Drsná matematika

Martin Panák, Jan Slovák

Pokus o učební text pro začínající studenty informatiky přibližující podstatnou část matematiky v rozsahu čtyř semestrálních přednášek. Prozatím první čtvrtina…

Obsah

Předmluva

Učební text vzniká průběžně při přípravě přednášek pro předměty Matematika I–IV na Fakultě informatiky MU. Standardní výklad se snaží akcentovat 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 dostávají a mají řešit a odevdávat 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, přikládáme ale i soubor zadávaných úloh.

Posluchači by se měli naučit:

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

Text je strukturován také pomocí barev 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 být při povrchnějším studiu přeskakovány jsou sázeny v barvě

Výhled obsahu pro všechny čtyři semestry je následující. Vměstná se do nich v dělení přibližně po dvou celcích v jednotlivých semestrech:

(1) Úvod a motivace
   - *Kombinatorické úvahy:* Pascalův trojúhelník, kombinační čísla, binomická věta, lineární rekurentní formule, diferenční rovnice (ekonomické a populační modely), konečná pravděpodobnost, geometrická pravděpodobnost, ...).
   - *geometrické úlohy v* $\mathbb{R}^2$*:* systémy rovnic, lineární zobrazení, rotace, afinní symetrie, zrcadlení, viditelnost stěn trojúhelníka
   - *relace a zobrazení:* uspořádání, ekvivalence, funkce (formální a operační definice zobrazení, definice na třídách ekvivalence pomocí reprezentantů apod.)

(2) Lineární modely (lineární algebra a geometrie)
   - vektor, matice, determinanty a maticový počet, vektorový prostor, lineární nezávislost, báze, lineární zobrazení, matice,
   - algebraické aplikace: systémy lineárních rovnic, lineární diferenční rovnice, Markovovy řetězce
   - geometrické aplikace: přímka, rovina, rovnice kontra parametrické vyjádření, poloha přímky a roviny, příčka mimoběžek, úhel, délka, objem, projektivní rozšíření R^3, projekticní transformace.

(3) Nelineární modely (diferenciální a integrální počet jedné proměnné)
   - posloupnosti a limity, funkce jedné proměnné, vyšetření průběhu funkce, Newtonův a Riemannův integrál.
   - aplikace: objemy, optimalizace, ODE, včetně konvolučních filtrů

(4) Přibližné modely (numerické metody)
   - interpolace,

- mocninné a Fourierovy řady,
- wavelety, spliny

(5) Nelineární modely podruhé (diferenciální a integrální počet více proměnných, ODE, PDE)
- kalkulus více proměnných,
- diferenciální a diferenční rovnice,
- přibližná řešení

(6) Kombinatorické metody (diskrétní matematika)
- rovinné grafy, barvení grafu, Eulerova kružnice, problém obchodního cestujícího, stromy, minimální kostry

(7) Obecné matematické struktury (algebra)
- grupy, algebry, svazy, okruhy, pole, dělitelnost, rozklad na prvočísla, Eulerova věta, RSA algoritmus.

(8) Pravděpodobnost a statistika
- Pravděpodobnostní prostor, hustota pravděpodobnosti, normální rozdělení, střední hodnota, medián, kvantil, rozptyl, příklady diskrétních a spojitých rozdělení
- statistické zpracování dat.

Náplň prvního semestru už můžete posoudit sami, Vaše odezva pomůže zlepšit ty další.

Leden 2006, 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

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

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 1.49, 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. Vlastnosti sčítání.

$$(a + b) + c = a + (b + c),\ \text{pro všechny } a, b, c \tag{KG1}$$

$$a + b = b + a,\ \text{pro všechny } a, b \tag{KG2}$$

$$\text{existuje prvek } 0 \text{ takový, že pro všechny } a \text{ platí } a + 0 = a \tag{KG3}$$

$$\text{pro všechny } a \text{ existuje prvek } (-a) \text{ takový, že platí } a + (-a) = 0. \tag{KG4}$$

[1] Podrobně lze formální základy matematiky nalézt např. ve skriptech Pavla Horáka [**3**].

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. 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) $$\text{existuje prvek } 1 \text{ takový, že pro všechny } a \text{ platí } 1 \cdot a = a$$

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

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. 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. 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. 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 $S = \{1, \dots, n\}$ prvních 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 nakonečné množině s n prvky je dán známou funkcí faktoriál:*

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

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 $k \leq n$)

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

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 $0 \leq k \leq n$ (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 $0 \leq k \leq n$ roven právě počtu možností, jak vybrat k-tici z n závorek v součinu (ty, kde bereme do výsledku a). Platí proto

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

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. 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). 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

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

$\square$

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

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

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. Počet čísel ze dvou cifer. *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. $\square$

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 $\binom{5}{2}(2^4-2)+5\cdot5(2^3-1)$ 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

$$\binom{5}{2}(2^4-2)+5\cdot5(2^3-1)-(2^3-1)4-(2^2-1)5=272.$$

$\square$

1.8. Kombinace a variace s opakováním. 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 $x_1, \dots, x_k$ je kombinace libovolných prvků z dané množiny

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

na které si zafixujeme uvedené pořadí prvků. Jednotlivé volby x_i přidáme do pořadí $a_1, \dots$ 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. □

Opět praktický příklad na procvičení:

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

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

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 $(r_1, \dots, r_k)$, $\sum_{i=1}^{k} r_i = n$ můžeme jednoznačně zašifrovat jako posloupnost jedniček a nul, ve které napíšeme nejprve c_1 jedniček, pak nulu, pak c_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

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

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

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.

