Lineární Algebra I.

Zápisky z přednášek Jiřího Fialy[*] na MFF UK, zimní semestr, ak. rok 2007/2008

Adam Liška[†]

8. prosince 2014

[*] http://kam.mff.cuni.cz/~fiala
[†] http://www.adliska.com

Obsah

1 Soustavy lineárních rovnic

Definice 1.1. Reálný n-složkový vektor $\mathbf{b}$ je uspořádaná n-tice reálných čísel:

$$\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Značíme $\mathbf{b} \in \mathbb{R}^n$. Všechny vektory jsou sloupcové. Pro řádkový zápis použijeme transposici:

$$(b_1, b_2, \ldots, b_n)^\top = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}; \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}^\top = (b_1, b_2, \ldots, b_n)$$

Podobně uspořádaná n-tice neznámých hodnot $\mathbf{x} = (x_1, \ldots, x_n)^\top$ se nazývá n-složkový vektor neznámých.

Definice 1.2. Reálná matice $\mathbf{A}$ řádu $m \times n$ je soubor $m \cdot n$ reálných čísel uspořádaných do útvaru o m řádcích a n sloupcích:

$$\mathbf{A} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$$

Píšeme $\mathbf{A} \in \mathbb{R}^{m \times n}$, prvky matice značíme versálkami s dolními indexy:

$$a_{ij} = (\mathbf{A})_{ij}$$

Čtvercová matice má stejný počet řádků a sloupců.

Definice 1.3. Nechť $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{b} \in \mathbb{R}^m$ a $x = (x_1, \ldots, x_n)^\top$ je vektor neznámých. Potom soustavou m lineárních rovnic o n neznámých rozumíme zápis:

$$\mathbf{Ax} = \mathbf{b}.$$

Tutéž soutavu lze zapsat v rozvinutém tvaru jako:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

Matice $\mathbf{A}$ se nazývá matice soustavy, vektor $\mathbf{b}$ se nazývá vektor pravých stran. Matice $(\mathbf{A}|\mathbf{b})$ je rozšířená matice soustavy.

Definice 1.4. Reálný vektor $x \in \mathbb{R}^n$ se nazývá řešením soustavy $\mathbf{Ax} = \mathbf{b}$, pokud splňuje všech m rovnic soustavy. To jest, $\forall i : a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i$.

2 Řešení soustav: Gaussova eliminační metoda

Pro řešení soustav lineárních rovnic se používají tzv. elementární ekvivalentní (řádkové) úpravy.

Definice 2.1. Elementární úpravou matice $\mathbf{A}$ vznikne matice $\mathbf{A}'$ (značíme $\mathbf{A} \sim \mathbf{A}'$), a to buď:

1. vynásobením i-tého řádku číslem $t \neq 0$:
$$a'_{kl} = \begin{cases} t \cdot a_{il}, & \text{pokud } k = i. \\ a_{kl}, & \text{jinak.} \end{cases}$$
2. přičtením j-tého řádku k i-tému:
$$a'_{kl} = \begin{cases} a_{il} + a_{jl}, & \text{pokud } k = i. \\ a_{kl}, & \text{jinak.} \end{cases}$$

Poznámka 2.2. Z těchto dvou úprav se dají odvodit i úpravy:

- přičtení t-násobku j-tého řádku k i-tému,
- záměna i-tého a j-tého řádku.

Nyní ukážeme, že výše zmíněné elementární úpravy nemění množinu řešení soustavy.

Věta 2.3. *Nechť $\mathbf{A}\mathbf{x} = \mathbf{b}$ a $\mathbf{A}'\mathbf{x} = \mathbf{b}'$ jsou soustavy takové, že $(\mathbf{A}|\mathbf{b}) \sim (\mathbf{A}'|\mathbf{b}')$. Potom obě soustavy mají shodné množiny řešení.*

Důkaz. Stačí dokázat pro úpravy 1 a 2 a pro i-tý řádek (jelikož ostatní řádky se nemění).

1. Vynásobení i-tého řádku číslem $t \neq 0$.

   Předpokládejme nejprve, že $\mathbf{x}$ je řešením $\mathbf{A}\mathbf{x} = \mathbf{b}$.
$$\begin{aligned} a'_{i1}x_1 + a'_{i2}x_2 + \cdots + a'_{in}x_n &= t \cdot a_{i1}x_1 + t \cdot a_{i2}x_2 + \cdots + t \cdot a_{in}x_n && \text{(definice 1. úpravy)} \\ &= t \cdot (a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n) \\ & && \text{(distributivita násobení ku sčítání zleva)} \\ &= t \cdot b_i && \text{(předpoklad } \mathbf{A}\mathbf{x} = \mathbf{b} \text{ } i\text{-té rovnice)} \\ &= b'_i && \text{(definice 1. úpravy)} \end{aligned}$$

   Obráceně, předpokládejme nyní, že $\mathbf{x}$ je řešením $\mathbf{A}'\mathbf{x} = \mathbf{b}'$.
$$\begin{aligned} a_{i1}x_1 + \cdots + a_{in}x_n &= \frac{t}{t}(a_{i1}x_1 + \cdots + a_{in}x_n) \\ &= \frac{1}{t}(ta_{i1}x_1 + \cdots + ta_{in}x_n) \\ &= \frac{1}{t}(a'_{i1}x_1 + \cdots + a'_{in}x_n) \\ &= \frac{1}{t}b'_i = \frac{1}{t}tb_i = b_i \end{aligned}$$

2. Přičtení i-tého řádku k j-tému.

   Předpokládejme, že $\mathbf{x}$ je řešením $\mathbf{Ax} = \mathbf{b}$.

$$\begin{aligned} a'_{i1}x_1 + a'_{i2}x_2 + \cdots + a'_{in}x_n &= (a_{i1} + a_{j1})x_1 + \cdots + (a_{in} + a_{jn})x_n \\ &= (a_{i1}x_1 + \cdots + a_{in}x_n) + (a_{j1}x_1 + \cdots + a_{jn}x_n) \\ &= b_i + b_j = b'_i \end{aligned}$$

   Předpokládejme, že $\mathbf{x}$ je řešením $\mathbf{A'x} = \mathbf{b'}$.

$$\begin{aligned} a_{i1}x_1 + \cdots + a_{in}x_n &= (a_{i1}x_1 + \cdots + a_{in}x_n) + (a_{j1}x_1 + \cdots + a_{jn}x_n) - (a_{j1}x_1 + \cdots + a_{jn}x_n) \\ &= (a_{i1} + a_{j1})x_1 + \cdots + (a_{in} + a_{jn})x_n - (a_{j1}x_1 + \cdots + a_{jn}x_n) \\ &= a'_{i1}x_1 + \cdots + a'_{in}x_n - (a_{j1}x_1 + \cdots + a_{jn}x_n) \\ &= b'_i - b_j = (b_i + b_j) - b_j = b_i \end{aligned}$$

$\square$

Postup řešení soustavy lineárních rovnic:

1. Sestavíme rozšířenou matici soustavy.
2. Tuto matici elementárními úpravami převedeme na odstupňovaný tvar.
3. Pomocí zpětné substituce popíšeme všechna řešení.

Definice 2.4. Říkáme, že matice $\mathbf{A} \in \mathbb{R}^{m \times n}$ je v odstupňovaném tvaru, pokud nenulové řádky jsou *ostře* uspořádány podle počtu počátečních nul a nulové řádky jsou až za nenulovými.[1] Formálně: $\exists r \in \{0; \ldots; m\}$ takové, že:

1. označíme-li pro $i \in \{1; \ldots; r\}$:

$$j(i) := min\{j | a_{ij} \neq 0\},$$

   tak platí: $j(1) < j(2) < \cdots < j(r) \leq n$

2. $\forall i > r, \forall j : a_{ij} = 0$

Prvkům $a_{i,j(i)}$ pro $i = 1, \ldots, r$ se říká pivoty.

Algoritmus 2.5. Algoritmus Gaussovy eliminace pro úpravu dané matice $\mathbf{A} \in \mathbb{R}^{m \times n}$ na odstupňovaný tvar elementárními řádkovými úpravami:

1. Setřídíme řádky vzestupně podle počátečních nul.

[1] Ostré uspořádání zajistí, že v matici nejsou žádné dva nenulové řádky o stejném počtu počátečních nul.

2. Pokud mají dva nenulové řádky stejně počátečních nul, tj. $j(i) = j(i+1)$, potom k $(i+1)$-tému řádku přičteme vhodný násobek i-tého řádku:

$$-\frac{a_{i+1,j(i)}}{a_{i,j(i)}}$$

3. Kroky 1 a 2 opakujeme, dokud některé řádky mají stené mnoho počátečních nul.

4. Matice $\mathbf{A}$ je v odstupňovaném tvaru.

Poznámka 2.6 (Složitost a konečnost Gaussovy eliminace)**.** Algoritmus Gaussovy eliminace je konečný, jelikož v každém kroku vzroste počet nul o jednu. Nejvýše tedy můžeme dosáhnout $m \cdot n$ iterací. Celková složitost algoritmu je $\mathcal{O}(mn(m \log m + n))$.

Tato složitost lze zlepšit, pokud ušetříme třídění: pro $i = 1, ..., m$ hledáme první sloupec $j(i)$ takový, že $a_{i,j(i)} \neq 0$ nebo $a_{k,j(i)} \neq 0$ pro nějaké $k > i$. V prvním případně eliminujeme prvky pod $a_{i,j(i)}$; v druhém nejprve zaměníme i-tý a j-tý řádek a teprve potom eliminujeme. Složitost v tomto případě je $\mathcal{O}(n^2 m)$.

Pozorování 2.7. *Nechť* $(\mathbf{A}'|\mathbf{b}')$ *je matice soustavy v odstupňovaném tvaru. Pokud poslední sloupec* $\mathbf{b}'$ *obsahuje pivot, potom soustava nemá řešení.*

Definice 2.8. Pro matici soustavy $(\mathbf{A}'|\mathbf{b}')$ v odstupňovaném tvaru nazveme proměnné, jež odpovídají sloupcům s pivoty v $\mathbf{A}'$, bázovými proměnnými.[2] Ostatní proměnné se nazývají volné.

Věta 2.9 (Věta o jednoznačnosti řešení)**.** *Nechť* $(\mathbf{A}'|\mathbf{b}')$ *je rozšířená matice soustavy v odstupňovaném tvaru, kde sloupec* $\mathbf{b}'$ *neobsahuje pivot. Potom libovolné hodnoty volných proměnných lze doplnit jednoznačně hodnotami bázových proměnných na řešení celé soustavy* $\mathbf{A}'\mathbf{x} = \mathbf{b}'$.

Důkaz. Větu dokážeme indukcí pro $i = r, r-1, r-2, \ldots, 1$.

Nechť $x_{j(i)}$ je i-tá bázová proměnná a hodnoty následujících bázových proměnných a všech volných proměnných jsou dány. Potom i-tá rovnice soustavy zní:

$$0x_1 + 0x_2 + \cdots + 0x_{j(i)-1} + a'_{i,j(i)} x_{j(i)} + a'_{i,j(i)+1} x_{j(i)+1} + \cdots + a'_{in} x_n = b'_i \tag{1}$$

Nechť $\alpha = a'_{i,j(i)+1} x_{j(i)+1} + \cdots + a'_{in} x_n$. Hodnotu tohoto výrazu známe (viz předpoklady). Z rovnice 1 se potom stává lineární rovnice s jednou neznámou a nenulovým koeficientem a ta má jednoznačné řešení:

$$a'_{i,j(i)} x_{j(i)} + \alpha = b'_i$$

□

Důsledek 2.10. *Každé řešení soustavy lze získat zpětnou substitucí.*

[2] Bázové proměnné jsou tedy proměnné $x_{j(i)}$ pro $i = 1, \ldots, r$ (nenulové řádky).

Důkaz. Nechť $\mathbf{x} = (x_1, \ldots, x_n)^\top$ je libovolné řešení. Vezmeme z $\mathbf{x}$ hodnoty volných proměnných a zpětnou substitucí dopočítáme bázové proměnné. Díky jednoznačnosti musíme dostat zpět $\mathbf{x}$. □

Věta 2.11. *Pro každou matici* $\mathbf{A}$ *platí, že sloupce s pivoty libovolné matice v odstupňovaném tvaru, kterou lze z* $\mathbf{A}$ *získat elementárními úpravami, jsou určeny jednoznačně.*

Důkaz. Sporem. Předpokládejme, že $\mathbf{A}', \mathbf{A}'' \sim \mathbf{A}$ mají pivoty v různých sloupcích. Sestrojme rozšířené matice soustav $(\mathbf{A}|0)$, $(\mathbf{A}'|0)$ a $(\mathbf{A}''|0)$. Nechť dále bez újmy na obecnosti x_k je proměnná, která je v $(\mathbf{A}'|0)$ bázická a zároveň v $(\mathbf{A}''|0)$ volná, a všechny následující proměnné mají v obou soustavách stejný charakter.

Zafixujeme hodnoty volných proměnných x_j pro $j > k$, ale potom x_k je určena jednoznačně v $(\mathbf{A}'|0)$ a zároveň může mít libovolnou hodnotu v $(\mathbf{A}''|0)$. Spor, jelikož obě soustavy mají mít stejné množiny řešení. □

Definice 2.12. Hodnost matice $\mathbf{A}$ je rovna počtu pivotů v libovolné matici $\mathbf{A}'$ v odstupňovaném tvaru, kterou lze z $\mathbf{A}$ získat elementárními úpravami. Značí se $\mathrm{rank}(\mathbf{A})$.

Věta 2.13. *Soustava* $\mathbf{A}\mathbf{x} = \mathbf{b}$ *má alespoň jedno řešení, právě když platí* $\mathrm{rank}(\mathbf{A}) = \mathrm{rank}(\mathbf{A}|\mathbf{b})$.

