdot p) \cdot u = p^{-1} \cdot 0 = 0$. □

V odstavci 2.11 jsme pracovali s tzv. lineárními kombinacemi řádků matice. S obecnými vektory budeme zacházet zcela analogicky: Výrazy tvaru $a_1 \cdot v_1 + \cdots + a_k \cdot v_k$ nazýváme *lineární kombinace* vektorů $v_1, \ldots, v_k \subset V$. Množina vektorů $M \subset V$ ve vektorovém prostoru V nad $\mathbb{K}$ se nazývá *lineárně nezávislá* jestliže pro každou k-tici vektorů $v_1, \ldots, v_k \in M$ a každé skaláry $a_1, \ldots, a_k \in \mathbb{K}$ platí:

$$a_1 \cdot v_1 + \cdots + a_k \cdot v_k = 0 \quad \Longrightarrow \quad a_1 = a_2 = \cdots = a_k = 0.$$

Posloupnost vektorů $v_1, \ldots, v_k$ nazveme *lineárně nezávislou* jestliže $v_1, \ldots, v_k$ jsou po dvou různé a $\{v_1, \ldots, v_k\}$ je lineárně nezávislá. Množina M vektorů je *lineárně závislá*, jestliže není lineárně nezávislá. Přímo z definice pak 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 lineární kombinace ostatních.

Přímo z definic plyne, že každá podmnožina lineárně nezávislé množiny M je lineárně nezávislá. Stejně snadno vidíme, že $M \subset V$ je lineárně nezávislá právě tehdy, když každá konečná podmnožina v M je lineárně nezávislá.

2.24. Vektorový prostor ano či ne? Rozhodněte o následujících množinách, jestli jsou vektorovými prostory nad tělesem reálných čísel:

(1) Množina řešení homogenní diferenční rovnice.
(2) Množina řešení nehomogenní diferenční rovnice.
(3) $\{f : \mathbb{R} \to \mathbb{R} | f(x) = c, c \in \mathbb{R}\}$

Řešení. (1) Ano. Množina řešení, tedy množina posloupností vyhovujících dané diferenční homogenní rovnici, je evidentně uzavřená vzhledem ke sčítání i násobení reálným číslem: mějme posloupnosti $(x_n)_{n=0}^{\infty}$ a $(y_n)_{n=0}^{\infty}$ vyhovující stejné homogenní diferenční rovnici, tedy

$$\begin{aligned} a(n)x_n + a(n-1)x_{n-1} + \cdots + a(1)x_1 &= 0 \\ a(n)y_n + a(n-1)y_{n-1} + \cdots + a(1)y_1 &= 0. \end{aligned}$$

Sečtením těchto rovnic dostaneme

$$a(n)(x_n + y_n) + a(n-1)(x_{n-1} + y_{n-1}) + \cdots + a(1)(x_1 + y_1) = 0,$$

tedy i posloupnost $(x_n + y_n)_{n=0}^{\infty}$, vyhovuje stejné diferenční rovnici. Rovněž tak pokud posloupnost $(x_n)_{n=0}^{\infty}$ vyhovuje dané rovnici, tak i posloupnost $(kx_n)_{n=0}^{\infty}$, kde $k \in \mathbb{R}$.

(2) Ne. Součet dvou řešení nehomogenní rovnice

$$\begin{aligned} a(n)x_n + a(n-1)x_{n-1} + \cdots + a(1)x_1 &= c \\ a(n)y_n + a(n-1)y_{n-1} + \cdots + a(1)y_1 &= c, \quad c \in \mathbb{R} - \{0\} \end{aligned}$$

vyhovuje rovnici

$$a(n)(x_n + y_n) + a(n-1)(x_{n-1} + y_{n-1}) + \cdots + a(1)(x_1 + y_1) = 2c \neq c,$$

zejména pak nevyhovuje původní nehomogenní rovnici.

(3) Vnímáme–li zadání jako „pro pevné $x \in \mathbb{R}$ a pevné c požadujeme po reálných funkcích, aby $f(x) = c$“, pak je to vektrorový prostor právě, když $c = 0$. Pokud nám jde naopak o konstantní funkce, ty pochopitelně vektorový prostor jsou (opět jednorozměrný reálný prostor $\mathbb{R}$). □

2.18

2.25. Generátory a podprostory. Podmnožina $M \subset V$ 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 n–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 dvourozměrný.

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 $\mathbb{R}_m[x] \subset \mathbb{R}_n[x]$ je vektorový podprostor pro všechna $m \leq n \leq \infty$. Podprostory jsou např. všechny sudé polynomy nebo liché polynomy $(f(-x) = \pm f(x))$.

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 všechny $i \in I$, $a \cdot u + b \cdot v \in W_i$, to ale znamená, že $a \cdot u + b \cdot v \in \cap_{i\in I} W_i$.

Zejména je tedy podprostorem průnik všech podprostorů $W \subset V$, které obsahují předem danou množinu vektorů $M \subset V$. Říkáme, že takto 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 podmnožinu $M \subset V$ platí*

(1) $\langle M\rangle = \{a_1 \cdot u_1 + \cdots + a_k \cdot u_k;\ k \in \mathbb{N}, a_i \in \mathbb{K}, u_j \in M, j = 1, \ldots, k\}$
(2) $M = \langle M\rangle$ *právě když M je vektorový podprostor*
(3) *jestliže $N \subset M$ pak $\langle N\rangle \subset \langle M\rangle$ je vektorový podprostor*
(4) $\langle\emptyset\rangle = \{0\} \subset V$*, triviální podprostor.*

Důkaz. (1) Platí $\{a_1u_1 + \cdots + a_ku_k\} \subset \langle M\rangle$ a zároveň je to vektorový podprostor (ověřte!), který obsahuje M. (2) plyne z (1) a definice vektorového podprostoru. (3): Nejmenší vektorový podprostor je $\{0\}$, protože prázdnou množinu obsahují všechny podprostory a každý z nich obsahuje 0. □

2.26. Báze a 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 $V_1, \ldots, V_k \subset V$,

$$V_1 + \cdots + V_k = \langle V_1 \cup V_2 \cup \cdots \cup V_k\rangle.$$

Viděli jsme, 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 $W = V_1 + \cdots + V_k \subset V$ se nazývá *přímý součet* podprostorů, jsou-li průniky všech dvojic triviální, tj. $V_i \cap V_j = \{0\}$ pro všechny $i \neq j$. V takovém případě lze každý vektor $w \in W$ napsat právě jedním způsobem jako součet

$$w = v_1 + \cdots + v_k,$$

kde $v_i \in V_i$. Pro přímé součty píšeme

$$W = V_1 \oplus \cdots \oplus V_k = \oplus_{i=1}^k V_i.$$

Podmnožina $M \subset V$ se nazývá *báze vektorového prostoru* V, jestliže $\langle M\rangle = V$ a M je lineárně nezávislá. Vektorový prostor, který má konečnou bázi nazýváme

konečněrozměrný, mohutnost báze nazýváme *dimenzí* V[2]. Nemá-li V konečnou bázi, říkáme, že V je *nekonečněrozměrný*. Píšeme $\dim V = k$, $k \in \mathbb{N}$, případně $k = \infty$. Bázi k-rozměrného prostoru budeme obvykle zapisovat jako k-tici $\underline{v} = (v_1 \dots, v_k)$ bázových vektorů. Jde tu především o zavedení konvence: U konečněrozměrných podprostorů budeme totiž vždy uvažovat bázi včetně zadaného pořadí prvků i když jsme to takto, striktně vzato, nedefinovali.

Zjevně, je-li $(v_1, \dots, v_n)$ bazí V, je celý prostor V přímým součtem jednorozměrných podprostorů

$$V = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle.$$

2.20 **2.27. Věta.** *Z libovolné konečné množiny generátorů vektorového prostoru V lze vybrat bázi. Každá báze V má přitom stejný počet prvků.*

Důkaz. První tvrzení je snadno vidět 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. Při $k = 1$ je $V = \langle \{v\} \rangle$ a $v \neq 0$ protože $\{v\}$ je lineárně nezávislá množina vektorů. Pak je ovšem $\{v\}$ zároveň báze 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

$$u = a_1 \cdot v_1 + \cdots + a_n \cdot v_n \in V$$

s $a_i \neq 0$ pro jisté i. Pak

$$v_i = \frac{1}{a_i}\big(u - (a_1 \cdot v_1 + \cdots + a_{i-1} \cdot v_{i-1} + a_{i+1} \cdot v_{i+1} + \cdots + a_n \cdot v_n)\big)$$

a proto také $\langle u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n \rangle = V$. Jistě je to opět báze, protože vektory $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$ byly nezávislé, takže kdyby přidáním u vznikly lineárně závislé vektory, pak by u bylo jejich lineární kombinací, ale to by znamenalo $V = \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n \rangle$, což není možné. Takže už víme, že pro libovolný nenulový vektor $u \in V$ existuje i, $1 \leq i \leq n$, takové, že $(u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$ je opět báze V.

Dále budeme místo jednoho vektoru u uvažovat lineárně nezávislou množinu $u_1, \dots, u_k$ a budeme postupně přidávat $u_1, u_2, \dots$, vždy výměnou za vhodné v_i podle předchozího postupu. Je třeba pouze ověřit, že takové v_i vždy bude existovat (tj. že se nebudou vektory u vyměňovat vzájemně). Předpokládejme tedy, že již máme umístěné $u_1, \dots, u_\ell$. Pak $u_{\ell+1}$ se jistě vyjádří jako lineární kombinace těchto vektorů a zbylých v_j. Pokud by pouze koeficienty u $u_1, \dots, u_\ell$ byly nenulové, znamenalo by to, že již samy vektory $u_1, \dots, u_{\ell+1}$ byly lineárně závislé, což je ve sporu s našimi předpoklady.

Pro každé $k \leq n$ tak po k krocích získáme bázi ve které z původní došlo k výměně k vektorů za nové. Pokud by $k > n$, pak již v n-tém kroku obdržíme bázi vybranou z těchto vektorů, což znamená, že nemohou být lineárně nezávislé. Zejména tedy není možné, aby dvě báze měly různý počet prvků. □

[2]Všimněme si, že triviální podprostor je generován prázdnou množinou, která je "prázdnou" bazí. Má tedy triviální podprostor dimenzi nulovou.

Ve skutečnosti jsme dokázali silnější tvrzení, tzv. *Steinitzovu větu o výměně*, která říká, že pro každou konečnou bázi a každý systém lineárně nezávislých vektorů ve V umíme najít podmnožinu bázových vektorů, které záměnou za zadané nové vektory dají opět bázi. Můžeme si také sformulovat zjevné důsledky:

Tvrzení. (1) *Každé dvě báze konečněrozměrného 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 konečněrozměrných vektorových prostorů jsou právě maximální lineárně nezávislé množiny*
(4) *Báze prostoru s konečnou dimenzí jsou právě minimální množiny generátorů*

Důsledek. *Nechť $W, W_1, W_2 \subset V$ jsou podprostory v prostoru konečné dimenze. Pak platí*

(1) $\dim W \leq \dim V$
(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 $\dim W_1 = r \neq 0$, $\dim W_2 = s \neq 0$ a nechť $(w_1 \dots, w_t)$ je báze $W_1 \cap W_2$ (nebo prázdná množina, pokud je průnik triviální). Podle předchozí věty lze tuto bázi doplnit na bázi $(w_1, \dots, w_t, u_{t+1} \dots, u_r)$ pro W_1 a bázi $(w_1 \dots, w_t, v_{t+1}, \dots, v_s)$ pro W_2. Vektory $w_1, \dots, w_t, u_{t+1}, \dots, u_r, v_{t+1} \dots, v_s$ jistě generují $W_1 + W_2$. Ukážeme, že jsou přitom lineárně nezávislé. Nechť

$$a_1 \cdot w_1 + \cdots + a_t \cdot w_t + b_{t+1} \cdot u_{t+1} + \cdots + b_r \cdot u_r + c_{t+1} \cdot v_{t+1} + \cdots + c_s \cdot v_s = 0$$

Pak $-(c_{t+1} \cdot v_{t+1} + \cdots + c_s \cdot v_s) = a_1 \cdot w_1 + \cdots + a_t \cdot w_t + b_{t+1} \cdot u_{t+1} + \cdots + b_r \cdot u_r$ musí patřit do $W_2 \cap W_1$. To ale má za následek, že $b_{t+1} = \cdots = b_r = 0$. 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) se nyní ověří přímým počítáním generátorů. □

2.21 **2.28. Příklady.** (1) $\mathbb{K}^n$ má (jako vektorový prostor nad $\mathbb{K}$) dimenzi n. Bazí je např. n-tice vektorů

$$((1, 0, \dots, 0), (0, 1, \dots, 0) \dots, (0, \dots, 0, 1)).$$

Tuto bázi nazýváme *standardní báze v* $\mathbb{K}^n$. V případě konečného pole skalárů, např. $\mathbb{Z}_k$, má celý vektorový prostor $\mathbb{K}^n$ jen konečný počet prvků. Kolik?

(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 $m + 1$, bazí je např. posloupnost $1, x, x^2, \dots, x^m$. Vektorový prostor všech polynomů $\mathbb{K}[x]$ má dimenzi ∞, umíme však ještě stále najít bázi (i když s nekonečně mnoha prvky): $1, x, x^2, \dots$.

(4) Vektorový prostor $\mathbb{R}$ nad $\mathbb{Q}$ má dimenzi ∞ a nemá spočetnou bázi.

(5) Vektorový prostor všech zobrazení $f : \mathbb{R} \to \mathbb{R}$ má také dimenzi ∞ a nemá spočetnou bázi.

2.22

2.29. Souřadnice vektorů. Když je množina $\{v_1, \dots, v_n\} \subset V$ je báze, můžeme každý vektor $v \in V$ vyjádřit jako lineární kombinaci $v = a_1v_1 + \cdots + a_nv_n$. Předpokládejme, že to uděláme dvěma způsoby:

$$v = a_1v_1 + \cdots + a_nv_n = b_1v_1 + \cdots + b_nv_n.$$

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 $i = 1, \dots, n$. Lze tedy každý vektor zadat právě jediným způsobem jako lineární kombinaci bázových vektorů. Koeficienty této jediné lineární kombinace vyjadřující daný vektor $v \in V$ ve zvolené bázi $(v_1, \dots, v_n)$ se nazývají *souřadnice vektoru* v v této bázi.

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:[3]

- $\underline{v}(u + w) = \underline{v}(u) + \underline{v}(w);\ \forall u, w \in V$
- $\underline{v}(a \cdot u) = a \cdot \underline{v}(u);\ \forall a \in \mathbb{K}, \forall u \in V.$

To jsou ale vlastnosti zobrazení, kterým jsme v geometrii roviny říkali lineární (zachovávaly naši lineární strukturu v rovině). Jsou tedy souřadnice vlastně lineární zobrazení z (abstraktního) vektororového prostoru V do n-tic skalárů $\mathbb{K}^n$, kde n je dimenze V. Než se budeme věnovat podrobněji závislosti souřadnic na volbě báze, podíváme se obecněji na pojem linearity zobrazení.

2.30. Příklad.

2.30.1. *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 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 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 hodnost než je počet řádků je ekvivalentní nulovosti determinantu dané matice. Podmíka 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 $a_1 = -1$, $a_{2,3} = \frac{1 \pm \sqrt{21}}{2}$. □

2.23

2.31. Lineární 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) $f(a \cdot u) = a \cdot f(u),\ \forall a \in \mathbb{K},\ \forall u \in V.$

[3] 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 nekonečněrozměrného) 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 $\mathbb{K}$).

Samozřejmě, že jsme taková zobrazení již viděli ve formě násobení matic:

$$\mathbb{K}^n \ni x \mapsto A \cdot x \in \mathbb{K}^m$$

s maticí typu m/n nad $\mathbb{K}$. *Obraz* $Imf := f(V) \subset W$ je zjevně vektorový podprostor. Stejně tak je vektorovým podprostorem množina všech vektorů $\operatorname{Ker} f := f^{-1}(\{0\}) \subset V$. Nazývá se *jádro lineárního zobrazení* f. Lineární zobrazení, které je bijekcí nazýváme *izomorfismus*.

Podobně jako u abstraktní definice vektorových prostorů, i zde je na místě z axiomů ověřit zdánlivě samozřejmá tvrzení:

Tvrzení. *Nechť $f : V \to W$ je lineární zobrazení. Pro všechny $u, u_1, \dots, u_k \in V$, $a_1, \dots, a_k \in \mathbb{K}$ platí:*

(1) $f(0) = 0$
(2) $f(-u) = -f(u)$
(3) $f(a_1 \cdot u_1 + \cdots + a_k \cdot u_k) = a_1 \cdot f(u_1) + \cdots + a_k \cdot f(u_k)$
(4) *pro každý vektorový podprostor $V_1 \subset V$ je jeho obraz $f(V_1)$ vektorový podprostor ve W.*
(5) *Pro každý podprostor $W_1 \subset W$ je množina $f^{-1}(W_1) = \{v \in V;\ f(v) \in W_1\}$ vektorový podprostor ve V.*

Důkaz. Počítáme s využitím axiomů a definic a již dokázaných výsledků – dohledejte samostatně!:
$f(0) = f(u - u) = f((1 - 1) \cdot u) = 0 \cdot f(u) = 0$.
$f(-u) = f((-1) \cdot u) = (-1) \cdot f(u) = -f(u)$.
Vlastnost (3) se ověří snadno indukcí z definičního vztahu.
Z (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 $f(a \cdot u + b \cdot v) = a \cdot f(u) + b \cdot f(v) \in W_1$. □

2.24

2.32. 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 $\operatorname{Ker} f = \{0\} \subset V$. Inverzní zobrazení k izomorfismu je opět izomorfismus.
(3) Pro podprostory V_1, V_2 a lineární zobrazení $f : V \to W$ platí $f(V_1 + V_2) = f(V_1) + f(V_2)$, $f(V_1 \cap V_2) \subset f(V_1) \cap f(V_2)$.
(4) Zobrazení "přiřazení souřadnic" $\underline{u} : V \to \mathbb{K}^n$ dané libovolně zvolenou bází $\underline{u} = (u_1, \dots, u_n)$ vektorového prostoru V je izomorfismus.
(5) Dva konečněrozměrné vektorové prostory jsou izomorfní právě když mají stejnou dimenzi.
(6) Složení dvou izomorfismů je izomorfismus.

Důkaz. Ověření prvního tvrzení je snadné cvičení. Pro druhé si uvědomme, že je-li f lineární bijekce, pak $w = f^{-1}(au + bv)$ právě, když $f(w) = f(a \cdot f^{-1}(u) + b \cdot f^{-1}(v))$. Je tedy 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. □

2.33. Opět souřadnice. Uvažujme libovolné vektorové prostory V, W nad $\mathbb{K}$ s $\dim V = n$, $\dim W = m$ a mějme lineární zobrazení $f : V \to W$. Pro každou volbu bází $\underline{u} = (u_1, \dots, u_n)$ na V, $\underline{v} = (v_1, \dots, v_n)$ na W, máme k dispozici příslušná přiřazení souřadnic:

$$\begin{array}{ccc} V & \xrightarrow{\quad f \quad} & W \\ {\scriptstyle \underline{u}}\downarrow\simeq & & \simeq\downarrow{\scriptstyle \underline{v}} \\ \mathbb{K}^n & \xrightarrow{\quad f_{\underline{u},\underline{v}} \quad} & \mathbb{K}^m \end{array}$$

Přitom je každé lineární zobrazení jednoznačně určeno svými hodnotami na libovolné množině generátorů, zejména tedy na bázi $\underline{u}$. 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 zobrazení f na bázových vektorech. Pro obecný vektor $u = b_1 \cdot u_1 + \cdots + b_n \cdot u_n$ spočteme

$$\begin{aligned} f(u) &= b_1 \cdot f(u_1) + \cdots + b_n \cdot f(u_n) \\ &= b_1(a_{11} v_1 + \cdots + a_{m1} v_m) + \cdots + b_n(a_{1n} v_1 + \cdots + a_{mn} v_m) \\ &= (b_1 a_{11} + \cdots + b_n a_{1n}) \cdot v_1 + \cdots + (b_1 a_{m1} + \cdots + b_n a_{mn}) \cdot v_m \end{aligned}$$

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 $\mathbb{K}^k$ chápeme jako sloupce, tj. matice typu $k/1$

$$f_{\underline{u},\underline{v}}(\underline{u}(w)) = \underline{v}(f(w)) = A \cdot \underline{u}(w).$$

Matici A nazýváme *maticí zobrazení* f v bázích $\underline{u}$, $\underline{v}$. Naopak, každá volba matice A typu m/n zadává jednoznačně lineární zobrazení $\mathbb{K}^n \to \mathbb{K}^m$. Máme-li tedy zvoleny báze prostorů V a W, odpovídá každé volbě matice typu m/n právě jedno lineární zobrazení $V \to W$.

Jestliže za V i W zvolíme tentýž prostor, ale s různými bazemi, a za f identické zobrazení, vyjadřuje náš postup vektory báze $\underline{u}$ v souřadnicích vzhledem k $\underline{v}$. Označme výslednou matici T. Když pak zadáme vektor u

$$u = x_1 u_1 + \cdots + x_n u_n$$

v souřadnicích vzhledem k $\underline{u}$ a dosadíme za u_i, obdržíme souřadné vyjádření $\bar{x}$ téhož vektoru v bázi $\underline{v}$. Stačí k tomu přeskládat pořadí sčítanců a vyjádřit skaláry u jednotlivých vektorů báze. Podle výše uvedeného postupu musí vyjít $\bar{x} = T \cdot x$. Tuto matici nazýváme *matice přechodu* od báze $\underline{u}$ k bázi $\underline{v}$. Matice T zadávající transformaci souřadnic z báze $\underline{u}$ do báze $\underline{v}$ je tedy maticí identického zobrazení $\mathrm{id}_V : V \to V$:

$$\begin{array}{ccc} V & \xrightarrow{\quad \mathrm{id}_V \quad} & V \\ {\scriptstyle \underline{u}}\downarrow\simeq & & \simeq\downarrow{\scriptstyle \underline{v}} \\ \mathbb{K}^n & \xrightarrow{\quad (\mathrm{id}_V)_{\underline{u},\underline{v}} \quad} & \mathbb{K}^n \end{array}$$

Přímo z definice vyplývá:

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 $\underline{u}$.

2.26

2.34. Více souřadnic. Nyní snadno vidíme, 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 $g_{\underline{v},\underline{w}}$. Pro matice těchto zobrazení dostáváme čímž jsme odvodili:

$$g_{\underline{v},\underline{w}} \circ f_{\underline{u},\underline{v}}(x) = B \cdot (A \cdot x) = (B \cdot A) \cdot x = (g \circ f)_{\underline{u},\underline{w}}(x)$$

pro všechny $x \in \mathbb{K}^n$. Všimněte si, 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:

$$\begin{array}{ccccccc} V & \xrightarrow{\mathrm{id}_V} & V & \xrightarrow{f} & W & \xrightarrow{\mathrm{id}_W} & W \\ {\scriptstyle \underline{u}'}\downarrow\simeq & & {\scriptstyle \underline{u}}\downarrow\simeq & & \simeq\downarrow{\scriptstyle \underline{v}} & & \simeq\downarrow{\scriptstyle \underline{w}'} \\ \mathbb{K}^n & \xrightarrow{T} & \mathbb{K}^n & \xrightarrow{f_{\underline{u},\underline{v}}} & \mathbb{K}^m & \xrightarrow{S^{-1}} & \mathbb{K}^m \end{array}$$

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 $f : V \to V$ vyjadřujeme zpravidla f pomocí jedné báze $\underline{u}$ prostoru V, to je přechod k nové bázi $\underline{u}'$ bude znamenat změnu na $A' = T^{-1}AT$.

2.35. Příklady.

2.35.1.

2.35.2. *Je dáno lineární zobrazení $\mathbb{R}^3 \to \mathbb{R}^3$ ve standardní bázi následujicí maticí:*

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 1 \\ 2 & 0 & 0 \end{pmatrix}.$$

Napište matici tohoto zobrazení v bázi

$$\begin{aligned} f_1 &= (1,1,0) \\ f_2 &= (-1,1,1) \\ f_3 &= (2,0,1). \end{aligned}$$

Řešení. Matice 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 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}, což je

$$\begin{pmatrix} \frac{1}{4} & \frac{3}{4} & -\frac{1}{2} \\ -\frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{4} & -\frac{1}{4} & \frac{1}{2} \end{pmatrix}.$$

Matice zobrazení v bázi $\underline{f}$ je potom

$$T^{-1}AT = \begin{pmatrix} \frac{1}{4} & 2 & -\frac{3}{4} \\ \frac{5}{4} & 0 & \frac{7}{4} \\ \frac{3}{4} & -2 & \frac{9}{4} \end{pmatrix}.$$

□

2.35.3. *Určete, jaké lineární zobrazení $\mathbb{R}^3 \to \mathbb{R}^3$ zadává matice*

$$\begin{pmatrix} -\frac{2}{3} & -\frac{1}{3} & -\frac{2}{3} \\ \frac{4}{3} & -\frac{7}{3} & -\frac{8}{3} \\ -1 & 1 & 1 \end{pmatrix}$$

Řešení. Dvojnásobná vlastní hodnota -1, příslušné vlastní vektory $[2,0,1]$, $[1,1,0]$, jednonásobná vlastní hodnota 0, vlastní vektor $[1,4,-3]$. Osová souměrnost podle přímky dané posledním vektorem složená s projekcí na rovinu kolmou k poslednímu vektoru, tedy danou obecnou rovnicí $x+4y-3z=0$.

□

2.27

2.36. Lineární a multilineární formy. Speciálním 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.

Při pevně zvolené bázi $\{1\}$ na $\mathbb{K}$ jsou s každou volbou báze na V lineární formy ztotožněny s maticemi typu $1/n$, tj. s řádky. Vyčíslení takové formy na vektoru je pak dáno vynásobením příslušného řádkového vektoru se sloupcem souřadnic.

Množina všech lineárních forem na daném prostoru V je opět vektorový prostor, značíme jej V^*. Pokud je V konečněrozměrný, je V^* izomorfní prostoru V. Realizace takového izomorfismu je dána např. volbou tzv. *duální báze* k zvolené bázi na V, jejímiž prvky α_i jsou právě formy zadávající i-tou souřadnici.

Podobně budeme pracovat i se zobrazeními ze součinu k kopií vektorového prostoru V do skalárů lineárních v každém argumentu. Hovoříme o *k-lineárních* formách. Budeme se setkávat (a již jsme je viděli v dimenzi 2) zejména s n-lineárními antisymetrickými formami (formy objemu) a symetrickými bilineárními formami.

2.28

2.37. Velikost vektorů. V geometrii roviny jsem již pracovali nejen s bázemi a lineárními zobrazeními, ale také s velikostí vektorů a jejich úhly. Pro zavedení těchto pojmů jsme použili souřadného vyjádření pro velikost $v=(x,y)$:

$$\|v\| = \sqrt{x^2+y^2},$$

zatímco úhel φ dvou vektorů $v=(x,y)$ a $v'=(x',y')$ byl dán

$$\cos\varphi = \frac{xx'+yy'}{\|v\|\|v'\|}.$$

Povšimněme si, že výraz v čitateli posledního výrazu je lineární v každém ze svých argumentů, značíme jej $\langle v, v' \rangle$ a říkáme mu skalární součin vektorů v a v'. Skalární součin je také symetrický ve svých argumentech a platí

$$\|v\|^2 = \langle v, v \rangle.$$

Zejména 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.

Analogicky budeme postupovat v obecném případě reálného vektorového prostoru. *Skalární součin* na vektorovém prostoru V nad reálnými čísly je bilineární symetrická forma $\langle\ ,\ \rangle : V \times V \to \mathbb{R}$ taková, že $\langle v, v \rangle \geq 0$ a je roven nule pouze při $v = 0$. Pro skalární součin se často používá také 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.

Vektory v a $w \in V$ se nazývají *ortogonální*, jestliže $\langle v, w \rangle = 0$. 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*.

Úhel φ dvou vektorů v a w je dán vztahem

$$\cos\varphi = \frac{\langle v, w \rangle}{\|v\|\|w\|}.$$

Tvrzení. *Skalární součin je v každé ortonormální bázi dán výrazem*

$$\langle x, y \rangle = x^T \cdot y.$$

V obecné bázi V existuje symetrická matice S taková, že

$$\langle x, y \rangle = x^T \cdot S \cdot y.$$

Důkaz. Skalární součin je plně určen svými hodnotami na dvojicích bázových vektorů. Zvolme tedy bázi $\underline{u}$ a označme

$$s_{ij} = \langle u_i, u_j \rangle.$$

Pak ze symetričnosti skalárního součinu plyne $s_{ij} = s_{ji}$ a z lineárnosti součinu v každém z argumentů dostáváme:

$$\langle \sum_i x_i u_i, \sum_j y_j u_j \rangle = \sum_{i,j} x_i y_j \langle u_i, u_j \rangle = \sum_{i,j} s_{ij} x_i y_j.$$

Pokud je báze ortonormální, je matice S jednotkovou maticí. □

Uvidíme o něco později, že na každém vektroovém prostoru se skalárním součinem existují ortonormální báze, viz 2.48.

2.38. Příklady.

2.38.1. *Označme S střed hrany AB krychle $ABCDEFGH$ (v obvyklém označení, s hranou AE). Určete cosinus odchylky úseček 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 cosinus odchylky ϕ tedy máme

$$\cos(\phi)=\left|\frac{(1/2,0,-1)\cdot(0,1,1)}{\|(1/2,0,-1)\|\,\|(0,1,1)\|}\right|=\frac{\sqrt{2}}{\sqrt{5}}$$

. □

4. Vlastnosti lineárních zobrazení

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.

2.29 **2.39. Příklady.** Začneme několika příklady v prostorech malých dimenzí. Ve standardní bázi $\mathbb{R}^2$ uvažujme následující matice zobrazení $f:\mathbb{R}^2\to\mathbb{R}^2$:

$$A=\begin{pmatrix}1&0\\0&0\end{pmatrix},\quad B=\begin{pmatrix}0&1\\0&0\end{pmatrix},\quad C=\begin{pmatrix}a&0\\0&b\end{pmatrix},\quad D=\begin{pmatrix}0&-1\\1&0\end{pmatrix}.$$

Matice A zadává kolmou projekci podél podprostoru

$$W\subset\{(0,a);\ a\in\mathbb{R}\}\subset\mathbb{R}^2$$

na podprostor

$$V\subset\{(a,0);\ a\in\mathbb{R}\}\subset\mathbb{R}^2.$$

Evidentně pro toto zobrazení $f:\mathbb{R}^2\to\mathbb{R}^2$ platí $f\circ f=f$ a tedy $f|_{\mathrm{Im}\,f}$ 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 $(1,x)$.

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. Např. volba $a=1$, $b=-1$ odpovídá komplexní konjugaci $x+iy\mapsto x-iy$ na dvourozměrném reálném prostoru $\mathbb{R}^2\simeq\mathbb{C}$ v bázi $(1,i)$. Toto je lineární zobrazení reálného vektorového prostoru, nikoliv však jednorozměrného komplexního prostoru $\mathbb{C}$. V geometrii roviny jde o zrcadlení podle osy x.

Matice D je maticí rotace o pravý úhel ve standardní bázi. Jako pro každé lineární zobrazení, které je bijekcí, umíme najít 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 začátku i konci. Zkusme však uvažovat matici C jako matici zobrazení $g:\mathbb{C}^2\to\mathbb{C}^2$. Pak umíme najít vektory $u=(i,1)$, $v=(1,i)$, pro které bude platit

$$g(u)=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\cdot\begin{pmatrix}i\\1\end{pmatrix}=i\cdot u,\ g(v)=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\cdot\begin{pmatrix}1\\i\end{pmatrix}=-i\cdot v.$$

To ale znamená, že v bázi (u,v) na $\mathbb{C}^2$ má g matici

$$K=\begin{pmatrix}i&0\\0&-i\end{pmatrix}$$

a povšimněme si, že tato komplexní analogie k případu matice C má na diagonále prvky $\pm a$, $a = \cos(\frac{1}{2}\pi) + i\sin(\frac{1}{2}\pi)$. Jinými slovy, argument v goniometrickém tvaru tohoto komplexního čísla udává úhel otočení. Navíc, můžeme si označit reálnou a imaginární část vektoru u takto

$$u = x_u + iy_u = \operatorname{Re} u + i \operatorname{Im} u = \begin{pmatrix}0\\1\end{pmatrix} + i \cdot \begin{pmatrix}1\\0\end{pmatrix}$$

a zúžení komplexního zobrazení g na reálný vektorový podprostor generovaný vektory x_u a iy_u (tj. násobení komplexní jednotkou i) je právě otočení o úhel $\frac{1}{2}\pi$.

2.30

2.40. 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 skaláry a. Zvolme tedy pevně lineární zobrazní $f : V \to V$ 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 bazích, jde o výraz

$$A \cdot x - a \cdot x = (A - a \cdot E) \cdot x = 0.$$

Z předchozího víme, že taková soustava rovnic má jediné řešení $x = 0$, pokud je matice $A - aE$ invertibilní. 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 2.22)

e2.1 (2.1) $$\det(A - a \cdot E) = 0.$$

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 $\mathbb{K}$.

Skaláry vyhovující rovnici $f(u) = a \cdot u$ pro nenulový vektor $u \in V$ nazýváme *vlastní čísla zobrazení* f, příslušné vektory u pak *vlastní vektory zobrazení* f.

Z definice vlastních čísel je zřejmé, že jejich výpočet nemůže záviset na volbě báze a tedy matice zobrazení f. Skutečně, jako přímý důsledek trasformačních vlastností z 2.34 a Cauchyovy věty 2.18 pro výpočet determinantu součinu dostáváme jinou volbou souřadnic matici $A' = P^{-1}AP$ s invertibilní maticí P a

$$|P^{-1}AP - \lambda E| = |P^{-1}AP - P^{-1}\lambda EP| = |P^{-1}(A - \lambda E)P| = |P^{-1})||(A - \lambda E||P|,$$

protože násobení skalárů je komutativní a $|P^{-1}| = |P|^{-1}$.

Obdobnou terminologii používáme i pro matice. 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 hodnoty 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 zobrazení $f : V \to V$ nezávislý na volbě báze V, $\dim V = n$, jsou i jeho koeficienty u jednotlivých mocnin proměnné λ skaláry vyjadřující vlastnosti zobrazení f, tj. nemohou záviset na naší volbě báze. Zejména je snadné vyjádřit koeficienty u nejvyšších a nejnižších mocnin:

$$|A - \lambda \cdot E| = (-1)^n\lambda^n + (-1)^{n-1}(a_{11} + \cdots + a_{nn}) \cdot \lambda^{n-1} + \cdots + |A| \cdot \lambda^0$$

Součet diagonálních členů matice se nazývá *stopa matice*, značíme ji TrA, *stopa zobrazení* je definována jako stopa jeho matice v libovolné bázi.

2.30a **2.41. Věta.** *Vlastní vektory lineárního zobrazení $f : V \to V$ příslušné různým vlastním hodnotám jsou lineárně nezávislé.*

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 $a_{l+1} \cdot u_{l+1} = \sum_{i=1}^{l} a_{l+1} \cdot c_i \cdot u_i$, 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 dostáváme $0 = \sum_{i=1}^{l} (a_{l+1} - a_i) \cdot c_i \cdot u_i$, všechny rozdíly vlastních hodnot jsou nenulové a alespoň jeden koeficient c_i je nenulový. To je spor s předpokládanou nezávislostí $u_1, \dots, u_\ell$. □

Důsledek. *Jestliže existuje n navzájem různých kořenů a_i charakteristického polynomu zobrazení $f : V \to V$, $\dim V = n$, 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. Příslušnou bázi (vyjádřenou v souřadnicích vzhledem k libovolně zvolené bázi V) obdržíme řešením n systémů homogenních lineárních rovnic o n neznámých s maticemi $(A - a_i \cdot E)$, kde A je matice f ve zvolené bázi.*

2.31 **2.42. Příklady.** (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 předchozí větě 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

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

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.

2.43. Příklad včetně změny báze.

2.43.1. *Uvažujme lineární zobrazení $\mathbb{R}^3 \to \mathbb{R}^3$ dané ve standardní bázi maticí:*

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & 2 & 1 \end{pmatrix}$$

Určete toto 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. Spočítejme nejprve vlastní čísla jim příslušné vlastní vektory: 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 $\mathbf{x} = (0, 0, 0)$. 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
$$\begin{pmatrix}-(1+\sqrt{2})&1&0\\1&-\sqrt{2}&1\\1&2&-(1+\sqrt{2})\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=0.$$
Řešením je jednodimenzionální prostor $\langle(1,1+\sqrt{2},1+\sqrt{2})\rangle$.
- $2-\sqrt{2}$: 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 $\langle(1,1-\sqrt{2},1-\sqrt{2})\rangle$.

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 priklané báze k bázi standardní, tedy matici T^{-1}. Souřadnice vektorů nové báze pouze zapíšeme do sloupců:
$$T^{-1}=\begin{pmatrix}1&1&0\\-1&2&1\\1&0&1\end{pmatrix}$$
Pro matici B zobrazení v nové bázi pak máme (viz 2.34).
$$B=TAT^{-1}=\begin{pmatrix}1&1&0\\1&2&1\\1&2&1\end{pmatrix}\cdot\begin{pmatrix}\frac{1}{2}&-\frac{1}{4}&\frac{1}{4}\\\frac{1}{2}&\frac{1}{4}&-\frac{1}{4}\\-\frac{1}{2}&\frac{1}{4}&\frac{3}{4}\end{pmatrix}\cdot\begin{pmatrix}1&1&0\\-1&2&1\\1&0&1\end{pmatrix}$$
□

2.44. Další příklady.

2.44.1. *Nalezňete vlastní čísla a jim příslušné (prostory) vlastních vektorů matice:*
$$\begin{pmatrix}-1&-\frac{5}{6}&\frac{5}{3}\\0&-\frac{2}{3}&-\frac{2}{3}\\0&\frac{1}{6}&-\frac{4}{3}\end{pmatrix}$$

Řešení. Trojnásobná vlastní hodnota -1, příslušný vektorový prostor je $\langle(1,0,0),(0,2,1)\rangle$.
□

2.32

2.45. Spektra a nilpotentní zobrazení. *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 $(u_1, \dots, u_n)$ prostoru V taková, že $f(u_1) = 0$ a $f(u_i) = u_{i-1}$ pro všechna $i = 2, \dots, n$. Jinými slovy, matice f v této bázi je tvaru

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & & \ddots \end{pmatrix}.$$

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 definovaný v předchozím příkladu 2.42 je příkladem cyklického zobrazení. Kupodivu to platí i naopak a každé nilpotentní zobrazení je přímým součtem cyklických. Navíc pro každé lineární zobrazení $f : V \to V$, pro které je součet algebraických násobností vlastních čísel roven dimenzi (to nastane vždy pro prostory nad komplexními skaláry), existuje jednoznačný rozklad V na invariantní podprostory V_i příslušné k jednotlivým vlastním číslům λ_i, na kterých je zobrazení $f - \lambda_i \,\mathrm{id}_{V_i}$ nilpotentní.

Tento dosti hluboký výsledek nebudeme dokazovat, sformulujeme jen výslednou *větu o Jordanově rozkladu*. V ní vystupují vektorové (pod)prostory a lineární zobrazení na nich s jediným vlastním číslem λ a maticí

$$J = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix}.$$

Takovýmto maticím (a odpovídajícím invariantním podprostorům) se říká *Jordanův blok*.

2.33

2.46. Věta. *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*

$$V = V_1 \oplus \dots \oplus V_k$$

takových, že $f(V_i) \subset V_i$, zúžení f na každé V_i má jediné vlastní číslo λ_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.

Všimněme si, že jsme tuto větu plně dokázali v případech, kdy jsou všechna vlastní čísla různá nebo když jsou geometrické a algebraické násobnosti vlastních čísel stejné.

2.47. Projekce. Lineární zobrazení $f : V \to V$ 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 přechozí 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.

Předpokládejme nyní, že na V je definován skalární součin, viz 2.37. Pro každý pevně zvolený podprostor $W \subset V$ definujeme jeho *ortogonální doplněk*

$$W^\perp = \{u \in V;\ \langle u, v\rangle = 0 \text{ pro všechny } v \in W\}.$$

Přímo z definice je zjevné, že $W^\perp$ je vektorový podprostor. Jestliže $W \subset V$ má bázi $(u_1, \dots, u_k)$ 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

$$V = W \oplus W^\perp.$$

Každý podprostor $W \neq V$ definuje *kolmou projekci* na W. Je to projekce na W podél $W^\perp$.

2.33a

2.48. Existence ortonormální báze. Přímočaré početní využití kolmých projekcí vede k tzv. *Grammovu–Schmidtovu ortogonalizačnímu procesu*. Cílem procedury je z dané posloupnosti nenulových generátorů $v_1, \dots, v_k$ konečněrozměrného prostoru V vytvořit ortogonální množinu nenulových generátorů pro V.

Začneme prvním (nenulovým) vektorem v_1 a spočteme kolmou projekci v_2 do

$$\langle v_1\rangle^\perp \subset \langle\{v_1, v_2\}\rangle.$$

Výsledek bude nenulový právě, když je v_2 nezávislé na v_1. Ve všech dalších krocích budeme postupovat obdobně.

V ℓ-tém kroku tedy chceme, aby pro $v_{\ell+1} = u_{\ell+1} + a_1 v_1 + \cdots + a_\ell v_\ell$ platilo $\langle v_{\ell+1}, v_i\rangle = 0$, pro všechny $i = 1, \dots, \ell$. 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. Dokázali jsme tedy následující tvrzení:

Tvrzení. *Nechť $(u_1, \dots, u_k)$ je lineárně nezávislá k-tice vektorů prostoru V se skalárním součinem. Pak existuje ortogonální systém vektorů $(v_1, \dots, v_k)$ takový, že $v_i \in \langle u_1, \dots, u_i\rangle$, $i = 1, \dots, k$. Získáme je následující procedurou:*

- *Z nezávislosti vektorů u_i plyne $u_1 \neq 0$. Položíme $v_1 = u_1$.*
- *Máme-li již vektory $v_1, \dots, v_\ell$ potřebných vlastností klademe*

$$v_{\ell+1} = u_{\ell+1} + a_1 v_1 + \cdots + a_\ell v_\ell, \quad a_i = -\frac{\langle u_{\ell+1}, v_i\rangle}{\|v_i\|^2}$$

Kdykoliv máme ortogonální bázi vektorového prostoru V, stačí vektory vynormovat a získáme bázi ortonormální. Dokázali jsme proto:

Důsledek. *Na každém vektorovém prostoru se skalárním součinem existuje ortonormální báze.*

V ortonormální bázi se obzvlášť snadno spočtou souřadnice a kolmé projekce. Skutečně, mějme ortonormální bázi $(e_1, \dots, e_n)$ prostoru V. Pak každý vektor $v = x_1e_1 + \cdots + x_ne_n$ splňuje

$$\langle e_i, v\rangle = \langle e_i, x_1e_1 + \cdots + x_ne_n\rangle = x_i$$

a platí tedy vždy

e2.2 (2.2) $$v = \langle e_1, v\rangle e_1 + \cdots + \langle e_n, v\rangle e_n.$$

Pokud máme zadán podprostor $W \subset V$ a jeho ortonormální bázi $(e_1, \dots, e_k)$, jde ji jistě doplnit na ortonormální bázi $(e_1, \dots, e_n)$ 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 ortonormání bázi podprostoru W, na nejž 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 z dvojice W, $W^\perp$, který má menší dimenzi.

Uvědomme si také, že existence ortonormální báze nám zaručuje, že pro každý prostor V 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 ve Tvrzení 2.37, 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 $\mathbb{R}^n$.

2.49. Příklad.

2.49.1. *Napište matici zobrazení kolmé projekce do roviny procházející počátkem a kolmé na vektor* $(1, 1, 1)$.

Řešení. Obraz libovolného bodu (vektoru) $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{R}^3$ 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 $\mathbf{p}$ je dána (viz přednáška) jako

$$\frac{(\mathbf{x}, (1,1,1))}{|(1,1,1)|^2} = (\frac{x_1 + x_2 + x_3}{3}, \frac{x_1 + x_2 + x_3}{3}, \frac{x_1 + x_2 + x_3}{3}).$$

Výsledné zobrazení je tedy

$$\mathbf{x}-\mathbf{p} = (\frac{2x_1}{3} - \frac{x_2 + x_3}{3}, \frac{2x_2}{3} - \frac{x_1 + x_3}{3}, \frac{2x_3}{3} - \frac{x_1 + x_2}{3}) = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

□

2.50. Tři příklady k samostatnému řešení.

2.50.1. 1. *Napište nějakou bázi reálného vektorového prostoru matic 3×3 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.

2.50.2. 2. *Zaveďte nějaký skalární součin na vektorovém prostoru matic z předchozího příkladu. Spočítejte normu matice z předchozího příkladu, která je indukovaná Vámi zavedeným součinem.*

2.50.3. 3. *Gramm-Schmidtovým ortogonalizačním procesem nalezněte nějakou ortonormální bázi podprostoru $V \subset \mathbb{R}$, kde $V = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 | x_1 + 2x_2 + x_3 = 0\}$.*

2.36

2.51. Ortogonální zobrazení.

Zobrazení $f : V \to W$, které zachovává velikosti pro všechny vektory $u \in V$, se nazývá *ortogonální zobrazení*. Požadujeme tedy

$$\langle f(u), f(u) \rangle = \langle u, u \rangle.$$

Z linearity f a symetrie skalárního součinu plyne

$$\langle f(u+v), f(u+v) \rangle = \langle f(u), f(u) \rangle + \langle f(v), f(v) \rangle + 2\langle f(u), f(v) \rangle,$$

je tedy ekvivalentní podmínkou i zdánlivě silnější požadavek, aby

$$\langle f(u), f(v) \rangle = \langle u, v \rangle,$$

pro všechny vektory $u, v \in V$. V úvodní diskusi o geometrii v rovině jsme ve Větě 1.37 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 musí vždycky být 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 bez újmy na obecnost můžeme rovnou předpokládat, že jsou stejné a $f : V \to V$ (pokud by nebyly, doplníme ortonormální bázi na oboru hodnot na bázi cílového prostoru a matice zobrazení bude čtvercovou maticí A doplněnou nulami na potřebnou velikost). 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 2! Dokázali jsme tak následující tvrzení:

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 všech) má matici A splňující $A^T = A^{-1}$.*

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.

Důsledkem této 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 báze ke druhé se tedy matice ortogonálního zobrazení mění podle vztahu

$$A' = S^T A S.$$

KAPITOLA 3

Linární modely

kde jsou matice užitečné?
– nakonec skoro všude...

1. Lineární rovnice a procesy

2.37

3.1. Systémy lineárních rovnic. Jednoduché lineární procesy jsou dány lineárními zobrazeními $\varphi : V \to W$ na vektorových prostorech. Pokud nám totiž vektor $v \in V$ představuje stav nějakého námi sledovaného jevu (třeba počty občanů tříděných dle nejvyšší dosažené kvalifikace, stav zásob jednotlivých dílů a výrobků atd.), pak $\varphi(v)$ může představovat výsledek provedené operace (výsledek vzdělávací činnosti školské soustavy nebo výroba a prodej za určité časové období apod.). Pokud chceme dosáhnout předem daného výsledku $b \in W$ takového jednorázového procesu, řešíme problém

$$\varphi(x) = b$$

pro neznámý vektor x. V pevně zvolených souřadnicích pak máme matici A zobrazení φ a souřadné vyjádření vektoru b. Jak jsme si povšimnuli už v úvodu druhé kapitoly, řešení tzv. *homogenní úlohy*

$$A \cdot x = 0$$

je vektorovým podprostorem. Pokud je dimenze V konečná, řekněme n, a dimenze obrazu zobrazení φ 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 a dosazením vždy jednoho z nich hodnotou jedna a vynulováním ostatních získáme právě k lineárně nezávislých řešení. Každé takové k–tici řešení říkáme *fundamentální systém řešení* daného homogenního systému rovnic.

Uvažme nyní obecný systém rovnic

$$A \cdot x = b.$$

Jestliže 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 systém rovnic nemůže mít řešení (prostě se naše φ vůbec do b nestrefí). Jestliže ale naopak máme stejný počet nezávislých řádků, znamená to, že sloupec b musí být lineární kombinací sloupců matice A. Koeficienty takové kombinace jsou právě řešení.

Mějme tedy 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:

- podprostor všech řešení homogenního systému rovnic $A \cdot x = 0$ má dimenzi $n - k$, kde n je počet proměnných a k je počet lineárně nezávislých rovnic,
- všechna řešení jsou generována tzv. fundamentálním systémem $n - k$ řešení, který lze obdržet z Gausovy eliminace postupným dosazováním nul a jedniček za volné parametry,
- řešení nehomogenního systému existuje právě, když přidáním sloupce b k matici A nezvýšíme počet lineárně nezávislých řádků. V takovém případě je prostor všech řešení dán součty jednoho pevně zvoleného *partikulárního řešení* systému a všech řešení systému homogenního se stejnou maticí.

2.38

3.2. Iterované procesy. Pokud je dán nějaký proces prostřednictvím lineární operace pro jednotlivá časová období, budeme patrně chtít umět studovat jeho chování během delší doby. Zatímco pro řešení systémů lineárních rovnic jsme potřebovali jen minumum znalostí o vlastnostech lineárních zobrazení, teď už to bude jinak. Uvedeme si alespoň ilustrativní příklady.

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 $(a_1, \dots, a_m)$ 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_k na t_{k+1}. Dobrým příkladem lineárních procesů je tzv. *Leslieho model růstu*, viz následující příklad 3.3. V takových modelech vystupuje matice popisující vývoj populace rozdělené na několik věkových skupin

$$A = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 \\ \tau_1 & 0 & 0 & 0 & 0 \\ 0 & \tau_2 & 0 & 0 & 0 \\ 0 & 0 & \tau_3 & 0 & 0 \\ 0 & 0 & 0 & \tau_4 & 0 \end{pmatrix},$$

kde 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 τ_i je relativní úmrtnost i-té skupiny během jednoho období.

Všechny koeficienty jsou tedy kladná reálná čísla a τ jsou mezi nulou a jedničkou. Přímým výpočtem (třeba využitím Laplaceova rozvoje) nyní spočteme charakteristický polynom

$$p(\lambda) = \det(A - \lambda E) = \lambda^5 - a\lambda^4 - b\lambda^3 - c\lambda^2 - d\lambda - e$$

s vesměs nezápornými koeficienty a, b, c, d, e, např. $e = \tau_1\tau_2\tau_3\tau_4 f_5$. Je tedy

$$p(\lambda) = \lambda^5(1 - q(\lambda))$$

kde q je ostře klesající a nezáporná funkce pro $\lambda > 0$. Evidentně bude proto existovat právě jedno kladné λ, pro které bude $q(\lambda) = 1$ a tedy $p(\lambda) = 0$. Jinými slovy, pro každou Leslieho matici existuje právě jedno kladné vlastní číslo.

Pro konkrétní koeficienty (např. když všechny f_i jsou také mezi nulou a jedničkou) můžeme dojít k závěru, že absolutní hodnoty ostatních vlastních čísel jsou ostře menší než jedna, zatímco dominantní vlastní číslo může být vetší než jedna. V takovém případě při iteraci kroků našeho procesu dojde při libovolné počáteční hodnotě x_0 k postupnému vymizení všech komponent v jednotlivých vlastních podprostorech a poměrné proporce rozložení populace do věkových skupin se budou blížit poměrům komponent vlastního vektoru k dominantnímu vlastnímu číslu. Například pro matici (uvědomme si význam jednotlivých koeficientů)

$$A = \begin{pmatrix} 0 & 0.2 & 0.8 & 0.6 & 0 \\ 0.95 & 0 & 0 & 0 & 0 \\ 0 & 0.8 & 0 & 0 & 0 \\ 0 & 0 & 0.7 & 0 & 0 \\ 0 & 0 & 0 & 0.6 & 0 \end{pmatrix}$$

vyjdou vlastní hodnoty přibližně

$$1.03,\ 0,\ -0.5,\ -0,27 + 0.74i,\ -0.27 - 0.74i$$

s velikostmi 1.03, 0, 0.5, 0.78, 0.78 a vlastní vektor příslušný dominantnímu vlastnímu číslu je přibližně

$$x = (30\ 27\ 21\ 14\ 8).$$

Zvolili jsme rovnou jediný vlastní vektor se součtem souřadnic rovným jedné, zadává nám proto přímo výsledné procentní rozložení populace.

3.3

3.3. Příklad – Leslieho růstový model. *Uvažujme následující model vývoje lidské populace. Buď*

- $x_1(t) =$ *počet jedinců starých* $0 - 14$ *let.*
- $x_2(t) =$ *počet jedinců starých* $15 - 29$ *let.*
- $x_3(t) =$ *počet jedinců starých* $30 - 44$ *let.*
- $x_4(t) =$ *počet jedinců starých* $45 - 59$ *let.*
- $x_5(t) =$ *počet jedinců starých* $60 - 75$ *let.*

Vše uvedeno v nějakém čase t. Pokud uvážíme časovou jednotku 15 let, tak v čase $(t+1)$ budeme mít následující počty:

$$\begin{array}{lcccccccccc} x_1(t+1) & = & f_1 x_1(t) & + & f_2 x_2(t) & + & f_3 x_3(t) & + & f_4 x_4(t) & + & f_5 x_5(t) \\ x_2(t+1) & = & \tau_{1,2} x_1(t) & & & & & & & & \\ x_3(t+1) & = & & & \tau_{2,3} x_2(t) & & & & & & \\ x_4(t+1) & = & & & & & \tau_{3,4} x_3(t) & & & & \\ x_5(t+1) & = & & & & & & & \tau_{4,5} x_4(t) & & \end{array}$$

Pokud označíme jako P následující matici

$$P := \begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 \\ \tau_{1,2} & 0 & 0 & 0 & 0 \\ 0 & \tau_{2,3} & 0 & 0 & 0 \\ 0 & 0 & \tau_{3,4} & 0 & 0 \\ 0 & 0 & 0 & \tau_{4,5} & 0 \end{pmatrix},$$

tak v maticové formě pak můžeme psát

$$\mathbf{x}(t+1) = P\mathbf{x}(t),$$

kde $\mathbf{x}(t) = (x_1(t), x_2(t), x_3(t), x_4(t), x_5(t))$.

3.4. Příklad. Usherův model růstu. *Variace předchozího. Mějme populaci jako v předchozím příkladě a uvažujme časovou jednotku* $7,5$ *let, tedy polovinu předchozí. Pak můžeme psát opět*

$$\mathbf{x}(t+1) = P\mathbf{x}(t),$$

kde ovšem nyní

$$P := \begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 \\ \tau_{1,2} & \tau_{2,2} & 0 & 0 & 0 \\ 0 & \tau_{2,3} & \tau_{3,3} & 0 & 0 \\ 0 & 0 & \tau_{3,4} & \tau_{4,4} & 0 \\ 0 & 0 & 0 & \tau_{4,5} & \tau_{5,5} \end{pmatrix}.$$

3.5. Příklad.

3.5.1. *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).*

Řešení. 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 $a = 1/4$. □

2. Lineární diferenční rovnice a filtry

Diferenčními rovnicemi jsme se zabývali již v první kapitole, viz např 1.16. Nyní si uvedeme náznak obecné teorie.

2.40

3.6. Diferenční rovnice. *Homogenní lineární diferenční rovnice* řádu k s konstantními koeficienty je dána výrazem

$$a_0 x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = 0, \quad a_0 \neq 0 \quad a_k \neq 0.$$

Říkáme také, že řešíme *homogenní lineární rekurenci* řádu k. Libovolným zadáním k po sobě jdoucích hodnot x_i jsou určeny i všechny ostatní hodnoty jednoznačně. Zároveň je zjevné, že součet dvou řešení nebo skalární násobek řešení je opět řešení. Opět tedy máme příklad vektorového prostoru. Uvědomme si, že vektroy jsou sice nekonečné posloupnosti čísel, samotný prostor všech řešení ovšem bude konečněrozměrný a předem víme, že jeho dimenze bude rovna řádu rovnice k.

Pokud tedy budeme předpokládat řešení v nějaké vhodné formě a podaří se nám najít k lineárně nezávislých možností, budeme mít opět *fundamentální systém řešení* a všechna ostatní budou jejich lineárními kombinacemi.

Uvažujme tedy stejně jako v 1.16 možnost $x_n = \lambda^n$ pro nějaký skalár λ. Pak dostáváme podmínku

$$\lambda^{n-k}(a_0\lambda^k + a_1\lambda^{k-1} \cdots + a_k) = 0$$

což znamená, že buď $\lambda = 0$ nebo je λ kořenem tzv. *charakteristického polynomu* v závorce. Předpokládejme, že má tento polynom k různých kořenů $\lambda_1, \dots, \lambda_k$. 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 i všechna 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 $n = 0, \dots, k-1$ pro k možností λ_i. Dostaneme tzv. Vandermondovu matici a je pěkným (ale ne úplně snadným) cvičením spočíst, že pro všechna k a jakékoliv k–tice různých λ_i je determinant takovéto matice nenulový. To ale znamená, že zvolená řešení jsou lineárně nezávislá.

Uvažme nyní násobný kořen λ a dosaďme do definiční rovnice předpokládané řešení $x_n = n\lambda^n$. Dostáváme podmínku

$$a_0 n\lambda^n + \dots a_k(n-k)\lambda^{n-k} = 0.$$

Tuto podmínku je možné přepsat pomocí tzv. derivace polynomu, kterou značíme apostrofem:

$$\lambda(a_0\lambda^n + \cdots + a_k\lambda^{n-k})'$$

a časem uvidíme, že kořen polynomu f je vícenásobný právě, když je kořenem i jeho derivace f'. Naše podmínka je tedy splněna. Při vyšší násobnosti ℓ kořene charakteristického polynomu λ dojdeme obdobně k řešením $x_n = n^j\lambda^n$ pro $j = 0, \dots, \ell - 1$.

Úplně obdobně jako u systémů lineárních rovnic můžeme dostat všechna řešení nehomogenních rovnic tak, že najdeme jedno řešení a přičteme celý vektorový prostor dimenze k řešení odpovídajících systémů homogenních. Za tímto účelem zpravidla hledáme řešení ve tvaru polynomu

$$x_n = \alpha_0 + \alpha_1 n + \cdots + \alpha_{k-1}n^{k-1}$$

s neznámými koeficienty α_i, $i = 1, \dots, k-1$. Dosazením do diferenční rovnice dostatneme systém k rovnic pro k proměnných α_i.

Nyní můžeme shrnout získané výsledky:

2.41

3.7. Vlastnosti řešení lineárních diferenčních rovnic s konstantními koeficienty.

- prostor všech řešení homogenního systému řádu k je vektroový prostor dimenze k,
- všechna řešení jsou generována fundamentálním systémem k řešení, který lze obdržet získat z kořenů charakteristického polynomu (λ_i^n, pokud jsou kořeny po dvou různé, složitěji v případě násobných kořenů),
- všechna řešení nehomogenního systému obdržíme, když přičteme jedno pevně zvolené partikulárního řešení systému ke všem řešením systému homogenního se stejnými koeficienty. Partikulární řešení můžeme hledat pomocí tzv. *metody neurčitých koeficientů*, tj. hledáme jej jako polynom s neznámými koeficienty a řešíme systém lineárních rovnic.

- řešení vyhovující daným počátečním podmínkám

$$x_0 = b_0, \ldots, x_{k-1} = b_{k-1}$$

hledáme z obecného řešení dosazením podmínek a určením koeficientů lineání kombinace funadamentálních řešení. Opět to znamená řešit systém lineárních rovnic.

Všimněme si také, že pro rovnice s reálnými koeficienty musí vždy kořeny charakterstického polynomu být reálné, nebo musí vystupovat po dvou komplexně združené nereálné kořeny. Jejich lineárními kombinacemi (součet a rozdíl goniometrických tvarů mocnin) lze pak přímo obdržet reálná řešení vyjádřená pomocí funkcí $\cos(n\varphi)$ a $\sin(n\varphi)$.

3.8. Příklad.

3.8.1. *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

$$a(-1)^n + b2^n - \frac{1}{2}.$$

Dosazením do počátečních podmínek zjistíme konstanty $a = -5/6$, $b = 5/6$. Dané rovnici s počátečními podmínkami tedy vyhovuje posloupnost

$$-\frac{5}{6}(-1)^n + \frac{5}{3}2^{n-1} - \frac{1}{2}.$$

□

3.9. Příklad.

3.9.1. *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

$$a(-1)^n + b\left(\frac{1}{2}\right)^n + 1.$$

Dosazením do počátečních podmínek zjistíme konstanty $a = 1$, $b = 4$. Dané rovnici s počátečními podmínkami tedy vyhovuje posloupnost

$$(-1)^n + 4\left(\frac{1}{2}\right)^n + 1.$$

□

3.10. Příklad. *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 z kořenů charakteristického polynomu dané rovnice. Charakteristická rovnice je

$$x^4 - x^3 + x^2 - x + 1 = 0.$$

Jedná se o reciprokou rovnici (to znamená, že koeficienty u $(n-k)$-té a k-té mocniny x, $k = 1, \dots, n$, jsou shodné). 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

$$x_{1,2,3,4} = \frac{1 \pm 5 \pm \sqrt{-10 \pm 2\sqrt{5}}}{4}.$$

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 charakteristikého polynomu jsou čísla $x_{1,2} = \cos(\frac{\pi}{5}) \pm \sin(\frac{\pi}{5})$ a $x_{3,4} = \cos(\frac{3\pi}{5}) \pm \sin(\frac{3\pi}{5})$. Tedy reálnou bází prostoru řešení dané diferenční rovnice je například báze posloupností $\cos(\frac{n\pi}{5})$, $\sin(\frac{n\pi}{5})$, $\cos(\frac{3n\pi}{5})$ a $\sin(\frac{3n\pi}{5})$, což jsou siny a cosiny argumentů příslušných mocnin kořenů charakteristického polynomu.

Všimněme si, že jsme mimochodem odvodili algebraické výrazy pro $\cos(\frac{\pi}{5}) = \frac{1+\sqrt{5}}{4}$, $\sin(\frac{\pi}{5}) = \frac{\sqrt{10-2\sqrt{5}}}{4}$, $\cos(\frac{3\pi}{5}) = \frac{\sqrt{5}-1}{4}$ a $\sin(\frac{3\pi}{5}) = \frac{\sqrt{10+2\sqrt{5}}}{4}$. □

2.39

3.11. Lineární filtry. Uvažujme nyní nekonečné posloupnosti

$$x = \dots, x_{-n}, x_{-n+1}, \dots, x_{-1}, x_0, x_1, \dots, x_n, \dots$$

a operaci T, která zobrazí posloupnost x na posloupnost $z = Tx$ se členy

$$z_n = a_1 x_n + a_2 x_{n-1} + \dots + a_k x_{n-k+1}.$$

Protože nekonečné posloupnosti x umíme sčítat i násobit skaláry po složkách, jedná se opět o příklad vektorového prostoru. Zjevně má dimenzi nekonečnou.

Posloupnosti můžeme chápat jako diskrétní hodnoty nějakého signálu, odečítané zpravidla ve velmi krátkých časových jednotkách, operace T je pak filtrem, který signál zpracovává. Z definice je zřejmé, že periodické posloupnosti x_n splňující pro nějaké pevné přirozené číslo p

$$x_{n+p} = x_n$$

budou mít i periodické obrazy $z = Tx$

$$\begin{aligned} z_{n+p} &= a_1 x_{n+p} + a_2 x_{n-1+p} + \dots + a_k x_{n-k+1+p} \\ &= a_1 x_n + a_2 x_{n-1} + \dots + a_k x_{n-k+1} = z_n \end{aligned}$$

se stejnou periodou p. Pro pevně zvolenou operaci T nás bude zajímat, které vstupní posloupnosti zůstanou přibližně stejné (případně až na násobek) a které budou utlumeny na nulové hodnoty.

Jde nám tedy v první řadě o vyčíslení jádra našeho lineárního zobrazení T. To je ale dáno homogenní diferenční rovnicí

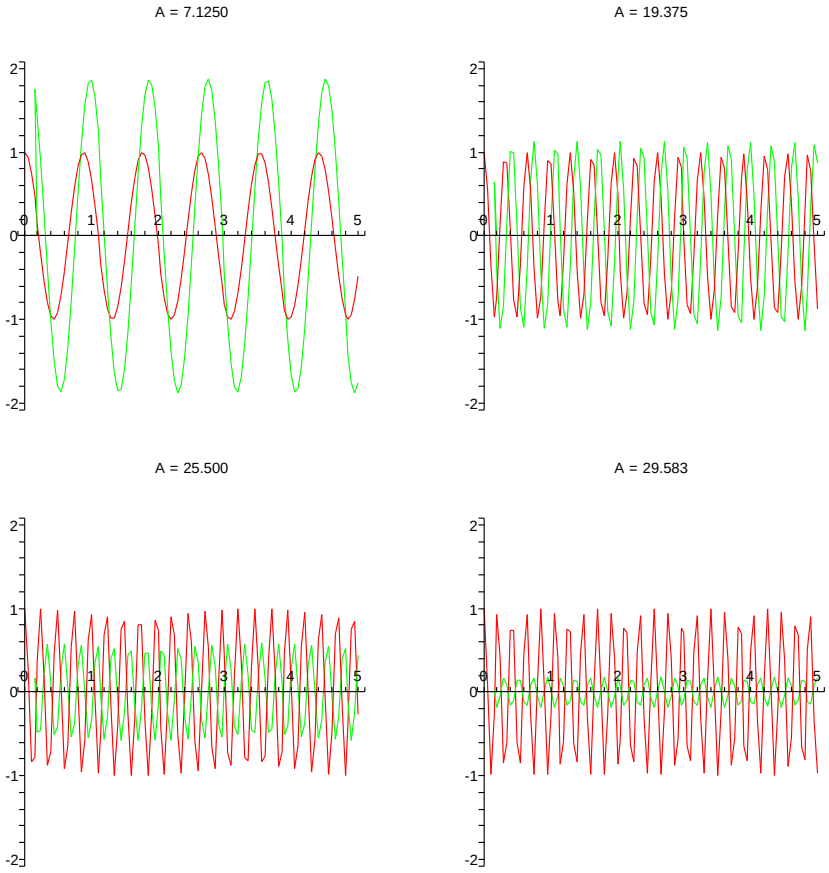
$$a_0 x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = 0, \quad a_0 \neq 0 \quad a_k \neq 0.$$

2.42

3.12. Špatný equalizer. Jako příklad uvažujme 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 $x_n = \cos(\varphi n)$. Červený je původní signál, zelený je výsledek po zpracování filtrem. Nerovnoměrnosti křivek jsou důsledkem nepřesného kreslení, oba signály jsou samozřejmě rovnoměrnými sinusovkami.



Všimněme si, že v oblastech, kde je výsledný signál přibližně stejně silný jako původní, dochází k dramatickému posuvu fáze signálu. Levné equalizery skutečně podobně špatně fungují.

Výsledek lze samozřejmě podrobně spočítat výše uvedenou metodikou.

3. Markovovy procesy

2.43

3.13. Markovovy řetězce. Velice častý a zajímavý případ lineárních procesů je popis systému, který se může nacházet v m různých stavech s různou pravděpodobností. V jistém okamžiku je ve stavu s pravděpodobností a_i pro stav 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 $x_n = (a_1, \ldots, a_m)$. 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, budou všechny sloupce matice T tvořeny také pravděpodobnostními vektory. Takovému procesu říkáme *Markovův proces*. Všimněme si, že každý pravděpodobnostní vektor x je opět zobrazen na vektor se součtem souřadnic jedna:

$$\sum_{i,j} t_{ij}x_j = \sum_j (\sum_i t_{ij})x_j = \sum_j x_j = 1.$$

Protože je součet řádků matice T vždy roven vektoru $(1, \ldots, 1)$, bude jednička zaručeně vlastním číslem matice T a k ní musí existovat vlastní vektor x_0. Abychom mohli podrobněji pochopit chování Markovových procesů, uvedeme si docela snadno pochopitelné obecné tvrzení o maticích, tzv. Perronovu–Frobeniovu větu. Její důkaz však uvádět nebudeme.

Věta. *Nechť A je reálná čtvercová matice dimenze m s kladnými prvky. Pak platí*

(1) *existuje reálné vlastní číslo λ_m matice A takové, že pro všechna ostatní vlastní čísla λ platí $|\lambda| < \lambda_m$,*
(2) *vlastní číslo λ_m má algebraickou násobnost jedna,*
(3) *vlastní podprostor odpovídající λ_m obsahuje vektor se všemi souřadnicemi kladnými*
(4) *platí odhad* $\min_i \sum_j a_{ij} \leq \lambda_m \leq \max_i \sum_j a_{ij}$.

Tvrzení bezezbytku platí i pro tzv. regulární matice, tj. takové, jejichž nějaká mocnina má výhradně kladné prvky.

Důsledkem této věty pro Markovovy procesy s maticí, která nemá žádné nulové prvky (nebo jejíž některá mocnina má tuto vlastnost), je

- existence vlastního vektoru x_∞ pro vlastní číslo 1, který je pravděpodobnostní
- přibližování hodnoty iterací $T^k x_0$ k vektoru x_∞ pro jakýkoliv pravděpodobnostní vektor x_0.

První tvrzení vyplývá přímo z kladnosti souřadnic vlastního vektoru zmíněné v Perronově–Frobeniově větě, druhé pak z toho, že absolutní hodnoty všech ostatních vlastních čísel musí být ostře menší než jedna.

3.14. 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 $X_j = (p_0(j), p_1(j), p_2(j), p_3(j), p_4(j), p_5(j))$, 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 v priklání z X_j vynásobením maticí

$$A := \begin{pmatrix} 1 & 0,5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0,5 & 0 & 0 & 0 \\ 0 & 0,5 & 0 & 0,5 & 0 & 0 \\ 0 & 0 & 0,5 & 0 & 0,5 & 0 \\ 0 & 0 & 0 & 0,5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0,5 & 1 \end{pmatrix}.$$

Na začátku máme

$$X_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

po čtyřech sázkách bude situaci popisovat náhodný vektor

$$X_5 = A^4 X_1 = \begin{pmatrix} \frac{1}{8} \\ \frac{3}{16} \\ 0 \\ \frac{5}{16} \\ 0 \\ \frac{3}{8} \end{pmatrix},$$

tedy pravděpodobnost, že hra skončí do čtvté 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 absolutníhodnotě 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 pravděpodobnostího vektoru tvaru $(a,0,0,0,0,1-a)$, kde hodnota a závisí na počtu krémrolí, se kterými hráč začíná. V našem případě je to $a = 0,4$, kdyby začal se 4 krémrolemi, bylo by to $a = 0,2$ atd. □

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 *Uvažte tuto úlohu jako Markovův proces a napište jeho matici.*

Řešení.

$$\begin{pmatrix} 1 & a & a & a & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 \\ 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & b & 1 \end{pmatrix},$$

kde $a = \frac{19}{37}$ a $b = \frac{18}{37}$. □

3.15. Příklad. 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}.

Řešení. Hra skončí po třech sázkách. Jsou tedy všechny mocniny A, počínaje A^3 shodné.

$$\begin{pmatrix} 1 & 7/8 & 3/4 & 1/2 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1/8 & 1/4 & 1/2 & 1 \end{pmatrix}$$

□

3.16. 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.*

Řešení.

$$\begin{pmatrix} \frac{5}{6} & \frac{1}{5} \\ \frac{1}{6} & \frac{4}{5} \end{pmatrix}.$$

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. □

4. Více maticového počtu

Na vcelku praktických příkladech jsme viděli, že porozumění vnitřní struktuře matic a jejim 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.

2.44

3.17. Invariantní podprostory. Mějme nějaké lineární zobrazení $f : V \to V$ na vektorovém prostoru V a předpokládejme, že pro nějaký podprostor $W \subset V$ platí $f(W) \subset W$. Říkáme, že W je *invariantní podprostor* pro zobrazení f. Jestliže je V konečněrozměrné a vybereme nějakou bázi $(u_1, \dots, u_k)$ podprostoru W, můžeme ji vždy doplnit na bázi $(u_1, \dots, u_n)$ celého V a v každé takové bázi má naše zobrazení matici A tvaru

e2.3 (3.1)
$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

kde B je čtvercová matice dimenze k, D je čtvercová matice dimenze $n - k$ a C je matice typu $n/(n-k)$. Naopak, jestliže existuje v nějaké bázi matice zobrazení f tvaru (3.1), je $W = \langle u_1, \dots, u_k \rangle$ invariantní podprostor zobrazení f.

Extrémní případy jsme viděli v odstavcích 2.40–2.45, kde jsme zkoumali vlastní vektory. Ke každému vlastnímu číslu zobrazení (resp. matice) existoval vlastní vektor a jím generovaný jednorozměrný podprostor je samozřejmě invariantní. V případě existence n různých vlastních čísel zobrazení f jsme dostali rozklad V na přímý součet n vlastních podprostorů a v bazích z vlastních vektorů má naše zobrazení diagonální tvar s vlastními čísly na diagonále. Zároveň jsme viděli dva různé příklady důvodů, proč zobrazení diagonální matici mít nemusí. První souvisel s nilpotentními zobrazeními, druhý s rotacemi v dvourozměrných podprostorech.

Nejsložitější a úplně obecný popis jsme potkali v odstavci 2.45, kde jsme pouze s mlhavým náznakem důkazu uvedli větu o Jordanově rozkladu. Ta říká, že nad algebraicky uzavřeným polem skalárů se celý prostor vždy rozloží na invariantní podprostory na kterých je zobrazení dáno tzv. Jordanovými bloky. Budeme teď pracovat se speciálními typy zobrazení, jejichž struktura je daleko jednodušší. První budou na řadě ortogonální zobrazení.

2.45

3.18. Rozklad ortogonálního zobrazení. Zkoumejme zobrazení na vektorovém prostoru V se skalárním součinem. Uvažme pevně zvolené ortogonální zobrazení $f : V \to V$ s maticí A v nějaké ortonormální bázi a zkusme postupovat obdobně jako s rotací v příkladu 2.39.

Nejprve se ale podívejme obecně na invariantní podprostory ortogonálních zobrazení a jejich ortogonální doplňky. Jestliže pro libovolný podprostor $W \subset V$ a ortogonální zobrazení $f : V \to V$ platí $f(W) \subset W$, 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 $f(W^\perp) \subset W^\perp$. 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 zorbazení reálná. Musíme si proto pomoci opět výletem do komplexnívh vektorových prostorů.

Jestliže budeme považovat matici A za matici lineárního zobrazení na komplexním prostoru $\mathbb{C}^n$ (která je jen shodou okolností reálná), budeme mít právě n kořenů charakteristického polynomu, včetně jejich algebraické násobnosti. Navíc, protože charakteristický polynom zobrazení bude mít výhradně reálné koeficienty, budou tyto kořeny buď reálné, nebo půjde o dvojice komplexně sdružených kořenů λ a $\bar\lambda$. Příslušné vlastní vektory v $\mathbb{C}^n$ k takové dvojici vektorů budou také komplexně sdružené, protože budou řešením dvou komplexně sdružených systémů lineárních rovnic.

Označme v_λ, stejně jako v případě rotace v 2.39, vlastní vektor příslušný k vlastnímu číslu $\lambda = \alpha + i\beta$, $\beta \neq 0$. Reálný vektorový podprostor P_λ generovaný reálnou a imaginární částí $x_\lambda = \operatorname{re} v_\lambda$, $y_\lambda = \operatorname{im} v_\lambda$ je zjevně invariantní vůči násobení maticí A a dostáváme

$$A \cdot x_\lambda = \alpha x_\lambda - \beta y_\lambda,\ A \cdot y_\lambda = \alpha y_\lambda + \beta x_\lambda.$$

To ale neznamená nic jiného, než že zúžení našeho zobrazení na P_λ je dáno složením rotace o argument vlastní honoty λ (úhel $\arccos \frac{\alpha}{\sqrt{\alpha^2+\beta^2}}$) s násobením velikostí vlastní hodnoty λ (skalárem $\sqrt{\alpha^2+\beta^2}$). Protože naše zobrazení zachovává velikosti, musí být velikost vlastní hodnoty λ rovna jedné.

Společně s předchozími úvahami jsme tedy dokázali úplný popis všech 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 λ. Všechny tyto různé podprostory jsou po dvou ortogonální.*

Příklad. Zkusme si předchozí větu na příkladu v dimenzi tři. Charakteristický polynom v tomto případě musí mít alespoň jeden reálný kořen, kterým musí být buď jednička nebo mínus jednička. Další dva musí být opět ± 1 nebo dva komplexně sdružené nereálné. V posledním případě zadává vlastní vektor odpovídající reálnému vlastnímu číslu osu rotace o argument vlastního čísla druhého. Pokud je reálné vlastní číslo -1, bude navíc ještě uplatněno zrcadlení podle roviny rotace.

Uvažme tedy zobrazení s maticí ve standardní bázi

$$f : \mathbb{R}^3 \to \mathbb{R}^3,\ A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}.$$

Dostaneme polynom $-\lambda^3 + \lambda^2 - \lambda + 1 = -(\lambda - 1)(\lambda^2 + 1)$ s kořeny $\lambda_1 = 1$, $\lambda = i$ a $\bar\lambda = -i$. Pochopitelně matice zadává rotaci o devadesát stupňů podle osy y.

2.46

3.19. Symetrická zobrazení. Uvažujme opět reálný vektorový prostor V se skalárním součinem. Zobrazení $f : V \to V$ se nazývá *symetrické*, jestliže pro všechny vektory $u, v \in V$ platí

$$\langle f(u), v\rangle = \langle u, f(v)\rangle.$$

V libovolné ortonormální bázi můžeme předchozí vztah v souřadnicích vyjádřit takto:

$$(A \cdot x)^T \cdot y = x^T \cdot (A \cdot y) = x^T \cdot (A^T y).$$

Volbou souřadnic bázových vektorů (tj. jedna jednička a zbytek nuly) se dostaneme ke vztahům $a_{ij} = a_{ji}$ pro jednotlivé komponenty matice A, tzn. ke vztahu $A = A^T$. Dokázali jsme tedy souřadný popis symetrických zobrazení:

Tvrzení. *Zobrazení $f : V \to V$ na vektorovém prostoru se skalárním součinem je symetrické právě tehdy, když v některé (a pak už všech) ortonormální bázi má symetrickou matici.*

3.15

3.20. Adjungovaná zobrazení. Jestliže zvolíme pevně jeden vektor $v \in V$, dosazování vektorů za druhý argument nám dává zobrazení $V \to V^* = \mathrm{Hom}(V, \mathbb{R})$

$$V \ni v \mapsto (w \mapsto \langle v, w\rangle \in \mathbb{R}).$$

Podmínka nedegenerovanosti skalárního součinu nám zaručuje, že toto zobrazení je bijekcí. Na první pohled je vidět, že vektory ortonormální báze jsou zobrazeny na formy tvořící bázi duální.

Každé zobrazení $f : V \to W$ mezi vektorovými prostory zadává tzv. duální zobrazení $f^* : W^* \to V^*$ mezi formami, definované pro všechny $w^* \in W^*$, $v \in V$ pomocí

$$f^*(w^*)(v) = w^*(f(v)).$$

V libovolných bazích na V a W a jejich duálních bazích na V^* a W^* pak tentýž definiční vztah má tvar (píšeme A^* pro matici zobrazení f^*, x^T jsou souřadnice formy w^*, y jsou souřadnice vektoru v)

$$(A^* x^T) \cdot y = x^T \cdot (A \cdot y)$$

a vidíme, že duální zobrazení má v duálních bazích transponovanou matici k maticí zobrazení původního.

V případě vektorových prostorů se skalárním součinem, převádí výše uvedené bijekce duální zobrazení f^* na tobrazení $f^* : W \to V$ zadané formulí

$$\langle f(u), v\rangle = \langle u, f^*(v)\rangle$$

a tomuto zobrazení se říká *adjungované zobrazení* k f. Předchozí výpočet v souřadnicích pro symetrická zobrazení nám ve skutečnosti sdělil, že je-li A matice zobrazení f v ortonormální bázi, pak matice adjungovaného zobrazení f^* je matice transponovaná A^T. Můžeme proto také přeformulovat definici takto: Symetrické je takové zobrazení $f : V \to V$, které je rovno svému adjungovanému zobrazení f^*. Často se takovým zobrazením také proto říká *samoadjungovaná*.

2.47

3.21. Spektrální rozklad symetrického zobrazení. Uvažujme symetrické zobrazení $f : V \to V$ s maticí A v nějaké ortonormální bázi a zkusme postupovat obdobně jako v 3.18. Opět se nejprve obecně podíváme na invariantní podprostory ortogonálních zobrazení a jejich ortogonální doplňky. Jestliže pro libovolný podprostor $W \subset V$ a symetrické zobrazení $f : V \to V$ platí $f(W) \subset W$, pak také platí pro všechny $v \in W^\perp$, $w \in W$

$$\langle f(v), w\rangle = \langle v, f(w)\rangle = 0.$$

To ale znamená, že také $f(W^\perp) \subset W^\perp$.

Představme si dále, že A je matice symetrického zobrazení a $A \cdot x = \lambda x$ pro nějaký komplexní vektor $x \in \mathbb{C}^n$. Rozšíříme si definici skalárního součinu $\langle\ ,\ \rangle$ na $\mathbb{C}^n$ vztahem

$$\langle x, y\rangle = x^T \cdot \bar{y}$$

kde $\bar{y}$ je vektor v $\mathbb{C}^n$ s komplexně konjugovanými souřadnicemi. Zjevně platí i pro rozšířené zobrazení $x \mapsto A \cdot x$ vztah

$$\langle A \cdot x, y\rangle = \langle x, A \cdot y\rangle$$

a pro náš vlastní vektor x tedy dostáváme

$$\lambda\langle x, x\rangle = \bar{\lambda}\langle x, x\rangle.$$

Kladným reálným číslem $\langle x, x\rangle$ můžeme krátit a proto musí být $\bar{\lambda} = \lambda$, tj. vlastní čísla jsou skutečně 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 symetrické zobrazení je také invariantní. Navíc jsou všechna vlastní čísla symetrické matice A reálná.*

Ze samotné definice je zřejmé, že zúžení symetrického zobrazení na invariantní podprostor je opět symetrické. Předchozí tvrzení nám tedy zaručuje, 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. Vlastní

vektory příslušející různým vlastním číslům jsou navíc kolmé, protože z rovností $f(u) = \lambda u$, $f(v) = \mu v$ vyplývá

$$\lambda\langle u, v\rangle = \langle f(u), v\rangle = \langle u, f(v)\rangle = \mu\langle u, v\rangle.$$

Obvykle se náš výsledek formuluje pomocí projekcí na vlastní podprostory. O projektoru $P : V \to V$ říkáme, že je *kolmý*, je-li $\operatorname{Im} P \perp \operatorname{Ker} P$. Dva kolmé projektory P, Q jsou *vzájemně kolmé*, je-li $\operatorname{Im} P \perp ImQ$.

3.17 **3.22. Věta.** *Pro každé symetrické zobrazení $f : V \to V$ na vektorovém prostoru se skalárním součinem existuje ortonormální báze z vlastních vektorů. Jsou-li $\lambda_1, \dots, \lambda_k$ všechna různá vlastní čísla f a $P_1, \dots, P_k$ příslušné kolmé a navzájem kolmé projektory na vlastní podprostory, pak*

$$f = \lambda_1 P_1 + \cdots + \lambda_k P_k.$$

Poznámka. Všechna zobrazení, pro která lze najít ortonormální bázi jako v této větě o spektrálním rozkladu se nazývají *normální*. Lze poměrně snadno ukázat, že zobrazení $f : V \to V$ je normální právě, když komutuje se svým adjungovaným zobrazením. Stopa zobrazení $f^* \circ f$ je rovna součtu absolutních hodnot kvadrátů všech prvků A. V bázi z předchozí věty je tento výraz ovšem roven součtu kvadrátů absolutních hodnot všech vlastních čísel λ_i matice A. Rovnost

$$\sum_{i,j} |a_{ij}|^2 = \sum_i |\lambda_i|^2$$

v některé a pak už ve všech ortonormálních bazích je nutnou a dostatečnou podmínkou pro to, aby zobrazení f bylo normální. Důkaz nebudeme uvádět.

2.48 **3.23. 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 $B = A^T \cdot A$ (tj. složení zobrazení $f^* \circ f$):

$$\langle B \cdot x, x\rangle = \langle A^T \cdot A \cdot x, x\rangle = \langle A \cdot x, A \cdot x\rangle \geq 0$$

pro všechny vektory x. Navíc zjevně

$$B^T = (A^T \cdot A)^T = A^T \cdot A = B.$$

Symetrickým maticím B s takovou vlastností říkáme *nezáporné* a pokud nastane nulová hodnota pouze pro $x = 0$, pak jim říkáme *kladné*. Obdobně hovoříme o *kladných* a *nezáporných* zobrazeních $f : V \to V$.

Pro každé nezáporné zobrazení $f : V \to V$ umíme najít jeho odmocninu, tj. zobrazení g takové, že $g \circ g = f$. Nejjednodušeji to uvidíme v ortonormální bázi, ve které bude mít f diagonální matici. Taková podle našich předchozích úvah vždy existuje a matice A zobrazení f v ní bude mít na diagonále nezáporná reálná vlastní čísla zobrazení f. Kdyby totiž bylo některé z nich záporné, nebyla by splněna podmínka nezápornosti již pro některý z bázových vektorů. Pak ovšem stačí definovat zobrazení g pomocí matice B s odmocninami příslušných vlastních čísel na diagonále.

5. Rozklady matic a pseudoinverze

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 abolutní hodnoty. V dalším textu si uvedeme stručně přehled několika takových rozkladů pro různé typy matic, které bývají nesmírně užitečné při numerických výpočtech s maticemi. Ve skutečnosti jsme příslušný rozklad pro nezáporné symetrické matice využili v předchoyím odstavci pro konstrukci odmocniny z matice.

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 zpravovávaným. Předpokládejme pro jednoduchost, že naše matice A je čtvercová a že má všechny hlavní minory nenulové. Pak se nemůže stát, že bychom potřebovali při Gausově eliminaci přehazovat řádky a všechny naše matice P_i mohou být dolní trojúhelníkové s jedničkami na diagonálách (nikdy nepotřebujeme přehaovat řádky). 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 Gausově eliminaci na řádkově schodovitý tvar potřebovat navíc permutace řádků, někdy i sloupců matice. Pak dostáváme obecněji $A = P \cdot L \cdot U \cdot Q$, kde P a Q jsou nějaké permutační matice.

Přímým důsledkem Gausovy 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 nulovými bloky všude kolem. To lze přeformulovat takto: Každou matici A typu m/n nad polem skalárů $\mathbb{K}$ lze rozložit na součin

$$A = P \cdot \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix} \cdot Q.$$

Pro čtvercové matice jsme v 2.46 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. Všimněme si, že násobení maticí P a její inverzí z opačných stran odpovídá v tomto případě právě změně báze na vektorovém prostoru V.

Obdobně, pro symetrické matice jsme dokázali, že jdou rozložit na součin

$$A = P \cdot B \cdot P^T,$$

kde B je diagonální matice se všemi (vždy reálnými) vlastními čísly na diagonále, včetně násobností. Zde jde také o součin s maticemi vystihující změnu báze, nicméně připouštíme nyní pouze změny mezi mezi ortonormálními bazemi a proto i matice přechodu P musí být ortogonální. Odtud $P^{-1} = P^T$.

Pro 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.

2.50

3.24. Věta o singulárním rozkladu. Jestliže se omezíme na ortonormální báze, ale chceme znát více informací o struktuře obecných lineárních zobrazení, musíme postupovat o hodně rafinovaněji, než v případě bazí libovolných:

Věta. *Nechť A je reálná matice typu m/n. Pak existují čtvercové ortogonální matice U a V dimenzí m a n, a reálná diagonální matice s nezápornými prvky D dimenze r, $r \leq \min\{m,n\}$, takové, že*

$$A = USV^T, \quad S = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix},$$

kde r je hodnost matice AA^T. Přitom je S určena jednoznačně až na pořadí prvků a prvky diagonální matice D jsou druhé odmocniny vlastních čísel d_i matice AA^T.

Důkaz. Předpokládejme nejprve $m \leq n$ a označme $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ zobrazení zadané maticí A ve standardních bazích. Máme vlastně ukázat, že existují ortonormální báze na $\mathbb{R}^n$ a $\mathbb{R}^m$ ve kterých bude mít φ matici S z tvrzení věty. Jak jsme viděli výše, matice A^TA je pozitivně semidefinitní. Proto má samá reálná nezáporná vlastní čísla a existuje ortonormální báze $\underline{w}$ v $\mathbb{R}^n$, ve které má příslušné zobrazení $\varphi^* \circ \varphi$ diagonální matici s vlastními čísly na diagonále. Jinými slovy, existuje ortogonální matice V taková, že $A^TA = VBV^T$ pro reálnou diagonální 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 $B = V^TA^TAV = (AV)^T(AV)$. To je ale je ekvivalentní tvrzení, že prvních r sloupců matice AV je ortogonálních a zbývající jsou nulové, protože mají nulovou velikost. Označme prvních r sloupců $v_1, \ldots, v_r \in \mathbb{R}^m$. Tzn. $\langle v_i, v_i \rangle = d_i$, $i = 1, \ldots, r$ a tedy vektory $u_i = \frac{1}{\sqrt{d_i}} v_i$ tvoří ortonormální systém nenulových vektorů. Doplňme je na ortonormální bázi $u_1, \ldots, u_n$ celého $\mathbb{R}^m$. Vyjádříme-li zobrazení φ v bazích $\underline{w}$ na $\mathbb{R}^n$ a $\underline{u}$ na $\mathbb{R}^m$, dostáváme matici $\sqrt{B}$. Přechody od standardních bází k nově vybraným odpovídají násobení zleva ortogonálními maticemi U a zprava $V^{-1} = V^T$.

Pokud je $m > n$, můžeme aplikovat předchozí část důkazu na matici A^T. Odtud pak přímo plyne požadované tvrzení. □

Tento důkaz věty o singulárním rozkladu je konstruktivní a můžeme jej opravdu použít pro výpočet ortogonálních matic U, V a diagonálních nenulových prvků matice S.

2.51

3.25. Geometrická interpretace singulárního rozkladu. Diagonálním hodnotám matice D z předchozí věty se říká *singulární hodnoty matice A*. Pro příslušné zobrazení $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ mají jednoduchý geometrický význam: Nechť $K \subset \mathbb{R}^n$ 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.

2.52

3.26. Věta o polárním rozkladu. Uvažujme společně nad důsledky věty o singulárním rozkladu. Plyne z ní $A = USW^T$ s diagonální S s nezápornými reálnými čísly na diagonále a ortogonálními U, W. Pak $A = USU^TUW^T$ a můžeme přímo definovat $P := USU^T$, $V := UW^T$. Odtud ale vyplývá, že P symetrická a pozitivně semidefinitní zatímco V je ortogonální. Navíc $A^T = WSU^T$ a tedy $AA^T = USSU^T = P^2$.

Předpokládejme, že $A = PV = QU$ jsou dva takové rozklady a A je invertibilní. Pak ovšem je $AA^T = PVV^TP = P^2 = QUU^TQ = Q^2$ positivně definitní a proto jsou matice $Q = P = \sqrt{AA^T}$ jednoznačně určené a invertibilní. Pak také $U = V = P^{-1}A$. Odvodili jsme tedy velice užitečnou analogii rozkladu reálného čísla na znaménko (ortogonální matice v případě dimenze jedna jsou právě ± 1) a absolutní hodnotu (matice P, ke které umíme odmocninu)

Věta. *Každou čtvercovou reálnou matici A dimenze n lze vždy vyjádřit ve tvaru $A = P \cdot V$, kde P je symetrická a positivně definitní čtvercová matice téže dimenze a V je ortogonální. Přitom $P = \sqrt{AA^T}$. Je-li A invertibilní, je rozklad jednoznačný a $V = (\sqrt{AA^T})^{-1}A$.*

Když budeme tutéž větu aplikovat na A^T místo A, dostaneme tentýž výsledek, ovšem s obráceným pořadím symetrických a ortogonálních matic. Matice v příslušných pravých a levých rozkladech budou samozřejmě obecně různé.

2.53

3.27. Poznámka. V tomto textu se bohužel z nedostatku prostoru vyhýbáme komplexním maticím. Ve skutečnosti jsou pro všechny koncepty a pojmy zavedené kolem skalárních součinů také přímočaré komplexní analogie a obvyklejší postup v literatuře je, že se z výsledků pro tzv. unitární prostory, hermiteovská zobrazení, samoadjungovaná zobrazení apod. odvozují i výsledky reálné. Například věta o spektrálním rozkladu pak pracuje s maticí s pozitivně definitní samoadjungovanou maticí P, která opět hraje roli absolutní hodnoty čísla, zatímco unitární matice V je analogií argumentu komplexního čísla (tj. komplexní jednotky, která se také rozkládá na součet $\varphi + i\psi$ se samoadjungovanými φ, ψ, které navíc splňují $\varphi^2 + \psi^2 = \mathrm{id}_V$). Přitom ale nyní není jedno v jakém pořadí samoadjungované a unitární matice chceme násobit. Umíme v obou, vyjdou ale pokaždé jiné.

Pro řadu aplikací bývá rychlejší použití tzv. QR rozkladu:

2.54

3.28. Věta. *Pro každou reálnou matici A typu m/n existuje ortogonální matice Q a horní trojúhelníková matice R takové, že $A = Q^TR$.*

Důkaz. V geometrické formulaci potřebujeme dokázat, že pro každé zobrazení $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ s maticí A v standardních bazích můžeme zvolit novou bázi na $\mathbb{R}^m$ tak, aby potom φ mělo horní trojúhelníkovou matici.