1.10. 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*

$$f(n+1) = a \cdot f(n) + b, \tag{1.5}$$

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.

$$f(n+1) = a_n \cdot f(n) + b_n \tag{1.6}$$

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

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

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. □

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

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

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. $\square$

Uveďme si praktický příklad na řešení diferenčních rovnic prvního řádu:

1.13. 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

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

Podle vztahu (1.8) je d_k dáno následovně

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

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

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

$\square$

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). $\square$

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

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

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

Lineární diferenční rovnicí druhého řádu rozumíme

$$f(n+2) = a \cdot f(n+1) + b \cdot f(n) + c, \tag{1.13}$$

kde a, b, c jsou známé skalární koeficienty. Dobře známým příkladem s $c = 0$ je např. Fibonacciho posloupnost čísel $y_0, y_1, \dots$, viz příklad 1.15. Zkusme dosadit do rovnice (1.10) 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 je opět řešením rovnice, odvodili jsme tedy 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.

$$\begin{aligned} y_{n+2} &= y_{n+1} + \frac{1}{2}y_n \\ y_0 &= 2, y_1 = 0. \end{aligned} \tag{1.14}$$

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:

1.15. 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*

$$p_{n+2} = p_{n+1} + p_n, \quad n = 1, \dots, \tag{1.15}$$

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:

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

$$r^2 = r + 1, \tag{1.17}$$

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

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

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

1.16. Zjednodušený model chování národního produktu.

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

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

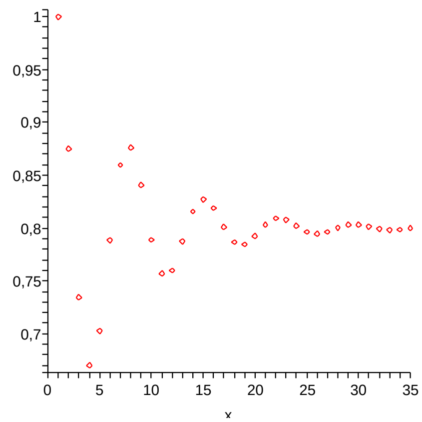
$$y(n) = \sum_{i=1}^{k} c_i f_i(n)$$

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

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



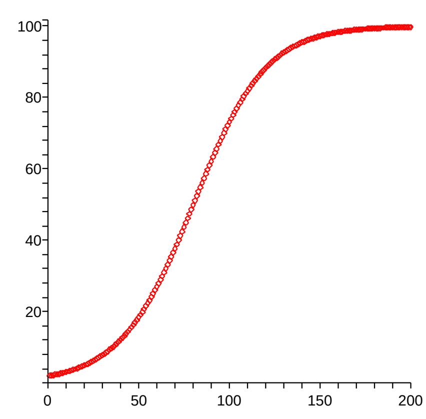
1.17. Nelineární příklad. Vraťme se na chvíli k rovnici prvního řádu, kterou jsme velice primitivně modelovali populační růst závisející přímo úměrně na okamžité velikosti populace p. Realističtější model bude mít takto úměrnou změnu populace $\Delta p(n) = p(n+1) - p(n)$ jen při malých hodnotách p, 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.

1.18. 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 nejjednodušším přiblížení. To, do jaké míry je takový popis adekvátní pro konkrétní pokusy či jiný problém, je záložitostí 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.

1.19. 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 $\mathcal{A}$).

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!

1.20. 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.

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

Uveďme nějaké praktičtější příklady:

1.21. Výtah. *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 1.8)

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

$\square$

1.22. Kino. *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

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

□

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

1.23. 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 $k \geq 1$. 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:

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

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

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

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

1.24. 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 $A_1,\dots,A_k$. Budeme psát $|M|$ pro počet prvků množiny M, tj. pro *mohutnost* množiny M.

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

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*.

1.25. 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.

1.26. 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 než dvěmi 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.

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

1.27. 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 ($i = 1, \dots, 5$), 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

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

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

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

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

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

□

1.28. 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:

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

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

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

Přímo z definice vyplývá tzv. „věta o násobení pravděpodobností" pro jevy $A_1, \dots, A_k$ splňující $P(A_1 \cap \dots \cap A_k) > 0$:

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

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. Opět házení kostkou. *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 sytém podmnožin, u kterých umíme určit jejich obsah. Třeba všechna konečná sjednocení trojůhelníků. 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 $\pi = 3,1415\dots$, která vyjadřuje poměr obsahu a čtverce poloměru. Pokud zvolíme za Ω jednotkový čtverec a za A průnik 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. Sekání tyče. *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:

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

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

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.

1.33. 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.

1.34. Přímky v rovině. Když se náš pozorovatel umí posouvat o libovolný násobek pevného vektoru, 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

$$ax + by = c, \tag{1.23}$$

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

$$a\alpha + b\beta = 0. \tag{1.24}$$

Výraz nalevo v rovnici přímky 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

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

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.

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:

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

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

Podobně, pokud místo vektoru v budeme zprava násobit jinou maticí B stejného rozměru jako je A, bude výsledkem aplikace předchozí formule po jednotlivých sloupcích matice B. 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

$$\det A = ad - bc = 0 \tag{1.26}$$

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.

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 *afinní zobrazení roviny* do sebe. Známými příklady jsou všechny afinní podobnosti. Lineární zobrazení pak odpovídají těm afinním, které zachovávají pevný bod O.

Co se stane, když pozorovatel tutéž rovinu bude 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 důvodu, proč tomu tak je ve všech dimenzích.

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, 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 $\cos\phi$. 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 $0 \le \sin\phi \le 1$ splňující $(\cos\phi)^2 + (\sin\phi)^2 = 1$.

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:

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

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:

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

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:

1.37. 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.

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

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

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 vol Δ 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).

1.39. 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. Konstrukce lichoúhelníka. *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 $A_1, A_2, \dots, A_{2n+1}$ a středy stran (od středu A_1A_2) postupně $S_1, S_2, \dots S_{2n+1}$, 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 $S_1, \dots, S_{2n+1}$. □

1.41. Kolize úseček. *Z bodu* $[-2, 0]$ *vyrazila v pravé poledne konstantní rychlostí* $1s^{-1}$ *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:

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

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

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

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

(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. □

1.42. 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. □

K dalšímu procvičení nejen geometrických úvah mohou posloužit následující dva příklady:

1.43. 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

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

□

1.44. 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

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

□

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.

1.45. 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.

1.46. 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 inverzní 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 indetické obrazení, u obecných relací tomu tak být nemusí.

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

$$\{\emptyset, \{\emptyset\}\} \subset \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}.$$

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.

1.48. 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 $R_a \cap R_b \neq 0$ 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".