Důkaz. Nechť má soustava alespoň jedno řešení a nechť $(\mathbf{A}|\mathbf{b}) \sim (\mathbf{A}'|\mathbf{b}')$. Potom

$$\begin{aligned} \mathrm{rank}(\mathbf{A}|\mathbf{b}) &= \mathrm{rank}(\mathbf{A}'|\mathbf{b}') && \text{(dle definice hodnosti)} \\ &= \mathrm{rank}(\mathbf{A}') && \text{(dle Pozorování 2.7)} \\ &= \mathrm{rank}(\mathbf{A}) && \text{(dle definice hodnosti)} \end{aligned}$$

Opačně, nechť platí $\mathrm{rank}(\mathbf{A}) = \mathrm{rank}(\mathbf{A}|\mathbf{b})$. Potom

$$\begin{aligned} \mathrm{rank}(\mathbf{A}'|\mathbf{b}') &= \mathrm{rank}(\mathbf{A}|\mathbf{b}) && \text{(dle definice hodnosti)} \\ &= \mathrm{rank}(\mathbf{A}) && \text{(předpoklad)} \\ &= \mathrm{rank}(\mathbf{A}'). && \text{(dle definice hodnosti)} \end{aligned}$$

Jelikož $\mathrm{rank}(\mathbf{A}'|\mathbf{b}') = \mathrm{rank}(\mathbf{A}')$, soustava $(\mathbf{A}'|\mathbf{b}')$ nemá pivot v posledním sloupci. Díky Větě 2.9 má tedy alespoň jedno řešení. □

Definice 2.14. Homogenní soustava lineárních rovnic je soustava tvaru $\mathbf{A}\mathbf{x} = \mathbf{0}$.

Pozorování 2.15. *Jsou-li* $\bar{\mathbf{x}}$ *a* $\mathbf{x}'$ *řešeními soustavy* $\mathbf{A}\mathbf{x} = \mathbf{b}$*, pak* $\bar{\mathbf{x}} - \mathbf{x}'$ *je řešením* $\mathbf{A}\mathbf{x} = \mathbf{0}$.

Důkaz. Podívejme se na i-tý řádek soustavy $\mathbf{A}\mathbf{x} = \mathbf{0}$ po dosazení $\bar{\mathbf{x}} - \mathbf{x}'$ za $\mathbf{x}$:

$$\begin{aligned} a_{i1}(\bar{x}_1 - x'_1) + \cdots + a_{in}(\bar{x}_n - x'_n) &= (a_{i1}\bar{x}_1 + \cdots + a_{in}\bar{x}_n) - (a_{i1}x'_1 + \cdots + a_{in}x'_n) \\ &= b_i - b_i = 0 \end{aligned}$$

□

Pozorování 2.16. *Jsou-li* $\bar{\mathbf{x}}$ *řešením* $\mathbf{Ax} = \mathbf{b}$ *a* $\mathbf{x}'$ *řešením* $\mathbf{Ax} = \mathbf{0}$, *pak* $\bar{\mathbf{x}} + \mathbf{x}'$ *je řešením* $\mathbf{Ax} = \mathbf{b}$.

Důkaz. Viz důkaz Pozorování 2.15. □

Věta 2.17. *Nechť* $\mathbf{A} \in \mathbb{R}^{m \times n}$ *je matice hodnosti* $r < n$. *Pak existují řešení* $\mathbf{h^1}, \mathbf{h^2}, \ldots, \mathbf{h^{n-r}}$ *soustavy* $\mathbf{Ax} = \mathbf{0}$ *taková, že každé řešení homogenní soustavy* $\mathbf{Ax} = \mathbf{0}$ *lze vyjádřit ve tvaru* $\mathbf{x} = p_1\mathbf{h^1} + p_2\mathbf{h^2} + \cdots + p_{n-r}\mathbf{h^{n-r}}$, *kde* $p_1, \ldots, p_{n-r}$ *jsou vhodná reálná čísla.*

Důkaz. Nechť $\mathbf{A}' \sim \mathbf{A}$ je v odstupňovaném tvaru. Všechny proměnné lze vyjádřit pomocí volných proměnných (indukcí podobně jako ve Větě 2.9). Tyto volné proměnné použijeme jako parametry $p_1, \ldots, p_{n-r}$. Řešení $\mathbf{h^1}, \ldots, \mathbf{h^{n-r}}$ jsou vektory koeficientů volných proměnných.

Mějmě například matici

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Proměnné x_1 a x_2 jsou bázové; proměnné x_3 a x_4 jsou volné. Vyjádříme všechny proměnné pomocí volných proměnných:

$$\begin{aligned} x_4 &= x_4 \\ x_3 &= x_3 \\ x_2 &= -2x_3 - 3x_4 \\ x_1 &= -2x_2 - 3x_3 - 4x_4 = 4x_3 + 6x_4 - 3x_3 - 4x_4 = x_3 + 2x_4 \end{aligned}$$

Řešení $\mathbf{h^1}$, odpovídající volné proměnné x_3, a řešení $\mathbf{h^2}$, odpovídající volné proměnné x_4, potom vyjádříme pomocí koeficientů volných proměnných:

$$\mathbf{h^1} = \begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix}; \mathbf{h^2} = \begin{pmatrix} 2 \\ -3 \\ 0 \\ 1 \end{pmatrix}$$

□

Důsledek 2.18. *Každé řešení řešitelné soustavy* $\mathbf{Ax} = \mathbf{b}$ *lze vyjádřit ve tvaru:*

$$\mathbf{x} = \mathbf{x^0} + p_1\mathbf{h}^1 + \cdots + p_{n-r}\mathbf{h}^{n-r},$$

kde $r = \mathrm{rank}(\mathbf{A})$, $\mathbf{h}^1, \ldots, \mathbf{h}^{n-r}$ *jsou řešeními homogenní soustavy* $\mathbf{Ax} = \mathbf{0}$, $p_1, \ldots, p_n$ *jsou vhodná reálná čísla a* $\mathbf{x}^0$ *je libovolné řešení* $\mathbf{Ax} = \mathbf{b}$.

Důkaz. Nechť $\bar{\mathbf{x}}$ je libovolné řešení soustavy $\mathbf{Ax} = \mathbf{b}$. Potom $\bar{\mathbf{x}} - \mathbf{x}^0$ je řešení $\mathbf{Ax} = \mathbf{0}$ a lze vyjádřit jako

$$(\bar{\mathbf{x}} - \mathbf{x}^0) = \sum_{i=1}^{n-r} p_i\mathbf{h}^i.$$

□

Definice 2.19. Matice v redukovaném odstupňovaném tvaru má všechny pivoty rovny 1 a ve sloupcích nad pivoty pouze nuly.

3 Operace s maticemi, speciální typy matic

Definice 3.1 (Terminologie, značení základních matic)**.**

- Nulová matice typu $m \times n$: $\mathbf{0}$, $\forall i, j (\mathbf{0})_{ij} = 0$.
- Jednotková matice řádu n je čtvercová matice $\mathbf{I_n}$ taková, že:

$$(\mathbf{I_n})_{i,j} = \begin{cases} 1, & \text{pokud } i = j. \\ 0, & \text{jinak.} \end{cases}$$

  Například:

$$\mathbf{I_3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- Hlavní diagonála čtvercové matice $\mathbf{A}$ je tvořena prvky $a_{i,i}$.

Definice 3.2. Transponovaná matice k matici $\mathbf{A}$ typu $m \times n$ je matice $\mathbf{A}^\top$ tupu $n \times m$ definovaná vztahem $\left(\mathbf{A}^\top\right)_{ij} = a_{ji}$. Čtvercová matice se nazývá symetrická, pokud splňuje $\mathbf{A}^\top = \mathbf{A}$.

Definice 3.3. Pro matice $\mathbf{A}$ a $\mathbf{B}$ stejného typu definujeme součet matic $\mathbf{A} + \mathbf{B}$ předpisem:

$$(\mathbf{A} + \mathbf{B})_{ij} = a_{ij} + b_{ij}.$$

Definice 3.4. Pro $\alpha \in \mathbb{R}$ a matici $\mathbf{A}$ definujeme α-násobek matice $\mathbf{A}$ předpisem:

$$(\alpha \mathbf{A})_{ij} = \alpha a_{ij}.$$

Nulový násobek libovolné matice je nulová matice.

Definice 3.5. Je-li $\mathbf{A}$ matice typu $m \times n$ a $\mathbf{B}$ matice typu $n \times p$, potom definujeme součin matic $\mathbf{A}$ a $\mathbf{B}$ jako matici $\mathbf{AB}$ typu $m \times p$, kde platí:

$$(\mathbf{AB})_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Poznámka 3.6 (Užití součinu)**.** Maticový součin má mnohá využití:

- Zápis soustav lineárních rovnic: $\mathbf{Ax} = \mathbf{b}$.
- Elementární úpravy lze vyjádřit součinem (viz podrobněji Poznámka 3.14 níže).
- Lineární zobrazení a výměna báze lze vyjádřit maticovým součinem (o tomto budeme mluvit podrobněji v kapitole 7).

Tvrzení 3.7. *Jsou-li výsledky operací definovány, pak platí:*

i. $(\mathbf{A}+\mathbf{B})+\mathbf{C}=\mathbf{A}+(\mathbf{B}+\mathbf{C})$

ii. $\mathbf{A}+\mathbf{0}=\mathbf{A}$

iii. $\mathbf{A}+\mathbf{B}=\mathbf{B}+\mathbf{A}$

iv. $\forall\mathbf{A}\exists!\mathbf{B}:\mathbf{A}+\mathbf{B}=\mathbf{0}$

v. $(\alpha\mathbf{A})^\top=\alpha\mathbf{A}^\top$

vi. $(\mathbf{A}^\top)^\top=\mathbf{A}$

vii. $\alpha(\beta\mathbf{A})=(\alpha\beta)\mathbf{A}$

viii. $(\alpha+\beta)\mathbf{A}=\alpha\mathbf{A}+\beta\mathbf{A}$

ix. $(\mathbf{A}+\mathbf{B})^\top=\mathbf{A}^\top+\mathbf{B}^\top$

Tvrzení 3.8. *Maticový součin není komutativní.*

Důkaz. Pokud matice nejsou čtvercové, důkaz je jednoduchý: Nechť $\mathbf{A}\in\mathbb{R}^{a\times b}$, $\mathbf{B}\in\mathbb{R}^{b\times c}$, a $a\neq c$. Potom součin $\mathbf{AB}$ je definován, kdežto součin $\mathbf{BA}$ definován není.

Pro dvě čtvercové matice $\mathbf{A}$ a $\mathbf{B}$ řádu 2 je

$$\mathbf{AB}=\begin{pmatrix}a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22}\\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22}\end{pmatrix}$$

a

$$\mathbf{BA}=\begin{pmatrix}b_{11}a_{11}+b_{12}a_{21} & b_{11}a_{12}+b_{12}a_{22}\\ b_{21}a_{11}+b_{22}a_{21} & b_{21}a_{12}+b_{22}a_{22}\end{pmatrix}.$$

Je zřejmé, že obecně $\mathbf{AB}\neq\mathbf{BA}$. □

Tvrzení 3.9. *Matice* $\mathbf{AA}^\top$ *je vždy symetrická.*

Důkaz. Nechť $\mathbf{A}\in\mathbb{R}^{m\times n}$. Dle definice součinu je matice $\mathbf{AA}^\top$ čtvercová matice typu $m\times m$. Dále:

$$(\mathbf{AA}^\top)_{ij}=\sum_{k=1}^{n}(\mathbf{A})_{ik}(\mathbf{A}^\top)_{kj}=\sum_{k=1}^{n}(\mathbf{A}^\top)_{ki}(\mathbf{A})_{jk}=(\mathbf{AA}^\top)_{ji}$$

. □

Tvrzení 3.10. *Nechť* $\mathbf{A}\in\mathbb{R}^{m\times n}$. *Potom platí:* $\mathbf{I_m A}=\mathbf{A}=\mathbf{AI_n}$.

Tvrzení 3.11. *Pro násobení blokových matic platí:*

$$\begin{pmatrix}\mathbf{A}_1 & \mathbf{A}_2\end{pmatrix}\cdot\begin{pmatrix}\mathbf{B}_1\\ \mathbf{B}_2\end{pmatrix}=\mathbf{A}_1\mathbf{B}_1+\mathbf{A}_2\mathbf{B}_2$$

$$\begin{pmatrix}\mathbf{A}_1 & \mathbf{A}_2\\ \mathbf{A}_3 & \mathbf{A}_4\end{pmatrix}\cdot\begin{pmatrix}\mathbf{B}_1 & \mathbf{B}_2\\ \mathbf{B}_3 & \mathbf{B}_4\end{pmatrix}=\left(\begin{array}{c|c}\mathbf{A}_1\mathbf{B}_1+\mathbf{A}_2\mathbf{B}_3 & \mathbf{A}_1\mathbf{B}_2+\mathbf{A}_2\mathbf{B}_4\\ \mathbf{A}_3\mathbf{B}_1+\mathbf{A}_4\mathbf{B}_3 & \mathbf{A}_3\mathbf{B}_2+\mathbf{A}_4\mathbf{B}_4\end{array}\right)$$

Tvrzení 3.12. *Pro matice* $\mathbf{A}$, $\mathbf{B}$ *a* $\mathbf{C}$ *platí:*

i. $(\mathbf{AB})^\top=\mathbf{B}^\top\mathbf{A}^\top$

ii. $(\mathbf{AB})\mathbf{C}=\mathbf{A}(\mathbf{BC})$

iii. $(\mathbf{A}+\mathbf{B})\mathbf{C}=\mathbf{AC}+\mathbf{BC}$

iv. $\mathbf{A}(\mathbf{B}+\mathbf{C})=\mathbf{AB}+\mathbf{AC}$

za předpokladu, že všechny výsledky operací jsou definovány.