Uvažme obrazy $\varphi(e_1), \dots, \varphi(e_n) \in \mathbb{R}^m$ vektorů standardní báze, vyberme z nich maximální lineárně nezávislý systém $v_1, \dots, v_k$ takovým způsobem, že vypouštěné závislé vektory jsou vždy lineární kombinací předchozích vektorů, a doplňme jej do báze $v_1, \dots, v_m$. Nechť $u_1, \dots, u_m$ je ortonormální báze vzniklá Gramm-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 $v_1, \dots, v_{i-1}$, proto ve vyjádření $\varphi(e_i)$ v bázi $\underline{u}$ vystupují pouze vektory $u_1, \dots, u_i$. Zobrazení φ má proto ve standardní bázi na $\mathbb{R}^n$ a ortonormální bázi $\underline{u}$ na $\mathbb{R}^m$ horní trojúhelníkovou matici R. Přechod k bázi $\underline{u}$ na $\mathbb{R}^m$ odpovídá násobení ortogonální maticí Q, tj. $R = QA$, ekvivalentně $A = Q^TR$. □

Závěrem této části textu si všimněme mimořádně užitečné a důležité aplikace našich výsledků pro přibližné numerické výpočty. Opět uvádíme pro jednoduchost pouze reálnou variantu, obdobně platí a dokazuje se i varianta komplexní.

2.55 **3.29. Definice.** Nechť A je reálná matice typu m/n a nechť$A = USV^T$ je její singulární rozklad, $S = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$. Matici $A^{(-1)} := VS'U^T$ s $S' = \begin{pmatrix} D^{-1} & 0 \\ 0 & 0 \end{pmatrix}$ nazýváme *pseudoinverzní matice* k matici A.

Jak ukazuje následující věta, je pseudoinverze důležité zobecnění pojmu inverzní matice.

2.56 **3.30. Věta.** *Nechť A je reálná matice typu m/n. Platí*

(1) *Je-li A invertibilní (zejména tedy čtvercová), pak*

$$A^{(-1)} = A^{-1}.$$

(2) *pro pseudoinverzi $A^{(-1)}$ platí, že $A^{(-1)}A$ i $AA^{(-1)}$ jsou symetrické a*

$$AA^{(-1)}A = A, \quad A^{(-1)}AA^{(-1)} = A^{(-1)}.$$

(3) *Uvažme pro danou matici A systém lineárních rovnic $Ax = b$, $b \in R^m$. Pak $y = A^{(-1)}b \in \mathbb{R}^n$ minimalizuje vzdálenost $\|Ax - b\|$ pro všechny $x \in \mathbb{R}^n$.*

Důkaz. (1): Je-li A invertibilní, pak i $S = U^TAV$ je invertibilní a přímo z definice je $S' = S^{-1}$. Odtud $A^{(-1)}A = AA^{(-1)} = E$.

(2): Přímým výpočtem dostáváme $SS'S = S$ a $S'SS' = S'$, proto

$$AA^{(-1)}A = USV^TVS'U^TUSV^T = USS'SV^T = USV^T = A$$

a analogicky pro druhou rovnost. Dále

$$(AA^{(-1)})^T = (USS'U^T)^T = U(S')^TS^TU^T = U(SS')^TU^T = USS'U^T = AA^{(-1)}$$

a podobně se ukáže $(A^{(-1)}A)^T = A^{(-1)}A$.

(3): Uvažme zobrazení $\varphi : \mathbb{R}^n \to \mathbb{R}^m$, $x \mapsto Ax$, a přímé součty $\mathbb{K}^n = (\operatorname{Ker}\varphi)^\perp \oplus \operatorname{Ker}\varphi$, $\mathbb{R}^m = \operatorname{im}\varphi \oplus (\operatorname{im}\varphi)^\perp$. 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 φ matici S a $\tilde{\varphi}$ matici D z věty o singulárním rozkladu. Pro dané $b \in \mathbb{R}^m$ je bod $z \in \operatorname{im}\varphi$ minimalizující vzdálenost $\|b - z\|$ (tj. realizující vzdálenost od podprostoru $\rho(b, \operatorname{Im}\varphi)$) 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 $\varphi^{(-1)}$, původně zadané ve standardních bazích pseudoinverzí $A^{(-1)}$, dáno maticí S' z věty o singulárním rozkladu, zejména je $\varphi^{(-1)}(\operatorname{Im}\varphi) = (\operatorname{Ker}\varphi)^\perp$ a D^{-1} maticí zúžení $\varphi^{(-1)}_{|\operatorname{Im}\varphi}$ a $\varphi^{(-1)}_{|(\operatorname{Im}\varphi)^\perp}$ je nulové. Je tedy skutečně

$$\varphi \circ \varphi^{(-1)}(b) = \varphi(\varphi^{(-1)}(z)) = z$$

a důkaz je ukončen. □

Lze také ukázat, že matice $A^{(-1)}$ minimalizuje výraz $\|AA^{(-1)} - E\|^2$ (tj. sumu kvadrátů všech prvků uvedené matice).

2.57

3.31. 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 je větší než n.

Např. máme experimentem dáno mnoho naměřených 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 $a_{ij} = f_i(y_j)$ a naším úkolem je tedy určit koeficienty $x_j \in \mathbb{R}$ tak, aby $\sum_{i=1}^{m}(b_i - (\sum_{j=1}^{n} x_j a_{ij}))^2$ byla minimální. Jinými slovy, hledáme lineární kombinaci funkcí f_i takovou, abychom "dobře" proložili zadané hodnoty b_i. Díky předchozí větě jsou hledané optimální koeficienty $A^{(-1)}b$.

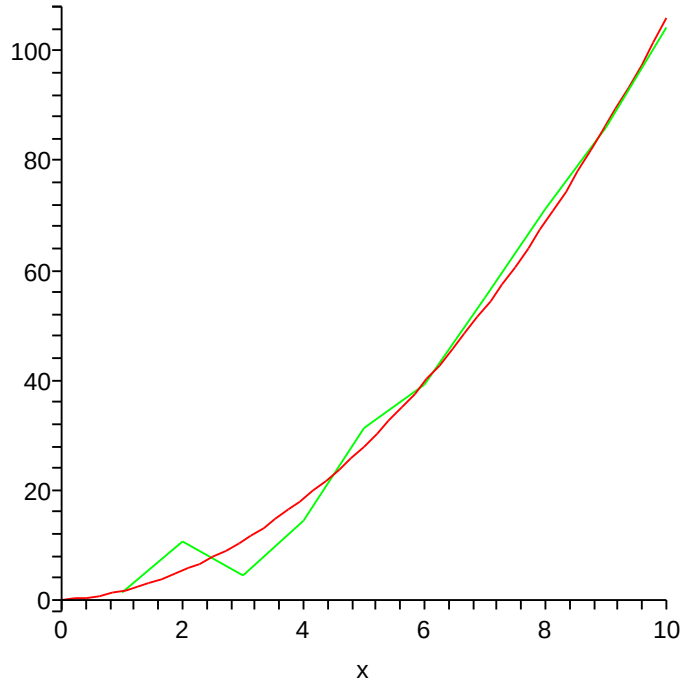
Abychom měli konkrétnější představu, uvažujme pouze dvě funkce $f_1(x) = x$, $f_2(x) = x^2$ a předpokládejme, že „naměřené hodnoty“ jejich neznámé kombinace $g(x) = y_1x + y_2x^2$ v celočíselných hodnotách pro x mezi 1 a 10 jsou

$$b^T = (1.44\ 10.64\ 4.48\ 14.56\ 31.12\ 39.20\ 54.88\ 71.28\ 85.92\ 104.16).$$

Tento vektor vzniknul výpočtem hodnot $x + x^2$ v daných bodech posunutých o náhodné hodnoty v rozmezí ± 8. Matice $B = (b_{ij})$ je tedy v našem případě rovna

$$B^T = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 9 & 16 & 25 & 36 & 49 & 64 & 91 & 100 \end{pmatrix}$$

a $y = B^{(-1)} \cdot b = (0.61, 0.99)$. Výsledné proložení je možné dobře vidět na obrázku, kde zeleně jsou proloženy zadané hodnoty b lomenou čarou, zatímco červený je graf příslušné kombinace g. Výpočty byly provedeny v systému Maple pomocí příkazu *leastsqrs(B,b)*.



Pokud jste spřáteleni s Maplem (nebo jiným podobným souftwarem), zkuste si zaexperimentovat s podobnými úlohami.

KAPITOLA 4

Analytická geometrie

poloha, incidence, projekce?
– a zase skončíme u matic...

1. Afinní geometrie

Vrátíme se teď k úlohám elementární geometrie z podobného pohledu, jako když jsme zkoumali polohy bodů v rovině v 5. části první kapitoly, viz 1.33. Motivací k abstraktní definici vektorového prostoru nám byly množiny řešení systémů lineárních diferenciálních rovnic s nulovou pravou stranou, kde součty i skalární násobky řešení byly opět řešeními, „dimenzi“ celého prostoru řešení ale určoval rozdíl mezi počtem proměnných a počtem nezávislých rovnic. Taková dimenze bývá výrazně menší než počet proměnných a už proto není ideální pracovat s vektory jen jako s n–ticemi skalárů. Když jsme pak zkoumali aplikace obecné teorie na systémy rovnic v první části předchozí kapitoly, zjistili jsme v ostavci 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 homogenní. Obdobně se chovají lineární diferenční rovnice, viz 3.6.

Návod na teoretické uchopení takové situace jsme viděli už při diskusi geometrie roviny, viz odstavec 1.34 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 dvěmi souřadnicemi. Prametricky 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.

2.58

4.1. Afinní prostory. *Standarní afinní prostor* $\mathcal{A}_n$ je množina všech bodů v $\mathbb{R}^n$ spolu s operací, kterou k bodu $A = (a_1, \dots, a_n) \in \mathcal{A}_n$ a vektoru $v = (v_1, \dots, v_n) \in \mathbb{R}^n$ přiřadíme bod $A + v = (a_1 + v_1, \dots, a_n + v_n) \in \mathbb{R}^n$. Tyto operace splňují následující tři vlastnosti:

(1) $A + 0 = A$ pro všechny body $A \in P$ a nulový vektor $0 \in V$
(2) $A + (v + w) = (A + v) + w$ pro všechny vektory $v, w \in V$, $A \in P$
(3) pro každé dva body $A, B \in P$ existuje právě jeden vektor $v \in P$ takový, že $A + v = B$. Značíme jej $B - A$, někdy také $\vec{AB}$.

Vektorový prostor $\mathbb{R}^n$ nazýváme *zaměření 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 $\mathbb{R}^n$. 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 $\mathbb{R}^n$? Je to patrně podstatný formální krůček pro pochopení geometrie v $\mathbb{R}^n$: Geometrické objekty jako jsou 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. Musíme ale mít možnost říci, co je to „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.

Definice. Afinním prostorem $\mathcal{A}$ se zaměřením V rozumíme množinu *bodů* P, spolu se zobrazením $P \times V \to P$, $(A, v) \mapsto A+v$, splňující vlastnosti (1)–(3). Pro libovolný pevně zvolený vektor $v \in V$ je tak definována *translace* $\tau_v : \mathcal{A} \to \mathcal{A}$ jako zúžené zobrazení

$$\tau_v : P \simeq P \times \{v\} \to P, \quad A \mapsto A + v.$$

Dimenzí afinního prostoru $\mathcal{A}$ rozumíme dimenzi jeho zaměření.

Nadále nebudeme rozlišovat $\mathcal{A}$ a P v označení. Z axiomů okamžitě plyne pro libovolné body A, B, C v afinním prostoru $\mathcal{A}$

$$A - A = 0 \in V \tag{4}$$

$$B - A = -(A - B) \tag{5}$$

$$(B - A) + (C - B) = (C - A). \tag{6}$$

(Dokažte si podrobně formálně sami!)

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 bazí zaměření $\underline{u}$. Hovoříme 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 n-rozměrný afinní prostor $\mathcal{A}$ se standardním afinním prostorem $\mathcal{A}_n$.

2.59

4.2. 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.

Definice. Neprázdná podmnožina $\mathcal{Q} \subset \mathcal{A}$ afinního prostoru $\mathcal{A}$ se zaměřením V se nazývá *afinní podprostor* v $\mathcal{A}$, je-li podmnožina $W = \{B - A; A, B \in \mathcal{Q}\} \subset V$ vektorovým podprostorem a pro libovolné $A \in \mathcal{Q}$, $v \in W$ je $A + v \in \mathcal{Q}$.

Skutečně je rozumné mít obě podmínky v definici, protože je snadné najít příklady podmnožin, které budou splňovat první, ale nikoliv druhou. Přemýšlejte např. o přímce v rovině s vyjmutým jedním bodem.

Pro libovolnou množinu bodů $M \subset \mathcal{A}$ v afinním prostoru se zaměřením V definujeme vektorový podprostor

$$Z(M) = \langle \{B - A; B, A \in M\} \rangle \subset V.$$

Zejména je $V = Z(\mathcal{A})$ a každý afinní podprostor $\mathcal{Q} \subset \mathcal{A}$ splňuje sám axiomy afinního prostoru se zaměřením $Z(\mathcal{Q})$.

Přímo z definic je 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 $M \subset \mathcal{A}$ je průnikem všech afinních podprostorů, které obsahují všechny body podmnožiny M.

Přímo z definic plyne, že pro kterýkoliv bod $A_0 \in M$ je $\langle M \rangle = \{A_0 + v; v \in Z(M) \subset Z(\mathcal{A})\}$, 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 bodů A s vektory v U je afinní podprostor. Takový postup vede k pojmu parametrizace podprostorů:

Nechť $\mathcal{Q} = A + Z(\mathcal{Q})$ je afinní podprostor v $\mathcal{A}_n$ a $(u_1, \dots, u_k)$ je báze $Z(\mathcal{Q}) \subset \mathbb{R}^n$. Pak vyjádření podprostoru

$$\mathcal{Q} = \{A + t_1 u_1 + \cdots + t_k u_k; t_1, \dots, t_k \in \mathbb{R}\}$$

nazýváme *parametrický popis* podprostoru $\mathcal{Q}$. Jeho zadání systémem rovnic v daných souřadnicích je *implicitní popis* podprostoru $\mathcal{Q}$.

2.60 **4.3. Příklady afinních prostorů.** (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 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 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 kodimenze 1), tj. tzv. *nadrovina v* A_n.

Poslední příklad je zvláštním případem následující obecné věty popisující geometrickou podstatu systémů lineárních rovnic.

2.61 **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 $\alpha_i(x) = b_i$, $b_i \in \mathbb{R}$, $i = 1, \dots, n-k$. Je-li $A = (a_1, \dots, a_n)^T \in \mathbb{R}^n$ libovolné pevně zvolené řešení tohoto (nehomogenního) systému rovnic a je-li $U \subset \mathbb{R}^n$ vektorový podprostor všech řešení zhomogenizovaného systému $\alpha_i(x) = 0$, pak dimenze U je k a podmnožina všech řešení daného systému je tvaru $\{B; B = A + (y_1, \dots, y_n)^T, y = (y_1 \dots, y_n)^T \in U\} \subset \mathbb{R}^n$, viz. 3.1. Příslušný afinní podprostor je tím popsán parametricky ve výchozích souřadnicích $(A_0; \underline{u})$.

Naopak, uvažme libovolný afinní podprostor $\mathcal{Q} \subset \mathcal{A}_n$ a zvolme nějaký jeho bod B za počátek afinního souřadného systému $(B, \underline{v})$ pro afinní prosotr $\mathcal{A}$. 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

$$\alpha_j(v) = 0, \quad j = k+1, \dots, n,$$

kde α_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 $\mathbb{R}^n$ je tedy skutečně dán jako řešení homogenního systému $n-k$ nezávislých rovnic. Popis zvoleného afinního podprostoru ve vybraném souřadném systému $(A_0; \underline{u})$ 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. □

2.62

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 bazí zaměření. Transformační rovnice tedy vyčteme ze vztahu pro obecný bod $X \in \mathcal{A}$

$$X = B_0 + x'_1 v_1 + \dots + x'_n v_n = B_0 + (A_0 - B_0) + x_1 u_1 + \dots + x_n u_n.$$

Označme $y = (y_1, \dots, y_n)^T$ 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

$$\begin{aligned} x'_1 &= y_1 + a_{11}x_1 + \dots + a_{1n}x_n \\ &\vdots \\ x'_n &= y_n + a_{n1}x_1 + \dots + a_{nn}x_n \end{aligned}$$

tj. maticově

$$x' = y + M \cdot x.$$

Jako příklad si můžeme spočítat dopad takové změny báze na vyjádření řešení systémů rovnic. Nechť v souřadnicích $(A_0; \underline{u})$ má systém rovnic tvar

$$S \cdot x = b$$

s maticí systému S. Pak $S \cdot x = S \cdot M^{-1} \cdot (y + M \cdot x) - S \cdot M^{-1} \cdot y = b$. Proto v nových výše uvažovaných souřadnicích $(B_0; \underline{v})$ bude mít náš systém rovnic tvar

$$(S \cdot M^{-1}) \cdot x' = b' = b + (S \cdot M^{-1}) \cdot y.$$

To plně dokončuje důkaz předchozí věty.

2.63

4.6. Afinní kombinace bodů. 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

$$\{A_0 + t_1(A_1 - A_0) + \cdots + t_k(A_k - A_0); t_1, \dots, t_k \in \mathbb{R}\}$$

a v libovolných afinních souřadnicích (tj. A_i je vyjádřen sloupcem skalárů) můžeme tutéž množinu zapsat jako

$$\langle A_0, \dots, A_k\rangle = \{t_0A_0 + t_1A_1 + \cdots + t_kA_k; t_i \in \mathbb{R}, \sum_{i=0}^{k} t_i = 1\}.$$

Obecně výrazy $t_0A_0 + t_1A_1 + \cdots + t_kA_k$ 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-rozměný podprostor. Z našich definic je vidět, že to nastane právě, když pro kterýkoliv z nich platí, že vektory vzniklé pomocí rozdílů tohoto pevného s ostatními jsou lineárně nezávislé. Všimněme si také, že zadání posloupnosti $\dim \mathcal{A}$ bodů v obecné poloze je ekvivalentní zadání afinního repéru s středem v prvním z nich.

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 odopovídá vnitřek trojúhelníku. Obecně budeme postupovat takto:

Nechť $A_0, \dots, A_k$ je $k+1$ bodů afinního prostoru $\mathcal{A}$ v obecné poloze. k–rozměrný *simplex* $\Delta = \Delta(A_0, \dots, A_k)$ generovaný těmito body je definován jako množina všech afinních kombinací bodů A_i s pouze nezápornými koeficienty, tzn.

$$\Delta = \{t_0A_0 + t_1A_1 + \cdots + t_kA_k; t_i \in [0, 1] \subset \mathbb{R}, \sum_{i=0}^{k} t_i = 1\}.$$

Jednorozměrný simplex je *úsečka*, dvourozměrný *trojúhelník*.

Zadání podprostoru jako množiny afinních kombinací bodů v obecné poloze je ekvivalentní parametrickému popisu. Obdobně pracujeme s parametrickými popisy simplexů.

2.64

4.7. 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.

Konvexními množinami jsou např.
(1) prázdná podmnožina
(2) afinní podprostory
(3) úsečky, polopřímky $p = \{P + t \cdot v;\ t \geq 0\}$, obecněji k– rozměrné poloprostory $\alpha = \{P + t_1 \cdot v_1 + \cdots + t_k \cdot v_k;\ t_1, \dots, t_k \in \mathbb{R}, t_k \geq 0\}$, úhly v dvojrozměrných podprostorech $\beta = \{P + t_1 \cdot v_1 + t_2 \cdot v_2;\ t_1 \geq 0, t_2 \geq 0\}$, atd.

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 podmnožiny $M \subset \mathcal{A}$ je*

$$\mathcal{K}(M) = \{t_1A_1 + \cdots + t_sA_s;\ \sum_{i=1}^{s} t_i = 1,\ t_i \geq 0\}$$

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:

$$\epsilon(t_1A_1 + \cdots + t_sA_s) + (1-\epsilon)(t'_1A_1 + \cdots + t'_sA_s),\ 0 \leq \epsilon \leq 1.$$

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 $A = t_1A_1 + \cdots + t_sA_s \in S$, $t_s \neq 1$, a afinní kombinace

$$\epsilon(t_1A_1 + \cdots + t_{s-1}A_{s-1}) + (1 - \epsilon(1-t_s))A_s,\ 0 \leq \epsilon \leq \tfrac{1}{1-t_s}.$$

Jde o úsečku s krajními body určenými parametry $\epsilon = 0$ (bod A_s) a $\epsilon = 1/(1-t_s)$ (bod v konvexním obalu bodů $A_1, \ldots, A_{s-1}$). Bod A je vnitřním bodem této úsečky s parametrem $\epsilon = 1$. □

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.

Jiným příkladem jsou konvexní podmnožiny generované jedním bodem a konečně mnoha vektory: Nechť $u_1, \ldots, u_k$, jsou libovolné vektory v zaměření $\mathbb{R}^n$, $A \in \mathcal{A}_n$ je libovolný bod. *Rovnoběžnostěn* $\mathcal{P}_k(A; u_1, \ldots, u_k) \subset \mathcal{A}_n$ je množina

$$\mathcal{P}_k(A; u_1, \ldots, u_k) = \{A + c_1u_1 + \cdots + c_ku_k;\ 0 \leq c_i \leq 1, i = 1, \ldots, k\}.$$

Jsou-li vektory $u_1, \ldots, u_k$ nezávislé, hovoříme o k-rozměrném rovnoběžnostěnu $\mathcal{P}_k(A; u_1, \ldots, u_k) \subset \mathcal{A}_n$. Z definice je zřejmé, že rovnoběžnostěny jsou konvexní. Ve skutečnosti jde o konvexní obaly jejich vrcholů.

2.65

4.8. 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.

$$\mathcal{Q} = A_1 + (Z(\{A_1, \dots, A_k\}) + Z(\mathcal{Q}_1) + \cdots + Z(\mathcal{Q}_s)).$$

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 $\mathcal{Q}_1, \dots, \mathcal{Q}_s$:*

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 oběmi 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 $q \subset \langle p \cup A \rangle$, máme opět nekonečně mnoho řešení, a pokud je průnik jednoprvkový, dostáváme právě jedno řešení.

Máme-li místo bodu dán směr $u \in \mathbb{R}^n$, tj. zaměření r, pak uvažujeme opět podprostor $\mathcal{Q}$ generovaný p a zaměřením $Z(p) + \langle u \rangle \subset \mathbb{R}^n$. Opět, pokud $q \subset \mathcal{Q}$, máme nekonečně mnoho řešení, jinak uvážíme průnik $\mathcal{Q}$ s q a úlohu dokončíme stejně jako v předchozím případě.

Řešení mnoha dalších standardních geometrických úloh spočívá v používání výše uvedených kroků.

4.9. Příklad. Uvádíme několik příkladů s výsledky.

4.9.1. 1. *Parametricky vyjádřete průnik následujících rovin v $\mathbb{R}^3$:*

$$\sigma : 2x + 3y - z + 1 = 0 \quad a \quad \rho : x - 2y + 5 = 0.$$

Řešení. Přímka $(2t, t, 7t) + [-5, 0, -9]$. □

4.9.2. 2. *Najděte příčku přímek (úsečku, jejíž jeden koncový bod leží na jedné z přímek, druhý pak na druhé z nich)*

$$p : [1, 1, 1] + t(2, 1, 0), \quad q : [2, 2, 0] + t(1, 1, 1),$$

takovou, že přímka jí určená prochází bodem $[1, 0, 0]$.

Řešení. Hledaný bod v q najdeme jako průnik přímky q s rovinou

$$[1,1,1]+t(2,1,0)+s(0,1,1).$$

Jde o úsečku s krajními body $[5,5,3]\in q$, $[7/3,5/3,1]\in p$. □

4.9.3. 3. *Určete osu mimoběžek*

$$\begin{aligned} p:&\quad [3,0,3]+(0,1,2)t\\ q:&\quad [0,-1,-2]+(1,2,3)t. \end{aligned}$$

Řešení. Úsečka $([2,3,4],[3,1,5])$. □

4.9.4. 4. *Nalezněte osu mimoběžek*

$$p:\ [1,1,1]+t(2,1,0),\quad q:\ [2,2,0]+t(1,1,1).$$

Řešení. $[3,2,1][8/3,8/3,2/3]$. □

4.9.5. 5. *Určete patu kolmice spuštěné z bodu* $[0,0,7]$ *na rovinu*

$$\rho:\ [0,5,3]+(1,2,1)t+(-2,1,1)s.$$

Řešení. $(-1,3,2)$. □

4.9.6. 6. *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. □

4.9.7. 7. *Na kolik částí mohou dělit prostor* ($\mathbb{R}^3$) *tři roviny? Pro každou možnost popište odpovídající případ.*

Řešení. 2, 3, 4, 6, 7, 8. Polohy rovin, které realizují dané počty si rozmyslete samostatně. □

4.9.8. 8. *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 lin. soustavu, pro koeficienty t_1, t_2, t_3, t_4, afinní kombinace daných bodů, která dává první bod (jsou určeny jednozačně, 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. Jejím řešením dostáváme $(t_1, t_2, t_3, t_4) = (1, 0, 1/2, -1/2)$, nejedná se tedy o konvexní kombinaci. (nelze odvodit pomocí projekcí na jednotlivé osy). □

4.9.9. 9. *Určete odchylku rovin*

$$\begin{aligned} \sigma: &\quad [1,0,2] + (1,-1,1)t + (0,1,-2)s \\ \rho: &\quad [3,3,3] + (1,-2,0)t + (0,1,1)s \end{aligned}$$

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 $60°$. □

4.9.10. 10. *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 udávající objem rovnoběžnostěnu při pohyblivém bodu X:

$$\begin{vmatrix} t & t & t \\ 2 & 1 & 0 \\ 1 & 2 & 0 \end{vmatrix}.$$

Podmínka, že má být roven jedné dává $t = 1/3$. □

4.9.11. 11. *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 φ těchto vektorů je pak

$$\cos(\varphi) = \frac{(1,0,1) \cdot (0,1,1)}{\| (1,0,1) \| \| (0,1,1) \|} = \frac{1}{2},$$

tedy $\varphi = 60°$.

□

2.66

4.10. Afinní zobrazení. Zobrazení $f : \mathcal{A} \to \mathcal{B}$ mezi afinními prostory nazýváme *afinní zobrazení*, jestliže existuje lineání 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 φ jsou jednoznačně zadána touto vlastnostní a libovolně zvolenými obrazy $(\dim \mathcal{A} + 1)$ bodů v obecné poloze.

Pro libovolnou afinní kombinaci bodů $t_0A_0 + \cdots + t_sA_s \in \mathcal{A}$ pak dostaneme

$$\begin{aligned} f(t_0A_0 + \cdots + t_sA_s) &= f(A_0) + t_1\varphi(A_1 - A_0) + \cdots + t_s\varphi(A_s - A_0) \\ &= t_0f(A_0) + t_1f(A_1) + \cdots + t_sf(A_s). \end{aligned}$$

Naopak, pokud pro nějaké zobrazení platí, že zachovává afinní kombinace, můžeme číst předchozí výpočet v opačném pořadí a zjistíme, se jedná o afinní zobrazení. Ekvivalentně lze tedy definovat afinní zobrazení jako ta, která zachovávají afinní kombinace bodů.

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 počátku souřadnic v $\mathcal{A}$ v souřadnicích na $\mathcal{B}$, tj. vyjádřit vektor $f(A_0) - B_0$ v bázi $\underline{v}$ a vše ostatní je pak určeno násobením maticí zobrazení φ ve zvolených bazích a přičtením výsledku.

4.11. Příklad. *Napište matici B afinního zobrazení f daného ve standardní bázi v $\mathbb{R}^2$ jako*

$$f(x_1, x_2) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

souřadné soustavě dané bází $\underline{u} = \{(1, 1), (-1, 1)\}$ a počátkem $[2, 0]$.

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 priklané 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 suouřadnic 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

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}^{-1} \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} - \begin{pmatrix} 2 \\ 0 \end{pmatrix}. \right) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

Pro matici zobrazení pak dostáváme

$$\begin{aligned} B &= \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \left[\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right) + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] + \begin{pmatrix} -1 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix} + \begin{pmatrix} 2 \\ -1 \end{pmatrix} \end{aligned}$$

□

4.12. Příklad.

4.12.1. *Mejme dánu standardní souřadnou soustavu v trojrozměrném Eukleidovském prostoru. 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 $(-1,2,2)$. □

2. Euklidovská geometrie

Na minulé kapitole jsme vytvořili východisko pro elementární geometrii a nepotřebovali jsme k tomu pojem vzdálenosti nebo velikosti. Ve skutečnosti jsme pojem velikosti vektorů a odchylku vektorů zavedli na konci třetí kapitoly této části. Několikrát jsme také nejen v geometrii roviny se vzdálenostmi pracovali, viz třeba optimalizační výsledek o neřešitelných systémech lineárních rovnic a pseudoinverzních maticích ve Větě 3.30. Asi proto dobře tušíme, jak se s problémem vypořádat:

4.13. Definice. 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

$$\langle x, z\rangle = x^T \cdot y.$$

Kartézská souřadná soustava je afinní souřadná soustava $(A_0; \underline{u})$ s ortonormální bazí $\underline{u}$. *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 $\mathcal{E}$ pak obecně rozumíme afinní prostor, jehož zaměření je 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.

Opět si napřed uvedeme několik jednoduchých tvrzení o euklidovských prostorech. K jejich formulaci i důkazům se ale musíme zamyslet nad standardními vztahy mezi velikostmi vektorů, které podobně jako v rovinné geometrii platí obecně:

4.12

4.14. Věta. *Pro každé vektory u a v, které leží v reálném vektorovém prostoru V se skalárním součinem, platí*

(1) $\|u+v\| \le \|u\| + \|v\|$ *(trojúhelníková nerovnost). Přitom rovnost nastane právě, když jsou u a v lineárně závislé.*

(2) $|u \cdot v| \le \|u\|\,\|v\|$ *(Cauchyova nerovnost). Přitom rovnost nastane právě, když jsou u a v lineárně závislé.*
(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 $(e_1, \dots, e_k)$ je $u \in \langle e_1, \dots, e_k\rangle$ 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 $u \in V$ 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 podstatě v přímých výpočtech:
(2): Definujme vektor $w := u - \frac{u\cdot v}{v\cdot v}v$, tzn. $w \perp v$ a počítejme

$$0 \le \|w\|^2 = \|u\|^2 - \frac{(u\cdot v)}{\|v\|^2}(u\cdot v) - \frac{u\cdot v}{\|v\|^2}(v\cdot u) + \frac{(u\cdot v)(u\cdot v)}{\|v\|^4}\|v\|^2$$
$$0 \le \|w\|^2\|v\|^2 = \|u\|^2\|v\|^2 - 2(u\cdot v)(u\cdot v) + (u\cdot v)(u\cdot v)$$

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.
(1): Opět stačí počítat

$$\begin{aligned}\|u+v\|^2 &= \|u\|^2 + \|v\|^2 + u\cdot v + v\cdot u = \|u\|^2 + \|v\|^2 + 2u\cdot v\\ &\le \|u\|^2 + \|v\|^2 + 2|u\cdot v| \le \|u\|^2 + \|v\|^2 + 2\|u\|\|v\|\\ &= (\|u\| + \|v\|)^2\end{aligned}$$

Protože se přitom jedná o kladná 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 $(e_1, \dots, e_n)$. Pak je pro každý vektor $u \in V$

$$\|u\|^2 = \sum_{i=1}^{n}(u\cdot e_i)(u\cdot e_i) = \sum_{i=1}^{n}|u\cdot e_i|^2 \ge \sum_{i=1}^{k}|u\cdot e_i|^2.$$

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 po řadě 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 $x_1 = u_1, \dots, x_k = u_k$. □

Nyní již dostáváme jednoduché důsledky pro euklidovskou geometrii:

4.13 **4.15. Věta.** *Pro body $A, B, C \in \mathcal{E}_n$ platí*
(1) $\rho(A, B) = \rho(B, A)$
(2) $\rho(A, B) = 0$ *právě, když* $A = B$
(3) $\rho(A, B) + \rho(B, C) \ge \rho(A, C)$

(4) *V každé kartézké souřadné soustavě* $(A_0; \underline{e})$ *mají body*

$$A = A_0 + a_1e_1 + \cdots + a_ne_n, \quad B = A_0 + b_1e_1 + \cdots + b_ne_n$$

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* $\mathcal{R}$ *a* $\mathcal{Q}$ *v* $\mathcal{E}_n$ *existují bod* $P \in \mathcal{Q}$ *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* $Z(\mathcal{Q})^\perp$ *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 vzdleností $\rho(A, B)$ 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 $B \in \mathcal{Q}$, $P = A + (-u_2) = B + u_1 \in \mathcal{Q}$ a $\|A - B\|^2 = \|u_1\|^2 + \|u_2\|^2 \geq \|u_2\|^2 = \|A - P\|$. Odtud již vyplývá, že infima je skutečně dosaženo, a to pro bod P. Vypočtená vzdálenost je skutečně $\|u_2\|$.

Obecný výsledek se dokáže zcela obdobně. □

4.16. Vzdálenost přímek. *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:

$$\rho(p, q) = \frac{|(-1, -6, 1) \cdot (4, -1, 2)|}{\|(4, -1, 2)\|} = \frac{4}{\sqrt{21}}.$$

□

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. Proto se nyní budeme chvíli věnovat opět reálným unitárním prostorům. Začneme s diskusí velikosti úhlů. Z Cauchyovy nerovnosti plyne $0 \leq \frac{|u \cdot v|}{\|u\|\|v\|} \leq 1$, má tedy smysl následující definice.

4.15

4.17. Definice. *Odchylka* $\varphi(u, v)$ *vektorů* $u, v \in V$ v reálném vektorovém prostoru se skalárním součinem je dána vztahem

$$\cos\varphi(u, v) = \frac{u \cdot v}{\|u\|\|v\|}, \quad 0 \leq \varphi(u, v) \leq 2\pi.$$

Jak jsme viděli, v rovině $\mathbb{R}^2$ pro (obvyklou) odchylku vektorů na jednotkové kružnici $u = (1, 0)$, $v = (\cos\varphi, \sin\varphi)$ skutečně platí $\cos\varphi = \frac{u\cdot v}{\|u\|\|v\|}$. Protože odchylka je nezávislá na velikostech vektorů, platí stejný vztah i pro vektory $u = (x_1, 0)$, $v = (a\cos\varphi, a\sin\varphi)$. Protože vhodnou rotací dosáhneme toho, že jeden z dvojice vektorů má tvar $(x_1, 0)$, platí náš vztah zcela obecně v rovině. Ve vícerozměrných prostorech je odchylka dvou vektorů vždy měřena v rovině, kterou tyto vektory generují (nebo je nula), jistě tedy náš definiční vztah odpovídá zvyklostem ve všech dimenzích.

V libovolném reálném vektorovém prostoru se skalárním součinem přímo z definic plyne

$$\|u - v\|^2 = \|u\|^2 + \|v\|^2 - 2(u \cdot v) = \|u\|^2 + \|v\|^2 - 2\|u\|\|v\|\cos\varphi(u, v).$$

To je tzv. *kosinová věta*.

Dále platí pro každou ortonormální bázi $\underline{e}$ a $u \in V$ vztah $\|u\|^2 = \sum_i |u \cdot e_i|^2$, tj.

$$1 = \sum_i (\cos\varphi(u, e_i))^2,$$

což je obvyklé tvrzení o směrových kosinech $\varphi(u, e_i)$ vektoru u.

Z definice odchylek vektorů nyní můžeme dovodit rozumné definice pro obecné podprostory v každém euklidovském vektorovém prostoru.

4.16 **4.18. Definice.** Nechť U_1, U_2 jsou podprostory v euklidovském prostoru V. *Odchylka podprostorů* U_1, U_2 je reálné číslo $\alpha = \varphi(U_1, U_2) \in [0, \frac{\pi}{2}]$ splňující:

(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 v zápětí, že takové minimum skutečně vždy existuje.

(3) Je-li $U_1 \subset U_2$ nebo $U_2 \subset U_1$ (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 korektosti 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:

4.19. Lemma. *Nechť v je vektor v euklidovském prostoru V a $U \subset V$ 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 φ 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 $u \in U$ platí

$$\begin{aligned}\frac{|u\cdot v|}{\|u\|\|v\|} &= \frac{|u\cdot(v_1+v_2)|}{\|u\|\|v\|} = \frac{|u\cdot v_1|}{\|u\|\|v\|}\\ &\le \frac{\|u\|\|v_1\|}{\|u\|\|v\|} = \frac{\|v_1\|}{\|v\|} = \frac{\|v_1\|^2}{\|v\|\|v_1\|} = \frac{|v_1\cdot v|}{\|v\|\|v_1\|}.\end{aligned}$$

Odtud plyne

$$\cos\varphi(\langle v\rangle, \langle u\rangle) \le \cos\varphi(\langle v\rangle, \langle v_1\rangle) = \frac{\|v_1\|}{\|v\|}$$

a protože funkce cos je na intervalu $[0, \frac{\pi}{2}]$ klesající, je tvrzení dokázané. □

4.20. Výpočet odchylek. Uvažujme dva podprostory U_1, U_2 v euklidovském prostoru V, $U_1 \cap U_2 = \{0\}$ a zvolme pevně ortonormální báze $\underline{e}$, a $\underline{e}'$ tak, aby $U_1 = \langle e_1, \dots, e_k\rangle$, $U_2 = \langle e'_1, \dots, e_l\rangle$. Nechť φ je kolmý průmět 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 bazích $(e_1, \dots, e_k)$ a $(e'_1, \dots, e_l)$ matice

$$A = \begin{pmatrix} e_1\cdot e'_1 & \dots & e_k\cdot e'_1\\ \vdots & & \vdots\\ e_1\cdot e'_l & \dots & e_k\cdot e'_l\end{pmatrix}, \qquad B = \begin{pmatrix} e'_1\cdot e_1 & \dots & e'_l\cdot e_1\\ \vdots & & \vdots\\ e'_1\cdot e_k & \dots & e'_l\cdot e_k\end{pmatrix}$$

Zejména platí $B = A^T$. Složené zobrazení $\psi\circ\varphi : U_1 \to U_1$ má tedy symetrickou matici A^TA. 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 3.21–3.23.

Nyní můžeme odvodit obecný postup pro výpočet odchylky $\alpha = \varphi(U_1, U_2)$.

Věta. *V předchozím označení nechť λ je největší vlastní hodnota matice A^TA. Pak* $\cos^2\alpha = \lambda$

Důkaz. Nechť $u \in U_1$ je vlastní vektor zobrazení $\psi\circ\varphi$ příslušný největší vlastní hodnotě λ, $\lambda_1, \dots, \lambda_k$ nechť jsou všechna vlastní čísla (včetně násobnosti) a nechť $\underline{u} = (u_1, \dots, u_n)$ 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 $v \in U_1$, $v = a_1u_1 + \dots + a_ku_k$, $\sum_{i=1}^k a_i^2 = \|v\|^2 = 1$. Pak

$$\|\varphi(v)\|^2 = \varphi(v)\cdot\varphi(v) = \psi\circ\varphi(v)\cdot v \le \|\psi\circ\varphi(v)\|\|v\| = \|\psi\circ\varphi(v)\|.$$

Předchozí lemma navíc dává i vzorec pro odchylku α vektoru v od U_2

$$\cos\alpha = \frac{\|\varphi(v)\|}{\|v\|} = \|\varphi(v)\|.$$

Protože jsme zvolili za λ_1 největší z vlastních hodnot, dostáváme

$$(\cos\alpha)^2 = \|\varphi(v)\|^2 \le \|\psi\circ\varphi(v)\| = \sqrt{\sum_{i=1}^{k}(\lambda_i a_i)^2} =$$

$$= \sqrt{\lambda_1^2 + \sum_{i=1}^{k} a_i^2(\lambda_i^2 - \lambda_1^2)} \le \sqrt{\lambda_1^2}.$$

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. □

4.21. Příklady standardních úloh. *1. Najděte vzdálenost bodu $A \in \mathcal{E}_n$ od podprostoru $\mathcal{Q} \subset \mathcal{E}_n$:*

Viz. věta 4.15.

2. V $\mathcal{E}_2$ veďte bodem A přímku q svírající s danou přímkou p daný úhel:

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:

Viz. důkaz předposledního bodu věty 4.15.

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:

Nechť η je rovina generovaná jedním bodem $A \in p$ a součtem $Z(p) + (Z(p) + Z(q))^\perp$. Pak průnik $\eta \cap q$ spolu se zaměřením $(Z(p) + Z(q))^\perp$ dávají parametrický popis hledané osy. (Prověřte, kolik má úloha obecně řešení!)

4.22. Příklad. *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 ϱ. Její zaměření bude kolmé na zaměření ϱ, pro vektory (a,b,c,d) patřící do jejího zaměření dostáváme tedy soustavu rovnic

$$\begin{aligned}(a,b,c,d)\cdot(1,2,-1,-2) = 0 \quad &\equiv \quad a + 2b - c - 2d = 0\\ (a,b,c,d)\cdot(1,0,0,1) = 0 \quad &\equiv \quad a + d = 0.\end{aligned}$$

Jejím řešením je dvojdimenzionální vektorový prostor $\langle(0,1,2,0),(-1,0,-3,1)\rangle$. Rovina τ kolmá k rovině ϱ 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:

$$\begin{aligned}1 + s + t &= 1 - v\\ 2s &= 2 + u\\ 1 - s &= 3 + 2u - 3v\\ -2s + t &= 4 + v,\end{aligned}$$

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 ϱ pak dostaneme souřadnice průniku $[45/19, -16/19, 11/19, 18/19]$ (stejný výsledek pochopitelně obdržíme, dosadíme-li hodnoty parametrů u a v do parametrického vyjádření roviny τ). □

4.23. Příklad. *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 $\underline{v}$ 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 $\underline{v}$ je tedy

$$\underline{v} = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} - \frac{1}{2} \\ \frac{\sqrt{3}}{2} + \frac{1}{2} \end{pmatrix}.$$

Rotovat jsme mohli i v opačném smyslu. Hledaná přímka (jedna ze dvou možných) má tedy parametrické vyjádření

$$[1,2] + (\frac{\sqrt{3}}{2} - \frac{1}{2}, \frac{\sqrt{3}}{2} + \frac{1}{2})t.$$

□

4.24. Příklad.

4.24.1. *Určete* $\cos\alpha$*, kde* α *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 $A = [\frac{\sqrt{2}}{2}, 0, 0]$, $B = [0, \frac{\sqrt{2}}{2}, 0]$, $C = [-\frac{\sqrt{2}}{2}, 0, 0]$, $D = [0, -\frac{\sqrt{2}}{2}, 0]$, $E = [0, 0, -\frac{\sqrt{2}}{2}]$ a $F = [0, 0, \frac{\sqrt{2}}{2}]$.

Určeme odchylku stěn CDF a BCF. Ta je dána odchylkou vektorů kolmých na jejich průnik a ležících v daných stěnách, tedy vekorů kolmých na CF. Těmi jsou vektory dané výškami z bodů D, resp. F na stranu CF v trojúhelnících CDF, resp. BCF. Výšky v rovostranném 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 $[-\frac{\sqrt{2}}{4}, 0, \frac{\sqrt{2}}{4}]$ a pro vektory máme $SD = (\frac{\sqrt{2}}{4}, -\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4})$ a $SB = (\frac{\sqrt{2}}{4}, \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4})$. Celkem

$$\cos\alpha = \frac{(\frac{\sqrt{2}}{4}, -\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4}) \cdot (\frac{\sqrt{2}}{4}, \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4})}{\|(\frac{\sqrt{2}}{4}, -\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4})\| \|(\frac{\sqrt{2}}{4}, \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{4})\|} = -\frac{1}{3}.$$

Je tedy $\alpha \doteq 132°$. □

4.21

4.25. Počítání objemu. Orientovaný (bodový) euklidovský prostor je euklidovský bodový prostor, jehož zaměření je orientované. V dalším budeme uvažovat standardní $\mathcal{E}_n$ spolu s orientací zadanou standardní bazí $\mathcal{R}^n$.

Nechť $u_1, \dots, u_k$, jsou libovolné vektory v zaměření $\mathbb{R}^n$, $A \in \mathcal{E}_n$ je libovolný bod. Rovnoběžnostěn $\mathcal{P}_k(A; u_1, \dots, u_k) \subset \mathcal{E}_n$ jsme definovali jako množinu

$$\mathcal{P}_k(A; u_1, \dots, u_k) = \{A + c_1u_1 + \cdots + c_ku_k; 0 \le c_i \le 1, i = 1, \dots, k\}.$$

Jsou-li vektory $u_1, \dots, u_k$ nezávislé, hovořili jsme o k–rozměrném rovnoběžnostěnu $\mathcal{P}_k(A; u_1 \dots, u_k) \subset \mathcal{E}_n$. Pro dané vektory $u_1, \dots, u_k$ máme k dispozici také rovnoběžnostěny menších dimenzí

$$\mathcal{P}_1(A; u_1), \dots, \mathcal{P}_k(A; u_1, \dots, u_k)$$

v euklidovských podprostorech $A + \langle u_1\rangle, \dots, A + \langle u_1, \dots, u_k\rangle$.

Jsou-li $u_1, \dots, u_k$ lineárně závislé definujeme objem $\operatorname{Vol} P_k = 0$. Pro nezávislé vektory pak platí $\langle u_1, \dots, u_k\rangle = \langle u_1, \dots, u_{k-1}\rangle \oplus (\langle u_1, \dots, u_{k-1}\rangle^\perp \cap \langle u_1, \dots, u_k\rangle)$. Navíc v tomto rozkladu se u_k jednoznačně vyjádří jako

$$u_k = u'_k + e_k, \text{ kde } e_k \perp \langle u_1, \dots, u_{k-1}\rangle.$$

Absolutní hodnotu objemu definujeme induktivně:

$$|\operatorname{Vol}|\mathcal{P}_1(A; u_1) = \|u_1\|$$
$$|\operatorname{Vol}|\mathcal{P}_k(A; u_1, \dots, u_k) = \|e_k\||\operatorname{Vol}|\mathcal{P}(A; u_1, \dots, u_{k-1}).$$

Je-li $u_1, \dots, u_n$ báze kompatibilní s orientací V, definujeme (orientovaný) objem rovnoběžnostěnu $\operatorname{Vol}\mathcal{P}_k(A; u_1, \dots, u_n) = |\operatorname{Vol}|\mathcal{P}_k(A; u_1, \dots, u_n)$, v opačném případě klademe $\operatorname{Vol}\mathcal{P}_k(A; u_1, \dots, u_n) = -|\operatorname{Vol}|\mathcal{P}_k(A; u_1, \dots, u_n)$.

Věta. *Nechť $\mathcal{Q} \subset \mathcal{E}_n$ je euklidovský podprostor a nechť $(e_1, \dots, e_k)$ je jeho ortonormální báze. Pak pro libovolné vektory $u_1, \dots, u_k \in Z(\mathcal{Q})$ a $A \in \mathcal{Q}$ platí*

(1) $$\operatorname{Vol}\mathcal{P}_k(A; u_1, \dots, u_k) = \det \begin{pmatrix} u_1 \cdot e_1 & \dots & u_k \cdot e_1 \\ \vdots & & \vdots \\ u_1 \cdot e_k & \dots & u_k \cdot e_k \end{pmatrix}$$

(2) $$(\operatorname{Vol}\mathcal{P}_k(A; u_1, \dots, u_k))^2 = \det \begin{pmatrix} u_1 \cdot u_1 & \dots & u_k \cdot u_1 \\ \vdots & & \vdots \\ u_1 \cdot u_k & \dots & u_k \cdot u_k \end{pmatrix}$$

Důkaz. Matice

$$A = \begin{pmatrix} u_1 \cdot e_1 & \dots & u_k \cdot e_1 \\ \vdots & & \vdots \\ u_1 \cdot e_k & \dots & u_k \cdot e_k \end{pmatrix}$$

má ve sloupcích souřadnice vektorů $u_1, \dots, u_k$ ve zvolené ortonormální bázi. Platí

$$|A|^2 = |A||A| = |A^T||A| = |A^TA| = \det \begin{pmatrix} u_1 \cdot u_1 & \dots & u_k \cdot u_1 \\ \vdots & & \vdots \\ u_1 \cdot u_k & \dots & u_k \cdot u_k \end{pmatrix}.$$

Přímo z definice je neorientovaný objem roven součinu $\|v_1\|\|v_2\| \dots \|v_k\|$, kde $v_1 = u_1$, $v_2 = u_2 + a_1^2v_1, \dots, v_k = u_k + a_1^kv_1 + \cdots + a_{k-1}^kv_{k-1}$ je výsledek Grammova-Schmidtova

ortogonalizačního procesu. Je tedy

$$\begin{aligned}\left(\operatorname{Vol}\mathcal{P}_k(A;u_1,\dots,u_k)\right)^2 &= \det\begin{pmatrix} v_1\cdot v_1 & \dots & v_k\cdot v_1\\ \vdots & & \vdots\\ v_1\cdot v_k & \dots & v_k\cdot v_k\end{pmatrix}\\ &= \det\begin{pmatrix} v_1\cdot v_1 & 0 & \dots & 0\\ \vdots & & \vdots & \\ 0 & 0 & \dots & v_k\cdot v_k\end{pmatrix}.\end{aligned}$$

Označme B matici jejíž sloupce jsou souřadnice vektorů $v_1,\dots,v_k$ v bázi $\underline{e}$. Protože $v_1,\dots,v_k$ vznikly z $u_1,\dots,u_k$ 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 $\operatorname{Vol}\mathcal{P}_k(A;u_1,\dots,u_k) = \pm|A|$. Přitom pokud jsou vektory $u_1,\dots,u_k$ závislé vyjde objem nulový, pokud jsou nezávislé, pak znaménko determinantu je kladné právě když je báze $u_1,\dots,u_k$ kompatibilní s orientací danou bazí $\underline{e}$. □

Determinant

$$\det\begin{pmatrix} u_1\cdot u_1 & \dots & u_k\cdot u_1\\ \vdots & & \vdots\\ u_1\cdot u_k & \dots & u_k\cdot u_k\end{pmatrix}$$

se nazývá *Grammův determinant* k–tice vektorů $u_1,\dots,u_k$. V geometrické formulaci dostáváme jako velice důžitý důsledek následující tvrzení:

4.26. 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.*

4.27. Příklad. *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 Tvrzení **??** je objem rovnoběžnostěnu $\mathcal{P}_3(0;\underline{u},\underline{v},\underline{t})$ dán jako abolutní hodnota determinantu

$$\begin{vmatrix} u_1 & v_1 & t_1\\ u_2 & v_2 & t_2\\ u_3 & v_3 & t_3\end{vmatrix} = \begin{vmatrix} t_1 & t_2 & t_3\\ u_1 & u_2 & u_3\\ v_1 & v_2 & v_3\end{vmatrix} = \underline{t}\cdot(\underline{u}\times\underline{v}) \le \|\underline{t}\|\|\underline{u}\times\underline{v}\| = \|\underline{u}\times\underline{v}\|.$$

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 maximálne rovna velikosti obsahu rovnoběžníka daného vektory $\underline{u}$, $\underline{v}$ (tj. velikosti vektoru $(\underline{u}\times\underline{v})$). Rovnost nastane právě když

$$t = \pm\frac{(\underline{u}\times\underline{v})}{\|(\underline{u}\times\underline{v})\|}.$$

□

4.28. Vnější a vektorový součin vektorů. Předchozí úvahy úzce souvisí s tzv. vnějším tensorovým součinem vektorů. Nepůjdeme do této technicky poněkud nepřehledné oblasti, ale zmíníme alespoňpřípad vnějšího součinu $n = \dim V$ vektorů $u_1, \dots, u_n \in V$.

Nechť $(u_{1j}, \dots, u_{nj})$ 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* $u_1, \dots, u_n$ a značíme $[u_1, \dots, u_n]$. Viz 4.25.

Přímo z definice nyní vyplývají užitečné vlastnosti vnějšího součinu

(1) Zobrazení $(u_1, \dots, u_n) \mapsto [u_1, \dots, u_n]$ 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 $u_1, \dots, u_n$ lineárně závislé
(3) Vektory $u_1, \dots, u_n$ tvoří kladnou bázi právě, když je jejich vnější součin kladný.

V $\mathbb{R}_3$ patrně již známe další významnou operaci, tzv. vektorový součin, který dvojici vektorů přiřazuje vektor třetí. Uvažme obecný euklidovský vektorový prostor V dimenze $n \geq 2$ a vektory $u_1, \dots, u_{n-1} \in V$. Vektor $v \in V$ nazveme *vektorový součin* vektorů $u_1, \dots, u_{n-1}$, jestliže pro každý vektor $w \in V$ platí

$$\langle v, w \rangle = [u_1, \dots, u_{n-1}, w].$$

Značíme $v = u_1 \times \dots u_{n-1}$.

V ortonormálních souřadnicích, kde $v = (y_1, \dots, y_n)^T$, $w = (x_1, \dots, x_n)^T$ a $u_j = (u_{1j}, \dots u_{nj})^T$, předchozí vztah znamená

$$y_1x_1 + \dots + y_nx_n = \begin{vmatrix} u_{11} & \dots & u_{1(n-1)} & x_1 \\ \vdots & & \vdots & \vdots \\ u_{n1} & \dots & u_{n(n-1)} & x_n \end{vmatrix}$$

Odtud vyplývá, že vektor v je tímto vztahem zadán jednoznačně a jeho souřadnice spočteme formálním rozvojem tohoto determinantu podle posledního sloupce.

Věta. *Pro vektorový součin $v = u_1 \times \dots \times u_{n-1}$ platí*

(1) $v \in \langle u_1, \dots, u_{n-1} \rangle^\perp$
(2) *v je nenulový vektor právě, když jsou vektory $u_1, \dots, u_{n-1}$ lineárně nezávislé*
(3) *velikost $\|v\|$ vektorového součinu je rovna absolutní hodnotě objemu rovnoběžníku $\mathcal{P}(0; u_1, \dots, u_{n-1})$*
(4) *$(u_1, \dots, u_{n-1}, v)$ je kladná 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 $u_1, \dots, u_{n-1}$ závislé, pak platí i (3). Nechť jsou tedy nezávislé, v je jejich vektorový součin a zvolme libovolnou ortonormální bázi $(e_1, \dots, e_{n-1})$ prostoru $\langle u_1, \dots, u_{n-1} \rangle$. Z již dokázáného vyplývá, že existuje nějaký násobek $(1/\alpha)v$, $0 \neq \alpha \in \mathbb{R}$, takový, že $(e_1, \dots, e_k, (1/\alpha)v)$ je ortonormální báze celého V. Souřadnice našich vektorů v této bázi jsou

$$u_j = (u_{1j}, \dots, u_{(n-1)j}, 0)^T, \quad v = (0, \dots, 0, \alpha)^T.$$

Proto je vnější součin $[u_1, \dots, u_{n-1}, v]$ roven (viz. definice vektorového součinu)

$$[u_1, \dots, u_{n-1}, v] = \begin{vmatrix} u_{11} & \dots & u_{1(n-1)} & 0 \\ \vdots & & \vdots & \vdots \\ u_{(n-1)1} & \dots & u_{(n-1)(n-1)} & 0 \\ 0 & \dots & 0 & \alpha \end{vmatrix} = \langle v, v \rangle = \alpha^2.$$

Rozvojem determinantu podle posledního sloupce zároveň obdržíme

$$\alpha^2 = \alpha \operatorname{Vol} \mathcal{P}(0; u_1, \dots, i_{n-1}).$$

Odtud už vyplývají obě zbylá tvrzení věty. □

4.29. Kvadratické formy. Závěrem zmíníme ještě pár poznámek o objektech v $\mathcal{E}_n$ zadaných 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 $(x_1, \dots, x_n)$ bodů $A \in \mathcal{E}_n$

$$\sum_{i,j=1}^{n} a_{ij} x_i x_j + \sum_{i=1}^{n} 2a_i x_i + a = 0, \quad a_{ij} = a_{ji}.$$

Můžeme ji 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 hodnost f je nenulová (jinak by se jednalo o lineární rovnici popisující euklidovský podprostor).

Začněme s 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 $x = x_1 e_1 + \dots + x_n e_n$ 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 uvedená formula pro hodnotu formy s použitím zvolených souřadnic se nazývá *analytický tvar* formy. Jestliže změníme bázi e_i na jinou bázi $e'_1, \dots, e'_n$, dostaneme pro stejný vektor jiné souřadnice $x = S \cdot x'$ 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 intepretovat 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.

4.30. Euklidovská klasifikace kvadrik. Z poslední věty 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). Předpokládejme tedy přímo rovnici ve tvaru

$$\sum_{i=1}^{n} \lambda_i x_i^2 + \sum_{i=1}^{n} b_i x_i + b = 0.$$

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, viz poznámka níže) Tak nám zůstanou nejvýše ty neznámé, pro které byl jejich koeficient u kvadrátu nulový, a získáme tvar

$$\sum_{i=1}^{n} \lambda_i (x_i - p_i)^2 + \sum_{j \text{ splňující } \lambda_j = 0}^{n} b_j x_j + c = 0.$$

Pokud nám opravdu zůstaly nějaké lineární členy, můžeme zvolit novou bázi zaměření tak, aby odpovídající lineární forma byla prvkem duální báze a novou volbou počátku v $\mathcal{E}_n$ pak dosáhneme výsledného tvaru

$$\sum_{i=1}^{k} \lambda_i y_i^2 + b y_{k+1} + c = 0,$$

kde k je hodnost kvadratické formy f, 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 $b = 0$.

4.31. Případ $\mathcal{E}_2$. Proveďme celou diskusi ještě jednou pro nejjednodušší případ netriviální dimenze. Původní rovnice má tvar

$$a_{11}x^2 + a_{22}y^2 + 2a_{12}xy + a_1 x + a_2 y + a = 0.$$

Volbou vhodné báze zaměření a následným doplněním čtverců dosáhneme tvaru (opět používáme stejného značení x, y pro nové souřadnice):

$$a_{11}x^2 + a_{22}y^2 + a_1 x + a_2 y + a = 0$$

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:

$0 = x^2/a^2 + y^2/b^2 + 1$	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
$0 = x^2/a^2 - y^2/b^2$	2 různoběžné přímky
$0 = x^2 - a^2$	2 rovnoběžné přímky
$0 = x^2$	2 splývající přímky
$0 = x^2 + a^2$	prázdná množina

4.32. 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.

Pochopitelně se můžeme ptát, do jaké míry umíme podobnou věc v afinních prostorech, tj. s volností výběru jakékoliv afinní souřadné soustavy. Např. v rovině to bude znamenat, že neumíme rozlišit kružnici od elipsy, samozřejmě bychom ale 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 níže.

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

$$f(x_1, n) = \sum_{ij} a_{ij}x_ix_j,$$

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 $i \neq j$. 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 bazemi. 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

$$\begin{aligned} f(x_1, \ldots, x_n) &= a_{11}x_1^2 + 2a_{12}x_1x_2 + \cdots + a_{22}x_2^2 + \ldots \\ &= a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n)^2 + \text{členy neobsahující } x_1 \end{aligned}$$

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 bilinerání 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} dosud 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). □

4.33. Příklad. Nechť $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x_1, x_2, x_3) = 3x_1^2 + 2x_1x_2 + x_2^2 + 4x_2x_3 + 6x_3^2$. Její matice je

$$A = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 6 \end{pmatrix}.$$

Podle bodu (1) algoritmu 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:

$$z_3 = y_3 = x_3,\ z_2 = \frac{2}{3}y_2 + 2y_3 = \frac{2}{3}x_2 + 2x_3,\ z_1 = y_1 = 3x_1 + x_2$$

Pokud by ale např. $f(x_1, x_2, x_3) = 2x_1x_3 + x_2^2$, tj. matice je

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

pak hned v prvním kroku můžeme přehodit proměnné: $y_1 = x_2$, $y_2 = x_1$, $y_3 = x_3$. Aplikace kroku (1) je pak triviální (nejsou tu žádné společné členy), pro další krok ale nastane situace z bodu (4). Zavedeme tedy transformaci $z_1 = y_1$, $z_2 = y_2$, $z_3 = y_3 - y_2$. Pak

$$f(x_1, x_2, x_3) = z_1^2 + 2z_2(z_3 + z_2) = z_1^2 + \frac{1}{2}(2z_2 + z_3)^2 - \frac{1}{2}z_3^2.$$

Matici přechodu do příslušné polární báze opět dostaneme posbíráním jednotlivých transformací (tj. vynásobením jednotlivých dílčích matic přechodu).

4.34. 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 na našich volbách v průběhu algoritmu. Tyto počty nyzýváme *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*

$$f(u) = (\varphi_1(u))^2 + \cdots + (\varphi_p(u))^2 - (\varphi_{p+1}(u))^2 - \cdots - (\varphi_r(u))^2.$$

Jinak řečeno, existuje polární báze, ve které má f analytické vyjádření

$$f(x_1, \dots, x_n) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_r^2.$$

Počet p kladných diagonálních koeficientů v matici dané kvadratické formy nezávisí na volbě polární báze.

Dvě symetrické matice A, B dimenze n jsou maticemi téže kvadratické formy v různých bazích právě, když mají stejnou hodnost a když matice příslušných forem v polární bázi mají stejný počet kladných koeficientů.

Důkaz. Lagrangeovým algoritmem obdržíme $f(x_1, \dots, x_n) = \lambda_1 x_1^2 + \cdots + \lambda_r x_r^2$, $\lambda_i \neq 0$, v jisté bázi na V. Předpokládejme navíc, že právě prvních p koeficientů λ_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 φ_i pak jsou právě formy z duální báze ve V^* k získané polární bázi. Musíme ale ještě ukázat, že p nezávisí na našem postupu. Přepokládejme, že se nám podařilo najít vyjádření téže formy f v polárních bazích $\underline{u}$, $\underline{v}$, tj.

$$f(x_1, \dots, x_n) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_r^2$$
$$f(y_1, \dots, y_n) = y_1^2 + \cdots + y_q^2 - y_{q+1}^2 - \cdots - y_r^2$$

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 $f(v) \le 0$. 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 semidefitních 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) *positivně definitní*, je-li $f(u) > 0$ pro všechny $u \neq 0$
(2) *positivně semidefinitní*, je-li $f(u) \ge 0$ pro všechny $u \in V$
(3) *negativně definitní*, je-li $f(u) < 0$ pro všechny $u \neq 0$
(4) *negativně semidefinitní*, je-li $f(u) \le 0$ pro všechny $u \in V$

(5) *indefinitní*, je-li $f(u) > 0$ a $f(v) < 0$ pro vhodné $u, v \in V$.

Stejné názvy používáme i pro symetrické reálné matice, jsou-li maticemi patřičných kvadratických forem. Signaturou symetrické matice pak rozumíme signaturu příslušné kvadratické formy.

3. Projektivní geometrie

V mnoha elementárních textech o analytické geometrii autoři končí afinními a euklidovskými objekty popsanými výše. Na mnoho 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 totiž 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.

4.35. 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 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 $\mathcal{P}_2$ 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 a alespoň jedno z nich musí být nenulové. Přímka v projektivní rovině je definována jako množina jednorozměrných podprostorů (tj. bodů v $\mathcal{P}_2$)

Příklad. V afinním prostoru $\mathbb{R}^2$ uvažujme dvě přímky $L_1 : y - x - 1 = 0$ a $L_2 : y - x + 1 = 0$.
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

$$L_1 : y - x - z = 0, \quad L_2 : y - x + z = 0.$$

Podívejme se, jak budou rovnice těchto přímek 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 $(1 : 1 : 0)$).

4.36. Projektivní prostory a transformace. Postup z roviny 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 generují. Zbylé jednorozměrné podprostory vyplní rovinu rovnoběžnou s $\mathcal{A}_n$ a říkáme jim „nekonečné body“ v projektivním rozšíření $\mathcal{P}_n$ afinní roviny $\mathcal{A}_n$. Zjevně je vždy množina nekonečných bodů v $\mathcal{P}_n$ projektivním prostorem dimenze o jedničku nižším. Abstraktněji hovoříme o *projektivizaci vektorového prostoru*: pro libovolný vektorový prostor V dimenze $n+1$ definujeme

$$\mathcal{P}(V) = \{P \subset V;\ P \text{ je jednorozměrný vektorový podprostor}\}.$$

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 $\underline{u}$. Afinní přímka má tedy ve svém projektivním rozšíření pouze jediný bod (oba konce se „potkají“ v nekonečnu a projektivní přímka vypadá jako kružnice), projektivní rovina má projektivní přímku nekonečných bodů atd.

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 opačném směru v příkladu projektivní roviny.

Každé prosté lineární zobrazení $\tau : V_1 \to V_2$ 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*. 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.

4.37. Perspektivní projekce. Velmi dobře jsou výhody projektivní geometrie vidět na perspektivní projekci $\mathbb{R}^3 \to \mathbb{R}^2$. Bod (X, Y, Z) „reálného světa“ se 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 prostou lineární formulí

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -f & 0 & 0 & 0 \\ 0 & -f & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix}$$

Tento jednoduchý výraz zadává perspektivní projekci pro všechny konečné body v $\mathbb{R}^3 \subset \mathcal{P}_3$, které dosazujeme jako výrazy s $W = 1$. Navíc jsme odstranili problémy

s body, jejichž obraz leží v nekonečnu. 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.

4.38. Afinní a projektivní transformace. Invertibilní projektivní zobrazení projektivního prostoru $\mathcal{P}_n$ na sebe 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 nekonečné body, budou transformace, které zachovávají konečné 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 jedné. Matice projektivních transformací zachovávajících konečné body 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.

4.39. Projektivní klasifikace kvadrik. Závěrem ještě poznámka o složitějších objektech studovaných v afinní geometrii nejlépe prostřednictvím projektivních rozšíření. Jestliže popíšeme kvadriku v afinních souřadnicích pomocí obecné kvadratické rovnice, viz výše, jejím přepsáním v homogenních souřadnicích dostaneme vždy výlučně homogenní výraz, jehož všechny členy jsou druhého řádu. Důvod je ten, že pouze takové homogenní výrazy budou mít pro homogenní souřadnice smysl nezávisle na zvoleném konstantním násobku souřadnic $(x_0, x_1, \ldots, x_n)$. Hledáme tedy takový, jehož zúžením na afinní souřadnice, tj. dosazením $x_0 = 1$, získáme původní výraz. 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.

Získáme tak dobře definovanou kvadratickou formu na našem pomocném vektorovém prostoru $\mathbb{R}^{n+1}$, ale jsme už vůči libovolné volbě báze klasifikovali. Zkuste si samostatně převést tuto klasifikaci do projektivní i afinní podoby. (Hezké a náročné cvičení na závěr semestru!)

4.40. Příklad. *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:

$$\begin{aligned}
f(x_1,x_2,x_3) &= 2x_1x_2 + x_2x_3 \\
&\quad \text{provedeme substituci podle bodu (4) algoritmu } y_2 = x_2 - x_1,\ y_1 = x_1, y_3 = x_3 \\
&= 2x_1(x_1+y_2) + (x_1+y_2)x_3 = 2x_1^2 + 2x_1y_2 + x_1x_3 + y_2x_3 = \\
&= \frac{1}{2}(2x_1 + y_2 + \frac{1}{2}x_3)^2 - \frac{1}{2}y_2^2 - \frac{1}{8}x_3^2 + y_2x_3 = \\
&\quad \text{substituce } y_1 = 2x_1 + y_2 + \tfrac{1}{2}x_3 \\
&= \frac{1}{2}y_1^2 - \frac{1}{2}y_2^2 - \frac{1}{8}x_3^2 + y_2x_3 = \frac{1}{2}y_1^2 - 2(\frac{1}{2}y_2 - \frac{1}{2}x_3)^2 + \frac{3}{8}x_3^2 = \\
&\quad \text{substituce } y_3 = \tfrac{1}{2}y_2 - \tfrac{1}{2}x_3 \\
&= \frac{1}{2}y_1^2 - 2y_3^2 + \frac{3}{8}x_3^2.
\end{aligned}$$

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 standardní báze ke zvolené polární je tedy

$$T = \begin{pmatrix} 2 & 1 & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}.$$

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 bazí dané kvadratické formy je tedy například báze $\{(1/3, 1/3, 0), (-2/3, 4/3, 0), (-1/2, 1/2, 1)\}$. □

4.41. Příklad. *Určete typ kuželosečky dané rovnicí:*

$$3x_1^2 - 3x_1x_2 + x_2 - 1 = 0.$$

Řešení. Pomocí algoritmu úpravy na čtverec postupně dostáváme:

$$\begin{aligned}
3x_1^2 - 3x_1x_2 + x_2 - 1 &= \frac{1}{3}(3x_1 - \frac{3}{2}x_2)^2 - \frac{3}{4}x_2^2 + x_2 - 1 = \\
&= \frac{1}{3}y_1^2 - \frac{4}{3}(\frac{3}{4}x_2 - \frac{1}{2})^2 + \frac{1}{3} - 1 = \\
&= \frac{1}{2}y_1^2 - \frac{4}{3}y_2^2 - \frac{2}{3}.
\end{aligned}$$

Podle uvedeného seznamu kuželoseček se tedy jedná o hyperbolu. □

KAPITOLA 5

Zřízení ZOO

jaké funkce potřebujeme pro naše modely?
– pořádný zvěřinec...

1. Interpolace polynomy

Touto kapitolou započneme budování nástrojů umožňujících modelování závislostí, které nejsou ani lineární ani diskrétní. S takovou potřebou se např. setkáme, kdykoliv 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 procesech), jindy je to vhodné přiblížení diskrétního modelu (třeba u ekonomických nebo populačních modelů).

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 okruh skalárů, případně $\mathbb{N} \to V$, kde V je vektorový prostor nad $\mathbb{K}$. Připomeňme si diskusi z odstavce 1.3, kde jsme přemýšleli nad způsoby, jak pracovat se skalárními funkcemi. Na této diskusi se vůbec nic nemění 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 případ s vektorovými hodnotami nad stejnými skaláry, ve výkladu se ale zpravidla omezíme jen na případ reálných čísel, případně komplexních čísel.

Čím větší třídu funkcí připustíme, tím obtížnější bude vybudovat nástroje pro naši práci. Když ale bude různých typů funkcí málo, nebudeme patrně umět budovat dostatek modelů pro reálné situace. Cílem našich prvních dvou kapitol matematické analýzy bude proto explicitně zavést několik typů elementárních funkcí, implicitně popsat více funkcí a vybudovat standardní nástroje pro práci s nimi. Souhrnně se tomu říká diferenciální a integrální počet jedné proměnné.

5.1

5.1. Polynomy. Připomeňme si vlastnosti skalárů. Umíme je sčítat i násobit a tyto operace splňují řadu vlastností, které jsme vyjmenovali už v odstavcích 1.1 a 1.2. *Polynomem* nad okruhem skalárů $\mathbb{K}$ rozumíme zobrazení $f : \mathbb{K} \to \mathbb{K}$ dané výrazem

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

kde a_i, $i = 0, \ldots, n$, 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. Stupěň 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 $f(x)$, tj. jako posloupnosti koeficientů $a_0, a_1, \ldots$ s konečně mnoha nenulovými

prvky. Následující jednoduché lemma ukazuje, 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. Připomeňte si při této příležitosti vlastnosti skalárů a ověřte!

Nad každým polem skalárů (viz axiom „P“ v odstavcích 1.1 a 1.2) funguje dělení polynomů se zbytkem, tj. pro polynomy f stupně n a g stupně m, existují jednoznačně určené polynomy q a r takové, že stupeň r je menší než m nebo je $r = 0$ a $f = q \cdot g + r$. 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 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 konstatnímu 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:

Lemma. *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. Uvažte např. polynom $x^2 + x$ nad $\mathbb{Z}_2$.

5.2

5.2. Interpolační polynom. Častá praktická úloha vyžaduje stanovení počítatelné formule pro funkci, pro kterou máme zadány hodnoty v předem daných daných bodech $x_0, \dots, x_n$. Pokud by šlo o nulové hodnoty, umíme přímo zadat polynom

$$f(x) = (x - x_0)(x - x_1) \dots (x - x_n),$$

který bude mít nulové hodnoty právě v těchto bodech a nikde jinde. To ale není jediná 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:

Věta. *Nechť $\mathbb{K}$ je nekonečné pole skalárů, pak pro každnou množinu po dvou různých bodů $x_0, \dots, x_n \in \mathbb{K}$ a předepsaných hodnot $y_0, \dots, y_n \in \mathbb{K}$ existuje právě jeden polynom f stupně nejvýše n (případně nulový polynom), pro který platí*

$$f(x_i) = y_i, \quad i = 0, \dots, n.$$

Důkaz. Označme si prozatím neznámé koeficienty polynomu f stupně n

$$f = a_n x^n + \dots + a_1 x + a_0.$$

Dosazením požadovaných hodnot dostaneme systém $n + 1$ rovnic pro stejný počet neznámých koeficientů a_i

$$\begin{aligned} a_0 + x_0 a_1 + \dots + (x_0)^n a_n &= y_0 \\ &\vdots \\ a_0 + x_n a_1 + \dots + (x_n)^n a_n &= y_n. \end{aligned}$$

Jak je dobře známo z lineární algebry, tento systém lineárních rovnic má právě jedno řešení pokud je determinant jeho matice invertibilní skalár, tj. pokud je nenulový (viz 3.1 a 2.22). Musíme tedy vyšetřit tzv. *Vandermondův determinant*

$$V(x_0,\dots,x_n) = \det \begin{pmatrix} 1 & x_0 & (x_0)^2 & \dots & (x_0)^n \\ 1 & x_1 & (x_1)^2 & \dots & (x_1)^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & (x_n)^2 & \dots & (x_n)^n \end{pmatrix}.$$

Tento determinant umíme nad libovolným nekonečným polem skalárů snadno spočíst:

Lemma. *Pro všechny hodnoty $x_0,\dots,x_n \in \mathbb{K}$ platí*

$$V(x_0,\dots,x_n) = \prod_{i>k=0}^{n} (x_i - x_k).$$

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.

$$V(x_0,\dots,x_{n-1}) = \prod_{i>k=0}^{n-1} (x_i - x_k).$$

Nyní považujme hodnoty $x_0,\dots,x_{n-1}$ za pevné a hodnotu x_n ponechme jako volnou proměnnou. Rozvojem determinantu podle posledního řádku (viz 2.19) obdržíme hledaný determinant jako polynom

e5.1 (5.1) $$V(x_0,\dots,x_n) = (x_n)^n V(x_0,\dots,x_{n-1}) - (x_n)^{n-1}\cdots .$$

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.

$$V(x_0,\dots,x_n) = c\cdot(x_n - x_0)(x_n - x_1)\cdots(x_n - x_{n-1}).$$

Porovnáním koeficientů u nejvyšší mocniny v (5.1) a tomto výrazu dostáváme

$$c = V(x_0,\dots,x_{n-1})$$

a tím je důkaz lemmatu ukončen. □

Ukázali jsme, že je determinant naší soustavy rovnic vždy roven součinu rozdílů definičních bodů. Pro naše po dvou různé body x_i tedy musí být nenulový. Odtud ale vyplývá jednoznačná existence řešení. Protože polynomy jsou jako zobrazení stejné, právě když mají stejné koeficienty, věta je dokázána. □

Jednoznačně určený polynom f z předchozí věty nazýváme *interpolační polynom* pro hodnoty y_i v bodech x_i.

5.3

5.3. Poznámky. Uvažujme nyní pro jednoduchost pouze reálné nebo případně racionální polynomy, tj. polynomiálně zadané funkce $\mathbb{R} \to \mathbb{R}$ nebo $\mathbb{Q} \to \mathbb{Q}$. Na první pohled se může zdát, že polynomy tvoří hezkou velikou třídu funkcí jedné proměnné, kterou můžeme použít na proložení 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 hustějších 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 intepolačního polynomu (tj. vybereme lepší bázi příslušného vektorového prostoru všech polynomů stupně nejvýše k, než je ta nejobvyklejší $1, x, x^2, \ldots, x^n$).

Jednou z možností je tzv. *Lagrangeův interpolační polynom*, kterým rychle a snadno zapíšeme řešení. Sestrojíme si nejprve pomocné polynomy ℓ_i s vlastností

$$\ell_i(x_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

Zřejmě musí být tyto polynomy až na konstantu rovny výrazům $(x - x_0) \ldots (x - x_{i-1})(x - x_{i+1}) \ldots (x - x_n)$ a proto

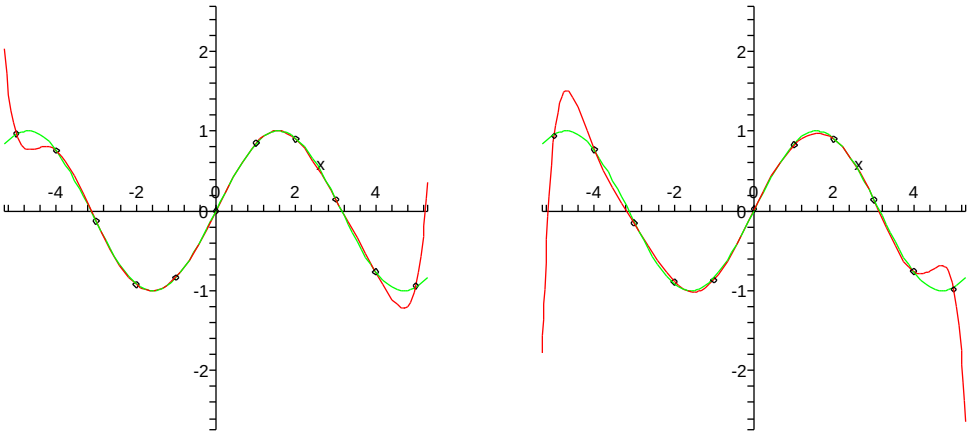
$$\ell_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}.$$

Hledaný Lagrangeův interpolační polynom pak snadno zadáme formulí

$$f(x) = y_0\ell_0(x) + y_1\ell_1(x) + \cdots + y_n\ell_n(x).$$

Toto vyjádření má nevýhodu ve velké citlivosti na nepřesnosti výpočtu při malých rozdílech zadaných hodnot x_i, protože se v ní těmito rozdíly dělí. Všimněme si ale, že přímá konstrukce Lagrangeova polynomu může nahradit existenční část důkazu v předchozí Větě 5.2. (Jednoznačnost pak je také jednoduchá i bez příslušné lineární algebry: dvě možná řešení f a g mají stejné hodnoty v $n + 1$ různých bodech, tj. polynom $f - g$ má $n + 1$ různých kořenů a stupeň nejvýše n a proto musí být nulovým polynomem.)

Ještě horším problémem 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. Zelenou barvou je vynesena aproximovaná funkce, kolečka jsou malinko posunuté hodnoty a červeně je vynesen jednoznačně zadaný interpolační polynom. Zatímco uvnitř intervalu je aproximace vcelku dobrá, stabilita na okrajích je otřesná.



Kolem interpolačních polynomů existuje bohatá teorie. Částečně se budeme k některým jejich vlastnostem vracet, podrobnější rozbor lze najít např. v pěkných textech [**11**].

5.4. Určování interpolačních polynomů.

5.4.1. *Nalezněte polynom P splňující následující podmínky:*

$$P(2) = 1,\ P(3) = 0,\ P(4) = -1,\ P(5) = 6.$$

Řešení. Řešíme buď přímo, t.j. 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 podmínky v zadání je dán jednoznačně.

$$\begin{aligned} a_0 + 2a_1 + 4a_2 + 8a_3 &= 1 \\ a_0 + 3a_1 + 9a_2 + 27a_3 &= 0 \\ a_0 + 4a_1 + 16a_2 + 64a_3 &= -1 \\ a_0 + 5a_1 + 25a_2 + 125a_3 &= 6. \end{aligned}$$

Každá rovnice vznikla z jedné z podmínek v zadání.

Druhou možností je vytvořit hledaný polynom pomocí fundamentálních Lagrangeových polynomů:

$$\begin{aligned} P(x) &= 1 \cdot \frac{(x-3)(x-4)(x-5)}{(2-3)(2-4)(2-5)} + 0 \cdot (\dots) + \\ &= (-1) \cdot \frac{(x-2)(x-3)(x-5)}{(4-2)(4-3)(4-5)} + 6 \cdot \frac{(x-2)(x-3)(x-4)}{(5-2)(5-3)(5-4)} = \\ &= \frac{4}{3}z^3 - 12z^2 + \frac{101}{3}z - 29. \end{aligned}$$

Koeficienty tohoto polynomu jsou samozřejmě jediným řešením výše sestavené soustavy lineárních rovnic. □

5.4.2. *Nalezněte polynom P splňující následující podmínky:*

$$P(1+i) = i,\ P(2) = 1,\ P(3) = -i.$$

Řešení. $P(x) = (-\frac{3}{5} - \frac{4}{5}i)x^2 + (2+3i)x - \frac{3}{5} - \frac{14}{5}i$. □

5.4

5.5. 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.

Pro tento účel 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

e5.2 (5.2) $$\frac{f(x+\Delta x) - f(x)}{\Delta x}$$

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

$$\begin{aligned}\frac{f(x+\Delta x) - f(x)}{\Delta x} &= a_n \frac{nx^{n-1}\Delta x + \cdots + (\Delta x)^k}{\Delta x} + \cdots + a_1 \frac{\Delta x}{\Delta x} \\ &= na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 + \Delta x(\dots),\end{aligned}$$

kde výraz v závorce je polynomiálně závislý na Δx. Evidentně pro hodnoty Δx velice blízké nule dostaneme hodnotu libovolně blízkou výrazu

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1,$$

který nazýváme *derivace polynomu* f podle proměnné x. 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, přímka

$$y = f'(x_0)(x - x_0) + f(x_0)$$

velice dobře aproximuje přímky procházející body $[x_0, f(x_0)]$ a $[x_0+\Delta x, f(x_0+\Delta x)]$ pro malé hodnoty Δx. 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. S tímto lineárním zobrazením jsme se již potkali v odstavci 2.45 o nilpotentních zobrazeních.

5.5

5.6. Hermiteův interpolační problém. Uvažme opět $m+1$ po dvou různých reálných nebo racionálních hodnot $x_0, \dots, x_m$, tj. $x_i \neq x_j$ pro všechna $i \neq j$. Předepišme dále hodnoty $y_i^{(k)}$ aproximované funkce a jejich derivací pro $k = 0$ a $k = 1$. To znamená, že máme předepsány hodnoty a první derivace v zadaných bodech x_i. Hledáme polynom f, který bude nabývat těchto předepsaných hodnot a derivací.

Zcela analogicky jako u interpolace pouhých hodnot obdržíme pro neznámé koeficienty polynomu $f(x) = a_n x^n + \dots a_0$ systém rovnic

$$\begin{aligned} a_0 + x_0 a_1 + \cdots + (x_0)^n a_n &= y_0^{(0)} \\ &\vdots \\ a_0 + x_m a_1 + \cdots + (x_m)^n a_n &= y_m^{(0)} \\ a_1 + 2x_0 a_2 + \cdots + n(x_0)^{n-1} a_n &= y_0^{(1)} \\ &\vdots \\ a_1 + 2x_m a_2 + \cdots + n(x_m)^{n-1} a_n &= y_m^{(1)}. \end{aligned}$$

Opět bychom mohli ověřit, že při volbě $n = 2m+1$ bude determinant tohoto systému rovnic nenulový a tudíž bude existovat právě jedno řešení. Nicméně, stejně jako při konstrukci Lagrangeova polynomu lze zkonstruovat takový polynom f přímo. Nazýváme jej *Hermiteův interpolační polynom.*

Hermiteův polynom můžeme určit podobně pomocí fundamentálních Hermiteových polynomů:

$$\begin{aligned} h_i^1(x) &= \left[1 - \frac{l''(x_i)}{l'(x_i)}(x - x_i)\right] (l_i(x))^2 \\ h_i^2(x) &= (x - x_i)\,(l_i(x))^2, \end{aligned}$$

kde $l(x) = \prod_{i=1}^n (x - x_i)$. Tyto polynomy splňují následující podmínky:

$$\begin{aligned} h_i^1(x_j) &= \delta_i^j = \begin{cases} 1 & \text{pro } i = j \\ 0 & \text{pro } i \neq j \end{cases} \\ (h_i^1)'(x_j) &= 0 \\ h_i^2(x_j) &= 0 \\ (h_i^2)'(x_j) &= \delta_i^j \end{aligned}$$

Máme-li dán systém podmínek $f(x_1) = y_1$, $f'(x_1) = y_1', \dots, f(x_k) = y_k$, $f'(x_k) = y_k'$, pak je odpovídající polynom dán předpisem

$$f(x) = \sum_{i=1}^{k} [y_i h_i^1(x_i) + y_i' h_i^2(x_i)].$$

Úplně nejjednodušší případ je zadání hodnoty a derivace v jediném bodě. Tím určíme beze zbytku polynom stupně 1

$$f(x) = f(x_0) + f'(x_0)(x - x_0)$$

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 v 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 $(a_3, a_2, a_1, a_0)^T$ koeficientů polynomu f, tj.

$$f(x) = (2y_0 - 2y_1 + y_0' + y_1')x^3 + (-3y_0 + 3y_1 - 2y_0' - y_1')x^2 + y_0'x + y_0.$$

V případě, že máme zadány hodnoty a derivace v jiných bodech x_0 a x_1, lze využít tohoto výsledku s pomocí vhodné afinní transformace $\mathbb{R} \to \mathbb{R}$ (pozor ale na vliv transformace na velikosti derivací, podrobněji budeme podobné úkony diskutovat později).

5.6.1. *Příklad Nalezněte polynom P splňující následující podmínky:*

$$P(1) = 0, P'(1) = 1, P(2) = 3, P'(2) = 3.$$

Řešení. Opět ukážeme dvě možnosti řešení. **1.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. $P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$):

$$\begin{aligned} P(1) = &\quad (a_3 + a_2 + a_1 + a_0 &&= 0,\\ P'(1) = &\quad 3a_3 + 2a_2 + a_1 = &&1,\\ P(2) = &\quad 8a_3 + 4a_2 + 2a_1 + a_0 = &&3,\\ P'(2) = &\quad 12a_3 + 4a_2 + a_1 = &&3. \end{aligned}$$

Vyřešením tohoto systému obdžíme polynom $P(x) = -2x^3 + 10x^2 - 13x + 5$.

2.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

$$P(x) = 0 \cdot h_1^1(x) + 3 \cdot h_2^1(x) + 1 \cdot h_1^2(x) + 3 \cdot h_2^2(x) = -2x^3 + 10x^2 - 13x + 5.$$

□

Obdobně lze předepisovat libovolný konečný počet derivací v jednotlivých bodech a vhodnou volbou stupně polynomu obdržíme vždy jednoznačné interpolace. Nebudeme zde uvádět podrobnosti, viz opět text [**11**].

Bohužel, u těchto interpolací pořád zůstávají problémy zmíněné už v případě jednoduchých interpolací hodnot – složitost výpočtů a nestabilita. Použití derivací však podbízí jednoduché vylepšení metodiky:

5.6

5.7. Interpolace splajny. [1] Jak jsme viděli na obrázcích demonstrujících nestabilitu interpolace jedním polynomem dostatečně vysokého stupně, malé lokální změny hodnot zapřičiňovaly dramatické celkové změkjny chování výsledného polynomu. Nabízí se tedy využití malých polynomiálních kousků, které ale musíme umět rozumně navazovat.

[1] Ošklivé české slovo „splajn“ vzniklo fonetickým přepisem anglického ekvivalentu „spline“, který znamenal tvárné pravítko užívané inženýry pro kreslení křivek.

Nejjednodušší je propojení vždy dvou sousedních bodů lineárním polynomem. 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 přiblížení po kouskách už bude mít tu vlastnost, že derivace na sebe budou navazovat.

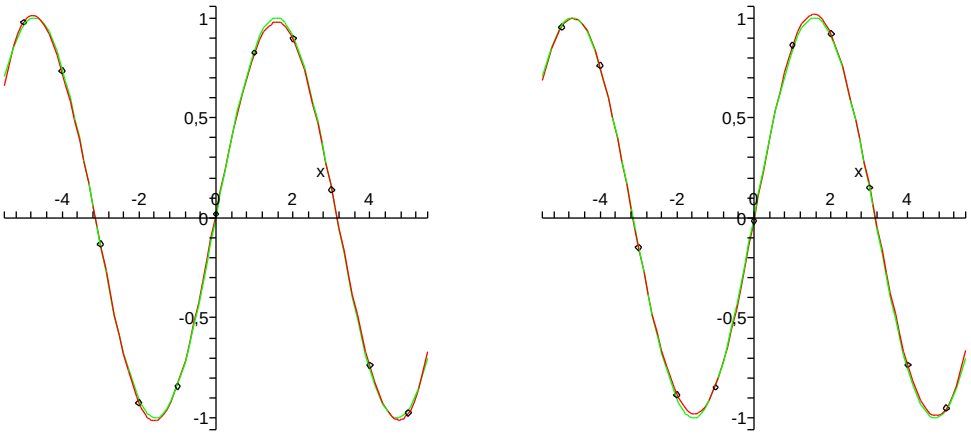
V praxi ale není pouhé navazování první derivace dostatečné a navíc při naměřených datech nemíváme hodnoty derivací k dispozici. Přímo se proto vnucuje pokus využívat pouze zadané hodnoty ve dvou sousedních bodech, ale požadovat zároveň rovnost prvních i druhých derivací u sousedních kousků polynomů třetího stupně:

Definice. Nechť $x_0 < x_1 < \cdots < x_n$ jsou reálné (nebo racionální) hodnoty, ve kterých jsou zadány požadované hodnoty $y_0, \ldots, y_n$. *Kubickým interpolačním splajnem* pro toto zadání je funkce $S : \mathbb{R} \to \mathbb{R}$ (nebot $S : \mathbb{Q} \to \mathbb{Q}$), která splňuje následující podmínky:

- zúžení S na interval $[x_{i-1}, x_i]$ je polynom S_i třetího stupně, $i = 1, \ldots, n$
- $S_i(x_{i-1}) = y_{i-1}$ a $S_i(x_i) = y_i$ pro všechny $i = 1, \ldots n$,
- $S_i'(x_i) = S_{i+1}'(x_i)$ pro všechny $i = 1, \ldots, n-1$,
- $S_i''(x_i) = S_{i+1}''(x_i)$ pro všechny $i = 1, \ldots, n-1$.

Kubický splajn 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*.

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. Podrobnosti vynecháme, lze je dohledat např. v [**11**]. Pro srovnání se podívejme na interpolaci stejných dat jako v případě Lagrangeova polynomu, nyní pomocí splajnů:



2. Spojité funkce

Viděli jsme právě, že 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 nástroje pro práci s nimi.

Polynomů je přitom zjevně příliš málo, i když jejich šikovné využití ve splajnech může ledacos vynahradit. Nejvýraznější 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

$$f(x) = \begin{cases} 0 & \text{pro všechny } x < 0 \\ 1/2 & \text{pro } x = 0 \\ 1 & \text{pro všechny } x > 0 \end{cases}$$

taková „nespojitost“ nastane pro $x = 0$.

Začneme formalizací takovýchto intuitivních výroků. K tomu budeme potřebovat upřesnit vlastnosti našich skalárů a zasvést pojem limity.

5.7

5.8. Reálná a komplexní 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 1.45). Připoměňme si nyní vlastnosti (axiomy) reálných čísel včetně souvislostí uspořádání a ostatních relací. Dělící čáry 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. druhá odmocnina ze dvou v číslech racionálních. Formálně poslední axiom vysvětlíme níže.

(R1)	$(a+b)+c = a+(b+c)$, pro všechny a, b, $c \in \mathbb{R}$
(R2)	$a+b = b+a$, pro všechny a, $b \in \mathbb{R}$
(R3)	existuje prvek $0 \in \mathbb{R}$ takový, že pro všechny $a \in \mathbb{R}$ platí $a+0 = a$
(R4)	pro všechny $a \in \mathbb{R}$ 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 všechny a, b, $c \in \mathbb{R}$
(R6)	$a \cdot b = b \cdot a$ pro všechny a, $b \in \mathbb{R}$
(R7)	existuje prvek $1 \in \mathbb{R}$ takový, že pro všechny $a \in \mathbb{R}$ platí $1 \cdot a = a$
(R8)	pro každý $a \in \mathbb{R}$, $a \neq 0$ 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 všechny a, b, $c \in \mathbb{R}$
(R10)	relace $\leq$ je úplné uspořádání, tj. reflexivní, antisymetrická, tranzitivní a úplná relace na $\mathbb{R}$
(R11)	pro všechny $a, b, c \in \mathbb{R}$ platí, že z $a \leq b$ vyplývá také $a+c \leq b+c$
(R12)	pro všechny $a, b \in \mathbb{R}$, $a > 0$, $b > 0$, platí také $a \cdot b > 0$
(R13)	každá neprázdná ohraničená množina $A \subset \mathbb{R}$ má supremum.

Pojem suprema má smysl pro každou uspořádanou množinu. Uvažme podmnožinu $A \subset B$ v uspořádané množině B. *Horní závorou* množiny A je každý prvek $b \in B$, pro který platí, že $b \geq a$ pro všechny $a \in A$. Obdobně definujeme *dolní závory* množiny A jako prvky $b \in A$ takové, že $b \leq a$ pro všechny $a \in A$.

Nejmenší horní závora podmnožiny A, pokud existuje, se nazývá *supremum* této podmnožiny a značíme ji $\sup A$. Přesněji:

$$\sup A = b, \text{ jestliže z } c \geq a \text{ pro všechny } a \in A \text{ vyplývá také } c \geq b.$$

Obdobně, největší dolní závora se nazývá *infimum*, píšeme $\inf A$, tzn.

$$\inf A = b, \text{ jestliže z } c \leq a \text{ pro všechny } a \in A \text{ vyplývá také } c \leq b.$$

Pro formální výstavbu další teorie potřebujeme vědět, zda námi požadované vlastnosti reálných čísel lze realizovat, tj. zda existuje taková množina $\mathbb{R}$ s operacemi a relací uspořádání, které (R1)–(R13) splňují. Skutečně 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, jednoznačnost nebudeme diskutovat vůbec a existenci jen naznačíme v dalším odstavci.

Pole komplexních čísel splňuje axiomy (R1)–(R9), není na nich ale žádným rozumným způsobem definováno uspořádání, které by naplnilo axiomy (R10)–R(13). Nicméně s nimi budeme také občas pracovat a již dříve jsme viděli, že rozšíření skalárů na komplexní čísla je často pro výpočty mimořádně užitečné. Protože jsou komplexní čísla $z = \operatorname{re} z + i \operatorname{im} z$ dána jako dvojice reálných čísel, je dobrou představou rovina komplexních čísel.