1.49. 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 jnám samozřejmě vždy výsledek dobře reprezentují. Zbývá jen dobře definovat, kdy jsou (z hlediska výsledku odečítání) takové dvojice ekvivalentní. Potřebný vztah tedy je:

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

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 $(a, 0)$, se kterými se nám bude patrně počítat nejlépe.

Tento jednoduchý příklad ukazuje, jak důležité je umět nahlížet na třídy ekvivalence jako na celistvý objekt a soustředit se na vlastnosti těchto objektů, nikoliv formální popisy jejich konstrukcí. Ty jsou však důležité k ověření, že takové objekty vůbec existují.

U celých čísel nám už platí všechny vlastnosti skalárů (KG1)–(KG4) a (O1)-(O4), viz 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:

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

Opět neumíme očekávané chování v prostřední rovnosti v množině $\mathbb{Z}$ formulovat, nicméně rovnost na pravé straně ano. Zjevně jde o dobře definovanou 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.

1.50. 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:

1.51. Ekvivalence ano či ne. *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. $S(1) + S(1) = 2$.

□

1.52. 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 $v(3,4) = 4 \cdot 3 \cdot 2 = 24$. □

1.53. 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

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

□

1.54. 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:

1.55. 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:

$$a^{p-1} \equiv 1 (\bmod p). \tag{1.31}$$

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. 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. 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 $1 \le i \le m,\ 1 \le j \le n$. 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. 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. 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

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

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. 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. 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. 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. 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)

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

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

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

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

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

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. 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. 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.

2.11. 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 $a_1 u_{i_1} + \dots + a_k u_{i_k}$, kde a_i jsou skaláry, $u_j = (a_{j1}, \dots, a_{jn})$ jsou řádky (nebo $u_j = (a_{1j}, \dots, a_{mj})$ 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 $h(A)$ linárně 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. *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 x:

$$\begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Rotace kolem osy y:

$$\begin{pmatrix} \cos\varphi & 0 & \sin\varphi \\ 0 & 1 & 0 \\ -\sin\varphi & 0 & \cos\varphi \end{pmatrix}$$

Rotace kolem osy z:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix}.$$

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. *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.

2.14. 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 $\{1, \dots, n\}$ 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 $a, b \in X = \{1, \dots, n\}$ 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 $X = \{1, 2, \dots, n\}$ 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 $\sigma(1) = a_1, \dots, \sigma(n) = a_n$. 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 $(a_1, \dots, a_i, a_{i+1}, \dots, n)$, ve kterém je r inverzí. Pak zjevně je v pořadí $(a_1, \dots, a_{i+1}, a_i \dots, n)$ buď $r - 1$ nebo $r + 1$ inverzí. Každou transpozici (a_i, a_j) lze přitom získat postupným provedením $(j - i) + (j - i - 1) = 2(j - i) - 1$ transpozic sousedních prvků. Proto se provedením libovolné transpozice parita permutace změní. Navíc již víme, že všechny permutace lze získat prováděním transpozic. $\square$

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. *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. □

2.16. 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. □

2.17. 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 $|A| = a_{11} \cdot a_{22} \cdots a_{nn}$. Předchozí věta tedy poskytuje velice efektivní metodu výpočtu determinantů pomocí Gaussovy eliminační metody, viz. 2.7.

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.*

2.19. 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. Jednoduchý příklad rozvoje. *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

$$\begin{aligned} \begin{vmatrix} 1 & 3 & 5 & 6 \\ 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{vmatrix} &= 1 \cdot \begin{vmatrix} 2 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{vmatrix} - 1 \cdot \begin{vmatrix} 3 & 5 & 6 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{vmatrix} + 1 \cdot \begin{vmatrix} 3 & 5 & 6 \\ 2 & 2 & 2 \\ 1 & 2 & 1 \end{vmatrix} \\ &\overset{\text{Podle Saarusova pravidla}}{=} -2 - 2 + 6 = 2. \end{aligned}$$

□

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

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj}$$

neboli jde právě o prvky součinu $A \cdot B$ a $|K| = |H|$. Přitom rozvojem podle posledních n sloupců dostáváme

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

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 1.14, 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:

2.23. 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).

Připomeňme 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 $v_1, \dots, v_k \subset V$. Množina vektorů $M \subset V$ ve vektorovém prostoru V nad $\mathbb{K}$ se nazývá *lineárně nezávislá* jestliže pro každou k-tici vektorů $v_1, \dots, v_k \in M$ a každé skaláry $a_1, \dots, a_k \in \mathbb{K}$ 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 $v_1, \dots, v_k$ nazveme *lineárně nezávislou* jestliže $v_1, \dots, v_k$ jsou po dvou různé a $\{v_1, \dots, v_k\}$ 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 $\mathbb{R}$). □

2.25. 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) $\langle M\rangle = \{a_1 \cdot u_1 + \dots + a_k \cdot u_k;\ k \in \mathbb{N}, a_i \in \mathbb{K}, u_j \in M, j = 1, \dots, k\}$
(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 $\{a_1u_1 + \dots + a_ku_k\} \subset \langle M\rangle$ 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 $V_1, \dots, V_k \subset V$,

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

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

$$V_1 + V_2 + \dots + V_k = \{v_1 + \dots + v_k;\ v_i \in V_i, i = 1, \dots, k\}.$$

Součet $W = V_1 + \dots + V_k \subset V$ 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

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

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

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

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

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

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)

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

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. □

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) $\dim W \le \dim V$
(2) $V = W$ *právě když* $\dim V = \dim W$
(3) $\dim W_1 + \dim W_2 = \dim(W_1 + W_2) + \dim(W_1 \cap W_2)$.

Důkaz. Zbývá dokázat pouze poslední tvrzení. To je zřejmé, pokud je dimenze jednoho z prostorů nulová. Předpokládejme tedy $\dim W_1 = r \neq 0$, $\dim W_2 = s \neq 0$ 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

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

Pak $-(c_{t+1} \cdot v_{t+1} + \dots + c_s \cdot v_s) = a_1 \cdot w_1 + \dots + a_t \cdot w_t + b_{t+1} \cdot u_{t+1} + \dots + b_r \cdot u_r$ musí patřit do $W_2 \cap W_1$. To ale má za následek, že $b_{t+1} = \dots = b_r = 0$. Pak ovšem i $a_1 \cdot w_1 + \dots + a_t \cdot w_t + c_{t+1} \cdot v_{t+1} + \dots + c_s \cdot v_s = 0$ a protože příslušné vektory tvoří bázi W_2, jsou všechny koeficienty nulové. Tvrzení (3) se nyní ověří přímým počítáním generátorů. □

2.28. 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.