Důkaz.

1. $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{B} \in \mathbb{R}^{n \times p}$.

$$((\mathbf{AB})^\top)_{ij} = (\mathbf{AB})_{ji} = \sum_{k=1}^{n} a_{jk}b_{ki} = \sum_{k=1}^{n} (\mathbf{A}^\top)_{kj}(\mathbf{B}^\top)_{ik} = \sum_{k=1}^{n} (\mathbf{B}^\top)_{ik}(\mathbf{A}^\top)_{kj} = (\mathbf{B}^\top \mathbf{A}^\top)_{ij}$$

2. $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{B} \in \mathbb{R}^{n \times p}$, $\mathbf{C} \in \mathbb{R}^{p \times q}$.

$$\begin{aligned} ((\mathbf{AB})\mathbf{C})_{ij} &= \sum_{k=1}^{p} (\mathbf{AB})_{ik} \mathbf{C}_{kj} = \sum_{k=1}^{p} \left(\sum_{l=1}^{n} a_{il} b_{lk} \right) \cdot c_{kj} = \sum_{k=1}^{p} \sum_{l=1}^{n} a_{il} b_{lk} c_{kj} \\ &= \sum_{l=1}^{n} \sum_{k=1}^{p} a_{il} b_{lk} c_{kj} = \sum_{l=1}^{n} a_{il} \cdot \left(\sum_{k=1}^{p} b_{lk} c_{kj} \right) = \sum_{l=1}^{n} a_{il} \cdot (\mathbf{BC})_{lj} = (\mathbf{A}(\mathbf{BC}))_{ij} \end{aligned}$$

3. $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{B} \in \mathbb{R}^{n \times p}$, $\mathbf{C} \in \mathbb{R}^{p \times q}$.

$$\begin{aligned} ((\mathbf{A}+\mathbf{B})\mathbf{C})_{ij} &= \sum_{k=1}^{n} (\mathbf{A}+\mathbf{B})_{ik} \cdot c_{kj} = \sum_{k=1}^{n} (a_{ik} + b_{ik}) \cdot c_{kj} = \sum_{k=1}^{n} (a_{ik}c_{kj} + b_{ik}c_{kj}) \\ &= \sum_{k=1}^{n} a_{ik}c_{kj} + \sum_{k=1}^{n} b_{ik}c_{kj} = (\mathbf{AC})_{ij} + (\mathbf{BC})_{ij} = (\mathbf{AC} + \mathbf{BC})_{ij} \end{aligned}$$

4. Obdobně.

□

Poznámka 3.13 (Složitost násobení matic)**.** Nechť $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{B} \in \mathbb{R}^{n \times p}$, $\mathbf{C} \in \mathbb{R}^{p \times q}$. Potom:

- Na součin $\mathbf{AB}$ je třeba mnp operací, $(\mathbf{AB})\mathbf{C}$ mpq operací. Celkem: $mp(n+q)$.
- Na součin $\mathbf{BC}$ je třeba npq operací, $\mathbf{A}(\mathbf{BC})$ mnq operací. Celkem: $nq(p+m)$.

Pokud $q << m, n, p$, tak poté $nq(m+p) << mp(n+q)$.

Poznámka 3.14 (Elementární úpravy jako součin matic)**.** Nechť $\mathbf{B}$ vznikne z $\mathbf{A} \in \mathbb{R}^{m \times n}$ vynásobením i-tého řádku číslem t. Potom platí $\mathbf{B} = \mathbf{EA}$, kde:

$$(\mathbf{E})_{kj} = \begin{cases} t & \text{pokud } k = j \text{ a } k = i; \\ 1 & \text{pokud } k = j \text{ a } k \neq i; \\ 0 & \text{pokud } k \neq j. \end{cases}$$

Jedná se tedy o jednotkovou matici řádu m, kde na i-tém řádku byla jednička na diagonále nahrazena číslem t.

Nechť naopak $\mathbf{B}$ vznikne z $\mathbf{A} \in \mathbb{R}^{m\times n}$ přičtením j-tého řádku k i-tému. Potom platí: $\mathbf{B} = \mathbf{EA}$, kde:

$$(\mathbf{E})_{kl} = \begin{cases} 1 & \text{pokud } k = i \text{ a } l = j; \\ 1 & \text{pokud } k = l; \\ 0 & \text{jinak.} \end{cases}$$

Mějme například matici $\mathbf{A} \in \mathbb{R}^{3\times 4}$. Přičtení třetího řádku k prvnímu lze vyjádřit jako maticový součin $\mathbf{EA}$, kde:

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

Definice 3.15. Nechť $\mathbf{A}$ je čtvercová matice řádu n. Pokud existuje matice $\mathbf{B}$ taková, že $\mathbf{AB} = \mathbf{I_n}$, potom se $\mathbf{B}$ nazývá inverzní maticí k matici $\mathbf{A}$ a značí se $\mathbf{A^{-1}}$.

Pokud k matici $\mathbf{A}$ existuje inverzní matice, potom se $\mathbf{A}$ nazývá regulární, v opačném případě se nazývá singulární.

Věta 3.16. *Pro čtvercovou matici $\mathbf{A}$ řádu n jsou následující podmínky ekvivalentní:*

1. *Matice $\mathbf{A}$ je regulární (t.j. $\exists \mathbf{B} : \mathbf{AB} = \mathbf{I_n}$).*
2. $\operatorname{rank}(\mathbf{A}) = n$.
3. *Matici $\mathbf{A}$ lze řádkovými elementárními úpravami převést na $\mathbf{I_n}$.*
4. *Homogenní soustava $\mathbf{Ax} = \mathbf{0}$ má pouze triviální řešení $\mathbf{x} = \mathbf{0}$.*

Důkaz.

- $3 \implies 2$

  $\mathbf{I_n}$ je v odstupňovaném tvaru s n pivoty, tudíž $\operatorname{rank}(\mathbf{I_n}) = 0$.

- $2 \implies 3$

  Převedeme $\mathbf{A}$ na odstupňovaný tvar. Jelikož matice $\mathbf{A}$ je čtvercová a $\operatorname{rank}(\mathbf{A}) = n$, máme v každém sloupci pivot. S pomocí posledního pivotu zeliminuji vše, co je nad ním, přejdu k předposlednímu pivotu, opakuji, atp.

- $2 \iff 4$

  $4 \iff$ matice $\mathbf{A}$ po převedení do odstupňovaného tvaru nemá žádné volné proměnné $\iff$ 2

- $2 \implies 1$

Označme $\mathbf{e^1}, \mathbf{e^2}, \ldots, \mathbf{e^n}$ sloupce jednotkové matice. Vyřešíme n soustav tvaru $\mathbf{Ax^i} = \mathbf{e^i}$ pro $i = 1, \ldots, n$. Jelikož $\operatorname{rank}(\mathbf{A}) = n$, každá soustava má právě jedno řešení $\mathbf{x^i}$. Nechť:

$$\mathbf{B} = \begin{pmatrix} \vdots & \vdots & \ldots & \vdots \\ \mathbf{x^1} & \mathbf{x^2} & \ldots & \mathbf{x^n} \\ \vdots & \vdots & \ldots & \vdots \end{pmatrix}$$

Potom $\mathbf{AB} = \mathbf{I_n}$.

- $1 \implies 2$

  Sporem. Nechť matice $\mathbf{A}$ je regulární a $\operatorname{rank}(\mathbf{A}) < n$. Potom existuje řádek i, který lze vynulovat přičtením vhodné kombinace ostatních řádků. Matice $(\mathbf{A}|\mathbf{e^i})$ je rozšířená matice soustavy $\mathbf{Ax^i} = \mathbf{e^i}$. Elementárními úpravami lze i-tý řádek této matice upravit na

  $$\begin{pmatrix} 0 & 0 & \ldots & 0 & | & 1 \end{pmatrix}.$$

  Tato soustava ovšem nemá řešení a tudíž inverzní matice $\mathbf{B}$ neexistuje a matice $\mathbf{A}$ není regulární.

□

Důsledek 3.17. *Pokud inverzní matice existuje, je určena jednoznačně.*

Tvrzení 3.18. *Pro regulární matici* $\mathbf{A}$ *platí:*

$$\mathbf{A^{-1}A} = \mathbf{AA^{-1}} = \mathbf{I_n}$$

Důkaz. Nejprve sporem ukážeme, že $\mathbf{A^{-1}}$ je regulární. Nechť $\mathbf{A^{-1}x} = \mathbf{0}$ má netriviální řešení $\mathbf{x}$. Potom:

$$\mathbf{x} = \mathbf{I_n x} = \mathbf{AA^{-1}x} = \mathbf{A0} = \mathbf{0}.$$

Tudíž existuje inverzní matice k matici $\mathbf{A^{-1}}$; označme ji $(\mathbf{A^{-1}})^{-1}$. Dále platí:

$$\mathbf{A^{-1}A} = \mathbf{A^{-1}AI_n} = \mathbf{A^{-1}AA^{-1}}(\mathbf{A^{-1}})^{-1} = \mathbf{A^{-1}I_n}(\mathbf{A^{-1}})^{-1} = \mathbf{A^{-1}}(\mathbf{A^{-1}})^{-1} = \mathbf{I_n}.$$

□

Poznámka 3.19 (Výpočet inverzní matice k dané čtvercové matici $\mathbf{A}$)**.**

1. Sestavíme $(\mathbf{A}|\mathbf{I_n})$ a elementárními řádkovými úpravami ji převedeme na tvar $(\mathbf{I_n}|\mathbf{B})$. Pokud tento postup selže, matice $\mathbf{A}$ je singulární.

2. Označme $\mathbf{E_1}, \mathbf{E_2}, \ldots, \mathbf{E_k}$ matice, které byly použity v těchto řádkových úpravách:

   $$\mathbf{E_k E_{k-1}} \ldots \mathbf{E_1} (\mathbf{A}|\mathbf{I_n}) = (\mathbf{I_n}|\mathbf{B}).$$

   Potom $\mathbf{E_k E_{k-1}} \ldots \mathbf{E_1 A} = \mathbf{I_n}$ a $\mathbf{E_k E_{k-1}} \ldots \mathbf{E_1 I_n} = \mathbf{B}$. Z toho vyplývá, že $\mathbf{BA} = \mathbf{I_n}$ a $\mathbf{B} = \mathbf{A^{-1}}$.

Pozorování 3.20. *Je-li matice* $\mathbf{R}$ *regulární, potom:*

$$\mathbf{A} = \mathbf{B} \iff \mathbf{AR} = \mathbf{BR}.$$

Důkaz.

- $\implies$: Triviální.
- $\impliedby$: $\mathbf{A} = \mathbf{AI_n} = \mathbf{ARR^{-1}} = \mathbf{BRR^{-1}} = \mathbf{BI_n} = \mathbf{B}$

$\square$

Tvrzení 3.21. *Pro regulární matice* $\mathbf{A}$ *a* $\mathbf{B}$ *stejného řádu platí:*

- $(\mathbf{A^{-1}})^{\mathbf{-1}} = \mathbf{A}$
- $\mathbf{AB}$ *je regulární.*
- $(\mathbf{AB})^{\mathbf{-1}} = \mathbf{B^{-1}A^{-1}}$
- $(\mathbf{A}^\top)^{\mathbf{-1}} = (\mathbf{A^{-1}})^\top$

Poznámka 3.22 (Řešení maticových rovnic)**.**

- $\mathbf{A} + \mathbf{X} = \mathbf{B} \implies \mathbf{X} = \mathbf{B} - \mathbf{A} = \mathbf{B} + (-1)\mathbf{A}$
- $\alpha\mathbf{X} = \mathbf{B} \implies \mathbf{X} = \frac{1}{\alpha}\mathbf{B}$
- $\mathbf{AX} = \mathbf{B} \implies \mathbf{X} = \mathbf{A^{-1}B}$, je-li $\mathbf{A}$ regulární.
- $\mathbf{XA} = \mathbf{B} \implies \mathbf{X} = \mathbf{BA^{-1}}$, je-li $\mathbf{A}$ regulární.

4 Algebraická tělesa

Definice 4.1. Binární operací na množině K rozumíme zorazení $K \times K \to K$.

Poznámka 4.2. Příklady binárních operací na $\mathbb{N}$:

i. $\varphi(a, b) = a + b$

ii. $\varphi(a, b) = \min\{a; b\}$

iii. $\varphi(a, b) = a + 18$

Naopak zobrazení $\varphi(a, b) = a+b-18$ binární operací na $\mathbb{N}$ není, jelikož výsledek této operace může být záporný.

Binární operaci můžeme definovat i tabulkou, např. na množině $\{0; 1\}$:

$a \backslash b$	0	1
0	0	1
1	0	0

Toto zobrazení odpovídá logické funkci $\varphi(a, b) = \neg a \wedge b$.

Binární zobrazení lze definovat např. i na reálných polynomech jedné proměnné: $\varphi(p(x), q(x)) = (p + q)(x)$.