Operací, která je u komplexních čísel navíc je tzv. *konjugace*. Je to zrcadlení podle přímky reálných čísel, tj. obrácení znaménka u imaginární složky. Značíme ji pruhem nad daným číslem, $\bar{z} = \operatorname{re} z - i \operatorname{im} z$. 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. Odmocnině z tohoto reálného nezáporného čísla říkáme absolutní hodnota komplexního čísla z, píšeme

e5.3 (5.3) $$|z|^2 = z \cdot \bar{z}$$

5.8.1. *Načrtněte následující podmnožiny v* $\mathbb{C}$

(1) $\{z \in \mathbb{C} |\, |z-1| = |z+1|\}$
(2) $\{z \in \mathbb{C} |\, 1 \le |z-i| \le 2\}$
(3) $\{z \in \mathbb{C} |\, \mathrm{Re}(z^2) = 1\}$
(4) $\{z \in \mathbb{C} |\, \mathrm{Re}(\frac{1}{z}) < \frac{1}{2}\}$

Řešení.

- imaginární osa
- mezikruží okolo i
- hyperbola $a^2 - b^2 = 1$.
- vnějšek jednotkového kruhu se středem v 1.

□

5.8

5.9. Hromadné body a konvergence. Uvažujme na chvíli nějaké pole skalárů $\mathbb{K}$, které splňuje axiomy (R1)–(R12). Takové určitě existuje, protože racionální čísla $\mathbb{Q}$ jsou příkladem. Zkonstruovali jsme je v odstavci 1.47 a čtenář si snadno může ověřit platnost všech požadovaných axiomů. Pro každý prvek $a \in \mathbb{K}$ definujeme jeho *absolutní hodnotu* $|a|$ takto

$$|a| = \begin{cases} a & \text{je-li } a \ge 0 \\ -a & \text{je-li } a < 0. \end{cases}$$

Samozřejmě platí pro každá dvě čísla $a, b \in \mathbb{K}$

e5.4 (5.4) $$|a+b| \le |a| + |b|.$$

Této vlastnosti říkáme trojúhelníková nerovnost a splňuje ji také absolutní hodnota komplexních čísel definovaná výše.

Uvažme nyní libovolnou posloupnost prvků $a_0, a_1, \dots$ v našem uspořádaném poli $\mathbb{K}$ takovou, že pro libolné pevně zvolené kladné číslo $\epsilon > 0$ platí pro všechny prvky a_k až na konečně mnoho výjimek

$$|a_i - a_j| < \epsilon.$$

Jinak řečeno, pro každé pevné $\epsilon > 0$ 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.

Pokud by taková hodnota $a \in \mathbb{K}$ existovala, očekávali bychom od ní patrně následující vlastnost: pro libovolné pevně zvolené číslo ϵ platí pro všechny i, až na konečně mnoho výjimek,

$$|a_i - a| < \epsilon.$$

Říkáme v takovém případě, že posloupnost a_i, $i = 1, 2, \dots$ *konverguje* k hodnotě $a \in \mathbb{K}$.

Uvažme nyní jakoukoliv množinu $A \subset \mathbb{K}$ a předpokládejme, že naše posloupnost je vybraná z prvků A. Pokud konverguje k $a \in \mathbb{K}$ a navíc je nekonečně mnoho bodů $a_i \in A$ různých od a, hovoříme o *hromadném bodu* množiny A.

Jestliže nějaká posloupnost $a_i \in \mathbb{K}$ konverguje k $a \in \mathbb{K}$, pak pro zvolené ϵ víme, že $|a_i - a| < \epsilon$ pro vhodné $N \in \mathbb{N}$ a všechny $i \geq N$. Pak pro $i, j \geq N$ dostaneme

$$|a_i - a_j| < |a_i - a_N| + |a_N - a_j| < 2\epsilon.$$

Vidíme tedy, že každá konvergující posloupnost je Cauchyovská.

V poli racionálních čísel se může snadno stát, že pro takovéto posloupnosti příslušná hodnota a neexistuje. Např. číslo $\sqrt{2}$ můžeme libovolně přesně přiblížit racionálními čísly a_i, ale samotná odmocnina racionální není. Uspořádaná pole skalárů, ve kterém všechny Caychyovské posloupnosti konvergují, se nazývají *úplná*. Následující tvrzení říká, že axiom (R13) takové chování zaručuje:

Lemma. *Každá Cauchyovská posloupnost reálných čísel a_i konverguje k reálné hodnotě $a \in \mathbb{R}$.*

Důkaz. Každá Cauchyovská posloupnost je zjevně ohraničená množina (dokažte si podrobně – pro libovolné ϵ ohraničíte všechny členy až na konečně mnoho z nich!). Definujme si množinu

$$B = \{x \in \mathbb{R},\ x < a_j \text{ pro všechny prvky } a_i, \text{ až na konečně mnoho z nich}\}.$$

Zřejmě má B horní závoru, tudíž podle axiomu (R13) má i supremum. Definujme $a = \sup B$. Nyní pro nějaké $\epsilon > 0$ zvolme N takové, aby $|a_i - a_j| < \epsilon$ pro všechny $i, j \geq N$. Zejména pak

$$a_j > a_N - \epsilon,\ a_j < a_N + \epsilon$$

takže $a_N - \epsilon$ patří do B, zatímco $a_N + \epsilon$ už nikoliv. Souhrnně z toho dostáváme, že $|a - a_N| \leq \epsilon$, a proto také

$$|a - a_j| \leq |a - a_N| + |a_N - a_j| \leq 2\epsilon$$

pro všechny $j > N$. To ale značí právě, že a je hromadný bod posloupnosti. □

Při jedné z možností, jak 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). Skutečně, vhodným formálním způsobem přidáme všechny chybějící hromadné body pro podmnožiny racionálních čísel (např. vhodným způsobem zavedeme ekvivalenci na množině všech Cauchyovských posloupností racionálních čísel). Pak se lze již snadno přesvědčit, že všechny požadované axiomy skutečně dojdou naplnění.

Další teorické nuance tady není vhodné rozebírat. Zájemce může ale nahlédnout např. do [5] pro další informace i odkazy.

5.9

5.10. Otevřené a uzavřené množiny. *Uzavřená podmnožina* v $\mathbb{R}$ je taková, která obsahuje i všechny své hromadné body. Typickou uzavřenou množinou je tzv. *uzavřený interval*

$$[a, b] = \{x \in \mathbb{R},\ a \leq x \leq b\}.$$

Zde a je reálné číslo nebo hraniční hodnota chybí a píšeme $a = -\infty$ (mínus nekonečno) a podobně $b > a$ je reálné číslo nebo $+\infty$. Uzavřenou množinu bude tvořit i posloupnost reálných čísel bez hromadného bodu nebo posloupnost s konečným počtem hromadných bodů spolu s těmito body. Zjevně je konečné sjednocení uzavřených množin opět uzavřená množina.

Otevřená množina v $\mathbb{R}$ je taková množina, jejíž doplněk je uzavřenou množinou. Typickou otevřenou množinou je *otevřený interval*

$$(a, b) = \{x \in \mathbb{R},\ a < x < b\},$$

kde pro hraniční hodnoty máme stejné možnosti jako výše.

Okolím bodu $a \in \mathbb{R}$ nazýváme libovolný otevřený interval $\mathcal{O}$, který a obsahuje. Je-li okolí definované jako interval

$$\mathcal{O}_\delta(a) = (a - \delta, a + \delta)$$

pro kladné číslo δ, hovoříme o δ-*okolí* bodu a.

Všimněme si, že pro libovolnou množinu A je $a \in \mathbb{R}$ hromadným bodem A, právě když v libovolném okolí a leží také alespoň jeden bod $b \in A$, $b \neq a$.

Lemma. *Množina reálných čísel A 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 $a_n \notin A$, $|a - a_n| \leq 1/n$. Pak je ovšem $a \in A$ hromadným bodem množiny $\mathbb{R} \setminus A$, 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 $\mathbb{R} \setminus A$ ležel v A. Je proto $\mathbb{R} \setminus A$ uzavřená a tedy je A otevřená. □

Zjevně je libovolné sjednocení otevřených množin opět otevřenou množinou a každý konečný průnik otevřených množin je opět otevřená množina.

Množina A reálných čísel se nazývá *ohraničená*, jestliže celá leží v nějakém konečném intervalu $[a, b]$, $a, b \in \mathbb{R}$. V opačném případě je *neohraničená*. Ohraničená a uzavřená množina se nazývá *kompaktní*.

5.10

5.11. Několik topologických vlastností. Přidejme ještě několik pojmů, které nám umožní účinné vyjadřování. *Vnitřním bodem množiny* A reálných 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 $\mathbb{R} \setminus A$. *Otevřené pokrytí* množiny A je takový systém otevřených intervalů 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 $\{a\}$.

Věta. *Pro podmnožiny A reálných čísel platí:*

(1) *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 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 pokrytí.*

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 (a, b) je v A. To je zjevně relace ekvivalence a její třídy 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 poslední argumentaci 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 a (nebo můžeme zvolit libovolnou horní a dolní závoru množiny A). Rozdělme nyní interval $[a, b]$ přesně na dvě poloviny $[a, \frac{1}{2}(b-a)]$ a $[\frac{1}{2}(b-a), b]$. V alespoň jedné z nich musí být nekonečně mnoho prvků a_i. Vyberme takovou polovinu, jeden z prvků v ní obsažených a následně tento interval opět rozdělme uvažovaný interval na poloviny. 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 si jen pozorné hraní 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. Jistě lze A pokrýt spočetným systémem intervalů $I_n = (n-2, n+2)$, $n \in \mathbb{Z}$, a jakýkoliv výběr konečně mnoha 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 $|a - a_n| < \frac{1}{n}$. Množiny

$$J_n = \mathbb{R} \setminus [a - \frac{1}{n}, a + \frac{1}{n}]$$

pro všechny $n \in \mathbb{N}$, $n > 0$, 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 je opět založený na existenci a vlastnostech suprem. 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 „nejzašší mez“, pro kterou ještě půjde konečné pokrytí vybrat:

$$B = \{x \in [a, b],\ \text{a existuje výběr konečného pokrytí } [a, x] \cap A \text{ z } \mathcal{C}\}.$$

Evidentně $a \in B$, jde tedy o neprázdnou zhora 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 $a < c \leq b$, předpokládejme tedy chvíli, že $c < b$. 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 $c \in A$ 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 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. □

5.11.1. *Určete hromadné, izolované, hraniční a vnitřní body následujících podmnožin v $\mathbb{R}$:*

(1) $\mathbb{N}$
(2) $\mathbb{Q}$
(3) $\{x \in \mathbb{R} | \, 0 \leq x < 1\}$.

Svá tvrzení zdůvodněte.

Řešení.

(1) $\emptyset$, $\mathbb{N}$, $\mathbb{N}$, $\emptyset$
(2) $\mathbb{R}$, $\emptyset$, $\mathbb{R}$, $\emptyset$
(3) $\langle 0, 1\rangle$, $\emptyset$, $\{0, 1\}$, $(0, 1)$

□

5.11

5.12. Limity funkcí a posloupností. Pro diskusi limit je vhodné rozšířit množinu reálných čísel $\mathbb{R}$ o dvě nekonečné hodnoty $\pm\infty$. Pro tyto účely si zavádíme i pravidla pro počítání s těmito formálně přidanými hodnotami pro libovolná „konečná“ čísla $a \in \mathbb{R}$:

$$\begin{aligned} a + \infty &= \infty \\ a - \infty &= -\infty \\ a \cdot \infty &= \infty, \text{ je-li } a > 0 \\ a \cdot \infty &= -\infty, \text{ je-li } a < 0 \end{aligned}$$

Okolím nekonečna rozumíme interval (a, ∞), resp. $(-\infty, a)$ je okolí $-\infty$. Pojem hromadného bodu množin rozšiřujeme tak, že ∞ je hromadným bodem množiny $A \subset \mathbb{R}$ jestliže každé okolí ∞ s ní má neprázdný průnik, tj. jestliže je A zprava neohraničená. Obdobně pro $-\infty$.

Protože je užitečné od začátku sledovat i možné komplexní hodnoty funkcí, rozšíříme také pojem okolí do komplexní roviny. Pro kladné reálné číslo δ rozumíme δ-okolím komplexního čísla $z \in \mathbb{C}$ množinu

$$\mathcal{O}_\delta(z) = \{w \in \mathbb{C}, |w - z| < \delta\}.$$

Definice. Nechť $A \subset \mathbb{R}$ je libovolná podmnožina a $f : A \to \mathbb{R}$ je reálná funkce (nebo $f : A \to \mathbb{C}$ je komplexní funkce) definovaná na A a nechť x_0 je hromadný bod množiny A. Říkáme, že f má v x_0 *limitu* $a \in \mathbb{R}$ (nebo $a \in \mathbb{C}$) a píšeme

$$\lim_{x \to x_0} f(x) = a,$$

jestliže pro každé okolí bodu $O(a)$ bodu a lze najít okolí $\mathcal{O}(x_0)$ bodu x_0 takové, že pro všechny $x \in A \cap (\mathcal{O}(x_0) \setminus \{x_0\})$ je $f(x) \in \mathcal{O}(a)$.

Limita reálné funkce se nazývá *nevlastní*, jestliže je $a = \pm\infty$, V opačném případě se nazává *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! Také je zřejmé, že nevlastní limity komplexních funkcí nejsou definovány.

5.12

5.13. Příklady. (1) Jestliže je $A = \mathbb{N}$, tj. funkce f je definována pouze pro přirozená čísla, hovoříme o limitách posloupností reálných nebo komplexních hodnot. Jediným hromadným bodem A je pak ∞ a píšeme pro $f(n) = a_n$

$$\lim_{n \to \infty} a_n = a.$$

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 všechny $n \geq N$. Ve skutečnosti jsme tedy v tomto speciálním případě přeformulovali definici konvergence posloupnosti (viz 5.9). Říkáme také, že posloupnost a_n konverguje k a.

Přímo z naší definice pro komplexní hodnoty je také 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) Jestliže je f definována na intervalu $A = [a, b]$ a x_0 je vnitřním bodem intervalu, hovoříme o limitě funkce ve vnitřním bodě jejího definičního oboru. 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 $\lim_{x\to 0} = 0$, přestože $f(0) = 1$ do malých okolí limitní hodnoty 0 nepatří.

(3) Je-li $A = [a, b]$ ohraničený interval a $x_0 = a$ nebo $x_0 = b$, hovoříme o limitě v hraničním bodě definičního oboru funkce f. Jestliže je ale bod x_0 vnitřním bodem, můžeme pro účely výpočtu limity definiční obor zúžit na $[x_0, b]$ nebo $[a, x_0]$. Výsledným limitám pak říkáme *limita zprava*, resp. *limita zleva* pro funkci f v bodě x_0. Označujeme ji výrazem $\lim_{x\to x_0^+} f(x)$, 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

$$\lim_{x\to 0^+} h(x) = 1, \quad \lim_{x\to 0^-} h(x) = 0.$$

Limita $\lim_{x\to 0} f(x)$ přitom neexistuje. Je snadné dokázat, že limita ve vnitřním bodu definičního oboru libovolné reálné funkce f existuje, právě když existují limity zprava i zleva a jsou si rovny.

(4) 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

$$\lim_{x\to x_0} f(x) = \lim_{x\to x_0} (\operatorname{re} f(x)) + i \lim_{x\to x_0} (\operatorname{im} f(x)).$$

(5) 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 δ se hodnotou libovolně blízko přiblížíme $f(x_0)$.

(6) Uvažme nyní obzvlášť ošklivou funkci definovanou na celém $\mathbb{R}$

$$f(x) = \begin{cases} 1 & \text{je-li } x \in \mathbb{Q} \\ 0 & \text{jestliže } x \notin \mathbb{Q}. \end{cases}$$

Jistě snadno ověříte, že tato funkce nemá limitu v žádném bodě (dokonce ani zleva nebo zprava).

(7) Ale definice spojitosti je ještě záludnější, než jsme viděli v předchozím případě. Definujme následující funkci $f : \mathbb{R} \to \mathbb{R}$:

$$f(x) = \begin{cases} \frac{1}{q} & \text{jestliže } x = \frac{p}{q} \in \mathbb{Q},\ p \text{ a } q \text{ nesoudělná} \\ 0 & \text{jestliže } x \notin \mathbb{Q} \end{cases}$$

Tato funkce je spojitá ve všech iracionálních bodech a nespojitá ve všech racionálních realných bodech. Důkaz přenecháváme jako cvičení.

5.14. Věta. Věta o třech limitách. *Buď f, g, h reálné funkce takové, že existuje okolí bodu $x_0 \in \mathbb{R}$, kde platí $f(x) \le g(x) \le h(x)$. Pak pokud existují limity $\lim_{x\to x_0} f(x) = f_0$ a $\lim_{x\to x_0} h(x) = h_0$ a navíc $f_0 = h_0$, pak také existuje limita $\lim_{x\to x_0} g(x) = g_0$ a platí $g_0 = f_0 = h_0$.*

Důkaz. Z definice limity, pro libovolné $\varepsilon > 0$ existuje okolí U bodu x_0, ve kterém je $f(x), h(x) \in (g_0 - \varepsilon, g_0 + \varepsilon)$. z podmínky $f(x) \le g(x) \le h(x)$ vyplývá, že i $g(x) \in (g_0 - \varepsilon, g_0 + \varepsilon)$, tedy $\lim_{x\to x_0} g(x) = g_0$. □

5.13

5.15. Věta. *Nechť $A \subset \mathbb{R}$ je definiční obor reálných nebo komplexních funkcí f a g, x_0 nechť je hromadný bod A a existují limity*

$$\lim_{x\to x_0} f(x) = a \in \mathbb{R}, \quad \lim_{x\to x_0} g(x) = b \in \mathbb{R}.$$

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 $b \neq 0$, 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 $\mathcal{O}_{2\epsilon}(a+b)$. Pro dostatečně malé okolí x_0 a $x \neq x_0$ bude jak $f(x)$, tak $g(x)$ v ϵ–okolích bodů a a b. Proto jejich součet bude v 2ϵ–okolí kýžené hodnoty $a + b$. Tím je důkaz ukončen.

(3) Obdobně postupujeme u součinu s $\mathcal{O}_{\epsilon^2}(ab)$. Pro malá okolí x_0 se nám hodnoty f i g trefí do ϵ–okolí hodnot a a b. Proto jejich součin bude v požadovaném ϵ^2–okolí.

(4) Podobný postup ponechán jako cvičení. □

Poznámka. Podrobnějším sledováním důkazů jednotlivých bodů věty můžeme její tvrzení rozšířit i na některé nekonečné hodnoty limit: 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 5.12. 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.

5.15.1. *Spočítejte následující limity posloupností:*

(1) $\lim\limits_{n\to\infty} \frac{2n^2+3n+1}{n+1}$,

(2) $\lim\limits_{n\to\infty} \frac{2n^2+3n+1}{3n^2+n+1}$,

(3) $\lim\limits_{n\to\infty} \frac{n+1}{2n^2+3n+1}$,

(4) $\lim\limits_{n\to\infty} \frac{\sqrt{4n^2+n}}{n}$,

(5) $\lim\limits_{n\to\infty} \sqrt{4n^2+n} - 2n$.

Řešení.

(1) $\lim\limits_{n\to\infty} \frac{2n^2+3n+1}{n+1} = \lim\limits_{n\to\infty} \frac{2n+3+\frac{1}{n}}{1+\frac{1}{n}} = \infty$.

(2) $\lim\limits_{n\to\infty} \frac{2n^2+3n+1}{3n^2+n+1} = \lim\limits_{n\to\infty} \frac{2+\frac{3}{n}+\frac{1}{n^2}}{3+\frac{1}{n}+\frac{1}{n^2}} = \frac{2}{3}$.

(3) $\lim\limits_{n\to\infty} \frac{n+1}{2n^2+3n+1} = \lim\limits_{n\to\infty} \frac{1+\frac{1}{n}}{2n+3+\frac{1}{n}} = \frac{1}{\infty} = 0$.

(4) Podle věty o třech limitách: $\forall n \in \mathbb{N} : \frac{\sqrt{4n^2}}{n} < \frac{\sqrt{4n^2+n}}{n} < \frac{\sqrt{4n^2+n+\frac{1}{16}}}{n}$.

Dále pak

$$\lim_{n\to\infty} \frac{\sqrt{4n^2}}{n} = \lim_{n\to\infty} \frac{2n}{n} = 2,$$

$$\lim_{n\to\infty} \frac{\sqrt{4n^2+n+\frac{1}{16}}}{n} = \lim_{n\to\infty} \frac{2n+\frac{1}{4}}{n} = 2.$$

Tedy i

$$\lim_{n\to\infty} \frac{\sqrt{4n^2+n}}{n} = 2$$

.

(5)

$$\begin{aligned}\lim_{n\to\infty} \sqrt{4n^2+n} - 2n &= \lim_{n\to\infty} \frac{(\sqrt{4n^2+n}-2n)(\sqrt{4n^2+n}+2n)}{\sqrt{4n^2+n}+2n} \\ &= \lim_{n\to\infty} \frac{n}{\sqrt{4n^2+n}+2n} = \\ &= \lim_{n\to\infty} \frac{1}{\frac{\sqrt{4n^2+n}}{n}+2} = \frac{1}{4}\end{aligned}$$

□

5.14

5.16. Spojité funkce. Nechť f je reálná nebo komplexní funkce definovaná na intervalu $A \subset \mathbb{R}$. Říkáme, že f je *spojitá v bodě* $x_0 \in A$, jestliže je

$$\lim_{x\to x_0} f(x) = f(x_0).$$

Funkce f je spojitá na A, jestliže je spojitá ve ve všech bodech $x_0 \in A$.

Všimněme si, že pro hraniční body intervalu A říká naše definice, že f v nich má být spojitá zprava, resp. zleva. Již jsme také viděli, že každý polynom je spojitou funkcí na celém $\mathbb{R}$, viz 5.13(5).

Z předchozí věty okamžitě vyplývá většina následujících tvrzení

Věta. *Nechť f a g jsou spojité funkce na intervalu A. Pak*

(1) *součet $f+g$ je spojitá funkce*
(2) *součin $f \cdot g$ je spojitá funkce*
(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 spojitá funkce h je definována na okolí hodnoty $f(x_0)$, pak složená funkce $h \circ f$ je definována na okolí bodu x_0 a je v 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 ϵ–okolí čísla $g(x_0)$ neobsahuje nulu pro dostatečně malé $\epsilon > 0$. Ze spojitosti g pak vyplývá, že na dostatečně malém δ–okolí x_0 bude g neulové 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:

5.15 **5.17. Věta.** *Nechť $f : \mathbb{R} \to \mathbb{R}$ je spojitá funkce. Pak*

(1) *vzor $f^{-1}(U)$ každé otevřené množiny je otevřená množina,*
(2) *vzor $f^{-1}(W)$ každé uzavřené množiny je uzavřená množina,*
(3) *obraz $f(K)$ každé kompaktní množiny je kompaktní množina,*
(4) *na libovolné kompaktní množině K dosahuje spojité zobrazení 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 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 stačilo 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. □

5.16 **5.18. 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.*

Důkaz. (1) Uvažme nějaký interval A (a ponechme stranou, jestli je A uzavřený nebo otevřený, ať už zleva nebo zprava) 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 $A_1 = f^{-1}(B_1)$ a $A_2 = f^{-1}(B_2)$ pokrývají A. Tyto množiny jsou přitom opět otevřené, jsou disjunktní a obě mají neprázdný průnik s A. Nutně tedy musí existovat bod $x \in A$, který neleží v B_1, je ale jejím hromadným bodem. Musí však ležet v B_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 jeho krajní body mohou a nemusí do obrazu patřit.

(2) Toto tvrzení je přímým důsledkem předchozího. □

5.17

5.19. Přírůstky do ZOO. Zatím jsme v podstatě pracovali pouze s polynomy a s funkcemi, které se z nich dají vyrobit „po částech“. Zároveň jsme dovodili spoustu vlastností pro obrovskou třídu spojitých funkcí, nemáme ale zatím moc prakticky zvladatelných příkladů. Naše úvahy nám teď umožňují alespoň trochu rozšířit naši zásobárnu funkcí.

(1) Nechť f a g jsou dva polynomy, které mohou mít i komplexní hodnoty (tj. připouštíme výrazy $a_n x^n + \cdots + a_0$ s komplexními $a_i \in \mathbb{C}$, ale dosazujeme jen reálné hodnoty za x). Pak funkce

$$h : \mathbb{R} \setminus \{x \in \mathbb{R}, g(x) = 0\} \to \mathbb{C}$$
$$h(x) = \frac{f(x)}{g(x)}$$

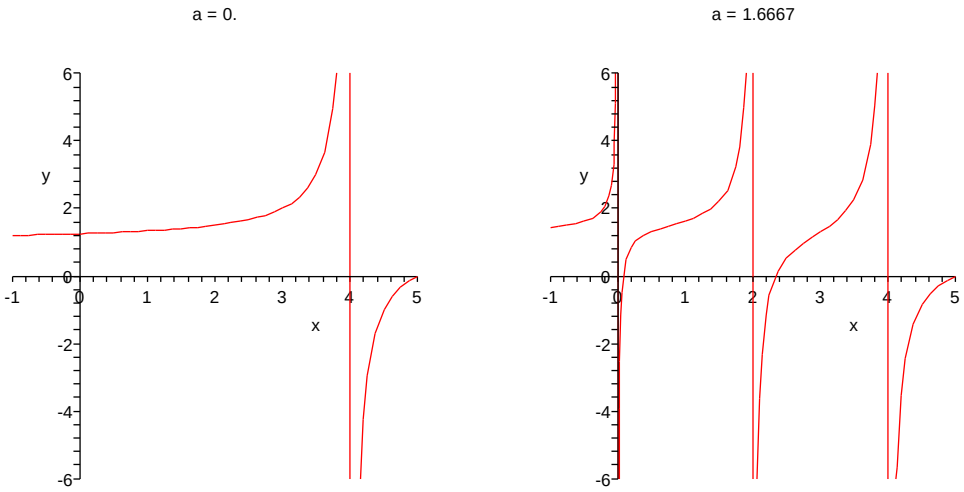
je dobře definována ve všech reálných bodech kromě kořenů polynomu g. Takové funkce nazýváme *racionální funkce*. Z věty 5.16 vyplývá, že racionální funkce jsou spojité ve všech bodech svého definičního oboru. V bodech, kde definovány nejsou mohou mít

- konečnou limitu, když jde o společný kořen polynomů f i g (a v tomto případě rozšířením jejich definice o limitní hodnotu v tomto bodě dostaneme funkci i v tomto bodě spojitou)
- nekonečnou limitu, když limity zprava a zleva v tomto bodě jsou stejné
- různé nekonečné limity zprava a zleva.

Názorně je možné tuto situaci vidět na obrázku, který ukazuje hodnoty funkce

$$h(x) = \frac{(x - 0.05a)(x - 2 - 0.2a)(x - 5)}{x(x-2)(x-4)}$$

pro hodnoty $a = 0$ (obrázek vlevo tedy vlastně zobrazuje racionální funkci $(x - 5)/(x - 4)$) a pro $a = 5/3$.



(2) Polynomy jsou pomocí sčítání a násobení skaláry seskládány z jednoduchých mocninných funkcí $x \mapsto x^n$ s přirozených číslem $n = 0, 1, 2, \ldots$. Samozřejmý smysl má také funkce $x \mapsto x^{-1}$ pro všechny $x \neq 0$. Tuto definici teď rozšíříme na obecnou *mocninnou funkci* s $n \in \mathbb{R}$.

Pro $n = -a$ s $a \in \mathbb{N}$ definujeme

$$x^{-a} = (x^a)^{-1} = (x^{-1})^a.$$

Dále jistě chceme, aby ze vztahu $b^n = x$ pro $n \in \mathbb{N}$ vyplývalo $b = x^{\frac{1}{n}}$. Je třeba ale ověřit, že taková b skutečně existují. Předpokládejme $x > 0$ a označme B množinu $B = \{y \in \mathbb{R}, y > 0,\ y^n \leq b\}$. To je zřejmě zhora ohraničená množina a lze ověřit, že pro $b = \sup M$ skutečně platí požadovaná rovnost.

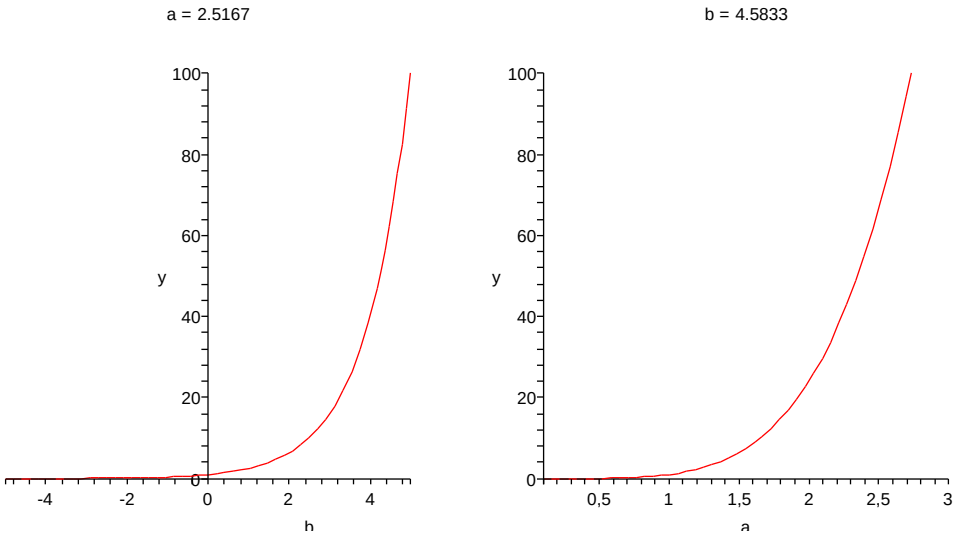
Zdůvodnili jsme tedy existenci x^a pro všechny $x > 0$ a $a \in \mathbb{Q}$. Konečně, pro $a \in \mathbb{R}$, $x > 1$ klademe

$$x^a = \sup\{x^y, y \in \mathbb{Q},\ y \leq a\}.$$

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.

Na obrázcích vidíme funkce $x \mapsto a^x$ a $x \mapsto x^b$ pro jednu konkrétní hodnotu $a = 2.5167$ a $b = 4.5833$.



Z našich definic je vcelku zřejmé, že mocninné i exponenciální funkce jsou spojité na celých svých definičních oborech. Zároveň se ze spojitosti definice pomocí suprem množin hodnot zjevně přenáší základní vlastnosti platné pro racionální čísla, a, x, y:

e5.3a (5.5) $$a^x \cdot a^y = a^{x+y}, \quad (a^x)^y = a^{x\cdot y}.$$

5.20. Příklady.

5.20.1. *Buď $c \in \mathbb{R}^+$ (kladné reálné číslo). Ukážeme, že* $\lim_{n\to\infty} \sqrt[n]{c} = 1$.

Řešení. Uvažme nejprve $c > 1$. Vzhledem k tomu, že funkce $\sqrt[n]{c}$ je vzhledem k n klesající a její hodnoty jsou stále větší než 1, tak 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 $1+\varepsilon+\frac{\varepsilon^2}{4}$, t.j. zejména $\sqrt[m]{c} < 1+\varepsilon+\frac{eps^2}{4}$. 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. □

5.20.2. *Určete limitu*

$$\lim_{x\to 0} \frac{1-\cos x}{x^2 \sin(x^2)}$$

Řešení. ∞. □

3. Derivace

U polynomů jsme již v odstavci 5.5 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 Δx nezávisle proměnné. Tehdejší úvaha funguje zrovna stejně pro libovolnou reálnou nebo komplexní funkci f, jen musíme místo intuitivního „zmenšování“ přírůstku Δx pracovat s pojmem limity.

5.18 **5.21. Definice.** Nechť f je reálná nebo komplexní funkce s definičním oborem $A \subset \mathbb{R}$ a $x_0 \in A$. Jestliže existuje limita

$$\lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0} = a$$

pak řídáme, že f má v bodě x_0 *derivaci* a. Píšeme často $a = f'(x_0)$ nebo $a = \frac{df}{dx}(x_0)$ případně $a = \frac{d}{dx} f(x_0)$.

Derivace 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.

Z formulace definice lze očekávat, že $f'(x_0)$ bude opět umožňovat dobře aproximovat danou funkci pomocí přímky

$$y = f(x_0) + f'(x_0)(x - x_0).$$

Takto lze snad vnímat následující lemma, které říká, že nahrazením konstantního koeficientu $f'(x_0)$ spojitou funkcí dostaneme přímo hodnoty f.

Lemma. *Reálná nebo komplexní funkce má v bodě x_0 vlastní derivaci, právě když existuje na nějakém okolí $\mathcal{O}(x_0)$ funkce ψ 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 $\psi(x_0) = f'(x_0)$.

Důkaz. Nejprve předpokládejme, že $f'(x_0)$ je vlastní derivace. Pokud má ψ existovat, má jistě tvar $\psi(x) = (f(x) - f(x_0))/(x - x_0)$ pro všechny $x \in \mathcal{O} \setminus \{x_0\}$. V bodě x_0 naopak definujme hodnotu derivací. Pak jistě

$$\lim_{x \to x_0} \psi(x) = f'(x_0) = \psi(x_0)$$

jak je požadováno.

Naopak, jestliže taková funkce ψ existuje, tentýž postup vypočte její limitu v x_0. Proto existuje i $f'(x_0)$ a je $\psi(x_0)$ rovna. □

5.18a **5.22. 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.

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 $f(b) > f(a)$ pro všechny body $a, b \in \mathcal{O}(x_0)$, $b > a$.*

Je-li derivace $f'(x_0) < 0$, pak naopak pro nějaké okolí $\mathcal{O}(x_0)$ platí $f(b) < f(a)$ pro všechny body $a, b \in \mathcal{O}(x_0)$, $b > a$.

Důkaz. Uvažme prvý případ. Pak podle předchozího lematu platí $f(x) = f(x_0) + \psi(x)(x - x_0)$ a $\psi(x_0) > 0$. Protože je ale ψ v x_0 spojitá, musí existovat okolí $\mathcal{O}(x_0)$, na kterém bude $\psi(x) > 0$. Pak ale s rostoucím x nutně poroste i hodnota $f(x)$.

Stejná argumentace ověří i tvrzení se zápornou derivací. □

Funkce, které mají vlastnost $f(b) > f(a)$ kdykoliv $b > a$ pro nějaké okolí bodu x_0 se nazývají *rostoucí v bodě* x_0. Funkce rostoucí ve všech bodech nějakého intervalu se nazývá *rostoucí na intervalu*. Podobně je funkce *klesající v bodu*, resp. *klesající na intervalu*, jestliže $f(b) < f(a)$ kdykoliv je $a < b$. 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.

5.19

5.23. Pravidla pro počítání. Uveďme si nyní několik základních tvrzení o výpočtech derivací. Říkají nám, jak dobře se snáší operace derivování s algebraickou strukturou sčítání a násobení na reálných nebo komplexních funkcích. Poslední z pravidel pak umožňuje efektivní výpočet derivace složených funkcí a říkává se mu „chain rule“. 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 $y = h(x) = f(x)g(x)$ je přírůstek

$$\begin{aligned}\Delta y &= f(x+\Delta x)g(x+\Delta x) - f(x)g(x)\\ &= f(x+\Delta x)(g(x+\Delta x) - g(x)) + (f(x+\Delta x) - f(x))g(x)\end{aligned}$$

Nyní ale když budeme zmenšovat přírůstek Δx, 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 očkávat pro derivaci součinu fg výraz $fg' + f'g$.

Ještě zajímavější je to pro derivaci 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:

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) *funkce f je v bodě x_0 spojitá,*
(2) *pro každé reálné nebo komplexní číslo c má funkce $x \mapsto c \cdot f(x)$ derivaci v x_0 a platí*
$$(cf)'(x_0) = c(f'(x_0)),$$
(3) *funkce $f + g$ má v x_0 derivaci a platí*
$$(f+g)'(x_0) = f'(x_0) + g'(x_0),$$
(4) *funkce $f \cdot g$ má v x_0 derivaci a platí*
$$(f \cdot g)'(x_0) = f'(x_0)g(x_0) + f(x_0)g'(x_0).$$
(5) *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) Předpokládejme, že $f'(x_0)$ existuje a je vlastní (tj. není nekonečná). Pak můžeme vyjádřit pro každé $x \neq x_0$

$$f(x) = \frac{f(x) - f(x_0)}{x - x_0}(x - x_0) + f(x_0).$$

Protože je ale limita součtu a součinu funkcí dána jako součet a součin limit (viz Věta 5.15), dostáváme

$$\lim_{x \to x_0} f(x) = f'(x_0) \cdot 0 + \lim_{x \to x_0} f(x_0) = f(x_0),$$

což ověřuje spojitost f v x_0.

(2) a (3) Opět přímé použití věty o součtech a součinech limit funkcí dává výsledek.

(4) Přepíšeme vztah pro podíl přírůstků, který jsme zmínili před formulací věty, takto

$$\frac{(f \cdot g)(x) - (f \cdot g)(x_0)}{x - x_0} = f(x)\frac{g(x) - g(x_0)}{x - x_0} + \frac{f(x) - f(x_0)}{x - x_0}g(x_0).$$

Limita tohoto výrazu pro $x \to x_0$ dá právě požadovaný výsledek, protože je funkce f spojitá v x_0.

(5) Podle předchozího lematu existují funkce ψ a φ 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. □

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 speciální případ formulky pro $h(x) = x^{-1}$. Přímo z definice derivace dostáváme

$$h'(x) = \lim_{\Delta x \to 0} \frac{\frac{1}{x+\Delta x} - \frac{1}{x}}{\Delta x} = \lim_{\Delta x \to 0} \frac{x - x - \Delta x}{\Delta x(x^2 + x\Delta x)} = \lim_{\Delta x \to 0} \frac{-1}{x^2 + x\Delta x}.$$

Z pravidel pro počítání limit okamžitě dostáváme

$$h'(x_0) = -x^{-2}.$$

Nyní pravidlo pro derivaci složené funkce říká, že $(g^{-1})' = -g^2 \cdot g'$ a konečně pravidlo pro derivaci součinu nám dává právě kýžený vzorec:

$$(f/g)' = (f \cdot g^{-1})' = f'g^{-1} - fg^{-2}g' = \frac{f'g - gf'}{g^2}.$$

□

5.20

5.24. Derivace inverzních funkcí. V odstavci 1.43 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 $A \subset \mathbb{R}$ a $f(A) = B$, je existence f^{-1} podmíněna stejnými vztahy s identickými zobrazeními id_A resp. id_B na pravých stranách.

Pokud bychom věděli, že pro diferencovatelnou funkci f je i f^{-1} diferencovatelná, pravidlo pro derivaci složené funkce nám říká

$$1 = (\mathrm{id})'(x) = (f^{-1} \circ f)'(x) = (f^{-1})'(f(x)) \cdot f'(x)$$

a tedy přímo víme formuli (zjevně $f'(x)$ v takovém případě nemůže být nulové)

e5.5

$$(f^{-1})'(f(x)) = \frac{1}{f'(x)}. \tag{5.6}$$

To dobře odpovídá intuitivní představě, že pro $y = f(x)$ je $f' = \frac{\Delta y}{\Delta x}$ zatímco pro $x = f^{-1}(y)$ je $(f^{-1})'(y) = \frac{\Delta x}{\Delta y}$. Takto skutečně můžeme derivace inverzních funkcí počítat:

Věta. *Je-li f diferencovatelná funkce na okolí bodu x_0 a $f'(x_0) \neq 0$, pak existuje na nějakém okolí bodu $y_0 = f(x_0)$ funkce f^{-1} inverzní k f a platí vztah (5.6).*

Pokud je $f'(x_0) = 0$ izolovaným nulovým bodem derivace $f'(x)$ a inverzní funkce k f na okolí $f(x_0)$ existuje, pak limity zprava i zleva funkce f' jsou v bodě x_0 nevlastní.

Důkaz. Nejprve si povšimněme, že nenulovost derivace znamená, že na nějakém okolí je naše funkce f buď ostře rostoucí nebo klesající, viz důsledek 5.22. Proto na nějakém okolí nutně existuje inverzní funkce. Přímo z definice spojitosti pomocí okolí je pak tato inverzní funkce také spojitá.

Pro odvození našeho tvrzení nyní postačí pozorně znovu pročíst důkaz pátého tvrzení věty 5.23. 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 její derivace je identita): Skutečně, podle lematu 5.21 existuje funkce ψ 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

$$x - x_0 = \varphi(f^{-1}(x))(f^{-1}(x) - f^{-1}(x_0)),$$

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

$$\frac{f^{-1}(x) - f^{-1}(x_0)}{x - x_0} = \frac{1}{\varphi(f^{-1}(x))} \neq 0,$$

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 $\varphi(y_0) = (f'(y_0))^{-1}$, proto i limita levé strany existuje a je rovna témuž výrazu.

Předpokládejme, že je x_0 izolovaný nulový bod derivace f' a že inverzní funkce na nějakém okolí $f(x_0)$ existuje. Pak je f' na okolí bodu x_0 nenulová, její hodnota se ale blíží nule. Proto má nalevo i napravo derivaci i inverzní funkce a na nějakém levém, resp. pravém, okolí bodu x_0 tato nemění znaménko. Odtud již vyplývá, že existují limity zprava i zleva pro f' v bodě x_0 a jsou nevlastní. □

5.22

5.25. Derivace vyšších řádů. Říkáme, že reálná nebo komplexní funkce f má v bodě x_0 derivaci druhého řádu v bodě x_0, jestliže derivace f' existuje na nějakém okolí bodu x_0 a existuje její derivace v bodě x_0. Píšeme

$$f''(x_0) = (f')'(x_0)$$

nebo také $f^{(2)}(x_0)$. Funkce f je *dvakrát diferencovatelná* na nějakém intervalu A, jestliže má druhou derivaci v každém jeho bodě.

Derivace vyšších řádů definujeme induktivně. Známe již pojem první a druhá derivace a říkáme, že reálná nebo komplexní funkce f je *k-krát diferencovatelná* pro nějaké přirozené číslo k v bodě x_0, jestliže je $(k-1)$-krát diferencovatelná na nějakém okolí bodu x_0 a její $(k-1)$-ní derivace má v bodě x_0 derivaci.

Pro k-tou derivaci funkce $f(x)$ užíváme značení $f^{(k)}(x)$.

Jestliže existují derivace všech řádů na intervalu, říkáme, že je tam funkce f *hladká*. Většinou se také užívá konvence, že 0-krát diferencovatelná funkce znamená spojitá funkce. Používáme pro takové funkce označení *třída funkcí* $C^k(A)$ na intervalu A, kde k může nabývat hodnot $0, 1, \ldots, \infty$. Často píšeme pouze C^k, je-li definiční obor znám z kontextu.

Ilustrovat můžeme rychle pojem derivace vyššího řádu 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 5.7, 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!

5.26. Zvěřinec. Zatím máme shromážděny ctyři typy funkcí:

- polynomy f definované na celém $\mathbb{R}$ s hodnotami v $\mathbb{R}$ nebo v $\mathbb{C}$,
- racionální funkce f/g definované na celém $\mathbb{R}$ kromě nejvýše konečné množiny kořenů polynomu g ve jmenovateli zlomku, s hodnotami v $\mathbb{R}$ nebo $\mathbb{C}$,
- mocninné funkce x^b s obecným $b \in \mathbb{R}$, definované pro $x > 0$ a hodnotami v $\mathbb{R}$,
- exponenciální funkce a^x o libovolném základu $a > 0$ definované pro všechna $x \in \mathbb{R}$ a s hodnotami v $\mathbb{R}$.

Polynomy. Derivace polynomů jsme spočítali již v odstavci 5.5. Ilustrujme naše nástroje pro výpočet derivací při diskusi kořenů polynomů. Předně platí tzv. *základní věta algebry*, kterou však nebudeme dokazovat:

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 kořenů včetně násobností a můžeme jej vždy psát jednoznačně ve tvaru

$$f(x) = (x - a_1)^{c_1} \cdot (x - a_q)^{c_q}$$

kde $a_1, \ldots, a_q$ jsou všechny kořeny polynomu f a $1 \leq c_1, \ldots, c_q \leq k$ jsou jejich násobnosti. Derivací dostaneme

$$f'(x) = c_1(x - a_1)^{c_1 - 1} \ldots (x - a_q)^{c_q} + \cdots + c_q(x - a_1)^{c_1} \ldots (x - a_q)^{c_q - 1}.$$

Jestliže je $c_1 = 1$, 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. Oddobně to bude i s ostatními kořeny. Ověřili jsme tedy užitečnou vlastnost, že kořen a polynomu f je vícenásobný tehdy a jen tehdy, když je zároveň kořenem derivace f'.

Protože polynomy jen zřídka jsou výhradně rostoucí nebo klesající funkce, nemůžeme očekávat, že by existovaly globálně definované inverzní funkce k nim. 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 řádu obdobně

$$y = ax^2 + bx + c$$

vede k formuli

$$x = \frac{-b \pm \sqrt{b^2 - 4a(c - y)}}{2a},$$

a inverze tedy existuje (a je dána touto formulí) jen pro x na intervalech $(-\infty, -\frac{b}{2a})$, $(-\frac{b}{2a}, \infty)$.

Pro práci s inverzními funkcemi k polynomům nevystačíme s našimi funkcemi a dostáváme v našem zvířetníku nové přírůstky.

Racionální funkce. Všechny racionální funkce jsou také třídy C^∞ ve všech bodech svého definičního oboru. Jejich derivace se snadno počítá pomocí formule pro derivaci podílu. Samozřejmě bude také racionální funkcí.

Inverze také budou jako u polynomů existovat obecně jen lokálně a jsou novými přírůstky do našeho společenstva funkcí.

Mocninné funkce. Obecnou mocninou funkci není tak snadné zderivovat, i když bychom mohli věřit, že formulka

e5.6 (5.7) $$(x^a)' = ax^{a-1}$$

známá pro přirozená a bude platit i pro obecné a. K tomu totiž máme dobrý důvod, protože ji umíme přímo ověřit pro racionální $a = p/q$. Je-li a celé a záporné, pak tvrzení přímo vidíme z věty o složené funkci:

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

Pokračujme dále s odmocninami, tj. $a = 1/q$. Pišme $x = h(y) = y^{1/q}$, $y = x^q$ a počítejme podle věty o derivaci inverzní funkce

$$h'(y) = \frac{1}{q}\frac{1}{x^{q-1}} = \frac{1}{q}y^{-(q-1)/q} = \frac{1}{q}y^{1/q-1}.$$

Pro obecné racionální $a = p/q$ máme

$$(x^{p/q})' = ((x^{1/q})^p)' = p(x^{1/q})^{p-1}\frac{1}{q}x^{1/q-1} = \frac{p}{q}x^{p/q-1}.$$

Nyní bychom mohli zvládnout důkaz platnosti formule (5.7) pomocí spojitosti definice mocninné funkce x^a v parametru a. Vrátíme se raději k důkazu z jiného pohledu za malou chvíli.

Funkce $f(x) = x^0 = 1$ má samozřejmě derivaci nulovou, pro všechny jiné hodnoty $a \neq 0$ je derivace nenulová. Je záporná pro $a \in (0,1)$, kladná pro $a \in (1,\infty)$. Proto je mocninná funkce na celém definičním oboru $(0,\infty)$ klesající v prvém případě a rostoucí v druhém. Její inverzní funkce je opět mocninnou funkcí.

Exponenciální funkce. Zbývají nám funkce $f(x) = a^x$. Zde se také budeme s derivací poněkud potýkat. Pokud budeme umět derivovat 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.

Exponenciální funkce jsou tedy zvláštními případy funkcí, kdy jejich derivace jsou úměrné hodnotám s konstantním koeficientem úměrnosti.

Spočtěme derivaci $f'(0)$, tj. výraz

$$\lim_{x\to 0}\frac{a^x-1}{x}$$

a předpokládejme, že naše $a > 1$. Z definice hodnot exponenciální funkce pomocí suprem množin hodnot s racionálními x je zjevné, že exponenciální funkce a^x je na celém svém definičním oboru rostoucí. Stačí nám proto při výpočtu derivace zprava dosazovat za x postupně hodnoty $x_n = 1/n$ a dostaneme

$$\lim_{x\to 0_+}\frac{a^x-1}{x} = \lim_{n\to\infty}\frac{a^{1/n}-1}{1/n}.$$

Zkusíme najít takové a, aby limita existovala a byla rovna jedné. Toho dosáhneme, pokud budeme umět s rostoucím n libovolně dobře přibližovat hodnotu $a^{1/n}$ k hodnotě $1+1/n$, tj. ekvivalentně (dle pravidel pro počítání limit) a je s rostoucím n libovolně přesně aproximováno hodnotou

$$a_n = \left(1+\frac{1}{n}\right)^n.$$

Z binomického rozvoje je zřejmé, že pro každé kladné číslo b a přirozené n platí $(1+b)^n > 1+nb$, dostáváme proto pro dva po sobě jdoucí členy naší posloupnosti podíl

$$\frac{(1+\frac{1}{n})^n}{(1+\frac{1}{n-1})^{n-1}} = \frac{(n^2-1)^n n}{n^{2n}(n-1)} = \left(1-\frac{1}{n^2}\right)^n\frac{n}{n-1} > (1-\frac{1}{n})\frac{n}{n-1} = 1.$$

Je tedy naše posloupnost rostoucí. Zároveň stejným výpočtem ověříme, že posloupnost čísel

$$b_n = (1+\frac{1}{n})^{n+1} = (1+\frac{1}{n})(1+\frac{1}{n})^n$$

je klesající a jistě je $b_n > a_n$. Ověřili jsme tedy existenci limity posloupnosti a_n (a zároveň vidíme, že je rovna limitě klesající posloupnosti b_n).

Tato limita je jedním z nejdůležitějších čísel v matematice (vedle nuly, jedničky a Ludolfova čísla π), nazýváme jej *Eulerovým číslem* e. Je tedy

$$\mathrm{e} = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n .$$

Náš postup zároveň ověřil, že existuje derivace v nule zprava exponenciální funkce e^x a je rovna jedné. Proto existuje ve všech bodech x také derivace zprava a je rovna e^x. Nyní můžeme spočíst derivaci zleva pomocí derivací složených funkcí. Skutečně,

$$\lim_{x\to 0_-} \frac{\mathrm{e}^x - 1}{x} = \lim_{x\to 0_+} \frac{\mathrm{e}^{-x} - 1}{-x} = (\mathrm{e}^0)^{-2}\,\mathrm{e}^0 = 1.$$

Derivace zleva i zprava tedy pro funkci $f(x) = \mathrm{e}^x$ existují ve všech bodech a jsou si rovny.

Přirozený logaritmus. Protože je exponenciální funkce e^x všude dobře definována a kladná, existuje všude i její funkce inverzní. Označujeme ji $\ln x$ a říkáme jí *přirozený logaritmus* nebo logaritmus se základem e. Je definována vztahem

$$\mathrm{e}^{\ln x} = x.$$

Z vlastností mocninných funkcí, viz vztahy (5.5), okamžitě dostáváme

5.6a (5.8) $$\ln(x \cdot y) = \ln x + \ln y, \quad \ln x^y = y \cdot \ln x.$$

Derivaci přirozeného logaritmu spočteme podle pravidla pro derivaci složené funkce (užíváme již, že e^x je rovno své derivaci, a také definiční vztah pro logaritmus):

e5.7 (5.9) $$(\ln)'(y) = (\ln)'(\mathrm{e}^x) = \frac{1}{(\mathrm{e}^x)'} = \frac{1}{\mathrm{e}^x} = \frac{1}{y}.$$

Derivaci obecné exponenciální funkce $f(x) = a^x$ můžeme nyní spočíst takto:

e5.8 (5.10) $$(a^x)' = (\mathrm{e}^{x\ln a})' = \mathrm{e}^{x\ln a}(x\ln a)' = a^x \ln a.$$

Podobně také můžeme konečně ověřit i formuli pro derivaci obecné mocninné funkce pro všechny $x > 0$:

$$(x^a)' = (\mathrm{e}^{a\ln x})' = \mathrm{e}^{a\ln x}(a\ln x)' = ax^{a-1}.$$

Pro obecnou exponenciální funkci a^x se základem $a \neq 1$, $a > 0$ také existuje všude inverzní funkce. Říkáme jí *logaritmus při základu* a, píšeme $\log_a x$.

Vlastnosti dosavadního osazenstva našeho zvířetníku funkcí zpřehledňuje následující tabulka, kde jsou shrnuty vlastnosti jednotlivých obyvatelů a jejich vztahy:

funkce	**definiční obor**	**třída**	**derivace**	**inverze**
polynomy f	celé $\mathbb{R}$	C^∞	f' opět polynom	f^{-1} existuje jen lokálně a neumíme obecnou formulí
kubické splajny h	celé $\mathbb{R}$	C^2	h' je opět splajn	formule s odmocninami a jen lokálně
racionální funkce f/g	celé $\mathbb{R}$ kromě kořenů jmenovatele g	C^∞	opět racionální funkce: $\frac{f'g-fg'}{g^2}$	existuje jen lokálně a neumíme obecnou formulí
mocninné funkce x^a	interval $(0,\infty)$	C^∞	funkce ax^{a-1}	existuje všude a je opět mocninnou funkcí $y^{1/a}$
exponenciální funkce a^x s $a>0$, $a\neq 1$	celé $\mathbb{R}$	C^∞	existuje všude a je $\ln a \cdot a^x$	logaritmická funkce $\log_a$

4. Mocninné řady

5.24

5.27. Vraťme se k exponenciální funkci e^x. Jestliže v posloupnosti $a_m = (1+\frac{1}{m})^m$ dosadíme za m hodnoty $m = n/x$ pro nějaké pevné $x \in \mathbb{R}$, dostaneme

$$b_n = \left(1+\frac{x}{n}\right)^{\frac{n}{x}}, \quad b_n^x = \left(1+\frac{x}{n}\right)^n.$$

Přitom, je limita b_n pro n jdoucí do nekonečna opět e. Odvodili jsme tedy důležitý vztah platný pro všechna $x \in \mathbb{R}$

e5.11 (5.11)
$$\mathrm{e}^x = \lim_{n\to\infty}\left(1+\frac{x}{n}\right)^n.$$

Označme si n-tý člen této posloupnosti $u_n(x)$ a vyjádřeme si jej pomocí binomické věty:

e5.11a (5.12)
$$\begin{aligned} u_n(x) &= 1 + n\frac{x}{n} + \frac{n(n-1)x^2}{2!n^2} + \cdots + \frac{n!x^n}{n!n^n} \\ &= 1 + x + \frac{x^2}{2!}\left(1-\frac{1}{n}\right) + \frac{x^3}{3!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right) + \dots \\ &\quad + \frac{x^n}{n!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\dots\left(1-\frac{n-1}{n}\right). \end{aligned}$$

Protože jsou všechny závorky v součinech menší než jedna, dostáváme také

$$u_n(x) < v_n(x) = \sum_{j=0}^{n}\frac{1}{j!}x^j.$$

Podívejme se nyní na formální nekonečný součet

e5.12 (5.13)
$$\sum_{j=0}^{\infty} c_j = \sum_{j=0}^{\infty}\frac{1}{j!}x^j$$

tj. $v_n(x)$ je právě částečný 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 $j > N$. Pro takto velké 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

$$v_n < \sum_{j=0}^{N} \frac{1}{j!}x^j + \frac{1}{j!}x^j \sum_{j=0}^{n-N} \frac{1}{2^j}.$$

Poslední sumu ovšem umíme snadno spočíst. Jde o zvláštní případ součtu geometrické řady $\sum_{j=0}^{k} q^j$. Protože platí pro každé q

$$(1-q)(1+q+\cdots+q^k) = 1-q^{k+1},$$

existuje limita částečných součtů v *geometrické řadě* $\sum_{j=0}^{\infty} q^k$ právě když $|q| < 1$ a v takovém případě platí

e5.13 (5.14)
$$\sum_{j=0}^{\infty} q^j = \lim_{k\to\infty} \sum_{j=0}^{k} q^j = \frac{1}{1-q}.$$

Protože čísla v_n tvoří rostoucí posloupnost, jistě také tato posloupnost konverguje. Říkáme, že řada (5.13) konverguje.

Nyní si prohlédněme pozorněji posloupnost čísel u_n, jejíž limitou je e^x. Budeme uvažovat $n > N$ pro nějaké pevné N (hodně velké) a zvolíme si $k < N$ pevné (docela malé). Pak pro dostatečně velká N umíme součet prvních k členů ve vyjádření u_N v (5.12) aproximovat libovolně přesně výrazem v_k. Protože je tato část součtu u_N ostře menší než u_N samotné, musí posloupnost u_n konvergovat k téže limitě jako posloupnost v_n. Dokázali jsme tedy:

Věta. *Exponenciální funkce je pro každé $x \in \mathbb{R}$ vyjádřena jako limita částečných součtů ve výrazu*

$$\mathrm{e}^x = 1 + x + \frac{1}{2!}x^2 + \cdots + \frac{1}{n!}x^n + \cdots = \sum_{n=0}^{\infty} \frac{1}{n!}x^n.$$

Při dovození tohoto mimořádně důležitého tvrzení jsme mimoděk pracovali s několika užitečnými pojmy a nástroji. Sformulujeme si je nyní obecněji:

5.25 **5.28. Definice.** *Nekonečná řada* 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

$$s = \lim_{k\to\infty} s_n.$$

K tomu, aby posloupnost 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 $\sum_{k=0}^{\infty} a_n$. Říkáme, že řada $\sum_{k=0}^{\infty} a_n$ *konverguje absolutně*, jestliže konverguje řada $\sum_{n=0}^{\infty} |a_n|$.

Jestliže posloupnost částečných součtů řady má nevlastní limitu, říkáme že řada *diverguje* k ∞ nebo $-\infty$.

Jednoduché algebraické operace s absolutně konvergentními řadami se chovají všechny dobře:

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

$$\left(\sum_{n=0}^{k} a_n\right) \cdot \left(\sum_{n=0}^{k} b_n\right) \to \left(\sum_{n=0}^{\infty} a_n\right) \cdot \left(\sum_{n=0}^{\infty} b_n\right).$$

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

$$\left(\sum_{n=0}^{k} a_n\right) \cdot \left(\sum_{n=0}^{k} b_n\right) = \sum_{0\le i,j\le k} a_i b_j, \quad c_n = \sum_{\substack{i+j=n \\ 0\le i,j\le k}} a_i b_j, \quad \sum_{n=0}^{k} c_n = \sum_{\substack{i+j\le k \\ 0\le i,j\le k}} a_i b_j.$$

Dostáváme tedy odhad

$$\left| \left(\sum_{n=0}^{k} a_n\right) \cdot \left(\sum_{n=0}^{k} b_n\right) - \sum_{n=0}^{k} c_k \right| = \left| \sum_{\substack{i+j>k \\ 0\le i,j\le k}} a_i b_j \right| \le \sum_{\substack{i+j>k \\ 0\le i,j\le k}} |a_i b_j|.$$

K odhadu posledního výrazu nám poslouží jednoduchý trik: aby mohl být součet idexů 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 $k/2$.

$$\sum_{\substack{i+j>k \\ 0\le i,j\le k}} |a_i b_j| \le \sum_{0\le i,j\le k} |a_i b_j| - \sum_{0\le i,j\le k/2} |a_i b_j|.$$

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. □

Jako obvykle si hned shrneme několik dalších jednoduchých tvrzení o řadách:

5.26 **5.29. Věta.** *Nechť $S = \sum_{n=0}^{\infty} a_n$ je nekonečná řada reálných nebo komplexních čísel.*

(1) *Jestliže 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, zatímco při $q > 1$ diverguje. Je-li $q = 1$, může konvergovat i divergovat.

Důkaz. (1) Jestliže $\lim_{n\to\infty} a_n$ neexistuje nebo je nenulová, exituje pro dostatečně malé číslo $\epsilon > 0$ nekonečně mnoho členů a_k s $|a_k| > \epsilon$. 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 jdoucích s_n a s_{n+1} o velikosti alespoň ϵ. Posloupnost částečných součtů proto nemůže být Cauchyovská a tedy ani konvergentní.

(2) Protože chceme dokazovat absolutní konvergenci, můžeme rovnou předpokládat $a_i > 0$. Důkaz jsme pro speciální hodnotu $q = 1/2$ provedli při dovození hodnoty e^x pomocí řady. Stejnou úvahou z existence limity podílů dovodíme pro dostatečně veliké N
$$a_{j+1} < q \cdot a_j < q^{-(j-N+1)} c_N.$$
To ale znamená, že částečné součty prvních s_n jsou shora ohraničeny součty
$$s_n < \sum_{j=0}^{N} a_j + c_N \sum_{j=0}^{n-N} \frac{1}{q^j}.$$
Je-li $0 < q < 1$, je množina všech částečných součtů shora ohraničená a proto je limitou naší řady její supremum.

Při hodnotě $q > 1$ použijeme obdobný postup, ale z existence limity q na začátku odvodíme
$$a_{j+1} < q \cdot a_j < q^{-(j-N+1)} c_N.$$
To ale znamená, že částečné součty prvních s_n jsou zdola ohraničeny součty
$$s_n > \sum_{j=0}^{N} a_j + c_N \sum_{j=0}^{n-N} \frac{1}{q^j}.$$
Při $q > 0$ tento výraz poroste nad všechny meze

(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
$$|a_n| < r^n$$
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 existecne 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 (včetně důkazu) 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, zatímco při $q > 1$ diverguje. Je-li $q = 1$, může konvergovat i divergovat.

5.29.1. *Ukažte, že tzv. harmonická řada*

$$\sum_{i=1}^{\infty} \frac{1}{i}$$

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 $1/2$. □

5.29.2. *Rozhodněte o následujících řadách, jestli konvergují či divergují:*

(1) $\sum_{n=1}^{\infty} \frac{2^n}{n}$

(2) $\sum_{n=1}^{\infty} \frac{1}{\sqrt{n}}$

(3) $\sum_{n=1}^{\infty} \frac{1}{n\cdot 2^{100000}}$

(4) $\sum_{n=1}^{\infty} \frac{1}{(1+i)^n}$

Řešení.

(1) 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.

(2) Odhadneme řadu ze spodu: víme, že pro libovolné přirozené n platí $\frac{1}{n} \le \frac{1}{\sqrt{n}}$. Pro posloupnost částečných součtů s_n zkoumané řady a posloupnost částečných součtů harmonické řady s'_n tedy platí:

$$s_n = \sum_{i=1}^{n}\frac{1}{\sqrt{n}} \ge \sum_{i=1}^{n}\frac{1}{n} = s'_n.$$

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.

(3) Diverguje, jedná se o násobek harmonické řady.

(4) 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:

$$\sum_{n=1}^{\infty}\frac{1}{(1+i)^n} = \frac{1}{1-\frac{1}{1+i}} = \frac{1+i}{i} = 1-i.$$

□

5.27

5.30. 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 řady a dostáváme pojem součtu *řady funkcí*

$$S(x) = \sum_{n=0}^{\infty} f_n(x).$$

Mocninná řada je dána výrazem

$$S(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Řekneme, že $S(x)$ má *poloměr konvergence* $\rho \ge 0$, jestliže $S(x)$ konverguje pro každé x splňující $|x| < \rho$ a diverguje při $|x| > \rho$.

Věta. *Nechť* $S(x) = \sum_{n=0}^{\infty} a_n x^n$ *je mocninná řada a existuje limita*

$$\rho = \lim_{n\to\infty}\sqrt[n]{a_n}.$$

Pak je poloměr konvergece řady S *roven* $r = \rho^{-1}$.

Mocninná řada $S(x)$ *je spojitá na celém svém intervalu konvergence (včetně krajních bodů, pokud v nich konverguje) a existuje také její derivace* $S'(x)$,

$$S'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}.$$

DŮKAZ. Pro ověření konvergence řady můžeme pro každou pevnou hodnotu x použít odmocninový test z věty 5.29(3). Počítáme přitom

$$\lim_{n\to\infty} \sqrt[n]{a_n x^n} = \rho x$$

a řada konverguje, resp. diverguje, jestliže je tato limita různá od 1.

Tvrzení o spojitosti a derivaci dokážeme později v obecnějším kontextu, viz 6.28–6.30. □

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 fomulí

$$r^{-1} = \limsup_{n\to\infty} \sqrt[n]{a_n}.$$

5.28 **5.31. Příklad.** Prodíváme se na mocninné řady

$$S(x) = \sum_{n=0}^{\infty} x^n, \quad T(x) = \sum_{n=1}^{\infty} \frac{1}{n} x^n.$$

První příklad je *geometrická řada*, kterou jsme se zabývali již dříve, a její součet je pro všechny x s $|x| < 1$

$$S(x) = \frac{1}{1-x},$$

zatímco $|x| > 1$ zaručuje divergenci. Pro $x = 1$ dostáváme také zjevně divergentní řadu $1 + 1 + 1 + \dots$ s nekonečným součtem, při $x = -1$ jde o řadu $1 - 1 + 1 - \dots$, jejíž částečné součty nemají limitu vůbec.

Věta 5.29(3) 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 $1 + \frac{1}{2} + \frac{1}{3} + \dots$ (dokažte si jako cvičení!). Naopak, řada $T(-1) = -1 + \frac{1}{2} - \frac{1}{3} + \dots$ konverguje. Vyplývá to z obecnějšího platného tvrzení:

O řadě $T = \sum_{n=0}^{\infty} b_n$ s reálnými členy řekneme, že je *alternující*, jestliže je znaménko dvou po sobě jdoucích členů vždy opačné. Pokud je navíc $|b_n|$ klesající posloupnost a pro řadu T platí nutná podmínka konvergence z 5.29, tj. $\lim_{n\to\infty} b_n = 0$, pak řada konverguje. Důkaz teď nebudeme provádět, vyplyne z obecnějších výsledků později, viz **??**.

5.31.1. 7. *Určete poloměr konvergence následujících mocninných řad:*

(1) $\sum_{n=1}^{\infty} \frac{2^n}{n} x^n$

(2) $\sum_{n=1}^{\infty} \frac{1}{(1+i)^n} x^n$

Řešení.

(1)

$$r = \frac{1}{\limsup_{n\to\infty} \left| \frac{a_{n+1}}{a_n} \right|} = \frac{1}{2},$$

viz úloha **??**. Daná mocniná 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 libovoné x ležící v komplexní rovině na kružnici o poloměru $\frac{1}{2}$ je těžší otázka a přesahuje rámec našeho kurzu.

(2) Opět díky přechozímu příkladu víme, že

$$\limsup_{n\to\infty} \left| \sqrt[n]{\frac{1}{(1+i)^n}} \right| = \limsup_{n\to\infty} \left| \frac{1}{1+i} \right| = \frac{\sqrt{2}}{2}.$$

je tedy poloměr konvergence dané mocninné řady $r = \sqrt{2}$.

□

5.29

5.32. Zvěřinec. S mocninnými řadami nám do našeho společenství přibyla spousta nových příkladů hladkých funkcí, tj. funkcí libovolněkrát diferencovatelných na celém svém definičním oboru. Pohrejme si chvíli s nejvýznamnějším a prvním naším příkladem, exponenciálou

$$\mathrm{e}^x = 1 + x + \frac{1}{2}x^2 + \cdots + \frac{1}{n!}x^n + \dots.$$

Tato mocninnná 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 ze spojitosti tedy musí pro ni platit i obvyklé vztahy, které jsme pro reálné hodnoty proměnné x již odvodili. Zejména tedy platí

$$\mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y,$$

viz (5.5) a věta 5.28(3). Dosaďme si hodnoty $x = i \cdot t$, kde $i \in \mathbb{C}$ je imaginární jednotka, $t \in \mathbb{R}$ libovolné.

$$\mathrm{e}^{it} = 1 + it - \frac{1}{2}t^2 - i\frac{1}{3!}t^3 + \frac{1}{4!}t^4 + i\frac{1}{5!}t^5 - \dots$$

a zjevně tedy je komplexně konjugované číslo k $z = \mathrm{e}^{it}$ číslo $\bar{z} = \mathrm{e}^{-it}$. Proto

$$|z|^2 = z \cdot \bar{z} = \mathrm{e}^{it} \cdot \mathrm{e}^{-it} = \mathrm{e}^0 = 1$$

a všechny hodnoty $z = \mathrm{e}^{it}$ proto leží na jednotkové kružnici v komplexní rovině.

Reálné a imaginární složky bodů na jednotkové kružnici přitom bývají popisovány pomocí *goniometrických funkcí* $\cos\theta$ a $\sin\theta$, kde θ je patřičný úhel. Derivací parametrického popisu bodů kružnice,

$$t \mapsto \mathrm{e}^{it}$$

dostáváme vektory „rychlostí“, které budou dány výrazem (lze např. zderivovat skutečně zvlášť reálnou a imaginární složku a sečíst výsledky)

$$t \mapsto \left(\mathrm{e}^{it}\right)' = i \cdot \mathrm{e}^{it}$$

a jejich velikost proto také bude pořád jednotková. Odtud lze tušit, že celou kružnici oběhneme po dosažení hodnoty parametru rovného délce oblouku, tj. 2π (i když ke skutečnému ověření této skutečnosti budeme potřebovat integrální počet). Takto bývá *Ludolfovo číslo* π také definováno. Můžeme se ale nyní aspoň částečně ujistit pohledem na nejmenší kladné kořeny reálné části částečných součtů naší řady, tj.

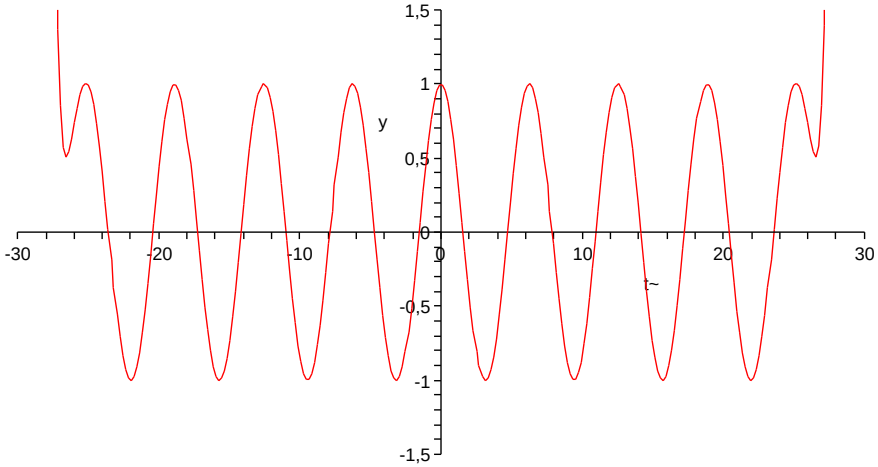
příslušných polynomů. Již při řádu deset nám vyjde číslo π přesně na 5 desetinných míst.

Dostali jsem tedy přímou definici goniometrických funkcí pomocí mocninných řad:

e5.15 (5.15) $$\cos t = \operatorname{re}\mathrm{e}^{it} = 1 - \frac{1}{2}t^2 + \frac{1}{4!}t^4 - \frac{1}{6!}t^6 + \cdots + (-1)^k\frac{1}{(2k)!}t^{2k} + \dots$$

e5.16 (5.16) $$\sin t = \operatorname{im}\mathrm{e}^{it} = t - \frac{1}{3!}t^3 + \frac{1}{5!}t^5 - \frac{1}{7!}t^7 + \cdots + (-1)^k\frac{1}{(2k+1)!}t^{2k+1} + \dots$$

Ilustraci konvergence řady pro funkci cos je vidět na 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

$$\sin^2 t + \cos^2 t = 1$$

a také z derivace $(\mathrm{e}^{it})' = i\,\mathrm{e}^{it}$ vidíme, že

$$(\sin t)' = \cos t, \qquad (\cos t)' = -\sin t.$$

Tentýž výsledek lze samozřejmě ověřit přímo derivací našich řad člen po členu.

Předpokládejme, že t_0 je 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 $t_0 = \frac{1}{2}\pi$. Pak $\mathrm{e}^{-i2t_0} = (\mathrm{e}^{-it_0})^2 = \mathrm{e}^{i2t_0}$ a jde proto o nulový bod funkce $\sin t$. Samozřejmě pak 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 funkce goniometrické funkce *periodické* s periodou 2π. Z našich definic je přitom vidět, že je to nejmenší jejich perioda.

Nyní můžeme snadno odvodit všechny obvyklé vztahy mezi goniometrickými funkcemi. Uvedeme na ukázku několik z nich. Nejprve si všimněme, že definice

vlastně říká

$$\cos t = \frac{1}{2}(\mathrm{e}^{it} + \mathrm{e}^{-it})$$
$$\sin t = \frac{1}{2i}(\mathrm{e}^{it} - \mathrm{e}^{-it}).$$

Součin těchto funkcí jde tedy vyjádřit jako

$$\sin t \cos t = \frac{1}{4i}(\mathrm{e}^{it} - \mathrm{e}^{-it})(\mathrm{e}^{it} + \mathrm{e}^{-it}) = \frac{1}{4i}(\mathrm{e}^{i2t} - \mathrm{e}^{-i2t}) = \frac{1}{2}\sin 2t.$$

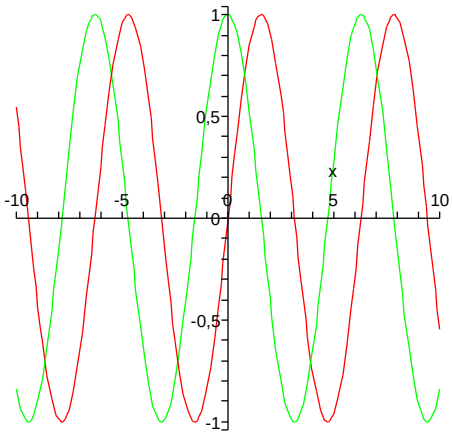
Dále můžeme využít naši znalost derivací:

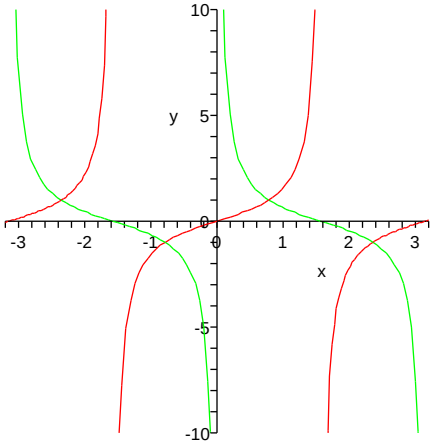
$$\cos 2t = (\frac{1}{2}\sin 2t)' = (\sin t \cos t)' = \cos^2 t - \sin^2 t.$$

Vlastnosti dalších goniometrických funkcí

$$\mathrm{tg}\, t = \frac{\sin t}{\cos t}, \qquad \mathrm{cotg}\, t = (\mathrm{tg}\, t)^{-1}$$

se snadno odvodí z jejich definice a pravidel pro derivování. Grafy funkcí sinus, cosinus, tangens a cotangens jsou na obrázcích (postupně červený a zelený vlevo, červený a zelený vpravo):





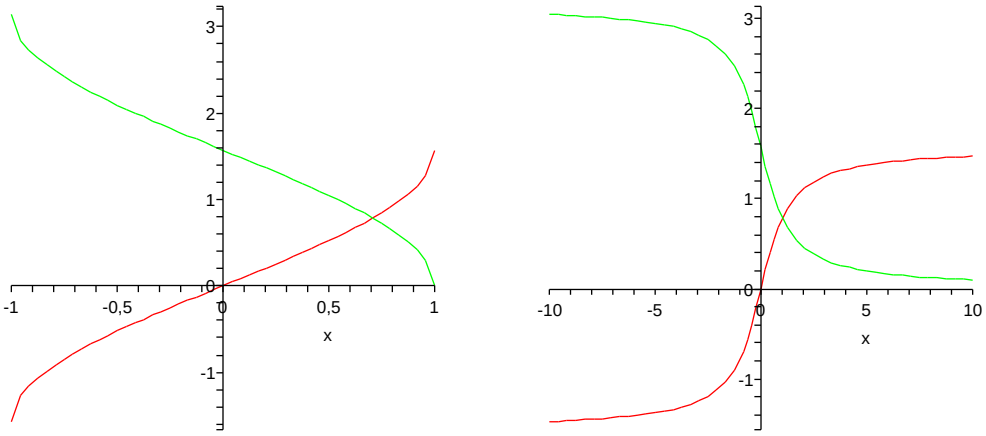
Cyklometrické funkce jsou inverzní ke goniometrickým. Protože jsou goniometrické funkce všechny periodické s periodou 2π, jsou jejich inverze definované vždy jen v rámci jedné periody a to ještě jen na části, kdy je daná funkce buď rostoucí nebo klesající. Jsou to funkce

$$\arcsin = \sin^{-1}$$

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.



Zbývají ještě funkce (zobrazené na obrázku vpravo)

$$\operatorname{arctg} = \operatorname{tg}^{-1}$$

s definičním oborem $[-\infty, \infty]$ a oborem hodnot $[-\pi/2, \pi/2]$ a konečně

$$\operatorname{arccotg} = \operatorname{cotg}^{-1}$$

s definičním oborem $[-\infty, \infty]$ a oborem hodnot $[0, \pi]$.

Velice často se také využívají tzv. *hyperbolické funkce*

$$\sinh x = \frac{1}{2}(\mathrm{e}^x - \mathrm{e}^{-x}), \qquad \cosh x = \frac{1}{2}(\mathrm{e}^x + \mathrm{e}^{-x}).$$

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)

$$(\cosh x)^2 - (\sinh x)^2 = 2\frac{1}{2}(\mathrm{e}^x\,\mathrm{e}^{-x}) = 1.$$

Body $[\cosh t, \sinh t]$ tedy skutečně parametricky popisují hyperbolu v rovině. Pro hyperbolické funkce lze snadno odvodit podobné identity jako pro funkce goniometrické. Mimo jiné je přímo z definice snadno vidět

$$\cosh x = \cos(ix), \qquad i \sinh x = \sin(ix)$$

(ověřte si jako cvičení).

5.32.1. *Sečtěte:*

$$2 + 1 + \frac{2}{2!} + \frac{1}{3!} + \frac{2}{4!} + \frac{1}{5!} + \frac{2}{6!} + \cdots$$

Řešení. Porovnáme tvar součtu s mocninným rozvojem funkcí sinh a cosh a dostáváme výsledek

$$\sinh(1) + 2\cosh(1)$$

. □

5.30

5.33. Poznámky. Mocninné řady můžeme zcela stejně 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 ρ je její poloměr konvergence. Říkáme, že S je *mocninná řada se středem v* x_0.

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 $S(y)$.

Zejména lze takto počítat členy mocninných řad zadávajících inverzní funkce. Nebudeme zde uvádět seznam formulí, snadno se k nim dostaneme například v Maplu procedurou „series“.

KAPITOLA 6

Diferenciální a integrální počet

zvěřinec teď máme, ale co s ním?
– naučíme se s ním zacházet...

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 jen minimum nástrojů a vše jsme počítali tak říkajíc na koleně. Teď dáme dohromady několik výsledků, které umožní snáze pracovat s funkcemi při modelování reálných problémů.

1. Derivování

Začneme několika jednoduchými výsledky o derivování funkcí.

6.1 **6.1. Věta.** *Nechť funkce $f : \mathbb{R} \to \mathbb{R}$ je spojitá na intervalu $[a, b]$ a diferencovatelná uvnitř tohoto intervalu. Jestliže platí $f(a) = f(b)$, pak existuje $c \in (a, b)$ takové, že $f'(c) = 0$.*

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 mimimum je jiné a nechť nastává jedno z nich ve vnitřním bodě c. Pak ovšem není možné, aby v c bylo $f'(c) \neq 0$, protože to by v tomto bodě byla byla funkce f buď rostoucí nebo klesající (viz 5.22) a jistě by tedy v okolí bodu c nabývala větších i menších hodnot, než je $f(c)$. □

Právě dokázanému tvrzení se říká *Rolleova věta*. Z ní snadno vyplývá následující důsledek, známý jako *věta o střední hodnotě*.

6.2 **6.2. 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 (namalujte si 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 $h'(c) = 0$. □

Větu o střední hodnotě můžeme také přepsat ve tvaru:

e6.1 (6.1) $$f(b) = f(a) + f'(c)(b - a).$$

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 takto:

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 funkcí. Je znám jako *L'Hospitalovo pravidlo*:

6.3 **6.3. 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. 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, zejména tedy pro dostatečně blízké body c k x_0 bude $g'(c) \neq 0$.[1]

$$\lim_{x\to x_0} \frac{f(x)}{g(x)} = \lim_{x\to x_0} \frac{f(x)-f(x_0)}{g(x)-g(x_0)} = \lim_{x\to x_0} \frac{f'(c_x)}{g'(c_x)},$$

kde c_x je číslo mezi x_0 a x. Nyní si všimněme, že 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. □

6.4

6.4. Důsledky. Jednoduše lze rozšířit L'Hospitalovo pravidlo i pro limity v nevlastních bodech $\pm\infty$ a v případě nevlastních hodnot limit. Je-li, např.

$$\lim_{x\to\infty} f(x) = 0, \quad \lim_{x\to\infty} g(x) = 0,$$

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

$$\lim_{x\to 0_+} \frac{(f(1/x))'}{(g(1/x))'} = \lim_{x\to 0_+} \frac{f'(1/x)(-1/x^2)}{g'(1/x)(-1/x^2)} = \lim_{x\to 0_+} \frac{f'(1/x)}{g'(1/x)} = \lim_{x\to\infty} \frac{f'(x)}{g'(x)}.$$

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

$$\lim_{x\to x_0} f(x) = \pm\infty, \quad \lim_{x\to x_0} g(x) = \pm\infty.$$

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:

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*

$$\lim_{x\to x_0} \frac{f'(x)}{g'(x)}$$

[1] 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 LHôpitals Rule, The American Mathematical Monthly, October 1986, Volume 93, Number 8, pp. 644–645."

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 y volíme nějaký pevný 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. □

6.4a

6.5. Příklady užití. Vhodnými úpravami sledovaných výrazů lze využít L'Hospitalova pravidla také na výrazy typu $\infty-\infty$, 1^∞, $0\cdot\infty$ apod. Zpravidla jde o prosté přepsání výrazů nebo o využití nějaké hladké funkce, např. exponenciální. Uveďme alespoň dva příklady hned:

$$\begin{aligned}\lim_{x\to0}\left(\frac{1}{\sin 2x}-\frac{1}{2x}\right)&=\lim_{x\to0}\frac{2x-\sin 2x}{2x\sin 2x}\\&=\lim_{x\to0}\frac{2-2\cos 2x}{2\sin 2x+4x\cos 2x}\\&=\lim_{x\to0}\frac{4\sin 2x}{4\cos 2x+4\cos 2x-8x\sin 2x}=0,\end{aligned}$$

přičemž získané tvrzení je třeba číst od konce. Tj. z existence poslední limity (podíl druhých derivací) vyplývá existence limity podílů prvních derivací a z toho plyne existence i hodnota původní limity.

Druhý příklad nám ukáže souvislost aritmetického a geometrického průměru z n hodnot. *Aritmetický průměr*

$$M^1(x_1,\dots,x_n)=\frac{x_1+\dots+x_n}{n}$$

je speciálním případem tzv. *mocninného průměru stupně* r:

$$M^r(x_1,\dots,x_n)=\left(\frac{x_1^r+\dots+x_n^r}{n}\right)^{\frac{1}{r}}.$$

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):

$$\begin{aligned}\lim_{r\to 0}\ln(M^r(x_1,\dots,x_n)) &= \lim_{r\to 0}\frac{\ln(\frac{1}{n}(x_1^r+\dots x_n^r))}{r}\\ &= \lim_{r\to 0}\frac{\frac{x_1^r\ln x_1+\dots+x_n^r\ln x_n}{n}}{\frac{x_1^r+\dots x_n^r}{n}}\\ &= \frac{\ln x_1+\dots+\ln x_n}{n} = \ln\sqrt[n]{x_1\cdot\dots\cdot x_n}.\end{aligned}$$

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*.

6.5

6.6. 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* dané funkce.

Je-li x_0 kritický 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, znamenená 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.

6.6

6.7. 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

$$S(x) = \sum_{n=0}^{\infty} a_n(x-a)^n$$

a derivujeme-li ji opakovaně, dostáváme mocninné řady (víme, že je možné takový výraz derivovat člen po členu, i když jsme to ještě 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 aproximaxi polynomy, tzv. *Taylorovými polynomy k–tého řádu*:

$$P_k f(x) = f(a) + f'(a)(x-a) + \frac{1}{2}f''(a)(x-a)^2 + \dots + \frac{1}{k!}f^k(a)(x-a)^k.$$

Přesná odpověď vypadá podobně jako věta o střední hodnotě, jen pracujeme s vyššími stupni plynomů (tzv. *Taylorův rozvoj se zbytkem*):

Věta. *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*

$$\begin{aligned} f(x) &= f(a) + f'(a)(x-a) + \dots + \frac{1}{(k-1)!}f^{(k-1)}(a)(x-a)^{k-1} + \frac{1}{k!}f^{(k)}(c)(x-a)^k \\ &= P_{k-1}f(x) + \frac{1}{k!}f^{(k)}(c)(x-a)^k. \end{aligned}$$

Důkaz. Definujme zbytek R (tj. chybu při aproximaci pro pevně zvolené x) takto

$$f(x) = P_{k-1}f(x) + R$$

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 je

$$\begin{aligned} F'(\xi) &= f'(\xi) + \sum_{j=1}^{k-1}\left(\frac{1}{j!}f^{(j+1)}(\xi)(x-\xi)^j - \frac{1}{(j-1)!}f^{(j)}(\xi)(x-\xi)^{j-1}\right) \\ &\quad - \frac{1}{(k-1)!}r(x-\xi)^{k-1} \\ &= \frac{1}{(k-1)!}f^{(k)}(\xi)(x-\xi)^{k-1} - \frac{1}{(k-1)!}r(x-\xi)^{k-1} \\ &= \frac{1}{(k-1)!}(x-\xi)^{k-1}(f^{(k)}(\xi) - r), \end{aligned}$$

protože výrazy v sumě se postupně vzájemně ruší. Nyní si stačí všimnout, že $F(a) = F(x) = f(x)$ (připoměňme, že x je pevně zvolená ale pevná hodnota). Proto podle Rolleovy věty existuje číslo c, $a < c < x$, takové, že $F'(c) = 0$. To ale je právě požadovaný vztah. □

Pokud tedy umíme odhadnout velikost k–té derivace na celém intervalu, dostaneme přímo odhady chyb. Speciálním případem je samozřejme věta o střední hodnotě coby aproximace řádu nula, viz (6.1). Dobrým příkladem jsou tady třeba goniometrické funkce. 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

$$|\sin x - (P_k \sin)(x)| \leq \frac{|x|^{k+1}}{(k+1)!}.$$

Vidíme tedy, že pro x výrazně menší než k bude chyba malá, pro x srovnatelné s k nebo větší ale bude obrovská.

6.8. Příklady.

6.8.1. *Určete Taylorovy rozvoje T^k_x (k-tého řádu v bodě x) z následujících funkcí:*
(1) T^3_0 *z funkce* $\sin x$,
(2) T^3_1 *z funkce* $\frac{e^x}{x}$.

Řešení.
(1) 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

$$T^3_0(\sin(x)) = x - \frac{1}{6}x^3.$$

(2) Opět $f(1) = e$,

$$\begin{aligned} f'(1) &= \frac{e^x}{x} - \frac{e^x}{x^2}\,(1) = 0 \\ f^{(2)} &= \frac{e^x}{x} - 2\frac{e^x}{x}^2 + \frac{2e^x}{x^3}\,(1) = e \\ f^{(3)} &= \frac{e^x}{x} - 3\frac{e^x}{x}^2 + \frac{6e^x}{x^3} - \frac{6e^x}{x^4}\,(1) = -2e \end{aligned}$$

Dostáváme tedy Taylorův rozvoj třetího řádu funkce $\frac{e^x}{x}$ v bodě 1:

$$T^3_1(\frac{e^x}{x}) = e + \frac{e}{2}(x-1)^2 - \frac{e}{3}(x-1)^3 = e(-\frac{x^3}{3} + \frac{3x^2}{2} - 2x + \frac{5}{6}).$$

□

6.8.2. *Určete Taylorův polynom T^6_0 funkce* sin *a pomocí věty* **6.6** *odhadněte chybu polynomu v bodě $\pi/4$.*

Řešení. Podobně jako v předchozím příkladu určíme

$$T^6_0(\sin(x)) = x - \frac{1}{6}x^3 + \frac{1}{120}x^5.$$

Dle věty 6.7 pak odhadneme velikost zbytku (chyby) R. Podle věty existuje $c \in (0, \frac{\pi}{4})$ takové, že

$$R(\pi/4) = \left|\frac{-\cos(c)\pi^7}{7!4^7}\right| < \frac{1}{7!} \doteq 0,0002.$$

□

6.8.3. *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. Rozvinout funkci do mocninné řady v daném bodě je to stejné, jako určit její Taylorův rovoj v daném bodě.

$$\begin{aligned}\ln(x+1) &= x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \frac{1}{4}x^4 + \dots \\ &= \ln(2) + \frac{1}{2}(x-1) - \frac{1}{8}(x-1)^2 + \frac{1}{3\cdot 2^3}(x-1)^3 - \frac{1}{4\cdot 2^4}(x-1)^4 + \dots\end{aligned}$$

První řada konverguje pro $-1 < x \leq 1$, druhá pro $-1 < x \leq 3$. □

6.8.4. *Rozviňte do mocninné řady funkci* $\cos^2(x)$ *v bodě* 0 *a určete pro která reálná čísla tato řada konverguje.*

Řešení.

$$\sum_{i=0}^{\infty} (-1)^i \frac{2^{2i-1}}{(2i)!} x^{2i},$$

konverguje pro libovolné reálné x. □

6.8.5. *Rozviňte do mocninné řady funkci* $\sin^2(x)$ *v bodě* 0 *a určete pro která reálná čísla tato řada konverguje.*

Řešení.

$$\sum_{i=1}^{\infty} (-1)^{i+1} \frac{2^{2i-1}}{(2i)!} x^{2i},$$

konverguje pro libovolné reálné x. □

6.7

6.9. Analytické a hladké funkce. Je-li f v bodě a hladká, pak můžeme napsat formálně mocninnou řadu

$$S(x) = \sum_{n=0}^{\infty} \frac{1}{k!} f^{(k)}(a)(x-a)^n.$$

Taylorova věta nám říká, že pokud tato mocninná řada má nenulový poloměr konvergence, pak je $S(x) = f(x)$ na příslušném intervalu. Takovým funkcím říkáme *analytické 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.

Abychom si alespoň představili podstatu problému, ukážeme si funkci, která má v nule všechny derivace nulové, je však všude kromě tohoto bodu nenulová:

$$f(x) = \mathrm{e}^{-1/x^2}.$$

Je dobře definovaná hladká funkce pro všechny body $x \neq 0$. Derivací dostaneme $f'(x) = f(x) \cdot 2x^{-3}$ a iterovanou derivací dostaneme součet konečně mnoha členů tvaru $C \cdot f(x) \cdot x^{-k}$, kde C je nějaké celé číslo a k je přirozené číslo. Pro každý výraz $P(x)e^{-1/x^2}$, kde P je nějaký polynom, lze opakovanou aplikací L'Hospitalova

pravidla snadno zjistit, že jde limitně k nule, při x jdoucím k nule. Dodefinujeme-li tedy hodnoty všech derivací naší funkce v nule rovnicí

$$f^{(k)} = 0,$$

získáme hladkou funkci na celém $\mathbb{R}$. Je vidět, že skutečně jde o nenulovou funkci všude mimo $x = 0$, všechny její derivace v tomto bodě jsou ale nulové. Samozřejmě to tedy není analytická funkce v bodě $x_0 = 0$.

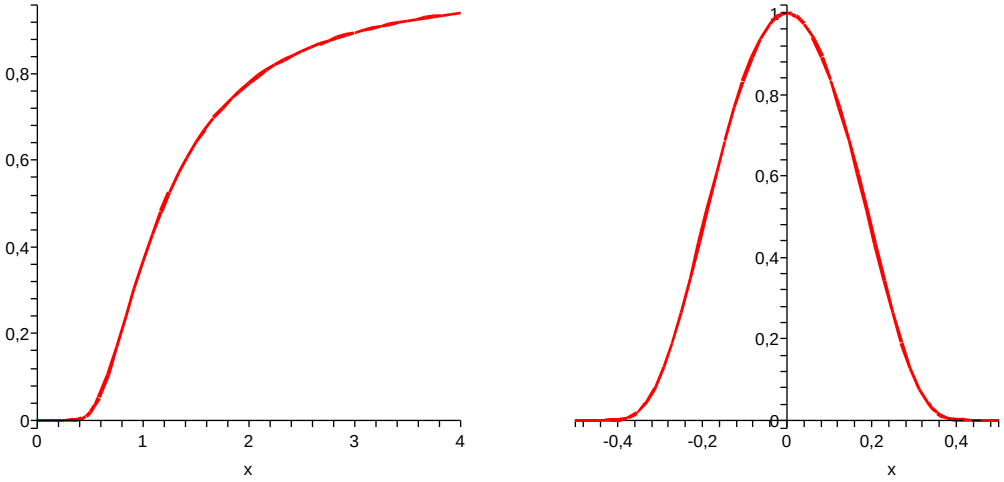
Snadno můžeme naši funkci modifikovat takto:

$$g(x) = \begin{cases} 0 & \text{je-li } x \leq 0 \\ \mathrm{e}^{-1/x^2} & \text{je-li } x > 0 \end{cases}.$$

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:

$$h(x) = \begin{cases} 0 & \text{je-li } |x| \geq a \\ \mathrm{e}^{\frac{1}{x^2 - a^2} + \frac{1}{a^2}} & \text{je-li } |x| < a. \end{cases}$$

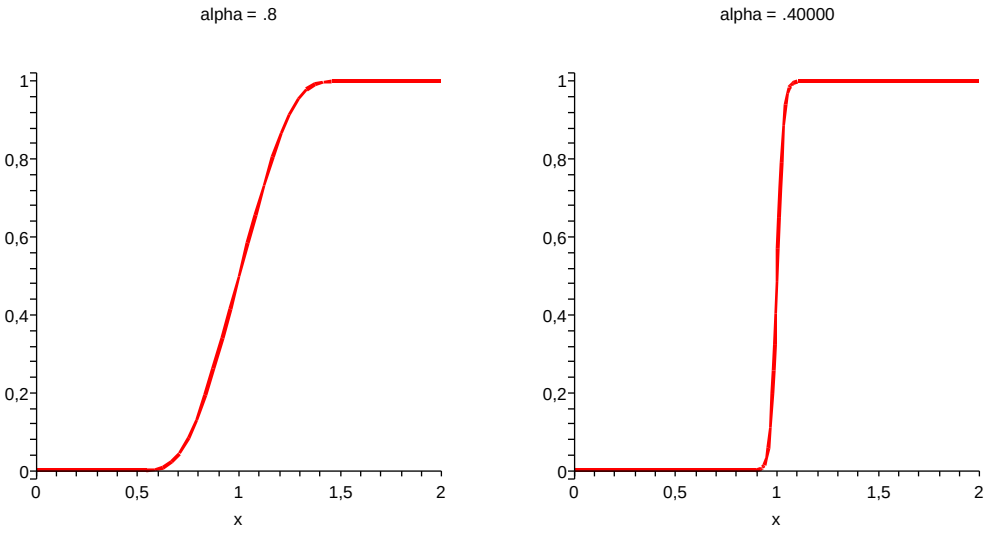
Tato funkce je opět hladká na celém $\mathbb{R}$. Poslední dvě funkce jsou na obrázcích, vpravo je použit parametr $a = 1$.