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

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

Potom ale

$$0 = (a_1 - b_1) \cdot v_1 + \dots + (a_n - b_n) \cdot v_n$$

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 $u = a_1v_1 + \dots + a_nv_n$ 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. 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) $f(a \cdot u) = a \cdot f(u),\ \forall a \in \mathbb{K},\ \forall u \in V$.

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* $Im f := f(V) \subset W$ 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) $f(a_1 \cdot u_1 + \dots + a_k \cdot u_k) = a_1 \cdot f(u_1) + \dots + a_k \cdot f(u_k)$
(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 $f(a \cdot u + b \cdot v) = a \cdot f(u) + b \cdot f(v) \in W_1$. □

[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 $\mathbb{K}$).

2.31. 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. □

2.32. 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:

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\underline{u}"', "\simeq"] & W \arrow[d, "\simeq"', "\underline{v}"] \\ \mathbb{K}^n \arrow[r, dotted, "f_{\underline{u},\underline{v}}"] & \mathbb{K}^m \end{tikzcd}$$

Přitom je každé lineární zobrazení jednoznačně určeno svými hodnotami na libovolné množině generátorů, zejména tedy na bázi $\underline{u}$. Označme

$$\begin{aligned} f(u_1) &= a_{11} \cdot v_1 + a_{21} \cdot v_2 + \dots + a_{m1} v_m \\ f(u_2) &= a_{12} \cdot v_1 + a_{22} \cdot v_2 + \dots + a_{m2} v_m \\ &\ \vdots \\ f(u_n) &= a_{1n} \cdot v_1 + a_{2n} \cdot v_2 + \dots + a_{mn} v_m \end{aligned}$$

tj. skaláry a_{ij} tvoří matici A, kde sloupce jsou souřadnice hodnot zobrazení f na bázových vektorech. Pro obecný vektor $u = b_1 \cdot u_1 + \dots + b_n \cdot u_n$ spočteme

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

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 $\mathrm{id}_V : V \to V$:

$$\begin{tikzcd}
V \arrow[r, "\mathrm{id}_V"] \arrow[d, "\underline{u}"', "\simeq"] & V \arrow[d, "\simeq"', "\underline{v}"] \\
\mathbb{K}^n \arrow[r, dotted, "(\mathrm{id}_V)_{\underline{u},\underline{v}}"] & \mathbb{K}^n
\end{tikzcd}$$

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 $\underline{u}$.

2.33. 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:

$$\begin{tikzcd}
V \arrow[r, "\mathrm{id}_V"] \arrow[d, "\underline{u}'"', "\simeq"] & V \arrow[r, "f"] \arrow[d, "\underline{u}"', "\simeq"] & W \arrow[r, "\mathrm{id}_W"] \arrow[d, "\simeq"', "\underline{v}"] & W \arrow[d, "\simeq"', "\underline{w}'"] \\
\mathbb{K}^n \arrow[r, dotted, "T"] & \mathbb{K}^n \arrow[r, dotted, "f_{\underline{u},\underline{v}}"] & \mathbb{K}^m \arrow[r, dotted, "S^{-1}"] & \mathbb{K}^m
\end{tikzcd}$$

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 $A' = T^{-1}AT$.

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

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

Napište matici tohoto zobrazení v bázi

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

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. 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.

2.36. 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 2.45.

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.

2.37. 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 $f|_{\operatorname{Im} f}$ 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 $\frac{1}{2}\pi$.

2.38. 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)

$$\det(A - a \cdot E) = 0. \tag{2.1}$$

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 2.33 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:

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

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

2.39. 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 $u_1, \dots, u_\ell$. $\square$

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.*

2.40. 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.

2.41. Příklad včetně změny báze. *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 2.33).
$$B = TAT^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & -\frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{2} & \frac{1}{4} & \frac{3}{4} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ -1 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$\square$

2.42. 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 2.40 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 $f - \lambda_i \operatorname{id}_{V_i}$ 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 řídá *Jordanův blok.*

2.43. 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 $f - \lambda_i \cdot \operatorname{id}$ 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.

2.44. Projekce. Lineární zobrazení $f : V \to V$ se nazývá *projekce*, jestliže platí

$$f \circ f = f.$$

V takovém případě je pro každý vektor $v \in V$

$$v = f(v) + (v - f(v)) \in \operatorname{Im}(f) + \operatorname{Ker}(f) = V$$

a je-li $v \in \operatorname{Im}(f)$ a $f(v) = 0$, pak je i $v = 0$. Je tedy přechozí součet podprostorů přímý. Říkáme, že f je projekce na podprostor $W = \operatorname{Im}(f)$ podél podprostoru $U = \operatorname{Ker}(f)$. 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 2.36. 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 $W^\perp$.

2.45. 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 $v_{\ell+1} = u_{\ell+1} + a_1 v_1 + \dots + a_\ell v_\ell$ platilo $\langle v_{\ell+1}, v_i \rangle = 0$, pro všechny $i = 1, \dots, \ell$. Odtud plyne

$$0 = \langle u_{\ell+1} + a_1 v_1 + \dots + a_\ell v_\ell, v_i \rangle = \langle u_{\ell+1}, v_i \rangle + a_i \langle v_i, v_i \rangle$$

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*

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

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 $v = x_1 e_1 + \dots + x_n e_n$ splňuje

$$\langle e_i, v \rangle = \langle e_i, x_1 e_1 + \dots + x_n e_n \rangle = x_i$$

a platí tedy vždy

$$v = \langle e_1, v \rangle e_1 + \dots + \langle e_n, v \rangle e_n. \tag{2.2}$$

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

$$v \mapsto \langle e_1, v \rangle e_1 + \dots + \langle e_n, v \rangle e_k.$$

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 2.36, 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 $\mathbb{R}^n$.