Definice 4.3. Nechť K je množina a $+, \cdot$ jsou dvě binární operace na K. Strukturu $(K, +, \cdot)$ nazveme tělesem, pokud jsou splněny následující axiomy:

(SA) $\forall a, b, c \in K : (a + b) + c = a + (b + c)$ (sčítání je asociativní)

(SK) $\forall a, b \in K : a + b = b + a$ (sčítání je komutativní)

(S0) $\exists 0 \in K : \forall a \in K : a + 0 = a$ (existence nulového prvku)

(SI) $\forall a \in K : \exists -a \in K : a + (-a) = 0$ (existence opačného prvku)

(NA) $\forall a, b, c \in K : (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(NK) $\forall a, b \in K : a \cdot b = b \cdot a$

(N1) $\exists 1 \in K : \forall a \in K : a \cdot 1 = a$

(NI) $\forall a \in K \setminus \{0\} : \exists a^{-1} \in K : a \cdot a^{-1} = 1$ (existence inverzního prvku)

(D) $\forall a, b, c \in K : a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivita násobení vůči sčítání)

(01) $0 \neq 1$ (axiom netriviality)

Poznámka 4.4 (Značení)**.**

- $ab \coloneqq a \cdot b$
- $a - b \coloneqq a + (-b)$
- $\frac{a}{b} \coloneqq a \cdot b^{-1}$

Poznámka 4.5 (Příklady těles)**.**

i. $(\mathbb{Q}, +, \cdot)$

ii. $(\mathbb{R}, +, \cdot)$

iii. $(\mathbb{C}, +, \cdot)$

iv. $(\mathbb{Z}_p, +, \cdot)$, t.j. počítání ve zbytkových třídách modulo prvočíslo

v. (racionální lomené funkce, $+, \cdot$)

Poznámka 4.6 (Příklady struktur, jež nejsou tělesa)**.**

i. $(\mathbb{N}, +, \cdot)$

ii. $(\mathbb{Z}, +, \cdot)$

iii. $(\mathbb{Z}_4, +, \cdot)$, $(\mathbb{Z}_6, +, \cdot)$[3]

iv. $(\mathbb{R}^n, +, \cdot)$

v. (polynomy, $+, \cdot$)

Metatvrzení 4.7. *Všechny definice a věty o řešení soustav a počítání s maticemi nad $\mathbb{R}$ platí také pro soustavy a matice nad libovolným tělesem, jelikož z $\mathbb{R}$ jsme využili pouze vlastnosti dané axiomy tělesa.*

Pozorování 4.8. *Prvky $0, -a, 1, a^{-1}$ jsou vždy určeny jednoznačně.*

Důkaz. Jednoznačnost 0 dokážeme sporem. Nechť $0, \bar{0}$ jsou dva různé neutrální prvky $0 \neq \bar{0}$. Potom:

$$\begin{aligned} 0 &= 0 + \bar{0} && \text{(S0)} \\ &= \bar{0} + 0 && \text{(SK)} \\ &= \bar{0} && \text{(S0)} \end{aligned}$$

Jednoznačnost $-a$ dokážeme taktéž sporem. Nechť $-a$ a $\overline{-a}$ jsou opačné prvky k a a $-a \neq \overline{-a}$:

$$\begin{aligned} -a &= -a + 0 && \text{(S0)} \\ &= -a + (a + (\overline{-a})) && \text{(SI)} \\ &= \overline{-a} + (a + (-a)) && \text{(SK, SA)} \\ &= \overline{-a} + 0 = \overline{-a} && \text{(SI, S0)} \end{aligned}$$

Zbytek analogicky. □

Pozorování 4.9. *Nechť K je algebraické těleso. Potom:*

i. $\forall a \in K : -(-a) = a$

ii. $\forall b \in K \setminus \{0\} : (b^{-1})^{-1} = b$

[3] Důvody viz Tvrzení 4.14

Důkaz.

i. $-(-a) = -(-a) + 0 = -(-a) + (a + (-a)) = a + (-a + -(-a)) = a + 0 = a$

ii. $(b^{-1})^{-1} = (b^{-1})^{-1} \cdot 1 = (b^{-1})^{-1} \cdot (b \cdot b^{-1}) = ((b^{-1})^{-1} \cdot b^{-1}) \cdot b = 1 \cdot b = b$

□

Pozorování 4.10. *Nechť K je algebraické těleso. Potom:*

i. $\forall a \in K : a \cdot 0 = 0$

ii. $\forall a \in K \setminus \{0\} : a \cdot (-1) = -a$

Důkaz.

i. $a \cdot 0 = a \cdot 0 + 0 = a \cdot 0 + (a \cdot 0 - a \cdot 0) = (a \cdot 0 + a \cdot 0) - a \cdot 0 = a \cdot (0 + 0) - a \cdot 0 = a \cdot 0 - a \cdot 0 = 0$

ii. $a \cdot (-1) = a \cdot (-1) + 0 = a \cdot (-1) + a - a = a \cdot (-1) + a \cdot 1 - a = a \cdot (-1 + 1) - a = a \cdot 0 - a = -a$

□

Pozorování 4.11. *Pokud $a \cdot b = 0$, potom buď $a = 0$ nebo $b = 0$.*

Důkaz. Sporem. Nechť $a \neq 0$ a $b \neq 0$. Potom existují opačné prvky a^{-1} a b^{-1}. Dále: $0 = b^{-1} \cdot a^{-1} \cdot 0 = b^{-1} \cdot a^{-1} \cdot a \cdot b = b^{-1} \cdot 1 \cdot b = b^{-1} \cdot b = 1$. □

Pozorování 4.12. $\forall a, b, a', b', a' \neq 0 : a + x = b$ *a* $a' \cdot x = b'$ *mají právě jedno řešení.*

Důkaz. Sporem. Nechť x_1 a x_2 jsou dvě různá řešení rovnice $a + x = b$. Potom:

$$x_1 = x_1 + 0 = x_1 + a - a = (x_1 + a) - a = b - a = (a + x_2) - a = x_2.$$

Podobně, nechť x_1 a x_2 jsou dvě různá řešení rovnice $a' \cdot x = b'$. Potom:

$$x_1 = x_1 \cdot 1 = x_1 \cdot a \cdot a^{-1} = b \cdot a^{-1} = a \cdot x_2 \cdot a^{-1} = x_2.$$

□

Pozorování 4.13.

i. $\forall a, b, c : a + b = a + c \iff b = c$

ii. $\forall a \neq 0, b, c : a \cdot b = a \cdot c \iff b = c$

Tvrzení 4.14. *Struktura $\mathbb{Z}_p$ je těleso, právě když p je prvočíslo.*

Důkaz.

- $\implies$: Nepřímo. p je složené, t.j. $\exists a, b : p = a \cdot b$. Potom v $\mathbb{Z}_p$ neplatí Pozorování 4.11.

- $\Longleftarrow$: Předpokládáme, že p je prvočíslo. Potom musíme ověřit všech 10 axiomů. Jediný obtížný axiom je existence opačného prvku (NI): $\forall a \neq 0 \exists a^{-1} : a \cdot a^{-1} = 1$, t.j. $a \cdot a^{-1} = 1 \mod p$.

  $\forall a$ definujeme zobrazení $f_a : \{1, 2, \dots, p-1\} \to \{1, 2, \dots, p-1\}$ takové, že:

  $$f_a(x) = a \cdot x \mod p.$$

  Potřebujeme ukázat, že zobrazení f_a je prosté. Poté už vyplyne, že je zároveň i na a tedy, že $\exists x : f_a(x) = 1$ čili $x = a^{-1}$.

  Důkaz provedeme sporem. Kdyby f_a nebylo prosté, potom $\exists x' \neq x'' : f_a(x') = f_a(x'')$, tedy $ax' \equiv ax'' \mod p$, čili $a \cdot (x' - x'') \equiv 0 \mod p$.

□

Věta 4.15. *Konečné těleso s n prvky existuje, právě když n je mocnina prvočísla.*

Poznámka 4.16. Konečné těleso s n prvky se značí $GF(n)$ (z anglického "Galois Field").

Definice 4.17. Pokud $\exists k \in \mathbb{N}$ takové, že v tělese K platí:

$$\underbrace{1 + 1 + \cdots + 1}_{k} = 0$$

tak potom nejmenší takové k se nazývá charakteristika tělesa K. Pokud takové k neexistuje, říkáme, že těleso K má charakteristiku 0.

Věta 4.18. *Charakteristika tělesa je vždy 0 nebo prvočíslo.*

Důkaz. Sporem. Nechť k je složené, t.j. $\exists a, b : k = a \cdot b$. Potom

$$0 = \underbrace{1 + 1 + \cdots + 1}_{k} = \underbrace{(1 + \cdots + 1)}_{a} \cdot \underbrace{(1 + \cdots + 1)}_{b} = x \cdot y,$$

což je spor, jelikož $x \neq 0$ a $y \neq 0$. □

5 Vektorové prostory

Definice 5.1. Nechť $(k, +, \cdot)$ je těleso. Množinu V spolu s binární operací $+$ na V a zobrazením $\cdot : k \times V \to V$ se nazývá vektorový prostor $(V, +, \cdot)$ nad k, pokud platí následující axiomy:

(SA) $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V : (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ (sčítání je asociativní)

(SK) $\forall \mathbf{u}, \mathbf{v} \in V : \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ (sčítání je komutativní)

(S0) $\exists \mathbf{0} \in V, \forall \mathbf{u} \in V : \mathbf{u} + \mathbf{0} = \mathbf{u}$ (existence nulového prvku)

(SI) $\forall \mathbf{u} \in V, \exists -\mathbf{u} \in V : \mathbf{u} + (-\mathbf{u}) = \mathbf{0}$ (existence opačného prvku)

(NA) $\forall a, b \in k, \forall \mathbf{u} \in V a \cdot (b \cdot \mathbf{u}) = (a \cdot b) \cdot \mathbf{u}$ (násobení vektoru je asociativní)

(N1) $\forall \mathbf{n} \in V : 1 \cdot \mathbf{n} = \mathbf{n}$, kde 1 je jednotkový prvek tělesa k (invariance vektoru při násobení jednotkovým prvkem tělesa)

(D1) $\forall a, b \in k, \forall \mathbf{u} \in V : (a + b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$ (distributivita násobení vektoru vzhledem ke sčítání prvků tělesa)

(D2) $\forall a \in k, \forall \mathbf{u}, \mathbf{v} \in V : a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ (distributivita násobení vektoru vzhledem ke sčítání vektorů)

Poznámka 5.2. Ingredience vektorového prostoru:

i. Těleso k s operacemi $+$ a $\cdot$. Jeho prvky se nazývají skaláry.

ii. Prostor V s operací $+$[4]. Jeho prvky se nazývají vektory.

iii. Operace $\cdot$ "mezi k a V".

Poznámka 5.3 (Příklady vektorových prostorů)**.**

i. $V = \{0\}$. Triviální vektorový prostor nad libovolným tělesem k.

ii. K^n. Aritmetický vektorový prostor dimenze n. Vektory jsou uspořádané n-tice prvků z K. Operace $+$ a $\cdot$ se provádějí po složkách. Z každého tělesa lze vybudovat vektorový prostor téže velikosti K^1.

iii. Matice typu $m \times n$ nad K.

iv. Polynomy omezeného stupně.

v. Spojité funkce, diferencovatelné funkce v $\mathbb{R}$.

[4] Operace $+$ na V je odlišná od operace $+$ na k. Obě se nicméně značí obvykle stejně.

vi. Systém podmožin nějaké množiny X jako prostor nad $\mathbb{Z}_2$.

Tvrzení 5.4. *Prvky* $\mathbf{0}$ *a* $-\mathbf{a}$ *jsou určeny jednoznačně.*

Důkaz. Důkaz je stejný jako pro skaláry. □

Tvrzení 5.5. $\forall \mathbf{u} \in V, \forall a \in K : 0 \cdot \mathbf{u} = a \cdot \mathbf{0} = \mathbf{0}$

Důkaz.

$$0\mathbf{u} = 0\mathbf{u} + 0 = 0\mathbf{u} + 0\mathbf{u} - 0\mathbf{u} = (0+0)\mathbf{u} - 0\mathbf{u} = 0\mathbf{u} - 0\mathbf{u} = \mathbf{0}$$
$$a\mathbf{0} = a\mathbf{0} + \mathbf{0} = a\mathbf{0} + a\mathbf{0} - a\mathbf{0} = a(\mathbf{0}+\mathbf{0}) - a\mathbf{0} = a\mathbf{0} - a\mathbf{0} = \mathbf{0}$$

□

Tvrzení 5.6. *Pokud* $a \cdot \mathbf{u} = \mathbf{0}$*, potom* $a = 0$ *nebo* $\mathbf{u} = \mathbf{0}$*.*

Důkaz. Sporem. Nechť $a \neq 0$ a $\mathbf{u} \neq \mathbf{0}$.

$$\mathbf{0} \neq \mathbf{u} = 1 \cdot \mathbf{u} = a^{-1} \cdot a \cdot \mathbf{u} = a^{-1} \cdot \mathbf{0} = \mathbf{0}$$

□

Definice 5.7. Nechť $(V, +, \cdot)$ je vektorový prostor nad tělesem K a U je neprázdná podmnožinu V taková, že:

i. $\forall \mathbf{u}, \mathbf{v} \in U : \mathbf{u} + \mathbf{v} \in U$

ii. $\forall \mathbf{u} \in V, \forall a \in K : a \cdot \mathbf{u} \in U$.

Potom $(U, +, \cdot)$ nazýváme podprostorem V.

Poznámka 5.8. Množinu U splňující výše uvedené podmínky nazýváme uzavřenou na operace $+$ a $\cdot$.

Pozorování 5.9. *Podprostor* $(U, +, \cdot)$ *vektorového prostoru* V *je vektorový prostor.*

Důkaz. Je třeba ověřit všech 8 axiomů z definice vektorového prostoru. Existence nulového a opačného prvku plyne z uzavřenosti U vůči operaci $\cdot$ $(0 \cdot \mathbf{a} = \mathbf{0}, -1 \cdot \mathbf{a} = -\mathbf{a})$. □

Poznámka 5.10 (Příklady podprostorů $\mathbb{R}^3$)**.**

- rovina π procházející počátkem
- přímka p procházející počátkem
- bod $\{0\}$

Tvrzení 5.11. *Nechť* $(U_i, i \in I)$ *je systém podprostorů nějakého vektorového prostoru* V*. Potom průnik těchto podprostorů, t.j.* $\cap_{i \in I} U_i$*, je podprostorem* V*.*

Důkaz. Je třeba ukázat uzavřenost W na $+$ a $\cdot$.