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 $x \leq a$ je přitom jmenovatel zlomku přímo dle definice funkce g nulový, při $x \geq b$ 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 $\alpha = 0.4$.



6.8

6.10. Popis lokálního chování funkcí. Už jsme se setkali s významem druhé derivace při popisu kritických bodů. Teď zobecníme diskusi kritických bodů pro všechny řády. 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.

Říkáme, že funkce f je v bodě a *konkávní* v bodě a, jestliže se její graf nachází v jistém okolí celý pod tečnou v bodě $[a, f(a)]$, tj.

$$f(x) < f(a) + f'(a)(x-a).$$

Říkáme, že funkce f je *konvexní* v bodě a, jetliže 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.

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.

Bod a nazýváme *inflexní bod* funkce f, jestliže graf funkce f přechází z jedné strany tečny na druhou. 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.

Poslední dobrou pomůckou pro náčrtek grafu funkce je zjištění *asymptot*, tj. přímek, ke kterým se blíží hodnoty funkce f. Asyptotou v nevlastním bodě ∞ je proto taková přímka $y = ax + b$, pro kterou je

$$\lim_{x\to\infty}(f(x) - ax - b) = 0.$$

Pokud asymptota existuje, platí

$$\lim_{x\to\infty}(f(x) - ax) = b$$

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 $-\infty$.

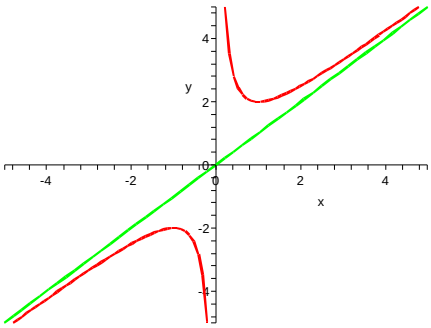
Tímto způsobem dohledáme všechny potenciální přímky splňující vlastnosti asymptot s konečnou reálnou směrnicí. Zbývají nám případné přímky kolmé na osu x: Asymptoty v bodech $a \in \mathbb{R}$ jsou přímky $x = a$ takové, že funkce f má v bodě a alespoň jednu nekonečnou jednostrannou limitu.

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 $x = 0$ (ověřte podrobně!). Derivací obdržíme

$$f'(x) = 1 - x^{-2}, \quad f''(x) = 2x^{-3}.$$

Funkce $f'(x)$ má dva nulové body ± 1. V bodě $x = 1$ má funkce lokální minimum, v bodě $x = -1$ lokální maximum. Druhá derivace nemá nulové body v celém definičním oboru $(-\infty, 0) \cup (0, \infty)$, f tedy nemá žádný inflexní bod.



6.11. Příklady.

6.11.1. *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?*

Řešení. 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 $(\sqrt{3}/8)a^2$. □

6.11.2. *Ve 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 PQ a QR (viz Matematika I). 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 $t = \frac{1}{\sqrt{6}}$, jde o minimum, navíc je hodnota determinantu v tomto bodě kladná a menší, než hodnota v bodě 0 (krajní bod intervalu, na kterém hledáme extrém), je tedy o globální minimum obsahu v čase. □

6.11.3. *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): $N = [2, 3]$, $P = [3, 3]$, $D = [0, 0]$, $C = [5, 5]$.*

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 ρ jejich drah v čase:

$$\rho(t) = (2 - \cos(4t) - 2\sqrt{2}t)^2 + (2 - \sin(4t) - 2\sqrt{2}t)^2$$
$$\rho'(t) = 16(\cos(4t) - \sin(4t))(\sqrt{2}t - 1) + 32t + 4\sqrt{2}(\cos(4t) + \sin(4t)) - 16\sqrt{2}$$

Řešit algebraicky rovnici $\rho'(t) = 0$ se nám nepodaří (ani to nelze), zbývá pouze najít řešení numericky (pomocí výpočetního softwaru). Zjistíme, že lokální minima nastávají 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 tedy má velký význam. □

6.11.4. *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 2 ($\frac{2-0}{2-1}$). Směrnice je určena derivací funkce v daném bodě, dostáváme tedy podmínku

$$\frac{2 - \ln(cx)}{2\sqrt{x}}(1) = 2,\ \text{neboli } 2 - \ln(c) = 4,$$

tedy $c = \frac{1}{e^2}$. Pro $c = \frac{1}{e^2}$ je však hodnota fce $\frac{ln(c\cdot x)}{\sqrt{x}}$ v bodě 1 rovna -2. Tedy žádné takové c neexistuje. □

6.11.5. *Vyšetřete průběh funkce*

$$\frac{x}{\ln(x)},$$

a načrtněte její graf.

Řešení.

(1) Nejprve určíme definiční obor funkce: $\mathbb{R}^+ \setminus \{1\}$.
(2) 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, ∞) 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 $f^{(2)}(e) > 0$)

(3) Určíme inflexní body:

$$f^{(2)}(x) = \frac{\ln(x) - 2}{x \ln^3(x)} = 0$$

Tato rovnice má kořen e^2, který musí být inflexním bodem (extrém to již být nemůže vzhledem k předchozímu bodu).

(4) Asymptoty. Funkce má asymptotu přímku $x = 1$. Dále hledejme asymptoty s konečnou směrnicí k:

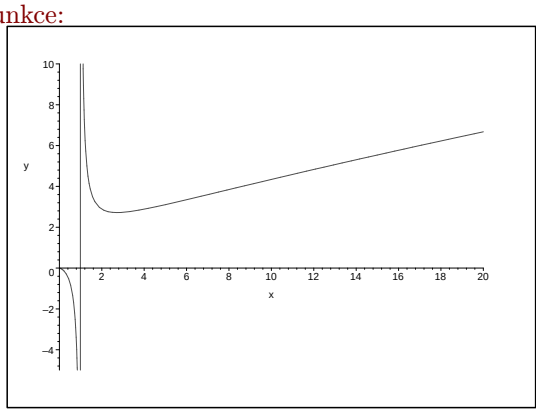
$$k = lim_{x\to\infty} \frac{\frac{x}{\ln(x)}}{x} = \lim_{x\to\infty} \frac{1}{\ln(x)} = 0.$$

Pokud asymptota existuje, má tedy směrnici 0. Pokračujme tedy ve výpočtu

$$\lim_{\times\to\infty} \frac{x}{\ln(x)} - 0 \cdot x = \lim_{x\to\infty} \ln(x) = \infty,$$

a protože limita není konečná, asymptota s konečnou směrnicí neexistuje.

Průběh funkce:



□

6.11.6. *Vyšetřete průběh funkce* $\frac{\ln(x)}{x}$ *(tj.* **mimo jiné** *najít extrémy, inflexní body, asymptoty) a načrtněte její graf.*

Řešení. Def. obor $\mathbb{R}^+$, globální maximum $x = e$, infl. bod $x = \sqrt{e^3}$, rostoucí na int $(0, e)$, klesající na (e, ∞), konkávní $(0, \sqrt{e^3}$, konvexní $(\sqrt{e^3}, \infty)$, asymptoty $x = 0$ a $y = 0$, $\lim_{x\to 0} f(x) = -\infty$, $\lim_{x\to\infty} f(x) = 0$. □

6.11.7. *Vyšetřete průběh funkce (***mimo jiné** *najít extrémy, inflexní body, asymptoty).*

$$\ln(x^2 - 3x + 2) + x.$$

Řešení. Def. obor $\mathbb{R} \setminus \langle 1, 2\rangle$. Lokální maximum $x = \frac{1-\sqrt{5}}{2}$, na celém def. oboru konkávní, asymptoty $x = 1$, $x = 2$. □

6.11.8. *Vyšetřete průběh funkce (***mimo jiné** *najít extrémy, inflexní body, asymptoty).*

$$\ln(x^2 - 3x + 2) + x.$$

Řešení. Def. obor $\mathbb{R} \setminus \langle 1, 2\rangle$. Lokální maximum $x = \frac{1-\sqrt{5}}{2}$, na celém def. oboru konkávní, asymptoty $x = 1$, $x = 2$. □

6.11.9. *Vyšetřete průběh funkce (***mimo jiné** *nalezněte extrémy, inflexní body a asymptoty):*

$$(x^2-2)e^{x^2-1}.$$

Řešení. Def. obor $\mathbb{R}$. Lokální minima v -1, 1, maximum v 0. Funkce sudá. Inflexní body $\pm\frac{1}{\sqrt{2}}$, bez asymptot. □

6.11.10. *Vyšetřete průběh funkce (***mimo jiné** *nalezněte extrémy, inflexní body a asymptoty):*

$$ln(2x^2-x-1).$$

Řešení. Def. obor $\mathbb{R}\setminus\langle-\frac{1}{2},1\rangle$. Glob. extrémy nemá. Bez inflexních bodů, asymptoty $x=-\frac{1}{2}$, $x=1$. □

6.11.11. *Vyšetřete průběh funkce (***mimo jiné** *nalezněte extrémy, inflexní body a asymptoty):*

$$\frac{x^2-2}{x-1}.$$

Řešení. 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 $y=x+1$. □

2. Integrování

6.9

6.12. Newtonův integrál. Předpokládejme, že známe na intervalu $[a,b]$ reálnou nebo komplexní funkci $F(x)$ reálné proměnné x a její derivaci

$$F'(x)=f(x).$$

Jestliže rozdělíme interval $[a,b]$ na n částí volbou bodů

e6.2 (6.2) $$a=x_0<x_1<\cdots<x_n=b$$

a přiblížíme hodnoty derivací v bodech x_i výrazy

$$f(x)\simeq\frac{F(x_{i+1})-F(x_i)}{x_{i+1}-x_i}$$

dostáváme součtem

$$F(b)-F(a)=\sum_{i=0}^{n-1}\frac{F(x_{i+1})-F(x_i)}{x_{i+1}-x_i}\cdot(x_{i+1}-x_i)\simeq\sum_{i=0}^{n-1}f(x_i)\cdot(x_{i+1}-x_i).$$

Funkci F nazýváme *antiderivace* nebo *neurčitý integrál* k funkci f a poslední výraz pro reálnou funkci $f(x)$ zjevně přibližně vyjadřuje plochu vytyčenou grafem funkce f, souřadnou osou x a přímkami $x=a$, $x=b$ (včetně znaménka zohledňujícího pozici plochy nad nebo pod osou x — namalujte si obrázek!). Dá se tedy očekávat, že takovou plochu skutečně spočteme jako rozdíl hodnot antiderivace v krajních bodech intervalu. Tomuto postupu se také říká *Newtonův integrál*. Píšeme

$$\int_a^b f(x)dx=[F(x)]_a^b=F(b)-F(a).$$

V případě komplexní funkce f je i reálná a imaginární část jejího integrálu jednoznačně dána reálnou a imaginární částí f, budeme proto v dalším pracovat výhradně s reálnými funkcemi.

V dalším skutečně ukážeme, že lze rozumně definovat pojem plocha v rovině tak, aby ji bylo možné počítat právě uvedeným způsobem. Newtonův integrál má ale jednu podstatnou vadu — jeho vyčíslení vyžaduje znalost antiderivace. Tu obecně není snadné spočíst i když ukážeme, že ke všem spojitým funkcím f existuje. Proto budeme napřed diskutovat i jinou definici integrálu.

Všimněme si ještě, že antiderivace je na každém souvislém intervalu $[a, b]$ určena jednoznačně až na konstantu. Skutečně, pokud je $F'(x) = G'(x) = f(x)$, pak Taylorův rozvoj prvního řádu se zbytkem v bodě a dává

$$F(x) - G(x) = F(a) - G(a) + (f(c) - f(c))(x - a) = F(a) - G(a)$$

na nějakém okolí bodu a. Pokud by ale $x_0 < b$ bylo supremem hodnot, pro které tento vztah ještě platí, opětovnou volbou tohoto bodu za a dosáhneme rozšíření tohoto vztahu i napravo od něj. Musí tedy platit na celém intervalu. S poukazem na toto pozorování budeme neurčitý integrál také zapisovat ve tvaru

$$F(t) = \int f(x)dx + C.$$

6.11

6.13. Riemannův integrál. Pro definici integrálu využijeme přímo intuitivní úvahy, kterou jsme v minulém odstavci odůvodňovali souvislost Newtonova integrálu s velikostí plochy.

Uvažme reálnou funkci f definovanou na intervalu $[a, b]$ a zvolme dělení (6.2) tohoto intervalu, spolu s výběrem reprezentantů ξ_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 takového dělení nazýváme číslo $\min\{x_i - x_{i-1}\}$. *Riemannův součet* odpovídající zvolenému dělení $\Xi = (x_0, \ldots, x_n)$ a reprezentantům ξ je dán výrazem

$$S_{\Xi,\xi} = \sum_{i=1}^{n} f(\xi_i) \cdot (x_i - x_{i-1})$$

Řekneme, že *Riemannův integrál* funkce f na intervalu $[a, b]$ existuje, jestliže pro každou posloupnost dělení s reprezentanty (Ξ_k, ξ_k) s normou dělení jdoucí k nule existuje limita

$$\lim_{k\to\infty} S_{\Xi_k,\xi_k} = S,$$

jejíž hodnota navíc nezávisí na volbě posloupnosti dělení a reprezentantů. Píšeme v takovém případě opět

$$S = \int_a^b f(x)dx.$$

Tato definice nevypadá příliš prakticky, nicméně nám dovolí sformulovat a dokázat některé jednoduché vlastnosti Riemannova integrálu.

Věta. *(1) Je-li f omezená reálná funkce definovaná na reálném intervalu $[a, b]$ a $c \in [a, b]$ nějaký vnitřní bod, potom 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 existují-li 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 $[a,b]$, $C \in \mathbb{R}$ konstanta a existuje-li 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 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 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. □

6.12 **6.14. Věta.** *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*

$$F(t) = \int_a^t f(x)dx$$

antiderivací funkce f na tomto intervalu.

Důkaz. Pro důkaz existence použijeme alternativní definici, která nahrazuje výběr reprezentatů a příslušné hodnoty $f(\xi_i)$ pomocí suprem hodnot $f(x)$ v příslušném podintervalu, resp. pomocí infim $f(x)$ tamtéž. Hovoříme o *horních Riemannových součtech*, resp. *dolních Riemannových součtech* (někdy také o tzv. *Darbouxově integrálu*). 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 součet příslušný dělení Ξ zadán výrazem

$$S_{\Xi,\sup} = \sum_{i=1}^{n} \sup_{x_{i-1}\le\xi\le x_i} f(\xi)\cdot(x_i - x_{i-1})$$

Zatímco dolní Riemannův součet je

$$S_{\Xi,\inf} = \sum_{i=1}^{n} \inf_{x_{i-1}\le\xi\le x_i} f(\xi)\cdot(x_i - x_{i-1}).$$

Protože zjevně pro každé dělení s reprezentanty (Ξ,ξ) platí

$$S_{\Xi,\inf} \le S_{\Xi,\xi} \le S_{\Xi,\sup}$$

a infima i suprema lze libovolně přesně aproximovat skutečnými hodnotami, 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.

Tvrzení. *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.

Důkaz. Pokud zjemníme nějaké rozdělení Ξ_1 na Ξ_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 Ξ s n vnitřními dělícími body intervalu $[a,b]$, a jiné dělení Ξ_1, jehož norma je hodně malé číslo δ. Ve společném zjemnění Ξ_2 bude jen n intervalů, které budou do součtu $S_{\sup}$ přispívat případně menším příspěvkem než je tomu v Ξ_1. Protože je f omezená funkce na $[a,b]$, bude každý z těchto příspěvků ohraničený univerzální konstantou krát velikost intervalu. Při zvolení dostatečně malého δ tedy nebude vzdálenost $S_{\Xi_1,\sup}$ od $S_{\sup}$ více než dvakrát vzdálenost $S_{\Xi,\sup}$ od $S_{\sup}$. Právě jsme ukázali, že pro libovolné číslo $\epsilon > 0$ umíme najít takové $\delta > 0$, že pro všechna dělení s normou nejvýše δ bude $|S_{\Xi,\sup} - S_{\Xi}| < \epsilon$. To je přesné 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. □

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 $S_{\sup} = S_{\inf}$. Ze definice spojitosti víme, že pro každý pevně zvolený bod $x \in [a,b]$ a každé okolí $\mathcal{O}_\epsilon(f(x))$ existuje okolí $\mathcal{O}_\delta(x)$ takové, že $f(\mathcal{O}_\delta(x)) \subset \mathcal{O}_\epsilon(f(x))$. Toto tvrzení lze přepsat takto: jsou-li $y, z \in \mathcal{O}_\delta(x)$, tzn. mimo jiné platí

$$|y - z| < 2\delta,$$

je také $f(y), f(z) \in \mathcal{O}_\epsilon(f(x))$, tzn. mimo jiné platí

$$|f(y) - f(z)| < 2\epsilon.$$

Budeme potřebovat globální variantu takového tvrzení:

Tvrzení. *Nechť je f spojitá funkce na uzavřeném konečném intervalu $[a,b]$. Pak pro každé číslo $\epsilon > 0$ existuje takové číslo $\delta > 0$, že pro všechny $z, y \in [a,b]$ splňující $|y - z| < \delta$ platí $|f(y) - f(z)| < \epsilon$.*

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 ϵ budeme uvažovat pořád stejná. Zvolíme konečně za δ minimum ze všech (konečně mnoha) $\delta(x)$. Naše spojitá funkce f tedy má požadovanou vlastnost (pouze zaměňujeme čísla ϵ a δ za jejich dvojnásobky). □

Nyní již snadno dokončíme celý důkaz existence Riemannova integrálu. Zvolme si ϵ a δ jako v posledním tvrzení a uvažujme jakékoliv dělení Ξ s n intervaly a normou nejvýš δ. Pak

$$\begin{aligned}\left|\sum_{i=1}^{n}\sup_{x_{i-1}\le\xi\le x_i} f(\xi)\cdot(x_i-x_{i-1}) - \sum_{i=1}^{n}\inf_{x_{i-1}\le\xi\le x_i} f(\xi)\cdot(x_i-x_{i-1})\right| \\ \le \sum_{i=1}^{n}\Big|\sup_{x_{i-1}\le\xi\le x_i} f(\xi) - \inf_{x_{i-1}\le\xi\le x_i} f(\xi)\Big|\cdot(x_i-x_{i-1}) \\ \le \epsilon\cdot(b-a).\end{aligned}$$

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.

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 jako výše k pevnému malému $\epsilon>0$ číslo $\delta>0$ tak, aby $|f(x+\Delta x)-f(x)|<\epsilon$ pro všechna $0\le\Delta x<\delta$. Potom ovšem při použití dostatečně jemného dělení intervalu $[a,t+\Delta t]$ dostaneme

$$\left|\frac{1}{\Delta t}\left(\int_a^{t+\Delta t} f(x)dx - \int_a^t f(t)dt\right) - f(t)\right| < \epsilon.$$

Skutečně, přiblížením integrálů kterýmkoliv Riemannovým součtem s dělením Ξ, v němž je t jedním z vnitřních bodů, dostaneme sčítance $f(\xi_i)(x_i-x_{i-1})$ s $\xi_i\in[t,t+\Delta t]$ (ostatní se vyruší v rozdílu). Všechny hodnoty $f(\xi_i)$ jsou ale k $f(t)$ blíže než o ϵ.

To ovšem znamená, že existuje v bodě t derivace funkce $F(t)$ zprava a je rovna $f(t)$. Stejně dokážeme výsledek pro derivaci zleva a celá věta je dokázaná. □

Důležité poznámky. (1) Předchozí dvě věty 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 (tj. lineární forma).

(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 $F(b)-F(a)$ antiderivace F.

(3) V prvním pomocném tvrzení v důkazu předchozí věty jsme dokázali důležité tvrzení, že pro omezenou funkci f na intervalu $[a,b]$ vždy existují limity horních součtů i dolních součtů. Říká se jim také *horní Riemannův integrál* a *dolní Riemannův integrál*. Takto lze pro omezené funkce ekvivalentně definovat i Riemannův integrál (jak jsme konečně v důkazu i činili).

(4) V dalším tvrzení 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.

(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, $a < c_i < b$. Vzhledem k aditivnosti integrálu vůči intervalu přes který se integruje, viz 6.13(1), existuje podle poslední věty v takovém případě integrál

$$F(t) = \int_a^t f(x)dx$$

pro všechna $t \in [a,b]$ a derivace funkce $F(t)$ existuje ve všech bodech t, ve kterých je f spojitá. Navíc se snadno ověří, že ve zbývajících bodech je funkce $F(t)$ spojitá, je to tedy spojitá funkce na celém intervalu $[a,b]$. Při výpočtu integrálu pomocí antiderivací je zapotřebí volit její jednotlivé části tak, aby na sebe navazovaly. Pak bude i celý integrál vyčíslen jako rozdíl v krajních hodnotách.

6.13

6.15. Integrace „po paměti“. Neurčitý integrál nám formálně dovoluje spočíst Riemannův integrál pro každou spojitou funkci. Nicméně prakticky bývá zejména použitelný tam, kde 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 $n \in \mathbb{Z}$, $n \neq -1$:

$$\int a\,dx = ax + C$$
$$\int ax^n\,dx = \frac{a}{n+1}x^{n+1} + C$$
$$\int \mathrm{e}^{ax}\,dx = \frac{1}{a}\,\mathrm{e}^{ax} + C$$
$$\int \frac{a}{x}\,dx = a\ln x + C$$
$$\int a\cos bx\,dx = \frac{a}{b}\sin bx + C$$
$$\int a\sin bx\,dx = -\frac{a}{b}\cos bx + C$$
$$\int a\cos bx\sin^n bx\,dx = \frac{a}{b(n+1)}\sin^{n+1} bx + C$$
$$\int a\sin bx\cos^n bx\,dx = -\frac{a}{b(n+1)}\cos^{n+1} bx + C$$
$$\int a\,\mathrm{tg}\,bx\,dx = -\frac{a}{b}\ln(\cos bx) + C$$
$$\int \frac{a}{a^2+x^2}\,dx = \mathrm{arctg}\left(\frac{x}{a}\right) + C$$
$$\int \frac{-1}{\sqrt{a^2-x^2}}\,dx = \arccos\left(\frac{x}{a}\right) + C$$
$$\int \frac{1}{\sqrt{a^2-x^2}}\,dx = \arcsin\left(\frac{x}{a}\right) + C$$

kde ve všech případech je zapotřebí zvážit definiční obor, na kterém je neurčitý integrál dobře definován.

K takovýmto tabulkovým hodnotám lze relativně snadno dodávat další jednoduchými pozorováními vhodné struktury integrovaných funkcí. Např.

$$\int \frac{f'(x)}{f(x)}\,dx = \ln f(x) + C.$$

6.13

6.16. Integrace per partes a substitucí. Výpočet integrálu pomocí antiderivace (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 v případě, že jeden z integrálů napravo máme počítat, zatímco druhý umíme počítat lépe.

Uveďme si nějaké příklady. Nejprve spočteme

$$I = \int x \sin x\,dx.$$

V tomto případě pomůže volba $F(x) = x$, $G'(x) = \sin x$. Odtud $G(x) = -\cos x$, proto také

$$I = -x\cos x - \int -\cos x\,dx = -x\cos x + \sin x + C.$$

Obvyklým trikem je také použít tento postup s $F'(x) = 1$:

$$\int \ln x\,dx = \int 1 \cdot \ln x\,dx = x\ln x - \int \frac{1}{x} x\,dx = x\ln x - x + C.$$

Další užitečný vzorec je odvozen z derivování složených funkcí. Je-li $F'(y) = f(y)$ a $y = \varphi(x)$, 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 antiderivaci. 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 Riemannových součtů je možné substituci porozumět snadno tak, že přírůstky v proměnné y a v x jsou vzájemně ve vztahu popsaném formálně jako

$$dy = \varphi'(x)\,dx$$

který odpovídá vztahu $\frac{dy}{dx} = \varphi'(x)$ a snadno jej spočítáme výpočtem derivace.

Jako příklad ověříme touto metodou předposlední integrál v seznamu v 6.14. 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 $t = \operatorname{acrsin} x$ dopočítáme již známý vzorec $I = \arcsin x + C$.

Při substitucích je třeba dát pozor na skutečnou existenci inverzní funkce k $y = \varphi(x)$ a při výpočtu určitého integrálu je třeba řádně přepočítávat i meze.

6.15

6.17. Příklad. Často vede použití substitucí a metody per partes k rekurentním vztahům, ze kterých teprve lze dopočíst hledané integrály. Spočtěme si alespoň jeden příklad. Metodou per partes počítáme

$$\begin{aligned} I_m &= \int \cos^m x\,dx = \int \cos^{m-1} x \cos x\,dx \\ &= \cos^{m-1} x \sin x - (m-1) \int \cos^{m-2} x(-\sin x) \sin x\,dx \\ &= \cos^{m-1} x \sin x + (m-1) \int \cos^{m-2} x \sin^2 x\,dx. \end{aligned}$$

Odtud díky vztahu $\sin^2 x = 1 - \cos^2 x$ dostáváme

$$mI_m = \cos^{m-1} x \sin x + (m-1) I_{m-2}$$

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 touto substitucí $dx = \cos^{-2} t\,dt$

$$J_k = \int \frac{dt}{\cos^2 t \left(\frac{\sin^2 t}{\cos^2 t} + 1\right)^k} = \int \cos^{2k-2} t\,dt.$$

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 $t = \operatorname{arctg} x$

$$J_2 = \frac{1}{2}\left(\frac{x}{1+x^2} + \operatorname{arctg} x\right) + C.$$

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 $[0, 2\pi]$ je

$$I_0 = \int_0^{2\pi} dx = [x]_0^{2\pi} = 2\pi$$
$$I_1 = \int_0^{2\pi} \cos x\, dx = [\sin x]_0^{2\pi} = 0$$
$$I_m = \int_0^{2\pi} \cos^m x\, dx = \begin{cases} 0 & \text{pro sudá } m \\ \frac{m-1}{m} I_{m-2} & \text{pro lichá } m \end{cases}.$$

Pro sudé $m = 2n$ tedy dostáváme přímo výsledek

$$\int_0^{2\pi} \cos^{2n} x\, dx = \frac{(2n-1)(2n-3)\dots 3 \cdot 1}{2n(2n-2)\dots 2} 2\pi,$$

zatímco u lichých m je to vždy nula (jak bylo možné přímo uhádnout z grafu funkce $\cos x$).

6.17.1. 1. *Vypočtěte:*

(1) $\int x \cos x \ \mathrm{d}x$
(2) $\int \ln x \, \mathrm{d}x$

Řešení. V obou případech řešíme metodou per partes.

(1) $x \sin x + \cos x$
(2) $x \ln x - x$

□

6.17.2. 2. *Vypočtěte:*

(1) $\int_0^{\frac{\pi}{2}} \sin x \sin 2x \, \mathrm{d}x$
(2) $\int \sin^2 x \sin 2x \, \mathrm{d}x$

Řešení.

(1) $\frac{2}{3}$
(2) $\frac{1}{2} \sin^4 x$

□

6.17.3. 3. *Dokažte, že*

$$\frac{1}{2} \sin^4 x = -\frac{1}{4} \cos(2x) + \frac{1}{16} \cos(4x) + \frac{3}{16}.$$

Řešení. Funkce na pravé a levé straně rovnosti mají shodné derivace, tudíž se liší o reálnou konstantu. Tuto konstantu určíme porovnáním funkčních hodnot v jednom bodě, například bodě 0. Hodnota obou funkcí je v nule nulová, jsou si tedy rovny. □

6.16

6.18. 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 v jmenovateli, je rozumné hned z kraje dělením se zbytkem 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. Toho skutečně dosáhneme prostým vydělením polynomů:

$$f = q \cdot g + h, \quad \frac{f}{g} = q + \frac{h}{g}.$$

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

$$\frac{4x+2}{x^2+3x+2} = \frac{A}{x+1} + \frac{B}{x+2}$$

a 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:

$$4x+2 = A(x+2) + B(x+1) \quad \Longrightarrow \quad 2A + B = 2,\ A + B = 4.$$

Odtud již přímo vychází náš rozklad. Říká se mu *rozklad na parciální zlomky.*

Zkusme nyní zobecnit naše pozorování. Předpokládejme, že jmenovatel $g(x)$ naší racionální funkce lomené má právě n různých reálných kořenů $a_1, \ldots, a_n$ a předpokládejme, že naopak čitatel $f(x)$ ani jedno z těchto čísel jako kořen nemá. Pak jsou body $a_1, \ldots a_n$ právě všechny body nespojitosti funkce $f(x)/g(x)$ a nabízí se tedy jako co nejjednodušší sčítance v součtu s podobnou vlastností výrazy tvaru

$$\frac{p(x)}{(x-a_i)^{n_i}}.$$

Chceme úspěšně použít stejný postup pro výpočet jako v předchozím jednoduchém příkladě. Musíme si proto hlídat, abychom po roznásobení uměli dosazením vhodných hodnot za volné koeficienty v polynomech $p(x)$ dostat napravo i nalevo stejné polynomy. Podbízí se tedy hledat sčítance, kde n_i bude násobnost kořene a_i, zatímco $p(x)$ bude polynom stupně $n_i - 1$. Ověřte si, že taková volba naplňuje právě sformulovaný záměr. Např. lze snadno spočíst, že

$$\frac{x-4}{(x+1)(x-2)^2} = \frac{-5}{9(x+1)} + \frac{5x-16}{9(x-2)^2}.$$

Takto to skutečně projde vždy, kdy má polynom $g(x)$ v čitateli právě tolik reálných kořenů včetně násobnosti, kolik je jeho stupeň. Opět už umíme integrovat výsledné

sčítance. První typ jsme už viděli. Druhý typ rozdělíme na součet dvou zlomků:

$$\frac{5x-16}{9(x-2)^2} = \frac{5}{9}\cdot\frac{x-2}{(x-2)^2} - \frac{6}{9}\cdot\frac{1}{(x-2)^2} = \frac{5}{9}\cdot\frac{1}{x-2} - \frac{6}{9}\frac{1}{(x-2)^2}.$$

tyto už opět integrovat umíme. Mohli jsme samozřejmě již rovnou hledat původní rozklad na parciální zlomky ve tvaru

$$\frac{x-4}{(x+1)(x-2)^2} = \frac{A}{x+1} + \frac{B}{x-2} + \frac{C}{(x-2)^2}.$$

Obdobně můžeme vždy spočíst rozklad na parciální zlomky u mocniny stupně n – bude v něm n sčítanců s konstantou v čitateli a postupně narůstajícími mocninami příslušného lineárního faktoru ve jmenovateli.

Zbývá ošetřit ještě případ, kdy reálných kořenů není dostatek. Vždycky ale existuje rozklad $g(x)$ na lineární a kvadratické faktory (ty kvadratické odpovídají dvojicím komplexně sdružených kořenů). Každý takový kvadratický faktor lze upravit na součet čtverců $(x-a)^2+b^2$, budeme pro zjednodušení rovnou počítat s x^2+b^2. Opět stejný požadavek na počet volných koeficientů a stupně nám naznačuje, že bude možné hledat příslušné sčítance ve tvaru

$$\frac{Bx+C}{(x-a)^2+b^2}.$$

Obdobně jako v případě násobných kořenů se i v případě mocniny $(x^2+b^2)^n$ takového faktoru druhého řádu 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 v proměnné x na parciální zlomky.

Všechny výše uvedené parciální zlomky už umíme integrovat. Připoměňme, že ty poslední zmíněné vedou mimo jiné na integrály diskutované v Příkladu 6.17.

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 určitých integrálů jsou ale problematické body nespojitosti racionálních funkcí lomených, v jejichž okolí jsou tyto funkce neohraničené. Tomuto problému se budeme obecně věnovat v následujícím odstavci.

6.17

6.19. Nevlastní a nekonečné integrály. Jak jsme právě viděli, občas musíme pracovat 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 je má funkce $f(x) = (2-x)^{-1/4}$ v bodě $b = 2$ limitu zleva rovnou ∞. V ostatních bodech je integrovaná funkce spojitá. Zajímáme se 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 δ a dolní mezí 2. Otočením mezí do obvyklé polohy jsme do výrazu přidali jedno znaménko $-$ 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. Hovoříme o *nekonečných integrálech*. 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.

$$\int_{-a}^a x\,dx = [\frac{1}{2}x^2]_{-a}^a = 0,$$

přestože hodnoty integrálů $\int_a^\infty x\,dx$ s jednou pevnou mezí utečou rychle k nekonečných hodnotám.

Ukažme si opět výpočet nekonečného integrálu na příkladě (jeden z typů parciálních zlomků, integrál vyřešíme snadno substitucí $x^2 + a^2 = t$, $2x\,dx = dt$)

$$\int_0^\infty \frac{x}{(x^2+a^2)^2}\,dx = \lim_{b\to\infty}\left[\frac{-1}{2(x^2+a^2)}\right]_0^b = \lim_{b\to\infty}\left(-\frac{1}{2b^2+2a^2} + \frac{1}{2a^2}\right) = \frac{1}{2a^2}.$$

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.

6.20. Příklady.

6.20.1. *Spočtěte neurčitý integrál*

$$\int \frac{1}{x^4+3x^3+5x^2+4x+2}\,\mathrm{d}x.$$

Řešení. $\frac{1}{2}\ln(x^2+2*x+2) - \frac{1}{2}\ln(x^2+x+1) + \frac{1}{3}\sqrt{3}\arctan\left(\frac{(2*x+1)\sqrt{3}}{3}\right) + C.$ □

6.20.2. *Vypočtěte integrál*

$$\int_{\frac{\pi}{4}}^{\frac{\pi}{2}} \frac{\sin(t)}{1-\cos^2 x}\,\mathrm{d}t.$$

Řešení. $\frac{1}{2}\ln\left(\frac{2+\ln(2)}{2-\ln(2)}\right)$. □

6.20.3. *Vypočtěte integrál*

$$\int_0^{\ln(2)} \frac{\mathrm{d}x}{e^{2x}-3e^x}.$$

Řešení. $-\frac{1}{6}-\frac{2}{9}\ln(2)$. □

6.18

6.21. Příklady užití integrálu. Sama definice Riemanova 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 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 je možné zatím přímo použít pouze 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 χ_A říkáme *charakteristická funkce 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 dvou Riemannovsky měřitelných disjunktních množin vyjde jako součet (detailně tu ani nebudeme dokazovat). 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.

Pro definici plochy (objemu) ve vícerozměrných prostorech budeme umět použít 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.

Střední hodnota funkce $f(x)$ na intervalu (konečném nebo nekonečném) $[a,b]$ je definována výrazem

$$m = \frac{1}{b-a}\int_a^b f(x)\,dx.$$

Z definice je m výška obdélníka (s orientací podle znaménka) nad intervalem $[a,b]$, který má stejnou plochu jako je plocha mezi osou x a grafem funkce $f(x)$.

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. Derivací tohoto zobrazení 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

$$s = \int_a^b h(t)\,dt = \int_a^b \sqrt{(f'(t))^2 + (g'(t))^2}\,dt.$$

Ve speciálním případě, kdy křivka je grafem funkce $y=f(x)$ mezi body $a<b$ obdžíme 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 Δs odpovídající přírůstku Δx proměnné x spočteme totiž právě

$$\Delta s = \sqrt{\Delta x^2 + \Delta y^2}$$

a to při pohledu přímo na naši definici integrálu znamená

$$s = \int_a^b \sqrt{1+\left(\frac{dy}{dx}\right)^2}\,dx.$$

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 2π, protože jsme takto číslo π definovali.

$$\begin{aligned} s &= 2\int_{-1}^1 \sqrt{1+(y')^2}\,dx = 2\int_{-1}^1 \sqrt{1+\frac{x^2}{1-x^2}}\,dx \\ &= 2\int_{-1}^1 \frac{1}{\sqrt{1-x^2}}\,dx = 2[\arcsin x]_{-1}^1 = 2\pi. \end{aligned}$$

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 $x=rt$ déku kružnice o poloměru r:

$$s(r) = 2\int_{-r}^r \sqrt{1+\frac{(x/r)^2}{1-(x/r)^2}}\,dx = 2\int_{-1}^1 \frac{r}{\sqrt{1-t^2}}\,dt = 2r[\arcsin x]_{-1}^1 = 2\pi r,$$

tzn. že je skutečně délka kružnice lineárně závislá na jejím poloměru.

Podobně plochu takové kružnice spočteme substitucí $x = r\sin t$, $dx = r\cos t\,dt$ (s využitím výsledku pro I_2 v 6.17)

$$a(r) = 2\int_{-r}^{r}\sqrt{r^2-x^2}\,dx = 2r^2\int_{-\pi/2}^{\pi/2}\cos^2 t\,dt = \frac{2r^2}{2}[\cos t\sin t + t]_{-\pi/2}^{\pi/2} = \pi r^2.$$

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 Δx nárůst plochy o násobek Δs délky křivky zadané grafem funkce f 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 $ds = \sqrt{dx^2+dy^2}$ je dán přírůstkem délky křivky $y = f(x)$.

Objem stejného tělesa naroste při změně Δx 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 posledních dvou vzorců odvodíme známé formule pro plochu jednotkové sféry a objem jednotkové koule.

$$A_r = 2\pi\int_{-r}^{r} r\sqrt{1-(x/r)^2}\,\frac{1}{\sqrt{1-(x/r)^2}}\,dt = 2\pi r\int_{-r}^{r} dt = 4\pi r^2$$
$$V_r = \pi\int_{-r}^{r} r^2-x^2\,dx = 2r\pi r^2 - \pi\left[\frac{1}{3}x^3\right]_{-r}^{r} = \frac{4}{3}\pi r^3.$$

6.21.1. *Odvoďte vzorec pro výpočet povrchu a objemu kužele.*

6.21.2. *Určete délku křivky dané parametricky*

$$x = \sin^2(t), \quad y = \cos^2(t),$$

pro $t \in \langle 0, \frac{\pi}{2}\rangle$.

Řešení. Možno počítat i přímo (jedná se o část přímky $y = 1-x$). $\sqrt{2}$. □

6.21.3. *Určete délku křivky dané parametricky*

$$x = t^2, \quad y = t^3$$

pro $t \in \langle 0, \sqrt{5}\rangle$.

Řešení. $\frac{335}{27}$ □

6.21.4. *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 $\int_1^\infty \frac{1}{x^3-1}\,\mathrm{d}x$. 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

$$\int_1^\infty \frac{1}{x^3-1}\,\mathrm{d}x=\frac{1}{3}\int_1^\infty\left(\frac{1}{(x-1)}-\frac{x+2}{x^2+x+1}\right)\mathrm{d}x$$

Nyní určíme zvlášť neurčitý integrál $\int \frac{x+2}{x^2+x+1}\,\mathrm{d}x$:

$$\begin{aligned}
&\int\frac{x+2}{x^2+x+1}\,\mathrm{d}x=\\
=\ &\int\frac{x+\frac{1}{2}}{(x+\frac{1}{2})^2+\frac{3}{4}}\,\mathrm{d}x+\frac{3}{2}\int\frac{1}{(x+\frac{1}{2})^2+\frac{3}{4}}\,\mathrm{d}x=\left|\begin{array}{l}\text{substituce u prvního integrálu}\\ t=x^2+x+1\\ \mathrm{d}t=2(x+\frac{1}{2})\,\mathrm{d}x\end{array}\right|\\
=\ &\frac{1}{2}\int\frac{1}{t}\,\mathrm{d}t+\frac{3}{2}\int\frac{1}{(x+\frac{1}{2})^2+\frac{3}{4}}=\left|\begin{array}{l}\text{substituce u prvního integrálu}\\ s=x+\frac{1}{2}\\ \mathrm{d}s=\mathrm{d}x\end{array}\right|\\
=\ &\frac{1}{2}\ln(x^2+x+1)+\frac{3}{2}\int\frac{1}{s^2+\frac{3}{4}}\,\mathrm{d}s=\\
=\ &\frac{1}{2}\ln((x^2+x+1)+\frac{3}{2}\frac{4}{3}\int\frac{1}{\left(\frac{2}{\sqrt{3}}s\right)^2+1}\,\mathrm{d}s=\left|\begin{array}{l}\text{substituce u druhého integrálu}\\ u=\frac{2}{\sqrt{3}}s\\ \mathrm{d}u=\frac{2}{\sqrt{3}}s\,\mathrm{d}s\end{array}\right|\\
=\ &\frac{1}{2}\ln(x^2+x+1)+2\frac{\sqrt{3}}{2}\int\frac{1}{u^2+1}\,\mathrm{d}u=\\
=\ &\frac{1}{2}\ln(x^2+x+1)+\sqrt{3}\arctan(u)=\frac{1}{2}\ln(x^2+x+1)+\sqrt{3}\arctan\left(\frac{2x+1}{\sqrt{3}}\right).
\end{aligned}$$

Celkem pak pro nevlastní integrál můžeme psát:

$$\begin{aligned}
\int_1^\infty\frac{1}{x^3-1}\,\mathrm{d}x &= \frac{1}{3}\lim_{\delta\to\infty}\left[\ln|x-1|-\frac{1}{2}\ln(x^2+x+1)-\sqrt{3}\arctan\left(\frac{2x+1}{\sqrt{3}}\right)\right]_3^\delta=\\
&= \frac{1}{3}\lim_{\delta\to\infty}\left(\frac{1}{3}\ln|\delta-1|-\frac{1}{2}\ln(\delta^2+\delta+1)-\sqrt{3}\arctan\left(\frac{2\delta+1}{\sqrt{3}}\right)\right)-\\
&\quad -\frac{1}{3}\ln(2)+\frac{1}{6}\ln(13)+\frac{\sqrt{3}}{3}\arctan\left(\frac{7}{\sqrt{3}}\right)=\\
&= \frac{1}{6}\ln(13)-\frac{1}{3}\ln(2)+\frac{\sqrt{3}}{3}\arctan\left(\frac{7}{\sqrt{3}}\right)-
\end{aligned}$$

$$-\frac{1}{3}\lim_{\delta\to\infty} ln\left|\frac{x-1}{\sqrt{x^2+x+1}}\right| - \frac{1}{3}\lim_{\delta\to\infty}\sqrt{3}\arctan\left(\frac{2\delta+1}{\sqrt{3}}\right) =$$
$$= \frac{1}{6}\ln(13) + \frac{1}{\sqrt{3}}\arctan\left(\frac{7}{\sqrt{3}}\right) - \frac{1}{3}\ln(2) - \frac{\sqrt{3}}{6}\pi$$

□

6.21.5. *Určete povrch a objem rotačního paraboloidu, který vznikne rotací části paraboly $y = 2x^2$ pro $x \in \langle 0, 1\rangle$ kolem osy y.*

Řešení. Vzorce uvedené v textech platí pro rotaci křivek kolem osy x! Je tedy nutno buď integrovat podle danou křivku neznámé y, nebo transformovat.

$$V = \int_0^2 \frac{x}{2}\,\mathrm{d}x = \pi$$
$$S = 2\pi\int_0^2 \sqrt{\frac{x}{2}}(\sqrt{1+\frac{1}{8x}})\,\mathrm{d}x = 2\pi\int_0^2\sqrt{\frac{x}{2}+\frac{1}{16}}\,\mathrm{d}x = \pi\frac{17\sqrt{17}-1}{24}\,\mathrm{d}x.$$

□

Pomocí nevlastního integrálu také umíme rozhodnout o konvegenci širší třídy nekonečných řad než doposud:

6.22. Věta. Integrální kriterium konvergence řad. *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 intergrál*

$$\int_1^\infty f(x)\,\mathrm{d}x.$$

Důkaz. Pokud interpretujeme integrál, jako plochu pod křivkou, je kriterium zřejmé.

Pokud daná řada diverguje, pak diverguje i řada $\sum_{n=2}^{\infty} f(n)$. Pro libovolné $k \in \mathbb{N}$ máme pro k-tý částečný součet s'_k (řady bez prvního člene) nerovnost

$$s'_k = \sum_{n=2}^{k} f(n) < \int_1^k f(x)\,\mathrm{d}x,$$

neboť s'_k je dolním součtem Riemannova integrálu $\int_1^k f(x)\,\mathrm{d}x$. Pak ale je

$$\int_1^\infty f(x)\,\mathrm{d}x = \lim_{k\to\infty}\int_1^k f(x)\,\mathrm{d}x > \lim_{k\to\infty} s'_k = \infty,$$

a uvažovaný integrál diverguje.

Předpokládeme nyní, že daný integrál konverguje a označme k-tý částečný součet dané řady jako s_k. Potom máme nerovnosti

$$\int_1^\infty f(x)\,\mathrm{d}x = \lim_{k\to\infty}\int_1^k f(x)\,\mathrm{d}x < \lim_{k\to\infty} s_k < \infty,$$

neboť s_k je horním součtem Riemannova integrálu $\int_1^k f(x)\,\mathrm{d}x$ a předpokádáme, že daná řada konverguje. □

6.22.1. 3. *Rozhodněte, zda následující sumy konvergují či divergují:*

a) $\sum_{n=1}^{\infty} \frac{1}{n\ln n}$,

b) $\sum_{n=1}^{\infty} \frac{1}{n^2}$.

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.

□

3. Nekonečné řady

Již jsme se při budování našeho zvířetníku funkcí setkali s mocninnými řadami, které přirozeným způsobem rozšiřují skupinu všech polynomů, viz 5.28. 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 diferencovat 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 spojisté periodické funkce, které jsou tak důležité pro modelování a zpracování audio a video signálů.

6.19

6.23. Jak ochočené jsou 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:

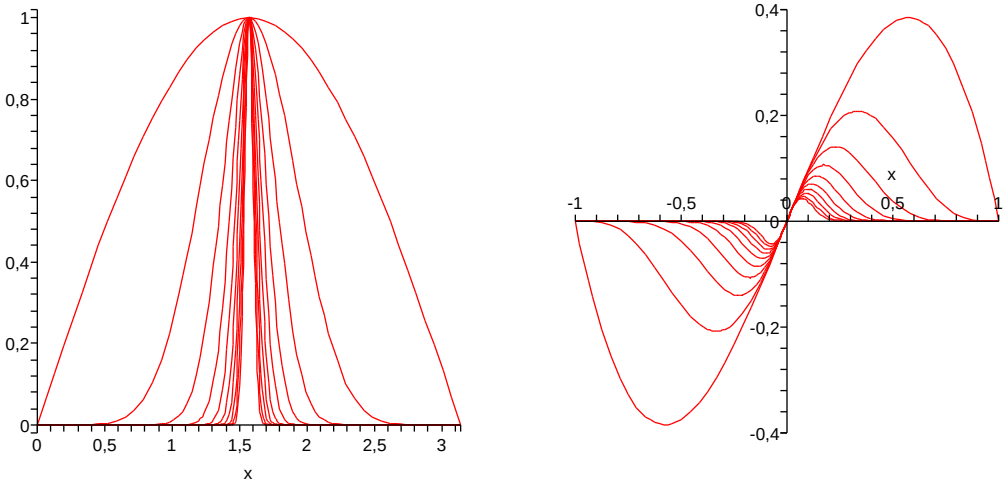
- Jsou-li všechny funkce $f_n(x)$ spojité v nějakém bodě $x_0 \in [a, b]$, je spojitá i funkce $S(x)$ v bodě x_0?
- Jsou-li všechny funkce $f_n(x)$ diferencovatelné v $a \in [a, b]$, je v něm diferencovatelná i funkce $S(x)$ a platí vztah $S'(x) = \sum_{n=1}^{\infty} f_n'(x)$?
- Jsou-li všechny funkce $f_n(x)$ integrovatelné na intervalu $[a, b]$, je integrovatelná i funkce $S(x)$ a platí vztah $S'(x) = \sum_{n=1}^{\infty} f_n'(x)$?

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 samozřejmě budou patřit mocninné řady.

Uvažme 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 hodnota 1. Proto

$$\lim_{n\to\infty} f_n(x) = \begin{cases} 0 & \text{pro všechna } x \neq \frac{\pi}{2} \\ 1 & \text{pro } x = \frac{\pi}{2}. \end{cases}$$

Zjevně tedy je limita posloupnosti funkcí f_n nespojitou funkcí. 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 $f_{n^3}(x)$ pro $n = 1, \dots, 10$.



Obrázek na pravo vykresluje $f_n(x) = x(1-x^2)^n$ na intervalu $[-1, 1]$ pro hodnoty $n = m^2$, $m = 1, \dots, 10$. Na první pohled je zjevné, že

$$\lim_{n\to\infty} f_n(x) = 0,$$

všechny funkce $f_n(x)$ jsou hladké, ale v bodě $x = 0$ je jejich derivace

$$f_n'(0) = (1 - x^2)^n - 2nx^2(1 - x^2)^{n-1}|_{x=0} = 1$$

nezávisle na n. Limitní funkce pro posloupnost f_n přitom má samozřejmě všude derivaci nulovou!

Protipříklad k třetímu tvrzení jsme už viděli. Charakteristickou funkci $\chi_{\mathbb{Q}}$ racionálních čísel můžeme vyjádřit jakou součet spočetně mnoha funkcí, které budou očíslovány právě racionálními čísly a budou vždy všude nulové, kromě množiny bodů, podle které jsou pojmenovány, kde jsou rovny 1. Riemannovy integrály všech takových funkcí budou nulové, jejich součet ale není Riemannovsky inegrovatelnou funkcí.

6.20

6.24. Stejnoměrná konvergence posloupností a řad funkcí. 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 podobně rychle po celém intervalu.

Říkáme, že posloupnost funkcí $f_n(x)$ *konverguje stejnoměrně* na intervalu $[a,b]$ k limitě $f(x)$, jestliže pro každé kladné (malé) číslo ϵ existuje (velké) přirozené číslo $N \in \mathbb{N}$ takové, že pro všechna $n \geq N$ a všechna $x \in [a,b]$ platí

$$|f_n(x) - f(x)| < \epsilon.$$

Graficky si definici můžeme představit tak, že do pásu vzniklého posunutím limitní funkce $f(x)$ na $f(x) \pm \epsilon$ pro libovolně malé, ale pevně zvolené kladné ϵ, 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'.

O řadě funkcí řekneme, že konverguje stejnoměrně na intervalu, jestliže stejnoměrně konverguje posloupnost jejích částečných součtů.

Následující tři věty lze stručně shrnout tvrzením, že všechna tři obecně neplatná tvrzení v 6.23 platí pro stejnoměrnou konvergenci (pozor ale na jemnosti u derivování).

6.21 **6.25. 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 pevný bod $x_0 \in [a,b]$ a jakékoliv pevně zvolené malé $\epsilon > 0$ bude $|f(x) - f(x_0)| < \epsilon$ pro všechna x dostatečně blízká k x_0. Z definice stejnoměrné spojitosti je pro naše $\epsilon > 0$

$$|f_n(x) - f(x)| < \epsilon$$

pro všechna $x \in [a,b]$ a všechna dostatečně velká n. Zvolme si tedy nějaké takové n a uvažme $\delta > 0$ tak, aby $|f_n(x) - f_n(x_0)| < \epsilon$ pro všechna x z δ-okolí x_0 (to je možné, protože všechny $f_n(x)$ jsou spojité). Pak

$$|f(x) - f(x_0)| < |f(x) - f_n(x)| + |f_n(x) - f_n(x_0)| + |f_n(x_0) - f(x_0)| < 3\epsilon$$

pro všechna x z námi zvoleného δ-okolí bodu x_0. □

6.22 **6.26. Věta.** *Nechť $f_n(x)$ je posloupnost Riemannovsky integrovatelných funkcí na konečném intervalu $[a,b]$, které stejnoměrně konvergují k funkci $f(x)$. Pak také $f(x)$ je integrovatelná a platí*

$$\lim_{n\to\infty} \int_a^b f_n(x)\,dx = \int_a^b (\lim_{n\to\infty} f_n(x))\,dx = \int_a^b f(x)\,dx.$$

Důkaz. Důkaz 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.

Řekneme, že posloupnost funkcí $f_n(x)$ na intervalu $[a,b]$ je *stejnoměrně Cauchyovská*, jestliže pro každé (malé) kladné číslo ϵ existuje (velké) přirozené číslo N takové, že pro všechna $x \in [a,b]$ a všechna $n \geq N$ platí

$$|f_n(x) - f_m(x)| < \epsilon.$$

Zřejmě je každá stejnoměrně konvergentní posloupnost funkcí na intervalu $[a,b]$ také stejnoměrně Cauchyovská na témže intervalu. 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 okamžitě 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

$$|f_n(x) - f_m(x)| < \epsilon$$

pro nějaké předem zvolené malé kladné ϵ a všechna $n \geq N$, $x \in [a,b]$. Nyní zvolíme pevně jedno takové n a odhadneme

$$|f_n(x) - f(x)| = \lim_{m\to\infty} |f_n(x) - f_m(x)| \leq \epsilon$$

pro všechna $x \in [a,b]$. □

Konečně se vrátíme ke snadnému důkazu 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

$$|f_n(x) - f_m(x)| < \epsilon$$

pro všechna $x \in [a,b]$, pak také

$$\left|\int_a^b f_n(x)\,dx - \int_a^b f_m(x)\,dx\right| \leq \epsilon|b-a|.$$

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 Riemannových součtům pro funkce f_n s dostatečně velkým n a limitní funkce $f(x)$ bude tedy opět integrovatelná. Zároveň

$$\left|\int_a^b f_n(x)\,dx - \int_a^b f(x)\,dx\right| \leq \epsilon|b-a|.$$

a musí proto jít o správnou limitní hodnotu. □

Pro příslušný výsledek o derivacích je třeba zvýšené pozornosti ohledně předpokladů:

6.23 **6.27. Věta.** *Nechť $f_n(x)$ je posloupnost funkcí diferencovatelných na intervalu $[a,b]$, která na tomto intervalu stejnoměrně konverguje k funkci $f(x)$. 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 $f(x)$ diferencovatelná na intervalu $[a,b]$ a platí zde $f'(x) = g(x)$.*

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že všechny naše funkce splňují $f_n(a) = 0$ (v opačném případě je pozměníme o konstanty a na výsledku úvah se nic nezmění). Pak ovšem můžeme psát pro všechny $x \in [a,b]$

$$f_n(x) = \int_a^x g_n(t)\,dt.$$

Protože ale funkce g_n stejnoměrně konvergují k funkci g na celém $[a,b]$, tedy tím spíše na intervalech $[a,x]$, kde $a \le x \le b$, platí také

$$f(x) = \int_a^x g(t)\,dt.$$

Protože je funkce g coby stejnoměrná limita spojitých funkcí opět spojitou funkcí, dokázali jsme vše potřebné, viz Věta 6.13 o Riemannově integrálu a antiderivaci. □

6.24 **6.28. Důsledek.** *Pro nekonečné řady můžeme předchozí výsledky shrnout takto: Uvažme funkce $f_n(x)$ na intervalu $I = [a,b]$.*

(1) Jsou-li všechny funkce $f_n(x)$ spojité na I a řada $S(x) = \sum_{n=1}^{\infty} f_n(x)$ konverguje stejnoměrně k funkci $S(x)$, je i funkce $S(x)$ spojitá na I.

(2) Jsou-li všechny funkce $f_n(x)$ spojitě diferencovatelné na I, a obě řady

$$S(x) = \sum_{n=1}^{\infty} f_n(x), \quad T(x) = \sum_{n=1}^{\infty} f_n'(x)$$

konvergují stejnoměrně, pak je také funkce $S(x)$ spojitě diferencovatelná 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 I a řada $S(x) = \sum_{n=1}^{\infty} f_n(x)$ konverguje stejnoměrně k funkci $S(x)$ na I, je tamtéž integrovatelná i funkce $S(x)$ a platí vztah

$$\int_a^b \left(\sum_{n=1}^{\infty} f_n(x)\right) dx = \sum_{n=1}^{\infty} \int_a^b f_n(x)\,dx.$$

6.25 **6.29. Test pro stejnoměrnou konvergenci.** Nejjednodušším způsobem pro zjištění stejnoměrné konvergence funkcí je porovnání s absolutní konvergencí vhodné posloupnosti. 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

$$|s_k(x) - s_m(x)| \le \left|\sum_{n=m+1}^{k} f_n(x)\right| \le \sum_{n=m+1}^{k} |f_n(x)| \le \sum_{n=m+1}^{k} a_k.$$

Pokud je řada (kladných) konstant $\sum_{n=1}^{\infty} a_n$ konvergentní, pak bude samozřejmě posloupnost jejích částečných součtů Caychyovská. Právě jsme ale spočetli, že v takovém případě bude posloupnost částečných součtů $s_n(x)$ stejnoměrně Caychyovská. Díky tvrzení dokázanému před chvílí v 6.26 jsme tedy právě dokázali následující

Tvrzení. *Nechť $f_n(x)$ je posloupnost funkcí definovaných na intervalu $I = [a,b]$ 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.*

6.26

6.30. Důsledky pro mocninné řady. Weistrassův testu je velice užitečný pro diskusi mocninných řad

$$S(x) = \sum_{n=1}^{\infty} a_n (x - x_0)^n$$

se středem v bodě x_0. Při našem prvním setkání s mocninnými řadami jsme ukázali v 5.30, že každá taková řada konverguje na $(x_0 - \delta, x_0 + \delta)$, kde tzv. poloměr konvergence $\delta \geq 0$ může být také nula nebo ∞. (viz také 5.33). Zejména jsme v důkazu věty 5.30 pro ověření konvergence řady $S(x)$ používali srovnání s vhodnou geometrickou posloupností. Podle Weistrassova 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

Důsledek. *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 v zápětí, 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 přibolížíme v další kapitole.

6.30.1. *Sečtěte řadu*

$$\sum_{n=1}^{\infty} \frac{1}{n 2^n}.$$

Nápověda: $\int_2^{\infty} \frac{\mathrm{d}x}{x^{n+1}} = \frac{1}{n 2^n}$.

Řešení. Zaměnou sumace s integrací dostaneme integrál $\int_2^{\infty} \left(\sum_{n=1}^{\infty} \frac{1}{x^{n+1}} \right) \mathrm{d}x = \ln 2$. □

KAPITOLA 7

Spojité modely

jak šikovně zachytit nelinární změny?
– pořádně si je lineárně přibližme...

V této kapitole se budeme snažit podat stručné náznaky, jak lze relativně jednoduše používat nástroje diferenciálního a integrálního počtu. V jistém smyslu půjde o postupy a nástroje podobné, jako jsme již viděli v kapitole třetí. Jen místo konečně rozměrných vektorů budou naše objekty nebo jejich stavy často prezentovány pomocí funkcí.

V první části budeme aproximovat funkce pomocí předem pevně zvolených sad generátorů. V zásadě budeme ideově pokračovat v postupech, které známe z konce třetí části druhé kapitoly. Poté se budeme zabývat integrálními operacemi, tj. lineárními operátory definovanými na funkcích pomocí integrování.

1. Aproximace pomocí Fourierových řad

7.1

7.1. Vzdálenosti funkcí. Zvolme si pevně nějaký interval $I = [a, b]$, konečný nebo nekonečný. Koncept integrování můžeme velice intuitivním způsobem využít pro vyjádření vzdálenosti funkcí definované na I: Pro každé dvě (reálné nebo komplexní) funkce f, g na I zkusíme definovat jejich vzdálenost $\|f - g\|$ jako plochu oblasti vymezené mezi jejich grafy, tj.

$$\|f - g\|^2 = \int_a^b |f(x) - g(x)|^2 \, dx.$$

Samozřejmě je třeba předpokládat, že tento Riemannův integrál existuje. Velikost $\|f\|$ funkce f je pak její vzdálenost od funkce nulové, tj.

$$\|f\|^2 = \int_a^b |f(x)|^2 \, dx.$$

Pro jednoduchost budeme pracovat s množinou $\mathcal{S} = \mathcal{S}[a, b]$ omezených a po částech spojitých reálných funkcí na I, ale úvahy lze rozšiřovat podle potřeby (často ale za cenu značné technické námahy).

Z námi již dokázaných vlastností integrování je okamžitě vidět, že $\mathcal{S}$ je vektorový prostor a že námi právě uvažovaná velikost je odvozena z dobře definovaného symetrického bilineárního zobrazení

$$\langle f, g \rangle = \int_a^b f(x)g(x) \, dx,$$

které má všechny vlastnosti skalárního součinu. V konečněrozměrném případě jsme takto definovali velikost vektorů v odstavci 2.37. Nyní je to naprosto stejné a pokud zúžíme naši definici na vektorový prostor generovaný nad reálnými čísly jen konečně

mnoha funkcemi $f_1, \dots, f_k$, dostaneme opět dobře definovaný skalární součin na tomto konečněrozměrném vektorovém podprostoru.

Jako příklad uvažme funkce $f_i = x^i$, $i = 0, \dots, k$. Jimi je v $\mathcal{S}$ 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 $f_0, \dots, f_k$. Pokud by navíc naše generátory měly tu vlastnost, že

e7.1 (7.1) $$\langle f_i, f_j \rangle = \begin{cases} 0 & \text{pro } i \neq j \\ 1 & \text{pro } i = j \end{cases}$$

jde o tzv. *ortonormální bázi*. Připomeňme si v této souvislosti proceduru Grammovy–Schmidtovy ortogonalizace, viz 2.48, která z libovolného systému generátorů f_i vytvoří nové 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 formulemi

$$g_{\ell+1} = f_{\ell+1} + a_1 g_1 + \cdots + a_\ell g_\ell, \quad a_i = -\frac{\langle f_{\ell+1}, g_i \rangle}{\|g_i\|^2}$$

pro $\ell > 1$.

Aplikujme tuto proceduru na první tři polynomy $1, x, x^2$ na intervalu $[-1, 1]$. Dostaneme $g_1 = 1$,

$$\begin{aligned} g_2 &= x - \frac{1}{\|g_1\|^2} \int_{-1}^{1} x \cdot 1 \, dx \cdot 1 = x - 0 = x \\ g_3 &= x^2 - \frac{1}{\|g_1\|^2} \int_{-1}^{1} x^2 \cdot 1 \, dx \cdot 1 - \frac{1}{\|g_2\|^2} \int_{-1}^{1} x^2 \cdot x \, dx \cdot x \\ &= x^2 - \frac{1}{3}. \end{aligned}$$

Příslušná ortogonální báze prostoru $\mathbb{R}_2[x]$ na intervalu $[-1, 1]$ je tedy $1, x, x^2 - 3$. Normalizací, tj. vhodným násobením skalárem tak, aby prvky v bázi měly velikost jedna dostaneme ortonormální bázi

$$h_1 = \sqrt{\frac{1}{2}}, \quad h_2 = \sqrt{\frac{3}{2}} x, \quad h_3 = \frac{1}{2}\sqrt{\frac{5}{2}}(3x^2 - 1).$$

Takovým ortonormálním generátorům $\mathbb{R}_k[x]$ se říká *Legendreovy polynomy*.

7.2 **7.2. Ortogonální systémy funkcí.** Připomeňme si výhody, které ortonormální báze podprostorů měly pro konečněrozměrné vektorové prostory. Můžeme pokračovat v předchozím příkladu polynomů a uvažovat třeba $V = \mathbb{R}_k[x]$ pro libovolné $k > 2$. Pro libovolnou funkci $h \in V$ bude funkce

$$H = \langle h, h_1 \rangle h_1 + \langle h, h_2 \rangle h_2 + \langle h, h_3 \rangle h_3$$

jednoznačně určenou funkcí, která minimalizuje vzdálenost $\|h - H\|$ mezi všemi funkcemi v $\mathbb{R}_2[x]$. Koeficienty pro nejlepší aproximaci zadané funkce pomocí funkce z vybraného podprostoru je možné tedy získat prostě integrací.

Uvedený příklad podbízí následující zobecnění: Když provedeme proceduru Grammovy–Schmidtovy ortogonalizace pro všechny monomy $1, x, x^2, \dots$, tj. pro spočetný systém generátorů, co z toho vznikne? Nebo ještě obecněji – co se stane, když zvolíme úplně libovolný spočetný systém lineárně nezávislých funkcí v $\mathcal{S}$ takový, že každé dvě různé z nich mají nulový skalární součin? Takovému systému

funkcí na intervalu I říkáme *ortogonální systém funkcí*. Jestliže jsou všechny funkce f_n v posloupnosti po dvou ortogonální a zároveň je pro všechna n velikost $\|f_n\| = 1$ normovaná, hovoříme o *ortonormálním systému funkcí*.

Nechť tedy tvoří posloupnost funcí f_n ortogonální systém po částech spojitých funkcí na intervalu $I = [a, b]$ a předpokládejme, že pro konstanty c_n konverguje řada

$$F(x) = \sum_{n=1}^{\infty} c_n f_n$$

stejnoměrně na I. Pak snadno vyjádříme skalární součin $\langle F, f_n\rangle$ po jednotlivých sčítancích (viz Důsledek 6.28) a dostaneme

$$\langle F, f_n\rangle = \sum_{m=1}^{\infty} c_m \int_a^b f_m(x) f_n(x)\,dx = c_n \|f_n\|^2.$$

Máme tedy tušení, v jakou přibližně odpověď je možné doufat, a docela přehledně nám ji skutečně dává následující věta:

7.3 **7.3. Věta.** *Nechť f_n, $n = 1, 2, \ldots$, je ortogonální posloupnost funkcí Riemannovsky integrovatelných na $I = [a, b]$ a nechť g je libovolná funkce Riemannovsky integrovatelná na I. Označme*

$$c_n = \|f_n\|^{-2} \int_a^b f_n(x) g(x)\,dx.$$

(1) Pro libovolné pevné $n \in \mathbb{N}$ má ze všech lineárních kombinací funkcí $f_1, \ldots, f_n$ nejmenší vzdálenost od g výraz

$$h_n = \sum_{i=1}^{n} c_i f_i(x).$$

(2) Řada čísel $\sum_{n=1}^{\infty} c_n^2 \|f_n\|^2$ vždy konverguje a platí

$$\sum_{n=1}^{\infty} c_n^2 \|f_n\|^2 \le \|g\|^2.$$

(3) Vzdálenost g od částečných součtů $s_k = \sum_{n=1}^{k} c_n f_n$ jde v limitě k nule, tj.

$$\lim_{k\to\infty} \|g - s_k\|^2 = 0,$$

tehdy a jen tehdy, když

$$\sum_{n=1}^{\infty} c_n^2 \|f_n\|^2 = \|g\|^2.$$

Ještě než se pustíme do důkazu, zkusíme lépe porozumět významu jednotlivých tvrzení této věty. Protože pracujeme s úplně libovolně zvoleným ortogonálním systémem funcí, nemůžeme očekávat, že lze dobře aproximovat jakoukoliv funkci pomocí lineárních kombinací funkcí f_i. Např. když se omezíme u ortogonálních polynomů pouze na sudé stupně, určitě budeme dobře aproximovat pouze sudé funkce. Nicméně hned první tvrzení nám říká, že vždycky budeme dosahovat nejlepší možné aproximace částečnými součty. Druhé a třetí tvrzení pak můžeme vnímat jako analogii ke komým průmětům do podprostorů vyjádřených pomocí souřadnic. Skutečně, že pokud k dané funkci g bodově konverguje řada $F(x) = \sum_{n=1}^{\infty} c_n f_n$, pak je funkce $F(x)$ kolmým průmětem g do vektorového podprostoru všech takovýchto řad.

Na druhé straně ale naše věta neříká, že by částečné součty uvažované řady musely bodově konvergovat k nějaké funkci. Tj. řada $F(x)$ nemusí být obecně konvergentní ani v případě, kdy nastane rovnost v (3). Pokud ale např. existuje konečná hodnota $\sum_{n=1}^{\infty} |c_i|$ a všechny funkce f_n jsou stejnoměrně omezené na I, pak zřejmě řada $F(x)$ konverguje v každém x.

DŮKAZ. Zvolme libovolnou lineární kombinaci $f = \sum_{n=1}^{k} a_n f_n$ a spočtěme její vzdálenost od g. Dostáváme

$$\begin{aligned}
\|g - \sum_{n=1}^{k} a_n f_n\|^2 &= \int_a^b \left(g - \sum_{n=1}^{k} a_n f_n\right)^2 dx \\
&= \int_a^b g^2\,dx - 2\int_a^b \sum_{n=1}^{k} a_n f_n g\,dx + \int_a^b \left(\sum_{n=1}^{k} a_n f_n\right)^2 dx \\
&= \|g\|^2 - 2\sum_{n=1}^{k} a_n c_n + \sum_{n=1}^{k} a_n^2 \|f_n\|^2 \\
&= \|g\|^2 + \sum_{n=1}^{k} \|f_n\|^2((c_n - a_n)^2 - c_n^2).
\end{aligned}$$

Evidentně lze poslední výraz minimalizovat právě volbou $a_n = c_n$ a tím 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 tzv. *Besselova nerovnost*

$$\sum_{n=1}^{k} c_n^2 \|f_n\|^2 \le \|g\|^2.$$

Tím je dokázáno 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, hovoříme o tzv. *Parsevalově rovnosti*. Přímo z definic vyplývá nyní tvrzení (3). □

Ortonogonální systém funkcí nazveme *úplný ortogonální systém* na intervalu $I = [a, b]$, jetliže platí Parsevalova rovnost pro každou funkci g s konečnou velikostí $\|g\|$ na tomto intervalu.

7.4

7.4. Fourierovy řady. Předchozí věta naznačuje, že umíme se spočetnými ortogonálními systémy f_n funkcí pracovat velice podobně jako s konečnými ortogonálními bazemi vektorových prostorů, jsou tu ale zásadní rozdíly:

- Není snadné říci, jak vypadá celý prostor konvergentních nebo stejnoměrně konvergentních řad $F(x) = \sum_{n=1}^{\infty} c_n f_n$.
- Pro danou integrovatelnou funkci umíme najít jen nejlepší možné přiblížení takovou řadou $F(x)$.

V případě, že místo ortonogonálního systému f_n máme systém ortonormální, jsou formulky ve větě o něco jednodušší, žádné další zlepšení ale nenastane.

Jako pěkný příklad na integrování lze elementárními metodami ověřit, že systém funkcí

$$1,\ \sin x,\ \cos x,\ \sin 2x,\ \cos 2x,\ \ldots,\ \sin nx,\ \cos nx,\ \ldots$$

je ortogonální systém na intervalu $[-\pi, \pi]$ (a také na kterémkoliv jiném intervalu o délce 2π). Řady z předchozí věty odpovídající tomuto systému nazýváme *Fourierovy řady*. I v obecném případě diskutovaném výše se někdy hovoří o obecných Fourierových řadách vzhledem k ortogonálnímu systému funkcí f_n. Koeficienty c_n se pak nazývají *Fourierovy koeficienty funkce* f.

Na intervalu $[-\pi, \pi]$ jsou velikosti všech funkcí kromě první vždy $\sqrt{\pi}$, první má velikost $\sqrt{2\pi}$. Lze dokázat, že náš systém funkcí je úplným ortogonálním systémem, nebudeme to zde ale dokazovat. Ve smyslu vzdálenosti funkcí definované pomocí našeho skalárního součinu proto budou částečné součty Fourierovy řady $F(x)$ pro libovolnou funkci $g(x)$ s konečným integrálem $\int_a^b g(x)^2\,dx$, tj.

$$F(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n \cos(nx) + b_n \sin(nx))$$

s koeficienty

$$a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} g(x)\cos(nx)\,dx, \quad b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} g(x)\sin(nx)\,dx,$$

vždy konvergovat k funkci $g(x)$.

Z obecnějších úvah lze dovodit, že z konvergence v tomto smyslu vždy vyplývá bodová konvergence částečných součtů ve skoro všech bodech $x \in I$. Nebudeme zde ale ani vysvětlovat, co znamená „skoro všechny“, ani nebudeme takový výsledek dokazovat.

Jako příklad Fourierovy řady si uvedeme Fourierovu řadu pro periodickou funkci vzniklou z Heavisideovy funkce zúžením na jednu periodu. Tj. naše funkce g bude na intervalu $[-\pi, 0]$ rovna -1 a na intervalu $[0, \pi]$ bude rovna 1. Protože jde o funkci lichou, jistě budou všechny koeficienty u funkcí $\cos(nx)$ nulové, a pro coeficienty u funkcí $\sin(nx)$ spočteme

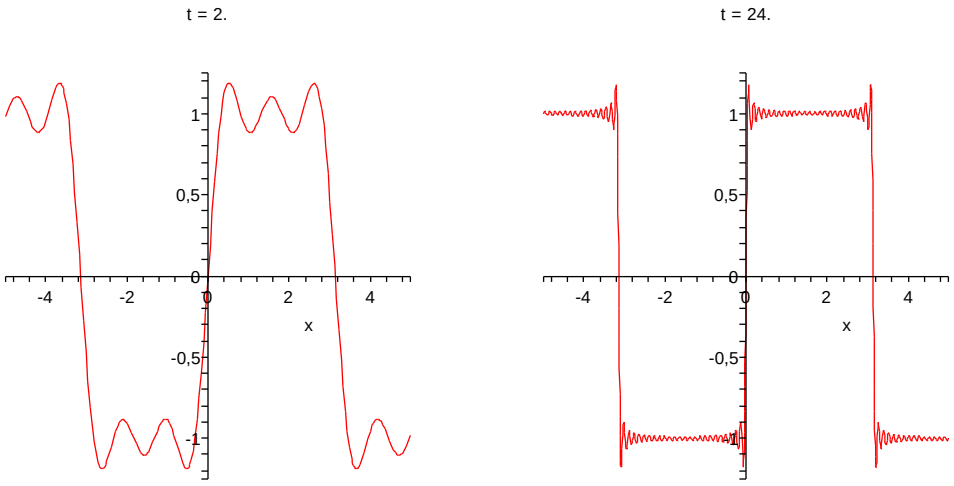
$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} g(x)\sin(nx)\,dx = \frac{2}{\pi}\int_0^{\pi}\sin(nx)\,dx = \frac{2}{n\pi}(1-(-1)^n).$$

Výsledná Fourierova řada je tedy tvaru

$$g(x) = \frac{4}{\pi}\left(\sin(x) + \frac{1}{3}\sin(3x) + \frac{1}{5}\sin(5x) + \ldots\right)$$

a součet jejích prvních pěti a prvních padesáti členů je na následujících dvou obrázcích.

Všimněme si, že se zvyšujícím se počtem členů řady se výrazně spřesňuje 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 Heavisideovu funkci.



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!).

Bez podrobného důkazu si uvedeme následující větu podávající ucelený obrázek o bodové konvergenci Fourierových řad. Nejde o nutné podmínky konvergence a v literatuře lze najít řadu jiných formulací. Tato je ale jednoduchá a postihuje velké množství užitečných případů.

Věta. *Nechť g je po částech spojitá a po částech monotonní funkce na intervalu $[-\pi,\pi]$. Pak její Fourierova řada $F(x)$ konverguje na $[-\pi,\pi]$ a její součet je*

- *roven hodnotě $g(x_0)$ v každém bodě $x_0 \in [-\pi,\pi]$, ve kterém je funkce $g(x)$ spojitá,*
- *v každém bodě nespojitosti x_0 funkce $g(x)$ roven*
$$\frac{1}{2}\left(\lim_{x\to x_0^+} g(x) + \lim_{x\to x_0^-} g(x)\right),$$
- *v krajních bodech intervalu $[-\pi,\pi]$ je roven*
$$\frac{1}{2}\left(\lim_{x\to -\pi^+} g(x) + \lim_{x\to \pi^-} g(x)\right).$$

Pokud navíc je funkce $g(x)$ spojitá, periodická s periodou 2π a všude existuje její po částech spojitá derivace, pak konverguje její Fourierova řada stejnoměrně.

7.5

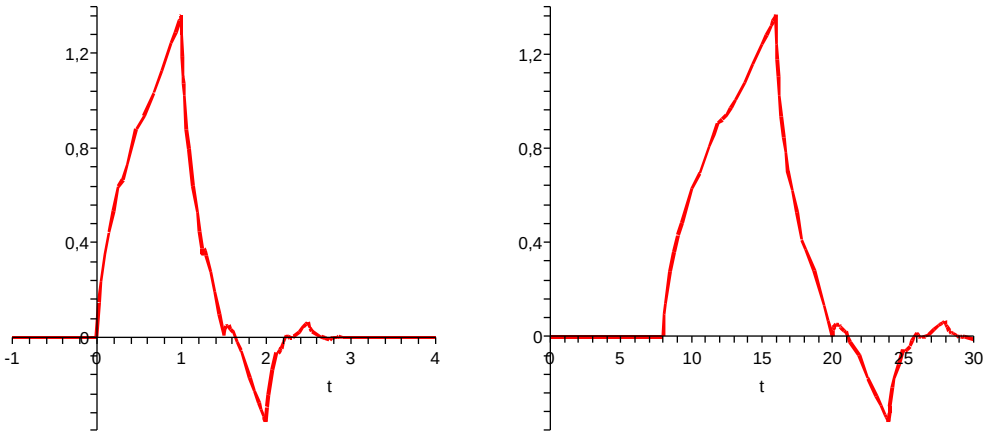
7.5. Wavelety. Fourierovy řady a další z nich vycházející nástroje jsou využívány ke zpracování různých signálů, obrázků apod. Povaha použitých periodických goniometrických funkcí a jejich prosté škálování pomocí zvětšující se frekvence zároveň omezují jejich použitelnost. V mnoha oborech proto vyvstala přirozená potřeba nalézt šikovnější úplné ortogonální systémy funkcí, které budou vycházet z předpokládané povahy dat a které bude možné efektivněji zpracovávat.

Takový systém se lze například vytvořit volbou vhodné spojité funkce ψ s kompaktním nosičem, ze které sestrojíme spočetně mnoho funkcí ψ_{ij}, $j,k \in \mathbb{Z}$, pomocí dyadických translací a dilatací:

$$\psi_{jk}(x) = 2^{j/2}\psi(2^j x - k).$$

Pokud tvar mateřské funkce ψ dobře vystihuje možné chování dat, a zároveň její potomci ψ_{jk} tvoří úplný ortogonální systém, pak se zpravidla dobře daří konkrétní zpracovávaný signál aproximovat pomocí jen několika málo funkcí.

Nebudeme zde zacházet do podrobností, jde o mimořádně živý směr výzkumu i základ komerčních aplikací. Zájemce snadno najde spoustu literatury. Na obrázku je ilustrována tzv. Daubechies mateřská wavelet $D4(x)$ a její dcera $D4(2^{-3}x - 1)$.



2. Integrální operátory

7.6

7.6. Integrální operátory. V případě konečněrozměrných vektorových prostorů jsme mohli vnímat vektory jako zobrazení z konečné množiny pevně zvolených generátorů do prostoru souřadnic. Nejjednodušší lineární zobrazení zobrazovala vektory do skalárů (tzv. lineární formy) a byla definována pomocí jednořádkových matic jako součet součinů těchto souřadnic s pevně zvolenými hodnotami na generátorech. Složitější zobrazení s hodnotami opět v tom samém prostoru pak byla obdobně zadána maticemi. Velice podobně umíme přistoupit k lineárním operacím na prostorech funkcí.

V případě vektorového prostoru $\mathcal{S}$ všech po částech spojitých funkcí na intervalu $I = [a, b]$ se lineární zobrazení $\mathcal{S} \to \mathbb{R}$ nazývají (reálné) *lineární funkcionály*. Jednoduše je můžeme zadat dvěma způsoby – pomocí vyčíslení funkce (případně jejích derivací) v jednotlivých bodech nebo pomocí integrování. Příkladem funkcionálu L tedy může být vyčíslení v jediném pevném bodě $x_0 \in I$

$$L(f) = f(x_0)$$

integrální funkcionál pak je 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. Dobrou představu dává také volba

$$g(x) = \begin{cases} 0 & \text{je-li } |x| \geq a \\ \mathrm{e}^{\frac{1}{x^2-a^2}+\frac{1}{a^2}} & \text{je-li } |x| < a. \end{cases}$$

To je funkce hladká na celém $\mathbb{R}$ s kompaktním nosičem v intervalu $(-a, a)$, viz 6.9. V bodě $x = 0$ má přitom hodnotu jedna. Integrální funkcionál

$$L_y(f) = \int_a^b f(x)g(y-x)\,dx$$

je možné vnímat jako „rozmlžené zprůměrování“ hodnot funkce f kolem bodu $x = y$ (obrázek funkce g je v 6.9 – ve svém středu má hodnotu jedna a hladkým monotonním způsobem se plynule přimkne k nule ve vzdálenosti a na obě strany). Ještě lepší volbou je z tohoto pohledu libovolná funkce g jejíž integrál přes celou reálnou osu je jednička.

7.7

7.7. Konvoluce funkcí. Pohled na integrální funkcionál L_y jako na zprůměrované chování funkce f v okolí daného bodu je názornější pro případ nevlastních mezí integrálu $a = -\infty$, $b = \infty$. Místo prostoru $\mathcal{S}$ všech po částech spojitých funkcí na $\mathbb{R}$ budeme uvažovat po částech spojité a v absolutní hodnotě integrovatelné funkce f v roli argumentu pro náš funkcionál. Volný parametr y může být vnímán jako nová nezávislá proměnná a naše operace 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 $f * g$. Většinou se konvoluce definuje pro reálné nebo komplexní funkce s kompaktním nosičem na celém $\mathbb{R}$. 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 na dvojicích funkcí s kompaktními nosiči komutativní.

Konvoluce je mimořádně užitečný nástroj pro modelování způsobu, jak můžeme pozorovat experiment 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.

Konvoluce jsou jedním z mnoha případů obecných integrálních operátorů na prostorech funkcí

$$K(f)(y) = \int_a^b f(x)k(y,x)\,dx$$

s jádrem daným funkcí dvou proměnných $k : \mathbb{R}^2 \to \mathbb{R}$. Definiční obor takových funkcionálů je nutné vždy volit s ohledem na vlastnosti jádra tak, aby vždy existoval použitý integrál.

7.8

7.8. Fourierova transformace. 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 teď alespoň na jeden mimořádně důležitý případ, tzv. *Fourierovu transformaci* $\mathcal{F}$, která úzce souvisí s Fourierovými řadami. Připomeňme si základní formuli pro parametrizaci jednotkové kružnice v komplexní rovině s rychlostí obíhání $\omega = 2\pi/T$, kde T je čas jednoho oběhu:

$$\mathrm{e}^{i\omega t} = \cos\omega t + i\sin\omega t.$$

Pro (reálnou nebo komplexní) funkci $f(t)$ můžeme spočíst její tzv. komplexní Fourierovy koeficienty jako komplexní čísla

$$c_n = \frac{1}{T}\int_{-T/2}^{T/2} f(t)\,\mathrm{e}^{-i\omega n t}\,dt.$$

Přitom platí vztahy mezi koeficienty a_n a b_n Fourierových řad (po přepočtu formulí pro tyto koeficienty pro funkce s obecnou periodou délky T) a těmito čísly c_n

$$c_n = \tfrac{1}{2}(a_n - ib_n), \quad c_{-n} = \tfrac{1}{2}(a_n + ib_n)$$

a při reálném f jsou samozřejmě c_n a c_{-n} komplexně konjugované. Označíme-li $\omega_n = \omega n$, bude tedy původní funkce $f(t)$ s konvergující Fourierovou řadou rovna

$$f(t) = \sum_{n=-\infty}^{\infty} c_n\,\mathrm{e}^{i\omega_n t}\,.$$

Při pevně zvoleném T vyjadřuje výraz $\Delta\omega = 2\pi/T$ právě změnu ve frekvenci způsobenou nárustem n o jedničku. Je to tedy právě diskrétní krok, se kterým při výpočtu koeficientů Fourierovy řady měníme frekvence. Koeficient $1/T$ u formule pro c_n 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 ω_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 poslední formuli 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 ω_n hodnoty

$$g(\omega_n) = \int_{-T/2}^{T/2} f(x)\,\mathrm{e}^{-i\omega_n x}\,dx.$$

Předpokládejme, že naše funkce f je integrovatelná v absolutní hodnotě přes celé $\mathbb{R}$. Pak můžeme limitně přejít $T \to \infty$ a dojde ke zejmňování normy $\Delta\omega$ našich intervalů. Zároveň se dostaneme v posledním výrazu k integrálu

$$g(\omega) = \int_{-\infty}^{\infty} f(x)\,\mathrm{e}^{-i\omega x}\,dx.$$

Můžeme tedy položit pro (každou v absolutní hodnotě Riemannovsky integrovatelnou) funkci f na $\mathbb{R}$

$$\mathcal{F}(f)(\omega) = \tilde{f}(\omega) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(t)\,\mathrm{e}^{-i\omega t}\,dt.$$

Této funkci $\tilde f$ říkáme Fourierova trasnformace funkce f. Přechozí úvahy pak ukazují, že pro „rozumné“ funkce $f(t)$ 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 existuje k právě definované *Fourierově transformaci* $\mathcal{F}$ inverzní operace $\mathcal{F}^{-1}$, které říkáme *inverzní Fourierova transformace*.

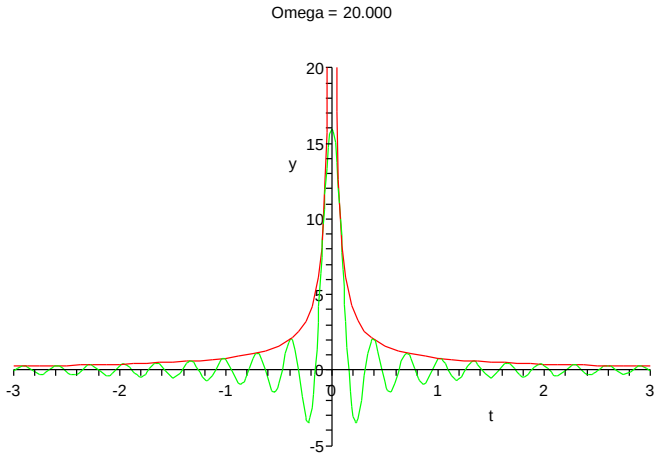
Všimněme si, že Fourierova transformace a její inverze jsou integrální operátory se skoro shodným jádrem $k(\omega, t) = \mathrm{e}^{\pm i\omega t}$.

7.9

7.9. Vlastnosti Fourierovy transformace. Fourierova transformace zajímavým způsobem převrací lokální a globální chování funkcí. Začněme jednoduchým příkladem, ve kterém najdeme funkci $f(t)$, která se ztransformuje na charateristickou 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

$$\begin{aligned} f(t) &= \frac{1}{\sqrt{2\pi}} \int_{-\Omega}^{\Omega} \mathrm{e}^{i\omega t}\, d\omega = \frac{1}{\sqrt{2\pi}} \left[\frac{1}{it}\, \mathrm{e}^{i\omega t}\right]_{-\Omega}^{\Omega} = \frac{2}{\sqrt{2\pi t}} \frac{1}{2i} (\mathrm{e}^{i\Omega t} - \mathrm{e}^{-i\Omega t}) \\ &= \frac{2}{\sqrt{2\pi t}} \sin(\Omega t). \end{aligned}$$

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 zelenou křivkou pro $\Omega = 20$. Zároveň je vynesena červenou křivkou oblast, ve které se s rostoucím Ω naše funkce $f(t)$ stále rychleji „vlní“.



V dalším příkladu spočtěme Fourierovu transformaci derivace $f'(t)$ pro nějakou funkci f. Pro jednoduchost předpokládejme, že f má kompaktní nosič, tj, zejména

$\mathcal{F}(f')$ i $\mathcal{F}(f)$ skutečně existují a počítejme metodou per partes:

$$\begin{aligned}\mathcal{F}(f')(\omega) &= \frac{1}{\sqrt{2\pi}}\int_{\infty}^{\infty} f'(t)\,\mathrm{e}^{-i\omega t}\,dt\\ &= \frac{1}{\sqrt{2\pi}}\left[\mathrm{e}\,-i\omega t f(t)\right]_{-\infty}^{\infty} + \frac{i\omega}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(t)\,\mathrm{e}^{-i\omega t}\,dt\\ &= i\omega\mathcal{F}(f)(\omega)\end{aligned}$$

Vidíme tedy, že Fourierova transformace převádí (infinitesimální) operaci derivování na (algebraickou) operaci prostého násobení proměnnou. Samozřejmě můžeme tento vzorec iterovat, tj.

$$\mathcal{F}(f'')(\omega) = -\omega^2\mathcal{F}(f), \ldots, \mathcal{F}(f^{(n)}) = i^n\omega^n\mathcal{F}(f).$$

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 integrovanání, což je krok, který ověříme teprve v diferenciálním a integrálním počtu později, viz 8.25. V dalším krůčku pak zavedeme substituci $t - x = u$.

$$\begin{aligned}\mathcal{F}(h)(\omega) &= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\left(\int_{-\infty}^{\infty} f(x)g(t-x)\,dx\right)\mathrm{e}^{-i\omega t}\,dt\\ &= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(x)\left(\int_{-\infty}^{\infty} g(t-x)\,\mathrm{e}^{-i\omega t}\,dt\right)dx\\ &= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(x)\left(\int_{-\infty}^{\infty} g(u)\,\mathrm{e}^{-i\omega(u+x)}\,du\right)dx\\ &= \frac{1}{\sqrt{2\pi}}\left(\int_{-\infty}^{\infty} f(x)\,\mathrm{e}^{-i\omega x}\,dx\right)\cdot\left(\int_{-\infty}^{\infty} g(u)\,\mathrm{e}^{-i\omega u)}\,du\right)\\ &= \sqrt{2\pi}\mathcal{F}(f)\cdot\mathcal{F}(g)\end{aligned}$$

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 $\mathcal{F}(g)$. Hovoříme o *dekonvoluci*.

Vraťme se nyní ještě k prvnímu příkladu s inverzní transformací k charakteristické funkci f_Ω intervalu $[-\Omega, \Omega]$. Zkusme provést limitní přechod pro Ω jdoucí k nekonečnu a označme $\sqrt{2\pi}\delta(t)$ kýženou limitní „funkci“ pro $\mathcal{F}^{-1}(f_\Omega)(t)$. Pro součin s libovolným obrazem $\mathcal{F}(g)$ platí

$$\mathcal{F}^{-1}(f_\Omega\cdot\mathcal{F}(g))(z) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} g(t)\mathcal{F}^{-1}(f_\Omega)(z-t)\,dt.$$

Při $\Omega\to\infty$ přejde výraz nalevo k $\mathcal{F}^{-1}(\mathcal{F}(g))(z) = g(z)$, 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* δ 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 δ představit jako jednotkový impulz v jediném bodě. Fourierova transformace jej pak přetransformuje na konstantní funkci $\mathcal{F}(\delta)(\omega) = \frac{1}{\sqrt{2\pi}}$. Naopak mnohé funkce, které nejsou integrovatelné v absolutní hodnotě na $\mathbb{R}$ transformuje Fourierova transformace na výrazy s Diracovým δ. Např.

$$\mathcal{F}(\cos(nt))(\omega) = \sqrt{\frac{\pi}{2}}(\delta(n-\omega) + \delta(n+\omega)).$$

7.10

7.10. Poznámky o dalších transformacích. Pokud použijeme Fourierovu transformaci na lichou funkci $f(t)$, tj. $f(-t) = -f(t)$, příspěvek integrace součinu $f(t)$ a funkce $\cos t$ 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. Vynecháním imaginární jednotky i dostáváme vzájemně inverzní transformace, kterým se říká *Fourierova sinusová transformace* pro liché funkce:

$$\tilde{f}_s(\omega) = \sqrt{\frac{2}{\pi}} \int_0^\infty f(t) \sin \omega t \, dt, \quad f(t) = \sqrt{\frac{2}{\pi}} \int_0^\infty \tilde{f}_s(t) \sin \omega t \, dt.$$

Obdobně se definuje *Fourierova cosinová transformace* pro sudé funkce.

Fourierovu transformaci nelze dobře využít pro funkce, které nejsou integrovatelné v absolutní hodnotě přes celé $\mathbb{R}$ (minimálně nedostáváme opravdové funkce). *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, proto bude existovat $\mathcal{L}(p(t))$ například pro každý polynom p 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.

KAPITOLA 8

Spojité modely s více proměnnými

jedna proměnná nám k modelování nestačí?
– nevadí, stačí vzpomenout na vektory ...

1. Funkce a zobrazení na $\mathbb{R}^n$

8.1

8.1. Funkce a zobrazení. Na počátku našeho putování matematickou krajinou snad čtenáři vstřebali, že s vektory lze počítat velice podobně jako se skaláry, jen je třeba si věci dobře rozmyslet. Zcela obdobně si budeme počínat nyní.

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. Připustíme proto funkce

$$f(x_1, x_2, \ldots, x_n) : \mathbb{R}^n \to \mathbb{R}$$

a budeme se snažit co nejlépe rozšířit naše metody pro sledování změn a hodnot do této situace. Říkáme jim *funkce více proměnných*.