2.46. Příklad. *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

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

□

2.47. 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

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.

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. 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:

$$\begin{array}{rcccccccccc} x_1(t+1) & = & f_1x_1(t) & + & f_2x_2(t) & + & f_3x_3(t) & + & f_4x_4(t) & + & f_5x_5(t) \\ x_2(t+1) & = & \tau_{1,2}x_1(t) & & & & & & & & \\ x_3(t+1) & = & & & \tau_{2,3}x_2(t) & & & & & & \\ x_4(t+1) & = & & & & & \tau_{3,4}x_3(t) & & & & \\ x_5(t+1) & = & & & & & & & \tau_{4,5}x_4(t) & & \end{array}$$

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

$$P := \begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 \\ \tau_{1,2} & \tau_{2,2} & 0 & 0 & 0 \\ 0 & \tau_{2,3} & \tau_{3,3} & 0 & 0 \\ 0 & 0 & \tau_{3,4} & \tau_{4,4} & 0 \\ 0 & 0 & 0 & \tau_{4,5} & \tau_{5,5} \end{pmatrix}.$$

2. Lineární diferenční rovnice a filtry

Diferenčními rovnicemi jsme se zabývali již v první kapitole, viz např 1.14. Nyní si uvedeme náznak obecné teorie.

3.5. Diferenční rovnice. *Homogenní lineární diferenční rovnice* řádu k s konstantními koeficienty je dána výrazem

$$a_0x_n + a_1x_{n-1} + \cdots + a_kx_{n-k} = 0, \quad a_0 \neq 0 \quad a_k \neq 0.$$

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 1.14 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:

$$\lambda(a_0\lambda^n + \dots + a_k\lambda^{n-k})'$$

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

$$x_n = \alpha_0 + \alpha_1 n + \dots + \alpha_{k-1}n^{k-1}$$

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:

3.6. 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

  $$x_0 = b_0, \dots, x_{k-1} = b_{k-1}$$

  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 $\sin(n\varphi)$.

3.7. 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 $\sin(\frac{3\pi}{5}) = \frac{\sqrt{10+2\sqrt{5}}}{4}$. □

3.8. 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.

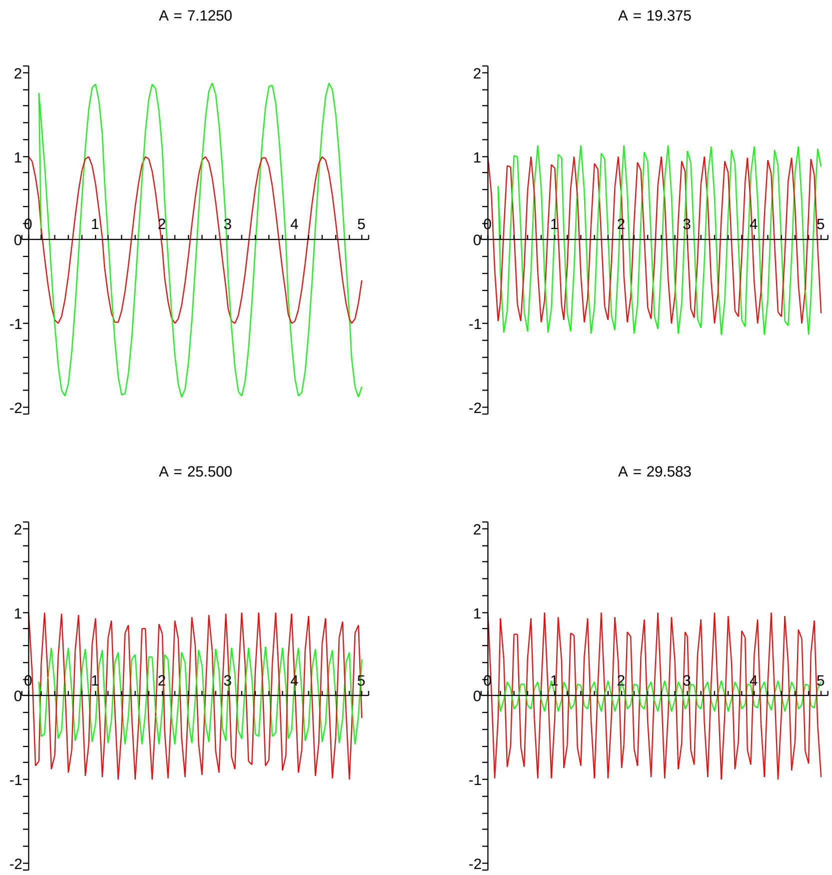
Jde nám tedy v první řadě o vyčíslení jádra našeho lineárního zobrazení T. To je ale dáno homogenní diferenční rovnicí

$$a_0 x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = 0, \quad a_0 \neq 0 \quad a_k \neq 0.$$

3.9. 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

3.10. 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 $x_n = (a_1, \dots, a_m)$. 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 $(1, \dots, 1)$, 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) *exituje reálné vlastní číslo λ_m matice A takové, že pro všchna 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 $\min_i \sum_j a_{ij} \le \lambda_m \le \max_i \sum_j a_{ij}$.*

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.

3.11. Příklad Markovova procesu. *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. □

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.

3.12. 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

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix} \tag{3.1}$$

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 2.38–2.42, 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 2.42, 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.

3.13. 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 2.37.

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 komplexníxh 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 2.37, 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. Všchny 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 stupnů podle osy y.

3.14. 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. 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*.

3.16. Spektrální rozklad symetrického zobrazení. Uvažujme symetrické zobrazení $f : V \to V$ s maticí A v nějaké ortonormální bázi a zkusme postupovat obdobně jako v 3.13. 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. 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*

$$f = \lambda_1 P_1 + \dots + \lambda_k P_k.$$

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.

3.18. 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 2.43 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.