Označme $W \coloneqq \cap_{i \in I} U_i$. Potom:

- uzavřenost na $+$: $u, v \in W \Rightarrow \mathbf{u}, \mathbf{v} \in \cap_{i \in I} U_i \Rightarrow \forall i \in I : \mathbf{u}, \mathbf{v} \in U_i \Rightarrow \forall i \in I : \mathbf{u} + \mathbf{v} \in U_i \Rightarrow \mathbf{u} + \mathbf{v} \in \cap_{i \in I} U_i = W$
- uzavřenost na $\cdot$: $a \in K, \mathbf{u} \in W \Rightarrow \forall i \in I : \mathbf{u} \in U_i \Rightarrow \forall i \in I : a \cdot \mathbf{u} \in U_i \Rightarrow a \cdot \mathbf{u} \in \cap_{i \in I} U_i = W$

□

Definice 5.12. Nechť V je vektorový prostopr nad K a X je podmnožina V. Potom $\mathrm{span}(X)$ značí podprostor generovaný X (či lineární obal množiny X), což je průnik všech podprostorů V, které obsahují X. Formálně:

$$\mathrm{span}(X) \coloneqq \cap \{U | X \subseteq U, U \text{ podprostor } V\}.$$

Tvrzení 5.13. *Nechť V je vektorový prostor nad K a $X \subseteq V$. Potom* $\mathrm{span}(X)$ *obsahuje všechny lineární kombinace vektorů z X, neboli*

$$\mathrm{span}(X) = \{\mathbf{u} | \mathbf{u} = \sum_{i=1}^{n} a_i \mathbf{x_i}, n \geq 0, \forall i = 1, \ldots, n : a_i \in K, \mathbf{x_i} \in X\}$$

Důkaz. Definujme:

$$W_1 \coloneqq \cap_{X \subseteq U \subseteq V} U$$
$$W_2 \coloneqq \left\{ \sum_{i=1}^{n} a_i \mathbf{x_i}, a_i \in K, \mathbf{x_i} \in X \right\}$$

Nejprve ukážeme, že množina W_2 je podprostorem V, t.j. že je uzavřená na $+$ a $\cdot$.

- Uzavřenost na $+$. Nechť $\mathbf{u}, \mathbf{v} \in W_2$. Potom:

$$\mathbf{u} = \sum_{i=1}^{k} a_i \mathbf{x_i}, a_i \in K, \mathbf{x_i} \in X$$

$$\mathbf{v} = \sum_{i=1}^{l} a'_i \mathbf{x'_i}, a'_i \in K, \mathbf{x'_i} \in X$$

Označme $\{\mathbf{y_1}, \ldots, \mathbf{y_n}\} = \{\mathbf{x_1}, \ldots, \mathbf{x_k}\} \cup \{\mathbf{x'_1}, \ldots, \mathbf{x'_l}\}$. Po přeznačení a doplnění koeficientů lze vyjádřit:

$$\mathbf{u} = \sum_{i=1}^{n} b_i \mathbf{y_i}$$

$$\mathbf{v} = \sum_{i=1}^{n} b'_i \mathbf{y_i}$$

Potom

$$\mathbf{u} + \mathbf{v} = \sum_{i=1}^{n} b_i \mathbf{y_i} + \sum_{i=1}^{n} b'_i \mathbf{y_i} = \sum_{i=1}^{n} (b_i + b'_i) \mathbf{y_i}$$

a $\mathbf{u} + \mathbf{v} \in W_2$ z definice W_2.

- Uzavřenost na $\cdot$. Nechť $\mathbf{u} \in W_2, c \in K$.

$$c \cdot \mathbf{u} = c \cdot \sum_{i=1}^{k} a_i \mathbf{x_i} = \sum_{i=1}^{k} \underbrace{(ca_i)}_{\in K} \underbrace{\mathbf{x_i}}_{\in X} \in W_2$$

Nyní $W_1 \subseteq W_2$, protože W_2 lze vzít za nějaké U_i, přes které děláme průniky, jelikož obsahuje X a je podprostorem V. Dále také $W_2 \subseteq W_1$, protože každé U_i musí být uzavřené na $+$ a $\cdot$, a tedy $\forall i : W_2 \subseteq U_i \implies W_2 \subseteq \cap U_i = W_1$. Z tohoto plyne $W_1 = W_2$. $\square$

Definice 5.14 (Prostory určené maticí)**.** Nechť $\mathbf{A}$ je matice typu $m \times n$ nad tělesem K.

- Sloupcový prostor $S(\mathbf{A})$ je podprostor $\mathbb{K}^m$ generovaný sloupci matice $\mathbf{A}$. Formálně: $S(\mathbf{A}) = \{\mathbf{u} \in \mathbb{K}^m, \mathbf{u} = \mathbf{A}\mathbf{x}, \mathbf{x} \in \mathbb{K}^n\}$.
- Řádkový prostor $R(\mathbf{A})$ je podprostor $\mathbb{K}^n$ generovaný řádky matice $\mathbf{A}$. Formálně: $R(\mathbf{A}) = \{\mathbf{v} \in \mathbb{K}^n, \mathbf{v} = \mathbf{A}^\top \mathbf{y}, \mathbf{y} \in \mathbb{K}^m\}$.
- Jádro matice $Ker(\mathbf{A})$ je podprostor $\mathbb{K}^n$ tvořený všemi řešeními homogenní soustavy $\mathbf{A}\mathbf{x} = \mathbf{0}$.

Pozorování 5.15. *Elementární úpravy nemění $R(A)$ ani $Ker(A)$.*

Pozorování 5.16. *Nechť $\mathbf{x} \in Ker(A)$ a $\mathbf{v} \in R(A)$. Potom $\mathbf{v}^\top \mathbf{x} = 0$.*

Důkaz. $\mathbf{v}^\top \mathbf{x} = (\mathbf{A}^\top \mathbf{y})^\top \mathbf{x} = \mathbf{y}^\top \mathbf{A}\mathbf{x} = \mathbf{y}^\top \cdot \mathbf{0} = 0$ $\square$

6 Lineární nezávislost

Definice 6.1. Nechť V je vektorový prostor nad tělesem K. Daná n-tice vektorů $\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n} \in V$ je lineárně nezávislá, pokud rovnice:

$$a_1 \cdot \mathbf{v_1} + a_2 \cdot \mathbf{v_2} + \cdots + a_n \cdot \mathbf{v_n} = \mathbf{0}$$

má pouze triviální řešení $a_1 = a_2 = \cdots = a_n = 0$. V opačném případě je daná n-tice vektorů lineárně závislá.

Poznámka 6.2 (Poznámky k definici lineární nezávislosti)**.**

- Na pořadí vektorů nezáleží.
- Pokud $\exists i \neq j : \mathbf{v_i} = \mathbf{v_j}$, potom je daná n-tice vektorů lineárně závislá.
- Pokud $\exists i : \mathbf{v_i} = \mathbf{0}$, potom je daná n-tice vektorů lineárně závislá.
- Rozšířená definice: Nekonečná množina je lineárně nezávislá, pokud všechny její konečné podmnožiny jsou lineárně nezávislé.
- Co znamená, že daná n-tice vektorů je lineárně závislá? Alespoň jeden vektor $\mathbf{v_i}$ lze vyjádřit jako lineární kombinace ostatních vektorů (nikoliv nutně všech).

Poznámka 6.3 (Příklady lineární (ne)závislosti)**.**

- Nechť $X \subseteq \mathbb{R}^2$ a $X \neq \emptyset$.
  - $X = \{\mathbf{x}\}$. Lineárně závislá, pouze když $\mathbf{x}$ je počátek; jinak lineárně nezávislá.
  - $X = \{\mathbf{x}, \mathbf{y}\}$. Pokud $\mathbf{0} \in X$, tak X je lineárně závislá. Podobně, leží-li $\mathbf{x}$ a $\mathbf{y}$ na přímce procházející počátkem. V ostatních případech je X lineárně nezávislá.
- Řádky nebo sloupce jednotkové nebo regulární matice jsou lineárně nezávislé.
- Nenulové řádky matice v odstupňovaném tvaru jsou lineárně nezávislé.
- Nechť je V prostor polynomů nad $\mathbb{R}$. Potom $X = \{x^0, x^1, \dots, x^n, \dots\}$ je lineárně nezávislá.

Pozorování 6.4.

i. Nechť X je lineárně nezávislá a $Y \subseteq X$. Potom Y je také lineárně nezávislá.

ii. Nechť X je lineárně závislá a $X \subseteq Y$. Potom Y je také lineárně závislá.

Pozorování 6.5. *X je lineárně nezávislá, právě když $\forall u \in X : u \notin \operatorname{span}(X \setminus \{u\})$.*

Poznámka 6.6 (Ověřování lineární (ne)závislosti)**.** Nechť $X \subseteq K^n, X = \{\mathbf{v_1}, \dots, \mathbf{v_k}\}$. Pro ověření lineární závislosti se nabízí dvě metody:

i. Řešíme $a_1 \cdot \mathbf{v_1} + \cdots + a_k \cdot \mathbf{v_k} = \mathbf{0}$, t.j. homogenní soustavu s n řádky a k sloupci, a hledáme netriviální řešení.

ii. Sestavíme matici, kde $\mathbf{v_1}, \ldots, \mathbf{v_k}$ tvoří řádky, a tuto matici převedeme do odstupňovaného tvaru. Dostaneme-li nulový řádek, je daná k-tice lineárně závislá; v opačném případě je lineární nezávislá.

Definice 6.7. Bazí prostoru V nazvneme libovolnou množinu $X \subseteq V$, která je lineárně nezávislá a navíc generuje celý prostor V, t.j. $\mathrm{span}(X) = V$.

Poznámka 6.8 (Význam báze)**.** Díky tomu, že báze generuje celý prostor V, lze každý vektor $\mathbf{u} \in V$ vyjádřit jako lineární kombinaci vektorů z báze. Navíc, jak ukazuje následující pozorování, díky lineární nezávislosti vektorů báze je toto vyjádření jednoznačné.

Pozorování 6.9. *Nechť $X = \{\mathbf{v_1}, \ldots, \mathbf{v_n}\}$ je konečná báze prostoru V a nechť $\mathbf{u} \in V$. Jelikož X generuje celý prostor V, lze vektor $\mathbf{u}$ vyjádřit jako lineární kombinaci vektorů báze:*

$$\mathbf{u} = \sum_{i=1}^{k} a_i \cdot \mathbf{v_i}.$$

Toto vyjádření je jednoznačné.

Důkaz. Sporem. Nechť existují dvě různá vyjádření vektoru $\mathbf{u}$ jako lineární kombinace vektorů báze, $\sum_{i=1}^{k} a_i \cdot \mathbf{v_i}$, a $\sum_{i=1}^{k} a'_i \cdot \mathbf{v_i}$. Jelikož jsou tato vyjádření různá, tak $\exists i : a_i - a'_i \neq 0$. Dále:

$$\begin{aligned}
\mathbf{0} &= \mathbf{u} - \mathbf{u} \\
&= \sum_{i=1}^{k} a_i \cdot \mathbf{v_i} - \sum_{i=1}^{k} a'_i \cdot \mathbf{v_i} \\
&= \sum_{i=1}^{k} (a_i - a'_i) \cdot \mathbf{v_i},
\end{aligned}$$

čímž dostáváme spor s lineární nezávislostí vektorů báze. □

Definice 6.10. Nechť $X = \{\mathbf{v_1}, \ldots, \mathbf{v_n}\}$ je konečná uspořádaná báze prostoru V nad K. Pro libovolný vektor $\mathbf{u} \in V$ nazveme koeficienty $(a_1, \ldots, a_n)^\top \in K^n$ z jednoznačného vyjádření:

$$\mathbf{u} = \sum_{i=1}^{n} a_i \cdot \mathbf{v_i}$$

vektorem souřadnic vektoru $\mathbf{u}$ vůči bázi X. Značí se $[\mathbf{u}]_X = (a_1, \ldots, a_n)$.

Poznámka 6.11 (Příklad bází a vektorů souřadnic)**.**

- Nechť $V = \{\text{kvadratické polynomy}\}$ a báze $X = \{x^2, x^1, x^0\}$. Potom funkci $f = 2x^2 + 3x - 1$ lze vyjádřit vektorem souřadnic jako $[f]_X = (2; 3; -1)^\top$.

- Pro vektorový prostor $V = K^n$ nazveme kanonickou bází bázi tvořenou vektory $\{\mathbf{e_1}, \dots, \mathbf{e_n}\}$, kde $\mathbf{e_i}$ je i-tý sloupec jednotkové matice.

Tvrzení 6.12. *Nechť X je taková množina, že generuje celý vektorový prostor V, t.j.* $\mathrm{span}(X) = V$*, ale $\forall Y \subset X : \mathrm{span}(Y) \neq V$. Potom X je báze vektorového prostoru V.*

Důkaz. Musíme ověřit obě podmínky báze:

i. $\mathrm{span}(X) = V$ víme z předpokladů.

ii. Lineární nezávislost množiny X plyne z toho, že $\forall \mathbf{u} \in X : \mathbf{u} \notin \mathrm{span}(X \setminus \{\mathbf{u}\})$.