Pro snažší pochopení budeme nejčastěji 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 ta která funkce definována.[1]

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

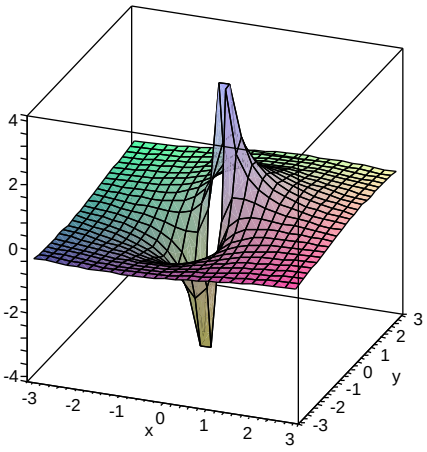
$$G_f = \{(x_1, \ldots, x_n, f(x_1, \ldots, x_n));\ (x_1, \ldots, x_n) \in A\},$$

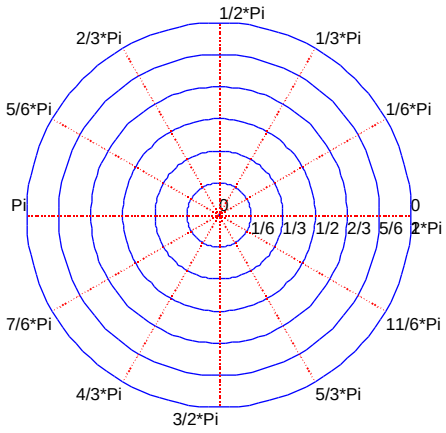
kde A je definiční obor f. Např. grafem funkce definované v rovině vztahem

$$f(x, y) = \frac{x + y}{x^2 + y^2}$$

je docela pěkná plocha na levém obrázku a jejím maximálním definičním oborem jsou všechny body roviny kromě počátku $(0, 0)$.

[1] Častou hříčkou pro písemky a úlohy je naopak úkol pro danou formuli pro funkci najít co největší definiční obor, na kterém má tato formule smysl.





Při definici a zejména při kreslení obrázku grafu jsme používali pevně zvolené *souřadnice* v rovině. Pro pevně zvolené x tak např. dostáváme zobrazení

$$\mathbb{R} \to \mathbb{R}^3,\ y \mapsto (x, y, f(x, y)),$$

tj. *křivku* v prostoru $\mathbb{R}^3$. Na obrázku jsou také čarami vyneseny obrazy takovýchto křivek pro některé pevně zvolené hodnoty souřadnic x a y. Křivky $c : \mathbb{R} \to \mathbb{R}^n$ jsou nejjednoduššími příklady *zobrazení* $F : \mathbb{R}^m \to \mathbb{R}^n$.

Stejně jako u vektorových prostorů, volba našeho „pohledu na věc“, tj. volba souřadnic, může zdánlivě zjednodušit nebo zhoršit naše vnímání studovaného objektu. Změna souřadnic je nyní na místě v daleko obecnější formě než jen u afinních zobrazení v kapitole čtvrté. Opět je ale vhodné na změnu souřadnic pohlížet jako na zobrazení $\mathbb{R}^n \to \mathbb{R}^n$. Velice obvyklý 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 úhlem $\varphi = \arctan(y/x)$ (pokud je $x \neq 0$) mezi spojnicí s počátkem a osou x. 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, φ) v rovině, aby existovalo i zobrazení inverzní. Kartézský obraz přímek v polárních souřadnicích s konstantními souřadnicemi r nebo φ je na obrázku vpravo.

8.2

8.2. Euklidovské prostory. Bude velice užitečné připomenout a rozšířit naše vědomosti o vlastnostech euklidovských afinních prostorů. Začneme připomenutím metrických (topologických) vlastností prostoru $E_n = \mathbb{R}^n$:

Prostor E_n vnímáme jako množinu 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. 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 P obdržíme Q. 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

$$\|P - R\| = \|(P - Q) + (Q - R)\| \leq \|(P - Q)\| + \|(Q - R)\|,$$

viz 4.14(1) (nebo stejnou nerovnost (5.4) pro skaláry). Můžeme proto bez probleému přenést (rozšířit) pro body P_i libovolného Euklidovského prostoru pojmy:

- *Cauchyovská posloupnost* – $\|P_i - P_j\| < \epsilon$, pro každé pevně zvolené $\epsilon > 0$ až na konečně mnoho výjimečných hodnot i, j,
- *konvergentní posloupnost* – $\|P_i - P\| < \epsilon$, pro každé pevně zvolené $\epsilon > 0$ 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 v A konvergující k P a vesměs různých od P,
- *uzavřená množina* – obsahuje všechny své hromadné body,
- *otevřená množina* – její doplněk je uzavřený,
- *otevřené δ–okolí bodu P* – množina $\mathcal{O}_\delta(P) = \{Q \in E_n;\ \|P - Q\| < \delta\}$,
- *hraniční bod P množiny A* – každé δ–okolí bodu P má neprázdný průnik s A i s komplementem $E_n \setminus A$,
- *vnitřní bod P množiny A* – existuje δ–okolí bodu P, které celé leží uvnitř A,
- *ohraničená množina* – leží celá v nějakém δ–okolí některého svého bodu (pro dostatečně velké δ),
- *kompaktní množina* – uzavřená a ohraničená množina.

Čtenář by měl nyní investovat něco málo úsilí do pročtení odstavců 4.14, 5.10 a 5.11 a zkusit si promyslet 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 předchozím 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 5.9 vyplývá, že každá Caychovská posloupnost bodů v E_n je konvergentní.

Stejně jako v případě E_1 definujeme otevřené pokrytí množiny a platí s drobnými formulačními úpravami i Věta 5.11:

Věta. *Pro podmnožiny $A \subset E_n$ v euklidovských prostorech platí:*

(1) *A je otevřená, právě když je sjednocením nejvýše spočetného systému δ–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 každé její otevřené pokrytí obsahuje konečné pokrytí.*

Důkaz z 5.11 lze bez úprav použít v případě tvrzení (1)–(3), byť s novým chápání pojmů a nahrazením „otevřených intervalů“ jejich vícerozměrnými δ–okolími vhodných bodů.

Důkaz pro zbylá dvě tvrzení je však třeba dosti zásadně upravit. Nebudeme se tu zabývat detaily, ambiciózнější čtenáři mohou zkusit samostatně princip ohraničování stále menšími a menšími intervaly modifikovat s použitím δ–okolí.

8.3. Příklady.

8.3.1. *Rozhodněte o následujících podmnožinách v E^3, zda jsou otevřené, uzavřené či kompaktní. Dále určete jejich hraniční a vnitřní body.*

(1) $M = \{(x,0,0) \in \mathbb{R}^3 | x \in (0,1)\}$
(2) $M = \{(x,0,0) \in \mathbb{R}^3 | x \in \langle 0,1\rangle\}$
(3) $M = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2+z^2 \leq 1\}$
(4) $M = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2 \leq 1\}$
(5) $M = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2 = 1\}$
(6) $M = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2-z^2 \leq 1\}$
(7) $M = \{(x,y,z) \in \mathbb{R}^3 | x \in \mathbb{N}\}$

Řešení. *V řešeních budeme ve zkratce uvádět, že množina je např. OU (otevřená i uzavřená, není kompaktní), $\emptyset$ znamená, že nemá žádnou z uvedených vlastností, množinu hraničních bodů budeme značit H, vnitřek množiny jako V.*

(1) $\emptyset$, $H = M$, $V = \emptyset$
(2) UK, $H = M$, $V = \emptyset$
(3) UK, $H = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2+z^2 = 1\}$, $V = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2+z^2 < 1\}$, M je koule
(4) U, $H = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2 = 1\}$, $V = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2 < 1\}$, M je (nekonečný) válec
(5) U, $H = M$, $V = \emptyset$, M je válcová plocha
(6) U, $H = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2-z^2 = 1\}$, $V = \{(x,y,z) \in \mathbb{R}^3 | x^2+y^2-z^2 < 1\}$ je dvojdílný hyperboloid
(7) U, $H = M$, $V = \emptyset$, M je sjednocení nekonečně mnoha rovnoběžných rovin

□

8.3

8.4. Křivky v E_n. Celá naše diskuse kolem limit, derivací a integrálů funkcí v 5. a 6. kapitole pracovala s funkcemi s jednou reálnou proměnnou a reálnými nebo komplexními hodnotami s odůvodněním, že používáme pouze trojúhelníkovou nerovnost platnou pro velikosti reálných i komplexních čísel. Ve skutečnosti se tento argument do značné míry přenáší na jakékoliv funkce jedné reálné proměnné s hodnotami v euklidovském prostoru $E_n = \mathbb{R}^n$.

Pro každou křivku[2], 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:* $\int_a^b c(t)dt \in \mathbb{R}^n$.

V případě integrálu přitom 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.

[2] 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.

U integrálu můžeme také přímo formulovat pro křivky analogii souvislosti Riemannova integrálu a antiderivace (viz 6.14): 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 6.2 a 6.7. Ve zvolených souřadnicích je můžeme aplikovat na jednotlivé souřadné funkce diferencovatelné křivky $c(t) = (c_1(t), \dots, c_n(t))$ 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 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

$$c(b) - c(a) = (x'(\xi)(b-a), y'(\eta)(b-a)) = (b-a) \cdot (x'(\xi), y'(\eta))$$

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 $a \le s \le t \le b$ platí*

$$\|c(t) - c(s)\| \le \sqrt{n} \max_{r\in[a,b]} \|c'(r)\| \cdot |t-s|.$$

Důkaz. Přímým použitím věty o střední hodnotě dostáváme pro vhodné body r_i uvnitř intervalu $[s,t]$:

$$\begin{aligned}
\|c(t) - c(s)\|^2 &= \sum_{i=1}^n (c_i(t) - c_i(s))^2 \le \sum_{i=1}^n (c_i'(r_i)(t-s))^2 \\
&\le (t-s)^2 \sum_{i=1}^n (\max_{r\in[s,t]} |c_i'(r)^2 \\
&\le n(\max_{r\in[s,t],\ i=1,\dots,n} |c_i'(r)|)^2 (t-s)^2 \\
&\le n \max_{r\in[s,t]} \|c'(r)\|^2 (t-s)^2.
\end{aligned}$$

□

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 $c'(t_0) \in \mathbb{R}^n$. Přímka T zadaná parametricky

$$T: \quad c(t_0) + \tau \cdot c'(t_0)$$

se nazývá *tečna ke křivce* c v bodě t_0. Na rozdíl od tečného vektoru, tečna T zjevně nezávisí na parametrizaci křivky c.

8.5. Příklad. Určete parametrické i obecné 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 vyjádření tečny tedy zní:

$$\begin{aligned} x &= c_1'(1)s + c_1(1) = t + 1 \\ y &= c_2'(1)s + c_2(1) = 2t + 1 \\ z &= c_3'(1)s + c_3(1) = 3t + 1. \end{aligned}$$

Vyloučením parametru t dostáváme obecné rovnice tečny (nejsou dány kanonicky):

$$\begin{aligned} 2x - y &= 1 \\ 3x - z &= 2. \end{aligned}$$

□

8.4

8.6. Parciální derivace a diferenciál. 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 $(f \circ c)(t) : \mathbb{R} \to \mathbb{R}$. Za hladké nebo diferencovatelné funkce bychom tedy mohli např. považovat ty, jejichž kompozice se všemi hladkými nebo diferencovatelnými funkcemi jsou opět hladké nebo diferencovatelné. Začneme ale raději s nejjednodušššími křivkami, tj. přímkami.

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.

$$d_v f(x) = \lim_{t \to 0} \frac{1}{t}(f(x + tv) - f(x)).$$

Často se $d_v f$ říká *směrová derivace*. Speciální volbou přímek ve sěru 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 fukci jako operace $\frac{\partial}{\partial x_i}$. Pro funkce v rovině tak dostáváme

$$\begin{aligned} \frac{\partial}{\partial x} f(x, y) &= \lim_{t \to 0} \frac{1}{t}(f(x + t, y) - f(x, y)), \\ \frac{\partial}{\partial y} f(x, y) &= \lim_{t \to 0} \frac{1}{t}(f(x, y + t) - f(x, y)). \end{aligned}$$

Se samotnými parciálními nebo směrovými derivacemi nevystačíme pro dobrou aproximaci chování funkce lineárními výrazy. Podívejme se např. na funkce v rovině dané výrazy

$$g(x, y) = \begin{cases} 1 & \text{když } xy = 0 \\ 0 & \text{jinak} \end{cases}, \quad h(x, y) = \begin{cases} 1 & \text{když } y = x^2 \neq 0 \\ 0 & \text{jinak} \end{cases}.$$

Evidentně žádná z nich neprodlužuje všechny hladké křivky procházející bodem $(0, 0)$ na hladké křivky. Přitom ale pro g existují obě parciální derivace v $(0, 0)$ a jiné směrové derivace neexistují, zatímco pro h existují všechny směrové derivace v bodě $(0, 0)$ a je dokonce $d_v h(0) = 0$ pro všechny směry v, takže jde o lineární závislost na $v \in \mathbb{R}^2$.

Budeme sledovat případ funkcí jedné proměnné co nejdůsledněji a podobné patologické chování vyloučíme přímo definicí:

Definice. Funkce $f : \mathbb{R}^n \to \mathbb{R}$ je *diferencovatelná v bodě* x, jestliže

- v bodě x existují všechny směrové derivace $d_v f(x)$, $v \in \mathbb{R}^n$,
- $d_v f(x)$ je lineární v závislosti na přírůstku v a
- $0 = \lim_{v \to 0} \frac{1}{\|v\|}\big(f(x + v) - f(x) - d_v f(x)\big)$.

Řečeno slovy požadujeme, aby v bodě x existovalo dobré lineární přiblížení přírůstků funkce f lineární funkcí přírůstků proměnných veličin. Lineární výraz $d_v f$ (ve vektorové proměnné v) nazýváme *diferenciál funkce* f vyčíslený na přírůstku v. V literatuře se často také říká *totální diferenciál* df funkce f.

Pro ilustraci se podívejme se, jak se chová diferenciál funkce $f(x,y)$ v rovině za přepokladu, 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 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 dovodíme

$$\begin{aligned}\frac{1}{t}(f(x(t),y(t)) - f(x_0,y_0)) &= \frac{1}{t}\big(f(x(t),y(t)) - f(x(0),y(t)\big) + \\ &\quad + \frac{1}{t}\big(f(x(0),y(t)) - f(x(0),y(0)\big) \\ &= \frac{1}{t}(x(t)-x(0))\cdot\frac{\partial f}{\partial x}(x(\xi),y(t)) + \frac{1}{t}(y(t)-y(0))\cdot\frac{\partial f}{\partial y}(x(0),y(\eta))\end{aligned}$$

pro vhodná čísla ξ a η mezi 0 a t. Limitním přechodem $t \to 0$ pak díky spojitosti parciálních derivací dostáváme

$$\frac{d}{dt}f(x(t),y(t))|_{t=0} = x'(0)\frac{\partial f}{\partial x}(x_0,y_0) + y'(0)\frac{\partial f}{\partial y}(x_0,y_0)$$

což je příjemné rozšíření platnosti věty o derivování složených funkcí. 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

$$d_v f(x_0,y_0) = \frac{\partial f}{\partial x}\xi + \frac{\partial f}{\partial y}\eta$$

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, diferenciál je lineární funkce $\mathbb{R}^n \to \mathbb{R}$ na přírůstcích se souřadnicemi danými právě parciálními derivacemi. Náš výpočet zároveň ukázal, že skutečně tato lineární funkce df má aproximační vlastnosti diferenciálu, kdykoliv parciální derivace jsou spojité v okolí daného bodu.

V případě funkcí více proměnných píšeme obdobně

e8.1 (8.1) $$df = \frac{\partial f}{\partial x_1}dx_1 + \frac{\partial f}{\partial x_2}dx_2 + \cdots + \frac{\partial f}{\partial x_n}dx_n$$

a platí:

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 rovnicí (8.1).*

Důkaz. Odvození věty je naprosto analogické výše uvedenému důkazu v případě $n = 2$. □

8.5

8.7. Tečná rovina ke grafu funkce. Uvažujme libovolnou diferencovatelnou funkci $f : E_n \to \mathbb{R}$. Protože každá směrová derivace je vyčíslena jako derivace funkce jedné proměnné $t \mapsto f(x + tv)$, můžeme i v této souvislosti využít větu o střední hodnotě:

e8.2 (8.2) $$f(x + tv) - f(x) = t \cdot df(x + t_0 v)(v) = t \cdot d_v f(x + t_0 v)$$

pro vhodné t_0 mezi nulou a t. Jinými slovy, přírůstek funkčních hodnot v bodech $x + tv$ a x je vždy vyjádřen pomocí směrové derivace ve vhodném bodě na jejich spojnici.

Pro případ funkce na E_2 a pevně zvoleného bodu $(x_0, y_0) \in E_2$ uvažme rovinu v E_3 zadanou rovnicí

$$\begin{aligned} z &= f(x_0, y_0) + df(x_0, y_0)(x - x_0, y - y_0) \\ &= f(x_0, y_0) + \frac{\partial f}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial f}{\partial y}(x_0, y_0)(y - y_0). \end{aligned}$$

Tato rovina má jako jediná ze všech rovin procházejících bodem (x_0, y_0) vlastnost, že v ní leží derivace a tedy i tečny všech křivek

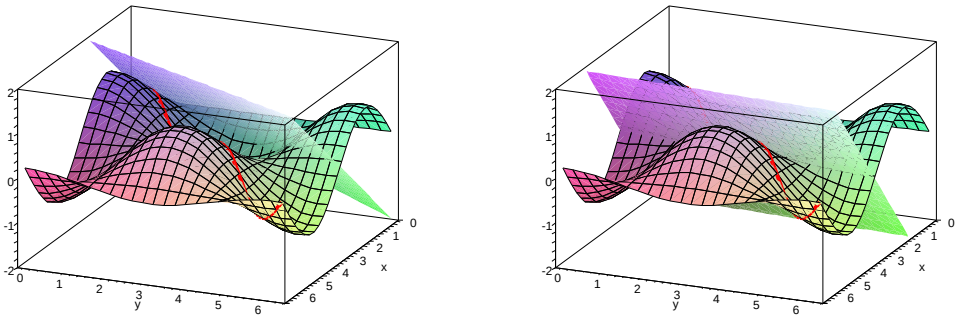
$$c(t) = (x(t), y(t), f(x(t), y(t))).$$

Říkáme jí *tečná rovina* ke grafu funkce f.

Na obrázku jsou zobrazeny dvě tečné roviny ke grafu funkce

$$f(x, y) = \sin(x)\cos(y).$$

Červená čára je obrazem křivky $c(t) = (t, t, f(t, t))$.



Pro funkce n proměnných definujeme tečnou rovinu jako afinní nadrovinu v E_{n+1}. Místo zaplétání se do spousty indexů bude snad užitečná vzpomínka na afinní geometrii: Je to 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 $x \in E_n$. Ještě jinak můžeme také říci, že směrová derivace $d_v f$ je dán přírůstkem na tečné 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 rovnoběžná s nadrovinou proměnných (tj. její zaměření je $E_n \subset E_{n+1}$ s nulovou přidanou souřadnicí pro hodnoty f). To ovšem 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.

8.8. Příklady.

8.8.1. *Určete, 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: $\frac{\partial f(x,y)}{\partial x} = \ln(y)$, $\frac{\partial f(x,y)}{\partial y} = \frac{x}{y}$, jejich hodnoty v bodě $(1, \frac{1}{e})$ jsou -1, e, dále $f(1, \frac{1}{e}) = -1$. Rovnice tečné roviny je tedy

$$\begin{aligned} z &= f\left(1, \frac{1}{e}\right) + \frac{\partial f(x,y)}{\partial x}\left(1, \frac{1}{e}\right)(x+1) + \frac{\partial f(x,y)}{\partial y}\left(1, \frac{1}{e}\right)\left(y - \frac{1}{e}\right) \\ &= -1 - x + ey. \end{aligned}$$

Této rovnici daný bod nevyhovuje, v tečné rovnině tedy neleží. □

8.8.2. *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

$$\begin{aligned} z &= f(2,1) + \frac{\partial f(x,y)}{\partial x}(2,1)(x - x_0) + \frac{\partial f(x,y)}{\partial y}(2,1)(y - y_0) \\ &= 5x + 2y - 12. \end{aligned}$$

Tečná rovina k grafu g je pak

$$\begin{aligned} z &= f(2,1) + \frac{\partial g(x,y)}{\partial x}(2,1)(x - x_0) + \frac{\partial g(x,y)}{\partial y}(2,1)(y - y_0) \\ &= 2y - 2. \end{aligned}$$

Průsečnicí těchto dvou rovin je přímka daná parametricky jako $[2, t, 2t - 2]$, $t \in \mathbb{R}$

Alternativně: 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 $[2, 1 + t, 2t]$, $t \in \mathbb{R}$.

□

8.6

8.9. Derivace vyšších řádů. 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

$$(\frac{\partial}{\partial x_j} \circ \frac{\partial}{\partial x_i})f = \frac{\partial^2}{\partial x_i \partial x_j} f = \frac{\partial^2 f}{\partial x_i \partial x_j}$$

v případě opakované volby $i = j$ píšeme také

$$(\frac{\partial}{\partial x_i} \circ \frac{\partial}{\partial x_i})f = \frac{\partial^2}{\partial x_i^2} f = \frac{\partial^2 f}{\partial x_i^2}.$$

Úplně stejně postupujeme při dalších iteracích a hovoříme o *parciálních derivacích k-tého řádu*

$$\frac{\partial^k f}{\partial x_{i_1} \dots \partial x_{i_k}}.$$

Obecněji můžeme iterovat (u dostatečně diferencovatelných funkcí) také libovolné směrové derivace, např. $d_v \circ d_w f$ pro dva pevné přírůstky $v, w \in \mathbb{R}^n$.

Abychom si vše ukázali v co nejjednodušší formě, budeme opět pracovat chvíli v rovině E_2 za přepokladu 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.

$$f_x = \frac{\partial f}{\partial x},\ f_{xx} = \frac{\partial^2 f}{\partial x^2},\ f_{yx} = \frac{\partial^2 f}{\partial x \partial y},\quad f_{xy} = \frac{\partial^2 f}{\partial y \partial x}.$$

Ukážeme, že ve skutečnosti spolu parciální derivace komutují, tzn. není potřeba dbát na pořadí, ve kterém je provádíme.

Podle předpokladu existuje limita

$$\begin{aligned} f_{xy}(x,y) &= \lim_{t\to 0} \frac{1}{t}\big(f_x(x,y+t) - f_x(x,y)\big) \\ &= \lim_{t\to 0} \frac{1}{t}\left(\lim_{s\to 0} \frac{1}{s}\big(f(x+s,y+t) - f(x,y+t) - f(x+s,y) + f(x,y)\big)\right) \\ &= \lim_{t\to 0} \frac{1}{t^2}\Big(\big(f(x+t,y+t) - f(x,y+t)\big) - \big(f(x+t,y) - f(x,y)\big)\Big) \end{aligned}$$

a 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 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 na t závisí), viz rovnost (8.2) s dosazenou hodnotou přírůstku $v = (0,1)$). Nyní $g_y(x,y) = f_y(x+t,y) - f_y(x,y)$ a proto můžeme psát φ 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 předpoklady 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 tvrzení:

Věta. *Nechť $f : E_n \to \mathbb{R}$ je k-krát diferencovatelná funkce se spojitými parciálními derivacemi až do řádu k včetně v okolí bodu $x \in \mathbb{R}^n$. Pak všechny parciální derivace nezávisí na pořadí derivování.*

DŮKAZ. Důkaz pro druhý řád byl proveden výše pro $n = 2$ a postup v obecném případě se nijak neliší. Formálně můžeme obecný případ u dvou derivací odbýt i tvrzením, že se vždy celá argumentace odehraje ve dvourozměrném afinních podprostoru.

U derivací vyššího řádu lze důkaz dokončit indukcí podle řádu. Skutečně, každé pořadí indexů lze vytvořit záměnami sousedících dvojic. □

Definice. Je-li $f : \mathbb{R}^n \to \mathbb{R}$ libovolná dvakrát diferencovatelná funkce, nazýváme symetrickou matici funkcí

$$Hf(x) = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}(x)\right) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1 \partial x_1}(x) & \dots & \frac{\partial^2 f}{\partial x_1 \partial x_n}(x) \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1}(x) & \dots & \frac{\partial^2 f}{\partial x_n \partial x_n}(x) \end{pmatrix}$$

Hessián funkce f v bodě x.

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 křivku $c(t) = (x(t), y(t)) = (x_0 + \xi t, y_0 + \eta t)$ budou totiž mít funkce jedné proměnné

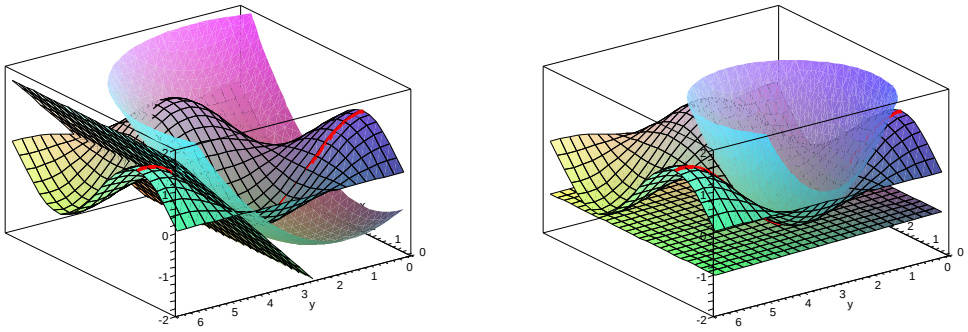
$$\begin{aligned} \alpha(t) &= f(x(t), y(t)) \\ \beta(t) &= f(x_0, y_0) + \frac{\partial f}{\partial x}(x_0, y_0)\xi + \frac{\partial f}{\partial y}(x_0, y_0)\eta \\ &\quad + \frac{1}{2}\left(f_{xx}(x_0, y_0)\xi^2 + 2f_{xy}(x_0, y_0)\xi\eta + f_{yy}(x_0, y_0)\eta^2\right) \end{aligned}$$

stejné derivace do druhého řádu včetně (přepočtěte!). Funkci β přitom můžeme zapsat vektorově jako

$$\beta(t) = f(x_0, y_0) + df(x_0, y_0) \cdot \begin{pmatrix} \xi \\ \eta \end{pmatrix} + \frac{1}{2}(\xi\ \eta) \cdot Hf(x_0, y_0) \cdot \begin{pmatrix} \xi \\ \eta \end{pmatrix}$$

nebo $\beta(t) = f(x_0, y_0) + df(x_0, y_0)(v) + \frac{1}{2}Hf(x_0, y_0)(v, v)$, 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 pro dva různé body a funkci $f(x, y) = \sin(x)\cos(y)$.



8.7

8.10. Taylorova věta. Vícerozměrná verze Taylorovy věty je také příkladem matematického tvrzení, kde složitou částí je nalezení správné formulace. Důkaz je už pak snadný. Budeme postupovat ve výše naznačeném směru a zavedeme si značení pro jednotlivé části $D^k f$ aproximací vyšších řádů. 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 $f : E_n \to \mathbb{R}$, body $x = (x_1, \dots, x_2) \in E_n$ a přírůstky $v = (\xi_1, \dots, \xi_n)$ klademe

$$D^k f(x)(v) = \sum_{1 \le i_1, \dots, i_k \le n} \frac{\partial^k f}{\partial x_{i_1} \dots \partial x_{i_k}}(x_1, \dots, x_n) \cdot \xi_{i_1} \cdots \xi_{i_k}.$$

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

$$D^k f(x,y)(\xi,\eta) = \sum_{\ell=0}^{k} \binom{k}{\ell} \frac{\partial^k f}{\partial x^{k-\ell} \partial y^\ell} \xi^{k-\ell}\eta^\ell.$$

Věta. *Nechť $f : E_n \to \mathbb{R}$ je k–krát diferencovatelná funkce 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 $v \in \mathbb{R}^n$ zvolme křivku $c(t) = x + tv$ 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 6.7)

e8.3 (8.3) $$\varphi(t) = \varphi(0) + \varphi'(0)t + \cdots + \frac{1}{(k-1)!}\varphi^{(k-1)}(0)t^{k-1} + \frac{1}{k!}\varphi^{(k)}(\theta)t^k.$$

Zbývá nám tedy jen ověřit, že postupným derivováním složené funkce φ dostaneme právě požadovaný vztah. To lze snadno provést indukcí přes řád k.

Pro $k = 1$ splývá Taylorova věta se vztahem v rovnosti (8.2). 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 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).

Předpokládejme, že

$$D^\ell f(x)(v) = \sum_{1 \le i_1, \dots, i_\ell \le n} \frac{\partial^\ell f}{\partial x_{i_1} \dots \partial x_{i_\ell}}(x_1(t), \dots, x_n(t)) \cdot x_{i_1}'(t) \cdots x_{i_\ell}'(t)$$

a spočtěme totéž pro $\ell + 1$. Derivování složené funkce dá podle pravidla o derivání součinu (viz Věta 5.23)

$$\frac{d}{dt} D^\ell f(c(t))(c'(t)) = \frac{d}{dt} \sum_{1 \le i_1, \dots, i_\ell \le n} \frac{\partial^\ell f}{\partial x_{i_1} \dots \partial x_{i_\ell}}(x_1(t), \dots, x_n(t)) \cdot x_{i_1}'(t) \cdots x_{i_\ell}'(t)$$

$$= \sum_{1 \le i_1, \dots, i_\ell \le n} \left(\sum_{j=1}^{n} \frac{\partial^{\ell+1} f}{\partial x_{i_1} \dots \partial x_{i_\ell} \partial x_j}(x_1(t), \dots, x_n(t)) \cdot x_j'(t) \cdot x_{i_1}'(t) \cdots x_{i_\ell}'(t) \right) + 0$$

a to skutečně je požadovaný vztah pro řád $\ell + 1$. Taylorova věta nyní vyplývá z vyčíslení v bodě $t = 0$ a dosazení do (8.3). □

8.11. Příklady.

8.11.1. *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 druhý totální diferenciál daný Hessiánem:

$$Hf = \begin{pmatrix} \frac{2y^2 - 2x^2 + 2}{(x^2+y^2+1)^2} & -\frac{4xy}{(x^2+y^2+1)^2} \\ -\frac{4xy}{(x^2+y^2+1)^2} & \frac{2x^2 - 2y^2 + 2}{(x^2+y^2+1)^2} \end{pmatrix}.$$

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 již můžeme napsat Taylorův rozvoj druhého řádu v bodě $[1, 1]$:

$$\begin{aligned} T^2(f)(1,1) &= f(1,1) + f_x(1,1)(x-1) + f_y(1,1)(y-1) + \\ &\quad + \frac{1}{2}(x-1, y-1) Hf(1,1) \begin{pmatrix} x-1 \\ y-1 \end{pmatrix} \\ &= \ln(3) + \frac{2}{3}(x-1) + \frac{2}{3}(y-1) + \frac{1}{9}(x-1)^2 - \\ &\quad - \frac{4}{9}(x-1)(y-1) + \frac{1}{9}(y-1)^2 \\ &= \frac{1}{9}(x^2 + y^2 + 8x + 8y - 4xy - 14) + \ln(3). \end{aligned}$$

□

8.11.2. *Určete Taylorův polynom druhého řádu funkce* $\ln(x^2y)$ *v bodě* $[1,1]$.

Řešení.

$$T^2_{\ln(xy+1)}(1,1) = \ln(2) + \frac{1}{4}(x^2+y^2+xy-x-y-1).$$

□

8.11.3. *Určete Taylorův rozvoj druhého řádu funkce* $f : \mathbb{R}^2 \to \mathbb{R}$,

$$f(x,y) = tan(xy+y)$$

v bodě $(0,0)$.

Řešení.

$$y + xy.$$

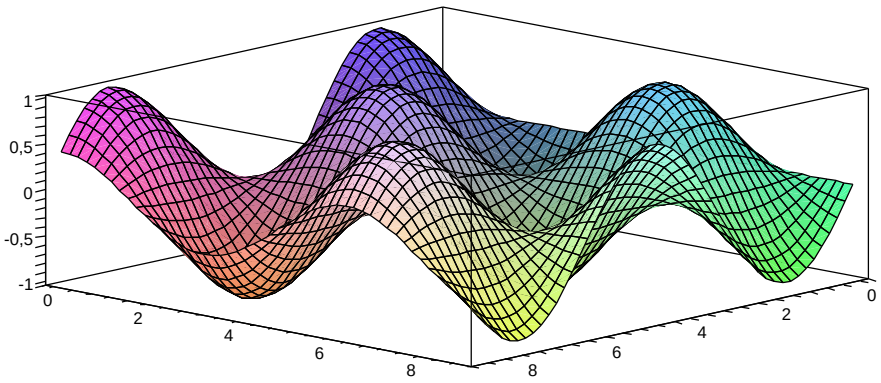
□

8.12. 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 $f(x) \leq f(x_0)$ nebo $f(x) \geq f(x_0)$. 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 je podél přímky $x_0 + tv$ na jednu stranu od bodu x_0 hodnota funkce roste a na druhou klesá, viz (8.2).

Vnitřní bod $x \in E_n$ definičního oboru funkce f, ve kterém je diferenciál $df(x)$ nulový nazýváme *stacionární bod funkce* f.

Budeme opět 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 8.7. Svým tvarem tato funkce připomíná známá kartonová plata na vajíčka, je tedy předem zřejmé, že najdeme řadu extrémů, ale ještě více stacionárních bodů, která ve skutečnosti extrémy nebudou (ta „sedýlka“ viditelná na obrázku).



Spočtěme si tedy první a poté druhé derivace:

$$f_x(x,y) = \cos(x)\cos(y),\ \ f_y(x,y) = -\sin(x)\sin(y),$$

takže obě derivace budou 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 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 ℓ 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 ℓ 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)

$$f(x,y) = f(x_0,y_0) + \frac{1}{2}Hf(x_0 + \theta(x-x_0), y_0 + \theta(y-y_0))(x-x_0, y-y_0),$$

kde Hf nyní vnímáme jako kvadratickou formu vyčíslenou na přírůstku $(x-x_0, y-y_0)$. 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 ℓ. 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 **??**–**??** v kapitole o afinní geometrii. Zavedli jsme tam pro kvadratickou formu $h : E_n \to \mathbb{R}$ 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 $u, v \in V$.

Zavedli jsme také nějaké metody, které umožňují přímo zjistit, zda daná forma má některý z těchto přívlastků.

Způsob našeho předchozího využití Taylorovy věty dokazuje i v obecném případě funkce f více proměnných následující výsledek:

Věta. *Nechť $f : E_n \to \mathbb{R}$ je dvakrát spojitě diferencovatelná funkce a $x \in E_n$ nechť je stacionární bod funkce f. 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.*

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.

8.13. Příklady.

8.13.1. *Určete stacionární body funkce $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^2y + y^2x - xy$ 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 Hf je $\begin{pmatrix} 2y & 2x + 2y - 1 \\ 2x + 2y - 1 & 2x \end{pmatrix}$.

Hodnoty ve stacionárních bodech jsou postupně $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$,

tedy první tři Hessiány jsou indefinitní, poslední pak pozitivně definitní, bod $[1/3, 1/3]$ je tedy lokálním minimem. □

8.13.2. *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. □

8.9

8.14. Zobrazení a transformace. 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 F je *diferencovatelné* nebo *spojitě diferencovatelné zobrazení*, jestliže tuto vlastnost mají všechny funkce $f_1, \dots, f_m$.

Diferenciály $df_i(x)$ jednotlivých funkcí f_i 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

$$D^1F(x) = \begin{pmatrix} df_1(x) \\ df_2(x) \\ \vdots \\ df_m(x) \end{pmatrix} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \dots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \dots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \frac{\partial f_m}{\partial x_2} & \dots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}(x)$$

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

$$\lim_{v \to 0} \frac{1}{\|v\|} \big(F(x + v) - F(x) - D^1F(x)(v)\big) = 0.$$

Přímé použití Věty 8.6 o existenci diferenciálu pro funkce n proměnných na jednotlivé souřadné funkce zobrazení F a sama definice euklidovské vzdálenosti vede k následujícímu tvrzení:

Důsledek. *Nechť $F : E_n \to E_m$ je zobrazení, jehož všechny souřadné funkce mají spojité parciální derivace v okolí bodu $x \in E_n$. Pak existuje diferenciál $D^1F(x)$ zadaný Jacobiho maticí.*

Diferencovatelná zobrazení $F : E_n \to E_n$, která mají inverzní zobrazení $G : E_m \to E_n$ definované na celém svém obrazu, se nazývají *(diferencovatelné) transformace*. Příkladem transformace byl přechod mezi kartézkými a polárními souřadnicemi, který jsme diskutovali hned na začátku této kapito v 8.1.

8.10

8.15. Věta („Chain Rule“)**.** *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 obodu F kompozicí diferenciálů*

$$D^1(G \circ F)(x) = D^1G(F(x)) \circ D^1F(x).$$

Příslušná Jacobiho matice je dána součinem příslušných Jacobiho matic.

Důkaz. V odstavci 8.6 a při důkazu Taylorovy věty jsme odvodili, jak se chová diferencování pro složená zobrazení vzniklá z funkcí a křivek. Tím jsme dokázali speciální případy této věty s $n = r = 1$. Obecný případ se ve prakticky stejným postupem, jen budeme pracovat více s vektory.

Zvolme libovolný pevný přírůstek v a počítejme směrovou derivaci pro kompozici $G \circ F$. Ve skutečnosti to znamená spočíst diferenciál pro jednu ze souřadných funkcí zobrazení G, pišme tedy 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

$$g(F(x+tv)) - g(F(x) = dg(F(x))(F(x+tv) - F(x)) + \alpha(F(x+tv) - F(x))$$

kde α je definovaná na okolí bodu $F(x)$, je spojitá a $\lim_{v\to 0} \frac{1}{\|w\|}\alpha(w) = 0$. Dosazením do rovnosti pro směrovou derivaci dostáváme

$$\begin{aligned} d_v(g \circ F)(x) &= \lim_{t\to 0} \frac{1}{t}\big(dg(F(x))(F(x+tv) - F(x)) + \alpha(F(x+tv) - F(x))\big) \\ &= dg(F(x))\left(\lim_{t\to 0} \frac{1}{t}\Big(F(x+tv) - F(x)\Big)\right) + \lim_{t\to 0} \frac{1}{t}\Big(\alpha(F(x+tv) - F(x))\Big) \\ &= dg(F(x)) \circ D^1F(x)(v) + 0, \end{aligned}$$

kde jsme využili skutečnosti, že lineární zobrazení mezi konečněrozměrnými prostory jsou vždy spojitá a vlastnosti funkce α.

Dokázali jsme tedy tvrzení pro jednotlivé funkce $g_1, \dots, g_r$ zobrazení G. Celá věta nyní vyplývá z toho, jak se násobí matice. □

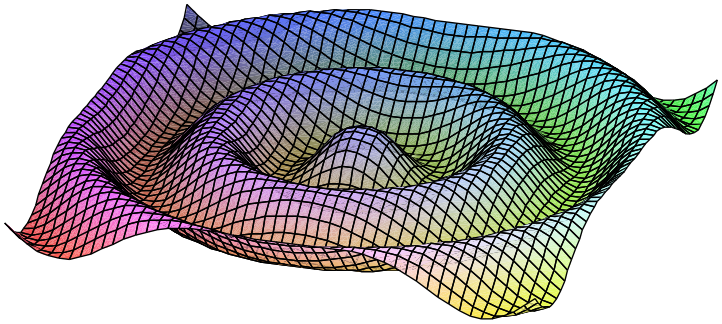
Příklad. Ukažme si na jednoduchém příkladě, jak funguje věta o derivování složených zobrazení. Polární souřadnice vzniknou z kartézských transformací $F : \mathbb{R}^2 \to \mathbb{R}^2$, kterou v souřadnicích (x, y) a (r, φ) zapíšeme takto (samozřejmě jen na vhodném definičním oboru)

$$r = \sqrt{x^2 + y^2},\ \varphi = \arctan \frac{y}{x}.$$

Uvažme funkci $g_t : E_2 \to \mathbb{R}$, která má v polárních souřadnicích vyjádření

$$g(r, \varphi, t) = \sin(\text{r-t})\,.$$

Funkce nám docela dobře přibližuje vlnění povrchu hladiny po bodovém vzruchu v počátku v čase t (časem i uvidíme proč), viz obrázek s hodnotou $t = -\pi/2$.



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

$$\begin{aligned}\frac{\partial g}{\partial y}(x,y,t) &= \frac{\partial g}{\partial r}(r,\varphi)\frac{\partial r}{\partial y}(x,y) + \frac{\partial g}{\partial \varphi}(r,\varphi)\frac{\partial \varphi}{\partial y}(x,y)\\ &= \cos(\sqrt{x^2+y^2}-t)\frac{y}{\sqrt{x^2+y^2}}.\end{aligned}$$

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:

8.11 **8.16. Věta** (O inverzním zobrazení)**.** *Nechť $F : E_n \to E_n$ je spojitě diferencovatelné zobrazení na nějakém okolí bodu $x_0 \in E_n$ a nechť je Jacobiho matice $D^1f(x_0)$ 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 $D^1F(x_0)$, 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

$$\mathrm{id}_{\mathbb{R}^n} = D^1(F^{-1}\circ F)(x_0) = D^1(F^{-1})\circ D^1F(x_0)$$

což ověřuje formuli v závěru věty. Víme proto od začátku, jaký diferenciál pro F^{-1} hledat.

V dalším kroku předpokládejme, že inverzní zobrazení existuje a je spojité a budeme ověřovat existenci diferenciálu. Z diferencovatelnosti F na okolí x_0 vyplývá,

že

$$F(x) - F(x_0) - D^1F(x_0)(x - x_0) = \alpha(x - x_0)$$

s funkcí $\alpha : \mathbb{R}^n \to 0$ splňující $\lim_{v\to 0} \frac{1}{\|v\|}\alpha(v) = 0$. Pro ověření aproximační vlastnosti lineárního zobrazení $(D^1F(x_0))^{-1}$ je třeba spočíst limitu pro $y = F(x)$ jdoucí k $y_0 = F(x_0)$

$$\lim_{y\to y_0} \frac{1}{\|y - y_0\|}\big(F^{-1}(y) - F^{-1}(y_0) - (D^1F(x_0))^{-1}(y - y_0)\big).$$

Dosazením z předchozí rovnosti dostáváme

e8.4

$$\begin{aligned}
&\lim_{y\to y_0} \frac{1}{\|y - y_0\|}\big(x - x_0 - (D^1F(x_0))^{-1}(D^1F(x_0)(x - x_0) + \alpha(x - x_0))\big) \\
&\quad = \lim_{y\to y_0} \frac{-1}{\|y - y_0\|}(D^1F(x_0))^{-1}(\alpha(x - x_0)) \qquad (8.4)\\
&\quad = (D^1F(x_0))^{-1} \lim_{y\to y_0} \frac{-1}{\|y - y_0\|}(\alpha(x - x_0)),
\end{aligned}$$

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.

Všimněme si, že jsme skoro dosáhli úplného úspěchu – limita na konci našeho výrazy je v důsledku vlastností funkce α nulová, pokud jsou velikosti $\|F(x)-F(x_0)\|$ větší než $C\|x - x_0\|$ pro nějakou konstantu C. Zbývá nám tedy už „jen“ dokázat existenci spojitého inverzního zobrazení k F a získat přitom dostatečnou kontrolu nad chováním hodnot 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 dostateme 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 nyní 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 podle našeho odhadu v Lemmatu 8.4 a díky definici euklidovské normy

$$\|K(x) - K(y)\| \le Cn^2\|x - y\|,$$

kde C je ohraničeno maximem přes všechny parciální derivace G na sledovaném okolí. Protože v našem případě je diferenciál K v $x_0 = 0$ nulový, můžeme volbou dostatečně malého okolí U 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. v podobě $\|u\| - \|v\| \le \|u - v\|$, dostáváme

$$\|y - x\| - \|F(x) - F(y)\| \le \|F(x) - F(y) + y - x\| \le \frac{1}{2}\|y - x\|$$

a tedy také

e8.5 (8.5) $$(1-\frac{1}{2})\|x-y\| = \frac{1}{2}\|x-y\| \le \|F(x)-F(y)\|.$$

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 spojité. Konečně, odhad (8.5) také zajišťuje existenci a nulovost limity, kterou jsme v (8.4) potřebovali pro pro aproximační vlastnosti a tudíž existenci diferenciálu F^{-1}.

Zdánlivě jsme tedy již úplně hotoví (s důkazem), to ale není pravda. Abychom skutečně dokončili důkaz, musíme ukázat, že je F zúžené na dostatečně malé okolí nejen vzájemně jednoznačné, ale že také zobrazuje otevřené okolí nuly na otevřené okolí nuly.

Zvolme si δ 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 $y \in \mathcal{O}_a(0)$. 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 (s naším pevně zvoleným bodem y) funkci

$$h(x) = \|F(x) - y\|^2$$

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 $j = 1, \dots, n$ platí

$$\frac{\partial h}{\partial x}(z) = \sum_{i=1}^{n} 2(f_j(z) - y_j)\frac{\partial f_i}{\partial x_i}(z) = 0.$$

Na tento systém rovnic se můžeme dívat jako na systém lineárních rovnic s proměnnými $\xi_j = f_j(z) - y_j$ 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. □

8.12

8.17. Věta o implicitní funkci. Naším dalším cílem je využít větu o inverzním zobrazení pro práci s implicitně definovanými funkcemi.

Uvažujme spojitě diferencovatelné zobrazení $F(x, y)$ definované v 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 (a,b) splňující rovnici kružnice a takový, že $b \neq t$ (to jsou totiž krajní body kružnice ve směru souřadnice x), najít okolí bodu a, na kterém bude buď $y = f(x) = t + \sqrt{(x-s)^2 - r}$ nebo $y = f(x) = t - \sqrt{(x-s)^2 - r}$.

Při načrtnutí obrázku je důvod zřejmý – nemůžeme chtít pomocí funkce $y = f(x)$ postihnout horní i dolní půlkružnici zároveň. Zajímavější jsou krajní body intervalu $[t-r, t+r]$. 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 derivace 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 $f'(x) = -F_x/F_y$. Dokážeme, že ve skutečnosti toto tvrzení platí vždy. Poslední tvrzení o derivaci přitom je dobře zapamatovalné (a při pečlivém vnímání věcí i pochopitelné) z výrazu pro diferenciál $dy = f'(x)dx$ a tedy:

$$0 = dF = F_x dx + F_y dy = (F_x + F_y f'(x))dx.$$

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

$$0 = F(x,y,z) = z - x^2 - y^2.$$

Než sformulujeme 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.

Viděli jsme 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 spojitě diferencovatelné zobrazení

$$F = (f_1, \ldots, f_n) : \mathbb{R}^{m+n} \to \mathbb{R}^n.$$

Jacobiho matice tohoto zobrazení bude mít n řádků a $m+n$ sloupců a můžeme si ji symbolicky zapsat jako

$$D^1F = (D^1_xF, D^1_yF) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_m} & \frac{\partial f_1}{\partial x_{m+1}} & \cdots & \frac{\partial f_1}{\partial x_{m+n}} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_m} & \frac{\partial f_n}{\partial x_{m+1}} & \cdots & \frac{\partial f_n}{\partial x_{m+n}} \end{pmatrix},$$

kde $(x_1, \ldots, x_{m+n}) \in \mathbb{R}^{m+n}$ 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_y byla invertibilní.

Věta. *Nechť $F : \mathbb{R}^{m+n} \to \mathbb{R}^n$ je spojitě diferencovatelné zobrazení 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 spojitě 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. Rozšíříme funkci F na

$$\tilde{F} : \mathbb{R}^2 \to \mathbb{R}^2, \quad (x, y) \mapsto (x, F(x, y)).$$

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. Vezměme tedy jednoznačně definované a spojitě 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 spojitě 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 2.22)

$$\begin{pmatrix} 1 & 0 \\ F_x(x, y) & F_y(x, y) \end{pmatrix}^{-1} = (F_y(x, y))^{-1} \begin{pmatrix} F_y(x, y) & 0 \\ -F_x(x, y) & 1 \end{pmatrix}.$$

Dle definice $f(x) = \pi\tilde{F}^{-1}(x,0)$ nás z této matice zajímá první položka na druhém řádku, která je právě Jakobiho 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 žádnou z uvedených formulí, 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 2.22. Snadnější je nechat se přímo inspirovat případem v dimenzi $m+n=2$, označit si matici

$$(D^1\tilde{F}^{-1}) = \begin{pmatrix} \mathrm{id}_{\mathbb{R}^m} & 0 \\ D^1_x F(x,y) & D^1_y F(x,y) \end{pmatrix}^{-1} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

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:

$$\begin{pmatrix} \mathrm{id}_{\mathbb{R}^m} & 0 \\ D^1_x F(x,y) & D^1_y F(x,y) \end{pmatrix} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} \mathrm{id}_{\mathbb{R}^m} & 0 \\ 0 & \mathrm{id}_{\mathbb{R}^n} \end{pmatrix}.$$

Zjevně odtud plyne $A = \mathrm{id}_{\mathbb{R}^m}$, $B = 0$, $D = (D^1_y F)^{-1}$ a konečně $D^1_x F + D^1_y F \cdot C = 0$. Z poslední rovnosti pak dostáváme požadovaný vztah

$$D^1 G = C = -(D^1_y F)^{-1} \cdot D^1_x F.$$

Tím je věta dokázána. □

8.18. Příklad. Buď dáno zobrazení $F : \mathbb{R}^2 \to \mathbb{R}$, $F(x,y) = xy \sin\left(\frac{\pi}{2}xy^2\right)$. Ukažte, že rovnost $F(x,y) = 1$ zadává v nějakém okolí U bodu 1 implicitně funkci $f : U \to \mathbb{R}$, tak že $F(x,f(x)) = 1$ pro $x \in U$. Navíc $f(1) = 1$. Určtete $f'(1)$.

Řešení. $F_y(1,1) = x\sin\left(\frac{\pi}{2}xy^2\right) + \pi x^2 y^2 \cos\left(\frac{\pi}{2}xy^2\right)(1,1) = 1$, tedy předpis $F(x,y) = 1$ zadává implicitně na okolí bodu $(1,1)$ funkci $f : \mathbb{R} \to \mathbb{R}$. Pro její derivaci potom platí

$$f'(x) = -\frac{F_x}{F_y}(1,1) = -\frac{1}{1} = -1.$$

□

8.13

8.19. Gradient funkce. Jak jsme viděli v minulém odstavci, je-li F spojitě diferencovatelná funkce n proměnných, zadává předpis $F(x_1,\dots,x_n) = b$ 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

$$D^1 F = \left(\frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}\right)$$

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 $\operatorname{grad} F$.

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 $v = (v_1, \dots, v_n) \in \mathbb{R}^n$ 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 φ je odchylka vektoru v od gradientu F, viz pojednání o odchylkách vektorů a přímek ve čtvrté kapitole (definice 4.17). 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.

Je tedy zřejmé, že tečná rovina k neprázdné úrovňové množině M_b v okolí jejího bodu s nenulovým gradientem $D^1 F$ je určena ortogonálním doplňkem ke gradientu a samotný gradient je tzv. *normálovým vektorem* nadplochy M_b.

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:

Věta. *Pro funkci F n proměnných a bod $P = (a_1, \dots, a_n) \in M_b$ v jehož okolí je M_b grafem funkce $(n-1)$ proměnných je implicitní rovnice pro tečnou nadrovinu*

$$0 = \frac{\partial f}{\partial x_1}(P) \cdot (x_1 - a_1) + \cdots + \frac{\partial f}{\partial x_n}(P) \cdot (x_n - a_n).$$

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 $\operatorname{grad} F$). Zvolený bod P přitom naší rovnici zjevně vyhovuje. □

Příklad. Uvažujme model osvětlení 3D objektu, kde známe směr v dopadu světla na 2D povrch, tj. množinu M zadanou implicitně rovnicí $F(x, y, z) = 0$. Intenzitu osvětlení bodu $P \in M$ pak definujme jako $I \cos\varphi$, kde φ je úhel mezi normálou zadanou gradientem a vektorem opačným ke směru světla. Znaménko našeho výrazu pak bude označovat, kterou stranu plochy osvětlujeme.

Např. směr osvětlení o intezitě I_0 může být $v = (1, 1, -1)$ (tj. „šikmo dolů“) a objektem může být třeba koule (tj. $F(x, y, z) = x^2 + y^2 + z^2 - 1$). Pro 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.

8.14

8.20. Tečny a normály k implicitně definovaným plochám. Přejděme nyní k obecným dimenzím. Máme-li zobrazení $F : \mathbb{R}^{m+n} \to \mathbb{R}^n$, tj. n rovnic

$$f_i(x_1, \dots, x_{m+n}) = b_i, \quad i = 1, \dots, n,$$

pak za podmínek věty o implicitní funkci je množina všech řešení $(x_1, \dots, x_{m+n})$ 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 a normálové směry. Je-li proto 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,

$$D^1F = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_{m+n}} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_{m+n}} \end{pmatrix}$$

potom bude afinní podprostor v $\mathbb{R}^{m+n}$ obsahující právě všechny tečny bodem P dán rovnicemi:

$$\begin{aligned} 0 &= \frac{\partial f_1}{\partial x_1}(P) \cdot (x_1 - a_1) + \cdots + \frac{\partial f_1}{\partial x_n}(P) \cdot (x_{m+n} - a_{m+n}) \\ &\vdots \\ 0 &= \frac{\partial f_n}{\partial x_1}(P) \cdot (x_1 - a_1) + \cdots + \frac{\partial f_n}{\partial x_n}(P) \cdot (x_{m+n} - a_{m+n}). \end{aligned}$$

Tento podprostor se nazývá *tečný prostor* k (implicitně zadané) ploše M v bodě P. *Normálový prostor* v bodě P je afinní podprostor generovaný bodem P a gradienty všech funkcí $f_1, \dots, f_n$ v bodě P, tj. řádky Jacobiho matice D^1F.

Jako jednoduchý příklad si spočtěme tečnu a normálový prostor ke kuželosečce v $\mathbb{R}^3$. Uvažujme rovnici

$$0 = f(x, y, z) = z - \sqrt{x^2 + y^2}$$

kuželu s vrcholem v počátku 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

$$\begin{aligned} 0 &= -\frac{1}{2\sqrt{x^2 + y^2}} 2x \Big|_{x=1,y=0} \cdot (x - 1) - \frac{1}{2\sqrt{x^2 + y^2}} 2y \Big|_{x=1,y=0} \cdot y + 1 \cdot (z - 1) \\ &= -x + z \\ 0 &= -2(x - 1) + y + (z - 1) = -2x + y + z + 1 \end{aligned}$$

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 τ a σ.

8.15

8.21. 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 spojitě diferencovatelné funkce h na množině bodů M zadaných implicitně rovnicí $F(x_1, \dots, x_{m+n}) = 0$. K tomu můžeme použít tytéž postupy jako dříve.

Pokud je M ve všech svých bodech grafem hladkého zobrazení v m proměnných, musí být každý extrém $P \in M$ stacionárním bodem, tj. 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 (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, kterému se říká *metoda Lagrangeových multiplikátorů*:

Věta. *Nechť $F = (f_1, \dots, f_n) : \mathbb{R}^{m+n} \to \mathbb{R}^n$ je spojitě diferencovatelná v okolí bodu P, $F(P) = 0$ a 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 $h : \mathbb{R}^{m+n} \to \mathbb{R}$ 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 počtu neznámých a rovnic v tomto algoritmu: 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, ale navíc také n parametrů λ_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 $n + m$ rovnic pro $n + m$ proměnných a proto lze očekávat, že řešením bude diskrétní množina bodů P (tj. každý z nich bude izolovaným bodem).

8.22. Příklady.

8.22.1. *Zkusme nějaký explicitní příklad. Za množinu S zvolme opět jednotkovou sféru v $\mathbb{R}^3$ a K bude kružnice $K \subset S$ vzniklá průnikem této sféry s rovinou zadanou rovnicí $x + y + z = 0$. Budeme hledat extrémní hodnoty funkce*

$$h(x, y, z) = x^3 + y^3 + z^3$$

na objektech zadaných implicitně pomocí buď jen funkce F nebo dvojice funkcí F a G, které jsou definovány výrazy

$$F(x, y, z) = x^2 + y^2 + z^2 - 1, \quad G(x, y, z) = x + y + z.$$

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 v Maplu).

Řešením systému (ať už rukou nebo opět v Maplu) obdržíme ve skutečnosti spoustu stacionárních bodů. Kromě šesti, o kterých už víme (dvě souřadnice nulové a jedna ± 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 η coby koeficient u jejího 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. □

8.22.2. *Určete, zda existují maxima a minima funkce* $f : (\mathbb{R}^+)^n \to \mathbb{R}$, $f(x_1, \dots, x_n) = \sqrt[n]{x_1 \cdots x_n}$ *za podmínky* $x_1 + \cdots + x_n = c$, $c \in \mathbb{R}^+$, $x_1 > 0, \dots, x_n > 0$.

Řešení. Normálový vektor k nadrovině definované podmínkou je $(1, \dots, 1)$. Extrém může nastat v bodech, kdy je gradient zkoumané funkce násobkem normály. Pro tyto body tedy dostáváme soustavu

$$\frac{1}{n}\sqrt[n]{x_1 \cdots \hat{x}_i \cdots x_n}\,\frac{1}{\sqrt[n]{x_i^{n-1}}} = k, \quad i = 1, \dots n.$$

Tato soustava má na zkoumané množině jediné řešení $x_1 = \cdots = x_n$, $k = 1$, což odpovídá maximu dané funkce. Pokud bychom totiž v omezení uvažovali x_i nezáporná, jednalo by se o kompaktní množinu, tedy daná funkce by na ní měla

jak maximum, tak minimum. Minimum (nula) by nastávalo, pokud by libovolná z proměnných byla nulová, v nalezeném bodě tedy musí nastat maximum. □

Poznamenejme, že předchozí příklad je důkazem známé AG nerovnosti. Pro n reálných čísel x_1, x_2,...,x_n definujeme jejich *aritmetický průměr* jako číslo

$$\mathcal{A}(x_1,\dots,x_n)=\frac{x_1+\cdots+x_n}{n}.$$

Geometrický průměr nezáporných reálných čísel $x_1,\dots,x_n$ pak definujeme jako číslo

$$\mathcal{G}(x_1,\dots,x_n)=\sqrt[n]{x_1\cdots x_n}.$$

Zmíněná nerovnost pak praví, že pro nezáporná reálná čísla $x_1,\dots,x_n$ platí

$$\mathcal{A}(x_1,\dots,x_n)\geq\mathcal{G}(x_1,\dots,x_n),$$

přičemž rovnost nastává právě pro $x_1=\cdots=x_n$.

8.22.3. *Rozhodněte, zda funkce $f:\mathbb{R}^3\to\mathbb{R}$, $f(x,y,z)=x^2y$ 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 $\mathbb{R}^n$ – musí na něm daná funkce nabývat jak minima, tak maxima. Navíc, protože vazební podmínka je dána spojitě diferencovatelnou funkcí a zkoumaná funce 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. □

8.22.4. *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 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. □

8.22.5. *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 $-\frac{1}{3\sqrt{3kl}}$. □

8.22.6. *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* $x \in \langle -1, 2 \rangle$. *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 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.

Jiné řešení. Z rovnic úsečky vyjádříme proměnné y a z pomocí proměnné x: $y = \frac{2}{3} - x$, $z = \frac{1}{3} - x$ a dosadíme do vyšetřované funkce: $27f(x,y,z) = 27f(x) = -27x^3 + 45x^2 - 24x + 4$ a vyšetříme extrémy funkce jedné proměnné: $f'(x) = -27x^2 + 30x - 8$, $f'(x) = 0$ pro $x = \frac{2}{3}$ nebo $x = \frac{4}{9}$ a porovnáme hodnoty funkce v těchto bodech s hodnotami v krajních bodech úsečky a dospějeme ke stejnému závěru jako výše. □

8.22.7. *Rozhodněte, zda existují extrémy funkce $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x,y,z) = x^2 + y^2 + z^2$, na přímce $x + y - z = 1$, $x - y + z = 0$. Pokud extrémy existují, určete je.*

Řešení. Pro stacionární body sestavíme soustavu:

$$\begin{aligned} 2x &= l + k \\ 2y &= l - k \\ 2z &= k - l \end{aligned}$$

Jejím jediným řešením je bod $(\frac{1}{2}, \frac{1}{4}, -\frac{1}{4})$. Vzhledem k tomu, že funkce f roste nade všechny meze na dané přímce jak pro $t \to \infty$, tak pro $t \to -\infty$, musí se jednat o globální minimum funkce (lze spočítat i Hessián Lagrangeovy funkce). Maximum daná funkce na zadaném objektu nemá.

Obdobně jako v předchozím příkladu jsme mohli úlohu převést na hledání extrémů funkce jedné proměnné. □

2. Integrování podruhé

Nyní se vrátíme k procesu integrování, který jsme částečně popsali v druhé části šesté kapitoly. Nepůjdeme do detailů a budeme se soutředit na rozšíření tohoto procesu pro veličiny závislé na více proměnných, případně závislé na parametrech.

8.16

8.23. Integrály závislé na parametrech. Jestliže integrujeme podle jedné proměnné x funkci $n+1$ proměnných $f(x, y_1, \dots, y_n)$, potom výsledek bude funkcí $F(y_1, \dots, y_n)$ v 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 následující věta to skutečně pro dosti širokou třídu funkcí potvrzuje:

Věta. *Pro spojitě diferencovatelnou funkci $f(x, y_1, \dots, y_n)$ definovanou pro x z konečného intervalu $[a, b]$ a na nějakém okolí bodu $c = (c_1, \dots, c_n) \in \mathbb{R}^n$ uvažujme integrál*

$$F(y_1, \dots, y_n) = \int_a^b f(x, y_1, \dots, y_n) dx.$$

Potom platí pro všechny indexy $j = 1, \dots, n$

$$\frac{\partial F}{\partial y_j}(c) = \int_a^b \frac{\partial f}{\partial y_j}(x, c_1, \dots, c_n) dx$$

Důkaz. Pro ověření našeho vztahu je třeba vzpomenout definici Riemannova integrálu. Ta vyčísluje pro libovolnou spojitou funkci jeho hodnotu pomocí aproximací konečnými součty (ekvivalentně horními, dolními nebo Riemannovými součty s libovolnými reprezentanty, viz odstavec 6.14 v šesté kapitole). Je zřejmé, že při důkazu je třeba brát v úvahu pouze souřadnici y_j parametrů (ostatní jsou prostě konstantní pro všechny naše úvahy), proto si technicky formulace zjednodušíme, když se rovnou omezíme na případ $n = 1$ a tedy $y = (y_1)$.

Zvolme proto nějaké dělení Ξ intervalu $[a, b]$ a jeho reprezentanty ξ_i a zkoumejme jednotlivé sčítance Riemannova součtu $S_{\Xi,\xi}$ pro integrál derivované funkce f. S využitím věty o střední hodnotě dostáváme pro každý malý přírůstek h parametru $c = (c_1)$:

$$f(\xi_i, c + h) - f(\xi_i, c) = h \frac{\partial f}{\partial y}(\xi_i, y)$$

s hodnotou $y \in [c, c + h]$. Díky předpokládané spojitosti parciálních derivací a při známé normě dělení Ξ lze proto odhadnout odchylku sčítance

$$\frac{\partial f}{\partial y}(\xi_i, c)(x_{i+1} - x_i)$$

v Riemannově součtu od výrazu v příslušné aproximaci Riemannovými součty pro derivaci integrálu

$$\frac{1}{h}(F(c + h) - F(c)) \simeq \sum_i \frac{1}{h}(f(\xi_i, c + h) - f(\xi_i, c))(x_{i+1} - x_i).$$

V limitě pro $h \to 0$ se tedy blížíme právě požadovanému tvrzení. Potřebujeme již pouze ověřit, že chybu v tomto odhadu budeme umět odhadnout pouze v závislosti na h, stejnoměrně přes celý interval přes který integrujeme.

Při důkazu existence Riemannova integrálu pro spojité funkce jsme dokazovali, že funkce spojitá na konečném intervalu je ve skutečnosti stejnoměrně spojitá, tj. rozdíly hodnot umíme kontrolovat podél celého intervalu stejnoměrně ohraničením vzdálenosti nezávisle proměnné. Jestliže se podíváme na tuto argumentaci pozorněji, zjistíme, že podstanou vlastností intervalu byla pouze jeho kompaktnost. Proto platí, že i funkce více proměnných spojité na kompaktním intervalu jsou zde spojité stejnoměrně.

Odtud vyplývá, že pro zvolenou malou mez δ pro vzdálenost $|y-c| \leq \delta$ máme k dispozici univerzální odhad $|\frac{\partial f}{\partial y}(\xi_i, y) - \frac{\partial f}{\partial y}(\xi_i, c)| \leq \epsilon(\delta)$ a $\epsilon(\delta) \to 0$ při $\delta \to 0$. V našem přiblížení Riemannovými součty můžeme proto přímo nahradit diferenci parciální derivací, aniž bychom chybu zvětšili o více než $\epsilon(\delta)$. Tím je důkaz ukončen. □

Předchozí věta má četná využití. Např. ji můžeme ocenit při zkoumání integrálních transformací, kterým jsme se věnovali v druhé části předchozí kapitoly sedmé. Derivacemi známých výsledků tak dostaneme v řadě případů snadno transformace derivací původně transformovaných funkcí.

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.

8.17

8.24. Integrace funkcí více proměnných. Tak jak jsme motivovali integrování představou o výpočtu plochy pod grafem funkce jedné proměnné, můžeme prakticky stejně postupovat u objemu části trojrozměrného prostoru pod grafem funkce $z = f(x, y)$ dvou proměnných. Místo výběru malých intervalů $[x_i, x_{i+1}]$ dělících celý interval, přes který integrujeme, a přiblížením příslušné části objemu ploškou obdélníku s výškou danou hodnotou funkce f v reprezentantu tohoto intervalu ξ, tj. výrazem

$$f(\xi)(x_{i+1} - x_i),$$

budeme pracovat s děleními v obou proměnných 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 S, 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 S jiná ohraničená množina v $\mathbb{R}^2$, pracujeme místo ní s dostatečně velikou oblastní $[a, b] \times [c, d]$, ale upravíme naši funkci tak, že $f(x, y) = 0$ pro všechny body mimo S. Pro naši kouli bychom tedy integrovali na množině $S = [-1, 1] \times [-1, 1]$ 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 6.13. Můžeme tak přitom činit pro libovolný konečný počet proměnných. Integrál existuje, jestliže pro každou volbu posloupnosti dělení Ξ (nyní ve všech proměnných

zároveň) a reprezentantů jednotlivých krychliček

$$\xi_i \in [x_i, x_{i+1}] \times \ldots \times [z_j, z_{j+1}] \subset \mathbb{R}^n,$$

s maximální velikostí mezi všemi použitými intervaly jdoucí k nule, budou integrální součty (všimněme si, že potřebujeme tolik indexů pro označování subintervalů, kolik máme souřadnic)

$$S_{\Xi,\xi} = \sum_{i,\ldots,j} f(\xi_{i,\ldots,j})(x_{i+1} - x_i) \ldots (z_{j+1} - z_j).$$

konvergovat k jedné hodnotě, kterou zapisujeme

$$\int_S f(x, \ldots, z)\, dx \ldots dz$$

Pro všechny spojité funkce f opět lze dokázat existenci Riemannova integrálu a tento výsledek lze snadno rozšířit pro „dostatečně spojité“ funkce na „dostatečně rozumných“ oborech integrace.

Omezenou množinu $S \subset \mathbb{R}^n$ označujeme za *Riemannovsky měřitelnou*, jestliže je její charakteristická funkce, definovaná $\chi(x_1, \ldots, x_n) = 1$ pro $(x_1, \ldots, x_n) \in S$ a $\chi(x_1, \ldots, x_n) = 0$ pro všechny ostatní body v $\mathbb{R}^n$, Riemannovsky integrovatelná.

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 6.13):

Věta. *Množina Riemannovsky integrovatelných funkcí na vícerozměrném intervalu $S \subset \mathbb{R}^n$ je vektorovým prostorem 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. Doporučujeme promyslet samostatně podrobnosti. □

První část věty lze zapsat obvyklou formulí říkající, že integrace lineární kombinace (nad skaláry v $\mathbb{R}$) integrovatelných funkcí $f_i : \mathbb{R}^n \to \mathbb{R}$, $i = 1, \ldots, k$, je vždy možná a spočte se takto:

$$\begin{aligned}\int_S &(a_1 f_1(x_1, \ldots, x_n) + \cdots + a_k f_k(x_1, \ldots, x_n))\, dx_1 \ldots dx_n \\ &= a_1 \int_S f_1(x_1, \ldots, x_n)\, dx_1 \ldots dx_n + \cdots + a_k \int_S f_k(x_1, \ldots, x_n)\, dx_1 \ldots dx_n.\end{aligned}$$

Druhá část pak říká že pro disjukntní Riemannovsky měřitelné množiny S_1 a S_2 a na obou těchto množinách integrovatelnou funkci $f : \mathbb{R}^n \to \mathbb{R}$ platí

$$\begin{aligned}\int_{S_1 \cup S_2} &f(x_1, \ldots, x_n)\, dx_1 \ldots dx_n \\ &= \int_{S_1} f(x_1, \ldots, x_n)\, dx_1 \ldots dx_n + \int_{S_2} f(x_1, \ldots, x_n)\, dx_1 \ldots dx_n.\end{aligned}$$

8.18

8.25. Násobné integrály. Riemannovsky integrovatelné množiny zejména zahrnují případy, kdy lze S definovat pomocí spojité funkční závislosti souřadnic hraničních bodů tak, že pro danou první souřadnici x umíme zadat dvěmi 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 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 objevovat i mezích pro integraci)

Věta. *Nechť S je ohraničená množina zadaná jako výše a f je spojitá funkce na S. Pak je Riemannův integrál funkce f přes množinu S vyčíslen formulí*

$$\int_S f(x_1, x_2, \dots, x_n) dx \dots dz$$
$$= \int_a^b \left(\int_{\varphi(x_1)}^{\psi(x_1)} \dots \left(\int_{\eta(x,y,\dots)}^{\zeta(x,y,\dots)} f(x_1, x_2, \dots, x_n)\, dx_n \right) \dots dx_2 \right) dx_1$$

Důkaz. Výsledek vyplývá docela snadno přímo z definice Riemannova integrálu pomocí konečných součtů. Stačí si pečlivě hlídat vhodné poskládání jednotlivých sčítanců konečných součtů tak, aby vycházely postupně přiblížení integrálů ve vnitřních závorkách. Díky stejnoměrné spojitosti □

Důsledek. *Pro vícerozměrný interval $S = [a_1, b_1] \times [a_2, b_2] \times \dots \times [a_n, b_n]$ a spojitou funkci $f(x_1, \dots, x_n)$ na S je násobný integrál*

$$\int_S f(x_1, \dots, x_n)\, dx_1 \dots dx_n = \int_{a_1}^{b_1} \int_{a_2}^{b_2} \dots \int_{a_n}^{b_n} f(x_1, \dots, x_n)\, dx_1 \dots dx_n$$

nezávislý na pořadí ve kterém postupně integraci provádíme.

Důkaz. V předchozí větě je v případě vícerozměrného intervalu S kterékoliv pořadí integrace vyjádřením oblasti S v požadovaném tvaru. Na výsledku integrálu tak pořadí integrace nemůže mít vliv. □

Tento důsledek jsme už jednou dříve využili při studiu vztahu Fourierových transformací a konvolucí, viz odstavec 7.9.

8.26. Změna souřadnic při integraci. Při výpočtu integrálů funkcí jedné proměnné jsme používali transformace souřadnic jako mimořádně silný nástroj. Zkusme proto závěrem naší diskuse o integrování naznačit, jak lze transformace souřadnic používat pro integrály funkcí více proměnných.

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 proužíváme pro Riemannovy integrály přiblížení, které bere objem (plochu) malého vícerozměrného intervalu a násobí tuto hodnotou funkce v reprezentujícím bodě. Pokud použijeme transformaci souřadnic, dostaneme nejen hodnotu funkce v reprezentujícím bodě v novém souřadném 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 4.25).

Věta. *Nechť $G(t_1, \dots, t_n) : \mathbb{R}^n \to \mathbb{R}^n$, $(x_1, \dots, x_n) = G(t_1, \dots, t_n)$, je spojitě diferencovatelné zobrazení, $S = G(T)$ a T jsou Riemannovsky měřitelné množiny a $f : S \to \mathbb{R}$ spojitá funkce. Potom platí*

$$\int_S f(x_1, \dots, x_n)dx_1 \dots x_n = \int_T f(G(t_1, \dots, t_n))|\det(D^1G(t_1, \dots, t_n))|dt_1 \dots dt_n.$$

Důkaz. Podrobný formální důkaz nebudeme prezentovat, je však přímočarou realizací výše uvedené úvahy ve spojení s definicí Riemannova integrálu. □

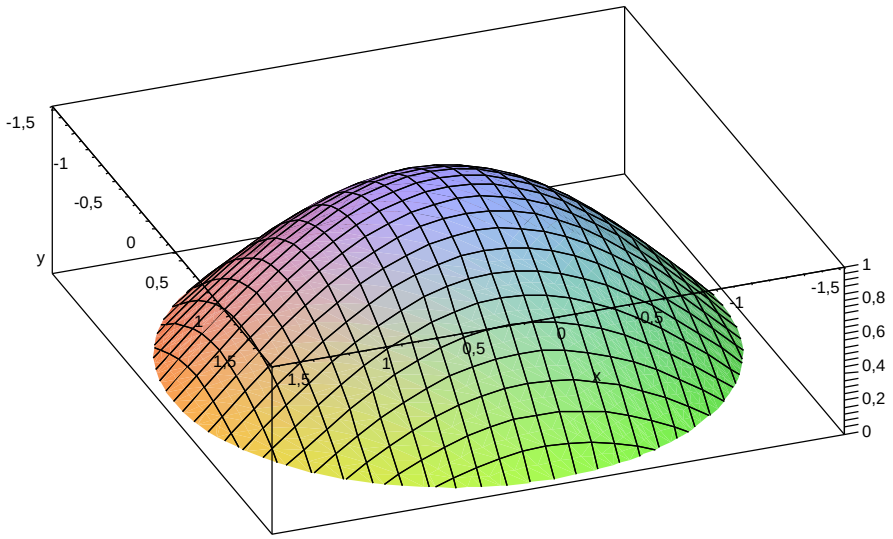
Abychom si přiblížili obsah tvrzení poslední věty, uvedeme jeho speciální případ pro integrál funkce $f(x, y)$ ve dvou proměnných a transformaci

$$G(s, t) = (g(s, t), h(s, t)).$$

Dostáváme

$$\int_{G(T)} f(x, y)dxdy = \int_T f(g(s, t), h(s, t)) \left|\frac{\partial g}{\partial s}\frac{\partial h}{\partial t} - \frac{\partial g}{\partial t}\frac{\partial h}{\partial s}\right| dsdt.$$

Úplně konkrétně, zkusme spočíst integrál z charakteristické funkce kružnice o poloměru R (tj. její plochu) 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).



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:

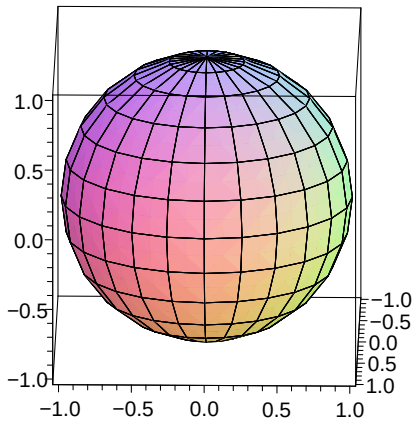
$$\int_S dxdy = \int_0^{2\pi}\int_0^R r dr\, d\theta = \int_0^R 2\pi r dr = \pi R^2.$$

Integrace funkce f proběhne s využitím násobného integrování a integrace per partés obdobně:

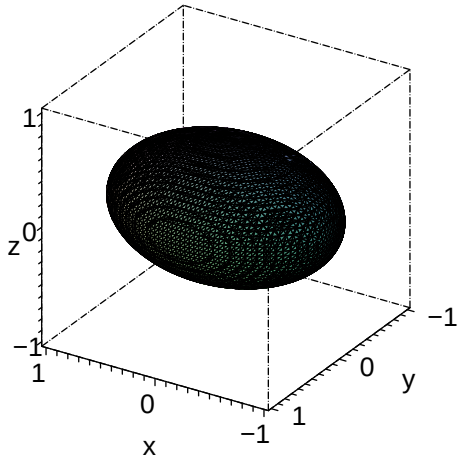
$$\int_S dxdy = \int_0^{2\pi}\int_0^{\pi/2} r\cos r dr\, d\theta = \pi^2 - 2\pi.$$

8.27. Určování integračních mezí v $\mathbb{R}^3$. Pokud integrujeme přes tělesa, která leží v $\mathbb{R}^3$, může nám při určování integračních mezí pomoci prostorová představivost. Uvádíme obrázky některých ploch v $\mathbb{R}^3$ a jejich rovnice v různých souřadných soustavách:

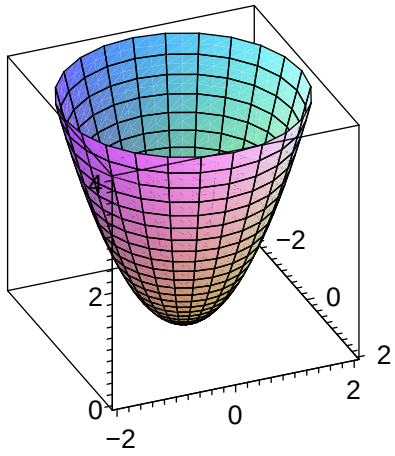
Koule se středem v bodě (x_0,y_0,z_0) a poloměrem r_0: $(x-x_0)^2 + (y-y_0)^2 + (z-z_0)^2 = r^2$.



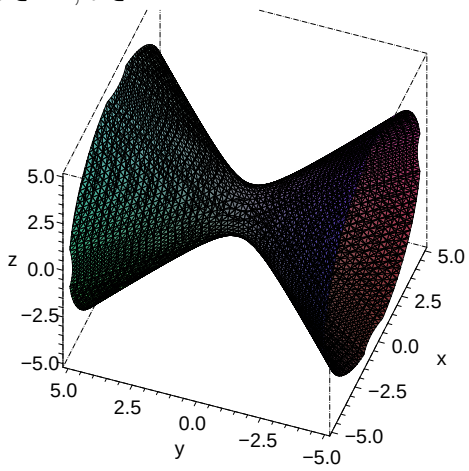
Elipsoid se středem v bodě (x_0, y_0, z_0): $a(x-x_0)^2+b(y-y_0)^2+(y-y_0)^2=r^2$, $a, b \in \mathbb{R}^+$.



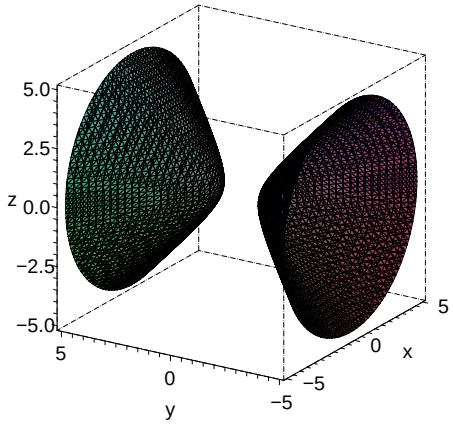
Paraboloid $a(x-x_0)^2+b(y-y_0)^2=z-z_0$, $a, b \in \mathbb{R}^+$, nebo $a, b \in \mathbb{R}^-$.



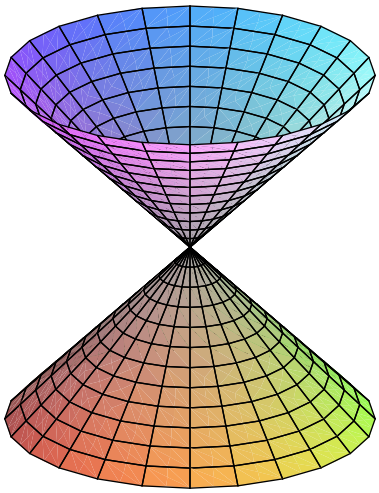
Jednodílný hyperboloid s vrcholem v bodě (x_0, y_0, z_0): $a(x-x_0)^2+b(y-y_0)^2+(z-z_0)^2=1$, $a \in \mathbb{R}^+$, $b \in \mathbb{R}^-$.



Dvoudílný hyperboloid s vrcholem v bodě (x_0, y_0, z_0): $a(x-x_0)^2+b(y-y_0)^2+(z-z_0)^2$=-1, $a \in \mathbb{R}^+$, $b \in \mathbb{R}^-$.



Kužel s vrcholem v bodě (S_x, S_y, S_z): $a(x - S_x)^2 + b(y - S_y)^2 = (z - S_z)^2$, $a, b \in \mathbb{R}^+$.

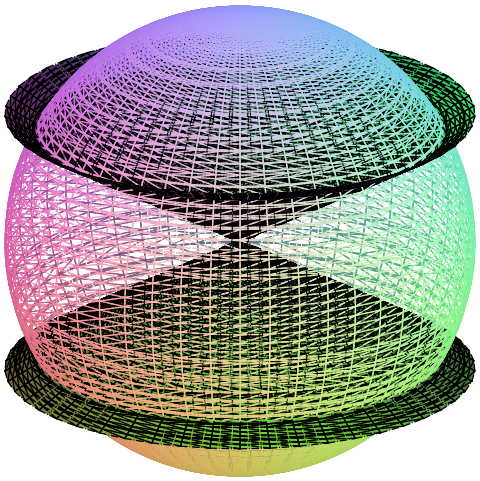


Demonstrujme si určování mezí na následujícím příkladu:

8.28. Příklady.

8.28.1. *Určete objem tělesa v $\mathbb{R}^3$, které je dáno nerovnostmi $x^2 + y^2 + z^2 \leq 1$, $3x^2 + 3y^2 \geq z^2$, $x \geq 0$.*

Řešení.



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.

$$\begin{aligned} x &= r\cos(\varphi)\sin(\psi) \\ y &= r\sin(\varphi)\sin(\psi) \\ z &= r\cos(\psi), \end{aligned}$$

$\varphi \in \langle 0, 2\pi)$, $\psi \in \langle 0, \pi)$, $r \in (0, \infty)$.

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

$$x^2 + y^2 + z^2 = r^2\cos^2(\phi)\sin^2(\psi) + r^2\sin^2(\phi)\sin^2(\psi) + r^2\cos^2(\psi) = r^2 \leq 1.$$

Hledejme integrační meze nejprve například pro proměnnou ϕ. Označíme-li π_ϕ projekci na souřadnici ϕ ve sférických souřadnicích ($\pi_\phi(\phi, \theta, r) = \phi$), pak obraz projekce π_ϕ uvažovaného tělesa nám udává integrační meze proměnné ϕ. Víme, že $\pi_\phi(koule) = \langle 0, 2\pi)$ (to víme buď díky naší prostorové představivosti, nebo z rovnice koule $r^2 \leq 1$, ve které proměnná ϕ 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 $\phi_0 \in \langle 0, 2\pi)$ a pro toto ϕ_0 (dále již pevně zvolené) určíme průnik tělesa (koule) s plochou $\phi = \phi_0$ a jeho projekci π_ψ na proměnnou ψ. Opět jako při určování mezí pro ϕ není proměnná ψ nijak omezena (ani nerovnicí $r^2 \leq 1$, ani rovnicí $\phi = \phi_0$] může tak nabývat všech svých hodnot, $\psi \in \langle 0, \pi)$.

Konečně hledáme pro libovolně (dále ale pevně) zvolené $\phi = \phi_0$ a $\psi = \psi_0$ průmět $\pi_r(U)$ objektu (úsečky) U dané omezeními $r^2 \leq 1$, $\phi = \phi_0$, $\psi = \psi_0$ na proměnnou r. Jediným omezením na r je podmínka $r^2 \leq 1$, tedy $r \in (0, 1\rangle$.

Všimněme si, že integrační meze proměnných jsou na sobě nezávislé, můžeme tedy integrovat v libovolném pořadí. Je tedy

$$V_{\text{koule}} = \int_0^1 \int_0^{2\pi} \int_0^{\pi} r^2 \sin(\psi)\, \mathrm{d}\psi\, \mathrm{d}\phi\, \mathrm{d}r = \frac{4}{3}\pi.$$

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, intergrační meze jednotlivých proměnných tedy budou na sobě nezávislé. Z podmínky $r^2 \leq 1$ máme $r \in (0, 1\rangle$, z podmínky $\tan(\psi) \geq \frac{1}{\sqrt{3}}$ vyplývá $\psi \in \langle 0, \frac{\pi}{6}\rangle$. Na proměnnou ϕ žádné podmínky neklademe, je tedy $\phi \in \langle 0, 2\pi\rangle$.

$$V_{\text{výseč}} = \int_0^{2\pi} \int_0^1 \int_0^{\frac{\pi}{6}} r^2 \sin\psi\, \mathrm{d}\psi\, \mathrm{d}r\, \mathrm{d}\varphi = \frac{2-\sqrt{3}}{3}\pi,$$

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 $r \leq \frac{1}{2}$, resp. $r \geq \frac{1}{2}$.

$$\begin{aligned} V = V_1 + V_2 &= \int_0^{2\pi} \int_0^{\frac{1}{2}} \int_0^{\sqrt{3}r} r\, \mathrm{d}z\, \mathrm{d}r\, \mathrm{d}\varphi + \int_0^{2\pi} \int_{\frac{1}{2}}^1 \int_0^{\sqrt{1-r^2}} r\, \mathrm{d}z\, \mathrm{d}r\, \mathrm{d}\varphi \\ &= \frac{\pi}{\sqrt{3}} \end{aligned}$$

□

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 $x^2 + y^2 \leq \frac{1}{4}$, $0 \leq z \leq \frac{\sqrt{3}}{2}$ a části kužele $3x^2 + 3y^2 \leq z^2$, $0 \leq z \leq \frac{\sqrt{3}}{2}$,

objem druhé pak jako rozdíl objemu rotačního tělesa vziklého rotací části oblouku $y = \sqrt{(1-x^2)}$, $\frac{1}{2} \le x \le 1$ kolem osy z a válce $x^2 + y^2 \le \frac{1}{4}$, $0 \le z \le \frac{\sqrt{3}}{2}$.

$$\begin{aligned} V = V_1 + V_2 &= \left(\frac{\pi\sqrt{3}}{8} - \frac{\pi\sqrt{3}}{24}\right) + \left(\pi \int_0^{\frac{\sqrt{3}}{2}} (1-r^2)\,\mathrm{d}r - \frac{\pi\sqrt{3}}{8}\right) \\ &= \frac{\pi\sqrt{3}}{4} + \frac{\pi}{4\sqrt{3}} = \frac{\pi}{\sqrt{3}} \end{aligned}$$

8.28.2. *Vypočtěte objem kulové úseče, který odřezává rovina $z = 1$ z koule $x^2 + y^2 + z^2 = 2$.*

Řešení. Spočítáme integrál v kulových souřadnicích. Úseč 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 $(0, \sqrt{2}) \times \langle 0, 2\pi) \times \langle 0, \pi/4\rangle$. Integrujeme tedy v daných mezích a to v **libovolném** pořadí.

$$\int_0^{2\pi} \int_0^{\sqrt{2}} \int_0^{\frac{\pi}{4}} r^2 \sin(\theta)\,\mathrm{d}\theta\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{4}{3}(\sqrt{2}-1)\pi.$$

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:

$$\begin{aligned} V &= V_{\text{výseč}} - V_{\text{kužel}} \\ &= \int_0^{2\pi} \int_0^{\arccos\left(\frac{R-v}{R}\right)} \int_0^{R} r^2 \sin(\theta)\,\mathrm{d}r\,\mathrm{d}\theta\,\mathrm{d}\phi - \frac{1}{3}\pi(2Rv - v^2)(R-v) \\ &= \frac{1}{3}\pi v^2(3R - v) \end{aligned}$$

□

8.28.3. *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 (záměníme-li x za $-x$, či y za $-y$, či z za $-z$ tak se rovnice tělesa nezmění). Část tělesa ležící v prvním kvadrantu je dána prostorem ležícím pod grafem funkce $z = \sqrt{16 - x^2}$ a nad čtvrtkruhem $x^2 + y^2 \le 16$, $x \ge 0$, $y \ge 0$. rovinou $z = 0$, je

$$S = 8 \int_0^4 \int_0^{\sqrt{16-x^2}} \frac{4}{\sqrt{16-x^2}}\,\mathrm{d}y\,\mathrm{d}x = 128.$$

□

8.28.4. *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 vrholy $[0,0,0], [0,0,2], [-2,0,0], [0,-2,0]$. Část tělesa ležící nad rovinou $z = 0$ tedy rozdělíme ještě na dvě části, jejichž objem spočítáme zvlášť.

$$\begin{aligned} V_1 - V_{\text{jehlan}} &= \int_{-\pi/2}^{\pi}\int_0^2 r^2(\sin(\varphi)+\cos(\varphi)) + 2r\,\mathrm{d}r\,\mathrm{d}\varphi = 6\pi + \frac{16}{3}, \\ V_{\text{jehlan}} &= \frac{4}{3} \end{aligned}$$

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 $V_1 + V_2 = 4\pi + \frac{40}{3}$. □

8.28.5. *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 kartézkých 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 $[\frac{4\sqrt{3}}{9\pi}, \frac{2\sqrt{2}}{\pi}]$. □

8.28.6. *Určete objem a souřadnice těžiště 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:

$$V = 4\int_0^{\pi/2}\int_0^r\int_{\frac{h}{r}\rho}^h \rho\,\mathrm{d}z\,\mathrm{d}\rho\,\mathrm{d}\varphi = \frac{1}{3}\pi h r^2.$$

Těžiště zjevně leží na ose z. Pro z-tovou souřadnici pak máme

$$z = \frac{1}{V}\int_{\text{kužel}} z dV = \frac{1}{V}\int_0^{\pi/2}\int_0^r\int_{\frac{h}{r}\rho}^h z\rho\,\mathrm{d}z\,\mathrm{d}\rho\,\mathrm{d}\varphi = \frac{3}{4}h.$$

Těžiště tedy leží ve výšce $\frac{1}{4}h$ nad středem podstavy kužele. □

8.28.7. *Určete objem tělesa v $\mathbb{R}^3$, které je dáno průnikem koule $x^2+y^2+z^2=4$ s válcem $x^2+y^2=1$.*

Opět 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 Jacobiánem dané trasformace $J = r$, 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

Řešení.

$$V = 8\int_0^{\pi/2}\int_0^1 r\sqrt{4-r^2}\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{2}{3}(8-3\sqrt{3})\pi.$$

□

8.28.8. *Určete objem tělesa v $\mathbb{R}^3$, které je dáno průnikem koule $x^2+y^2+z^2=2$ s paraboloidem $z = x^2+y^2$. Použijeme opět válcových souřadnic.*

Řešení.

$$V = \int_0^{2\pi}\int_0^1\int_{r^2}^{\sqrt{(2-r^2)}} r\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{4\sqrt{2}\pi}{3} - \frac{7\pi}{6}.$$

□

8.28.9. *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 $x = \frac{1}{2}r\cos(\varphi)$, $y = r\cos(\varphi)$, $z = z$, s Jakobiánem příslušné transformace $J = \frac{1}{2}r$. Eliptický válec má v těchto souřadnicích rovnici $r^2 = 1$.

$$\begin{aligned} V &= \int_0^{\pi}\int_0^1 r\sin(\varphi)\frac{1}{2}r\,\mathrm{d}r\,\mathrm{d}\varphi \\ &= \int_0^{\pi}\int_0^1 r^2\sin(\varphi)\,\mathrm{d}r\,\mathrm{d}\varphi = \int_0^{\pi}\frac{1}{3}\sin(\varphi)\,\mathrm{d}\varphi = \frac{2}{3}. \end{aligned}$$

□

8.28.10. *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 Jacobiánem $J = \frac{1}{\sqrt{2}}r$. Rovnice

paraboloidu je v těchto souřadnicích $z = r^2$ a pro objem tělesa můžeme psát

$$\begin{aligned} V &= 4\int_0^{\pi/2}\int_0^{\sqrt{2}}\int_{r^2}^{2}\frac{1}{\sqrt{2}}r\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi = \\ &= 2\sqrt{2}\int_0^{\pi/2}\int_0^{\sqrt{2}}2r - r^3\,\mathrm{d}r\,\mathrm{d}\varphi = 2\sqrt{2}\int_0^{\pi/2}\mathrm{d}\varphi = \\ &= \sqrt{2}\pi. \end{aligned}$$

□

8.28.11. *Vypočtěte objem elipsoidu $x^2 + 2y^2 + 3z^2 = 1$.*

Řešení. Uvážíme souřadnice

$$\begin{aligned} x &= r\cos(\phi)\sin(\theta) \\ y &= \tfrac{1}{\sqrt{2}}r\sin(\phi)\sin(\theta) \\ z &= \tfrac{1}{\sqrt{3}}r\cos(\theta) \end{aligned}$$

Odpovídající determinant z Jakobiánu je pak $\frac{1}{\sqrt{6}}r^2\sin(\theta)$, objem je tedy

$$\int_0^{2\pi}\int_0^{\pi}\int_0^{1}\frac{1}{\sqrt{6}}r^2\sin(\theta)\,\mathrm{d}r\,\mathrm{d}\theta\,\mathrm{d}\phi = \frac{4}{3\sqrt{6}}\pi r^3.$$

□

8.28.12. *Vypočtěte objem tělesa omezeného paraboloidem $2x^2 + 5y^2 = z$ a rovinou $z = 1$.*

Řešení. Volíme souřadnice

$$\begin{aligned} x &= \tfrac{1}{\sqrt{2}}r\cos(\phi) \\ y &= \tfrac{1}{\sqrt{5}}r\sin(\phi) \\ z &= z \end{aligned}$$

Determinant Jakobiánu je $\frac{r}{\sqrt{10}}$, objem je tedy

$$\int_0^{2\pi}\int_0^{1}\int_{r^2}^{1}\frac{r}{\sqrt{10}}\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\phi = \frac{\pi}{2\sqrt{10}}.$$

□

8.28.13. 2. *Určete objem tělesa ležícího v prvním oktantu a ohraničeném plochami $y^2 + z^2 = 9$ a $y^2 = 3x$.*

Řešení. Ve válcových souřadnicích

$$\int_0^{\pi/2}\int_0^{3}\int_0^{\frac{r^2}{3}\cos^2(\varphi)} r\,\mathrm{d}x\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{27}{16}\pi.$$

□

8.28.14. *Určete objem tělesa v $\mathbb{R}^3$, které je ohraničeno částí kužele $2x^2 + y^2 = (z-2)^2$, $z \geq 2$ a paraboloidem $2x^2 + y^2 = 8 - z$ (malý návrh: určete nejprve průnik zadaných ploch)*

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 φ roven intervalu $\langle 0, 2\pi\rangle$, pro dané $\varphi_0 \in \langle 0, 2\pi\rangle$ je potom průmět průniku tělesa s rovinou $\varphi = \varphi_0$ do souřadnice r roven (pro lib φ_0) intervalu $\langle 0, 2\rangle$. Pro dané r_0 a φ_0 je pak průmět průniku tělesa s přímkou $r = r_0$, $\varphi = \varphi_0$ na souřadnici z roven intervalu $\langle r_0 + 2, 8 - r_0^2\rangle$. Jakobián uvažované transformace je $J = \frac{1}{\sqrt{2}} r$, celkem tedy můžeme psát

$$V = \int_0^{2\pi}\int_0^2\int_{r+2}^{8-r^2} \frac{r}{\sqrt{2}}\,\mathrm{d}z\,\mathrm{d}r\,\mathrm{d}\varphi = \frac{16\sqrt{2}}{3}\pi.$$

□

8.28.15. *Určete objem tělesa ležícího uvnitř válce $y^2 + z^2 = 4$, dále v polorovině $x \geq 0$ a konečně ohraničeného plochou $y^2 + z^2 + 2x = 16$.*

Řešení. Ve válcových souřadnicích

$$\int_0^{2\pi}\int_0^2\int_0^{8-\frac{r^2}{2}} r\,\mathrm{d}x\,\mathrm{d}r\,\mathrm{d}\varphi = 28\pi.$$

□

3. Diferenciální operátory

7.11

8.29. Lineární a nelineární 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 rovnicím. Nejjednodušším modelem bylo úročení vkladů nebo půjček (a totéž pro tzv. Malthusiánský model populace). Přírůstek byl úměrný hodnotě, viz 1.11. V rámci spojitého modelování by stejný požadavek vedl na rovnici vztahující derivaci funkce $y'(x)$ s její hodnotou

e7.20 (8.6) $$y'(x) = r \cdot y(x)$$

s konstantou úměrnosti r. Je snadné uhodnout řešení této rovnosti

$$y(x) = C\,\mathrm{e}^{rx}$$

s libovolnou konstantou C. Tuto konstantu určíme jednoznačně volbou tzv. *počáteční hodnoty* $y_0 = y(x_0)$ v nějakém bodě x_0. Pokud by část růstu v našem modelu byla dána konstatním působením nezávislém na hodnotě y nebo x (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

e7.21 (8.7) $$y'(x) = r \cdot y(x) + s.$$

Zjevně bude řešením této rovnice funkce

$$y(x) = C\,\mathrm{e}^{rx} - \frac{s}{r}.$$

K tomuto závěru je velice lehké dojít, pokud si uvědomíme, že množinou věech řešení rovnice (8.6) je jednorozměrný vektorový prostor, zatímco řešení rovnice (8.7) se obdrží přičtením kteréhokoliv jednoho jejího řešení ke všem řešením předchozí rovnice. Lze pak snadno najít konstantní řešení $y(x) = k$ pro $k = -\frac{s}{r}$.