3.19. 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, $r \le \min\{m, n\}$, 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 $m \le n$ 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 $(d_1, d_2, \dots, d_r, 0, \dots, 0)$ na diagonále, $d_i \ne 0$ pro všechny $i = 1, \dots, r$. 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 $v_1, \dots, v_r \in \mathbb{R}^m$. Tzn. $\langle v_i, v_i\rangle = d_i$, $i = 1, \dots, r$ a tedy vektory $u_i = \frac{1}{\sqrt{d_i}} v_i$ tvoří ortonormální systém nenulových vektorů. Doplňme je na ortonormální bázi $u_1, \dots, u_n$ 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.

3.20. 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.

3.21. 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.

3.22. 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 $\varphi^2 + \psi^2 =$

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:

3.23. Věta. *Pro každou reálnou matici A typu m/n existuje ortogonální matice Q a horní trojúhelníková matice R takové, že $A = Q^T R$.*

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, $j \le i$, 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 $A = Q^T R$. $\square$

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.

3.24. 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.

3.25. 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 $S = U^T AV$ 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
$$AA^{(-1)}A = USV^T VS'U^T USV^T = USS'SV^T = USV^T = A$$
a analogicky pro druhou rovnost. Dále
$$(AA^{(-1)})^T = (USS'U^T)^T = U(S')^T S^T U^T = U(SS')^T U^T = USS'U^T = AA^{(-1)}$$
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).

3.26. 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 $A^{(-1)}b$.

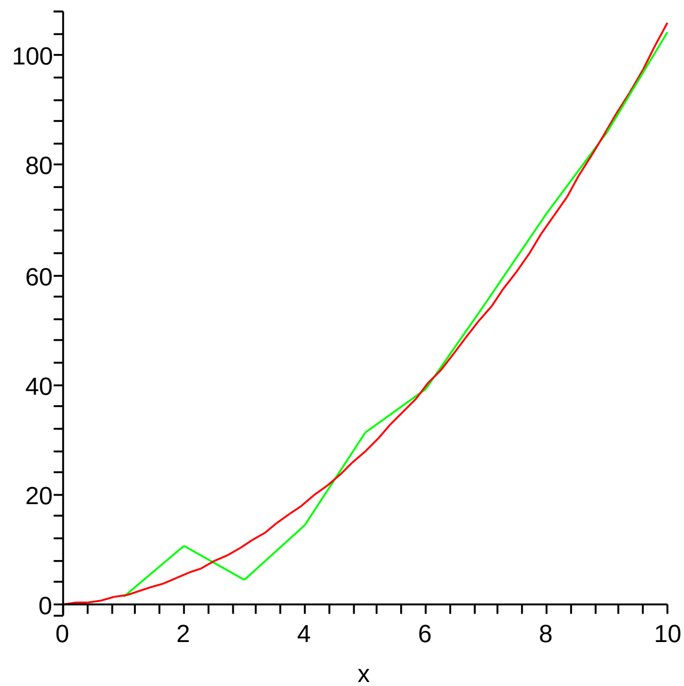
Abychom měli konkrétnější představu, uvažujme pouze dvě funkce $f_1(x) = x$, $f_2(x) = x^2$ a předpokládejme, že „naměřené hodnoty“ jejich neznámé kombinace $g(x) = y_1 x + y_2 x^2$ v celočíselných hodnotách pro x mezi 1 a 10 jsou

$$b^T = (1.44\ 10.64\ 4.48\ 14.56\ 31.12\ 39.20\ 54.88\ 71.28\ 85.92\ 104.16).$$

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 difereční rovnice, viz 3.5.

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.

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* $(A_0; u_1, \dots, u_n)$ 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 $\mathcal{A}_n$.

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 $\mathcal{Q}$.

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.

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. □

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.

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 splňujícícmi $\sum_{i=0}^k t_i = 1$ 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.

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*

$$\mathcal{K}(M) = \{t_1 A_1 + \cdots + t_s A_s;\ \sum_{i=1}^{s} t_i = 1,\ t_i \geq 0\}$$

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, $j = 1, \dots, s_2$ 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:

$$\epsilon(t_1 A_1 + \cdots + t_s A_s) + (1 - \epsilon)(t'_1 A_1 + \cdots + t'_s A_s),\ 0 \leq \epsilon \leq 1.$$

Zřejmě jsou opět všechny v S.

Zbývá ukázat, že konvexní obal bodů $A_1, \dots, A_s$ 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 $A_1, \dots, A_{s-1}$ je (podle předpokladu) tvořen právě těmi kombinacemi z pravé strany dokazované rovnosti, kde $t_s = 0$. Uvažme nyní libovolný bod $A = t_1 A_1 + \cdots + t_s A_s \in S$, $t_s \neq 1$, a afinní kombinace

$$\epsilon(t_1 A_1 + \cdots + t_{s-1} A_{s-1}) + (1 - \epsilon(1 - t_s))A_s,\ 0 \leq \epsilon \leq \tfrac{1}{1 - t_s}.$$

Jde o úsečku s krajními body určenými parametry $\epsilon = 0$ (bod A_s) a $\epsilon = 1/(1 - t_s)$ (bod v konvexním obalu bodů $A_1, \dots, A_{s-1}$). Bod A je vnitřním bodem této úsečky s parametrem $\epsilon = 1$. □

Konvexní obaly konečných množin bodů se nazývají *konvexní mnohostěny*. Jsou-li definující body $A_0, \dots, A_k$ 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 $u_1, \dots, u_k$, jsou libovolné vektory v zaměření $\mathbb{R}^n$, $A \in \mathcal{A}_n$ je libovolný bod. *Rovnoběžnostěn* $\mathcal{P}_k(A; u_1, \dots, u_k) \subset \mathcal{A}_n$ je množina

$$\mathcal{P}_k(A; u_1, \dots, u_k) = \{A + c_1 u_1 + \cdots + c_k u_k;\ 0 \leq c_i \leq 1, i = 1, \dots, k\}.$$

Jsou-li vektory $u_1, \dots, u_k$ nezávislé, hovoříme o k-rozměrném rovnoběžnostěnu $\mathcal{P}_k(A; u_1, \dots, u_k) \subset \mathcal{A}_n$. Z definice je zřejmé, že rovnoběžnostěny jsou konvexní. Ve skutečnosti jde o konvexní obaly jejich vrcholů.

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 $t_1, \dots, t_k$ vyeliminovat a získáme právě rovnice zadávající daný podprostor implicitně.