□

Důsledek 6.13. *Z každého konečného systému generátorů lze vybrat bázi.*

Důkaz. Stačí vzít nějakou minimální vzhledem k inkluzi, která generuje V. □

Věta 6.14. *Každý vektorový prostor má bázi.*

Důkaz. Bez důkazu pro vektorové prostory s nekonečným systémem generátorů, jelikož by byl třeba axiom výběru. □

Lemma 6.15 (Lemma o výměně)**.** *Nechť $\{\mathbf{v_1}, \dots, \mathbf{v_n}\}$ je systém generátorů V a $\mathbf{u} \in V$. Potom pro všechna i taková, pro která existuje výjádření $\mathbf{u} = \sum_{j=1}^{n} a_j \cdot \mathbf{v_j}$, kde $a_i \neq 0$, platí, že $\{\mathbf{v_1}, \dots, \mathbf{v_{i-1}}, \mathbf{u}, \mathbf{v_{i+1}}, \dots, \mathbf{v_n}\}$ je opět systém generátorů V.*

Důkaz. Vyjádříme $\mathbf{v_i}$ jako:

$$\mathbf{v_i} = \frac{1}{a_i}\left(\mathbf{u} - \sum_{j=1, j\neq i}^{n} a_j \mathbf{v_j}\right).$$

Potom libovolné $\mathbf{w} \in V, \mathbf{w} = \sum_{j=1}^{n} b_j \mathbf{v_j}$ lze zapsat jako:

$$\begin{aligned}
\mathbf{w} &= \sum_{j=1, j\neq i}^{n} b_j \mathbf{v_j} + b_i \cdot \frac{1}{a_i}\left(\mathbf{u} - \sum_{j=1, j\neq i}^{n} a_j \mathbf{v_j}\right) \\
&= \sum_{j=1, j\neq i}^{n} b_j \mathbf{v_j} + \frac{b_i}{a_i}\mathbf{u} - \sum_{j=1, j\neq i}^{n} \frac{b_i a_j}{a_i}\mathbf{v_j} \\
&= \frac{b_i}{a_i}\mathbf{u} + \sum_{j=1, j\neq i}^{n} \left(b_j - \frac{b_i a_j}{a_i}\right)\mathbf{v_j}
\end{aligned}$$

□

Věta 6.16 (Steinitzova věta o výměně)**.** *Nechť V je vektorový prostor, X je linárně nezávislá ve V a Y je konečný systém generátorů V. Potom existuje Z takové, že $X \subseteq Z \subseteq X \cup Y, L(Z) = V$ a $|Z| = |Y|$. Navíc platí $|X| \leq |Y|$.*

Důkaz. Označme $X \setminus Y = \{u_1, \dots, u_n\}$ a položme $Z_0 \coloneqq Y$. Pro $i = 1, \dots, n$ provedeme: Z_{i-1} generuje V. Vyjádříme u_i vůči Z_{i-1}:

$$u_i = \sum_{w_j \in Z_{i-1}} a_j w_j.$$

X je lineárně nezávislá, a tedy $a_j \neq 0$ pro nějaké $w_j \in Y \setminus X$. Položíme $Z_i \coloneqq Z_{i-1} \cup \{u_i\} \setminus w_j$. Dle lemmatu o výměně $\operatorname{span}(Z_i) = V$. Nakonec, $Z \coloneqq Z_n, |Z| = |Z_n| = |Z_{n-1}| = \dots = |Z_0| = |Y|$.

Pokud by $|X| > |Y|$, potom $\exists i < n : Z_i \subset X$ a $\operatorname{span}(Z_i) = V$. Dostáváme spor s lineární nezávislostí množiny X. □

Důsledek 6.17. *Pokud má vektorový prostor V konečnou bázi, potom všechny jeho báze mají stejnou mohutnost.*

Důkaz. Nechť X a Y jsou dvě různé báze vektorového prostoru V. Potom:

a. X je lineárně nezávislá a $\operatorname{span}(Y) = V$. Potom dle Věty 6.16 je $|X| \leq |Y|$.

b. Podobně Y je lineárně nezávislá, $\operatorname{span}(X) = V$ a $|Y| \leq |X|$.

Vyplývá, že $|X| = |Y|$. □

Důsledek 6.18. *Pokud má vektorový prostor V konečný systém generátorů, potom lze každou lineárně nezávislou množinu X doplnit na bázi.*

Definice 6.19. Nechť má vektorový prostor V konečnou bázi. Potom se o V říká, že je konečně generovaný a mohutnost jeho libovolné báze nazveme dimenzí prostoru V. Značí se $\dim V$.

Poznámka 6.20 (Příklady bází a jejich dimenzí)**.**

- $\dim K^n = n$
- Je-li matice $\mathbf{A}$ v odstupňovaném tvaru, potom $\dim R(\mathbf{A}) = \operatorname{rank} \mathbf{A}$.

Pozorování 6.21. *Je-li W podprostor vektorového prostoru V konečné dimenze, pak* $\dim W \leq \dim V$.

Důkaz. Báze W je lineárně nezávislá v V, ale lze ji doplnit na bázi celého prostoru V. □

Pozorování 6.22. *Pro podprostory $U, V \subseteq W$, kde* $\dim W < \infty$*, platí:*

$$\dim U + \dim V = \dim U \cap V + \dim(\operatorname{span}(U \cup V)).$$

Pozorování 6.23. *Pro všechna $\mathbf{A} \in K^{m \times n}$ platí* $\dim R(\mathbf{A}) = \operatorname{rank} \mathbf{A}$.

Důkaz. Je-li $\mathbf{A} \sim \mathbf{A'}$ v odstupňovaném tvaru:

$$\dim R(\mathbf{A}) = \dim R(\mathbf{A'}) = \operatorname{rank} \mathbf{A'} = \operatorname{rank} \mathbf{A}.$$

$\square$

Poznámka 6.24. Pozorování 6.23 lze využít k nalezení báze a určení dimenze podmnožin K^n: Sestavíme matici z vektorů po řádcích a převedeme ji do odstupňovaného tvaru. Výsledné nenulové řádky tvoří bázi.

Věta 6.25. *Nechť* $\mathbf{A} \in K^{m \times n}$. *Potom platí:*

$$\dim R(\mathbf{A}) = \dim S(\mathbf{A}).$$

Důkaz.

I. Nejdříve ukážeme, že přinásobením matice zleva dimenze sloupcového prostoru nevzroste. Matice $\mathbf{R}$ a $\mathbf{A}$ jsou dány. Spočteme $\mathbf{A'} = \mathbf{R} \cdot \mathbf{A}$. Označme $\mathbf{u_1}, \cdots, \mathbf{u_n}$ sloupce matice $\mathbf{A}$ a $\mathbf{u'_1}, \cdots, \mathbf{u'_n}$ sloupce matice $\mathbf{A'}$. Platí $\mathbf{u'_i} = \mathbf{R} \cdot \mathbf{u_i}$.

   Nechť $w' \in S(\mathbf{A'})$, tedy $w' = \sum_{i=1}^{n} a_i \mathbf{u'_i} = \sum_{i=1}^{n} a_i \cdot \mathbf{R} \cdot \mathbf{u_i} = \mathbf{R} \cdot \sum_{i=1}^{n} a_i \mathbf{u_i} = \mathbf{R} \cdot \mathbf{w}$ pro nějaké $\mathbf{w} \in S(A)$.

   Nyní vyjádříme $\mathbf{w}$ vůči bázi $\mathbf{v_1}, \cdots, \mathbf{v_d}$ prostoru $S(\mathbf{A})$, čili $\mathbf{w} = \sum_{i=1}^{d} b_i \mathbf{v_i}$. Potom $\mathbf{w'} = \mathbf{R} \cdot \mathbf{w} = \mathbf{R} \cdot \sum_{i=1}^{n} b_i \mathbf{v_i} = \sum_{i=1}^{d} b_i \mathbf{R} \mathbf{v_i} = \sum_{i=1}^{d} b_i \mathbf{v'_i}$, kde $\mathbf{v'_i} \in S(\mathbf{A'})$, čili $\mathbf{v'_1}, \cdots, \mathbf{v'_d}$ tvoří systém generátorů $S(\mathbf{A'})$.

   Tedy: $\dim S(\mathbf{A'}) \leq \dim S(\mathbf{A})$.

II. Je-li matice $\mathbf{R}$ regulární, dimenze zůstane zachována: $\mathbf{A} = \mathbf{R^{-1}} \cdot \mathbf{A'}$, tedy $\dim S(\mathbf{A}) \leq \dim S(\mathbf{A'})$.

III. Pro matici $\mathbf{A'}$ v odstupňovaném tvaru platí $\dim R(\mathbf{A'}) = \dim S(\mathbf{A'})$, jelikož sloupce s pivoty jsou lineárně nezávislé a tvoří bázi $S(\mathbf{A'})$.

IV. Pro danou matici $\mathbf{A}$ nalezneme $\mathbf{A'} \sim \mathbf{A}$, $\mathbf{A'}$ je v odstupňovaném tvaru. Víme, že platí: $\mathbf{A'} = \mathbf{R} \cdot \mathbf{A}$, $\mathbf{R}$ je regulární.

   $$\dim S(\mathbf{A}) \overset{\text{II}}{=} \dim S(\mathbf{A'}) \overset{\text{III}}{=} \dim R(\mathbf{A'}) \underbrace{=}_{\text{Pozorování 6.23}} \dim R(\mathbf{A})$$

$\square$

Důsledek 6.26. $\operatorname{rank} \mathbf{A} = \operatorname{rank} \mathbf{A}^{\top}$

Důsledek 6.27. *Nechť* $\mathbf{R}$ *je regulární. Potom:*

$$\operatorname{rank} \mathbf{A} = \operatorname{rank} \mathbf{R} \cdot \mathbf{A}$$

$$\operatorname{rank} \mathbf{A} = \operatorname{rank} \mathbf{A} \cdot \mathbf{R}$$

Důsledek 6.28. $S(\mathbf{A} \cdot \mathbf{B}) \subseteq S(\mathbf{A})$ *a* $R(\mathbf{A} \cdot \mathbf{B}) \subseteq R(\mathbf{B})$

Důkaz. $S(\mathbf{AB}) = \text{span}(\{x | x = \mathbf{A} \cdot u, u \text{ je sloupec } \mathbf{B}\}) = \{x' | x' = \mathbf{A} \cdot u', u' \in S(\mathbf{B})\} \subseteq \{x' | x' = \mathbf{A} \cdot u', u' \in K^n\} = S(\mathbf{A})$ □

Důsledek 6.29 (Při násobení padáme s hodností)**.** $\text{rank}\,\mathbf{AB} \leq min\{\text{rank}\,\mathbf{A}; \text{rank}\,\mathbf{B}\}$.

Tvrzení 6.30. *Pro matici* $\mathbf{A}$ *řádu* $m \times n$ *platí:*

$$\dim Ker(\mathbf{A}) + \text{rank}\,\mathbf{A} = n$$

Důkaz.

i. Hodnost matice $\text{rank}\,\mathbf{A}$ určuju počet pivotů, tedy počet bázových proměnných.

ii. Pokud $\mathbf{x} \in Ker(\mathbf{A})$, potom $\mathbf{x}$ řeší $\mathbf{Ax} = \mathbf{0}$. Vektor $\mathbf{x}$ lze vyjádřit jako:

$$\mathbf{x} = p_1 \mathbf{x^1} + \cdots + p_2 \mathbf{x^{n-r}}$$

Množina $\left\{\mathbf{x^i}\right\}_{i=1}^{n-r}$ generuje $Ker(\mathbf{A})$. Navíc, x_i jsou lineárně nezávislé, jelikož $\mathbf{x_i}$ má ve složce odpovídající i-té volné proměnné jedničku, zatímco ostatní složky jsou rovny nule. Plyne, že $\left\{\mathbf{x^i}\right\}_{i=1}^{n-r}$ je báze $Ker(\mathbf{A})$ a $\dim Ker(\mathbf{A}) = n - r$.

□

7 Lineární zobrazení

Pozorování 7.1. *Nechť* $\mathbf{A} \in K^{m\times n}$ *a* $f : K^n \to K^m$ *je zobrazení definováno předpisem* $f(\mathbf{u}) = \mathbf{A}\cdot\mathbf{u}$. *Potom platí:*

i. $f(\mathbf{u}+\mathbf{v}) = \mathbf{A}(\mathbf{u}+\mathbf{v}) = \mathbf{Au}+\mathbf{Av} = f(\mathbf{u})+f(\mathbf{v})$

ii. $f(a\cdot\mathbf{u}) = \mathbf{A}(a\cdot\mathbf{u}) = a\cdot\mathbf{Au} = a\cdot f(\mathbf{u})$

Definice 7.2. Nechť V a W jsou vektorové prostory nad stejným tělesem K. Zobrazení $f : V \to W$ se nazývá lineární zobrazení, pokud platí:

i. $\forall \mathbf{u},\mathbf{v} \in V : f(\mathbf{u}+\mathbf{v}) = f(\mathbf{u})+f(\mathbf{v})$

ii. $\forall \mathbf{u} \in V, \forall a \in K : f(a\cdot\mathbf{u}) = a\cdot f(\mathbf{u})$

Poznámka 7.3 (Příklady lineárních zobrazení)**.**

- Pro libovolné V a W můžeme vzít $f(\mathbf{u}) = \mathbf{0}$ pro $\forall\mathbf{u} \in V$, tzv. nulové zobrazení.
- Pro $V \subseteq W$ můžeme vzít $f(\mathbf{u}) = \mathbf{u}$, čili identita na V, neboli vnoření V do W.
- Pro aritmetické vektorové prostory $V = K^n$, $W = K^1$ definujeme projekci na i-tou souřadnici π_i předpisem:
$$\pi_i(\mathbf{u}) = u_i.$$
- Nechť V je vektorový prostor a $X = \{\mathbf{v_1},\ldots,\mathbf{v_n}\}$ jeho konečná báze. Nechť dále $\mathbf{u},\mathbf{v} \in V$, a $\mathbf{u} = \sum a_i\mathbf{v_i}$, $\mathbf{b} = \sum b_i\mathbf{v_i}$. Potom zobrazení $f : V \to K^n$ na vektor souřadnic je lineární zobrazení:
$$f(\mathbf{u}+\mathbf{v}) = [\mathbf{u}+\mathbf{v}]_X = \left[\sum a_i\mathbf{v_i} + \sum b_i\mathbf{v_i}\right]_X = \left[\sum (a_i+b_i)\mathbf{v_i}\right]_X = [\mathbf{u}]_X + [\mathbf{v}]_X = f(\mathbf{u})+f(\mathbf{v})$$
Násobení analogicky.
- Geometrická zobrazení v rovině:
  - Posunutí není lineární zobrazení, jelikož počátek ve V se musí zobrazit na počátek ve W.
  - Osová souměrnost, otočení a stejnolehlost jsou lineární zobrazení, pokud zachovávají počátek.
- Obecně v $\mathbb{R}^2$:
$$f(\mathbf{u}) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} u_x \\ u_y \end{pmatrix},$$
- V prostoru diferencovatelných funkcí je derivace lineární zobrazení.