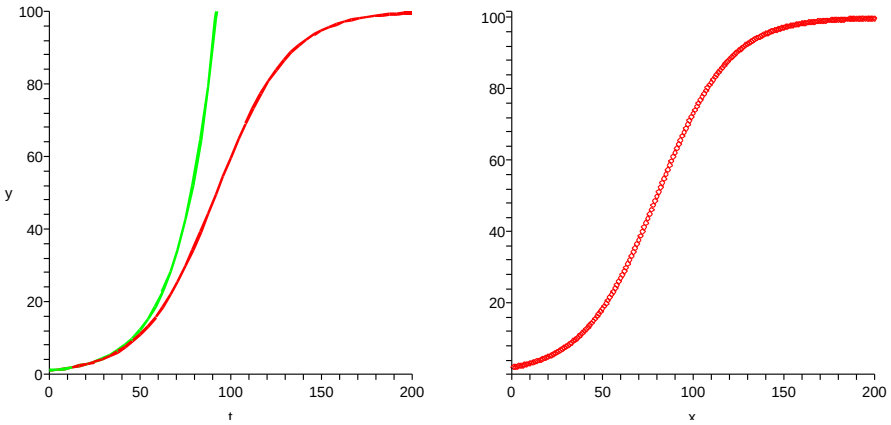
Podobně se nám v odstavci 1.18 podařilo vytvořit tzv. logistický model populačního růstu založený na předpokladu, že poměr změny velikosti populace $p(n+1) - p(n)$ a její velikosti $p(n)$ je v afinní závislosti na samotné velikosti populace. Nyní bychom tentýž vztah pro spojitý model patrně formulovali pro populaci $p(t)$ závislou na čase t jako

e7.22 (8.8) $$p'(t) = p(t)\left(-\frac{r}{K}p(t) + r\right),$$

tj. při hodnotě $p(t) = K$ pro velkou konstantu K je přírůstek nulový, zatímco pro $p(t)$ blízké nule je poměr rychlosti růstu populace k její velikosti blízký r, což je 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 lze jistě ověřit, že následující funkce řešením pro každou konstantu C je

$$p(t) = \frac{K}{1 + CK\,\mathrm{e}^{-rt}}.$$



Srovnáním červeného grafu (levý obrázek) této funkce s volbou $K = 100$, $r = 0,05$ a $C = 1$ (první dvě jsme takto použili v 1.18, poslední odpovídá přibližně počáteční hodnotě $p(0) = 1$) s pravým obrázkem (řešení diferenční rovnice z 1.18) vidíme, že skutečně oba přístupy k modelování populací dávají docela podobné výsledky. Pro srovnání výstupu je také do levého obrázku zeleně vkreslen graf řešení rovnice (8.6) s touž konstantou r a počáteční podmínkou.

7.12 **8.30. Diferenciální rovnice prvního řádu.** Obecně rozumíme (obyčejnou) diferenciální rovnicí prvního řádu vztah mezi derivací funkce $y'(x)$ v proměnné x, její hodnotou $y(x)$ a samotnou proměnnou, který lze zapsat jako

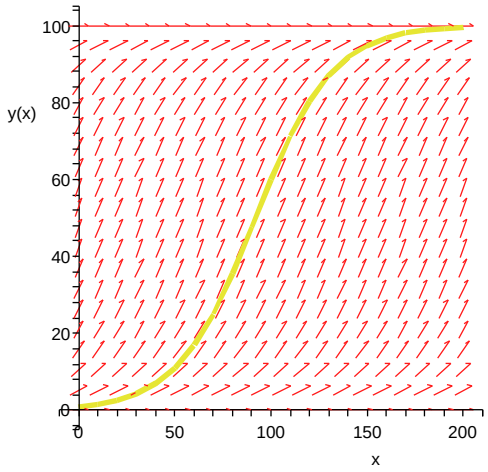
$$F(y'(x), y(x), x) = 0$$

nějakou pevnou funkci F, která každé trojici reálných čísel přiřadí jedno reálné číslo. Zápis připomíná implicitně zadané funkce $y(x)$, nicméně navíc je tu závislost na

derivaci hledané funkce $y(x)$. Pokud je alespoň rovnice explicitně vyřešena vzhledem k derivaci, tj.

$$y'(x) = f(x, y(x)),$$

můžeme si dobře graficky představit, co taková rovnice zadává. Pro každou hodnotu (x, y) v rovině si totiž můžeme představit šipku udávající vektor $(1, f(x, y))$, tj. rychlost se kterou nám rovnice grafu řešení přikazuje pohybovat se rovinou. Např. pro rovnici (8.8) 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. Takové tvrzení skutečně platí pro všechny rozumné funkce f, my si výsledek sformulujeme pro dosti velkou třídu rovnic takto:

Věta (O existenci a jednoznačnosti řešení ODE)**.** *Nechť funkce $f(x, y) : \mathbb{R}^2 \to \mathbb{R}$ má spojité parciální derivace. Pak pro každý bod $(x_0, y_0) \in \mathbb{R}^2$ existuje interval $[x_0 - a, x_0 + a]$, s $a \in \mathbb{R}$ kladným, a právě jedna funkce $y(x) : \mathbb{R} \to \mathbb{R}$, která je řešením rovnice*

$$y'(x) = f(x, y(x)).$$

Důkaz. Všimněme si, že funkce $y(x)$ je řešením naší rovnice tehdy a jen tehdy, když

$$y(x) = y_0 + \int_{x_0}^{x} y'(x)\,dx = y_0 + \int_{x_0}^{x} f(x, y(x))\,dx.$$

Pravá strana tohoto výrazu je ovšem, až na konstantu, integrální operátor

$$L(y)(x) = y_0 + \int_{x_0}^{x} f(x, y(x))\,dx$$

a při řešení diferenciální rovnice vlastně hledáme pevný bod pro tento operátor L, tj. chceme najít funkci $y = y(x)$ s $L(y) = y$.

Pro operátor L můžeme docela lehce odhadnout, jak se liší jeho hodnoty $L(y)$ a $L(z)$ pro různé argumenty $y(x)$ a $z(x)$. Skutečně, díky spojitosti parciálních derivací funkce f (ve skutečnosti využíváme pouze tzv. Lipschitzovy podmínky pro parciální derivaci podle y) dostáváme,

viz **??**

$$\begin{aligned}|(L(y)-L(z))(x)| &= \left|\int_{x_0}^{x} f(x,y(x)) - f(x,z(x))\,dx\right| \\ &\le \int_{x_0}^{x} |f(x,y(x)) - f(x,z(x))|\,dx \\ &\le C\int_{x_0}^{x} |y(x)-z(x)|\,dx \\ &\le D|x-x_0|\,dx\end{aligned}$$

pro vhodné konstanty C a D. Pro a dostatečně malé proto bude platit

$$\sup_{|x-x_0|<a} |L(y)(x) - L(z)(x)| < \sup_{|x-x_0|<a} |y(x)-z(x)|.$$

Takovýmto operátorům se říká *kontrakce*.

Dokončit – poznámka o větě o kontrakci... ???????? □

8.22

8.31. Rovnice se separovanými proměnnými. Užitečným typem rovnic, pro který máme elementární postup k řešení jsou tzv. *rovnice se separovanými proměnnými*:

7.23 (8.9) $$y'(x) = f(x)\cdot g(y(x))$$

pro dvě dostatečně hladké funkce jedné reálné proměnné f a g. Obecné řešení tu lze získat integrací, tj. nalezením primitivních funkcí

$$G(y) = \int \frac{dy}{g(y)}, \quad F(x) = \int f(x)dx.$$

Pak totiž spočtením funkce $y(x)$ z implicitně zadaného vztahu $F(x)+C = G(y)$ s libovolnou konstantou C vede k řešení, protože derivováním této rovnosti (s použitím pravidla pro derivování složené funkce $G(y(x))$ dostaneme skutečně $\frac{1}{g(y)}\cdot y'(x) = f(x)$.

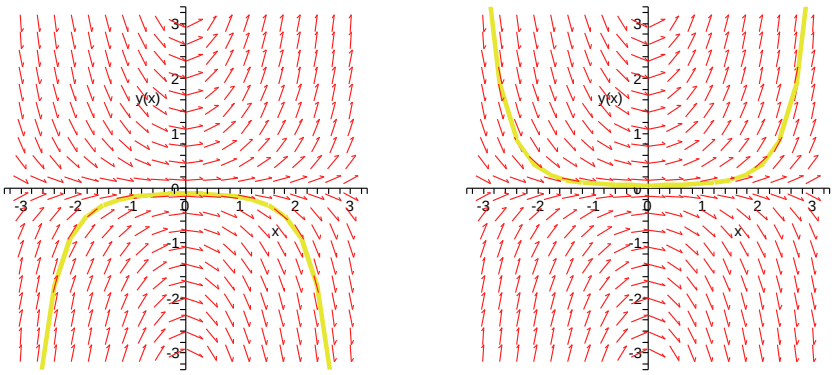
Jako příklad najděme řešení rovnice

$$y'(x) = x\cdot y(x).$$

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.

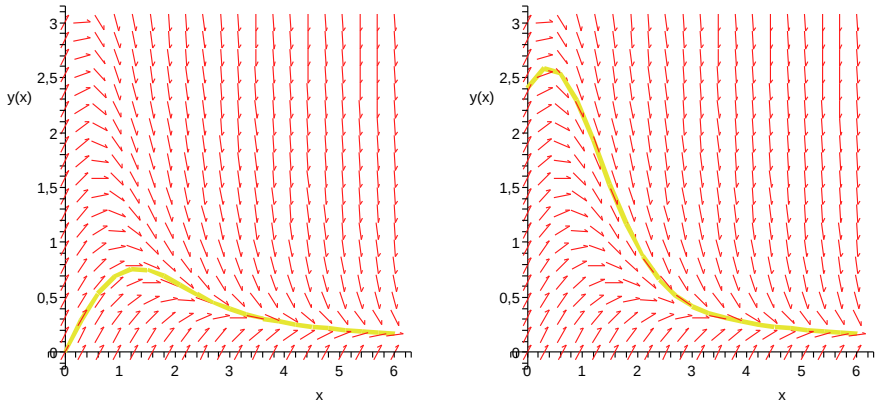


Na obrázku jsou vynešena dvě řešení, která ukazují na nestabilitu rovnice vůči počátečním podmínkám: Jestliže pro libovolné x_0 volíme y_0 blízké nule, pak se nám dramaticky mění chování výsledného řešení. Navíc si povšimněme konstatního řešení $y(x) = 0$, které odpovídá počáteční podmínce $y(x_0) = 0$.

Jestliže lehce pozměníme rovnici na

$$y'(x) = 1 - x \cdot y(x),$$

narazíme naopak na stabilní chování viditelné na následujícím obrázku. Tuto rovnici už ale neumíme řešit pomocí separace proměnných.



Zato umíme stejným postupem vyřešit nelineární model z předchozího odstavce, která popisovala logistický model populace. Zkuste si jako cvičení.

8.31.1. *Vyřešte diferenciální rovnici pro funkci $y = y(x)$*

$$\frac{dy}{dx} = \frac{1+y^2}{1+x^2}.$$

Řešení. $y = \frac{x+C}{1-Cx}$. (použijte součtového vzorce pro tangens). □

8.31.2. *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). Za infinitezimální (nekonečně malou) časovou jednotku $\mathrm{d}t$ 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 $t \doteq 6\,\mathrm{h}\ 35\,\mathrm{min}$. □

8.31.3. *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?*

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. □

8.31.4. *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 přechozím příkladě sestavíme diferenciální rovnici

$$\frac{df}{dt} = k \cdot f(t)\,(P - f(t))\,.$$

Opět separací proměnných a zavedením vhodných konstant K a L dostáváme

$$f(t) = \frac{K}{1 + Le^{-Kkt}}.$$

□

8.31.5. *Rychlost, kterou se rozpadá daný izotop daného prvku, je přímo úměrná množství daného izotopu. Poločas rozpadu izotopu Plutonia, $^{239}_{94}Pu$, 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 pak přibližně 349 let. □

8.31.6. *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 $5ms^{-1}$ v gravitačním poli $g = 10ms^{-2}$, konstanta odporu prostředí je $k = 0.5s^{-1}$. Jaká bude rychlost předmětu za 3 vteřiny?

Řešení.

$$v = \frac{g}{k} - (\frac{g}{k} - v_0)e^{-kt},$$

po dosazení $v(3) = 20 - 15e^{-\frac{3}{2}} ms^{-1}$. □

8.31.7. 1. *Rychost 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:

$$\frac{dP}{dt} = \frac{k}{P},$$

$P = \sqrt{Kt + c}$. Dopočtením ze zadaných hodnot $P(2) = \sqrt{7} \cdot 100$, což je odhad skutečného množství brouků (což musí být přirozené číslo). □

8.23

8.32. Systémy obyčejných diferenciálních rovnic prvního řádu. Na řešení rovnice $y'(x) = f(x, y)$ 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

$$x'(t) = f(t, x(t), y(t)), \quad y'(t) = g(t, x(t), y(t))$$

se dvěmi funkcemi $f, g : \mathbb{R}^3 \to \mathbb{R}$ se spojitými derivacemi. Obdobně pro více proměnných.

Jednoduchým příkladem v rovině může sloužit systém rovnic

$$x'(t) = -y(t), \quad y'(t) = x(t).$$

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.

Na takové systémy umíme přímo rozšířit platnost věty o jednoznačnosti a řešení:

Věta (O existenci a jednoznačnosti řešení systémů ODE)**.** *Nechť funkce* $f_i(t, x_1, \dots, x_n) : \mathbb{R}^{n+1} \to \mathbb{R}$*,* $i = 1, \dots, n$ *všechny mají spojité parciální derivace. Pak pro každý bod* $(t_0, z_1, \dots, z_n) \in \mathbb{R}^2$ *existuje interval* $[t_0 - a, t_0 + a]$*, s* $a \in \mathbb{R}$ *kladným, a právě jedna funkce* $y(t) : \mathbb{R} \to \mathbb{R}^n$*, která je řešením systému rovnic*

$$x_1'(x) = f_1(t, x_1(t), \dots, x_n(x)), \dots x_n'(x) = f_n(t, x_1(t), \dots, x_n(x))$$

s počáteční podmínkou

$$x_1(t_0) = z_1, \dots, x_n(t_0) = z_n.$$

Důkaz. Důkaz je skoro identický s důkazem existence a jednoznačnosti pro jednu rovnici s jednou neznámou funkcí, viz Věta 8.30. Neznámá funkce $y = (x_1(t), \dots, x_n(t))$ je křivkou v $\mathbb{R}^n$ vyhovující nejen zadané rovnici ale také jsou její komponenty opět vyjádřitelné pomocí integrálů

$$x_i(t) = x_i(t_0) + \int_{t_0}^{t} x_i'(t)\,dt = x_i(0) + \int_{t_0}^{t} f_i(t, y(t))\,dt.$$

Opět tedy pracujeme s integrálním operátorem $y \mapsto L(y)$, tentokrát definovaným na křivkách v $\mathbb{R}^n$ a hledáme jeho pevný bod. Protože je euklidovská vzdálenost dvou bodů v $\mathbb{R}^n$ vždy shora odhadnuta součtem velikostí rozdílů jednotlivých komponent, důkaz se dokončí stejně jako v případě 8.30. Je pouze zapotřebí si povšimnout, že velikost vektoru

$$\|f(t, z_1, \dots, z_n) - f(t, y_1, \dots, y_n)\|$$

je odhadnuta shora součtem

$$\|f(t, z_1, \dots, z_n) - f(t, y_1, z_2 \dots, z_n)\| + \dots + \|f(t, y_1, \dots, y_{n-1}, z_n) - f(t, y_1, \dots, y_n)\|.$$

□

Jako o něco složitější příklad systému rovnic prvního řádu si uveďme klasický populační model „dravec – kořist“, který zavedli ve dvacátých létech minulého století pánové Lotka a Volterra.

Označme $x(t)$ vývoj počtu jedinců v populaci kořisti a $y(t)$ totéž pro dravce. Přepokládáme, že přírůstek kořisti by se řídil Malthusiánským modelem (tj. exponenciální růst), kdyby nebyli loveni. U dravce naopak očekáváme, že by bez kořisti pouze přirozeně vymíral (tj. exponenciální pokles stavů). Přitom ale ještě musíme uvážit interakci dravce s kořistí, kterou očekáváme přímo úměrnou počtu obou. Dostáváme tak tzv. Lotka–Volterra model

$$x'(t) = \alpha x(t) - \beta y(t) x(t)$$
$$y'(t) = -\gamma y(t) + \delta \beta x(t) y(t)$$

kde koeficient δ vyjadřuje efektivitu růstu populace dravců v důsledku lovu.

Tento model je krásným příkladem pro studium stability či nestability řešení v důsledku volby počátečních hodnot, nebudeme zde však zacházet do podrobností. O tomto a podobných modelech lze nalézt nepřeberné množství literatury.

8.24

8.33. Rovnice vyšších řádů. Obyčejnou diferenciální rovnicí řádu k (vyřešenou vzhledek k nejvyšší derivaci) rozumíme rovnici

$$y^{(k)}(x) = f(x, y(x), y'(x), \dots, y^{(k-1)}(x)),$$

kde f je známá funkce v $k + 1$ proměnných, x je nezávisle proměnná a $y(x)$ je neznámá funkce v jedné proměnné.

Ukážeme, že taková rovnice je vždy ekvivalentní systému k rovnic prvního řádu: Zavedeme nové neznámé funkce v proměnné x takto: $y_0(x) = y(x)$, $y_1(x) = y_0'(x)$,

$\dots$, $y_{k-1}(x) = y'_{k-2}$. Nyní je funkce $y(x)$ řešením naší původní rovnice tehdy a jen tehdy, když je první komponentou řešení systému rovnic

$$\begin{aligned} y'_0(x) &= y_1(x) \\ y'_1(x) &= y_2(x) \\ &\vdots \\ y'_{n-2}(x) &= y_{n-1}(x) \\ y'_{n-1}(x) &= f(x, y_0(x), y_1(x), \dots, y_{n-1}(x)). \end{aligned}$$

Přímým důsledkem Věty 8.32 je proto následující

Věta (O existenci a jednoznačnosti řešení ODE)**.** *Nechť funkce $f(x, y_0, \dots, y_{k-1}) : \mathbb{R}^{k+1} \to \mathbb{R}$, má spojité parciální derivace. Pak pro každý bod $(x_0, z_0, \dots, z_{k-1}) \in \mathbb{R}^2$ existuje interval $[x_0 - a, x_0 + a]$, s $a \in \mathbb{R}$ kladným, a právě jedna funkce $y(x) : \mathbb{R} \to \mathbb{R}^n$, která je rovnice*

$$y^{(k)}(x) = f(x, y(x), y'(x), \dots, y^{(k-1)}(x))$$

s počáteční podmínkou

$$y(x_0) = z_0, \dots, y_{k-1}(x_0) = z_{k-1}.$$

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.

7.13

8.34. 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 $a_j(x)$ a výrazy sečteme, dostaneme tzv. *lineární diferenciální operátor*:

$$y(x) \mapsto D(y)(x) = a_k(x)y^{(k)}(x) + \dots + a_1(x)y'(x) + a_0y(x).$$

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

$$D(y_1 + y_2)(x) = D(y_1)(x) + D(y_2)(x).$$

Obdobně je také konstantní násobek řešení opět řešením. Celá mmnožina všech řešení lineární diferenciální rovnice k-tého řádu je tedy vektorovým prostorem. Přímou aplikací předchozí věty o jednoznačnosti a existenci řešení rovnic dostáváme:

Důsledek. *Vektorový prostor všech řešení homogenní lineární diferenciální rovnice k–tého řádu je vždy 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 $y(x)$ jejích prvních $(k-1)$ derivací.*

8.35. 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. Dostáváme tedy tzv. rovnici oscilátoru

$$y''(t) = -y(t).$$

Tato rovnice odpovídá systému rovnic

$$x'(t) = -y(t), \quad y'(t) = x(t)$$

z 8.32. Řešením takového systému je

$$x(t) = R\cos(t-\tau), \quad y(t) = R\sin(t-\tau)$$

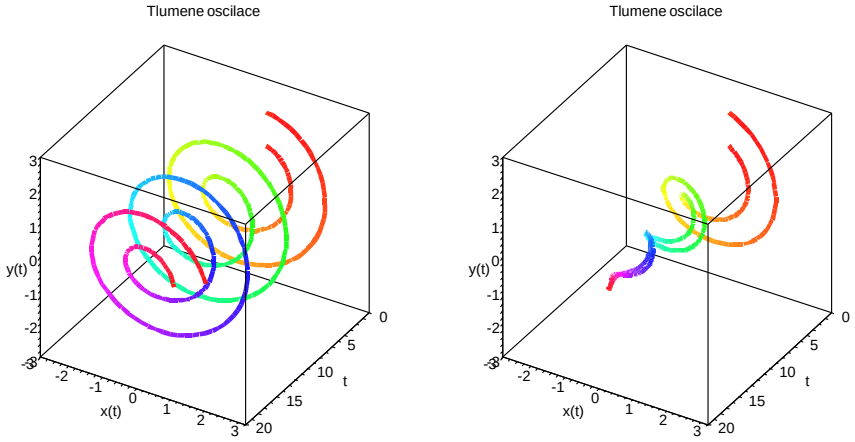
s libovolnou nezápornou konstantou R, která určuje maximální amplitudu, a konstantou τ, která určuje fázový posun.

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

$$y''(t) = -y(t) - \alpha y'(t),$$

kde α je konstanta, která vyjadřuje velikost tlumení. Na následujícím obrázku jsou vynešeny tzv. fázové diagramy pro řešení s dvěmi 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.

8.27

8.36. Lineární diferenciální rovnice s konstantními koeficienty. To vše jistě připomíná situaci s homogenními lineárními diferenčními rovnicemi, se kterými jsme se potýkali v odstavci 3.6 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 (8.6), že řešením je exponenciála s vhodnou konstantou u argumentu. Stejně jako u diferenčních rovnic se podbízí vyzkoušet, zda takový

tvar řešení $y(x) = \mathrm{e}^{\lambda x}$ s neznámým parametrem λ může splnit rovnici k–tého řádu. Dosazením dostaneme

$$D(\mathrm{e}^{\lambda x}) = \left(a_k\lambda^k + a_{k-1}\lambda^{k-1} + \cdots + a_1\lambda + a_0(x)\right)\mathrm{e}^{\lambda x}\,.$$

Parametr λ tedy vede na řešení lineární diferenciální rovnice s konstantními koeficienty tehdy a jen tehdy, když je λ 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 λ násobný kořen, přímým výpočtem s využitím toho, že je pak také kořenem derivace charakteristického polynomu, dostaneme, že je řešením i funkce $x\,\mathrm{e}^{\lambda x}$. Podobně pak pro vyšší násobnost ℓ dostáváme ℓ různých řešení $\mathrm{e}^{\lambda}, x\,\mathrm{e}^{\lambda x}, \ldots, x^{\ell}\,\mathrm{e}^{\lambda x}$.

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

$$D(y)(x) = b(x)$$

pro nějakou pevně zadanou funkci $b(x)$ je součtem jednoho jakéhokoliv řešení této rovnice a množiny všech možných řešení příslušné homogenní rovnice $D(y)(x) = 0$. Celý prostor řešení je tedy opět pěkný konečněrozměrný afinní prostor, byť ukrytý v obrovském prostoru funkcí.

8.37. Příklady.

8.37.1. 1. *Určete obecné řešení rovnice*

$$y'' + 3y' + 2y = e^{-2x}.$$

Řešení. 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 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 $c_1e^{-x} + c_2e^{-2x} - xe^{-2x}$, $c_1, c_2 \in \mathbb{R}$. □

8.37.2. *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 $c_1 + c_2 e^{-x}$, kde $c_1, c_2 \in \mathbb{R}$.

Partikulární řešení hledáme ve tvaru ax, $a \in \mathbb{R}$. Po dosazení do původní rovnice dostáváme $a = 1$. Obecné řešení dané nehomogenní rovnice je $c_1 + c_2 e^{-x} + x$, $c_1, c_2 \in \mathbb{R}$. □

8.37.3. *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 $c_1 e^{-2x} + c_2 e^{-3x}$, $c_1, c_2 \in \mathbb{R}$. 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 $c_1 e^{-2x} + c_2 e^{-3x} + xe^{-2x}$. □

8.37.4. *Určete obecné řešení rovnice*

$$y'' - y' = 5.$$

Řešení. Charakteristický polynom je $x^2 - x$ s kořeny 1, 0, obecné řešení zhomogenizované rovnice je tedy $c_1 + c_2 e^x$, 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 $c_1 + c_2 e^x - 5x$. □

8.37.5. *Určete jedinou funkci y vyhovující lineární diferenciální rovnici $y^{(3)} + 3y'' + 3y' + y = 4$ s počátečními podmínkami $y(0) = 1$, $y'(0) = 0$, $y''(0) = 0$.*

Řešení. Charakteristický polynom zhomogenizované rovnice je $x^3 + 3x^2 + 3x + 1 = (x + 1)^3$ s trojnásobným kořenem -1. Obecné řešení zhomogenizované rovnice je tedy $c_1 e^{-x} + c_2 xe^{-x} + c_3 x^2 e^{-x}$, $c_1, c_2, c_3 \in \mathbb{R}$. Partikulární řešení hledáme ve tvaru konstanty a dosazením snadno zjistíme, že jím je konstanta 4. Nyní hledáme takové obecné řešení dané nehomogenní rovnice, tedy funkci tvaru $y_p(x) = c_1 e^{-x} + c_2 xe^{-x} + c_3 x^2 e^{-x} + 4$, $c_1, c_2, c_3 \in \mathbb{R}$, které splňuje počáteční podmínky:

$$\begin{aligned} y_p(0) = 1 \quad &\equiv \quad c_1 + 4 \quad = \quad 1 \\ y_p'(0) = 0 \quad &\equiv \quad -c_1 + c_2 = 0 \\ y_p''(0) = 0 \quad &\equiv \quad c_1 - 2c_2 + 2c_3 = 0 \end{aligned}$$

Tato lineární soustava má jediné řešení $c_1 = -3$, $c_2 = -3$, $c_3 = -\frac{3}{2}$. Jedinou funkcí splňující danou diferenciální rovnici s uvedenými počátečními podmínkami je funkce

$$y(x) = -3e^{-x} - 3xe^{-x} - \frac{3}{2}x^2 e^{-x} + 4.$$

□

8.37.6. *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

$$c_1 e^{2x} + c_2 e^{-x} + c_3 x e^{-x} - \frac{1}{2}e^x.$$

Dosazením do počátečních podmínek získáme jedninou funkci vyhovující zadání

$$\frac{2}{9}e^{2x} + \frac{5}{18}e^{-x} + \frac{1}{3}xe^{-x} - \frac{1}{2}e^x.$$

□

4. Poznámky o numerických metodách

Kromě tak jednoduchých rovnic, jako jsou ty lineární s konstantními koeficienty se v praxi většinou setkáváme s postupy, jak přibližně spočíst řešení rovnice, se kterou 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.

8.28

8.38. Odhady „velké O“. Pro funkci $f(x)$ v proměnné x řekneme, 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

$$|f(x)| \le C \cdot |\varphi(x)|$$

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.

8.29

8.39. 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.

8.40. Další metody. (metoda Taylorových řad, Runge–Kutta atd) ??????????????

KAPITOLA 9

Kombinatorické metody

že tak často myslíme raději v obrázcích?
– ano, ale spočíst zvládneme jen diskrétní věci ...

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 1.5–1.18.

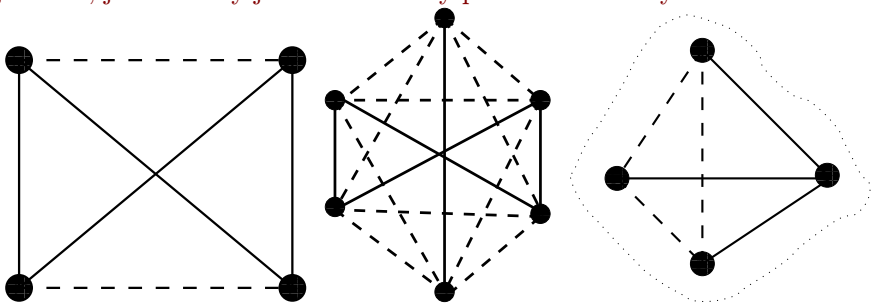
1. Grafy a algoritmy

Začneme dvěma příklady docela typických kombinatorických postupů:

9.1

9.1. Dva 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 budou buď navzájem znát nebo neznát?

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 nejdeme trojúhelník, jehož strany jsou buď všechny plné nebo všechny čárkované?

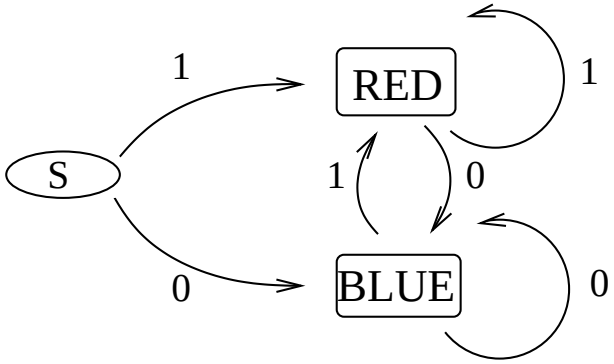


Na levém obrázku se čtyřmi puntíky takový trojúhelník není, uprostřed je. Snadno ověříme, že jej najdeme vždy, když počet hostů bude alespoň pět:

Skutečně, 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 znázorněná na pravém obrázku. Ve 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.

Nyní předpokládejme, že máme krabičku, která požírá jeden bit za druhým (třeba podle toho, jestli dveřmi zrovna prošel muž nebo žena – jednička nechť označuje třeba ženu), a má svítit buď modře nebo červeně podle toho, zda byl

poslední bit nula nebo jednička (a bodle barvy světla tedy můžeme tedy poznat, zda je za dveřmi muž nebo žena). Opět si schéma můžeme pěkně znázornit:



Třetí uzel, ze kterého pouze vychází dvě šipky naznačuje start před prvním zaslaným bitem.

9.2

9.2. Základní pojmy grafů. V obou příkladech máme společné schéma. Máme nějakou konečnou množinu objektů, kterou si znázorňujeme jako uzly a jejich vlastností, které znázorňujeme spojnicemi mezi nimi. Už dávno víme, že takové situace umíme popisovat pomocí tzv. relací, viz. text začínající odstavcem 1.43 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 dvěmi komplementárními symetrickými a antireflexními relacemi, ve druhém pak jde o příklad dvou antisymetrických relací na třech prvcích.

My teď ale můžeme na relace pozapomnět 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.

Definice. *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 ve hraně $e = \{v, w\}$, $v \neq w$, říkáme *hraniční 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 $E \subset V \times V$. 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 vrchol pro jednu koncový a pro druhou počáteční. Naopak, sousední vrcholy jsou ty, které jsou hraničními pro tutéž hranu.

Grafy jsou mimořádně dobrým jazykem pro přemýšlení o postupech a odvozování vztahů týkajících konečných množin objektů. Jsou totiž pěkným příkladem kompromisu mezi přirozeným sklonem k „přemýšlením v obrázcích“ a přesným matematickým vyjadřováním. Obecný jazyk teorie grafů nám v konkrétních úlohách také umožňuje přidávat informace o vrcholech nebo hranách. Můžeme tak např. „obarvit“ vrcholy podle příslušnosti objektů k několika disjunktním skupinám nebo můžeme označit hrany několika různými hodnotami apod. Existence hrany mezi vrcholy různých barev může naznačit „konflikt“. Např. když modré a červené uzly

představují pánskou a dámskou část večírku, pak hrana mezi vrcholy různých barev může znamenat potenciální nevhodnost sdílení pokoje pro přenocování. Náš první příklad v předchozím odstavci můžeme tedy chápat jako graf s obarvenými hranami. Dokázané tvrzení v této řeči zní: *V grafu $K_n = (V, \binom{V}{2})$ s n vrcholy a se všemi možnými hranami obarvenými na dvě barvy je vždy alespoň jeden trojúhelník z hran o stejné barvě, pokud je počet vrcholů alespoň šest.*

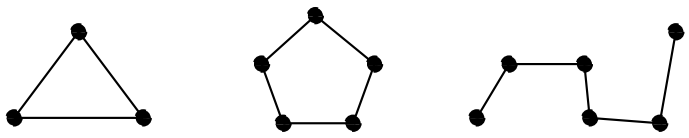
Výše znázorněný orientovaný graf s označenými hranami (hodnotami nula nebo jedna) představuje jednoduchý *konečný automat*. Tento název odráží představu, že graf popisuje proces, který se vždy nachází ve stavu popsaným některým z uzlů a další stav nastane procesem, odpovídajícím jedn z hran, které z vrcholu vychází. Teorií konečných automatů se zde nebudeme podrobněji zabývat.

9.3

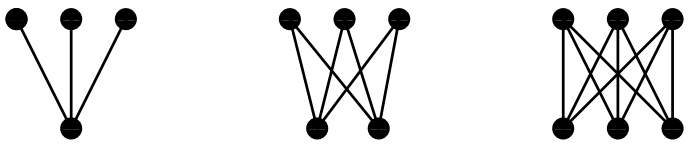
9.3. Příklady užitečných jednoduchých grafů. Nejjednodušším grafem je graf bez hran, pro ten si ale ani nebudeme zavádět zvláštní označení.

Opačný extrém je naopak užitečný a grafu se všemi možnými hranami říkáme *úplný graf*. Značíme symbolem K_n, kde n je počet vrcholů grafu. Graf K_4 a K_5 jsme již viděli, K_3 je trojúhelník, K_2 je úsečka.

Dalším důležitým grafem je *cesta*, tj. graf, kde existuje uspořádání vrcholů $(v_0, \dots, v_n)$ takové, že $E = \{e_1, \dots, e_n\}$, kde $e_i = \{v_{i-1}, v_i\}$, pro všechny $i = 1, \dots, n$. Hovoříme o *cestě délky* n a značíme ji P_n. Pokud cestu upravíme tak, že poslední a první vrchol splývají, dostaneme *kružnici délky* n a značíme C_N. Na dalším obrázku vidíme $K_3 = C_3$, C_5 a P_5



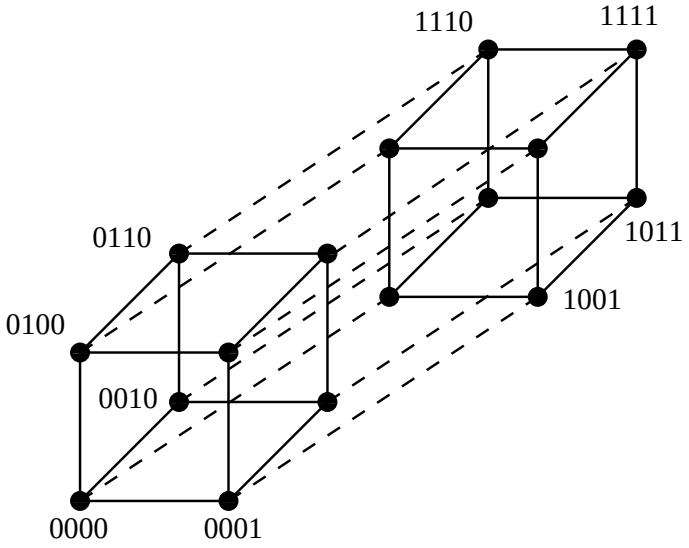
Dalším příkladem je tzv. úplný *bipartitní graf*, který vznikne tak, že vrcholy si obarvíme dvěmi barvami a pak přidáme všechny hrany, které spojí vrcholy různých barev. Značíme jej $K_{m,n}$, kde m a n jsou počty vrcholů s jednotlivými barvami. Na obrázku je vidět $K_{1,3}$, $K_{2,3}$ a $K_{3,3}$.



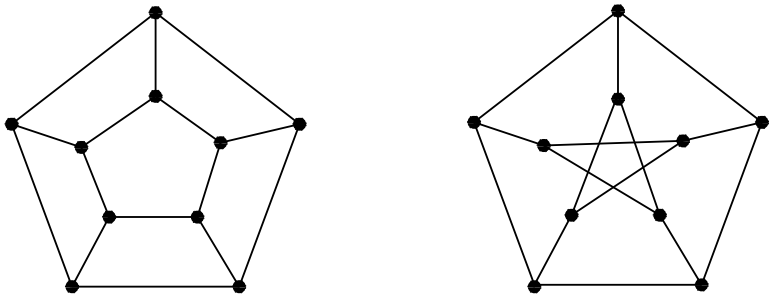
Dobrým příkladem grafu je také tzv. hyperkostka H_n v dimenzi n, která vznikne tak, že vrcholy jsou všechna čísla $0, \dots, 2^n - 1$. Hrany spojí právě ta čísla, která se v zápisu v dvojkové soustavě liší v právě jednom bitu. Na obrázku níže je H_4 a popis vrcholů je naznačen.

Všimněme si, že přímo z definice vyplývá, že hyperkostku v dané dimenzi vždy cky dostaneme tak, že vhodně spojíme hranami dvě hyperkostky o jednu dimenzi menší. Na obrázku je to naznačeno tak, že příslušné hrany mezi dvěmi disjunktními

kopiemi H_3 jsou čárkované. Samozřejmě ale můžeme tímto způsobem rozložit H_4 mnoha různými způsoby.



Poslední dva príklady jsou tzv. *cyklický žebřík* CL_n s $2n$ vrcholy, který je složen 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 nejjednoduší „vyvraceč nesprávných úvah“ – graf, na němž se vyplatí testovat tvrzení, než je začneme dokazovat.



9.4

9.4. Morfismy grafů a podgrafy. Jako u všech matematických pojmů, klíčovou roli hrají zobrazení mezi objekty, která zachovávají uvažovanou strukturu.

Definice. Pro grafy grafy $G = (V, E)$ a $G' = (V', E')$ budeme za morfismus $f : G \to G'$ považovat zobrazení $f_V : V \to V'$ mezi množinami vrcholů takové, že je-li $e = \{v, w\}$ hrana v E, pak $e' = \{f(v), f(w)\}$ 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 $f_E : E \to E'$, $f(e) = e'$, 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, taková hrana je 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 V pomocí m různých jmen uzlů K_m tak, že stejně obarvené uzly nejsou spojeny hranou. Hovoříme v tomto případě o *barvení grafu* pomocí m barev.

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.

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.

Jednoduchými a mimořádně užitečnými příklady morfismů grafů jsou pojmy *cesta*, *sled* a *kružnice* v grafu:

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). *Sled délky* n v grafu G je jakýkoliv morfismus $s : P_n \to G$ (tj. v obrazu se mohou opakovat vrcholy).

Sled si můžeme představit jako dráhu „přičinlivého ale tápajícího“ poutníka z uzlu $f(v_0)$ do uzlu f_{v_n}. Poutník se totiž v žádném uzlu nezastaví, ale klidně se po cestě grafem vrací do uzlů nebo i dokonce po hranách, kterými dříve šel. Cesta je naopak průchod grafem z počátečního uzlu $f(v_0)$ do koncového $f(v_n)$ bez takových zbytečných oklik.

Obrazy cest i sledů jsou příkladem tzv. *podgrafů*, ne však stejným způsobem. Definujme nejprve obecně, co je to podgraf.

Uvažujme graf $G = (V, E)$ a nějakou podmnožiny $V' \subset V$. *Indukovaný podgraf* je graf $G' = (V', E')$, kde $e \in E$ patří i do E' právě, když oba krajní vrcholy hrany e patří do V'. *Podgraf* $G' = (V, E')$ je takový graf, který má stejnou množinu vrcholů jako G, ale jeho množina hran E' je libovolnou podmnožinou. Obecně můžeme pro konstrukci podgrafu použít oba procesy – napřed zvolíme $V' \subset V$ a pak v indukovaném podgrafu vybereme cílovou množinu hran E'. Úplně formálně tedy dostáváme:

Definice. Graf $G' = (V', E')$ je podgrafem v grafu $G = (V, E)$, jestliže $V' \subset V$, $E' \subset E$.

Snadno je vidět, že každý obraz homomorfismu (tj. obraz jak vrcholů tak hran) tvoří podgraf. Podgraf, který je homomorfním obrazem cesty nazýváme také cestou. Je zřejmé, každá taková cesta o $n \geq 2$ vrcholech v grafu vzniká právě dvěma způsoby jako homomorfní obraz P_n, které se liší v počátečním a koncovém uzlu. Naopak, jestliže obraz sledu obsahuje k uzlů, můžeme obecně pro $n > k$ najít nepřeberně způsobů, jak takový obraz obdržet.

Kružnice v grafu G je injektivním homomorfním obrazem grafu C_n v G. Všimněte si, že sama kružnice C_n je také homomorfním obrazem cesty P_n, kdy první a poslední bod cesty zobrazíme do téhož vrcholu a zvolíme orientaci cesty.

Najděte si v předchozích obrázcích cesty nebo kružnice obsažené ve větších grafech.

9.5

9.5. Kolik je vlastně neizomorfních grafů? Odpovědět přesně je děsně těžké. Odhadnout, že je neizomorfních grafů moc, je poměrně snadné:

Všech možných grafů na n vrcholech je tolik, kolik je všech podmnožin v množině všech hran. Všech podmnožin o mohutnosti N je 2^N. Isomorfních grafů nemůže být víc, než kolik je

bijekcí na n vrcholech. 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 (s využitím zjevného vztahu $n! \leq n^n$)

$$\log_2 k(n) = \binom{n}{2} - \log_2 n! \geq \frac{n^2}{2}\left(1 - \frac{1}{n} - \frac{2\log_2 n}{n}\right)$$

Pro $n \to \infty$ tedy zjevně dostáváme

$$\log_2 k(n) = \frac{1}{2}n^2 - O(n \log_2 n)$$

viz terminologii pro odhady z 8.38. To znamená, že počet neizomorfních grafů na n uzlech roste asymptoticky stejně rychle jako množství všech možných grafů, tj. číslo $2^{\binom{n}{2}}$. Můžeme to nepřesně formulovat tak, že velká většina všech možných grafů bude po dvou neizomorfní.

9.6. Příklad.

9.6.1. *Určete, kolik existuje homomorfismů grafů*

a) *z P_2 do K_5,*
b) *z K_3 do K_5*

Řešení.

a) $5 \cdot 4 \cdot 4 = 80$.
b) $5 \cdot 4 \cdot 3 = 60$.

Jediné omezení je, že se uzly mezi kterými vede hrana nesmí zobrazit na tentýž uzel. □

9.6

9.7. Stupně uzlů a skóre grafu. Izomorfní grafy se od sebe liší pouze přejmenováním vrcholů. Proto musí mít stejné všechny číselné charakteristiky, které se přešíslováním vrcholů nemění. Jednoduché údaje tohoto typu můžeme dostat sledováním počtů hran vycházejících z jednotlivých vrcholů.

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 $V = (v_1, \ldots, v_n)$ je posloupnost

$$(\deg v_1, \deg v_2, \ldots, \deg v_n)$$

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.

Zajímají nás samozřejmě také kritéria, jaká skóre mohou vůbec grafy mít. Protože každá hrana vychází ze dvou vrcholů, musí být v celkovém součtu skóre započtena každá hrana dvakrát. Proto platí

e9.1

$$\sum_{v \in V} \deg v = 2|E|. \tag{9.1}$$

Zejména tedy musí být součet všech hodnot skóre sudý.

Následující věta je naší první úvahou o operacích nad grafy. Protože je důlaz konstruktivní, jde vlastně o návod, jak pro dané skóre buď zjistit

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 zadaným skóre, pak můžeme přidat ke grafu G' nový vrchol v_n a spojit jej hranou s posledními d_n uzly 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 uzel v_n je spojen hranou právě s posledními d_n uzly $v_{n-d_n}, \ldots, v_{n-1}$.

Idea je jednoduchá — pokud některý z posledních d_n uzlů 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_j 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 největší index vrcholu, který není spojen hranou s v_n. Nechť G je nyní pevně zvolený graf s $\nu(G)$ nejmenším možným. Pak buď je $\nu(G) = n - d_n - 1$ a tedy jsme získali požadovaný graf nebo je $\nu(G) \ge n - d_n$.

V posledním případě ale musí být v_n spojen hranou s některým v_i, $i < \nu(G)$. Protože je $\deg v_{\nu(G)} \ge \deg v_i$, nutně existuje také hrana spojující $v_{\nu(G)}$ s v_ℓ pro $\ell < i$. Nyní záměnou hran $\{v_\ell, v_{\nu(G)}\}$ s $\{v_\ell, v_i\}$ a $\{v_i, v_n\}$ s $\{v_{\nu(G)}, v_n\}$ dostáváme graf G' s týmž skóre, ale menším $\nu(G')$, což je spor s naší volbou. (Namalujte si obrázek!)

Nutně tedy platí první z možností a důkaz je hotov. □

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 odečítáme tolikrát jedničku, kolik je největší hodnota d_n. Uspořádáme znovu výsledné skóre 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 uzel a hrany podle toho, jak jsme odečítali jedničky. Zkuste si několik jednoduchých příkladů sami. Důležité upozornění — lgoritmus sestrojuje pouze jeden z mnoha grafů, které mohou k danému skóre existovat!

U orientovaných grafů rozlišujeme *vstupní stupeň* $\deg_+ v$ vrcholu v a *výstupní stupeň* $\deg_- v$. Říkáme, že orientovaný graf je *vyvážený*, když pro všechny uzly platí $\deg_- v = \deg_+ v$.

9.7

9.8. 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 uzlu do uzlu podél

orientovaných hran a přitom zpracováváme informace, které jsou určeny a ovlivněny výsledkem předchozích operací, uzlem, ve kterém se zrovna nacházíme, a hranou, kterou jsme do uzlu 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.

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). Graf $G = (V, E)$ si v něm reprezentujeme jako dva seznamy V a E propojené ukazately tak, že každý vrchol ukazuje na všechny z něj vycházející 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 málo hran, dostáváme tzv. řídkou matici se skoro všemi prvky nulovými. Existují ovšem postupy, jak tyto řídké matice uchovávat v paměti efektivněji.

Promyslete si podrobně, 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*

Jako jednoduchou aplikaci maticového počtu si uvedeme následující tvrzení:

9.8 **9.9. Věta.** *Nechť $G = (V, E)$ je graf s uspořádanými vrcholy $V = (v_1, \ldots, v_n)$ 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. Tvrzení je pouze jiným vyjádřením definice matice sousednosti pro případ $k = 1$ a celý důkaz povedeme indukcí přes délku k. Předpokládejme tedy, 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 uzlu v_ℓ a nějakého sledu délky k mezi v_ℓ a v_j. Různé volby přitom dávají vždy různé výsledky. Proto, označíme-li $a_{\ell j}^{(k)}$ počet různých sledů délky k z

v_ℓ 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 formulka pro násobení matice A_G s mocninou A_G^k. Dokázali jsme, že naše čísla $a_{ij}^{(k+1)}$ jsou prvky matice A_G^{k+1}. □

Důsledek. *Jsou-li $G = (V, E)$ a A_G jako v předchozí větě, pak lze všechny vrcholy G spojit cestou právě, když má matice $(A + \mathbb{I}_n)^{n-1}$ samé nenulové členy (zde $\mathbb{I}_n$ označuje jednotkovou matici s n řádky a sloupci).*

Důkaz. Díky distributivitě násobení matic a skutečnosti, že jednotková matice I_n komutuje s každou jinou maticí stejného rozměru, dostaneme roznásobením

$$(A + \mathbb{I}_n)^{n-1} = A^{n-1} + \binom{n-1}{1} A^{n-2} + \cdots + \binom{n-1}{n-2} A + I_n.$$

Výsledná matice má za členy čísla (ve značení jako v minulé větě)

$$a_{ij}^{(n-1)} + \binom{n-1}{1} a_{ij}^{(n-2)} + \cdots + \binom{n-1}{\ell} a_{ij}^{(n-1-\ell)} + \cdots + (n-1)a_{ij} + \delta_i j,$$

kde $\delta_{ii} = 1$ pro všechny i a $\delta_{ij} = 0$ pro $i \neq j$.

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. □

9.9 **9.10. Poznámka.** Ještě si všimněme vlivu permutace našeho uspořádání uzlů V na matici sousednosti grafu. Není obtížné si uvědomit, že permutace uzlů grafu G má za následek jednu a tutéž permutaci řádků a 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 parmutační matice, pak nová matice sousednosti izomorfního grafu G' bude

$$A_{G'} = P \cdot A_G \cdot P^T,$$

kde P^T značí transponovanou matici a tečkou označujeme násobení matic. Každou permutaci umíme napsat jako složení transpozic a proto příslušnou permutační matici dostaneme jako součin příslušných matic pro transpozice.

V případě permutačních matic je matice transponovaná zároveň maticí inverzní. Tyto úvahy lze dále rozvíjet a přemýšlet o souvislostech matic sousednosti a matic lineárních zobrazení mezi vektorovými prostory. Nebudeme zde zacházet do podrobností.

9.10 **9.11. Prohledávání v grafu.** Mnoho užitečných algoritmů je založeno na postupném prohledávání všech 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*, tj. ty, které jsme již při běhu algoritmu procházeli a definitivně zpracovali;
- *aktivní*, tj. ty vrcholy, které jsou detekovány a připraveny pro zpracovávání;
- *spící*, tj. 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 tedy máme jeden aktivní vrchol a všechny ostaní 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 algortimů 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:

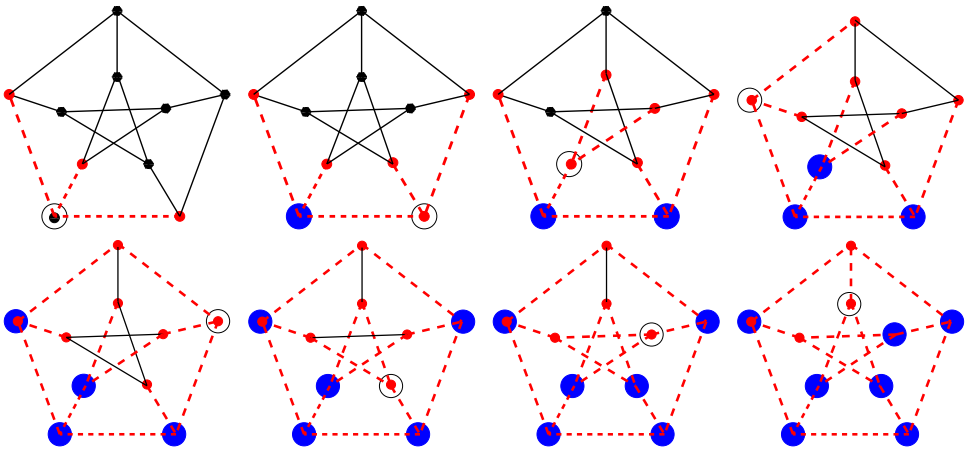
(1) vrcholy vybíráme pro další zpracování ve stejném pořadí, jak se stávaly aktivními (fronta)
(2) dalším vrcholem vybraným pro zpracování je poslední zaktivněný vrchol (zásobník).

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 v čase $O((n+m)*K)$, 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.*

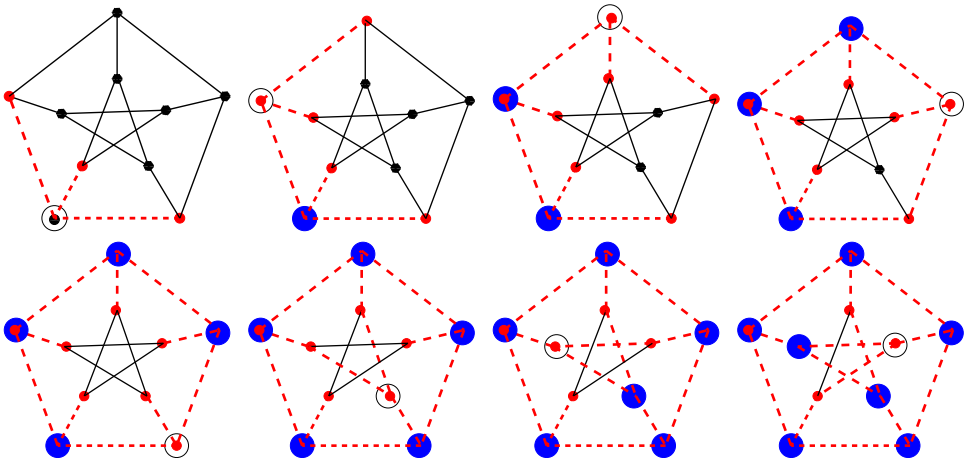
Následující obrázky slouží pro ilustraci prohledávání do šířky a do hloubky:



Je na nich zachyceno prvních osm kroků prohledávání do šířky Petersenova grafu na 10 vrcholech.

Zakroužkovaný vrchol je ten právě zpracovávaný, modré velké puntíky jsou již zpracované uzly, čárkované červené hrany jsou již zpracované a červené drobné uzly jsou ty aktivní (poznají se také podle toho, že do nich již vede některá zpracovaná hrana). Hrany zpracováváme v pořadí orientace proti hodinovým ručkám, přičemž za „první“ bereme směr „kolmo dolů“.

Totéž je dalších obrázcích postupem „do hloubky“. Všimněte si, že první krok je stejný jako v předchozím případě.



9.11

9.12. 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 $G_{[v]} \subset G$ a disjunktní sjednocení těchto podgrafů je ve skutečnosti původní graf G. Skutečně, podle definice naší ekvivalence, žádná hrana původního grafu nemůže

propojovat uzly z různých komponent. Podgrafům $G_{[v]}$ říkáme *souvislé komponenty grafu* G.

Je-li graf G orientovaný, pak postupujeme úplně stejně, pouze u definice relace výslovně požadujeme aby cesta existovala z uzlu v do uzlu w nebo naopak z uzlu w do uzlu v.

Jako skutečně jednoduchý příklad prohledávání v grafu si můžeme uvést algoritmus na vyhledání všech souvislých komponent v grafu. Jedinou informací, kterou musíme zpracovávat je, kterou komponentu aktuálně procházíme. Samotné prohledávání, tak jak jsme jej prezentovali, projde právě všechny vrcholy jedné komponenty. 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.

Definice. Řekneme, že graf $G = (V, E)$ je

- *souvislý*, jestliže má právě jednu souvislou komponentu;
- *vrcholově k–souvislý*, jestliže má alespoň $k + 1$ vrcholů a bude souvislý po odebrání libovolné podmnožiny $k - 1$ vrcholů;
- *hranově k–souvislý*, jestliže bude souvislý po odebrání libovolné podmnožiny $k - 1$ hran.

Případ $k = 1$ v definici jen opakuje souvislost grafu G. 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 lze dokázat tvrzení tzv. *Mengerovy věty*, kterou teď nebudeme dokazovat:

Tvrzení. *Pro každé dva vrcholy v a w v grafu $G = (V, E)$ je 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.*

Speciálním případem je 2–souvislý graf. To je takový souvislý graf o alespoň třech vrcholech, kdy vynecháním libovolného vrcholu nenarušíme jeho souvislost. Na tomto příkladu si odvodíme několik pěkných charakterizací:

Věta. *Pro graf $G = (V, E)$ s alespoň třemi vrcholy jsou následující podmínky ekvivalentní:*

- *G je 2–souvislý;*
- *každé dva vrcholy v a w v grafu G leží na společné kružnici;*
- *graf G je možné vytvořit z trojúhelníku K_3 pomocí postupných dělení hran.*

Důkaz. Na jednu stranu je implikace zřejmá: Jestliže každé dva vrcholy sdílejí kružnici, pak jsou mezi nimi vždy alespoň dvě různé cesty a tedy odebrání vrcholu nemůžeme pokazit souvislost.

Opačná implikace není o mnoho složitější. Budeme postupovat indukcí podle minimální délky cesty spojující vrcholy v a w. Pokud vrcholy sdílí hranu e, pak díky 2–souvislosti je i graf bez této hrany souvislý a je v něm proto cesta mezi v a w. Spolu s hranou e tato cesta vytváří kružnici. Předpokládejme, že umíme takovou sdílenou kružnici sestrojit pro všechny vrcholy spojitelné cestou délky nejvýše k a uvažujme vrcholy v a w a je spojující nejkratší cestu $(v = v_0, e_1, \ldots, v_k = w)$ 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 cesta, která vznikne složení 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!). □

9.12

9.13. Metrika na grafech. V posledním důkazu jsme používali délku cest pro měření „vzdálenosti“ vrcholů. Ukážeme, že takto skutečně lze matematicky vybudovat pojem vzdálenosti na grafu:

Na každém (neorientovaném) grafu definujeme *vzdálenost uzlů* 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 graf G. Pak pro takto zadanou funkci $d_G : V \times V \to \mathbb{N}$ platí obvyklé tři vlastnosti vzdálenosti:

- $d_G(v,w) \geq 0$ 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 standardních tří 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 a 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 lze nadefinovat hrany E tak, aby $G = (V,E)$ byl graf s metrikou d_G. Zkuste si ukázat jako cvičení!

9.13

9.14. Dijkstrův algoritmus pro hledání nejkratších cest. Dá se tušit, že nejkratší cestu v grafu, která vychází z daného uzlu v a končí v jiném uzlu 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 v realističtější podobě, kdy jednotlivé hrany e jsou ohodnoceny „vzdálenostmi“, tj. kladnými reálnými čísly $w(e)$. Kromě aplikace na hledání vzdáleností v silničních nebo jiných sítích to mohou být také výnosy, 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 podstatné, že všechna naše ohodnocení jsou kladná. Zkuste si rozmyslet třeba cestu P_3 se záporně ohodnocenou prostřední hranou. Při procházení sledu mezi krajními vrcholy bychom

„vzdálenost“ zmenšovali každým prodloužením sledu o průchod prostřední hranou tam a zpět.

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. $d(v) = d_w(v)$.
- 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 rovno ∞, algoritmus končí, v opačném případě pokračujeme dalším krokem. (Algoritmus tedy zejména končí, pokud je $Z = \emptyset$.)

(3) *Aktualizace statutu 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.

9.14 **9.15. Věta.** *Pro všechny vrcholy v v souvislé komponentě vrcholu v_0 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 grafu G.*

Důkaz. Napřed ukážeme správnost algoritmu, tj. budeme muset ověřit, že

- algortimus po končeném 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

e9.1 (9.2) $$d(v) \geq d_w(v)$$

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

$$d_w(y) \le d_w(v) + w(\{v,y\}) \le d(v) + w(\{v,y\}) = d(y),$$

kde napravo již máme nově změněnou hodnotu.

Rovnost (9.2) 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. Označme si $0 = d_0 < \cdots < d_k$ všechny existující různé konečné vzdálenosti $d_v(v)$ 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 δ 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 $\cup_{i=0}^{j} V_i = V \setminus N$. 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

e9.2 (9.3) $$d_w(v_\ell) \le d_{j+1} - w(\{v_\ell, y\}) < d_{\ell+1}$$

Podle našeho předpokladu tedy již dříve (v některém z předchozích průchodů hlavním cyklem) byl vrchol v_ℓ aktivní a tedy již v tom průchodu bylo jeho ohodnocení rovno $d_w(v_\ell) = d(v_\ell) = d_i$ pro některé $i \le j$. Proto při stávajícím průchodem 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 (9.2) 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 struktruře umožňující vyhledání množiny N aktivních vrcholů v čase $O(\log n + |N|)$. To lze dosáhnout datovou strukturou, které se říká halda. Každá hrana bude právě jednou zpracovávána v kroku 4 protože vrcholy jsou aktivní pouze při jednom průchodu cyklem. □

Všimněme si, že pro nerovnost (9.3), 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 $d^0_w(v)$ vrcholů v a v_0 takové, že pro všechny hrany $e = \{v, y\}$ platí

$$|d^0_w(v) - |d^0_w(y)| \le w(e)$$

a tato nerovnost nám stačí pro důkaz správnosti algoritmu.

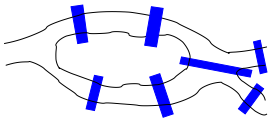
9.15

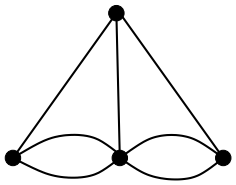
9.16. Eulerovy sledy a Hamiltonovy kružnice. Každý si asi pamatujeme na hříčky typu „nakreslete obrazek jedním tahem“.

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 sled* a souvislým grafům, které takový sled připouští říkáme *eulerovské*.

Eulerovský sled 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 sled. 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 Leonharta Eulera z roku 1736.





Situace je znázorněna na obrázku. 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 vstupujeme. Proto nutně musí být stupeň každého vrcholu sudý. Kdo důkaz této implikace formalizovanější, může uvážit kružnici, která 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 $(v_0, e_1, \dots, v_k)$ v G bez opakujících se hran. Předpokládejme na okamžik, že $v_k \ne v_0$. To znamená, že do v_0 vchází nebo vychází v tomto sledu jen lichý počet hran a tedy jistě existuje nějaká hrana vyházející 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 $V' \ne V$, 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 $E' = E$. Předpokládejme, že by hrana $e = \{v, w\} \notin V'$. 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. □

Obdobný požadavek na průchod grafem, ovšem tak, abychom prošli právě jednou každým vrcholem (tj. zároveň nejvýše jednou každou hranou), vede 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. Lze ukázat, že neexistuje algoristmus, který by v polynomiálním čase rozhodnul, zda je graf hamiltonovský.

Problém nalezení hamiltonovské kružnice je podstatou mnoha problémů v logistice, tj. když řešíme optimální cesty při dodávkách zboží.

9.17. Příklady.

9.17.1. *Dokažte, že vrcholový graf 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 uzly dvě neprotínající se cesty („oblouky“ hamiltonovské kružnice). Odstraněním jednoho bodu, se tedy zjevně neporuší souvislost grafu (odstraněný bod může ležet pouze na jedné ze dvou cest). □

9.17.2. *Dokažte nebo vyvraťte:*

a) *Každý graf s méně než devíti hranami je rovinný.*
b) *Graf, který není rovinný, není ani hamiltonovský.*
c) *Graf, který není rovinný, je hamiltonovský.*
d) *Graf, který není rovinný, není eulerovský.*
e) *Graf, který není rovinný, je eulerovský.*
f) *Každý hamiltonovský graf je rovinný.*
g) *Každý eulerovský graf je rovinný.*

Řešení.

a) Ano. Triviální důsledek charakterizace rovinných grafů ($K_{3,3}$ i K_5 mají minimálně 9 hran)
b) Ne. ($K_{3,3}$)
c) Ne. (k libovolnému nerovinnému grafu přidáme jeden vrchol a ten spojíme jedinou hranou s libovolným vrcholem původního grafu)

d) Ne. (Protipříklad K_5)
e) Ne. ($K_{3,3}$)
f) Ne. (K_5)
g) Ne. (K_5)

□

9.16

9.18. 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 samozřejmě je vždy možné, dokud je v grafu alespoň jedna kružnice.

Souvislý graf, ve kterém není žádná kružnice, se nazývá *strom*. Graf neobsahující kružnice nazýváme *les* (nepožadujeme přitom souvislost grafu). Můžeme tedy formulovat matematickou větu: „Strom je souvislý les."

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. Pro důkaz existence listů opět použijeme cestu nejdelší možné délky v grafu G. Nechť $P = (v_0, \dots, v_k)$ je taková cesta. Pokud by v_0 nebyl list, pak by z něj vedla hrana e s druhým koncovým vrcholem v, který nemůže být vrhcolem 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 totž platí o v_k.

Předpokládejme nyní, že v je list stromu G. Uvážíme-li libovolné dva jiné vrcholy w, z v 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 odbrání v zůstane graf spojitý. Samozřejmě v něm nemůže být kružnice, když ze stromu vzniknul odebráním vrcholu.

Je-li naopak $G \setminus v$ strom, nemůže přídání 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:

9.17

9.19. 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 v do w;*
(3) *graf G je souvislý, ale vyjmutím libovolné hrany vznikne nesouvislý graf*
(4) *graf G neobsahuje kružnici, každým přidáním hrany do grafu G však již 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 sformulovat než dokázat.

Dokážeme nejprve, že vlastnosti 2–5 platí pro stromy. Každý strom o alespoň dvou vrcholech má 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.

Pro důkazy opačných implikací opět nemusíme dělat mnoho. V případě vlastností 2 a 3 pracujeme se souvislým stromem 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 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 vzniknul přidáním listu ke stromu. □

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.

9.18

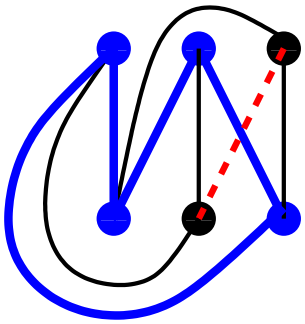
9.20. Rovinné grafy. Velice často se setkáváme s grafy, které jsou nakresleny v rovině. To znamená, že každý vrchol grafu je ztotožněn s nějakým bodem v rovině a hrany mezi vrcholy v a w odpovídají spojitým křivkám $c : [0,1] \to \mathbb{R}^2$ spojujícím vrcholy $c(0) = v$ a $c(1) = w$.

Pokud navíc platí, že se jednotlivé dvojice hran protínají nejvýše v koncových vrcholech, pak 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 rodinných domků. Chtějí je všichni 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 bipartitní úplný 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 alespoň naznačíme:

Můžeme se opřít o docela pracně dokazatelný topologický výsledek, 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. Protože jsou v grafu $K_{3,3}$ jednotlivé vrcholy v každé z trojic vrcholů nespojených hranami stejné, až na volbu pořadí, můžeme naši modrou silnou kružnici považovat za obecný případ kružnice 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 modrými silnými a dvěma černými hranami (tj. přes tři modré 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. Obecně se dá dokázat tzv. Kuratowského věta:

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 a aplikacích hodně pozornosti, my se zde omezíme pouze na vybrané ilustrace.

Zmiňme alespoň naokraj, že existují algoritmy, které testují rovinatost grafu na n vrcholech v čase $O(n)$, což určitě nejde přímou aplikací Kuratowského věty.

9.19

9.21. Stěny v rovinných grafech. Uvažme (konečný) 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 příklad si můžme 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

$$|V| - |E| + |S| = 2.$$

Vztah mezi počty hran, stěn a vrcholů lze odvodit pro všechny rovinné grafy. Jde o tzv Eulerův vztah. 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. Pokud G neobsahuje kružnici, tj. jde o strom, tvrzení jsme již dokázali v 9.19(5), protože každý strom má zjevně pouze jedinou stěnu S_0.

Předpokládejme dále, že hrana e v grafu G je obsažena v kružnici. Pak je i graf $G' \setminus e$ souvislý. Můžeme tedy postupovat indukcí přes počet hran. Graf s jedinou hranou vztah splňuje a jestliže jej splňuje i G', pak to znamená

$$|V| - |E| + 1 + |S| - 1 = 2$$

protože s odebráním jedné hrany dojde nutně i k propojení právě dvou stěn grafu G do jedné v G'. □

9.20

9.22. 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 hvořit o stěnách a pro takovýto graf pak jsou všechny jeho stěny rovnocenné (i stěna S_0 je ohraničená).

Naopak, každý konvexní mnohostěn $P \subset \mathbb{R}^3$ 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 stane neohraničenou stěnou S_0) pak obdržíme rovinný graf jako výše tak, že „proděravěnou sféru natáhneme do roviny“.

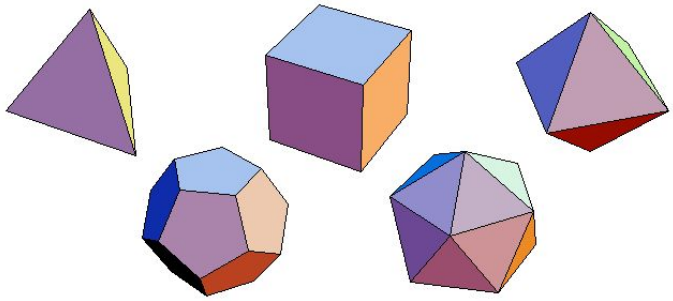
Rovinné grafy, které vzniknou z konvesních mnohočlenů zjevně 2–souvislé, protože každé dva vrcholy v konvexním mnohoúhelníku leží na společné kružnici. Navíc v nich platí, že každá stěna kromě S_0 je vnitřkem nějaké kružnice a S_0 je vnějškem nějaké kružnice (při kreslení na sféře jsou všechny stěny vnitřek nějaké kružnice). Názorné se zdá i to, že ve skutečnosti budou grafy vznikající z konvexních mnohoúhelníků 3–souvislé.

Ve skutečnosti platí dosti náročná Steinitzova věta:

Věta. *Libovolný vrcholově* 3*–souvislý rovinný graf* G *vzniká z konvexního mnohostěnu v* $\mathbb{R}^3$.

9.21

9.23. 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 každá 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:

$$dn = 2e$$

a podobně počítáme počet hran, které ohraničují jednotlivé stěny, a bereme v úvahu, že každé je hranicí dvou stěn, tj.

$$2e = ks.$$

Eulerův vztah pak říká

$$2 = n - e + s = \frac{2e}{d} - e + \frac{2e}{k}.$$

Úpravou odtud dostáváme pro naše známé d a k vztah

$$\frac{1}{d} + \frac{1}{k} = \frac{1}{2} + \frac{1}{e}.$$

Protože nejen d a k, ale také e a n musí být přirozená čísla (tj. zejména je $\frac{1}{e} > 0$), dostáváme z této rovnosti velice silné omezení možností. Dosadíme-li minimální možnou hodnotu $d = 3$, obdržíme drobnou úpravou nerovnost

$$-\frac{1}{6} + \frac{1}{k} = \frac{1}{e} > 0.$$

Odtud vyplývá $k, d \in \{3, 4, 5\}$ a dopočítáním ostatních hodnot pro jednotlivé možnosti těcho hodnot dostáváme následující výčet všech možností 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

Ve skutečnosti ale také všechny odpovídající pravidelné mnohostěny existují - již jsme je viděli na obrázcích výše. U prvních třech jistě nejsou pochybnosti, naznačíme pro ilustraci konstrukci dvanáctistěnu (malujte si přitom obrázek). Začneme s krychlí a na všech jejích stěnách budeme zaráz 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 zaráz stejně všechny stany při zachovávání poměrů tří stran lichoběžníku. Jistě nastane právě jednou okamžik, ve kerém budou sousední lichoběžníkové a trojůhelníkové stěny koplanární (tj. v jedné rovině). Tak vznikne pravidelný dvanáctistěn.

Zkuste si sestrojit dvacetistěn jako cvičení.

9.24. Příklady.

9.24.1. *Kolik minimálně hran může mít šestistěn?*

Řešení. V libovolném mnohostěnu je každá stěna ohraničena minimálně třemi hranami. Každá hrana pak leží ve dvou stěnách. Označíme-li s počet stěn a h počet hran mnohostěnu dostáváme tak odhad $3s \leq 2h$. 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 moľný počet hran šestistěnu je tedy devět. □

2. Aplikace kombinatorických postupů

I v této části budeme nejprve pokračovat v úvahách založených na grafových postupech.

9.22

9.25. 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.

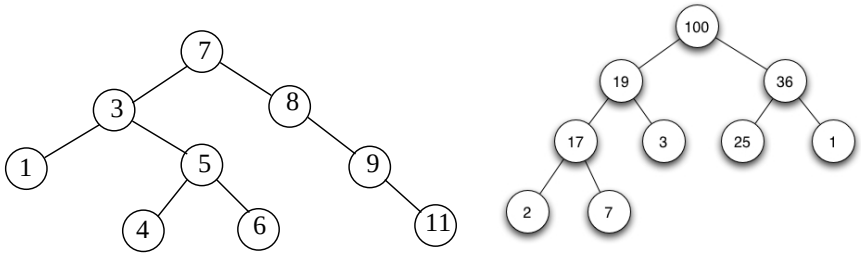
Situace se tedy po výběru jednoho vrcholu začíná více podobat skutečnému stromu v přírodě – jeden jeho vrchol je výjimečný tím, že roste ze země. Stromy s jedním vybraným „počátečním“ vrcholem nazýváme *kořenové stromy*, význačný vrchol v_r je *kořen stromu*.

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 ve 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 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 konstatním 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 (který ale není vyvážený), napravo je příklad maximální haldy.

9.23

9.26. Izomorfismy stromů. Stromům, jejich různým variantám a použití je věnována obsáhlá literatura. My se zde už pouze na chvíli zamyslíme nad obecným 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 ν je částečné uspořádání na hranách takové, že srovnatelné jsou vždy právě hrany směřující od jednoho otce k synům.

Morfismem 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 ν a ν'.

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 má-li otec v syny uspořádány jako posloupnost $v_1, \dots, v_\ell$, a jsou-li již jednotliví synové označeni slovy $W_1, \dots W_\ell$, pak pro otce použijeme slovo

$$0W_1 \dots W_\ell 1.$$

Strom na levém obrázku výše tedy zapíšeme postupně takto (přidáváme postupně vrcholy podle vzdálenosti od kořene, syny máme uspořádány zleva doprava)

$$01,\ 01,\ 01 \mapsto 01,\ 001011,\ 0011 \mapsto 0010010111,\ 000111 \mapsto 000100101110001111.$$

Hovoříme o *kódu pěstěného stromu*. Ověřte si, že skutečně kreslením cest dolů a nahoru (třeba si můžeme představit že dolů 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 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 $W = W_1W_2 \dots W_\ell$. 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 uspořádní synů podle jejich kódů. Tzn. že kód $W_1 > W_2$ jestliže buď ve W_1 narazíme při čtení z leva 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 $W_1, \dots W_\ell$, pak pro otce použijeme slovo

$$0W_1 \dots W_\ell 1$$

kde pořadí $W_1, \dots, W_\ell$ je zvoleno tak aby $W_1 \le W_2 \le \dots \le W_\ell$.

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*. 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 maximální hodnoty excentricity vždy dosahuje buď právě jeden vrchol nebo právě dva vrcholy. Skutečně, nejdelší možná cesta z kteréhokoliv vrcholu stromu nutně končí v některém z jeho listů. Pro strom na dvou vrcholech tvrzení platí a u stromu na $n \ge 3$ vrcholech odebráním listů dostaneme strom menší, u nějž se excentrity všech vrcholů, které zůstaly, zmenší právě o jedničku. Tvrzení tedy plyne indukcí podle počtu vrcholů stromu. Navíc je zřejmé, že dva vrcholy s maximální excentricitou musí být spojeny hranou.

Nyní tedy můžeme přiřadit jednoznačný kód, až na izomorfismus i každému stromu. Pokud existuje jediný vrchol s maximální excentricitou, použijeme jej jako kořene, v opačném případě postupujeme stejně pro dva stromy vzniklé z T odebráním hrany spojující vrcholy s maximální excentricitou a kód vznikne zřetězením kódů obou stromů v pořadí podle lexikografického uspořádání.

9.24 **Důsledek.** *Dva stromy T a T' jsou izomorfní právě, když mají společný kód.*

9.27. 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 $G = (V, E)$, $E' \subset E$ se nazývá *kostra* grafu G.

Evidentně může kostra v grafu existovat pouze, pokud je graf G souvislý. Místo formálního důkazu, že platí i opak uvedeme přímo algoritmus, jak kostru grafu sestrojit.

Algoritmus 1. Postupovat můžeme například takto: Seřadíme zcela libovolně všechny hrany $e_1, \dots, e_m$ v E do pořadí a postupně budujeme množiny hran E'_i tak, že v $(i+1)$–vém 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 pokud buď má již graf G_i pro nějaké i právě $n-1$ hran nebo je již $i = m$. 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 pro dosažení $n-1$ 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 9.19.

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 ze jednoho stromu v T ležet všechny v jedné komponentě G. Pokud by ale existovala v G cesta z v do w takové, že její koncové vrcholy leží v různých stromech v T, pak na ní existuje poslední vrchol v_i v komponentě určené v a v_{i+1} v ní 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 zůstavat 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 dán pevným vztahem mezi počtem vrcholů a hran ve stromech. □

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 tříd 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 $O(n \log n + m)$. Dokažte si jako cvičení!

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 prázdnou množinou hran, tj. $T_0 = (\{v\}, \emptyset)$. V i–tém kroku hedáme mezi hranami, které dosud nejsou v T_{i-1}, mají v T_{i-1} jeden koncový vrchol, ale druhý koncový vrchol fo 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 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 lematu na ní najdeme poslední vrchol v_i, který ještě do T patří. Další hrana cesty by ale v okamžiku ukončení algoritimu připadal 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.

9.28. Počet koster úplného grafu. K určení počtu koster úplného grafu o n uzlech může sloužit pojem Prüferovy posloupnosti kostry grafu. Prüferovu posloupnost můžeme přiřadit kostře grafu K_n a to následujícím způsobem: označme vrcholy v grafu K_n postupně od 1 do n a odstraňujme postupně listy dané kostry (od nejmenšího) a s každým odstraněným listem zapíšme do posloupnosti souseda právě odstraněného listu. Opakujeme tak dlouho, dokud v kostře nezbubou pouze dva vrcholy.

Získaná posloupnost má evidentně $n-2$ členů, které mohou nabývat hodnot od 1 do n. Obráceně není těžké dokázat, že pro každou takovou posloupnost existuje právě jedna kostra grafu K_n, která se do této posloupnosti výše popsaným postupem zakóduje.

Celkem dostáváme, že existuje právě n^{n-2} různých koster grafu K_n.

9.29. Příklady.

9.29.1. *Kolik existuje různých koster 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 různých koster, což souhlasí s obecným vzorcem pro počet koster úplného grafu. □

9.25

9.30. Minimální kostra. Protože je to obecnou vlastností stromů, každá kostra grafu G má stejný počet hran. 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 ohodnocenými hranami s nezápornými vahami $w(e)$ pro všechny hrany. Jeho *minimální kostra* T je taková kostra grafu G, která má mezi všemi jeho kostrami minimální součet ohodnocení všech hran.

O praktičnosti takové úlohy můžete přemýšlet třeba v souvislosti s rozvodnými sítěmi elektřiny, plynu, vody apod.

Kupodivu je docela jednoduché minimální kostru najít za 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 „hladoveckého přístupu“, kdy se k maximalizaci zisku (nebo minimalizaci nákladů) snažíme dostat výběrem momentálně (snad) nejvýhodnějšího kroku. Často tento přístup zklame, protože nízké náklady na začátku procesu mohou zavinit vysoké na jeho konci. 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. POZDEJI ??? □

9.26

9.31. Další algoritmy pro minimální kostru. I druhý z našich algoritmů pro kostru grafu v předchozím odstavci vede na minimální kostru, když v každém okamžiku volíme ze všech možných hran $e_i = \{v_i, v_{i1+}\}$, $v_i \in V_i$, $v_{i+1} \in V \setminus v_i$ 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. 1928.

Věta. *Jarníkův algoritmus najde minimální kostru pro každý souvislý graf s libovolným ohodnocením hran.*

Důkaz. POZDEJI ??? □

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 takto obdržíme minimální kostru. V pseudokódu by šel tento algoritmus zapsat následovně:

(1) *Inicializace.* Udělej graf S složený z vrcholů grafu G;
(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;

9.32. Příklady.

9.32.1. *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.*

Řešení. Postup není správný. Stačí uvážit například kružnici s hranami ohodnocenými až na jednu jedničkami, zbývající hrana ohodnocená dvojkou. □

9.32.2. *Máme dánu následující tabulku vzdáleností světových metropolí: Londýna, Mexico City, New Yorku, Paříže, Pekingu a Tokia:*

	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

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).

Řešení. Aplikací algoritmu na hledání minimální kostry zjistíme, že hledaná délka je 12154. (v kostře jsou hrany LPe, LP, LNY, PeT, MCNY). □

9.32.3. *Určete počet podgrafů 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 5 grafů.
- $v = 2$. Dva vrcholy můžeme vybrat $\binom{5}{2}$ způsoby, mezi vybranými vrcholy pak buď vede nebo nevede hrana. Celkem $\binom{5}{2}2$ 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.
- $v = 4$. $\binom{5}{4} \cdot 2^{\binom{4}{2}}$ grafů.
- $v = 5$. $\binom{5}{5} \cdot 2^{\binom{5}{2}}$ grafů.

Celkem 1550 podgrafů grafu K_5. □

9.32.4. *Určete počet kružnic v grafu K_5.*

Řešení. Počet kružnic spočítáme postupně podle jejich délky. Nejkratší kružnice může mít délku 3, nejdelší kružnice v K_5 pak délku pět. Kružnice je určena svými vrcholy, tak jak v ní jdou popořadě, přičemž je jedno, který vrchol prohlásíme za počáteční a který za koncový. Počet kružnic je tedy $5{\cdot}4{\cdot}3/3{\cdot}2{+}5{\cdot}4{\cdot}3{\cdot}2/4{\cdot}2{+}5!/5{\cdot}2 = 10 + 15 + 12 = 37$. □

9.32.5. *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 v daném pořadí dva vrcholy, přes které cesta půjde), 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. □

9.32.6. *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. □

9.32.7. *Označme vrcholy v grafu K_6 postupně čísly* $1, 2, \dots 6$ *a každou hranu* $\{i, j\}$ *ohodnoťme číslem* $[(i + j) \bmod 3] + 1$. *Kolik existuje různých maximálních koster v tomto grafu?*

Řešení. Hrany s ohodnocením tři tvoří kruľnici 23562 délky čtyři a hranu 14. Jde tedy o nesouvislý podgraf daného grafu. Není tedy moľné 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 můľeme vybrat. Z hran s ohodnocením 3 můľeme vypustit libovolnou hranu ze zmiňované kruľnice 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. □

9.32.8. *Označme vrcholy v grafu K_7 postupně čísly* $1, 2, \dots 7$ *a každou hranu* $\{i, j\}$, *ohodnoťme číslem* $[(i + j) \bmod 3] + 1$. *Kolik existuje různých minimálních koster v tomto grafu?*

Řešení. 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 $6 \times 1 + 2 = 8$. 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 kruľnice a to délky 4, přičemľ kaľdá ze šesti hran této komponenty leží právě ve dvou kruľnicích. Abychom z dané komponenty získali strom, musíme dvě hrany vypustit, to můľeme udělat $6 \cdot 4/2$ způsoby. Celkem dostáváme $12 \cdot 6 = 72$ různých minimálních koster. □

9.32.9. *Označme vrcholy v grafu K_7 postupně čísly* $1, 2, \dots 7$ *a každou hranu* $\{i, j\}$, *ohodnoťme číslem* $[(i + j) \bmod 3] + 1$. *Kolik existuje různých maximálních koster v tomto grafu?*

Řešení. Nejdraľší hrany s ohodnocením tři tvoří v daném grafu podgraf obsahující všechny vrcholy a mající dvě komponenty a to dvě kruľnice délek tři a čtyři. Pouze z hran s tímto ohodnocením tedy maximální kostru nesloľíme. Bude v ní tedy minimálně jedna levnější hrana. Kostry s právě jednou hranou s ohodnocením 2 pak skutečně existují. Existuje šest hran s ohodnocením 2 propojující dvě zmíněné komponenty. Abychom dostali kostru, musíme ještě vypustit po jedné hraně z kaľdé z kruľnic. To můľeme udělat $3 \cdot 4 = 12$ způsoby. Celkem máme 72 různých maximálních koster. □

9.32.10. *Označme vrcholy v grafu K_5 postupně čísly* $1, 2, \dots 5$ *a každou hranu* i, j, $i = 1, \dots, 5$ *ohodnoťme číslem* 1, *pokud je* $(i + j)$ *liché, číslem* 2, *pokud je* $(i + j)$ *sudé. Kolik existuje různých maximálních koster v tomto grafu?*

Řešení. 18. □

9.32.11. *Označme vrcholy v grafu K_5 postupně čísly* $1, 2, \dots 5$ *a každou hranu* $\{i, j\}$, $i = 1, \dots, 5$ *ohodnoťme číslem* 1, *pokud je* $(i + j)$ *liché, číslem* 2, *pokud je* $(i + j)$ *sudé. Kolik existuje různých minimálních koster v tomto grafu?*

Řešení. 12. □

9.32.12. *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?*

Řešení. 16. □

9.32.13. *Označme vrcholy v grafu K_6 postupně čísly* 1, 2,... 5 *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?*

Řešení. 16. □

9.27

9.33. 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, teoretické výsledky pouze ukazují, že algoritmus fungující alespoň v polynomiálním čase neexistuje a používají se takové, které dávají výsledky rozumně dobré, nikoliv však optimální.

Jedním z nejsledovanějších takových kombinatorických problémů je úloha, kdy máme najít v grafu s ohodnocenými hranami 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 např. 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. při kladení tapet jejich dělení na použité pásy tak, aby navazoval vzorek a došlo k co nejmenším ztrátám)

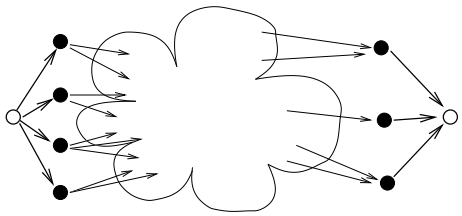
I v případě hledání minimální hamiltonovské kružnice můžeme uplatnit hladovecký (anglicky „greedy“) přístup. Algoritmus začne v libovolném vrcholu v_1, který se stane aktivním a všechny ostatní si označí za spící. Postupuje pak postupně v krocích tak, že vždy najde ten dosud neumístěný vrchol z spících, do kterého vede z aktivního vrcholu nejméně ohodnocená hrana, aktivní vrchol označí jako zpracovaný, tento nový vrchol se stane aktivním. Algoritmus skončí buď neúspěchem, když nenajde žádnou hranu z aktivního uzlu do spícího uzlu, ale hamiltonovská kružnice ještě nebyla nalezena, nebo využitím všech vrcholů. Pokud ve druhém případě existuje hrana z posledního přidaného uzlu 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. Je dokázáno, že se dokonce polynomiálně rychlými algoritmy nelze libovolně přibližovat k optimálnímu řešení.

9.28

9.34. 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.



Definice. 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 $w : E \to \mathbb{R}$. *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.

$$\sum_{e \in IN(v)} f(e) = \sum_{e \in OUT(v)} f(e).$$

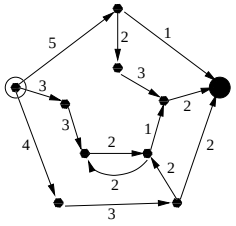
Velikost toku f je dána celkovou balancí hodnot u zdroje

.

Z definice je zřejmé, že velikost toku můžeme stejně dobře vypočíst jako hodnotu

$$|f| = \sum_{e \in IN(s)} f(e) - \sum_{e \in OUT(v)} f(e).$$

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.



9.29

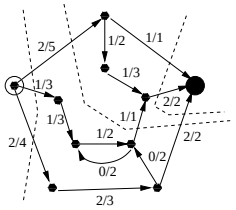
9.35. Problém maximálního toku v síti. Naší úlohou bude pro zadanou síť na grafu G určit maximální možný tok. Na konci minulého odstavce jsme pohledem na obrázek zjistili, že maximální tok v této síti nemůže přesáhnout číslo 5. Podstatné na naší úvaze bylo, že jsme sečetli hodnoty maximálních kapacit u množiny hran, pres které musí jít každá cesta ze z do s. Zároven umíme snadno najít tok, který toto maximum skutecne realizuje (protože je naše sít tak jednoduchá). Tuto rozvahu mužeme zformalizovat takto:

Definice. *Řezem v síti* $S = (V, E, z, s, w)$ rozumíme takovou množinu hran $C \subset E$, že po jejím odebrání nebude v grafu $G = (V, E \setminus C)$ žádná cesta z z do s. Číslo

$$|C| = \sum_{e \in C} w(e)$$

nazýváme *velikost řezu* C.

Evidentně platí, že nikdy nemůžeme najít větší tok, než je hodnota kteréhokoliv z řezů. N a dalším obrázku máme zobrazen tok sítí s hodnotou 5 a čárkovanými lomenými čarami jsou naznačeny řezy o hodnotách 12, 8 a 5.



Sestavíme funkční algoritmus, který pomocí postupných konstrukcí vhodných cest najde řez s minimální možnou hodnotou 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 velikosti řezu v této síti.*

Myšlenka algoritmu je vcelku prostá – prohledáváme cesty mezi uzly grafu a snažíme se je „nasytit“ co největším tokem. Zavedeme si za této účelem 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 $f(e) > 0$ pro hrany orientované opačně. 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 rezervu kapacity minimální rezervu kapacity z jejích hran.

Fordův-Fullkersonův algoritmus. Vstupem je síť $S = (V, E, z, s, w)$ a výstupem maximální možný tok $f : E \to \mathbb{R}$.

- *Iniciace:* zadáme $f(e) = 0$ pro všechny hrany $e \in E$ a prohledáváním do šířky z vrcholu z najdeme množinu vrcholů $U \subset V$, 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.
- na výstup dáme maximální tok f a minimální řez C tvořený všemi hranami vycházejícími z U a končícími v doplňku $V \setminus U$.

Důkaz správnosti algoritmu. Jak jsme viděli, velikost každého toku je nejvýše rovna hodnotě 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

$$|f| = \sum_{\text{hrany z } U \text{ do } V \setminus U} f(e) - \sum_{\text{hrany z } V \setminus U \text{ do } U} f(e).$$

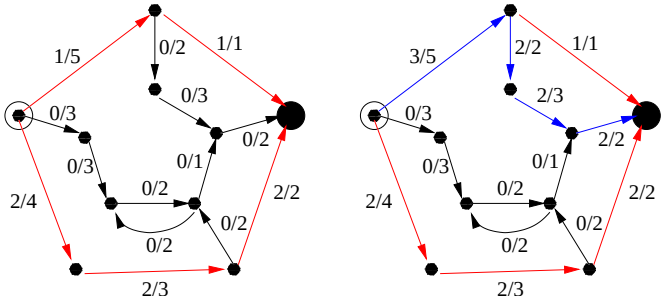
Tento výraz je ovšem v okamžiku zastavení roven

$$\sum_{\text{hrany z } U \text{ do } V \setminus U} f(e) = \sum_{\text{hrany z } U \text{ do } V \setminus U} w(e) = |C|,$$

což jsme chtěli dokázat.

Zbývá ovšem ukázat, že algoritmus skutečně zastaví.

Všimněme si, že pro celočíslené hodnoty ohodnocení hran získáme také celočíselný tok.