(2) *Nalézt podprostor generovaný několika podprostory $\mathcal{Q}_1, \dots, \mathcal{Q}_s$ (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.

$$\mathcal{Q} = A_1 + (Z(\{A_1, \dots, A_k\}) + Z(\mathcal{Q}_1) + \dots + Z(\mathcal{Q}_s)).$$

Pokud jsou podprostory zadány implicitně, je možné je nejdříve převést na parametrický tvar. V konkrétních situacích býají 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. 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 $t_0A_0 + \dots + t_sA_s \in \mathcal{A}$ pak dostaneme

$$\begin{aligned} f(t_0A_0 + \dots + t_sA_s) &= f(A_0) + t_1\varphi(A_1 - A_0) + \dots + t_s\varphi(A_s - A_0) \\ &= t_0 f(A_0) + t_1 f(A_1) + \dots + t_s f(A_s). \end{aligned}$$

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.

4.10. Příklad. *Vyjádřete afinní zobrazení f dané ve standardní afinní 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 $\underline{u} = \{[2, 0], (1, 1), (-1, 1)\}$.

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 dané 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

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}^{-1} \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} - \begin{pmatrix} 2 \\ 0 \end{pmatrix}. \right) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

V zadané bázi pak vyjádříme zobrazení následovně:

$$\begin{aligned} B &= \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \left[\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right) + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] + \begin{pmatrix} -1 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix} + \begin{pmatrix} 2 \\ -1 \end{pmatrix}. \end{aligned}$$

□

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 3.25. Asi proto dobře tušíme, jak se s problémem vypořádat:

4.11. 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. 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*
   $\|u\|^2 \ge |u \cdot e_1|^2 + \dots + |u \cdot e_k|^2$ *(Besselova nerovnost).*
4. *Pro ortonormální systém vektorů $(e_1, \dots, e_k)$ je $u \in \langle e_1, \dots, e_k \rangle$ právě když*
   $\|u\|^2 = |u \cdot e_1|^2 + \dots + |u \cdot e_k|^2$ *(Parsevalova rovnost).*
5. *Pro ortonormální systém vektorů $(e_1, \dots, e_k)$ a $u \in V$ je vektor*

   $$w = (u \cdot e_1)e_1 + \dots + (u \cdot e_k)e_k$$

   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 $\|u+v\| \leq \|u\|+\|v\|$. 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 $u \in V$

$$\|u\|^2 = \sum_{i=1}^{n}(u \cdot e_i)(u \cdot e_i) = \sum_{i=1}^{n} |u \cdot e_i|^2 \geq \sum_{i=1}^{k} |u \cdot e_i|^2.$$

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

$$\|u - v\|^2 = |u_1 - x_1|^2 + \dots + |u_k - x_k|^2 + |u_{k+1}|^2 + \dots + |u_n|^2$$

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. 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) $\rho(A, B) + \rho(B, C) \geq \rho(A, C)$
(4) *V každé kartézké souřadné soustavě $(A_0; \underline{e})$ mají body*

$$A = A_0 + a_1 e_1 + \dots + a_n e_n, \quad B = A_0 + b_1 e_1 + \dots + b_n e_n$$

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. □

4.14. Vzdálenost přímek. *Určete vzdálenost přímek v $\mathbb{R}^3$.*

$$p: [1, -1, 0] + t(-1, 2, 3), \quad a \quad q: [2, 5, -1] + t(-1, -2, 1).$$

Řešení. Vzdálenost je dána jako velikost kolmého průmětu libovolné příčky (spojnice) daných přímek do ortogonálního doplňku vektorového podprostoru generovaného jejich zaměřeními. Tento ortogonální doplňek 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 $0 \le \frac{|u\cdot v|}{\|u\|\|v\|} \le 1$, má tedy smysl následující definice.

4.15. Definice. *Odchylka* $\varphi(u,v)$ *vektorů* $u, v \in V$ v reálném vektorovém prostoru se skalárním součinem je dána vztahem

$$\cos\varphi(u,v) = \frac{u\cdot v}{\|u\|\|v\|}, \quad 0 \le \varphi(u,v) \le 2\pi.$$

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. 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:

4.17. 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

$$\begin{aligned}\frac{|u\cdot v|}{\|u\|\|v\|} &= \frac{|u\cdot(v_1+v_2)|}{\|u\|\|v\|} = \frac{|u\cdot v_1|}{\|u\|\|v\|}\\ &\leq \frac{\|u\|\|v_1\|}{\|u\|\|v\|} = \frac{\|v_1\|}{\|v\|} = \frac{\|v_1\|^2}{\|v\|\|v_1\|} = \frac{|v_1\cdot v|}{\|v\|\|v_1\|}.\end{aligned}$$

Odtud plyne

$$\cos\varphi(\langle v\rangle, \langle u\rangle) \leq \cos\varphi(\langle v\rangle, \langle v_1\rangle) = \frac{\|v_1\|}{\|v\|}$$

a protože funkce cos je na intervalu $[0, \frac{\pi}{2}]$ klesající, je tvrzení dokázané. □

4.18. 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 $A^T A$. 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 3.16–3.18.

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 $A^T A$. 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 $v \in U_1$, $v = a_1 u_1 + \dots + a_k u_k$, $\sum_{i=1}^k a_i^2 = \|v\|^2 = 1$. 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. □

4.19. Příklady standardních úloh. *1. Najděte vzdálenost bodu $A \in \mathcal{E}_n$ od podprostoru $\mathcal{Q} \subset \mathcal{E}_n$:*

Viz. věta 4.13.

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 4.13.

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!)