Pozorování 7.4. *Nechť $f : U \to V$ a $g : V \to W$ jsou lineární zobrazení. Potom je jejich složení $g \circ f : U \to W$, $(g \circ f)(\mathbf{u}) = g(f(\mathbf{u}))$ také lineární zobrazení.*

Důkaz. Ověříme podmínky:

i. $(g\circ f)(\mathbf{u}+\mathbf{v}) = g(f(\mathbf{u}+\mathbf{v})) = g(f(\mathbf{u})+f(\mathbf{v})) = g(f(\mathbf{u}))+g(f(\mathbf{v})) = (g\circ f)(\mathbf{u})+(g\circ f)(\mathbf{v})$.

ii. $(g \circ f)(a \cdot \mathbf{v})$ analogicky.

□

Věta 7.5. *Nechť V a W jsou vektorové prostory nad společným tělesem a X je báze V. Potom pro všechna zobrazení $f_0 : X \to W$ existuje právě jedno lineární zobrazení $f : V \to W$, které rozšiřuje f_0:*

$$\forall \mathbf{v} \in X : f(\mathbf{v}) = f_0(\mathbf{v}).$$

Důkaz. Vyjádříme $\mathbf{u} \in V$ vůči bázi: $\mathbf{u} = \sum a_i \mathbf{v_i}$. Potom $f(\mathbf{u}) = f(\sum a_i \mathbf{v_i}) = \sum a_i f(\mathbf{v_i}) = \sum a_i f_0(\mathbf{v_i})$. □

Důsledek 7.6. *Označíme-li $f(V) = \cup_{\mathbf{u}\in V} f(\mathbf{u})$, potom $f(V)$ je podprostor prostoru W a* $\dim f(V) \leq \dim V$*, protože obraz báze V je systém generátorů $f(V)$.*

Definice 7.7. Nechť V a W jsou vektorové prostory nad K a $X = \{\mathbf{v_1}, \dots, \mathbf{v_n}\}$ a $Y = \{\mathbf{w_1}, \dots, \mathbf{w_m})$ jsou jejich báze. Potom pro lineární zobrazení $f : V \to W$ nazveme matici $[f]_{XY} \in K^{m\times n}$ sestavenou z vektorů souřadnic obrazů vektorů báze X vůči Y maticí zobrazení f vůči bázím X a Y:

$$[f]_{XY} = \begin{pmatrix} \vdots & \vdots & \dots & \vdots \\ [f(\mathbf{v_1})]_Y & [f(\mathbf{v_2})]_Y & \dots & [f(\mathbf{v_n})]_Y \\ \vdots & \vdots & \dots & \vdots \end{pmatrix}$$

Pozorování 7.8.

$$[f(\mathbf{u})]_Y = [f]_{XY}[\mathbf{u}]_X$$

Důkaz. Vyjádříme $\mathbf{u}$ vůči bázi: $\mathbf{u} = \sum_{i=1}^n a_i \mathbf{v_i}$. Potom $[\mathbf{u}]_X = (a_1, \dots, a_n)^\top$, $f(\mathbf{u}) = \sum a_i f(\mathbf{v_i})$ a:

$$[f(\mathbf{u})]_Y = \left[\sum a_i f(\mathbf{v_i})\right]_Y = \sum a_i [f(\mathbf{v_i})]_Y = [f]_{XY}[\mathbf{u}]_X$$

□

Pozorování 7.9. *Jsou-li U, V, a W prostory nad K s bázemi X, Y a Z, a $f : U \to V$ a $g : V \to W$ jsou lineární zobrazení, tak platí:*

$$[g \circ f]_{XZ} = [g]_{YZ}[f]_{XY}$$

Důkaz.

$$[(g \circ f)(\mathbf{u})]_Z = [g(f(\mathbf{u}))]_Z = [g]_{YZ}[f(\mathbf{u})]_Y = [g]_{YZ}[f]_{XY}[\mathbf{u}]_X$$

□

Definice 7.10. Nechť V je prostor nad K a X, Y jsou jeho dvě konečné báze. Maticí přechodu od báze X k bázi Y rozumíme matici $[id]_{XY}$, kde id je identita.

Pozorování 7.11.

i. $[\mathbf{u}]_Y = [id(u)]_Y = [id]_{XY}[\mathbf{u}]_X$

ii. $[id]_{XY}[id]_{YX} = [id]_{YY} = \mathbf{I_n}$

Poznámka 7.12 (Výpočet matice přechodu pro $V = K^n$)**.** Pro báze $X = \{\mathbf{v_1}, \ldots, \mathbf{v_n}\}$ a $Y = \{\mathbf{w_1}, \ldots, \mathbf{w_n}\}$ sestavíme matice:

$$\mathbf{A} = \begin{pmatrix} \vdots & \ldots & \vdots \\ \mathbf{v_1} & \ldots & \mathbf{v_n} \\ \vdots & \ldots & \vdots \end{pmatrix}; \mathbf{B} = \begin{pmatrix} \vdots & \ldots & \vdots \\ \mathbf{w_1} & \ldots & \mathbf{w_n} \\ \vdots & \ldots & \vdots \end{pmatrix}$$

Platí $\mathbf{u} = \sum a_i \mathbf{v_i} = \mathbf{A}[\mathbf{u}]_X$ a $\mathbf{u} = \sum b_i \mathbf{w_i} = \mathbf{B}[\mathbf{u}]_Y$. Potom:

$$\mathbf{A}[\mathbf{u}]_X = \mathbf{B}[\mathbf{u}]_Y$$

$$[\mathbf{u}]_Y = \mathbf{B^{-1}}\mathbf{A}[\mathbf{u}]_X$$

Tedy: $[id]_{XY} = \mathbf{B^{-1}A}$. Prakticky: $(\mathbf{B}|\mathbf{A}) \sim (\mathbf{I_n}|[id]_{XY})$.

Definice 7.13. Nechť V a W jsou vektorové prostory nad K. Lineární zobrazení, které je prosté a na, nazveme isomorfismem prostorů V a W.

Pozorování 7.14. *Zobrazení f^{-1} je také isomorfismem.*

Důkaz. Musíme dokázat, že zobrazení f^{-1} je lineární zobrazení:

i. $f^{-1}(\mathbf{w} + \mathbf{w'}) = f^{-1}(f(\mathbf{u}) + f(\mathbf{u'})) = f^{-1}(f(\mathbf{u} + \mathbf{u'})) = \mathbf{u} + \mathbf{u'} = f^{-1}(\mathbf{w}) + f^{-1}(\mathbf{w'})$.

ii. Násobení analogicky.

□

Věta 7.15. *Nechť V a W jsou vektorové prostory nad K s konečnými bázemi X a Y. Potom platí, že lineární zobrazení $f : V \to W$ je isomorfismus, právě když matice $[f]_{XY}$ je regulární. Navíc platí:*

$$[f^{-1}]_{YX} = ([f]_{XY})^{-1}.$$

Důkaz.

- $\Longleftarrow$: $[f]_{XY}$ je regulární. Vezmeme zobrazení $g : W \to V$ definované maticí: $[g]_{YX} = ([f]_{XY})^{-1}$. Ukážeme, že $g = f^{-1}$ a ověříme vlastnosti isomorfismu.

  i. $[g \circ f]_{XX} = [g]_{YX}[f]_{XY} = \mathbf{I_n}$. Tedy $g \circ f$ je identita na V a f je prosté.

ii. $[f \circ g]_{YY} = [f]_{XY}[g]_{YX} = \mathbf{I_n}$. Tedy $f \circ g$ je identita na W a f je na.

- $\Longrightarrow$: Máme zobrazení f a f^{-1}. Pro jejich matice platí:

  i. $[f^{-1}]_{YX}[f]_{XY} = [id]_{XX} = \mathbf{I_n}, \dim V = n$

  ii. $[f]_{XY}[f^{-1}]_{YX} = [id]_{YY} = \mathbf{I_m}, \dim W = m$

  Vyplývá, že $n = m$ a $[f]_{XY}$ je regulární.

□

Tvrzení 7.16. *Každý prostor dimense n nad K je isomorfní s K^n.*

Důkaz. Zvolíme bázi X, potom zobrazení $f : \underbrace{\mathbf{u}}_{\in V} \rightarrow \underbrace{[u]_X}_{\in K^n}$ je isomoforfismem. $[f]_{Xk} = \mathbf{I_n}$ tvoří kanonickou bázi. □

Tvrzení 7.17. *Nechť $f : V \rightarrow W$ je lineární zobrazení. Potom platí:*

i. $Ker(f) \coloneqq \{\mathbf{x}|f(\mathbf{x}) = \mathbf{0}\}$ *je podprostor V.*

ii. Pokud má rovnice $f(\mathbf{x}) = \mathbf{b}$ alespoň 1 řešení $\mathbf{x_0}$, potom lze každé řešení $\mathbf{x}$ této rovnice vyjádřit jako $\mathbf{x} = \mathbf{x_0} + \mathbf{x'}$, kde $\mathbf{x'} \in Ker(f)$.

Důkaz.

i. Nechť $\mathbf{x_1}, \mathbf{x_2} \in Ker(f) : f(\mathbf{x_1}+\mathbf{x_2}) = f(\mathbf{x_1})+f(\mathbf{x_2}) = \mathbf{0}+\mathbf{0} = \mathbf{0}$, tedy $\mathbf{x_1}+\mathbf{x_2} \in Ker(f)$. Násobení analogicky.

ii. $f(\mathbf{x} - \mathbf{x_0}) = f(\mathbf{x}) - f(\mathbf{x_0}) = \mathbf{b} - \mathbf{b} = \mathbf{0}$, tedy $\mathbf{x} - \mathbf{x_0} \in Ker(f)$.

□

8 Skalární součin

Definice 8.1. Nechť V je vektorový prostor nad $\mathbb{C}$. Zobrazení, které dvojici vektorů $\mathbf{u}, \mathbf{v} \in V$ přiřadí $\langle \mathbf{u}|\mathbf{v} \rangle \in \mathbb{C}$, se nazývá <u>skalární součin</u>, pokud splňuje následující axiomy:

(N) $\forall \mathbf{u} \in V : \langle \mathbf{u}|\mathbf{u} \rangle = 0 \iff \mathbf{u} = \mathbf{0}$

(L1) $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V : \langle \mathbf{u} + \mathbf{v}|\mathbf{w} \rangle = \langle \mathbf{u}|\mathbf{w} \rangle + \langle \mathbf{v}|\mathbf{w} \rangle$

(L2) $\forall \mathbf{u}, \mathbf{v} \in V, \forall a \in \mathbb{C} : \langle a \cdot \mathbf{u}|\mathbf{v} \rangle = a \cdot \langle \mathbf{u}|\mathbf{v} \rangle$

(KS) $\forall \mathbf{u}, \mathbf{v} \in V : \langle \mathbf{u}|\mathbf{v} \rangle = \overline{\langle \mathbf{v}|\mathbf{u} \rangle}$

(P) $\forall \mathbf{u} \in V : \langle \mathbf{u}|\mathbf{u} \rangle \geq 0$

Poznámka 8.2 (Poznámka k axiomu (P))**.** Jelikož $\forall \mathbf{u} \in V : \langle \mathbf{u}|\mathbf{u} \rangle \geq 0$, vyplývá tedy, že $\langle \mathbf{u}|\mathbf{u} \rangle \in \mathbb{R}$.

Poznámka 8.3 (Příklady skalárních součinů)**.**

- Skalární součin pro aritmetické vektorové prostory:
  - $V = \mathbb{C}^n : \langle \mathbf{u}|\mathbf{v} \rangle = \sum_{i=1}^{n} u_i \overline{v_i}$
  - $V = \mathbb{R}^n : \langle \mathbf{u}|\mathbf{v} \rangle = \sum_{i=1}^{n} u_i v_i$
- Skalární součin na $\mathbb{R}^n$ definovaný pomocí regulární matice: $\langle \mathbf{u}|\mathbf{v} \rangle = \mathbf{u}^\top \cdot \mathbf{A}^\top \cdot \mathbf{A} \cdot \mathbf{v}$
- Skalární součin na prostoru reálných spojitých funkcí integrovatelných na intervalu $(a; b)$: $\langle f(x)|g(x) \rangle \coloneqq \int_a^b f(x)g(x)\, dx$

Pozorování 8.4. $\langle \mathbf{x}|\mathbf{0} \rangle = \langle \mathbf{0}|\mathbf{x} \rangle = 0$

Důkaz. $\langle \mathbf{x}|\mathbf{0} \rangle = \langle \mathbf{x}|0 \cdot \mathbf{x} \rangle = 0 \cdot \langle \mathbf{x}|\mathbf{x} \rangle = \langle 0 \cdot \mathbf{x}|\mathbf{x} \rangle = \langle \mathbf{0}|\mathbf{x} \rangle$ □

Definice 8.5. Nechť V je vektorový prostor se skalárním součinem, potom <u>norma</u> odvozená od skalárního součinu je zobrazení $\| \bullet \| : V \to \mathbb{R}$ dané předpisem:

$$\|\mathbf{u}\| \coloneqq \sqrt{\langle \mathbf{u}|\mathbf{u} \rangle}.$$

Poznámka 8.6 (Geometrická interpretace normy a skalárního součinu v $\mathbb{R}^n$)**.**

- $\|\mathbf{u}\|$ určuje délku vektoru $\mathbf{u}$
- $\|\mathbf{u} - \mathbf{v}\|$ určuje vzdálenost vektorů $\mathbf{u}$ a $\mathbf{v}$
- $\langle \mathbf{u}|\mathbf{v} \rangle$ určuje úhel mezi vektory $\mathbf{u}$ a $\mathbf{v}$

Pozorování 8.7. *Pro standardní skalární součin a jím určenou normu na $\mathbb{R}^n$ platí:*

$$\langle \mathbf{u} | \mathbf{v} \rangle = \|\mathbf{u}\| \cdot \|\mathbf{v}\| \cdot \cos\varphi,$$

kde φ je úhel sevřený vektory $\mathbf{u}$ a $\mathbf{v}$.