Chod algoritmu je ilustrován na obrázku. Vlevo jsou vybaveny dvě nejkratší nenasycené cesty ze zdroje do stoku (horní má dvě hrany, spodní tři). Jsou vyznačeny červeně. Napravo je pak nasycena další cesta v pořadí a je vyznačena modře. Je nyní zjevné, že nemůže existovat další nenasycená cesta ze zdroje do stoku. Proto algoritmus v tomto okamžiku skončí.

9.30

9.36. Dodatečné podmínky na tok. 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.

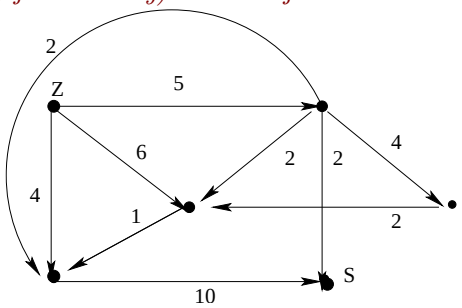
Přidání kapacit vrcholů je jednoduché – prostě vrcholy zdvojíme a dvojčata označující vstup do vrcholu a výstup z vrcholu spojíme právě jednou hranou s příslušnou kapacitou.

Omezení minimálními průtoky lze zahrnout do iniciace našeho algoritmu. Je ovšem zapotřebí otestovat, jestli takový tok vůbec existuje.

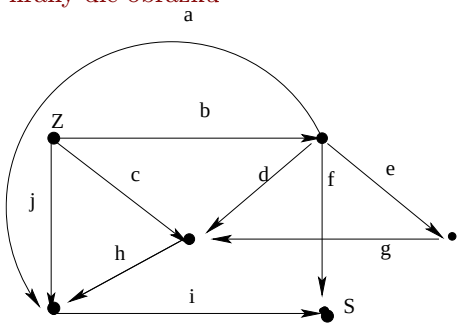
V literatuře lze najít řadu dalších nuancí, nebudeme se jim zde věnovat.

9.37. Příklady.

9.37.1. *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

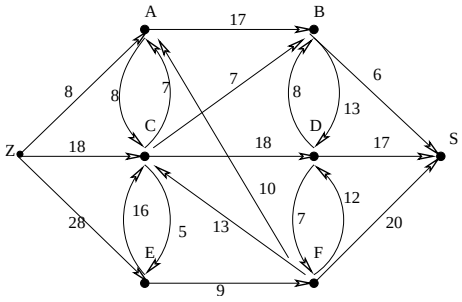


pak jsou řezy následující: {f,i},{f,h,j,a},{f,j,c,a,d,e},{f,j,c,a,d,f}, {b,j,c},{b,j,h},{b,i}, jejich hodnoty jsou pak 12, 9, 20, 18, 15, 10, 15. □

9.37.2. *Najděte maximální tok v síti z předchozího příkladu.*

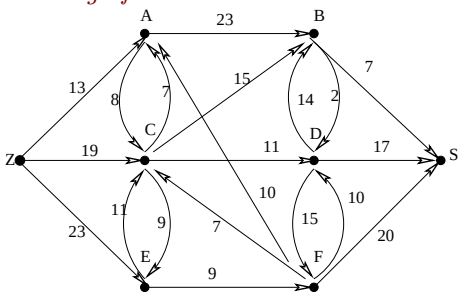
Řešení. Z teorie a předchozího příkladu víme, že hodnota maximálního řezu je 9. Tento tok f není zadán jednoznačně. Můžeme volit například $f(a) = 2, f(b) = 4, f(c) = 1, f(h) = 1, f(j) = 4, f(f) = 2, f(i) = 7,\ f(v) = 0$ pro všechny ostatní hrany v daného grafu. □

9.37.3. *Určete maximální tok a jemu odpovídající minimální řez v následujícím ohodnoceném orientovaném grafu:*



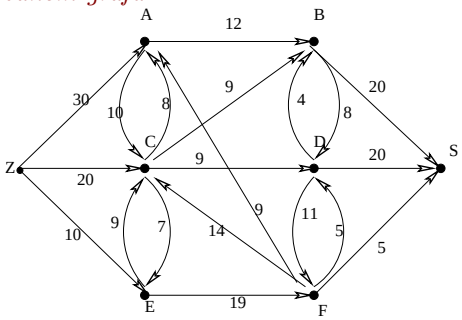
Řešení. Min. řez. dán množinou $\{F, S\}$, jeho hodnota je 39. □

9.37.4. *Určete maximální tok a jemu odpovídající minimální řez v následujícím ohodnoceném orientovaném grafu:*



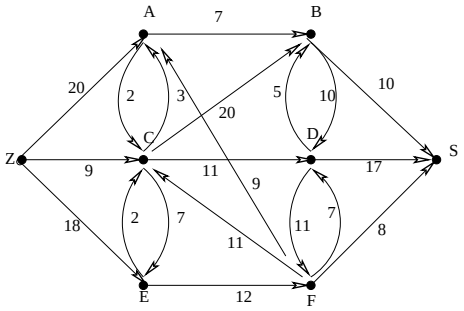
Řešení. Řez je dán množinou $\{F, S, D\}$, hodnota je 29. □

9.37.5. *Určete maximální tok a jemu odpovídající minimální řez v následujícím ohodnoceném orientovaném grafu:*



Řešení. Min. řez odpovídá množině (B, D, S). Hodnota je 40. □

9.37.6. *Určete maximální tok a jemu odpovídající minimální řez v následujícím ohodnoceném orientovaném grafu:*



Řešení. Min. řez je dán množinou $\{Z, A, E\}$. Hodnota je 32. □

9.31

9.38. Další aplikace. Hezkým využitím toků v sítí je řešení úlohy bipartitního párování. Úlohou je v bipartitním grafu najít maximální párování, tedy maximální podmnožinu hran takovou, aby žádné dvě hrany nesdílely vrchol.

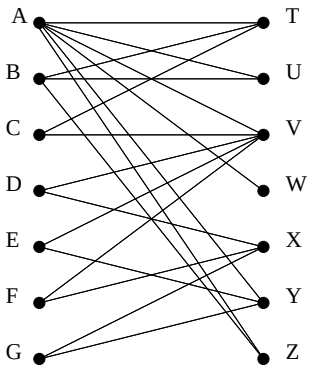
Jde o abstraktní variantu docela obvyklé úlohy – třeba spárování kluků a holek k tanci v tanečních, kdybychom měli předem známé možnosti, ze kterých vybíráme.

Tento problém docela 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 využitím toků je důkaz tzv. Mengerovy věty (uvedli jsme ji jako tvzerní v 9.12). 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 hodnota minimálního řezu je rovna hodnotě toku v síti nyní vyplývá požadované tvrzení.

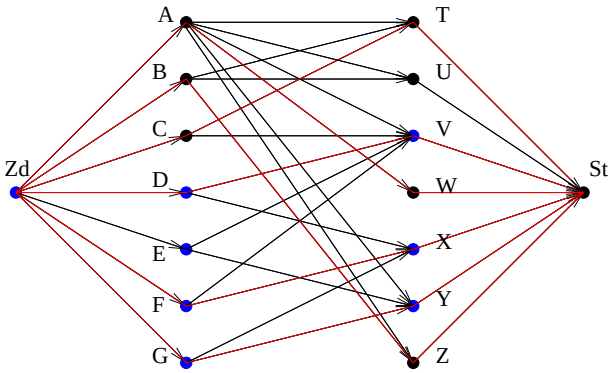
9.39. Příklady.

9.39.1. *Nalezněte maximální párování následujícího bipartitního grafu:*



Pro maximální tok určující Vámi nalezené maximální párování dále určete jemu odpovídající minimální řez v síti.

Řešení. Z daného bipartitního grafu vyrobíme síť přidáním zdroje Zd a stoku St, orientovaných hran $(Zd, A), \ldots, (Zd, G)$, $(T, St), \ldots, (Z, St)$, stávající hrany orientujeme „abecedně“ od nižšího písmena k vyššímu, všem hranám pak přiřadíme kapacitu 1. Ford-Fulkersonovým algoritmem pak snadno nalezneme některý maximální tok a jemu odpovídající max. párování. Jeden z možných maximálních toků je vyznačen na následujícím obrázku (červené hrany znázorňují tok o velikosti 1 danou hranou zleva do prava):



Odpovídající maximální párování (A, W), (B, Z), (C, T), (D, V), (F, X), (G, Y). Modře jsou v obrázku vyznačeny vrcholy, do nichž existuje rezervní cesta, minimální řez je pak tvořen hranami jdoucích z modrých vrcholů do černých vrcholů, tedy hranami (Zd, A), (Zd, B),(Zd, C),(V, St),(X, St),(Y, St). □

9.32

9.40. 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.

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 uzly všechny možné stavy hry, a tyto uzly 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*. (Název zavedl patrně Charles Bouton ve své analýze těchto her z roku 1901 – prý pochází z německého „Nimm!“, což česky znamená „Ber!“.)

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 setrojit následovně:

- Stavu s ℓ sirkami na stole a s prvním hráčem na tahu odpovídá podstrom s kořenem označeným F_ℓ, stavu s týmž počtem sirek a druhým hráčem na tahu odpovídá podstrom s kořenem S_ℓ.
- Uzel F_ℓ má levého syna $S_{\ell-1}$ a pravého syn $S_{\ell-2}$, u uzlu S_ℓ 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 explicitní formuli, viz. část o diferenčních rovnicích v první kapitole. Známe proto i formuli pro počet možných průběhů her. Počet možných stavů hry je přitom roven počtu všech uzlů ve stromu. Hra přitom vždy skončí výhrou buď prvního nebo druhého hráče. U podobných her může kromě toho hra končit také remízou.

9.33

9.41. Analýza hry. Připravená stromová struktura nám teď snadno umožní analyzovat hru tak, abchom mohli sestavit skutečně algoritmickou strategii pro každého hráče. Je k tomu jednoduchý rekurzivní postup pro ohodnocení kořene podstromu. Budeme označovat jako W uzly ve kterých (při optimální strategii obou) vítězí první hráč a L v případě opačném, případně ještě můžeme značit jako T (z anglického „win“ a „loose“ z pohledu prvého hráče, znak T odpovídá anglickému „tie“ ro remízu). 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) Uzel F_ℓ označíme W, jestliže existuje syn, který je W. Pokud takový syn neexistuje, ale mezi syny existuje uzel s označením T, bude i označovaný uzel T. Ve zbývajícím případě, kdy jsou všichni synové L bude i označovaný uzel L.
(3) Uzel S_ℓ označíme L, jestliže existuje syn označený L. Pokud takový syn neexistuje, ale mezi syny existuje uzel s označením T, bude i označovaný uzel T. Ve zbývajícím případě, kdy jsou všichni synové W bude i označovaný uzel W.

Voláním této procedury na kořen stromu obdžíme ohodnocení všech uzlů a tím také i strategii pro každého z hráčů:

- První hráč se snaží v každém svém kroku přesunout do uzlu označeném W, pokud to ale nejde, hledá alespoň T
- Druhý hráč je se snaží v každém svém kroku dostat hru do uzlu označeného L, pokud to nejde, hledá alespoň T.

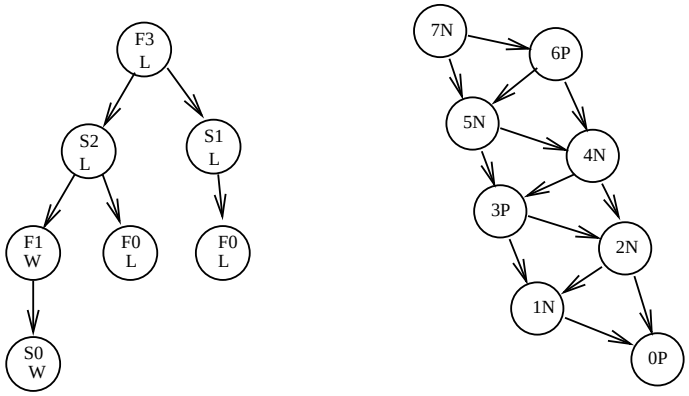
Hloubka rekurze je dána hloubkou stromu. Např. u našeho Nim s k sirkami je to právě k.

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 3×3 má příslušný strom jednotlivé desítky tisíc uzlů). 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 uzly počty zývajících 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!



Orientovaný acyklický graf má pro každý počet sirek právě jeden vrchol a ten zároveň nese označení, zda při jeho průchodu celkově vyhrá 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 uzlu, ve kterém se hráč nachází, vychází hrana končící v uzlu s označením P, hráč použije tento tah.

Naopak, každý acyklický orientovaný graf můžeme považovat za popis hry. Výchozími situacemi jsou v ní ty uzly, do kterých nevedou žádné hrany (jeden nebo více), hra končí v listech (opět jeden nebo více). Strategii hry obdržíme opět jednoduchou rekurzivně volanou procedurou:

- Listy označíme písmenem P (skutečně prohrává ten, kdo je na tahu a nachází se v listu).
- Uzel grafu označíme jako N, pokud z něj vede hrana do uzlu označeného jako P. V opačném případě označíme uzel jako P.

(Pro zjednodušení nyní uvádíme pouze případy her bez remíz.)

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 po dělení třemi.

Hry, které umíme reprezentovat výše uvedeným způsobem pomocí acyklického orientovaného grafu nazýváme *nestranné*. Jde právě o takévé 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 zrovna mají k dispozici.

9.34

9.42. Součet 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. Vyhrává, při normální hře, 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 se nám patrně nechce věřit, že znalost analýzy možností pro jednu hromádku nebude pro takovouto kombinovanou hru užitečná.

Zavedeme si 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). Jsou-li $G_1 = (V_1, E_1)$ a $G_2 = (V_2, E_2)$ dva acyklické orientované grafy, pak jejich součtem rozumíme graf $G = (V, E)$, kde

$$V = V_1 \times V_2$$
$$E = \{(v_1v_2, w_1v_2);\ (v_1, w_1) \in E_1\} \cup \{(v_1v_2, v_1w_2);\ (v_2, w_2) \in E_2\}.$$

V případě jedné hry jsme si vystačili s postupným označováním uzlů 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 uzlů značených jako P z dalších uzlů. Dobře k tomu poslouží tzv. *Spragueova–Grundyova funkce* $g : V \to \mathbb{N}$, kterou definujeme na acyklickém orientovaném grafu $G = (v, E)$ rekurzivně takto:

(1) Všechny listy v označíme $g(v) = 0$.
(2) Pro vrchol $v \in V$ definujeme

$$g(v) = \min\{a \in N; \text{neexistuje hrana } (v, w) \text{ s } g(w) = a\}.$$

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 podél hran vidím z vrcholu v.

Na přirozených číslech definujeme 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 vektrovém prostoru $(\mathbb{Z}_2)^k$ nad $\mathbb{Z}_2$ sečteme (k je dostatečně velké). Výsledkem je opět vyjádření pro $a \oplus b$ ve dvojkové soustavě. Sčítání vektorů ve $(\mathbb{Z}_2)^k$ je známá operace XOR na jednotlivých bitech.

Věta. (1) *Vrchol $v \in V$ v orientovaném acyklickém grafu $G = (V, E)$ je P pozice právě, když je hodnota Spragueovy–Grundyho funkce $g(v) = 0$.*

(2) *Pro orientované acyklické grafy* $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ *a* $G = (V, E) = G_1 + G_2$ *a jejich Spragueovy–Grundyovy funkce* g_1, g_2 *a* g *platí:*

$$g(v_1v_2) = g_1(v_1) \oplus g_2(v_2)$$

Důkaz. První tvrzení věty je zřejmé.

Důkaz druhé části povedeme následovně: nechť (v_1v_2) je pozice hry $G_1 + G_2$ a nechť $a \in \mathbb{N}_0$, $a < g_1(v_1) \oplus g_2(v_2)$ je jinak libovolné. Ukážeme, že existuje stav (x_1x_2) hry $G_1 + G_2$ tak, že $(v_1v_2, x_1x_2) \in E$ a zároveň pro žádnou hranu $(v_1v_2, y_1y_2) \in E$ neplatí $g_1(y_1) \oplus g_2(y_2) = g_1(v_1) \oplus g_2(v_2)$.

i) Nechť tedy $a < g_1(v_1) \oplus g_2(v_2)$. 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 v binárním rozvoji čísla $g_1(v_1) + g_2(v_2)$ musí být cifra 1 (právě jedno z čísel a a $g_1(v_1) \oplus g_2(v_2)$ tam musí mít cifru 1 a nemůže to být 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 ujmy na obecnosti předpokládejme, že to je $g_1(v_1)$, a uvažme číslo $c := g_1(v_1) \oplus b$. Toto číslo je v binárním zápise nejvýše $k-1$ ciferné (obě sčítaná čísla mají v k-tém řádu cifru 1), je tedy menší než $g_1(v_1)$. Potom dle definice funkce 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 $(v_1v_2, w_1v_2) \in H$ a $g_1(w_1) \oplus g_2(v_2) = c \oplus g_2(v_2) = g_1(v_1) \oplus b \oplus g_2(v_2) = g_1(v_1) \oplus a \oplus g_1(v_1) \oplus g_2(v_2) \oplus g_2(v_2) = a$.

ii) Nechť (v_1v_2, y_1y_2), kde $(v_1, y_1) \in E_1$), je hrana v G a nechť $g_1(y_1) \oplus g_2(y_2) = g_1(v_1) \oplus g_2(v_2)$. Pak ovšem $g_1(y_1) \oplus g_2(v_2) = g_1(v_1) \oplus g_2(v_2)$ a tedy $g_1(y_1) = g_1(v_1)$, ale to je ve sporu s vlastnostmi Spragueovy-Grundyovy funkce g_1 hry G_1.

□

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.

9.35

9.43. 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 shodí 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 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)

$$(1+x^2+x^3+x^4)(x^2+x^4+x^6+x^8+x^{10})(x^5+x^{10}+x^{15}).$$

Mělo by být zřejmé, že hledaný počet řešení je právě koeficient u x^{22} ve výsledném polynomu. Skutečně tak dostáváme 4 možnosti $3*5+3*2+1*1$, $3*5+2*2+3*1$, $2*5+5*2+2*1$ a $2*5+4*2+4*1$.

Tento prostinký příklad zasluhuje větší pozornost, než by se mohlo na první pohled zdát. Jednotlivé polynomy svými koeficienty vyjadřovaly posloupnost hodnot, kterých jsem 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 poslounosti 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 nulovými členy můžeme přiřadit polynom a hodou okolností řešení naší úlohy bylo možné odečíst ze součinu těchto polynomů. Takový postup můžeme používat obecně pro práci s posloupnostmi.

Definice. Vytvořující funkce pro nekonečnou posloupnost $a = (a_0, a_1, a_2, \dots)$ je (formální) mocninná řada

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{i=0}^{\infty} a_i x^i.$$

Některým jednoduchým operacím s posloupnostmi odpovídají jednoduché operace nad 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 α 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.
- Pro posunutí posloupnosti doleva o k míst (tj. vynechání prvních k míst posloupnosti) nejprve od $a(x)$ odečteme polynom $b_k(x)$ odpovídají posloupnosti $(a_0, \dots, a_{k-1}, 0, \dots)$ a poté podělíme vytvořující funkci x^k.
- Dosazením monomu $f(x)$ za x vytvoříme specifické kombinace členů původní posloupnosti. Jednoduše je vyjádříme pro $f(x) = \alpha x$, což odpovídá vynásobení k–tého členu posloupnosti skalárem α^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 prostorem skalárů.

9.36

9.44. 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 $(1,1,1,\dots)$. 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 5.31 a 6.30). Můžeme s nnimi pak opravdu na konvergenčním intervalu zacházet jako s funkcemi, zejména je umíme sčítat, násobit, skládat, derivovat a integrovat.

9.37 Několik jednoduchých příkladů – DODĚLAT ????

9.45. 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. 1.16. Tam jsme ale přímo odvodili vzorec pro rovnice prvního řádu, odůvodnili jednoznačnost a existenci řešení, ale řešení samo jsme pak v podstatě „uhádli“. Nyní můžeme řešení skutečně odvodit.

Zkusme nejprve dobře známý příklad Fibonaciovy 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 6.18. Tímto postupem vyjádříme

$$\begin{aligned} F(x) = \frac{1}{1 - x - x^2} &= \frac{A}{x - x_1} + \frac{B}{x - x_2} \\ &= \frac{a}{1 - \lambda_1 x} + \frac{b}{1 - \lambda_2 x} \end{aligned}$$

kde A, B jsou vhodné (obecně) komplexní konstanty a x_1, x_2 jsou kořeny polynomu ve jmenovateli. Konstanty a, b, λ_1 a λ_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 obecně řešení naší rekurence. Srovnejte tento postup s výsledkem v 1.17.1.

Pro obecné lineární diferenční rovnice řádu k je účinný stejný postup. Je-li

$$F_{n+k} = a_0F_n + \dots + a_{k-1}F_{n+k-1},$$

pak vytvořující funkce pro výslednou posloupnost je

$$F(x) = \frac{x^{k-1}}{1 - a_0x^{k-1} - \dots - a_{k-1}x}.$$

Rozkladem na parciální zlomky dostaneme obecný výsledek, který jsme zmiňovali již v odstavci 3.6.

9.38

9.46. Pěstované binární stromy. Jako další příklad uvedeme výpočet počtu p_n neizomorfních pěstovaných binárních stromů na n vrcholech.

Každý takový pěstovaný strom je vyjádřen jako kořen, podstrom jeho levého syna a podstrom jeho pravého syna (které mohou být i prázdné). Výjimkou je pouze strom na prázdné množině uzlů, který nemá ani kořen. Pro nízké hodnoty n můžeme určit přímo (jediný prázdný strom, na jednom uzlu pouze kořen, na dvou uzlech je buď pravý nebo levý syn atd.):

$$p_0 = 1,\ p_1 = 1,\ p_2 = 2,\ p_3 = 5, \dots .$$

Označme si $P(x) = p_0 + p_1 x + p_2 x^2 + \dots$ vytvořující funkci pro naši posloupnost p_i. Protože pro každé rozdělení $n-1$ uzlů mezi dva syny můžeme použít kterékoliv ze synů nezávisle na sobě, platí pro počet všech různých možností vztah

$$p_n = \sum_{i+j=n-1} p_i \cdot p_j$$

kde $i, j \geq 0$. To je ovšem koeficient u x^{n-1} ve funkci $P(x)P(x)$. Odvodili jsme tedy vztah (konstatní jednička napravuje první člen po posuvu o jednu pozici doprava)

$$P(x) = 1 + x(P(x))^2.$$

Odtud spočteme $P(x)$ jako řešení kvadratické rovnice (x považujeme za parametr, zatímco $P(x)$ hledanou neznámou), tj.

$$P(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Protože naše hodnota $P(x)$ se pro $x \to 0_+$ blíží k hodnotě $p_0 = 1$, nemůže vyhovovat řešení se znaménkem $+$. Zkusíme tedy znaménko mínus. Abychom dostali řešení, potřebujeme vyjádřit jako mocnicnou řadu výraz $\sqrt{1-4x}$. Dosazením této řady a dalšími úpravami dostáváme

$$p_n = -\frac{1}{2}(-4)^{n+1}\binom{1/2}{n+1} = \frac{1}{n+1}\binom{2n}{n}.$$

Jsou to tzv. *Catalánova čísla*, která se v kombinatorice často objevují.

KAPITOLA 10

Algebraické struktury a techniky

čím větší abstrakce, tím větší zmatek?
– ne, často to bývá naopak ...

Nyní se vrátíme k docela formálnímu studiu pojmů, jejichž na první pohled zcela abstraktní definice ve skutečnosti odráží velmi širokou třídu reálných vlastností věcí kolem nás. Určitě bude užitečné si před dalším čtením připomenout první a šestou část první kapitoly, kde jsme podobně abstraktně pohlíželi na čísla, se kterými počítáme, a obecněji na vztahy mezi objekty, které jsme abstrahovali do tzv. relací.

1. Grupy

Budeme si pohrávat s objekty a se situacemi, ve kterých je možné rovnice $a \cdot x = b$ vždy jednoznačně řešit (tak jako u lineárních rovnic jsou objekty a a b jsou dány, zatímco x hledáme). Půjde o tzv. teorii grup. Všimněme si, že zatím nic nevíme o povaze objektů, ani co znamená ta tečka.

Nejprve si zavedeme malý slovníček pojmů. Následně projdeme příklady, ve kterých se s takovými objekty potkáváme. A pak už budeme moci „budovat“ teorii...

10.1 **10.1. Definice.** Pro libovolnou množinu A:

- *binární operace* na A je zobrazení $A \times A \to A$, které budeme zpravidla značit $(a, b) \mapsto a \cdot b$, množina s binární operací je *grupoid*
- binární operace je *asociativní*, jestliže pro všechny prvky v A platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- binární operace je *komutativní*, jestliže pro všechny prvky v A platí $a \cdot b = b \cdot a$
- *levá jednotka* v A 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
- *pologrupa* $(A, \cdot)$ je grupoid s binární operací, která je asociativní
- 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 neutrálním prvkem
- *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.

- Je-li $(A, \cdot)$ grupa (případně pologrupa), pak její podmnožinu $B \subset A$, která je uzavřená vůči zúžení operace $\cdot$ a zároveň je spolu s touto operací grupou, nazýváme *podgrupa*.

10.2

10.2. Řešené příklady.

(1) Přirozená čísla $\mathbb{N} = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkou, neexistují v ní ale inverzní prvky.
(2) Celá čísla $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ jsou grupoid vůči kterékoliv z operací sčítání, odčítání, násobení. Jsou dokonce komutativní grupou vzhledem ke sčítání, jsou však jen komutativní pologrupou vůči násobení (neexistují inverze k prvkům $a \neq \pm 1$). Operace odčítání není ani asociativní (např. $(5-3)-2 = 0 \neq 5-(3-2) = 4$). Všimněte si také, že pro odečítání je nula pravý neutrální prvek, ne však levý. Dokonce v tomto případě levý neutrální prvek neexistuje.
(3) Racionální čísla $\mathbb{Q}$ jsou komutativní grupou vzhledem ke sčítání a nenulová racionální čísla jsou grupou vůči násobení. Celá čísla spolu se sčítáním jsou jejich podgrupou.
(4) Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa 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 $G = \{1, i, -1, -i\}$.
(5) Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic (viz odstavce 2.2–2.5).
(6) 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 2.31).
(7) v obou předchozích příkladech, podmnožina invertibilních objektů uvažované pologrupy tvoří grupu. V případě (5) jde o tzv. grupu invertibilních matic, ve druhém o grupu lineárních transformací vektorového prostoru.

10.2.1. *Rozhodněte o následujících množinách a operacích, jaké tvoří struktury (grupoid, pologrupa, grupa, monoid):*

(1) *podmnožiny množiny přirozených čísel spolu s operací sjednocení*
(2) *přirozená čísla spolu s binární operací největší společný dělitel*
(3) *přirozená čísla spolu s binární operací nejmenší společný násobek*
(4) *množina všech invertibilních matic 2×2 nad $\mathbb{R}$ spolu se sčítáním*
(5) *množina všech matic 2×2 nad $\mathbb{R}$ spolu s násobením matic*
(6) *množina všech matic 2×2 spolu s odčítáním matic*
(7) *množina všech invertibilních matic 2×2 nad $\mathbb{Z}_2$ s násobením matic*
(8) *množina $\mathbb{Z}_6$ spolu s násobením (modulo 6)*
(9) *množina $\mathbb{Z}_7$ spolu s násobením (modulo 7)*

Svá tvrzení zdůvodněte (proč je něco např. pouze grupoid a není pologrupa . . .). U třetího příkladu od konce sestavte tabulku dané operace.

Řešení.

(1) monoid (neutrálním prvkem je prázdná množina)
(2) pologrupa (bez neutrálního prvku)
(3) monoid (číslo 1 je neutrálním prvkem)

(4) není ani grupoid (uvážíme $A + (-A)$ pro nějakou invertibilní matici A)
(5) monoid (násobení matic je asociativní operace, viz 2.5, jednotková matice je neutrálním prvkem)
(6) grupoid (není asociativní)
(7) grupa (je monoidem stejně jako v bodě 5, z definice má každá invertibilní matice inverzi, tedy jde o grupu)
(8) monoid (operace je indukována klasickým násobením, je tedy asociativní, třída $[1]_{\mathbb{Z}_6}$ je neutrálním prvkem, např. třída $[2]_{\mathbb{Z}_6}$ nemá inverzi, není tedy grupou)
(9) grupa (jedná se o monoid ze stejných důvodů jako v předchozím bodě, z Bezoutovy věty věty vyplývá, že každý prvek v $\mathbb{Z}_p$, kde p je prvočíslo je invertibilní)

V příkladě 7 má grupa následující prvky:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, E = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, F = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Tabulka operace násobení těchto 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

□

10.2.2. *Doplňte následující tabulku operace $\star$ na množině $\{a, b, c\}$ tak, aby zadávala pologrupu.*

	a	b	c
a	b	a	a
b			
c			

Je toto doplnění jednoznačné? Kolik jich existuje?

Řešení.

Začneme postupně tabulku doplňovat:
$ba = (aa)a = a(aa) = ab = a$,
$bb = (aa)b = a(ba) = aa = b$,
$bc = (aa)c = a(ac) = aa = b$,
$a(ca) = (ac)a = aa = b$, tedy $(ca) = a$.
Dále $cb = c(aa) = (ca)a = aa = b$.

Na cc dostáváme omezení (díky $acc = ac$) $cc = b$, nebo $cc = c$. Obě možnosti jsou možné.

Existují tedy dvě různá doplnění:

	a	b	c
a	b	a	a
b	a	b	b
c	a	b	$[b, c]$

□

10.2.3. *Doplňte následující tabulku operace tak, aby zadávala strukturu pologupy na množině* $\{a, b, c, d\}$.

	a	b	c	d
a	d	d	a	c
b		b		
c				
d				

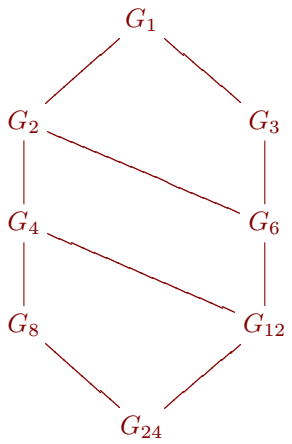
Řešení. $db = aab = ad = c$, $db = abb = ab = d$, tabulku nelze doplnit tak, aby zadávala pologrupu. □

10.2.4. *Nakreslete Hasseův diagram (viz* **??***) uspořádané množiny všech podgrup* $(\mathbb{Z}_{24}, +)$ *uspořádaných inkluzí.*

Řešení. Nejprve určeme všechny podgrupy $(\mathbb{Z}_{24}, +)$. Každá podgrupa je dána třídami násobků některého dělitele čísla 24 (vyplývá z Bezoutovy věty, viz **??**). Jedná se tedy o následující grupy:

$$\begin{aligned}
G_1 &= (Z_{24}, +) \\
G_2 &= (\{[0], [2], [4], [6], [8], [10], [12], [14], [16], [18], [20], [22]\}, +) \\
G_3 &= (\{[0], [3], [6], [9], [12], [15], [18], [21]\}, +) \\
G_4 &= (\{[0], [4], [8], [12], [16], [20]\}, +) \\
G_6 &= (\{[0], [6], [12], [18]\}, +) \\
G_8 &= (\{[0], [8], [16]\}, +) \\
G_{12} &= (\{[0], [12]\}, +) \\
G_{24} &= (\{[0]\}, +)
\end{aligned}$$

Hasseův diagram potom vypadá následovně:



□

10.3

10.3. Grupy permutací. Zpravidla grupy a pologrupy potkáváme jako množiny zobrazení na pevně dané množině M, které jsou uzavřeny vůči skládání zobrazení. Často si ale tuto skutečnost přímo neuvědomujeme.

Nejsnáze je tato souvislost vidět na konečných množinách M. Na každé takové množině o $m = |M| \in \mathbb{N}$ prvcích (prázdná množina má 0 prvků) máme k dispozici m^m možných definic zobrazení (každý z m prvků můžeme zobrazit na kterýkoliv v M) a všechna taková zobrazení umíme skládat.

Pokud chceme, aby existovala k zobrazení $\alpha : M \to M$ jeho inverze α^{-1}, musí být α bijekcí. Složením dvou bijekcí vznikne opět bijekce a proto podmnožina Σ_m všech bijekcí na množině M o m prvcích je grupa. Říkáme jí *grupa permutací* (na m prvcích). Sám název přitom uvádí jinou souvislost, kdy místo bijekcí na konečné množině vnímáme permutace jako přerovnání rozlišitelných prvků. Potkávali jsme se s ní např. při studiu determinantů, 2.14.

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 Σ_3 na číslech $\{1, 2, 3\}$ označíme jednotlivá pořadí

$$a = (1, 2, 3),\ b = (2, 3, 1),\ c = (3, 1, 2),$$
$$d = (1, 3, 2),\ e = (3, 2, 1),\ f = (2, 1, 3),$$

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:

$$b^2 = c,\ b^3 = a,\ c^2 = b,\ c^3 = a$$

a samy o sobě jsou tyto tři prvky komutativní podgrupou. V ní a je jednotka, a b s 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 v 10.2(4).

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.

Obdobně se chovají všechny grupy permutací Σ_m konečných množin o m prvcích. Každá permutace σ 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 $\sigma^k(x)$, $k = 1, 2, \dots$, 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 σ na M_x. Pokud přitom očíslujeme prvky v M_x jako pořadí $(1, 2, \dots, |M_x|)$ 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 σ složíme.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ 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 nakonec), lze každou permutaci napsat jako složení transpozic sousedních prvků. Můžeme samozřejmě vyjádřit pomocí transpozic i jinak, ale skutečnost, jestli potřebujeme sudý nebo lichý počet permutací je na volbách nezávislá. Máme tedy definováno dobře zobrazení $\operatorname{sgn} : \Sigma_m \to \mathbb{Z}_2 = \{\pm 1\}$, 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 ℓ lze vyjádřit jako složení $\ell-1$ transpozic. Parita cyklu délky ℓ je $(-1)^{\ell-1}$. Parita složení permutací je součinem parit jednotlivých z nich, tzn. že zobrazení* sgn *převádí složení permutací $\sigma \circ \tau$ na součin $\operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$ v komutativní grupě $\mathbb{Z}_2$.*

10.4. Příklady.

10.4.1. *Rozložte na součin transpozic následující permutaci:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 6 & 7 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Spočtěte σ^{336}.

Řešení. Danou permutaci nejprve rozložíme na součin nezávislých cyklů: v dvojřádkovém zápisu permutace vybereme první prvek (číslo 1), to se zobrazuje na číslo 9, devítka se zobrazuje na pětku, pětka na jedničku a dostáváme první cyklus (159). Dále vybereme číslo neobsažené v prvním cyklu, např. dvojku a pokračujeme stejně, tedy dvojka se zobrazuje na osmičku, osmička na čtyřku, čtyřka na sedmičku, sedmička na trojku, trojka na šestku a konečně šestka na dvojku a dostáváme cyklus $(2, 8, 4, 7, 3, 6)$ (tento cyklus bychom také jako v prvním případě mohli zapsat jako (284736) protože nemůže dojít k nedorozumění). Celkem

$$\sigma = (159)(284736)$$

Každý z cyklů dále rozložíme na transpozice a dostáváme

$$\sigma = (15) \circ (59) \circ (2, 8) \circ (8, 4) \circ (4, 7) \circ (7, 3) \circ (3, 6).$$

Při počítání σ^{336} využijeme toho že σ je složením dvou cyklů délky tři a šest. Pro cyklus c délky l zřejmě platí $c^l = \mathrm{id}$, tedy $\sigma^6 = \mathrm{id}$ a

$$\sigma^{336} = \left(\sigma^6\right)^{56} = \mathrm{id}$$

□

10.4.2. *Rozložte na součin transpozic permutaci*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 8 & 5 & 1 & 10 & 2 & 3 & 4 & 6 & 7 \end{pmatrix}$$

Řešení. $\sigma = (19) \circ (96) \circ (62) \circ (28) \circ (84) \circ (73) \circ (35) \circ (5, 10)$. □

10.4

10.5. Symetrie ohraničených 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 také, že matice zadávají lineární zobrazení $\mathbb{R}^2 \to \mathbb{R}^2$, které zachovávají standardní vzdálenosti právě, když jsou jejich sloupce ortonormální bazí $\mathbb{R}^2$ (což je jednoduchá podmínka na souřadnice matice, viz 1.36). Ve skutečnosti není obtížné dokázat (ale nebudeme to tu dělat), že každé zobrazení roviny do sebe, které zachovává velikosti je affinní, tj. je složením lineárního a vhodné translace. [1] 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_φ o jakýkoliv úhel φ kolem počátku a zrcadlení Z_ℓ vůči jakékoliv přímce ℓ procházející počátkem (povšimněme si, že středová souměrnost je totéž jako rotace o π).

Uvažme nyní nějaký rovinný obrazec, pro začátek třeba úsečku a rovnostranný trojúhelník. Ptáme se, jak moc jsou symetrické, tzn. vůči kterým trasformacím (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 π, zrcadlení vůči ose této úsečky a zrcadlení vůči úsečce samotné a všechny tyto symetrie jsou samy sobě inverzí. Celá grupa symetrií úsečky má tedy čtyři prvky. Její tabulka násobení vypadá takto:

$\cdot$	R_0	R_π	Z_H	Z_V
R_0	R_0	R_π	Z_H	Z_V
R_π	R_π	R_0	Z_V	Z_H
Z_H	Z_H	Z_V	R_0	R_π
Z_V	Z_V	Z_H	R_π	R_0

a je tedy celá tato grupa komutativní.

Pro rovnostranný trojúhelník už symetrií nacházíme víc: můžeme rotovat o $\pi/3$ nebo můžeme zrcadlit vůči osám stran. Abychom dostali grupu celou, musíme přidat všechna složení takovýchto transformací. Už v 1.36 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, který bude dohromady šest. Jestliže si umístíme trojúhelník v

[1] 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. Zkuste si aspoň začít výpočet jako cvičení! (Návod: máme ukázat, že všechny parciální derivace F jsou nulové. To ale je podmínka nezávislá na volbě afinních souřadnic, proto složením F s lineárním zobrazením výsledek nemění. Můžeme proto pro pevný bod (x, y) složit $(DF)^{-1} \circ F$, takže bez újmy na obecnosti lze rovnou předpokládat, že $DF(x, y)$ je matice identického zobrazení. Derivováním rovnic pak dostáváme důsledky, které přímo říkají požadované tvrzení.) Ve skutečnosti vede stejný postup ke stejnému výsledku pro euklidovské prostory libovolné dimenze.

souřadnicích jako na obrázku, bude našich šest transformací zadáno maticemi

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ b = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix},\ c = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$
$$d = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},\ e = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix},\ f = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

Sestavením tabulky pro násobení, tak jak jsme ji udělali pro grupu permutací Σ_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 všechny $k \geq 3$, zatímco D_2 je komutativní. Název patrně je odvozen od skutečnosti, že D_2 je grupa symetrií molekuly vodíku.

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 trojúhelníku na obrázku. Všimněme si, že grupu C_2 lze realizovat dvěma způsoby – buď jedinou netriviální rotací o π nebo jediným zrcadlením.

Věta. *Nechť je M ohraničená množina v rovině $\mathbb{R}^2$ s nejvýše spočetnou grupou grupou symetrií G. Pak je grupa G buď triviální nebo jedna z grup C_k, D_k, s $k \geq 1$.*

Důkaz. Kdyby nějaká množina M připouštěla jako svoji symetrii translaci, nemůže být ohraničená. Pokud by M připouštěla netriviální rotace s různými středy, opět nemůže 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 procházející. Zbývá tedy dokázat, že je celá grupa složena vždy buď pouze z rotací nebo vždy ze stejného počtu rotací a symetrií. Protože je ale vždy složením dvou různých zrcadlení rotace o úhel rovný polovině úhlu svíraného osami zrcadlení (viz 1.36) a tedy i naopak složením zrcadlení podle přímky p s rotací o úhel $\varphi/2$ dostame zrcadlení podél přímky svírající úhel φ s p. Odtud již vcelku snadno lze odvodit požadované tvrzení. □

10.5

10.6. Symetrie rovinných dláždění. Složitější chování lze vypozorovat u rovinných obrazců v pásech nebo v celé rovině (něco jako možnosti symetrií pro různé dlažby).

Nejprve uvažme množinu M, která je celá obsažena v pásu uzavřeném mezi dvěma rovnoběžkami. Pro symetrie takové množiny nepřicházejí v úvahu žádné netriviální rotace, kromě R_π, a jediná možná zrcadlení jsou buď podle osy pásu nebo vertikální. Zůstavají ještě pouze translace podle vektoru rovnoběžného s osou pásu. Všimněme si, že každá netriviální translace svými iteracemi zapříčiní, že celá grupa symetrií M bude již nutně nekonečná.

Nepříliš složitá diskuse vede k popisu všech tzv. *diskrétních grup* symetrií pro rovinné pásy. Jsou to takové, kdy obraz libovolného bodu při působení všemi prvky grupy je diskrétní podmnožinou v rovině. Každá takové grupa je generována některými z následujících možných symetrií: translace T, posunutá reflexe G, vertikální reflexe V, horizontální reflexe H a rotace R o π.

Věta. *Každá grupa symetrií je jednoho z následujících sedmi typů. Jsou generovány*

(1) *jedinou translací T*
(2) *jedinou posunutou translací 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 nebudeme uvádět, zkuste si alespoň vykreslit symbolicky vzory s těmito symetriemi.

Složitější je to se symetriemi obrazců, 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 konečné nebo spočetné grupy symetrií. Bohatá teorie byla vypracována zejména v 19. století v souvislosti se studiem symetrií krystalů a molekul chemických prvků.

(symbolický obrázek všech symetrií, odkazy na literaturu a trochu podrobnější diskusi dodám snad později ...)

10.6

10.7. Homomorfismy grup. Zobrazení $f : G \to H$ mezi dvěmi 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*
(2) *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
(3) *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*
(4) *obraz inverze k prvku je inverzí obrazu. tj. $f(a^{-1}) = f(a)^{-1}$.*
(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 $K \subset G$ 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 podgrupa.

Specielně, triviální podgrupy mají za obrazy opět podgrupy. Protože z rovnosti $a \cdot a = a$ vynásobením prvkem a^{-1} vyplývá $a = e$, ověřili jsme, že jedinou jednoprvkovou podgrupou je triviální podgrupa $\{e\}$, zejména tedy $f(e) = e$.

Stejně postupujeme u vzorů: jestliže $a, b \in G$ splňují $f(a)$, $f(b) \in K \subset H$, 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 $f(G)$.

10.7

10.8. Řešené příklady. (1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\operatorname{sgn} : \Sigma_n \to \mathbb{Z}_2$ přiřazující permutaci její paritu. Z tvrzení Věty 10.3 vyplývá, že jde o homomorfismus grup. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.
(2) Při studiu grupy symetrií rovnostranného trojúhelníka jsme našli izomorfismus této grupy s grupou permutací Σ_3. Realizaci Σ_3 si snadno můžeme zvolit tak, že za množinu tří prvků pro permutace vezmeme vrcholy trojúhelníka a jednotlivým symetriím přiřadíme permutace těchto vrcholů, které vyvolají.
(3) Zobrazení $\exp : \mathbb{R} \to \mathbb{R}_+$ (nebo $\mathbb{C} \to \mathbb{C} \setminus 0$, pokud pracujeme s příslušnou mocninnou řadou a rozšíříme zobrazení na komplexní čísla) je homomorfismus aditivní grupy reálných nebo komplexních čísel na multiplikativní grupu kladných reálných čísel, resp. na multiplikativní grupu všech nenulových komplexních čísel. V případě reálných čísel jde o izomorfismus. Pro komplexní čísla 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 $e^{s+it} = e^s \cdot e^{it}$ v jádru, musí být $e^s = 1$, tj. $s = 0$, a pak zbývá pouze $t = 2k\pi$ pro libovolné celé k).
(4) Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár v $\mathbb{K}$ (pracovali jsme s $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Cauchyova věta o determinantu součinu čtvercových matic $\det(A \cdot B) = (\det A) \cdot (\det B)$ je tvrzením, že pro grupu $G = GL(n, \mathbb{K})$ invertibilních matic je $\det : G \to \mathbb{K} \setminus 0$ homomorfismem grup.
(5) 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. Zobrazení

$$p_G : G \times H \ni (a, x) \mapsto a \in G, \ p_H : G \times H \ni (a, x) \mapsto x$$

jsou surjektivní homomorfismy s jádry

$$\ker p_G = \{(e_G, x);\ x \in H\} \quad \ker p_H = \{(a, e_H); a \in G\}.$$

(6) 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 $\frac{2\pi}{k}$.
(7) 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 pravidleného šestiúhelníku, $\mathbb{Z}_2$ pak odpovídá ± 1, $\mathbb{Z}_3$ 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) izomorfismus:

$$[0]_6 \mapsto ([0]_2, [0]_3)$$
$$[1]_6 \mapsto ([1]_2, [2]_3)$$
$$[2]_6 \mapsto ([0]_2, [1]_3)$$
$$[3]_6 \mapsto ([1]_2, [0]_3)$$
$$[4]_6 \mapsto ([0]_2, [2]_3)$$
$$[5]_6 \mapsto ([1]_2, [1]_3)$$

Zkuste se přesvědčit, že to takto skutečně funguje. Umíte tvrzení zobecnit?
(8) Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{a, a^2, a^3, \dots\}$, 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. 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).

10.8.1. *Určete všechny podgrupy grupy invertibilních čtvercových matic nad $\mathbb{Z}_2$ (vzhledem k násobení matic), viz 10.2. Je tato grupa isomorfní grupě S_3? Zdůvodněte (buď najděte isomorfismus, nebo udejte důvod, proč neexistuje).*

Řešení. Grupy jsou isomorfní, transposice odpovídají prvkům řádu 2. Podgrupy pak odpovídají podgrupám S_3 □

10.8.2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

(1) $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
(2) $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
(3) $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
(4) $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [3a]_{\mathbb{Z}_{15}^*}$
(5) $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [4a]_{\mathbb{Z}_{15}^*}$
(6) $f : (\mathbb{Z}_k^*, \cdot) \to (\mathbb{Z}_k^*, \cdot)$, $f([a]_{\mathbb{Z}_k^*}) = [l \cdot a]_{\mathbb{Z}_k^*}$, $k, l \in \mathbb{N}, k, l > 1$
(7) $f : S_k \to S_k$, $f(\sigma) = \sigma^2$

Řešení.

(1) není zobrazení
(2) není zobrazení
(3) je isomorfismus
(4) není zobrazení
(5) je bijekce, není isomorfismus
(6) je bijekce pro $(k, l) = 1$ (pro $l \equiv 1 \mod k$), jinak není zobrazení
(7) je zobrazení, je homomorfismem pouze pro $k = 2$

□

10.8

10.9. Rozklady podle podgrup. Uvažme grupu G a její podgrupu H. Na množině prvků grupy G nyní definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$. Snadno ověříme, že je takto definována relace ekvivalence:

- $a^{-1} \cdot a = e \in H$,
- je-li $b^{-1} \cdot a = h \in H$, potom $a^{-1} \cdot b = (b^{-1} \cdot a)^{-1} = h^{-1} \in H$,
- je-li $c^{-1} \cdot b \in H$ a zároveň je $b^{-1} \cdot a \in H$, potom $c^{-1} \cdot a = c^{-1} \cdot b \cdot b^{-1} \cdot a \in H$.

Celá grupa G se tedy rozpadá na tzv. *levé třídy rozkladu* podle podgrupy H vzájemně ekvivalentních prvků. Třídu 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 platí:*

(1) *Levé a pravé třídy rozkladu podle podgrupy $H \subset G$ 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, 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 $h = h'$. □

10.9

10.10. Důsledek. *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.

Druhá je okamžitým důsledkem prvního.

Každý prvek 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 již $a^k = e$, je také $a^n = (a^k)^s = e$.

Jestliže je $n > 1$, pak existuje prvek $a \in G$ různý od jednotky. Jeho řád je přirozené číslo různé od jedničky a nutně dělí n. Proto musí být rovno n. Pak ovšem jsou všechny prvky G tvaru a^k pro $k = 1, \ldots, n$. □

10.10

10.11. 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

$$(a \cdot h \cdot b \cdot h') \cdot H = ((a \cdot b) \cdot (b^{-1} \cdot h \cdot b) \cdot h') \cdot H.$$

Totéž si můžeme odůvodnit tak, že nezáleží na tom jestli pracujeme s pravými nebo levými třídami, můžeme 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 všechny podgrupy normální. Podmnožina

$$n\mathbb{Z} = \{na;\ a \in \mathbb{Z}\} \subset \mathbb{Z}$$

zadává v celých číslech podgrupu a její faktorgrupou je právě (aditivní) grupa zbytkových tříd $\mathbb{Z}_n$.

Jak jsme viděli, všechna jádra homomorfismů jsou normální podgrupy. Naopak, jestliže je podgrupa $H \subset G$ 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 to musí být homomorfismus a je zjevně na. Je tedy vidět, že normální podgrupy jsou právě všechna jádra homomorfismů.

Dále, pro libovolný homomorfismus grup $f : G \to K$ 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 $\mathbb{C}^* \to \mathbb{C}^*$ 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 přehledný jako u konečných grup v Důsledku 10.10.

10.12. Řešené příklady.

10.12.1. *Rozhodněte, zda jsou podgrupy generované*

- *cyklem* $(1,2,3)$ *v* S_3,
- *cyklem* $(1,2,3,4)$ *v* S_4
- *cyklem* $(1,2,3)$ *v* A_4

normální. V posledním případě určete pravé třídy rozkladu A_4 *podle uvažované podgrupy. Určete, kdy je podmnožina všech cyklů délky* n *podgrupou grupy* S_n. *Ukažte, že se pak jedná o normální podgrupu.*

Řešení.

- Jde o normální podgrupu A_3.
- Není to normální podgrupa ($(1,2)(1,3)(2,4)(1,2) = (4,1)(2,3)$).
- Podgrupa není normální. Pravé třídy rozkladu jsou pak $\{(124),(243),(13)(24)\}$, $\{(142),(143),(14)(23)\}$, $\{(234),(12)(34),(134)\}$, $\{\mathrm{Id},(123),(132)\}$.

Podmnožina je podgrupou pouze pro $n = 3$. Potom jde o podgrupu A_3 sudých permutací v S_3, jedná se tedy o normální podgrupu. (pro jiná n snadno najdeme dva cykly délky n jejichž složením není cyklus délky n). □

10.12.2. *Určete podgrupu v S_6 generovanou permutacemi* $(12)(34)(56)$, (1234) *a* (56). *Je tato podgrupa normální? Pokud ano, popište třídy rozkladu S_6/H.*

Řešení. Nejprve si všimněme, že všechny zadané permutace leží v podgrupě $S_4 \times S_2 \subset S_6$. Proto i jimi generovaná podgrupa bude ležet v této podgrupě. Dále zřejmě (protože mezi generátory je transposice (56)) je hledaná podgrupa tvaru $H \times S_2$, kde $H \subset S_4$. Stačí tedy popsat H, tato grupa je generována prvky $(12)(34)$ a (1234) (projekce generátorů na S_4). Máme

$$\begin{aligned}
(1234)^2 &= (13)(24)\\
(1234)^3 &= (4321)\\
(1234)^4 &= \mathrm{id}\\
[(12)(34)]^2 &= \mathrm{id}\\
(12)(34)\circ(1234) &= (24)\\
(1234)\circ(12)(34) &= (13)\\
(12)(34)\circ(4321) &= (13)\\
(4321)\circ(12)(34) &= (24)\\
(12)(34)\circ(13)(24) &= (14)(23)\\
(13)(24)\circ(12)(34) &= (14)(23)\\
(12)(34)\circ(42) &= (1234)\\
(13)\circ(42) &= (13)(24)
\end{aligned}$$

Stačí si rozmyslet, že dalším skládáním již nedostaneme nic nového (např $(13)\circ(1234) = (12)(34)\circ(4321)\circ(1234) = (12)(34)\circ\mathrm{id} = (12)(34)$). Podgrupa $H \subset S_4$ má tedy osm prvků (osm je dělitel čísla 24, tedy podle Lagrangeovy věty je to skutečně možný počet prvků podgrupy).

$$H = \{\mathrm{id},(1234),(13)(24),(4321),(12)(34),(13),(24),(14)(23)\}.$$

Všech prvků hledané podgrupy v S_6 je tedy 16 (pro každý prvek $h \in H$ jsou v ní prvky $h \times \mathrm{id}$ a $h \times (56)$).

□

10.12.3. *Určete podgrupu v S_4 generovanou permutacemi* $(12)(34)$, (123).

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

$$\begin{aligned}
[(12)(34)]^2 &= \mathrm{id}\\
(123)^2 &= (321)\\
(12)(34)\circ(123) &= (243)\\
(123)\circ(12)(34) &= (134)\\
(12)(34)\circ(321) &= (314)\\
(321)\circ(12)(34) &= (234)
\end{aligned}$$

a v tomto okamžiku máme již sedm prvků hledané podgrupy A_4, protože A_4 má dvanáct prvků a počet prvků podgrupy musí být dělitem čísla dvanáct, musí být hledanou podgrupou celá grupa A_4. □

10.11

10.13. 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 můžeme 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 2π je ale identické zobrazení.

Formálně si můžeme takovou situaci popsat jako tzv. (levou) *akci grupy G na množině S*. Jde o 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 se k vyjádření akce prvku grupy na prvku S používá pouze zápis $a \cdot x$ (byť jde o jinou tečku než u násobení uvnitř grup), definiční vlastnost pak vypadá takto:

$$(a \cdot b) \cdot x = a \cdot (b \cdot x).$$

Obraz prvku $x \in S$ v akci celé grupy G nazýváme *orbita* S_x prvku x

$$S_x = \{y = \varphi(a, x);\ a \in G\}.$$

Pro každý bod $x \in S$ definujeme *izotropní podgrupu* $G_x \subset G$ akce φ,

$$G_x = \{a \in G;\ \varphi(a, x) = x\}.$$

Je-stliže pro každé dva prvky x, $y \in S$ existuje $a \in G$ tak, že $\varphi(a, x) = y$, pak říkáme, že akce φ je *tranzitivní*. Snadno se vidí, že u tranzitivních akcí jsou všechny izotropní podgrupy stejně mohutné.

Jako příklad tranzitivní akce konečné grupy můžeme uvést např. zjevnou akci grupy permutací pevně zvolené množiny X na samotné množině X. Přirozená akce všech lineárních transformací na nenulových prvcích vektorového prostoru V je také tranzitívní. Pokud vezmeme ale prostor V celý, je nulový vektor zvláštní orbitou.

Jiný příklad akce grupy G je přirozená akce na množině levých tříd G/H pro nějakou podgrupu H zadaná levým násobením na reprezentantech tříd.

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) *(Burnsidovo 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. Uvažmě $x \in S$ a izotropní podgrupu $G_x \subset G$. Akce grupy G zadává 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 zobrazaní injektvní. Zároveň je zjevně surjektivní, proto $|G/G_x| = |S_x|$. Odtud již vyplývá první vlastnost z věty, protože $|G| = |G/G_x| \cdot |G_x|$.

Druhé tvrzení dokážeme tak, že dvěma způsoby spočteme mohutnost množiny pevných bodů akce v jejím grafu:

$$F = \{(x, g) \in S \times G;\ g(x) = x\} \subset S \times G.$$

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 $x_1, \ldots, x_N$ z každé orbity v S. 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. □

Tato tvrzení jsou velice často užitečná pro řešení kombinatorických úloh.

Příklad. 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.

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 Burnsidovy věty:

$$N = \frac{1}{|D_9|} \sum_{g \in D_9} |S_g| = \frac{126}{18} = 7.$$

Najděte si příslušných sedm různých náhrdelníků!

10.14. Příklady.

10.14.1. *Určete počet obarvení políček tabulky 3×3 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 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

$$\frac{1}{8}(3^9 + 2 \cdot 3^4 + 3^5 + 4 \cdot 3^6) = 2862.$$

□

10.14.2. a) *Určete všechny rotační symetrie pravidelného osmistěnu.*

b) *Určete počet obarvení 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 z osmi 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 $\pm 90°$ a o $180°$ okolo os procházejících protějšími vrcholy, o rotace o $180°$ podle os procházejících středy protějších hran a konečně o rotace o $\pm 120°$ 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:
   - 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

$$\frac{1}{24}(3^8 + 6 \cdot 3^2 + 17 \cdot 3^4) = 333.$$

□

10.14.3. *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

$$\frac{1}{36}(4084080 + 2 \cdot \binom{6}{3}\binom{3}{3} + 9 \cdot \binom{8}{4}\binom{4}{3}) = 113590.$$

□

2. Okruhy polynomů a tělesa

10.12

10.15. Okruhy a tělesa. Jak jsme viděli, s grupami se potkáváme nejčastěji jako s množinami transformací. Zároveň ale byly vlastnosti grupy podstatné u skalárů i vektorů, tam ovšem vystupovalo několik obdobných struktur zároveň. Zaměříme se teď právě na takové případy. Jako standardní příklady přitom mějme na mysli skaláry (tj. celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, komplexní čísla $\mathbb{C}$) a množiny polynomů nad takovými skaláry $\mathbb{K}$.

Celá čísla mají následující vlastnosti tzv. okruhu:

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 všechny $a, b, c \in M$;
- $a \cdot b = b \cdot a$, pro všechny $a, b \in M$;
- existuje prvek 1 takový, že pro všechny $a \in M$ platí $1 \cdot a = a$;
- $a \cdot (b + c) = a \cdot b + a \cdot c$, pro všechny $a, b, c \in M$;

se nazývá *komutativní okruh*.

Jestliže v okruhu $\mathbb{K}$ platí $c \cdot d = 0$ právě, 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*. Pokud neplatí vlastnost komutativity operace $\cdot$, hovoříme o (nekomutativním okruhu). V dalším se ovšem omezíme pouze na okruhy komutativní. Operaci $+$ budeme říkat sčítání a operaci $\cdot$ násobení. Navíc budeme vždy předpokládat existenci jedničky 1 pro operaci násobení, neutrálnímu prvku pro sčítání říkáme nula.

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 $a|c$. Dodatečnou vlastností oboru integrity oproti obecnému okruhu je neexistence netriviálních dělitelů nuly. Okamžitě odtud také vyplývá jednoznačnost dělitelů: je-li $b = a \cdot c$ a $b \neq 0$, pak c je jednoznačně dáno volbou a, b. Pro $b = ac = ac'$ totiž platí $0 = a \cdot (c - c')$ a $a \neq 0$, proto $c = c'$.

Dělitelé jedničky, tj. invertibilní prvky v $\mathbb{K}$, se nazývají *jednotky*. Jednotky v komutativním okruhu vždy tvoří komutativní grupu. Netriviální (komutativní) okruh, ve kterém jsou všechny nenulové prvky invertibilní, se nazývá (komutativní) *těleso*. Komutativní těleso se také nazývá *pole*.

Typickým příkladem komutativních okruhů, tj. polí, jsou číslené 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 $\mathbb{H}$.

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 všechny $c \in \mathbb{K}$,
(2) $-c = (-1) \cdot c = c \cdot (-1)$ pro všechny $c \in \mathbb{K}$,
(3) $-(c \cdot d) = (-c) \cdot d = c \cdot (-d)$ pro všechny $c, d \in \mathbb{K}$,
(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:

$$c \cdot a = c \cdot (a + 0) = c \cdot a + c \cdot 0 = c \cdot a$$

a protože jediným neutrálním prvkem vůči sčítání je nula, dostáváme $a \cdot 0 = 0$. Stejně se dokáže i $0 \cdot a$. 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 $c = 1 \cdot c = 0 \cdot c = 0$. □

10.13

10.16. Polynomy. 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:[2]

Definice. Nechť $\mathbb{K}$ je jakýkoliv komutativní okruh skalárů s jedničkou. Polynomem nad $\mathbb{K}$ rozumíme konečný výraz

$$f(x) = \sum_{i=0}^{k} a_i x^i$$

[2]Ne náhodou je pro okruh použit symbol $\mathbb{K}$ – představujte si pod ním třeba kterýkoliv okruh naších skalárů, definice je ovšem obecná.

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 různá 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. Zároveň ale platí tvrzení, které dokážeme zanedlouho:

Tvrzení. *Jestliže je $\mathbb{K}$ nekonečný okruh, pak dva polynomy $f(x)$ a $g(x)$ nad $\mathbb{K}$ jsou stejné právě, když jsou stejná příslušná zobrazení f a g.*

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:

$$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k$$

$$(f \cdot g)(x) = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + \cdots + (a_0 b_\ell + a_1 b_{\ell-1} + \cdots + a_\ell b_0)x^\ell + \ldots$$

kde uvažujeme nulové koeficienty všude, kde v původním výrazu pro polynomy nenulové koeficienty nejsou[3] a u sčítání nechť je k maximální ze stupňů f a g.

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.

Lemma. *Okruh polynomů nad oborem integrity je opět obor integrity.*

Důkaz. Máme ukázat, že v $\mathbb{K}[x]$ mohou být netriviální dělitelé nuly pouze, jetliže 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 ℓ 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 $\mathbb{K}$. □

10.14

10.17. 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 budeme diskutovat kořeny polynomů.

Směřujeme tedy ke zobecnění rozkladů polynomů nad číslenými obory a k tomu nejprve potřebujeme ujasnit, co je dělitelnost v základním okruhu $\mathbb{K}$ samotném. Uvažujme proto nějaký pevně zvolený obor integrity $\mathbb{K}$, třeba celá čísla $\mathbb{Z}$ nebo okruh $\mathbb{Z}_p$ s prvočíselným p.

- je-li $a|b$ a zároveň $b|c$ pak také $a|c$;

[3] Formálně bychom mohli naopak za polynom považovat nekonečný výraz pro $i = 0, \ldots, \infty$ s podmínkou, že jen konečně mnoho koeficientů je nenulových.

- $a|b$ a zároveň $a|c$ pak také $a|(\alpha b+\beta c)$ pro všechny $\alpha,\beta\in\mathbb{K}$;
- $a|0$ pro všechny $a\in\mathbb{K}$ (je totiž $a\cdot 0=0$);
- 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})

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 $a_1,\dots,a_r\in\mathbb{K}$ takové, že $a=a_1\cdot a_2\dots a_r$
- jsou-li prvky $a_1,\dots,a_r$ a $b_1,\dots,b_s$ nerozložitelné, nejsou mezi nimi žádné jednotky a $a=a_1a_2\dots a_r=b_1b_2\dots b_s$, pak je $r=s$ a ve vhodném přeuspořádání platí $a_j=e_jb_j$ pro vhodné jednotky e_j.

Příklad. (1) $\mathbb{Z}$ je obor integrity s jednoznačným rozkladem.
(2) Každé pole (komutativní těleso) je obor integrity s jednoznačným rozkladem (a každý nenulový prvek je jednotka).
(3) Nechť $\mathbb{K}$ má prvky tvaru $a_0+\sum_{i=1}^k a_i\left(\sqrt[2^{n_i}]{x^{m_i}}\right)$ kde $a_0,\dots,a_k\in\mathbb{Z}$, $m_i,n\in\mathbb{Z}_{>0}$. Pak jednotky jsou pouze prvky ±1, všechny prvky s $a_0=0$ jsou rozložitelné, ale např. výraz x nelze vyjádřit jako součin nerozložitelných. (Nerozložitelných je zde příliš málo.)

10.15

10.18. Dělení se zbytkem a kořeny polynomu. Základním nástrojem pro diskusi dělitelnosti, společných dělitelů apod. v okruhu celých čísel $\mathbb{Z}$ je 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, $g\neq0$. Pak existuje $a\in\mathbb{K}$, $a\neq0$, 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 $f=a_0+\dots+a_nx^n$, $g=b_0+\dots+b_mx^m$. Buď platí $b_mf-a_nx^{n-m}g=0$ a nebo je $\deg(b_mf-a_nx^{n-m}g)<\deg f$. V prvém případě jsme hotovi, ve druhém pak, podle indukčního předpokladu, existují a',q',r' splňující $a'(b_mf-a_nx^{n-m}g)=q'g+r'$ a buď $r'=0$ nebo $\deg r'<\deg g$. Tzn.

$$a'b_mf=(g'+a'a_nx^{n-m})g+r'.$$

Přitom je-li $b_m=1$ nebo $BbbK$ je pole, pak podle indukčního předpokladu lze volit $a'=1$ a q',r' jsou tak určeny jednoznačně. V takovém případě ovšem získáme $b_mf=(g'+a_nx^{n-m})g+r'$ a je-li $BbbK$ pole, můžeme rovnost vynásobit b^{-1}.

Předpokládejme, že $f=q_1g+r_1$ 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 $q-q_1\neq0$ (určitě existuje). Potom jeho součin se členem nejvyššího stupňe 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 $r = r_1$. □

Proceduru dělení se zbytkem můžeme okamžitě využít k diskusi kořenů polynomů. Uvažme tedy polynom $f(x) \in \mathbb{K}[x]$, $\deg f > 0$, 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. $r \in BbbK$. 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.*

Tento výsledek také ověřil Tvrzení 10.16, protože dva polynomy nad nekonečným komutativním okruhem, které zadávají stejné zobrazení $\mathbb{K} \to \mathbb{K}$, mají rozdíl, jehož kořenem je každý prvek v $\mathbb{K}$. To však není možné, protože rozdíl polynomů má jen konečný stupeň, pokud není nulový.

10.16

10.19. Největší společný dělitel polynomů. Nejprve si připomeňme, že h je *největší společný dělitel* dvou polynomů a f a $g \in \mathbb{K}[x]$ jestliže:

- $h|f$ a zároveň $h|g$
- jestliže $k|f$a zároveň $k|g$ pak také $k|h$.

Důsledek (Bezoutova rovnost)**.** *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 (K je pole, takže to vždy umíme jednoznačně, viz. předchozí 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.

$$\begin{aligned} h = r_p &= r_{p-2} - q_p r_{p-1} \\ &= r_{p-2} - q_p(r_{p-3} - q_{p-1}r_{p-2}) \\ &= -q_p r_{p-3} + (1 + q_{p-1})r_{p-2} \\ &= -q_p r_{p-3} + (1 + q_{p-1}q_p)r_{p-2} \\ &= -q_p r_{p-3} + (1 + q_p q_{p-1})(r_{p-4} - q_{p-2}r_{p-3}) \\ &\vdots \\ &= Af + Bg. \end{aligned}$$

□

Zformulujeme si nyní velice elegantní tvrzení, jehož důkaz je poměrně technický a nebudeme jej prezentovat v detailech (i když jsme si vše potřebné pro něj již v podstatě připravili).

10.17 **10.20. 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 jednoznačný rozklad. Pokud je totiž f_1 dále rozložitelné, 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 $f = f_1 \dots f_r$ na nerozložitelné polynomy $f_1, \dots, f_r$.

Z našeho dodatečného předpokladu také plyne, že každý nerozložitelný polynom h dělící f, dělí některý z $f_1, \dots, f_r$. Proto pro každý další rozklad $f = f'_1 f'_2 \dots f'_s$ 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. Tento důkaz zde nebudeme provádět. □

Důsledkem této věty je skutečnost, že každý polynom nad komutativním okruhem s jednoznačným rozkladem můžeme rozložit tak, jak to známe s polynomy s reálnými nebo komplexními koeficienty. Pokud má polynom tolik kořenů, včetně násobnosti, jako je jeho stupeň $\deg f = k$, je odpovídající rozklad tvaru

$$f(x) = (x - a_1) \cdot (x - a_2) \dots (x - a_k).$$

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 s (v podstatě) kompletním důkazem:

10.18 **10.21. 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 všechny $z \in \mathbb{C}$. Definujme zobrazení

$$\varphi : \mathbb{C} \to \mathbb{C}, \quad z \mapsto \frac{f(z)}{|f(z)|}$$

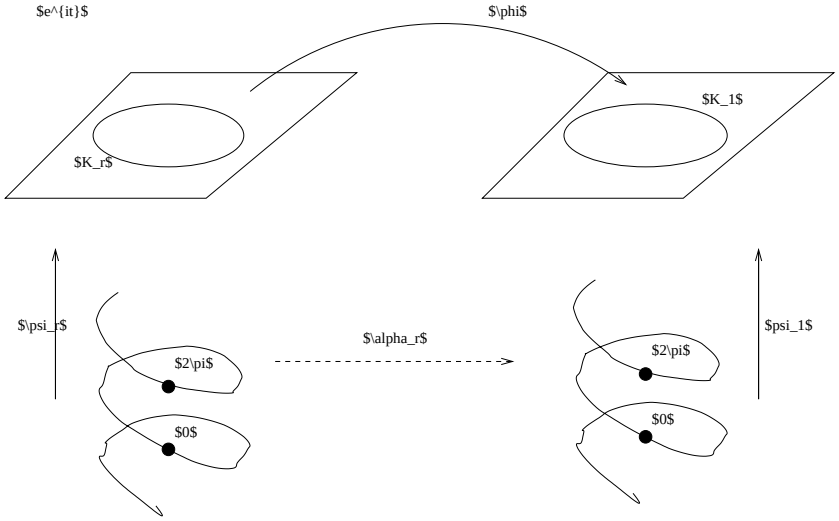
tj. φ zobrazí celé $\mathbb{C}$ do jednotkové kružnice $K_1 = \{\mathrm{e}^{it}, t \in \mathbb{R}\} \subset \mathbb{R}^2 = \mathbb{C}$. Díky našemu předpokladu o nenulovosti $f(z)$ je to skutečně dobře definované zobrazení. Dále definujme zobrazení s hodnotami v kružnici $K_r \subset \mathbb{C}$ se středem 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 κ na parametru r navíc vyplývá existence zobrazení $\alpha_r : \mathbb{R} \to \mathbb{R}$ jednoznačně zadaných podmínkami $0 \leq \alpha_r(0) < 2\pi$ a $\kappa_r(t) = e^{i\alpha_r(t)}$. Získané zobrazení α_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 α 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 α_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.

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 $z = r(\cos\alpha + i \sin\alpha)$.

$$z^d = r^d(\cos d\alpha + i \sin d\alpha) = r^d e^{id\alpha}$$
$$\frac{z^d}{|z^d|} = 1(\cos d\alpha + i \sin d\alpha) = e^{id\alpha}$$

zobrazení φ je tedy v tomto případě pouze „zatočení“ na jednotkové kružnici. Pak tedy $\kappa_r(t) = e^{idt}$ 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 $d = 0$. □

10.22. Řešené příklady.

10.22.1. *Určete inverze prvků* 17, 18 *a* 19 *v* $(\mathbb{Z}_{131}^*, \cdot)$, *tedy v grupě invertibilních prvků ze* $\mathbb{Z}_{131}$ *s operací násobení.*

Řešení. Nalezneme pomocí Eukleidova algoritmu: $131 = 7 \cdot 17 + 12$,
$17 = 12 + 5$,
$12 = 2 \cdot 5 + 2$,
$5 = 2 \cdot 2 + 1$,
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 $[19]^{-1} = 69$.

□

10.22.2. *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 okruhem skalárů jsou jednotky právě všechny skaláry. Násobíme tak, abychom se v co největší míře vyhnuli počítání se zlomky.

$$2x^4+4x^3+6x^2+4x+2 : 2x^3+3x^2+3x+1 = x+\frac{1}{2}$$
$$2x^4+3x^3+3x^2+x$$
$$x^3+3x^2+3x+2$$
$$x^3+\frac{3}{2}x^2+\frac{3}{2}x+\frac{1}{2}$$
$$\frac{3}{2}x^2+\frac{3}{2}x+\frac{3}{2}$$

Dále dělíme polynom $2x^3+3x^2+3x+1$ zbytkem $\frac{3}{2}x^2+\frac{3}{2}x+\frac{3}{2}$ (pronásobeným jednotkou $\frac{2}{3}$)

$$2x^3+3x^2+3x+1 : x^2+x+1 = 2x+1$$
$$2x^3+2x^2+2x$$
$$x^2+x+1$$

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):

$$x^4+2x^3+3x^2+2x+1 = (x+\frac{1}{2}-i\frac{\sqrt{3}}{2})^2(x+\frac{1}{2}+i\frac{\sqrt{3}}{2})^2.$$

Rozklad nad $\mathbb{R}$ pak dostaneme vynásobením kořenových závorek odpovídajících komplexně sdruženým kořenům polynomu (tento součin musí být polynom s reálnými koeficienty, ověřte!):

$$x^4+2x^3+3x^2+2x+1 = (x^2+x+1)^2.$$

- 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.

□

10.23. Poznámka. Připomeňme na tomto místě známé tvrzení, že jedinými ireducibilními polynomy nad $\mathbb{R}$ jsou lineární polynomy a kvadratické polynomy se záporným diskriminantem. Toto tvrzení vyplývá i z úvah v předchozím příkladě.

10.23.1. *Rozložte polynom*
$$x^5+3x^3+3$$
na ireducibilní složky nad
(1) $\mathbb{Q}$
(2) $\mathbb{Z}_7$

Řešení.

(1) Podle Eisensteinova kriteria je daný polynom ireducibilní nad $\mathbb{Z}$ i $\mathbb{Q}$ (použijeme prvočíslo 3)
(2) $(x-1)^2(x^3+2x^2-x+3)$. 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).

□

10.23.2. *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
$$(x-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2})(x-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2})(x+\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2})(x-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}).$$
- Vynásobením kořenových činitelů komplexně sdružených kořenů v rozkladu nad $\mathbb{C}$ dostáváme rozklad nad $\mathbb{R}$:
$$(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1).$$

□

10.23.3. *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 $\operatorname{st} Q(x) \leq 2007$. 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 (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 $P(x)$. □

10.23.4. *Najděte všechny irreducibilní polynomy stupně nejvýše 2 nad $\mathbb{Z}_3$.*

Řešení. Nerozložitelné jsou z definice všechny lineární mnohočleny. Nerozložitelné polynomy stupně dva dostame 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: $(x+1)^2 = x^2+2x+1$, $(x+2)^2 = x^2+x+1$, $(2x+1)^2 = (2\cdot(x+2))^2 = x^2+x+1$, $(2x+2) = x^2+2x+1$, 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. □

10.23.5. *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

$$x^4+x^3+x+2 = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd.$$

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, b je nula, z první rovnice je pak druhé z nich jednička. Ze třetí rovnice $2a+c=1$, je tedy $a=0$, $c=1$. Celkem

$$x^4+x^3+x+2 = (x^2+1)(x^2+x+2).$$

□

10.23.6. *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. □

10.24. Příklady na procvičení.

10.24.1. *Nalezněte inverzi prvku $[49]_{\mathbb{Z}_{253}}$ v $\mathbb{Z}_{253}$*

Řešení. 31 □

10.24.2. *Nalezněte inverzi prvku $[37]_{\mathbb{Z}_{208}}$ v $\mathbb{Z}_{208}$.*

Řešení. 45 □

10.24.3. *Nalezněte inverzi prvku* $[57]_{\mathbb{Z}_{359}}$ *v* $\mathbb{Z}_{359}$.

Řešení. 63. □

10.24.4. *Nalezněte inverzi prvku* $[17]_{\mathbb{Z}_{40}}$ *v* $\mathbb{Z}_{40}$.

Řešení. 33. □

10.24.5. *Rozhodněte, zda je následující polynom nad* $\mathbb{Z}_3$ *ireducibilní, případně nalezněte jeho rozklad na ireducibilní faktory:*

$$x^5 + x^2 + 2x + 1$$

Řešení. $x^5 + x^2 + 2x + 1 = (x^2 + 1)(x^3 + 2x + 1)$ □

10.24.6. *Rozhodněte, zda je následující polynom nad* $\mathbb{Z}_3$ *ireducibilní, případně nalezněte jeho rozklad:*

$$x^4 + 2x^3 + 2$$

Řešení. $x^4 + 2x^3 + 2$ je ireducibilní. Nemá kořeny a není součinem dvou polynomů stupně 2 (nutno početně ověřit!). □

10.24.7. *Nalezněte všechny normované ireducibilní polynomy stupně* 3 *nad* $\mathbb{Z}_3$.

10.25. Eulerova funkce. Eulerova funkce $\varphi : \mathbb{N} \to \mathbb{N}$ udává počet čísel nepřevyšujících n s číslem n nesoudělných. Je-li $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ rozklad přirozeného čísla n na prvočísla, pak

$$\varphi(n) = \prod_{i=1}^{s} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$$

Tvrzení. *Eulerova věta. Pro nesoudělná* (a, m), $a, m \in \mathbb{Z}$ *platí*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Důkaz. Grupa všech invertibilních prvků v Z_m má $\varphi(m)$ prvků, jedná se tedy o speciální případ důsledku 10.10. □

Bezprostředním důsledkem je potom

10.26. Důsledek. *Malá Fermatova věta. Buď* p *prvočíslo a nechť* a *je celé číslo, které není násobkem* p. *Potom*

$$a^{p-1} \equiv 1 \pmod{p}$$

10.27. Čínská věta o zbytcích. Vrátíme se nyní k dělitelnosti v oboru celých čísel a souvisejícím pojmům, které nám budou později užitečné při diskusi některých kódů a šifer.

Čínská věta o zbytcích, nebo též Čínská zbytková věta, má, jak její název napovídá, původ v Číně. Objevuje se v knize Sun Tsu Suan Ching (Sun Tsuovy klasické počty) ze 4.století, kde je ilustrována na příkladu:

> Máme jistý neznámý počet předmětů. Pokud je rozdělíme do trojic, zbydou dva. Při dělení do pětic zbydou tři, při dělení do sedmic zůstanou opět dva. Kolik předmětů máme?

Tvrzení. *Buď $m_1, m_2, \ldots, m_n$ navzájem nesoudělná přirozená čísla (větší než jedna) a nechť $a_1, a_2, \ldots, a_r$ jsou libovolná celá čísla, pak má soustava kongurencí*

$$\begin{aligned} x &\equiv a_1 && \pmod{m_1} \\ x &\equiv a_2 && \pmod{m_2} \\ &\vdots \\ x &\equiv a_r && \pmod{m_r} \end{aligned}$$

s jednou neznámou x, právě jedno řešení v množině $\{1, 2, \ldots, m_1 m_2 \cdots m_r\}$.

Důkaz. Označme $M := m_1 m_2 \cdots m_r$. Potom pro libovolné i, $1 \leq i \leq r$ je m_i nesoudělné s M/m_i, existuje tedy nějaké $b_i \in \{1, \ldots, m_i - 1\}$ tak, že $b_i(M/m_i) \equiv 1 \pmod{m_i}$ (čísla 0, $1 \cdot M/m_i$, $2 \cdot M/m_i, \ldots, (m_i - 1)(M/m_i)$ vyčerpávají díky nesoudělnosti m_i a M/m_i všechny zbytkové třídy při dělení m_i). Všimněme si, že $b_i(M/m_i)$ je dělitelné všemi m_j, $1 \leq j \leq n$, $i \neq j$. Proto je $x := a'_1 b_1(M/m_i) + a'_2 b_2(M/m_2) + \cdots + a'_n b_n(M/m_n)$ řešením dané kongruence, kde $a'_i \equiv a_i \pmod{m_i}$ a $a'_i \in \{0, \ldots, m_i - 1\}$. □

Čínskou větu o zbytcích můžeme také ekvivalentně sformulovat v řeči okruhů a jejich izomorfismů:

Tvrzení. *Okruh $\mathbb{Z}_{mn}$ je izomorfní okruhu $\mathbb{Z}_m \times \mathbb{Z}_n$ právě, když je největší společný dělitel (m, n) roven 1.*

Důkaz. Definujeme $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ vztahem

$$f([x]_{mn}) = ([x]_m, [x]_n).$$

To je zjevně homomorfismem aditivních grup a zároveň přímý výpočet ukazuje, že jde i o homomorfismus multiplikativních grup, který jedničku zobrazuje na jedničku. □

10.28. Příklady.

10.28.1. *Najděte poslední dvě cifry čísla 7^{9^9}.*

Řešení. Poslední dvě cifry daného čísla je jeho zbytek po dělení číslem 100. Stačí tedy určit zbytek čísla 7^{9^9} po dělení číslem 100. K tomu si všimněme, že $7^4 \equiv 1 \pmod{100}$ (z Eulerovy věty víme pouze, že $7^{\varphi}(100) = 7^40 \equiv 1 \pmod{100}$ a nejmenší číslo t splňující $7^t \equiv 1 \pmod{100}$ musí být dělitelem $\phi(100) = 40$.). Dále víme, že $9 \equiv 1 \pmod 4$, proto i $9^9 \equiv 1 \pmod 4$. Celkem

$$7^{9^9} = 7^{4k+1} = \underbrace{\left(7^k\right)^4}_{\equiv 1} \cdot 7 \equiv 7 \pmod{100}.$$

Poslední dvě cifry čísla 7^{9^9} jsou tedy 07. □

10.28.2. *Určete poslední tři cifry čísla $13^{10^{11}}$.*

Řešení. Tři poslední cifry jsou zbytkem po dělení daného čísla čísla číslem 1000. Ten jednoznačně určíme podle Čínské zbytkové věty pokud určíme zbytky po dělení nesoudělnými čísly 125 a 8. Protože $(13, 125) = 1$ $\varphi(125) = 100$, platí

$$13^{100} \equiv 1 \pmod{1}25.$$

Zřejmě $10^1 1$ je násobkem čísla 100, a tedy

$$13^{10^{11}} = 13^{10^2 \cdot 10^9} = \left(13^{10^2}\right)^{10^9} \equiv 1^{10^9} \equiv 1 \pmod{125}.$$

Podobně $(8, 13)$=1, $\varphi(8) = 4$ a

$$13^{10^{11}} = 13^{4k} = \left(13^4\right)^k \equiv 1^k \equiv 1 \pmod{8}$$

Mezi čísly 0,1,...,999 existuje podle Čínské zbytkové věty právě jedno číslo, které dává zbytek 1 jak po dělení osmi tak po dělení 125 a tím je číslo 1. Poslední tři cifry čísla $13^{10^{11}}$ jsou tedy 001.

Mohli vyšetřovat přímo zbytek po dělení číslem 1000. Víme, že $\varphi(1000) = 400$ a $400|10^{11}$, tedy $13^{10^{11}} \equiv 1 \pmod{1000}$. Obecně ale bývá početně výhodnější pracovat s nižšími moduly. □

10.28.3. *Určete poslední tři cifry čísla* $12^{10^{11}}$.

Řešení. Stejně jako v předchozím příkladě budeme zkoumat zbytky po dělení nesoudělnými čísly 125 a 8. Víme, že $(12, 125) = 1$, tedy

$$12^{10^{11}} \equiv 12^{10^2 \cdot 10^9} = \left(12^{10^2}\right)^{10^9} \equiv 1^{10^9} \equiv 1 \pmod{1)25}.$$

Dále $4|12$ tedy $12^{10^{11}}$ je dělitelné dokonce číslem $4^{10^{11}}$, zejména tedy číslem 8, tedy $12^{10^{11}} \equiv 0 \pmod{8}$. Podle Čínské zbytkové věty existuje je právě jedno z čísel $0, 1, \cdot 999$, které 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 po té zkoumáme dělitelnost osmi). Poslední tři cifry čísla $13^{10^{11}}$ jsou tedy 376. □

10.28.4. *Dokažte, že pro libovolné prvočíslo* $p \in \mathbb{N}$ *platí:* $p|(p-1)^{p^2-1} - 1$.

Řešení.

$$(p-1)^{p^2-1} - 1 = \left((p-1)^{(p-1)}\right)^{(p+1)} - 1 \equiv 1^{(p+1)} - 1 = 0 \pmod{p}$$

□

10.19

10.29. Polynomy více proměnných. Okruhy polynomů v proměnných $x_1, \ldots, x_r$ definujeme induktivně vztahem

$$\mathbb{K}[x_1, \ldots, x_r] := \mathbb{K}[x_1, \ldots, x_{r-1}][x_r].$$

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 (proveďte si to!), že polynomy v proměnných $x_1, \ldots, x_r$ lze 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 se často zavádí tzv. multiidexová symbolika. *Multiindex* α délky r je r-tice nezáporných celých čísel $(\alpha_1, \ldots, \alpha_r)$. Celé číslo $|\alpha| = \alpha_1 + \cdots + \alpha_r$ nazýváme *velikost*

multiindexu α. Stručně pak píšeme x^α místo $x_1^{\alpha_1}x_2^{\alpha_2}\dots x_r^{\alpha_r}$. Pro polynomy v r proměnných pak máme symbolické vyjádření velice podobné obvyklému značení pro polynomy v jedné proměnné:

$$f=\sum_{|\alpha|\le n} a_\alpha x^\alpha,\ g=\sum_{|\beta|\le m} a_\beta x^\beta \in \mathbb{K}[x_1,\dots,x_r].$$

Říkáme, že f má celkový stupeň n, je-li alespoň jeden z koeficientů s multiindexem α velikosti n nenulový.

Okamžitě se také nabízejí analogické vzorce pro sčítání a násobení polynomů

$$f+g=\sum_{|\alpha|\le \max(m,n)} (a_\alpha+b_\alpha)x^\alpha$$

$$fg=\sum_{|\gamma|=0}^{m+n}\left(\sum_{\alpha+\beta=\gamma}(a_\alpha b_\beta)x^\gamma\right)$$

kde multiindexy se sčítají po složkách a formálně neexistující koeficienty považujeme za nulové.

Samozřejmě musíme ověřit, že tyto vzorce opravdu popisují sčítání a násobení v induktivně definovaném okruhu polynomů v r proměnných. Dokážeme to indukcí přes počet proměnných. Předpokládejme, že vztahy platí v $\mathbb{K}[x_1,\dots,x_{r-1}]$ a počítejme součet

$$f=a_k(x_1,\dots,x_{r-1})x_r^k+\dots+a_0(x_1,\dots,x_{r-1})=\left(\sum_\alpha a_{k,\alpha}x^\alpha\right)x_r^k+\dots$$

$$g=b_l(x_1,\dots,x_{r-1})x_r^l+\dots+b_0(x_1,\dots,x_{r-1})=\left(\sum_\beta b_{l,\beta}x^\beta\right)x_r^k+\dots$$

$$\begin{aligned} f+g&=\big(a_0(x_1,\dots,x_{r-1})+b_0(x_1,\dots,x_{r-1})\big)+\\ &\qquad+\big(a_1(x_1,\dots,x_{r-1})+b_1(x_1,\dots,x_{r-1})\big)x_r+\dots\\ &=\big(\sum_\gamma(a_{k,\gamma}+b_{k,\gamma})(x_1,\dots,x_{r-1})^\gamma\big)x_r^k+\dots+\big(\sum_\gamma(a_{0,\gamma}+b_{0,\gamma})(x_1,\dots,x_{r-1})^\gamma\big)\\ &=\sum_{(\gamma,j)}(a_{j,\gamma}+b_{j,\gamma})(x_1,\dots,x_{r-1})^\gamma x_r^j. \end{aligned}$$

Podobně se provede důkaz pro součin (proveďte!).

Jako důsledek naší definice a předchozích výsledků pro polynomy nad obecnými komutativními okruhy dostaneme:

Důsledek. (1) *Jestliže v okruhu $\mathbb{K}$ nejsou dělitelé nuly, pak také v okruhu polynomů $\mathbb{K}[x_1,\dots,x_r]$ nejsou dělitelé nuly.*

(2) *Je-li $\mathbb{K}$ obor integrity s jednoznačným rozkladem, pak také okruh polynomů $\mathbb{K}[x_1,\dots,x_r]$ je obor integrity s jednoznačným rozkladem.*

Důkaz. Budeme postupovat indukcí přes počet proměnných r. [4] Pro $r=1$ uvažujme polynomy $f=a_nx_1^n+\dots+a_1x_1+a_0$ a $g=b_mx^m+\dots+b_0$, přičemž $b_m\neq 0$ a $a_n\neq 0$. Vedoucí člen součinu fg je $a_nb_mx^{n+m}$, protože $a_nb_m\neq 0$, 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 $\mathbb{K}[x_1,\dots,x_{r-1}]$.

Druhé tvrzení vyplývá s induktivní definice polynomů v r proměnných a z Věty 10.20. □

[4] Důkaz lze vést také přímo s použitím multiindexových formulí pro součin, ale museli bychom si nadefinovat určité vhodné uspořádání monomů, abychom mohli pracovat s vedoucím koeficientem. Zkuste si to!

10.20

10.30. Podílová tělesa. 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 $\mathbb{K}[x_1,\dots,x_r]$ nazýváme *těleso racionálních funkcí* a značíme je $\mathbb{K}(x_1,\dots,x_r)$. Všechny algebraické operace s polynomy v softwarových systémech jako je Maple nebo Mathematica jsou prováděny ve skutečnosti nad podílovými tělesy, tj. v tělesech raciolnálních funkcí, zpravidla s použitím $\mathbb{K}=\mathbb{Q}$.

3. Uspořádané množiny a Booleovská algebra

Tak jako jsme z vlastností čísel nebo symetrií objektů abstrahovali podstatné axiomy a dostali jsme daleko šířeji použitelné nástroje linerární algebry, teorie grup apod., nyní budeme postupovat obdobně a za východisko si vezmeme základní operace s množinami, tj. jejich sjednocení, průnik a vztahy inkluze.

10.21

10.31. Množinová algebra. S každou množinou M máme 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 se častěji značí $\cup$ a $\cap$. Dále máme ke každé množině $A\in K$ také její množinu doplňkovou 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, a obdobně se chová prázdná množina $\emptyset\in K$ vůči operaci $\wedge$. Tu budeme v této souvislosti značit jako 0.

Na množině K všech podmnožin v M přitom platí pro všechny prvky A,B,C následující vlastnosti:

(1) $A\wedge(B\wedge C)=(A\wedge B)\wedge C$, $\quad A\vee(B\vee C)=(A\vee B)\vee C$

(2) $A\wedge B=B\wedge A$, $\quad A\vee B=B\vee A$

(3) $A\wedge(B\vee C)=(A\wedge B)\vee(A\wedge C)$, $\quad A\vee(B\wedge C)=(A\vee B)\wedge(A\vee C)$

(4) existuje 0 tak, že $A\vee 0=A$

(5) existuje 1 tak, že $A\wedge 1=A$

(6) $A\wedge A'=0$, $\quad A\vee A'=1$.

Vlastnost (1) je asociativní zákon pro obě operace, (2) je komutativita, (3) je distributivita obou operací. Poslední vlastnost (6) vystihuje vlastnosti komplementu.

Definice. Množině K spolu s dvěmi binárními operacemi $\wedge$ a $\vee$ a jednou unární operací $'$ splňující vlastnosti (1)–(7) říkáme *Booleovská algebra*. Operaci $\wedge$ budeme říkat *infimum* (případně *sjednocení*, anglicky často také *meet*), operaci $\vee$ budeme říkat *supremum* (případně *průnik*, anglicky také *join*). Prvku A' se říká *doplněk* k prvku A.

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*.

Jako obvykle si hned odvodíme několik elementárních důsledků axiomů. Zejména si povšimněme, že stejně jako u speciálního případu Booleovské algebry všech podmnožin v dané množině M je doplněk k $A \in K$ určen jednoznačně (tj. máme-li dáno $(K, \wedge, \vee)$, může existovat nejvýše jedna unární operace, se kterou dostaneme Booleovskou algebru). Skutečně, pokud B a $C \in K$ splňují vlastnosti A', 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 podobně také $C = C \vee B$. Je tedy nutně $B = C$.

V následujícím výčtu se vlastnostem (2) říká *absorpční zákony*, vlastnosti (3) popisují *idempotentnost* operací a (4) jsou tzv. *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:

$$A \wedge 0 = A \wedge (A \wedge A') = (A \wedge A) \wedge A' = A \wedge A' = 0$$
$$A \wedge (A \vee B) = (A \vee 0) \wedge (A \vee B) = A \vee (0 \wedge B) = A \vee 0 = A$$
$$A = A \wedge (A \vee A') = (A \wedge A) \vee 0 = A \wedge A$$

a první tři dvojice tvrzení máme dokázány. 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

$$(A \wedge B) \wedge (A' \vee B') = ((A \wedge B) \wedge A') \vee ((A \wedge B) \wedge B') = (0 \wedge B) \vee (A \wedge 0) = 0.$$

Obdobně, s použitím (2) dostáváme

$$(A \wedge B) \vee (A' \wedge B') = (A \vee (A' \vee B')) \vee (B \vee (A' \vee B')) = (1 \vee B') \wedge (1 \vee A') = 1.$$

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 $A = (A')'$. □

10.22

10.32. Výroková logika jako Booleova algebra. V předchozím odstavci jsme použili symboliku, kterou je často rozumné interpretovat tak, že z prvků $A, B, \dots \in K$ tvoříme „slova“ pomocí operací $\vee$, $\wedge$, $'$ a závorek vyjasňujících v jakém pořadí a na jaké argumenty jsou operace aplikovány. Samotné axiomy 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 $A, B, \dots$ a logických operací AND (binární operace $\wedge$), OR (binární operace $\vee$) a negace NOT (unární operace $'$). Takové 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 nejjednoduší 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.

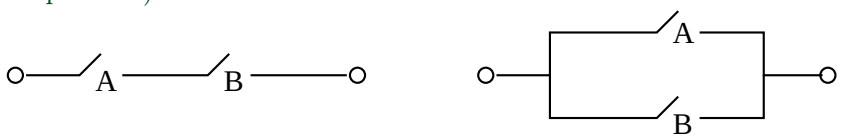
Výrok obsahující k elementárních výroků tedy představuje funkci $(\mathbb{Z}_2)^k \to \mathbb{Z}_2$ a dva výroky nazýváme logicky ekvivalentní, jestliže zadávají stejnou funkci. Snadno se nyní přímo ověří, že na množině tříd logicky ekvivalentních výroků jsme takto zadefinovali strukturu Booleovy algebry (je pouze třeba projít naše axiomy a ověřit je). 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 $A' \vee B'$. Všimněme si také, že XOR odpovídá v množinové algebře symetrickému rozdílu množin.

10.23

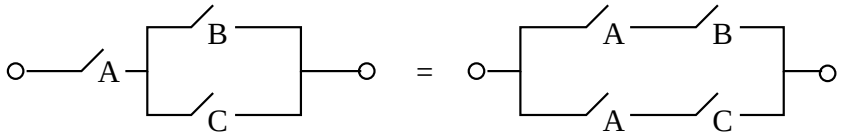
10.33. Přepínače jako Booleova algebra. Přepínač je pro nás černá skříňka, která má jen dva stavy, buď je zapnut (a signál prochází) nebo naopak vypnut (a signál neprochází).