4.20. 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). □

4.21. 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

$$[1, 2] + (\frac{\sqrt{3}}{2} - \frac{1}{2}, \frac{\sqrt{3}}{2} + \frac{1}{2})t.$$

□

4.22. 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

$$\mathcal{P}_k(A; u_1, \dots, u_k) = \{A + c_1 u_1 + \dots + c_k u_k; 0 \le c_i \le 1, i = 1, \dots, k\}.$$

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

$$|A|^2 = |A||A| = |A^T||A| = |A^T A| = \det \begin{pmatrix} u_1 \cdot u_1 & \dots & u_k \cdot u_1 \\ \vdots & & \vdots \\ u_1 \cdot u_k & \dots & u_k \cdot u_k \end{pmatrix}.$$

Přímo z definice je neorientovaný objem roven součinu $\|v_1\|\|v_2\|\dots\|v_k\|$, kde $v_1 = u_1$, $v_2 = u_2 + a_1^2 v_1, \dots, v_k = u_k + a_1^k v_1 + \dots + a_{k-1}^k v_{k-1}$ je výsledek Grammova-Schmidtova ortogonalizačního procesu. Je tedy

$$\begin{aligned}(\operatorname{Vol}\mathcal{P}_k(A; u_1, \dots, u_k))^2 &= \det\begin{pmatrix} v_1 \cdot v_1 & \dots & v_k \cdot v_1 \\ \vdots & & \vdots \\ v_1 \cdot v_k & \dots & v_k \cdot v_k \end{pmatrix} \\ &= \det\begin{pmatrix} v_1 \cdot v_1 & 0 & \dots & 0 \\ \vdots & & \vdots & \\ 0 & 0 & \dots & v_k \cdot v_k \end{pmatrix}.\end{aligned}$$

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 $\underline{e}$. $\square$

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:

4.23. Důsledek. *Pro každé lineární zobrazení $\varphi : V \to V$ euklidovského vektorového prostoru V je $\det \varphi$ roven (orientovanému) objemu obrazu rovnoběžnostěnu určeného vektory ortonormální báze. Obecněji, obraz rovnoběžnostěnu $\mathcal{P}$ určeného libovolnými $\dim V$ vektory má objem roven $\det \varphi$–násobku původního objemu.*

4.24. 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 Věty 4.22 je objem rovnoběžnostěnu $\mathcal{P}_3(0; \underline{u}, \underline{v}, \underline{t})$ dán jako abolutní hodnota determinantu

$$\begin{vmatrix} u_1 & v_1 & t_1 \\ u_2 & v_2 & t_2 \\ u_3 & v_3 & t_3 \end{vmatrix} = \begin{vmatrix} t_1 & t_2 & t_3 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix} = \underline{t} \cdot (\underline{u} \times \underline{v}) \leq \|\underline{t}\|\|\underline{u} \times \underline{v}\| = \|\underline{u} \times \underline{v}\|.$$

Použité znaménko nerovnosti vyplývá z Cauchyovy nerovnosti, přičemž víme, že rovnost nastává právě pro $\underline{t} = c(\underline{u} \times \underline{v})$, $c \in \mathbb{R}$. Velikost objemu hledaného rovnoběžnostěnu tedy může být maximálne rovna velikosti obsahu rovnoběžníka daného vektory $\underline{u}$, $\underline{v}$ (tj. velikosti vektoru $(\underline{u} \times \underline{v})$). Rovnost nastane právě když

$$t = \pm\frac{(\underline{u} \times \underline{v})}{\|(\underline{u} \times \underline{v})\|}.$$

$\square$

4.25. 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 4.22.

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

$$y_1 x_1 + \dots + y_n x_n = \begin{vmatrix} u_{11} & \dots & u_{1(n-1)} & x_1 \\ \vdots & & \vdots & \vdots \\ u_{n1} & \dots & u_{n(n-1)} & x_n \end{vmatrix}$$

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. $\square$

4.26. 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.

4.27. 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 $b = 0$.

4.28. 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

4.29. 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 $u = x_1u_1 + \dots + x_nu_n$ 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. Nasledující 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 $\underline{u} = (u_1, \dots, u_n)$ na V a předpokládejme $a_{11} \neq 0$. Pak můžeme psát

$$\begin{aligned} f(x_1, \dots, x_n) &= a_{11}x_1^2 + 2a_{12}x_1x_2 + \dots + a_{22}x_2^2 + \dots \\ &= a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n)^2 + \text{členy neobsahující } x_1 \end{aligned}$$

Provedeme tedy transformaci souřadnic (tj. změnu báze) tak, aby v nových souřadnicích bylo

$$x_1' = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n,\ x_2' = x_2, \dots, x_n' = x_n.$$

To odpovídá nové bázi (spočtěte si jako cvičení příslušnou matici přechodu!)

$$v_1 = a_{11}^{-1}u_1,\ v_2 = u_2 - a_{11}^{-1}a_{12}u_1, \dots, v_n = u_n - a_{11}^{-1}a_{1n}u_1$$

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). □

4.30. 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).

4.31. Afinní klasifikace kvadratických forem. Po výpočtu polární báze Lagrangeovým algoritmem můžeme ještě vylepšit bázové vektory pomocí násobení skalárem tak, aby v příslušném analytickém vyjádření naší formy vystupovaly v roli koeficientů u kvadrátů jednotlivých souřadnic pouze skaláry 1, -1 a 0. Následující *věta o setrvačnosti* říká navíc, že počet jedniček a mínus jedniček nezávisí 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.

4.32. 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 $(1 : 1 : 0)$).

4.33. 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.

4.34. 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.

4.35. 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 $b = (b_1, \dots, b_n)^T \in \mathbb{R}^n$ a $A = (a_{ij})$ je invertibilní matice dimenze n. Působení takové matice na vektoru $(1, x_1, \dots, x_n)$ je právě obecná afinní transformace.

4.36. 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 $(x_0, x_1, \dots, x_n)$. 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 – žádny 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!)

4.37. 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 $\{(1/3, 1/3, 0), (-2/3, 4/3, 0), (-1/2, 1/2, 1)\}$. □

4.38. 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. □

Literatura

[1] Budíková, Mikoláš, Osecký: Teorie pravděpodobnosti a matematická statistika. Sbírka příkladů. MU Brno

[2] Herman, Kučera, Šimša: Metody řešení matematických úloh II, skripta MU Brno

[3] Pavel Horák, skripta MU Brno

[4] Miloš Zahradník, Luboš Motl: Pěstujeme lineární algebru, Karolinum (dostupné i v elektronické verzi)

[5] A. Prágerová: Diferenční rovnice, SNTL, Praha 1971