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 $A, B, \dots$ 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 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.



10.24

10.34. Dělitelé. Dalším přirozeným příkladem Booleovské algebry je systém dělitelů přirozeného čísla nebo polynomu.

Zvolme pevně takové 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 klademe $p = 1 \in D_p$ a neutrálním prvkem vůči supremu je jednička v $\mathbb{Z}$, resp. $1 \in \mathbb{K} \subset \mathbb{K}[x_1, \ldots, x_s]$. Unární operaci $'$ dostáváme pomocí dělení: $q' = p/q$.

Lemma. *Množina D_p spolu s výše uvedenými operacemi $\wedge$, $\vee$ a $'$ je Booleova algebra právě, když rozklad p neobsahuje kvadráty (tj. v jednoznačném rozkladu $p = q_1 \ldots q_n$ 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 nešeho 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 axiomu (1) v 10.31. Komutativita, tj. axiom (2) je zcela zřejmá.

Pro tři libovolné prvky a, b, a c můžeme bez újmy na obecnosti psát jejich rozklad ve tvaru $a = q_1^{p_1} \ldots q_s^{p_s}$, $b = q_1^{m_1} \ldots q_s^{m_s}$ a $c = q_1^{k_1} \ldots q_s^{k_s}$, kde připouštíme i mocniny 0 a všechny prvky q_j jsou po dvou nesoudělné. $a \wedge b$ 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. Přímo se nyní snadno ověří distributivní zákony.

Problém nemáme ani s existencí prvku 0 a 1, které jsme přímo definovali a zjevně splňují axiomy (4) a (5). Existecne kvadrátů ale znemožní definici 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 jako $q' = p/q$. Snadno ověříme potřebné vlastnosti z axiomů (4)–(6). □

10.25

10.35. 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 hovoříme také o *částečném uspořádání* a množina $(K, \leq)$ vybavená částečným uspořádáním se nazývá *poset* (z anglického „partial ordered set“).

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 $A \subset B$ právě, když $A \wedge B = A$. Ekvivalentně, $A \subset B$ právě, když $A \vee B = B$.

Lemma. *Je-li $(K, \wedge, \vee, ')$ Booleova algebra, pak relace $\leq$ definovaná vytahem $A \leq B$ právě, když $A \wedge B = A$, je částečné uspořádání. Navíc 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* $A \leq 1$ *pro všechny $A \in K$.*

Důkaz. Všechny dokazované vlastnosti a vztahy jsou výsledkem jednoduchého výpočtu v Booleovské algebře K. Začněme s vlastnostmi uspořádání pro $\leq$. Reflexivita je přímým důsledkem 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 dává tranzitivitu.

Dále počítáme $(A \wedge B) \wedge A = (A \wedge A) \wedge B = A \wedge B$, takže $A \wedge B \leq A$. Ze vztahu $A \wedge (A \vee B) = A$ plyne $A \leq A \vee B$, což dokazuje tvrzení (2). Distributivita ukazuje $(A \vee B) \wedge C = (A \wedge C) \vee (B \wedge C)$, což zapředpokladu (3) dává $A \vee B$, takže skutečně platí (3). Tvrzení (5) plyne přímo z axiomů pro 1 a 0. 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 dokázali jsme i zbývající tvrzení (4). □

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.

10.26

10.36. Svazy. Viděli jsme, že každá Booleova algebra zadává poset $(K, \leq)$. Zdaleka ne každý poset 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 zvoleným posetem $(K, \leq)$. O prvku $C \in K$ řekneme, že je *dolní závorou* pro nějakou množinu prvků $L \subset K$, je-li $C \leq A$ pro všechny $A \in L$. Prvek $C \in K$ je *infimem množiny* $L \subset K$, jestliže je dolní závorou a pro každou jinou dolní závoru D téže množiny platí $D \leq C$.

Obdobně definujeme *horní závory* a *supremum* podmnožiny L záměnou $\leq$ za $\geq$ v posledním odstavci.

Konečné posety 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* posetu je zakreslení takového grafu v rovině tak, že větší prvky jsou zobrazeny vždy výš než menší (a orientace hran je tedy dána takto implicitně).

Definice. *Svaz* je poset $(K, \leq)$, ve kterém každá dvouprvková množina $\{A, B\}$ má supremum $A \vee B$ a infimum $A \wedge B$ 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.

Snadno lze ale nakreslit Hasseho diagram svazu, který není distributivní.

Nyní 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.

Ověřili jsme již, že v takovém případě komplementy jsou definovány jednoznačně (viz úvahy za definicí 10.31), takže je naše alternativní definice Booleovské algebry korektní.

Všimněme si také, při diskusi dělitelů daného čísla nebo polynomu p jsme narazili na svazy D_p, které jsou Booleovskou algebrou právě tehdy, když rozklad p neobsahuje kvadráty.

10.27

10.37. Normální tvary. 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 o becné Booleovy algebry sestrojíme jeho tzv. *normální disjunktivní tvar*, tj. napíšeme jej pomocí vybrané skupiny nejjednodušších prvků a operace $\vee$.

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 $B \leq A$ implikuje $B = 0$ nebo $B = A$.

Lemma. *Booleova algebra funkcí přepínačového systému s n přepínači $A_1, \dots, A_n$ má 2^n atomů, které jsou tvaru $A_1^{\sigma_1} \wedge \cdots \wedge A_n^{\sigma_n}$, kde buď $A_i^\sigma = A_i$ nebo $A_i^{\sigma_i} = A_i'$.*

Důkaz. Pro dvě funkce φ a ψ je jejich infimem funkce $\varphi \wedge \psi$, jejíž hodnoty jsou dány součinem jejich hodnot v $\mathbb{Z}_2$. Platí tedy $\varphi \leq \psi$ jestliže φ má hodnotu 1 všude kde má ψ hodnotu $1 \in \mathbb{Z}_2$. Odtud už plyne, že v naší Booleově algebře hodnotových funkcí je funkce φ atomem právě, když z 2^n hodnot φ na jednotlivých možnostech hodnot jednotlivých argumentů má právě jednou hodnotu $1 \in \mathbb{Z}_2$. Všechny takové funkce ovšem lze vytvořit právě způsobem uvedeným v dokazovaném tvrzení. □

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. Uvažme všechny atomy $A_1, A_2, \dots, A_k$ v K, které jsou menší nebo rovny B. Z vlastností uspořádání na množině K (viz 10.35(3)) je okamžitě vidět, že také

$$Y = A_1 \vee \cdots \vee A_k \leq B.$$

Dokážeme, že $B \wedge Y' = 0$, což podle 10.35(4) zaručuje $B \leq Y$. Tím bude dokázána rovnost $B = Y$.

Budeme postupně potřebovat tři jednoduchá tvrzení:

Tvrzení. *Jestliže jsou $Y, X_1, \dots, X_\ell$ atomy v K, pak $Y \le X_1 \vee \dots \vee X_\ell$ tehdy a jen tehdy, když $Y = X_i$ pro nějaké $i = 1, \dots, \ell$.*

Tvrzení. *Pro každý prvek $Y \neq 0$ v K existuje atom X, pro který je $X \le Y$.*

Tvrzení. *Jestliže jsou $X_1, \dots, X_r$ všechny atomy v K, pak $Y = 0$ právě, když $Y \wedge X_i = 0$ pro všechny $i = 1, \dots, r$.*

Důkaz. Dokončím později...

□

□

10.38. Řešené příklady.

10.38.1. *Nalezněte disjuktivní normální formu výrazu*

$$((A \wedge B) \vee C)' \wedge (A' \vee (B \wedge C \wedge D))$$

Řešení.

$$(A' \wedge C')$$

□

10.38.2. *Buď A a B prvky boolovy algebry. Ukažte, že jestliže v ní existuje prvek X takový, že $A \wedge X = B \wedge X$ a $A \vee X = B \vee X$ pak $A = B$.*

Řešení.

$$A = A \wedge (A \vee X) = A \wedge (B \vee X) = (A \wedge B) \vee (A \wedge X) = (A \wedge B) \vee (B \wedge X) \le B$$

poslední nerovnost plyne z toho, že spojení dvou prvků menších rovných než B je menší rovno B. Vzhledem k symetrii $B \le A$, tedy $A = B$. □

10.28

10.39. Homomorfismy. Jak jsme již viděli u mnoha matematických struktur, o objektech se dozvídáme informace pomocí tzv. homomorfismů, tj. zobrazení, které zachovávají příslušné operace. V případě Booleovských algeber definujeme podobně jako u okruhů:

Definice. 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) $f(A') = f(A)'$.

Homomorfismus f je izomorfismus Booleovských algeber, jestliže je f bijektivní.

Snadno se ověří, že bijektivnost f již zaručí, že f^{-1} je opět homomorfismem.

Z definice uspořádání na Booleových algebrách je zřejmé, že každý homomorfismus $f : K \to L$ bude také splňovat $f(A) \le f(B)$ pro všechny prvky $A \le B$ v K. To je definiční vlastnost pro tzv. *izotonní zobrazení* neboli *homomorfismy posetů*.

Jakkoliv umíme rekonstruovat operace suprema a infima z uspořádání, pokud toto vzniklo z Booleovy algebry, není pravda, že by každý homomorfismus posetů byl automaticky homomorfismem příslušných algeber. Zkuste si najít příklad (stačí vkládat algebru se dvěma atomy do algebry s alespoň čtyřmi atomy)!

Věta. *Každá konečná Booleova algebra je izomorfní Booleově algebře $K = 2^M$, kde M je množina atomů v K.*

Důkaz. Dokončím později. □

4. Kódy a šifry

Kódy a šifry spolu často úzce souvisí. 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 přebnášení správy. To vše je úkol kódování. Pokud navíc chceme, aby zprávu mohl číst pouze adresát, potřebujeme i tzv. šifrování.

10.29

10.40. Kódování. 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 $\mathbb{Z}_2$) a přenášíme slova o k bitech. Obdobné postupy jsou možné nad konečnými poli. Přenosové chyby chceme

- rozpoznávat
- opravovat

a za tím účelem přidáváme dodatečných $n-k$ bitů informace pro pevně zvolené $n > k$.

Všech slov o k bitech je 2^k a každé z nich má jednoznačně určovat jedno *kódové slovo* z 2^n možných. Máme tedy ještě

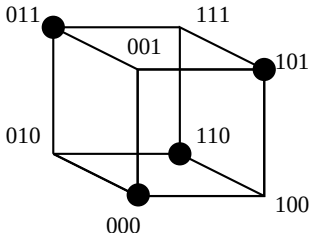
$$2^n - 2^k = 2^k(2^{n-k} - 1)$$

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 byl zaručen sudý počet jedniček ve slově.

Pokud při přenosu dojde k lichému počtu chyb, přijdeme na to. Dvě různá kódová slova se při tomto kódu vždy liší alespoň ve dvou pozicích, chybové slovo se ale od dvou různých kódových slov liší pouze v pozici jedné. Nemůžeme proto umět chyby opravovat ani kdybychom věděli, že došlo k právě jedné. Přehledně jsou všechna možná slova vidět na obrázku níže, kódová slova jsou zvýrazněna tučným puntíkem.

Navíc neumíme detekovat tak obvyklé chyby, jako je záměna dvou sousedních hodnot ve slově.



10.30

10.41. Vzdálenost slov.

Definice. *Hammingova vzdálenost* dvou slov je rovna počtu bitů, ve kterých se liší.

Věta. (1) *Kód odhaluje r a méně chyb právě, když je minimální Hammingova vzdálenost kódových slov právě $r+1$.*

(2) *Kód opravuje r a méně chyb právě, když je minimální Hammingova vzdálenost kódových slov právě $2r+1$.*

Důkaz. Obě tvrzení jsou zřejmá z předchozí diskuse. □

10.31

10.42. Konstrukce polynomiálních kódů. K praktickému použití potřebujeme efektivně konstruovat kódová slova tak, abychom je mezi všemi slovy sladno 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

$$m(x) = b_0 + b_1x + \cdots + b_{k-1}x^{k-1}.$$

Definice. Nechť $p(x) = a_0 + \cdots + a_{n-k}x^{n-k} \in \mathbb{Z}_2[x]$ je polynom s $a_0 = 1$, $a_{n-k} = 1$. *Polynomiální kód generovaný polynomem $p(x)$* je (n,k)–kód jehož slova jsou polynomy stupně menšího než n dělitelné $p(x)$.

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 víme

$$v(x) = x^{n-k}m(x) + r(x) = q(x)p(x) + r(x) + r(x) = q(x)p(x).$$

Budou tedy všechna kódová slova dělitelná $p(x)$.

Původní zpráva je obsažena přímo v polynomu $v(x)$, takže dekódování správného slova je snadné.

Příklad. (1) Polynom $p(x) = 1 + x$ generuje $(n, n-1)$–kód kontroly parity pro všechna $n \geq 3$.
(2) Polynom $p(x) = 1 + x + x^2$ generuje $(3,1)$–kód opakování bitů.

První tvrzení plyne z toho, že $1+x$ dělí polynom $v(x)$ tehdy a jen tehdy, když $v(1) = 0$ a to nastane tehdy, když je ve $v(x)$ sudý počet nenulových koeficientů. Druhé je zřejmé.

10.32

10.43. Detekce chyb. Přenos slova $v \in (\mathbb{Z}_2)^n$ dopadne příjmem polynomu

$$u(x) = v(x) + e(x)$$

kde $e(x)$ je tzv. *chybový polynom* repzentující vektor chyby přenosu.

Chyba je rozpoznatelná pouze, když generátor kódu $p(x)$ nedělí $e(x)$. Máme proto zájem o polynomy, které 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 $n \leq 2^m - 1$ rozpoznává příslušný $(n, n-m)$–kód všechny jednoduché a dvojité chyby.*

Důkaz. Důkaz doplním. □

Důsledek. *Je-li $q(x)$ primitivní polynom stupně m, pak pro všechna $n \leq 2^m - 1$ rozpoznává $(n, n-m-1)$–kód generovaný polynomem $p(x) = q(x)(1+x)$ všechny dvojité chyby a všechna slova s lichým počtem chyb.*

Tabulka dává o informace o výsledcích předchozích dvou vět pro několik polynomů:

primitivní polynom	kontrolní bity	délka slova
$1+x+x^2$	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.[5].

10.33

10.44. Lineární kódy. Polynomiální kódy lze efektivně popisovat také pomocí elemnetárního maticového počtu. Vyjdeme z obecnější definice, která požaduje lieární závislost kdového slova na původní informaci:

Definice. *Lineární kód* je injektivní lineární zobrazení $g : (\mathbb{Z}_2)^k \to (\mathbb{Z}_2)^n$. Matice G typu k/n reprezentující toto zobrazení v standardních bazích se nazývá generující *matice kódu*.

Pro každé slovo v je

$$u = G \cdot v$$

příslušné kódové slovo.

Věta. *Každý polynomiální (n,k)–kód je lineární kód.*

Důkaz. Vyplývá přímo z vlastností dělení polynomů se zbytkem. □

Např. matice příslušná k polynomu $p(x) = 1+x+x^2$ a odpovídajícímu $(6,3)$–kódu je

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

10.34

10.45. Věta. *Je-li g lineární kódování s maticí*

$$G = \begin{pmatrix} P \\ \mathbb{I}_k \end{pmatrix},$$

potom zobrazení $h : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^k$ s maticí

$$H = \begin{pmatrix} \mathbb{I}_{n-k} & P \end{pmatrix}$$

má následující vlastnosti

[5] detaily později

(1) $\operatorname{Ker} h = \operatorname{Im} g$
(2) *přijaté slovo u je kódové slovo právě, když je $H \cdot u = 0$*

DŮKAZ. Dodám později (je snadný) □

Matici H z věty se říká *matice kontroly parity* přílušného (n,k)–kódu.

10.35

10.46. 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 podprostor $V \subset (\mathbb{Z}_2)^n$ správných kódových slov, víme u každého výsledku, že správné slovo (s opravenými přípdnými chybami) je ve třídě rozkladu $v + V$ v prostoru $(\mathbb{Z}_2)^n/V$.

Zobrazení $h : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^{n-k}$ 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 $H \cdot u$.

Definice. Hodnota $H \cdot u$ se nazývá *syndrom* slova u.

Věta. *Dvě slova jsou ve stejné třídě rozkladu $u + V$ právě, když sdílí syndrom.*

Samoopravné kódy lze konstruovat tak, že pro každý syndrom určíme prvek v příslušné třídě, který je nejvhodnějším slovem.

10.47. Příklady.

10.47.1. *Buď dán $(6,3)$ kód nad $\mathbb{Z}_2$ generovaný polynomem $x^3 + x^2 + 1$.*

(1) *Určete jeho generující matici a matici kontroly parity.*
(2) *Dekódujte zprávu* 111101 *předpokládáte-li, že při přenosu došlo k nejmenšímu možnému počtu chyb.*

Řešení.

(1) Protože se jedná o lineární kód, stačí určit jak se zakódují bázové vektory 1, x a x^2, tedy určit zbytky polynomů x^3, x^4 a x^5 po dělení polynomem x^3+x^2+1. Máme

$$\begin{aligned} x^3 &\equiv x^2 + 1 \pmod{x^3 + x^2 + 1} \\ x^4 &= x(x^3) \equiv x(x^2+1) = x^3 + x \equiv x^2 + x + 1 \pmod{x^3 + x^2 + 1} \\ x^5 &= x(x^4) \equiv x(x^2+x+1) = x^3 + x^2 + x \equiv x + 1 \pmod{x^3 + x^2 + 1} \end{aligned}$$

Bázové vektory (zprávy) 100, 010 a 001 se tedy zakódují do vektorů (kódů) 101100, 111010 a 110001, generující matice kódu je tedy

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

Matice kontroly parity je pak dle věty 10.45

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(2) Vynásobíme-li přijatou zprávu 111101 maticí kontroly parity, dostáváme

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

tedy nenulový vektor a víme, že při přenosu došlo k chybě. Syndrom naší kódové zprávy je tedy 100. Sestavme tabulku všech syndromů a jim odpovídajících kódových slov. Syndrom 000 mají všechna kódová slova. Všechna slova s daným syndromem pak dostaneme přičtením syndromu (doplněného nulami na délku kódového slova) ke všem kódovým slovům.

Syndrom	Kódová slova s daným syndromem							
000	**000000**	110001	111010	101100	010110	001011	011101	100111
001	**001000**	111001	110010	100100	011110	000011	010101	101111
010	**010000**	100001	101010	111100	000110	011011	001101	110111
100	**100000**	010001	011010	001100	110110	101011	111101	000111
011	**011000**	101001	100010	110100	001110	010011	**000101**	111111
101	101000	011001	010010	**000100**	111110	100011	110101	001111
110	110000	**000001**	001010	011100	100110	111011	101101	010111
111	111000	001001	**000010**	010100	101110	110011	100101	011111

Počínaje druhým řádkem, je každý řádek tabulky afinním prostorem jehož zaměřením je vektorový prostor daný prvím řádkem (daný kód je lineární, všechna kódová slova tedy tvoří vektorový prostor). Zejména je tedy rozdíl každých dvou slov ve stejném řádku nějakým kódovým slovem. Tučně vyznačená slova jsou takzvaní vedoucí representanti třídy (řádku, afinního prostoru) odpovídajícího danému syndromu. Jsou to slova s nejmenším počtem jedniček v řádku. Udávají tak nejmenší počet bitových změn, které musíme v libovolném slovu na řádku provést, abychom dostali kódové slovo.

Naše kódové slovo má syndrom 100, vedoucím representantem ve třídě tohoto syndromu je slovo 100000 a jeho odečtením od obdrženého kódového slova dostaneme platné kódové slovo 011101. Je to platné kódové slovo s nejmenší Hammingovou vzdáleností od obdrženého slova (pro malý počet kódových slov lze nalézt přímo, pro větší počet je vhodnější – rychlejší – námi uvedená metoda). Odeslaná zpráva tedy byla 101.

□

10.47.2. *V lineárním* $(6,3)$*-kódu nad* $\mathbb{Z}_2$ *zadaném maticí*

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

byla přijata zpráva 110100. *Dekódujte ji (tj. nalezněte odesílanou zprávu) za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.*

Řešení. 101 □

10.47.3. *V lineárním* $(6,3)$*-kódu nad* $\mathbb{Z}_2$ *zadaném maticí*

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

byla přijata zpráva 001001. *Dekódujte ji (tj. nalezněte odesílanou zprávu) za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.*

Řešení. 011 □

10.47.4. *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 když pokud ve dvou kódových slovech změním jeden bit, nemohu dostat stejná slova. Množina slov, které dostanu z jednoho kódového slova změnou nejvýše jednoho bitu čítá (včetně původního slova) $n+1$ slov. Pro různá kódová slova musím dostat různé 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 splněna až pro $n \leq 5$. Kódová slova musí tedy mít délku minimálně 5. Hledaná kódová slova délky 5 s minimální Hammingovou vzdáleností 3 jsou například: 00111, 01001, 10100, 11010. □

10.36

10.48. Poznámky o šifrách. Šifrování slouží k tomu, abychom přenesli mezi danými (dvěma) uživateli tajnou informaci, který by měl zůstat ostatním lidem nepřístupný. Historie šifrování sahá až do starověku, kde je známým příkladem Spartská skytála. Šifry nacházely využití zejména pro vojenské účely a například prolomení německé šifry Enigma za druhé světové války poskytlo spojencům možná rozhodující převahu. V současné době se šifrují například i televizní kanály, i když názvosloví je zde odlišné od matematematického, protože se spíše hovoří o kódovaných kanálech, nikoliv o šifrovaných.

10.49. RSA Algoritmus. Jde o algoritmus, který byl publikován v sedmdesátých letech dvacátého století pány Ronem Rivestem, Adi Shamirem a Leonardem Aldlemanem v roce 1978. Tento algoritmus umožňuje výměnu soukromých informací aniž by si odesílatel a příjemce museli vyměnit nějaký tajný klíč, na jehož utajení by závisla bezpečnost algoritmus.

Vlastní algoritmus probíhá v těchto fázích:

(1) Příjemce zvolí dvě velká prvočísla p a q a dále zvolí přirozené e nesoudělné s $\varphi(N)$, kde $N = pq$, tedy $\varphi(N) = (p-1)(q-1)$.
(2) Příjemce zveřejní N a e.
(3) Příjemce spočítá $d = e^{-1} \pmod{\varphi(N)}$.

(4) Odesílatel chce odeslat zprávu Z, kde $Z \in \mathbb{N}$, $1 \leq Z \leq N-1$. Odesílatel spočítá $S \equiv Z^e \pmod{N}$, kde $1 \leq S \leq N-1$.
(5) Odesílatel odešle šifru S.
(6) Příjemce dešifruje, tedy nalezne W, $1 \leq W \leq N-1$, $W \equiv S^d \pmod{N}$. Potom $W = Z$.

Důkaz. Ukažme si, že algoritmus skutečně funguje, tedy že popsaným procesem dostaneme po dešifrování zašifrované zprávy skutečně původní zprávu.

a) Nejprve rozeberme případ, kdy je zpráva Z nesoudělná s číslem N. Potom podle Eulerovy věty
$$S^d \equiv (Z^e)^d = Z^{ed} = Z^{k\varphi(N)+1} = \underbrace{Z^{k\varphi(N)}}_{\equiv 1} Z \equiv Z \pmod{N}.$$

b) N a Z jsou soudělná čísla. Potom je vzhledem k velikosti Z největším společným násobkem buď prvočíslo p, nebo q. Bez újmy na obecnosti předpokládejme, že největším společným násobkem je číslo p, tedy že $Z = ap$, kde $1 \leq a < q$. Potom dle Malé Fermatovy věty je
$$S^d = (ap)^{ed} = (ap)^{k\varphi(N)+1} = \big((ap)^k(p-1)\big)^{(q-1)}(ap) \equiv ap = Z \pmod{q}.$$
Triviálně ovšem
$$S^d = (ap)^{ed} \equiv ap = Z (\equiv 0) \pmod{p},$$
a protože kongruence $S^d \equiv Z$ platí podle dvou nesoudělných modulů, platí i podle jejich součinu, což je to, co chceme.

□

10.50. Poznámka. Dodejme, že tento algoritmus je hojně používán v praxi. Panuje obecný názor[6], že bezpečnost tohoto algoritmu je založena na tom, že problém faktorizace (rozklad na součin mocnin prvočísel) velkých přirozených čísel je těžký problém (pro velká čísla – řádově se stovkami cifer – to neumíme v rozumném čase). Nicméně nebylo dokázáno, že by prolomení RSA-algoritmu bylo ekvivalentní nalezení efektivního algoritmu na faktorizaci velkých čísel a nebylo ani dokázáno, že takový algoritmus neexistuje.

Velkou výhodou algoritmu je, že není třeba žádné domluvy (výměny tajné informace, klíče) před vlastním použitím algoritmu. To je zřejmě důvod popularity tohoto algoritmu.

10.51. Rabinův kryptosystém. Je prvním veřejným kryptosystémem, o kterém bylo dokázáno, že jeho prolomení je stejně obtížné jako faktorizace velkých čísel. Uvedeme si jej ve zjednodušené verzi:

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě podobně velká prvočísla $p, q \equiv 3 \pmod{4}$, vypočte $n = pq$.
- $V_A = n$, $S_A = (p, q)$
- zašifrování numerického *kódu* zprávy Z: $S = S_e(Z) \equiv Z^2 \pmod{n}$
- dešifrování šifry S: vypočtou se (čtyři) odmocniny z S modulo n a snadno se otestuje, která z nich byla původní zprávou.

  Výpočet druhé odmocniny z S modulo $n = pq$, kde $p \equiv q \equiv 3 \pmod{4}$:

[6]Říká se, že ve fyzice tato formulace znamená „ještě jeden můj známý si to také myslí“, nicméně my máme na mysli běžný význam tohoto sousloví.

- vypočti a, b tak, že $ap + bq = 1$
- vypočti $r = S^{(p+1)/4} \pmod p$ a $s = S^{(q+1)/4} \pmod q$
- polož $x = (aps + bqr) \pmod n$, $y = (aps - bqr) \pmod n$
- druhými odmocninami z S modulo n jsou $\pm x$, $\pm y$.

10.52. Algoritmus ElGamal.

- Odesílatel zvolí cyklickou grupu G spolu s generátorem g.
- Odesílatel zvolí **tajný klíč** x, spočítá $h = g^x$ a zveřejní **veřejný klíč** (G, g, h).
- Šifrování zprávy Z: Bob zvolí náhodné y a vypočte $S_1 = g^y$ a $S_2 = Z \cdot h^y$ a pošle (S_1, S_2).
- Dešifrování zprávy: $M = C_2/C_1^x$

10.53. Příklady.

10.53.1. *Martin a Honza chtějí komunikovat šifrou ElGamal navrženou podle protokolu pánu Diffieho a Hellmana. Domluvili se na cyklické grupě $\mathbb{Z}_{41}^+$ a Martin si náhodně zvolil generátor grupy 11 a číslo 10 a zveřejnil trojici $(\mathbb{Z}_{41}, 11, A)$, kde $A \equiv 11^{10} \pmod{41}$. Honza mu pošle veřejně dvojici $(22, 6)$. Jakou zprávu Honza poslal?*

Řešení. $A = 9$ (k dekódování není třeba). Zprávu Z dostaneme jako $Z \equiv (6/22^{10}) \pmod{41}$. Spočtěme nejprve $22^{10} \equiv 22^2 \cdot (22^2)^2 \cdot ((22^2)^2) \equiv (-8) \cdot (-8)^2 \cdot (-8)^2 \equiv (-8) \cdot 23 \cdot 23 \equiv -9 \pmod{41}$, $(-9)^{-1} = 9$, $Z = 9 \cdot 6 \equiv 13 \pmod{41}$. □

10.53.2. *Martin a Honza chtějí komunikovat šifrou ElGamal navrženou podle protokolu pánu Diffieho a Hellmana. Domluvili se na cyklické grupě $\mathbb{Z}_{37}^+$ a Martin si náhodně zvolil generátor grupy 5 a číslo 10 a zveřejnil trojici $(\mathbb{Z}_{37}, 5, A)$, kde $A \equiv 5^{10} \pmod{37}$. Honza mu pošle veřejně dvojici $(17, 21)$. Jakou zprávu Honza poslal?*

Řešení. Zprávu spočteme jako $Z \equiv 21/17^10 \pmod{37}$. Spočtěme nejprve $17^10 = 17^2 \cdot (17^2)^2 \cdot (17^2)^2 \equiv (-7) \cdot (-7)^2 \cdot (-7)^2 \equiv (-7) \cdot 12 \cdot 12 \equiv 28 \pmod{37}$, $28^{-1} \equiv 4 \pmod{37}$, tedy $Z \equiv 4 \cdot 21 \equiv 10 \pmod{37}$. □

KAPITOLA 11

Statistické metody

Je statistika částí matematiky?
– když ano, tak matematiky potřebuje hodně . . .

11.1

11.1. Pravděpodobnost nebo statistika? Statistika v širším slova smyslu je jakékoliv zpracování číselných dat o nějakém souboru objektů a jejich více či méně přehledná prezentace. V tomto smyslu hovoříme také o *popisné statistice*, když jsou zpracovávána a zpřehledňována data o všech objektech daného souboru (např. roční příjmy všech občanů zpracovávané z kompletních dat finančních úřadů), a *matematické statistice*, když matematickými metodami zkoumáme jen data menšího počtu objektů (např. zjišťujeme údaje o příjmech pomocí dat získaných u několika nahodile vybraných osob).

Podstatou *matematické statistiky* je pro prezentovaná data zjišťovat, jaké vlastnosti skutečně mají objekty, které jou daty popisovány, a zároveň, jak věrohodné odvozené výsledky jsou. 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. Jinak řečeno, výsledkem práce matematického statistika 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 se opírá o teorii pravděpodobnosti, o které jsme něco málo uváděli na samotném počátku naší cesty matematikou, ve čtvrté části první kapitoly. Zatímco teorie pravděpodobnosti se zabývá modely popisujícími chování abstraktních souborů (hovořili jsme o pravděpodobnosti jevů z jevového pole), statistika pracuje se skutečným náhodným výběrem z nějakého základního souboru a poskytuje podklady pro výběr teoretického pravděpodobnostního modelu, resp. kvalitativní informace o jeho parametrech. Uvidíme, že při zpracovávání statistických dat provádíme v podstatě úkony popisné statistiky, teorii pravděpodobnosti však potřebujeme pro vyslovení kvalitativních údajů o výsledcích.

Ne náhodou se právě k této části našich motivačních náznaků z první kapitoly vracíme až na samém konci našich přednášek. 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.

Příklad. Za soubor objektů vezměme všechny studenty této přednášky „Drsná matematika“, jako číselný údaj můžeme uvažovat

(1) „průměrný počet bodů“ dosažený při hodnocení tohoto předmětu v minulém semestru,

(2) „průměrnou známku“ dosaženou u zkoušky z tohoto a z jiných pevně vybraných předmětů,
(3) číslená data vypovídající o historii dřívějšího studia,
(4) počet pracovních hodin týdně odpracovaných studentem či studentkou mimo fakultu

a mnoho dalších údajů. 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 studetnů. 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. V uvedených příkladech se jim říká *medián*, *kvartil*, *decil* apod. Takové statistiky budou jistě zajímavé pro samotné studenty a je docela jednoduché je zavést a spočíst.

Z obecné zkušenosti nebo jako výsledek teoretických úvah mimo samotnou matematiku víme, že rozumné hodnocení by na 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 a 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 měřit polohy 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 něco v nepořádku.

Daleko zajímavější vývody ovšem můžeme činit, 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 vývod, že je přednáška prostě špatná.

Zamysleme se nad závěry našich úvodních úvah:

- V matematice pracujeme s abstraktním matematickým popisem pravděpodobnosti.
- Vývody pro konktrétní soubory dat, pro které je zvolený model relevantní, dává matematická statistika.
- To, zda je takový popis adekvátní pro konkrétní výběr dat, je také možné podpořit nebo zavrhnout pomocí metod matematické statistiky.

Než se pustíme do elementárního náznaku statistických postupů, budeme se věnovat chvíli matematické pravděpodobnosti.

1. Pravděpodobnost

11.2

11.2. Jevová pole. Před dalším čtením lze čtenářům vřele doporučit zopakování obsahu čtvrté části první kapitoly (tj. odstavce **??**–**??**). Tehdy jsme pracovali převážně s tzv. klasickou konečnou pravděpodobností zavedli jsme základy formalismu, který nyní zobrecníme. Hlavní změnou bude, že náš základní prostor Ω už nebude obecně obsahovat jen konečně mnoho prvků.

Budeme pracovat s neprázdnou pevně zvolenou množinou Ω všech možných výsledků, kterou nazýváme *základní prostor*. Prvky $\omega \in \Omega$ představují jednotlivé *možné výsledky*. Systém podmnožin $\mathcal{A}$ základního prostoru se nazývá *jevové pole* a jeho prvky se nazývají *jevy*, jestliže

- $\Omega \in \mathcal{A}$, 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. $\cup_{i\in I} A_i \in \mathcal{A}$.

V souladu s obvyklými verbálními popisy skutečných problémů používáme také následující 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
$$A \setminus (\Omega \setminus B) = A \cap B.$$

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 $\mathcal{A}$).

Jako příklad, proč nám i u zdánlivě klasických problémů nestačí konečná klasická pravděpodobnost, můžeme promyslet třeba experiment, ve kterém opakovaně házíme mincí dokud nepadne líc. Ptáme se, jaká je pravděpodobnost, že budeme házet právě 3–krát nebo právě 35–krát nebo nejvýš 10–krát apod. Elementární jevy jsou tedy tvaru $\omega_k \in \mathbb{N}_{\geq 1} \cup \{\infty\}$, které slovně vyjadřujeme „líc padne poprvé právě v k–tém hodu“.

Zjevně můžeme takový problém dobře zvládat, když vyjdeme z pravděpodobnosti 0,5 pro obě možné strany mince při jednom hodu, nemůžeme ale v abstraktním modelu vyloučit možnost neustálých rubů a už vůbec ne omezit celkový počet hodů nějakým povným přirozeným číslem N. Na druhé straně, očekávaná pravděpodobnost, že padne právě $(k-1)$–krát rub v $n \geq k$ pokusech 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 dvě hodnoty do $n-k$ pozic) a ve jmenovateli je počet všech možností výsledků. Podle očekávání tato pravděpodobnost nezávisí na zvoleném n a platí $\sum_{k=1}^{\infty} 2^{-k} = 1$ a tedy musí být pravděpodobnost neustálého opakování rubu nulová.

11.3

11.3. Pravděpodobnostní prostor. Souvislosti s popisem skutečných jevů a jejich formálním pravděpodobnostním popisem vedou k definicím:

- celý základní prostor Ω se nazývá *jistý jev*, prázdná podmnožina $\emptyset \in \mathcal{A}$ se nazývá *nemožný jev*,
- jednoprvkové podmnožiny $\{\omega\} \in \Omega$ 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 $A \subset B$,
- je-li $A \in \mathcal{A}$, pak se jev $B = \Omega \setminus A$ nazývá *opačný jev k jevu* A, píšeme $B = A^c$.

Konečně umíme popsat, co je v našem matematickém modelu pravděpodobnost:

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

- je nezáporná, tj. $P(A) \geq 0$ pro všechny jevy A,
- je 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 nazýváme *pravděpodobností* na jevovém poli $(\Omega, \mathcal{A})$.

Příklad takto definované pravděpodobnosti na nekonečné množině elementárních jevů jsme viděli na konci předchozího odstavce.

Jako přímé důsledky naší definice vidíme, že pro všechny jevy platí

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

Zdůrazněme také, že additivnost platí pro jakýkoliv spočetný počet neslučitelných jevů $A_i \subset \Omega$, $i \in I$, tj.

$$P(\cup_{i\in I} A_i) = \sum_{i\in I} P(A_i), \text{ kdykoliv je } A_i \cap A_j = \emptyset,\ i \neq j,\ i, j \in I.$$

Připomeňme si dále klasickou konečnou pravděpodobnost: Nechť Ω je konečný základní prostor a nechť jevové pole $\mathcal{A}$ je právě systém všech podmnožin v Ω. *Klasická pravděpodobnost* je pravděpodobnostní prostor $(\Omega, \mathcal{A}, P)$ s pravděpodobnostní funkcí $P : \mathcal{A} \to \mathbb{R}$,

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

Zjevně takto zadaná funkce skutečně definuje pravděpodobnost.

11.4

11.4. Peterburgský paradox. (Bernoulli, 1738) Typický příklad klasické pravděpodobnosti jsou jevy související s házením mincí. Představme si následující pravidla kasina:

Návštěvník zaplatí vklad C a poté hází mincí. Je-li T počet hodů potřebných k první hlavě, pak obdrží výhru 2^T. Jaká je „fér hodnota“ pro vklad C?

Pravděpodobnostní model pro tuto hru jsme zavedli na konci 11.2. Pravděpodobnost, že padne hlava je u férové mince $1/2$, je proto $P(T = k) = 2^{-k}$. Sečteme-li všechny pravděpodobnosti výsledků vynásobené výhrami 2^k, dostaneme $\sum_1^\infty 1 = \infty$. Zdá se proto, že se vyplatí vložit i velký vklad...

Ve skutečnosti simulací hry zjistíme, že nezávisle na počtu pokusů se prakticky všechny výhry budou pohybovat v rozmezí 3 až 6. Důvodem je, že vysoké výhry jsou velice nepravděpodobné a proto je při reálných úvahách nelze brát vážně. Zkuste si promyslet zdůvodnění podrobněji.

11.5

11.5. Podmíněná pravděpodobnost. Obvyklé je klást dotazy s dodatečnou podmínkou. Např. „jaká je pravděpodobnost, že při hodu dvěmi kostkami padly dvě pětky, je-li součet hodnot deset?“. Připomeneme, že formalizovat takové úvahy umíme 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 požadavku, že jevy A a H nastanou zároveň, za předpokladu, že A nastal s pravděpodobností $P(A \cap H)/P(A)$.

Je také vidět přímo z definice, hypotéza H a jev A jsou nezávislé tehdy a jen tehdy, je-li $P(A) = P(A|H)$.

Přepsáním formule pro podmíněnou pravděpodobnost dostáváme

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

Věta (Bayesovy věty)**.** *Pro pravděpodobnost jevů A a B platí*

$$P(A|B) = \frac{P(A)P(B|A)}{P(B)} \tag{1}$$

$$P(A|B) = \frac{P(A)P(B|A)}{P(A)P(B|A) + P(A')P(B|A')}. \tag{2}$$

Důkaz. První tvrzení je přepsáním předchozí formule, druhé z prvého plyne doszením $P(B) = P(A)P(B|A) + P(A')P(B|A')$. □

11.6. Poznámka. Dodejme ještě, že vztahům z předchozí věty se někdy říká Bayesovy vzorce a že druhý z nich bývá formulován i v lehce obenějším tvaru: nechť je jevový prostor sjednocením disjunktních jevů $A_1,\dots A_n$. Pak pro libovolné $i \in \{1, \dots, n\}$ platí

$$P(A_i|B) = \frac{P(B|A_i)P(A_i)}{\sum_{i=1}^{n} P(B|A_i)P(A_i)}. \tag{3}$$

11.7. Důsledek. *Pro jevy A, B, C platí*

$$P(A|B \cap C) = \frac{P(A|B)P(C|A \cap B)}{P(C|B)} = \frac{P(A)P(B|A)P(C|A \cap B)}{P(B)P(C|B)} \tag{4}$$

Důkaz.

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

Poslední výraz pak dostaneme dalším dosazením (1) za $P(A|B)$. □

Uveďme si ještě jedno lemma, které vyplývá z definice podmíněné pravděpodobnosti:

11.8. Lemma. *Nechť jev B je disjunktním sjednocením jevů B_1, B_2,…,B_n. Potom*

$$P(A|B) = \sum_{i=1}^{n} P(A|B_i)P(B_i|B) \tag{5}$$

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

$$\begin{aligned} P(A|B_1 \cup \cdots \cup B_n) &= \frac{P\left(A \cap (B_1 \cup \cdots \cup B_n)\right)}{P(B_1 \cup \cdots \cup B_n)} = \\ &= \frac{P\left((A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)\right)}{P(B)} = \\ &= \frac{\sum_{i=1}^{n} P(A \cap B_i)}{P(B_i)} \cdot \frac{P(B_i)}{P(B)} = \\ &= \sum_{i=1}^{n} P(A|B_i) P(B_i|B). \end{aligned}$$

□

11.6

11.9. Příklad – preventivní screening. Předpokládejme, že krevní test na HIV pozitivní osoby má 99% správnost v případě osoby skutečně HIV pozitivní. Zároveň předpokládejme, že u HIV negativní osoby dopadne test pozitivně v 0.2% případů.

Náhodně z populace vybereme osobu a otestujeme pozitivně. S jakou pravděpodobností je skutečně HIV pozitvní, jestliže četnost výskytu HIV v populaci je p promile (tj. p osob z tisíce je skutečně HIV pozitivní).

Označme A jev, že je daná osoba HIV pozitivní, a B jev, že daná osoba má pozitivní test. Dle druhé Bayesovy věty je hledaná pravděpodobnost

$$P(A|B) = \frac{p/1000 \cdot 99/100}{p/1000 \cdot 99/100 + (1000 - p)/1000 \cdot 2/1000}.$$

Jestliže zvolíme za p nějaké konkrétní četnosti, dostaneme příslušné očekávatelné spolehlivosti testu. V následující tabulce je spočten výsledek pro 100 promile (tj. jeden z deseti je nemocný), pro 10 promile (tj. každý stý člověk je infikován), 1 promile a 1/10 promile (tj. pouze jeden z deseti tisíc je infikován – to asi může odpovídat realitě).

p	100	10	1	0.1
$P(A\|B)$	0.982	0.8333	0.3313	0.0471

Výsledek asi neodpovídá naší intuici a může se zdát šokující ve vztahu k použití takovýchto testů. V případě 0,1 promile nakažených lidí totiž při pozitivním testu nemáme ani 5% pravděpodobnost, že je dotčená osoba skutečně infikovaná.

Všimněme si také, že i 100% účinný test při testu pozitvní osoby v podstatě neovlivní výsledné pravděpodobnosti.

Evidentně prostý výběr náhodné osoby a použití jediného testu, byť velmi citlivého, specifického a účinného, nejsou vhodné ani na otestování skutečného stavu populace, ani na preventivní vyšetření jednotlivců, pokud nemáme další podpůrné informace a lepší nástroje.

Právě matematická statistika dává nástroje na kvalifikovanější postupy v medicínské i průmyslové diagnostice, ekonomických modelech, vyhodnocování experimentálních dat atd. Opírají se většinou o několik parametrů, které k danému jevu přiřazujeme a při praktickém vyhodnocování je zjišťujeme a zpracováváme. Jsou obdobou obyčejných funkcí, potřebujeme je ale vztáhnout k danému prvděpodobnostnímu prostoru.

11.10. Příklady.

11.10.1. *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 můžememe 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 $P(A_1|A) = \frac{\frac{4}{16}}{\frac{9}{16}} = \frac{4}{9}$, $P(A_2|A) = \frac{3}{9} = \frac{1}{3}$, $P(A_3|A) = \frac{2}{9}$. Použitím vztahu (5) pak dostáváme

$$\begin{aligned} P(B|A) &= P(B|A_1)P(A_1|A) + P(B|A_2)P(A_2|A) + P(B|A_3)P(A_3|A) = \\ &= P(B|A_1) \cdot \frac{P(A_1)}{P(A)} + P(B|A_2) \cdot \frac{P(A_2)}{P(A)} + P(B|A_3) \cdot \frac{P(A_3)}{P(P(A)} = \\ &= 1 \cdot \frac{4}{9} + \frac{2}{3} \cdot \frac{3}{9} + \frac{1}{3}\frac{2}{9} = \frac{20}{27}. \end{aligned}$$

□

11.10.2. *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 disjuktním 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 $P(B|A_1) = \frac{7}{12}$ (opět můžeme použít klasickou pravděpodobnost, protože v každém sáčku je stejný počet koulí a tedy má každá stejnou pravděpodobnost, že bude vytažena). Obdobně $P(B|A_2) = \frac{8}{12}$ a $P(B|A_3) = \frac{9}{12}$. Pak podle (5) je hledaná pravděpodobnost

$$P(B|A) = P(B|A_2)P(A_2|A) + P(B|A_3)P(A_3|A) + P(B|A_4)P(A_4|A) = \\ = \frac{7}{12}\cdot\frac{1}{6} + \frac{8}{12}\cdot\frac{1}{3} + \frac{9}{12}\cdot\frac{1}{2} = \frac{25}{36}.$$

□

11.10.3. *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 druhý, resp. třetí, resp. čtvrtý sáček. Pravděpodobnost vytažení bílé koule z prvního sáčku je $P(A_1) = \frac{1}{4}\cdot\frac{1}{2}$ (jev A_2 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 3kouli a znovu budeme chtít použít vztah (5). Zbývá ještě dopočítat $P(B|A_i)$, $i = 1,\dots 4$. 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

$$P(B|A_1) = P(B_2|A_1) + P(B_3|A_1) + P(B_4|A_1) = \frac{1}{3}\frac{3}{4} + \frac{1}{3}\frac{1}{3} + \frac{1}{3}\frac{1}{4} = \frac{4}{9}$$

Obdobně

$$\begin{aligned} P(B|A_2) &= \tfrac{1}{3}\tfrac{1}{2} + \tfrac{1}{3}\tfrac{1}{3} + \tfrac{1}{3}\tfrac{1}{4} &&= \frac{13}{36}, \\ P(B|A_3) &= \tfrac{1}{3}\tfrac{1}{2} + \tfrac{1}{3}\tfrac{3}{4} + \tfrac{1}{3}\tfrac{1}{4} &&= \frac{1}{2}, \\ P(B|A_4) &= \tfrac{1}{3}\tfrac{1}{2} + \tfrac{1}{3}\tfrac{3}{4} + \tfrac{1}{3}\tfrac{1}{3} &&= \frac{19}{36}. \end{aligned}$$

Celkem pak

$$P(B|A) = P(B|A_1)P(A_1|A) + P(B|A_2)P(A_2|A) + P(B|A_3)P(A_3|A) + P(B|A_4)P(A_4|A) = \\ = \frac{4}{9}\frac{3}{11} + \frac{13}{36}\frac{9}{22} + \frac{1}{2}\frac{2}{11} + \frac{19}{36}\frac{3}{22} = \\ = \frac{19}{44}$$

□

11.7

11.11. Náhodné veličiny. Vraťme se k jednoduchému a názornému příkladu statistik kolem výsledků studentů[1] 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 (celá čísla od 0 do 20). Zároveň ale není patrně vhodné představovat si výsledky jednotlivých studentů jako analogii nezávislého házení pravidelnou kostkou (jednak neexituje pravidelný 21–stěn, ale hlavně by to byla skutečně divně vedená přednáška). Na základním (konečném) prostoru Ω všech studentů máme ve skutečnosti definovánu funkci bodového ohodnocení $X : \Omega \to \mathbb{R}$, která má tu vlastnost, že můžeme modelovat pravděpodobnosti, že její hodnota při náhodném výběru studenta padne do předem zvoleného intervalu. Např. můžeme chtít modelovat pravděpodobnost, že student uspěl s hodnocením A nebo B.

Je to typický příklad *náhodné veličiny* a každá taková náhodná veličina je spojena s vhodnou množinou jevů. V našem příkladě bychom tedy měli umět říci pravděpodobnost pro kterýkoliv interval $(a, b) \subset [0, 20]$ s reálnými čísly a, b a uzavřenými i otevřenými konci intervalu. 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.

I obecné pro takové číselné veličiny X na základním prostoru požadujeme, abychom mohli pracovat s pravděpodobnostmi příslušnosti hodnoty X do předem zadaného intervalu. Musíme proto uvést do souladu požadavky na pravděpodobnostní prostor s vlastnostmi takových funkcí:

Na prostoru $\mathbb{R}^k$ uvažujme nejmenší jevové pole $\mathcal{B}$ obsahující všechny k–rozměrné intervaly. Množinám v $\mathcal{B}$ říkáme *Borelovské množiny* na $\mathbb{R}^k$. Specielně pro $k = 1$ půjde o všechny množiny, které ze všech intervalů obdržíme konečnými průniky a nejvýše spočetnými sjednoceními. [2]

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 Borelovských množinách $B \subset \mathbb{R}$ se nazývá *rozdělení (pravděpodobnosti) náhodné veličiny* X

Všimněme si, že pro klasickou konečnou pravděpodobnost je náhodnou veličinou každá reálná funkce $X : \Omega \to \mathbb{R}$. Skutečně, na konečné množině Ω nabývá X jen konečně mnoho hodnot a každá podmnožina v Ω je jevovým prostorem.

Rozdělení pravděpodobnosti náhodných veličin zadáváme nejčastěji pomocí pravidla, jak roste pravděpodobnost s přírůstkem intervalu B:

11.8

11.12. Distribuční funkce. Definice náhodné veličiny zajišťuje, že pro všechny $-\infty \le a \le b \le \infty$ existují pravděpodobnost $P(a < X < b)$, kde používáme stručné

[1] Myslíme samozřejmě na „studenty a studentky“, pro zestručnění textu ale používám podobně jako v legislativních textech bezpohlavní označní „student“

[2] V této souvislosti se často také hovoří o tzv. *σ–algebře Borelovsky měřitelných množin na $\mathbb{R}^k$* a následující definici lze formulovat tak, že náhodné veličiny jsou Borelovsky měřitelné funkce.

značení pro jev $A = (\omega \in \Omega;\ a < X(\omega) < b)$). Stejně tak existují pravděpodobnosti pro hodnoty v intervalech uzavřených nebo z jedné strany uzavřených.

Definice. *Distribuční funkcí* náhodné veličiny X je funkce $F : \mathbb{R} \to \mathbb{R}$ definovaná pro všechny $x \in \mathbb{R}$ vztahem[3]

$$F(x) = P(X < x).$$

11.9

11.13. 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.

Předpokládejme nejprve, že náhodná veličina X na pravděpodobnostním prostoru $(\Omega, \mathcal{A}, P)$ nabývá jen konečně mnoha hodnot $x_1, x_2, \ldots, x_n \in \mathbb{R}$. Pak existuje tzv. *pravděpodobnostní funkce* $f(x)$ taková, že

$$f(x) = \begin{cases} P(X = x_i) & x = x_i \\ 0 & \text{jinak.} \end{cases}$$

Evidentně $\sum_{i=1}^{n} f(x_i) = 1$ a pro rozdělení pravděpodobnosti platí

$$P(X^{-1}B) = \sum_{x_i \in B} f(x_i)$$

a tedy zejména je distribuční funkce tvaru

$$F_X(t) = \sum_{x_i < t} f(x_i).$$

Říkáme, že X je *diskrétní náhodná veličina*.

Každá náhodná veličina definovaná pro klasickou pravděpodobnost je diskrétní.

Obdobně lze definici pravděpodobnostní funkce rozšířit na veličiny se spočetně mnoha hodnotami. Pracujeme pak s nekonečnými řadami a musíme hlídat pečlivě jejich konvergenci.

I když hodnoty náhodné veličiny X nejsou diskrétní, můžeme postupovat podobně s užitím ideí diferenciálního a integrálního počtu. Intuitivně lze při infinitesimální změně hodnoty x o dx uvažovat takto: *hustotu* $f(x)$ *pravděpodobnosti* pro X si představíme jako

$$P(x \le X < x + dx) = f(x)dx.$$

To znamená, že chceme pro $-\infty \le a \le b \le \infty$

$$(*) \qquad P(a \le X < b) = \int_a^b f(x)dx.$$

Definice. Náhodná veličina X, pro kterou existuje její *hustota pravděpodobnosti* splňující $(*)$, se nazývá *spojitá náhodná veličina*.

11.10

11.14. Věta. *Nechť X je náhodná veličina, $F(x)$ je její distribuční funkce.*

(1) *F je zleva spojitá*[4], $\lim_{x\to-\infty} = 0$ *a* $\lim_{x\to\infty} = 1$.

(2) *Vždy platí* $P(a \le X < b) = F(b) - F(a)$.

[3] V literatuře se stejně často potkáváme také s definicí s neostrou nerovností, tj. pravděpodobnost $P(X = x)$ je ještě započtena také.

[4] Pokud definujeme distribuční funkci s neostrou nerovností, bude naopak zprava spojitá, ostatní tvrzení této věty zůstavají v platnosti beze změny.

(3) *Je-li X diskrétní s hodnotami $x_1, \dots, x_n$, pak je $F(x)$ po částech konstantní, $F(x) = \sum_{x_i<x} P(X = x_i)$ a $F(x) = 1$ kdykoliv $x > x_n$.*
(4) *Je-li X spojitá, pak je $F(x)$ diferencovatelná a její derivace se rovná hustotě pravděpodobnosti X, tj. platí $F'(x) = f(x)$.*

Důkaz. Dodám později... □

11.11 **11.15. Důsledek.** *Distribuční funkce náhodné veličiny má vždy nejvýše spočetně mnoho bodů nespojitosti.*

Důkaz. Dodám později... □

Dodat poznámku o distribuci u veličin, které mají spojité i diskrétní chování současně (Riemann–Stieltjesův integrál a něco málo o míře).

11.12 **11.16. Příklady 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 nejprve několik jednoduchých diskrétních rozdělení.

Degenerované rozdělení $\mathrm{Dg}(\mu)$**.** Toto rozdělení odpovídá konstantní hodnotě $X = \mu$. Distribuční funkce F_X a pravděpodobnostní funkce f_X jsou tedy rovny

$$F_X(t) = \begin{cases} 0 & t \le \mu \\ 1 & t > \mu \end{cases} \qquad f_X(t) = \begin{cases} 1 & t = \mu \\ 0 & \text{jinak} \end{cases}.$$

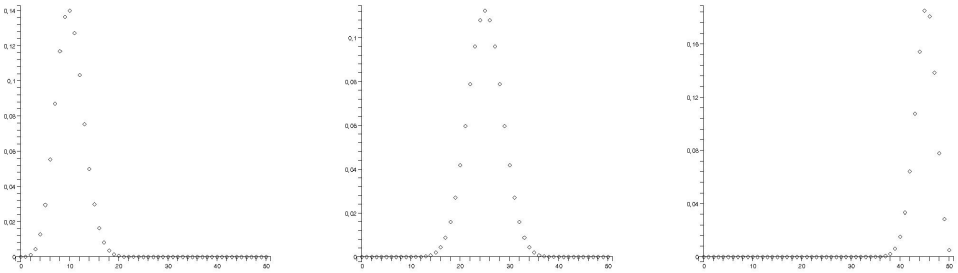
Alternativní rozdělení $\mathrm{A}(p)$ popisuje pokus s pouze dvěma možnými výsledky, kterým budeme říkat zdar a nezdar. Náhodné veličině X pro určitost přiřadíme hodnotu 0 pro nezdar a 1 pro zdar. Pokud má zdar pravděpodobnost p, pak nezdar musí mít pravděpodobnost $1-p$. Jsou tedy distribuční a pravděpodobnostní funkce tvaru:

$$F_X(t) = \begin{cases} 0 & t \le 0 \\ 1-p & 0 < t \le 1 \\ 1 & t > 1 \end{cases} \qquad f_X(t) = \begin{cases} p & t = 1 \\ 1-p & t = 0 \\ 0 & \text{jinak} \end{cases}.$$

Binomické rozdělení $\mathrm{Bi}(n, p)$ odpovídá 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). Je tedy

$$f_X(t) = \begin{cases} \binom{n}{t} p^t (1-p)^{1-t} & t \in \{0, 1, \dots, n\} \\ 0 & \text{jinak} \end{cases}.$$

Na obrázku jsou pravděpodobnostní funkce pro $\mathrm{Bi}(50, 0.2)$, $\mathrm{Bi}(50, 0.5)$ a $\mathrm{Bi}(50, 0.9)$. Rozdělení pravděpodobnosti dobře odpovídá intuici, že nejvíce výsledků bude blízko u hodnoty np:



S binomickým rozdělením se potkáváme velice často v praktických úlohách. Jednou z nich je popis náhodné veličiny, která popisuje počet X předmětů v jedné zvolené příhrádek z n možných, do nichž jsme náhodně rozdělili r předmětů. Umístění kteréhokoliv předmětu do pevně zvolené přihrádky má pravděpodobnost $1/n$ (každá z nich je stejně pravděpodobná). Zjevně tedy bude pro jakýkoliv počet $k = 0, \dots, r$

$$P(X = k) = \binom{r}{k} \left(\frac{1}{n}\right)^k \left(1 - \frac{1}{n}\right)^{r-k} = \binom{r}{k} \frac{(n-1)^{r-k}}{n^r},$$

jde proto o rozložení X typu $\mathrm{Bi}(r, 1/n)$.

Jestliže nám 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 λ, můžeme dobře vyjádřit chování našeho rozdělení veličin X_n při limitním přechodu $n \to \infty$. Takovéto chování popisuje např. fyzikální soustavy s velikým počtem molekul plynu. Standardní úpravy (s řádným připomenutím analýzy funkcí jedné proměnné!) vedou při $\lim_{n\to\infty} r_n/n = \lambda$ k výsledku:

$$\begin{aligned}
\lim_{n\to\infty} P(X_n = k) &= \lim_{n\to\infty} \binom{r_n}{k} \frac{(n-1)^{r_n-k}}{n^{r_n}} \\
&= \lim_{n\to\infty} \frac{r_n(r_n-1)\dots(r_n-k+1)}{(n-1)^k} \frac{1}{k!} \left(1 - \frac{1}{n}\right)^{r_n} \\
&= \frac{\lambda^k}{k!} \lim_{n\to\infty} \left(1 + \frac{-\frac{r_n}{n}}{r_n}\right)^{r_n} \\
&= \frac{\lambda^k}{k!}\, \mathrm{e}^{-\lambda}
\end{aligned}$$

protože obecně funkce $(1 + x/n)^n$ konvergují stejnoměrně k funkci e^x na každém omezeném intervalu v $\mathbb{R}$.

Poissonovo rozdělení $\mathrm{Po}(\lambda)$ popisuje náhodné veličiny s pravděpodobnostní funkcí

$$f_X(t) = \begin{cases} \frac{\lambda^k}{k!}\, \mathrm{e}^{-\lambda} & t \in \mathbb{N} \\ 0 & \text{jinak.} \end{cases}$$

Jak jsme odvodili výše, toto diskrétní rozdělení (rozložené do nekonečně mnoha bodů) dobře aproximuje binomická rozložení $\mathrm{Bi}(n, \lambda/n)$ pro konstantní $\lambda > 0$ a veliká n.

Přímým výpočtem snadno ověříme, že

$$\sum_{k=0}^{\infty} f_X(k) = \sum_k \frac{\lambda^k}{k!}\, \mathrm{e}^{-\lambda} = \mathrm{e}^{-\lambda} \sum_k \frac{\lambda^k}{k!} = \mathrm{e}^{-\lambda+\lambda} = 1.$$

Takové chování lze očekávat při sledování výskytu jevů v prostoru s konstatní 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 λ, pak při rozdělení celé oblasti na n stejných částí bude výskyt k jevů v jedné výbrané 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.

Další případ výskytu Poissonova rozdělení jsou události, které se vyskytují náhodně v čase a přitom pravděpodobnost výskytu v následujícím časovém intervalu o jednotkové délce nezávisí na předchozí historii a je rovna stále stejné hodnotě λ. Označme si náhodnou veličinu X_t vyčíslující počet výskytu sledovaného jevu v intervalu $[0, t)$.

Přesněji řečeno, požadujeme aby

- pravděpodobnost události v každém časovém úseku o délce h byla rovna $h\lambda + o(h)$
- pravděpodobnost více než jedné události v časovém úseku délky h je $o(h)$
- 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-li si funkce $p_k(t) = P(X_t = k)$, $k \in \mathbb{N}$, a položíme přirozené okrajové podmínky $p_k(0) = 0$ pro $k > 0$ a $p_0(0) = 1$, pak limitními přechody s využitím předchozích podmínek (dodat podrobnosti!!!!!!!!!!!!) obdržíme pro derivace funkcí p_k

$$p_0'(t) = -\lambda p_0(t),\ t > 0,\ p_0(0) = 1$$
$$p_k'(t) = -\lambda p_k(t) + \lambda p_{k-1}(t),\ t > 0,\ k > 0,\ p_k(0) = 0.$$

To je nekonečný (!) systém obyčejných diferenciálních rovnic s počáteční podmínkou, z nichž první má jediné řešení $p_0(t) = \mathrm{e}^{-\lambda t}$. Pak okamžitě můžeme dosadit a vyřešit druhou a 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

$$p_k(t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t},\ t > 0,\ k \in \mathbb{N}.$$

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.

11.13

11.17. Příklady spojitých rozdělení. Nejjednoduším příkladem spojitého rozdělení je tzv. **rovnoměrné rozdělení**. Na něm lze dobře ilustrovat, že při jednoduše formulovaném požadavku na chování rozdělení nám nezbude moc prostoru pro jeho definici. Nyní chceme, aby pravděpodobnost každé hodnoty v předem daném intervalu $(a, b) \subset \mathbb{R}$ byla stejná, tj. hustota f_X našeho rozdělení náhodné veličiny X má být konstantní. Pak ovšem jsou pro libovolná reálná čísla $-\infty < a < b < \infty$ jen jediné možné hodnoty

$$f_X(t) = \begin{cases} 0 & t \le a \\ \frac{1}{b-a} & t \in (a, b) \\ 0 & t \ge b, \end{cases} \qquad F_X(t) = \begin{cases} 0 & t \le a \\ \frac{t-a}{b-a} & t \in (a, b) \\ 1 & t \ge b. \end{cases}$$

Exponenciální rozdělení $\mathrm{ex}(\lambda)$ je dalším rozdělením, které je snadno určeno požadovanými vlastnostmi náhodné veličiny. Předpokládejme, že sledujeme výskyt náhodného jevu tak, že 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

$$\lim_{s \to 0_+} \frac{\ln P(t+s) - \ln P(t)}{s} = P'(0).$$

Označme si spočtenou derivaci zprava v nule jako $-\lambda \in \mathbb{R}$. Pak tedy pro $P(t)$ platí $\ln P(t) = -\lambda t + C$ a počáteční podmínka dává jediné řešení

$$P(t) = e^{-\lambda t}.$$

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

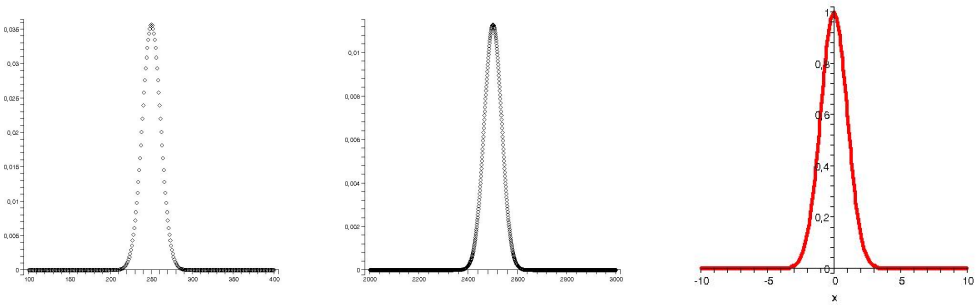
$$F_X(t) = 1 - P(t) = \begin{cases} 1 - e^{-\lambda t} & t > 0 \\ 0 & t \leq 0. \end{cases}$$

Je vidět, že skutečně jde rostoucí funkci s hodnotami mezi nulou a jedničkou a správnými limitami v $\pm\infty$.

Hustotu tohoto rozdělení dostaneme derivováním distribuční funkce, tj.

$$f_X = \begin{cases} \lambda e^{-\lambda t} & t > 0 \\ 0 & t \leq 0. \end{cases}$$

Normální rozdělení je ze všech nejdůležitější. Jestliže v binomiálním rozdělení zachováme konstatní 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 slívat do křivky, pro hodnoty $\mathrm{Bi}(500, 0.5)$ a $\mathrm{Bi}(5000, 0.5)$ je výsledek vidět na obrázku níže, rozdělení $\mathrm{Bi}(50, 0.5)$ jsme viděli dříve. Třetí křivka na obrázku je grafem funkce $f(x) = \mathrm{e}^{-x^2/2}$.



Podbízí se proto hledat vhodné spojité rozdělení, které by mělo hustotu danou nějakou obdobnou funkcí. Protože je $\mathrm{e}^{-x^2/2}$ vždy kladná funkce, potřebovali bychom spočíst $\int_a^b \mathrm{e}^{-x^2/2}\,dx$ což není pomocí elementárních funkcí možné. Je však možné (i když ne úplně snadné) ověřit, že příslušný nevlastní integrál konverguje k hodnotě

$$\int_{-\infty}^{\infty} \mathrm{e}^{-x^2/2}\,dx = \sqrt{2\pi}.$$

Odtud vyplývá, že možná hustota rozdělení náhodného rozdělení může být

$$f_X(x) = \frac{1}{\sqrt{2\pi}} e^x.$$

Rozdělení s touto hustotou se nazývá *normální rozdělení* $\mathrm{N}(0,1)$. Příslušnou distribuční funkci

$$F_X(x) = \int_{-\infty}^{x} \mathrm{e}^{-x^2/2}\, dx$$

nelze vyjádřit pomocí elementárních funkcí, přesto se s ní numericky běžně počítá (pomocí tabulek nebo softwarových aplikací).

Hustotě f_X se také často říká *Gaussova křivka*.

Abychom uměli pořádněji sformulovat asymptotickou blízkost normáního a binomického rozdělení pro $n \to \infty$, musíme si vytvořit další nástroje pro práci s náhodnými veličinami. Budeme k tomu používat funkce dvojím různým způsobem.

11.18. Příklady.

11.18.1. *Určete konstantu a tak aby funkce*

$$f(x) = \begin{cases} 0 & \text{pro} \quad x \le 1 \\ a\ln(x) & \text{pro} \quad 1 < x < 2 \\ 0 & \text{pro} \quad 2 \le x \end{cases}$$

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 $a = \frac{1}{2\ln(2)-1}$. □

11.18.2. *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 část a.

- 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:

$$f(x) = \begin{cases} 0 & \text{pro } x \le 0 \\ \frac{8(\frac{\sqrt{3}}{2}a-y)}{3a^2} & \text{pro } y \in \langle 0, \frac{\sqrt{3}}{2}a\rangle \\ 0 & \text{pro } y \ge \frac{\sqrt{3}}{2}a \end{cases}$$

□

11.18.3. *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:

$$f(x) = \begin{cases} 0 & \text{pro} \quad x \le 0 \\ \sqrt[3]{\frac{1}{36\pi r^3}}\, x^{-\frac{2}{3}} & \text{pro} \quad 0 < x < \frac{4}{3}\pi r^3 \\ 0 & \text{pro} \quad x \ge \frac{4}{3}\pi r^3 \end{cases}$$

□

11.18.4. *Stanovte hodnotu parametru $a \in \mathbb{R}$ tak, aby funkce*

$$f(x) = \begin{cases} 0 & \textit{pro} \quad x \le 0 \\ ax^2 & \textit{pro} \quad 0 < x < 3 \\ 0 & \textit{pro} \quad x \ge 3 \end{cases}$$

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.

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 $13, 5$. □

11.18.5. 2. *Stanovte hodnotu parametru $a \in \mathbb{R}$ tak, aby funkce*

$$f(x) = \begin{cases} 0 & pro \quad x \leq 0 \\ ax & pro \quad 0 < x < 3 \\ 0 & pro \quad x \geq 3 \end{cases}$$

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 $4, 5$. □

11.18.6. *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 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

$$F(d) = P[S \leq d] = P[X(l - X) \leq d]$$

Hledáme tedy ty hodnoty x, pro které je $x(l - x) \leq d$. Řešíme kvadr. nerovnici, kořeny odpovídající kvadratické rovnice jsou $\frac{l-\sqrt{l^2-4d}}{2}$ a $\frac{l+\sqrt{l^2-4c}}{2}$, hodnoty x uvnitř tohoto intervalu nerovnici nesplňují, hodnoty vně potom ano. Je tedy

$$P[X(l - X) \leq d] = P[X \in \langle 0, l\rangle \setminus (\frac{l - \sqrt{l^2 - 4d}}{2}, \frac{l + \sqrt{l^2 - 4d}}{2})] = \frac{l - \sqrt{l^2 - 4d}}{l} = \\ = 1 - \frac{\sqrt{l^2 - 4d}}{l}$$

Celkem

$$F(x) = \begin{cases} 0 & \text{pro} \quad x \leq 0 \\ 1 - \frac{\sqrt{l^2-4x}}{l} & \text{pro} \quad 0 \leq x \leq \frac{l^2}{4} \\ 1 & \text{pro} \quad x > \frac{l^2}{4} \end{cases}$$

Hustotu pravděpodobnosti pak dostaneme derivací:

$$x(x) = \begin{cases} 0 & \text{pro} \quad x \leq 0 \\ \frac{2}{l\sqrt{l^2-4x}} & \text{pro} \quad 0 \leq x \leq \frac{l^2}{4} \\ 0 & \text{pro} \quad x > \frac{l^2}{4} \end{cases}$$

□

11.18.7. *Nechť X, Y jsou nezávislé náhodné veličiny, přičemž X má rovnoměrné rozdělení pravděpodobnosti na intervalu $(0,2)$, Y je pak dána následující hustotou pravděpodobnosti:*

$$f(x) = \begin{cases} 0 & pro \quad x \leq 0 \\ 2x & pro \quad 0 < x < 1 \\ 0 & pro \quad x \geq 1. \end{cases}$$

Určete pravděpodobnost, že Y je menší než X^2.

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 $Y < X^2$:

$$P = \iint\limits_{O} f_{(X,Y)} \,\mathrm{d}x\,\mathrm{d}y = 1 - \iint\limits_{\mathbb{R}^2 \setminus O} f_{(X,Y)} \,\mathrm{d}x\,\mathrm{d}y = 1 - \int_0^1 \int_{x^2}^1 y \,\mathrm{d}y\,\mathrm{d}x = \frac{3}{5}.$$

□

11.18.8. *Nechť X, Y jsou nezávislé náhodné veličiny, přičemž X je dána následující hustotou pravděpodobnosti:*

$$f(x) = \begin{cases} 0 & pro \quad x \leq 0 \\ 2x & pro \quad 0 < x < 1 \\ 0 & pro \quad x \geq 1, \end{cases}$$

veličina Y pak touto hustotou pravděpodobnosti:

$$f(x) = \begin{cases} 0 & pro \quad x \leq 0 \\ \frac{x}{2} & pro \quad 0 < x < 2 \\ 0 & pro \quad x \geq 2. \end{cases}$$

Určete pravděpodobnost, že Y je větší než X^2.

Řešení. Obdobně jako v předchozím příkladě určíme, že $f_{(X,Y)}(u,v) = uv$, pro $(u,v) \in (0,1) \times (0,2)$, $f_{(X,Y)}(u,v) = 0$ jinak. Pro hledanou pravděpodobnost P pak máme

$$P = \int_0^1 \int_{x^2}^2 xy \,\mathrm{d}y\,\mathrm{d}x = \frac{11}{12}.$$

□

11.18.9. *Nechť X, Y jsou nezávislé náhodné veličiny, přičemž X je dána následující hustotou pravděpodobnosti:*

$$f(x) = \begin{cases} 0 & pro \quad x \leq 0 \\ \frac{2x}{9} & pro \quad 0 < x < 3 \\ 0 & pro \quad x \geq 1, \end{cases}$$

veličina Y pak touto hustotou pravděpodobnosti:

$$f(x) = \begin{cases} 0 & pro \quad x \leq 0 \\ \frac{x}{2} & pro \quad 0 < x < 2 \\ 0 & pro \quad x \geq 2. \end{cases}$$

Určete pravděpodobnost, že Y je větší než X^3.

Řešení.

$$P = \int_0^{\sqrt[3]{2}} \int_{x^3}^{2} xy \,\mathrm{d}y \,\mathrm{d}x = \frac{\sqrt[3]{4}}{12}.$$

□

11.14

11.19. Funkce náhodných veličin. 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 se značnou sociální solidaritou je první veličina hodně variabilní, zatímco druhá může být skoro konstantní. Statisticky se proto budou značně odlišovat.

Nejjednodušší funkcí, po konstantách, je afinní závislost

$$\psi(x) = a + bx$$

s konstatními $a, b \in \mathbb{R}$, $b \neq 0$. 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 $x = \frac{1}{b}(y - a)$ je proto pravděpodobnostní funkce nenulová právě v bodech $y_i = ax_i + b$. V případě rozdělení X_n typu $\mathrm{Bi}(n, p)$ převádí transformace

$$x = y\sqrt{np(1-p)} + np$$

náhodnou veličinu X_n na rozdělení Y_n s distribuční funkcí blízkou distribuční funkci spojitého rozdělení $N(0, 1)$.

Podobně zkusme opačnou transformaci provést na veličinu Y s normálním rozdělením $N(0, 1)$. Pro pevně zvolená čísla $\mu, \sigma \in \mathbb{R}$, $\sigma > 0$ spočtěme rozdělení náhodné veličiny $Z = \mu + \sigma Y$. Dostáváme distribuční funkci

$$\begin{aligned} F_Z(z) &= P(Z < z) = P(\mu + \sigma Y < z) \\ &= F_Y(\frac{z-\mu}{\sigma}) = \int_{-\infty}^{\frac{z-\mu}{\sigma}} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-t^2/2} \, dt \\ &= \int_{-\infty}^{z} \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}} \, dx, \end{aligned}$$

kde poslední úprava vychází ze substituce $x = \mu + \sigma t$. Hustota naší nové náhodné veličiny Z je proto

$$f_Z = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

a takovému rozdělení se říká normální typu $\mathrm{N}(\mu, \sigma)$.

11.15

11.20. Číselné charakteristiky náhodných veličin. Při statistickém zkoumání hodnot náhodných veličin (např. zpracování výsledků nějakého měření) hledáme výpovědi o náhodné veličině pomocí různých z ní odvozených čísel.

Jako nejjednodušší příklad může sloužit *střední hodnota* EX náhodné veličiny X, která je definována

$$EX = \begin{cases} \sum_i x_i f_X(x_i) & \text{pro diskrétní veličinu} \\ \int_{-\infty}^{\infty} x f_X(x) dx & \text{pro spojitou veličinu.} \end{cases}$$

Obecně střední hodnota náhodných veličin nemusí existovat, protože příslušné sumy či integrály nemusí konvergovat. Obvykle říkáme, že střední hodnota existuje, když nastává absolutní konvergence.

Střední hodnotu můžeme přímo vyjádřit také pro funkce $Y = \psi(X)$ náhodné veličiny X. V diskrétním případě můžeme přímo spočíst

$$\begin{aligned} EY &= \sum_j y_j P(Y = y_j) \\ &= \sum_j y_j \sum_{\psi(x_i)=y_j} P(X = x_j) \\ &= \sum_i \psi(x_i) P(X = x_i). \end{aligned}$$

Je tedy $E\psi(X)$ přímo spočítatelná pomocí pravděpodobnostní funkce f_X.

Podobně vyjadřujeme střední hodnotu funkce ze spojité náhodné veličiny:

$$E\psi(X) = \int_{-\infty}^{\infty} \psi(x) f_X(x) dx$$

pokud tento integrál absolutně konverguje.

Dalšími užitečnými charakteristikami jsou tzv. *kvantily*. Pro ryze monotónní distribuční funkci F_X (tj. spojitou náhodnou veličinu X s všude nenulovou hustotou, jako je tomu např. u normálního rozdělení) jde prostě o inverzní funkci $F_X^{-1} : (0,1) \to \mathbb{R}$. To znamená, že hodnota $y = F^{-1}(\alpha)$ je taková, že $P(X < y) = \alpha$.

Obecněji, je-li $F_X(x)$ distribuční funkce náhodné veličiny X, pak definujeme *kvantilovou funkci*

$$F^{-1}(\alpha) = \inf\{x \in \mathbb{R};\ F(x) \geq \alpha\},\ \alpha \in (0,1).$$

Zřejmě jde o zobecnění předchozí definice.

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 α rovno násobkům desetin a setin). K těmto hodnotám se vrátíme v popisné statistice později.

11.16

11.21. Střední hodnoty některých rozložení. Spočtěme si nejprve střední hodnotu náhodné veličiny X s rozdělením $\mathrm{Bi}(n,p)$.

$$EX = \sum_{i=0}^{n} i\binom{n}{i}p^i(1-p)^{(n-i)} = \sum_{i=1}^{n} i\binom{n}{i}p^i(1-p)^{(n-i)} \tag{11.1}$$

$$= np\sum_{i=1}^{n}\binom{n-1}{i-1}p^{(i-1)}(1-p)^{(n-i)} = \tag{11.2}$$

$$= np\sum_{j=0}^{n-1}\binom{n-1}{j}p^{j}(1-p)^{(n-1)-j} = \tag{11.3}$$

$$= np. \tag{11.4}$$

11.17

11.22. Náhodné vektory.

11.17

11.23. Elementární vlastnosti střední hodnoty.

11.24. Věta. *Buď X náhodná veličina s existující střední hodnotou. Potom*

$$E(a+bX) = a + bE(X),$$

pro libovolná reálná a, b.

Důkaz. Snadný, plyne z možnosti vytýkat reálná čísla ze sumy, resp. integrálu. □

11.25. Věta. *Pro náhodné veličiny X, Y s existujícími středními hodnotami platí*

$$E(X+Y) = EX + EY.$$

Důkaz. Nechť například X je spojitá náhodná veličina s hustotou pravděpodobnosti f a Y spojitá náhodná veličina s hustotou pravděpodobnosti g a nechť h je hustota pravděpodobnosti $X+Y$. Potom ... □

Následující věta nám poskytuje návod, jak počítat střední hodnotu transformované náhodné veličiny.

i_hodnota_transformovane

11.26. Věta. *Nechť X je spojitá náhodná veličina s hustotou pravděpodobnosti f a $g : \mathbb{R} \to \mathbb{R}$ je hladká funkce. Pak*

$$E(g(X)) = \int_{-\infty}^{\infty} g(x)f(x)\,\mathrm{d}x.$$

11.19

Důkaz. □

11.27. Rozptyl a směrodatná odchylka. Rozptyl a směrodatná odchylka náhodné veličiny popisují, do jaké míry se hodnoty náhodné veličiny kumulují kolem její střední hodnoty. Pro náhodnou veličinu X s konečnou střední hodnotou definujeme její *rozptyl*

$$\operatorname{var} X = E\left((X-EX)^2\right).$$

Snadno se ukáží tyto vlastnosti konečného rozptylu náhodné veličiny X:

$$\begin{aligned} \operatorname{var} X &= E(X^2) - (EX)^2 \\ \operatorname{var}(a+bX) &= b^2 \operatorname{var} X \end{aligned}$$

11.20

11.28. Momenty a momentová funkce rozdělení.

11.29. Definice. 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. Funkci $M_X(t) : \mathbb{R} \to \mathbb{R}$ definovanou předpisem

$$M_X(t) = Ee^{tX}$$

pak *momentovou vytvořující funkcí* náhodné veličiny X.

11.30. Věta. *(doplnit předpoklady!) Koeficienty Taylorova rozvoje funkce $M_X(t)$ jsou právě centrální momenty náhodné veličiny X.*

Momentová funkce poskytuje za jistých podmínek úplnou charakterizaci náhodné veličiny, obdobně jako její distribuční funkce.

Spočítejme momentovou funkci náhodné veličiny X s normálním rozložením. Použijeme pro to větu 11.26.

$$\begin{aligned} M_X(t) &= \int_{-\infty}^{\infty} e^{tx} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}\,\mathrm{d}x = \\ &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}(x^2-2tx+t^2-t^2)}\,\mathrm{d}x = \\ &= e^{\frac{t^2}{2}} \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{(z-t)^2}{2}}\,\mathrm{d}x = \\ &= e^{\frac{t^2}{2}}. \end{aligned}$$

11.21

11.31. Kovariance. Pro náhodné veličiny X, Y s existujícími rozptyly definujeme jejich *kovarianci* $C(X, Y)$ (též $\operatorname{cov}(X, Y)$) jako

$$C(X, Y) = E\left((X - EX)(Y - EX)\right)$$

11.32. Poznámka.

Pro kovarianci náhodných veličin X, Y, Z platí

$$\begin{aligned} \operatorname{cov}(X, Y) &= E(XY) - (EX)(EY) \\ \operatorname{cov}(X + Y, Z) &= \operatorname{cov}(X, Z) + \operatorname{cov}(Y, Z) \\ \operatorname{cov}(a + bX, c + dY) &= bd \operatorname{cov}(X, Y), \quad a, b, c, d \in \mathbb{R} \end{aligned}$$

Důkaz. Vyplývá z vlastností střední hodnoty náhodné veličiny. Proveďme např. důkaz třetího vztahu:

$$\begin{aligned} \operatorname{cov}(a + bX, c + dY) &= E\left((a + bX - E(a + bX))(c + dY - E(c + dY))\right) \\ &= E\left((bX - bE(X))(dY - dE(Y))\right) = \\ &= E\left(bd(X - E(X))(Y - E(Y)\right) = \\ &= bdE\left((X - EX)(Y - EY)\right) = \\ &= bd \operatorname{cov}(X, Y). \end{aligned}$$

□

Vidíme, že podle definice je $\operatorname{var}(X,X) = \operatorname{cov}(X,Y)$. Pokud uvážíme náhodné veličiny s definovaným rozptylem jako vektorový prostor nad $\mathbb{R}$, tak kovariance je symetrická bilineární forma a rozptyl jí odpovídající kvadratická forma. Odtud

kovariance

$$\operatorname{cov}(X,Y) = \frac{1}{2}\left(\operatorname{var}(X+Y) - \operatorname{var}(X) - \operatorname{var}(Y)\right). \tag{11.5}$$

Korelace dvou náhodných veličin vypovídá o míře jejich závislosti.

11.33. Věta. *Pokud jsou X a Y nezávislé, pak $C(X,Y) = 0$.*

Důkaz. Jsou-li X a Y nezávislé, jsou nezávislé též veličiny $(X-EX)$ a $(Y-EY)$ a tudíž

$$\begin{aligned} C(X,Y) &= E\left((X-EX)(Y-EY)\right) = E(X-EX)E(Y-EY) = \\ &= (EX-EX)(EY-EY) = 0. \end{aligned}$$

□

Bezprostředním důsledkem předchozí věty a vztahu (11.5) je potom

11.34. Důsledek. *Pro nezávislé náhodné veličiny X a Y platí*

$$\operatorname{cov}(X+Y) = \operatorname{cov}(X) + \operatorname{cov}(Y).$$

Ještě lépe než kovariance (i když opět ne úplně) vystihuje míru (ne)závislosti dvou náhodných veličin korelační koeficient.

náhodných veličin X a Y rozumíme hodnotu

$$\rho_{X,Y} = \frac{\operatorname{cov}(X,Y)}{\sqrt{\operatorname{var} X}\sqrt{\operatorname{var} Y}}.$$

Schwarzova nerovnost pro positivně semi-definitní formu cov nám pak říká, že

$$|\rho_{X,Y}| \leq 1$$

Dále snadno dostáváme

$$\rho_{a+bX,c+dY} = \operatorname{sign}(bd)\rho_{X,Y}$$

a pro nezávislé veličiny X, Y pak $\rho_{X,Y} = 0$.

11.35. Příklady.

11.35.1. *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 pravdivostní 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, Y^2, XY:

$$\begin{aligned} E(X) \quad &= E(Y) \quad &&= 0 \cdot \frac{1}{4} + 1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} = 1 \\ E(X^2) \quad &= E(Y^2) \quad &&= 0 \cdot \frac{1}{4} + 1 \cdot \frac{1}{2} + 4 \cdot \frac{1}{4} = \frac{3}{2} \\ E(XY) \quad & &&= 0 \cdot \frac{3}{8} + 1 \cdot \frac{1}{4} + 2 \cdot \frac{1}{4} + 4 \cdot \frac{1}{8} = \frac{5}{4} \end{aligned}$$

Máme tedy

$$\begin{aligned} \sigma^2(X) \quad &= \varsigma^2(Y) \quad &&= E(X^2) - [E(X)]^2 = \frac{1}{2} \\ \operatorname{cov}(X,Y) \quad & &&= E(XY) - E(X)E(Y) = \frac{1}{4} \end{aligned}$$

Celkem

$$\rho_{X,Y} = \frac{\operatorname{cov}(X,Y)}{\sigma(X) \cdot \sigma(Y)} = \frac{1}{2}$$

□

11.35.2. *Dvakrát hodíme šestibokou kostkou. Určete korelační koeficient veličiny X udávající počet padlých sudých čísel a veličiny Y udávající počet padlých lichých čísel.*

Řešení. Řešíme analogicky jako předchozí příklad:

$$\rho_{X,Y} = -1.$$

□

11.22

11.36. Přehled rozdělení odvozených od normálního.

11.23

11.37. Limitní vlastnosti.

11.24

11.38. Věta (Centrální limitní věta)**.**

11.39. Příklady.

11.39.1. *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 Φ standardního normálního rozdělení. Hledaná pravděpodobnost je tedy

$$\begin{aligned} P \quad &= \quad 1 - P[759 \leq X \leq 841] = 1 - P\left[-2,05 \leq \frac{X - 800}{20} \leq 2,05\right] \doteq \\ &\doteq \quad 2\Phi(-2,05) \doteq 0,0404. \end{aligned}$$

□

11.39.2. *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 $n = 1600$ podle Moivreovy-Laplaceovy věty velmi dobře odhadnout jako distribuční funkci Φ standardního normálního rozdělení. Hledaná pravděpodobnost je tedy

$$\begin{aligned} P[1767 \leq X \leq 1833] &= P\left[-1,1 \leq \frac{X-1800}{30} \leq 1,1\right] \doteq \\ &\doteq \Phi(1,1) - \Phi(-1,1) \doteq 0,7498. \end{aligned}$$

□

11.39.3. *Pravděpodobnost narození chlapce je* $0,515$. *Jaká je pravděpodobnost, že mezi deseti tisíci novorozenci bude stejně nebo více děvčat než chlapců.*

Řešení.

$$P[X < 5000] = P[\underbrace{\frac{X-5150}{\sqrt{5150 \cdot 0,485}}}_{\sim N(0,1)} < \underbrace{\frac{-150}{\sqrt{5150 \cdot 0,485}}}_{-3,001\ldots}] \doteq$$
$$\doteq 0,00135$$

□

11.39.4. *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 Φ stadardního normálního rozložení:

$$P[X \geq 3100] = P[\frac{X-3000}{50} \geq \frac{3100-3000}{50}] = P[\frac{X-3000}{50} \geq 2] \doteq 1-\Phi(2) \doteq 0,0228.$$

□

2. Popisná statistika

11.25 **11.40. Soubor hodnot a jeho popis.**

11.26 **11.41. Číselné charakteristiky polohové.**

11.27 **11.42. Míry variability souboru.**

11.28 **11.43. Další výběrové koeficienty.**

11.29 **11.44. Diagramy.**

11.30

3. Matematická statistika

11.45. Výběry z populace. V praxi často potkáváme veliký základní statistický soubor s N jednotkami, který budeme stručně nazývat *populace*. Na každé z N jednotek přitom můžeme měřit hodnotu nějakého pevně zvoleného *číselného znaku* X, čímž bychom celkem získali N hodnot $x_1, x_2, \dots, x_N$. Průměr $\bar{x}$ všech hodnot x_i označíme μ a populační rozptyl σ^2, tj.

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i, \qquad \sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2.$$

Je-li naše populace skutečně veliká, nemůžeme (nebo alespoň z různých důvodů nechceme) získávat skutečně všechny hodnoty x_i. Místo toho provedeme *výběr* (tj. zvolíme tzv. *výběrový soubor*) o rozsahu $n < N$ jednotek, který bude „dobře“ reprezentovat celou populaci. Pro naše potřeby budeme nyní za dobrý považovat takový výběr, kdy všechny n–tice jednotek mají stejnou šanci na vybrání.

Uvažme neprve případ, kdy použijeme *náhodný výběr bez vracení*, tzn. že postupně vybíráme jednotky jednu za druhou, aniž bychom dosud zpracované do základní populace vraceli. Pro celý výběrový soubor máme zjevně $\binom{N}{n}$ možností a každou pevně zvolenou n–tici indexů ω můžeme zvolit $\frac{(N-n)!}{N!}$ způsoby.

Pracujeme tedy s konečným jevovým polem s elementárními jevy ω a přiřazování číslené charakteristiky x_i má charakter náhodného vektoru

$$(X_1(\omega), X_2(\omega), \dots, X_n(\omega)),$$

který vzniká z n–násobného výběru elemntárního jevu ω a přiřazení příslušné číselné honoty znaku. Při výpočtech průměrů a rozptylů pracujeme se symetrickými funkcemi, budou nás proto nyní skutečně zajímat pouze neuspořádané n–tice. Každý z takových výběrů je sjednocením $n!$ jevů a má tedy pravděpodobnost $\frac{1}{\binom{N}{n}}$.

Chceme nyní ověřit, do jaké míry vede použití standardních formulí pro výběrové průměry a rozptyly k dobrým odhadům skutečných hodnot pro celou populaci. Uvažujme proto náhodné veličiny

$$\bar{X} = \bar{X}(s) = \frac{1}{n}\sum_{i=1}^{n} X_i, \quad S^2 = \frac{1}{n}\sum_{i=1}^{n}(X_i - \bar{X})^2.$$

Věta. *Za výše uvedených podmínek a označení platí*

$$E\bar{X} = \mu, \quad ES^2 = \frac{N}{N-1}\sigma^2, \quad \operatorname{var}\bar{X} = \frac{N-n}{N-1}\frac{\sigma^2}{n}.$$

Tvrzení řeší, zda průměr číselného znaku X populace a příslušný rozptyl tohoto znaku jsou ve střední hodnotě (tj. „v průměru“) stejné jako odpovídající hodnoty spočtené na náhodném výběru. Pokud ano, říkáme, že jde o *nestranné odhady*. Výběrový průměr tedy je nestranným odhadem, zatímco výběrový rozptyl se jím stane teprve po korekci koeficientem $\frac{N-1}{N}$. K nestranným odhadům se jestě vrátíme obecněji.

Důkaz. Za tím účelem si technicky popišme naše náhodné výběry pomocí N náhodných veličin W_i, které jsou definovány tak, aby pro výběr n–tice s bylo $W_i(s) = 1$ pokud $i \in s$ a nula jinak (tzv. *indikátory zahrnutí*). Snadno se pak ukáže ...

□

11.31

11.46. Poznámky o statistické indukci.

11.32

11.47. Poznámky o testování hypotéz.

11.33

11.48. Poznámky o lineárních modelech.

11.34

11.49. Závěrem.

4. Poznámky o některých aplikacích

AŽ NĚKDY BUDE DELŠÍ SEMESTR!!!! (třeba pravděpodobnostní model datového kanálu, Kalmanův filtr v matematické ekonomii atd.)

Literatura

[1] Frank Ayres, Jr., Theory and Problems of Differential and Integral Calculus, second edition, Schaum publishing, New York, 1964, 336s.

[2] Marie Budíková, Štěpán Mikoláš, Pavel Osecký, Teorie pravděpodobnosti a matematická statistika (sbírka příkladů), Masarykova univerzita, 3. vydání, 2004, 117 stran, ISBN 80-210-3313-4.

[3] Marie Budíková, Štěpán Mikoláš, Pavel Osecký, Popisná statistika, Masarykova univerzita, 3. vydání, 2002, 48 stran, ISBN 80-210-1831-3.

[4] Marie Budíková, Tomáš Lerch, Štěpán Mikoláš, Základní statistické metody, Masarykova univerzita, 2005, 170 stran, ISBN 80-210-3886-1.

[5] Zuzana Došlá, Jaromír Kuben, Diferenciální počet funkcí jedné proměnné, MU Brno, 2003, 215 s., ISBN 80-210-3121-2.

[6] Zuzana Došlá, Roman Plch, Petr Sojka, Diferenciální počet funkcí více proměnných s programem Maple, MU Brno, 1999, 273 s.

[7] William J. Gilbert, W. Keith Nicholson, Modern algebra with applications, 2nd ed. John Wiley and Sons (Pure and applied mathematics) ISBN 0-471-41451-4

[8] Jiří Herman, Radan Kučera, Jaromír Šimša, Metody řešení matematických úloh I, MU Brno, 2. přepsané vydání, 1996

[9] Jiří Herman, Radan Kučera, Jaromír Šimša, Metody řešení matematických úloh II, MU Brno, 2. přepsané vydání, 1997

[10] Pavel Horák, Úvod do lineární algebry, MU Brno, skripta.

[11] Ivana Horová, Jiří Zelinka, Numerické metody, MU Brno, 2. rozšířené vydání, 2004, 294 s., ISBN 80-210-3317-7.

[12] Jiří Matoušek, Jaroslav Nešetřil, Kapitoly z diskrétní matematiky, Univerzita Karlova v Praze, Karolinum, Praha, 2000, 377 s.

[13] Luboš Motl, Miloš Zahradník, Pěstujeme lineární algebru, 3. vydání, Univerzita Karlova v Praze, Karolinum, 348 stran (elektronické vydání také na http://www.kolej.mff.cuni.cz/~lmotm275/skripta/).

[14] Riley, K.F., Hobson, M.P., Bence, S.J. Mathematical Methods for Physics and Engineering, second edition, Cambridge University Press, Cambridge 2004, ISBN 0 521 89067 5, xxiii + 1232 pp.

[15] František Šik, Lineární algebra zaměřená na numerickou analýzu, MU, 1998, 176 s. ISBN 80-210-1996-2.

[16] Jan Slovák, Lineární algebra. učební texty, Masarykova univerzita, elektronicky dostupné na www.math.muni.cz/~slovak

[17] Pavol Zlatoš, Lineárna algebra a geometria, skripta MFF Univerzity komenského v Bratislavě.

[18] Karel Zvára, Josef Štěpán, Pravděpodobnost a matematická statistika, Matfyzpress, Universita Karlova, 2006, 230 s.