Důkaz. Vektory $\mathbf{u}$, $\mathbf{v}$ a $\mathbf{u} - \mathbf{v}$ tvoří trojúhelník. Podle kosinové věty:

$$\|\mathbf{u} - \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2 \cdot \|\mathbf{u}\| \cdot \|\mathbf{v}\| \cdot \cos\varphi,$$

tedy:

$$\langle \mathbf{u} - \mathbf{v} | \mathbf{u} - \mathbf{v} \rangle = \langle \mathbf{u} | \mathbf{u} \rangle + \langle \mathbf{v} | \mathbf{v} \rangle - 2 \cdot \|\mathbf{u}\| \cdot \|\mathbf{v}\| \cdot \cos\varphi.$$

Podle axiomů skalárního součinu ovšem také platí:

$$\begin{aligned} \langle \mathbf{u} - \mathbf{v} | \mathbf{u} - \mathbf{v} \rangle = & \\ &= \langle \mathbf{u} | \mathbf{u} - \mathbf{v} \rangle - \langle \mathbf{v} | \mathbf{u} - \mathbf{v} \rangle \\ &= \langle \mathbf{u} - \mathbf{v} | \mathbf{u} \rangle - \langle \mathbf{u} - \mathbf{v} | \mathbf{v} \rangle \\ &= \langle \mathbf{u} | \mathbf{u} \rangle - \langle \mathbf{v} | \mathbf{u} \rangle - \langle \mathbf{u} | \mathbf{v} \rangle + \langle \mathbf{v} | \mathbf{v} \rangle \\ &= \langle \mathbf{u} | \mathbf{u} \rangle - 2 \cdot \langle \mathbf{u} | \mathbf{v} \rangle + \langle \mathbf{v} | \mathbf{v} \rangle \end{aligned}$$

Odečteme-li tento výsledek od rovnice kosinové věty, dostáváme (po úpravách):

$$\langle \mathbf{u} | \mathbf{v} \rangle = \|\mathbf{u}\| \cdot \|\mathbf{v}\| \cdot \cos\varphi$$

□

Věta 8.8 (Cauchy-Schwarzova nerovnost)**.** *Nechť V je vektorový prostor nad $\mathbb{C}$ se skalárním součinem a s normou určenou tímto součinem. Potom platí:*

$$\forall u, v \in V : |\langle \mathbf{u} | \mathbf{v} \rangle| \leq \|\mathbf{u}\| \cdot \|\mathbf{v}\|.$$

Důkaz. Je-li $\mathbf{u} = \mathbf{0}$ nebo $\mathbf{v} = \mathbf{0}$, nerovnost platí.

Určitě $\forall a \in \mathbb{C} : \|\mathbf{u} + a \cdot \mathbf{v}\|^2 \geq 0$. Tedy:

$$\begin{aligned} 0 \leq \|\mathbf{u} + a\mathbf{v}\|^2 = & \\ &= \langle \mathbf{u} + a\mathbf{v} | \mathbf{u} + a\mathbf{v} \rangle \\ &= \langle \mathbf{u} | \mathbf{u} + a\mathbf{v} \rangle + \langle a\mathbf{v} | \mathbf{u} + a\mathbf{v} \rangle \\ &= \overline{\langle \mathbf{u} + a\mathbf{v} | \mathbf{u} \rangle} + a\overline{\langle \mathbf{u} + a\mathbf{v} | \mathbf{v} \rangle} \\ &= \langle \mathbf{u} | \mathbf{u} \rangle + \overline{a \langle \mathbf{v} | \mathbf{u} \rangle} + a\overline{\langle \mathbf{u} | \mathbf{v} \rangle} + a\overline{a} \langle \mathbf{v} | \mathbf{v} \rangle \\ &= \overline{a} \langle \mathbf{u} | \mathbf{v} \rangle + \langle \mathbf{u} | \mathbf{u} \rangle + a \langle \mathbf{v} | \mathbf{u} \rangle + a\overline{a} \langle \mathbf{v} | \mathbf{v} \rangle \end{aligned}$$

Dosadíme $a := -\frac{\langle \mathbf{u} | \mathbf{v} \rangle}{\langle \mathbf{v} | \mathbf{v} \rangle}$, čímž se zbavíme prvního a posledního členu. Zbývá:

$$0 \leq \langle \mathbf{u} | \mathbf{u} \rangle - \frac{\langle \mathbf{u} | \mathbf{v} \rangle \langle \mathbf{v} | \mathbf{u} \rangle}{\langle \mathbf{v} | \mathbf{v} \rangle}$$

$$\langle \mathbf{u} | \mathbf{v} \rangle \langle \mathbf{v} | \mathbf{u} \rangle \leq \langle \mathbf{u} | \mathbf{u} \rangle \langle \mathbf{v} | \mathbf{v} \rangle$$

Upravíme levou stranu nerovnosti:

$$\langle \mathbf{u}|\mathbf{v}\rangle\langle \mathbf{v}|\mathbf{u}\rangle = \langle \mathbf{u}|\mathbf{v}\rangle\overline{\langle \mathbf{u}|\mathbf{v}\rangle} = |\langle \mathbf{u}|\mathbf{v}\rangle|^2,$$

a tedy:

$$\begin{aligned} |\langle \mathbf{u}|\mathbf{v}\rangle|^2 &\le \langle \mathbf{u}|\mathbf{u}\rangle\langle \mathbf{v}|\mathbf{v}\rangle \\ |\langle \mathbf{u}|\mathbf{v}\rangle| &\le \|\mathbf{u}\|\|\mathbf{v}\| \end{aligned}$$

□

Důsledek 8.9 (Vztah mezi aritmetickým a kvadratickým průměrem)**.** *Nechť* $u_i \in \mathbb{R}$*. Potom:*

$$\frac{1}{n}\sum_{i=1}^{n} u_i \le \sqrt{\frac{1}{n}\sum_{i=1}^{n} u_i^2}$$

Důkaz. Položme

$$\begin{aligned} \mathbf{v} &= (1, 1, \dots, 1)^\top \\ \mathbf{u} &= (\text{seřazená čísla})^\top. \end{aligned}$$

Potom

$$\langle \mathbf{u}|\mathbf{v}\rangle = \sum_{i=1}^{n} u_i, \|\mathbf{u}\| = \sqrt{\sum_{i=1}^{n} u_i^2}, \text{ a } \|\mathbf{v}\| = \sqrt{n}.$$

□

Důsledek 8.10 (Trojúhelníková nerovnost)**.** *Norma odvozená od skalárního součinu splňuje trojúhelníkovou nerovnost:*

$$\|\mathbf{u}+\mathbf{v}\| \le \|\mathbf{u}\| + \|\mathbf{v}\|$$

Důkaz.

$$\begin{aligned} \|\mathbf{u}+\mathbf{v}\| &= \sqrt{\langle \mathbf{u}+\mathbf{v}|\mathbf{u}+\mathbf{v}\rangle} \\ &= \sqrt{\langle \mathbf{u}|\mathbf{u}+\mathbf{v}\rangle + \langle \mathbf{v}|\mathbf{u}+\mathbf{v}\rangle} \\ &= \sqrt{\langle \mathbf{u}|\mathbf{u}\rangle + \langle \mathbf{u}|\mathbf{v}\rangle + \langle \mathbf{v}|\mathbf{u}\rangle + \langle \mathbf{v}|\mathbf{v}\rangle} \\ &= \sqrt{\langle \mathbf{u}|\mathbf{u}\rangle + \langle \mathbf{u}|\mathbf{v}\rangle + \overline{\langle \mathbf{u}|\mathbf{v}\rangle} + \langle \mathbf{v}|\mathbf{v}\rangle} \\ &\le \sqrt{\langle \mathbf{u}|\mathbf{u}\rangle + 2|\langle \mathbf{u}|\mathbf{v}\rangle| + \langle \mathbf{v}|\mathbf{v}\rangle} && (\text{V } \mathbb{C}\text{: } a + \overline{a} \le 2\cdot|a|) \\ &\le \sqrt{\langle \mathbf{u}|\mathbf{u}\rangle + 2\|\mathbf{u}\|\|\mathbf{v}\| + \langle \mathbf{v}|\mathbf{v}\rangle} \\ &= \sqrt{\|\mathbf{u}\|^2 + 2\|\mathbf{u}\|\|\mathbf{v}\| + \|\mathbf{v}\|^2} \\ &= \sqrt{(\|\mathbf{u}\| + \|\mathbf{v}\|)^2} = \|\mathbf{u}\| + \|\mathbf{v}\| \end{aligned}$$

□

Definice 8.11. Obecně norma na vektorovém prostoru V je zobrazení $\| \bullet \| : V \to \mathbb{R}$, které splňuje následující podmínky:

i. $\|\mathbf{0}\| = 0$

ii. $\|\mathbf{u}\| \geq 0$

iii. $\|a \cdot \mathbf{u}\| = a \cdot \|\mathbf{u}\|$

iv. $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$

Poznámka 8.12 (Příklady norm)**.**

- Norma odvozená od skalárního součinu (viz definici 8.5).
- L_p norma, definovaná:

$$\|\mathbf{u}\|_p = \sqrt[p]{\sum_{i=1}^{n} |u_i|^p}.$$

  Obvyklá Eukleidovská norma ($\sqrt{\sum_{i=1}^{n} |u_i|^2}$) je tedy speciální případ L_p normy s $p = 2$.

9 Ortogonalita

Definice 9.1. Vektory $\mathbf{u}$ a $\mathbf{v}$ z prostoru se skalárním součinem se nazývají vzájemně kolmé, pokud platí:

$$\langle \mathbf{u} | \mathbf{v} \rangle = 0.$$

Značíme $\mathbf{u} \perp \mathbf{v}$.

Pozorování 9.2. *Každý systém vzájemně kolmých netriviálních vektorů je lineárně nezávislý.*

Důkaz. Sporem. Nechť $\mathbf{u_0} = \sum_{i=1}^{n} a_i \mathbf{u_i}$. Potom:

$$0 \neq \langle \mathbf{u_0} | \mathbf{u_0} \rangle = \langle \mathbf{u_0} | \sum_{i=1}^{n} a_i \mathbf{u_i} \rangle = \sum_{i=1}^{n} \overline{a_i} \underbrace{\langle \mathbf{u_0} | \mathbf{u_i} \rangle}_{0 \text{ pro } \forall i} = 0$$

□

Pozorování 9.3. *Nechť V je vektorový prostor se skalárním součinem. Potom:*

$$\forall \mathbf{v} \in V : \mathbf{v} \perp \mathbf{0}.$$

Definice 9.4. Nechť V je vektorový prostor se skalárním součinem a Z jeho báze taková, že:

- $\forall \mathbf{v} \in Z : \|\mathbf{v}\| = 1$
- $\forall \mathbf{v} \neq \mathbf{v}' \in Z : \mathbf{v} \perp \mathbf{v}'$

Potom se Z nazývá ortonormální báze prostoru V.

Tvrzení 9.5. *Nechť $Z = \{\mathbf{v_1}, \dots, \mathbf{v_n}\}$ je ortonomální báze prostoru V. Potom $\forall \mathbf{u} \in V$ platí:*

$$\mathbf{u} = \langle \mathbf{u} | \mathbf{v_1} \rangle \mathbf{v_1} + \langle \mathbf{u} | \mathbf{v_2} \rangle \mathbf{v_2} + \dots + \langle \mathbf{u} | \mathbf{v_n} \rangle \mathbf{v_n}$$

Důkaz. $\mathbf{u} = \sum_{i=1}^{n} a_i \mathbf{v_i}$, a tedy: $[\mathbf{u}]_Z = (a_1, \dots, a_n)^\top$. Potom:

$$\langle \mathbf{u} | \mathbf{v_1} \rangle = \langle \sum_{i=1}^{n} a_i \mathbf{v_i} | \mathbf{v_1} \rangle = \sum_{i=1}^{n} a_i \langle \mathbf{v_i} | \mathbf{v_1} \rangle = a_i,$$

neboť:

$$\langle \mathbf{v_i} | \mathbf{v_1} \rangle = \begin{cases} 0 \text{ pro } i \neq 1, \\ 1 \text{ pro } i = 1 \end{cases}$$

□

Definice 9.6. Nechť W je prostor se skalárním součinem, V je podprostor W, a $Z = \{\mathbf{v_1}, \dots, \mathbf{v_n}\}$ je nějaká ortonormální báze V.

Zobrazení $p_Z : W \to V$ definované předpisem:

$$p_Z(\mathbf{u}) = \sum_{i=1}^{n} \langle \mathbf{u} | \mathbf{v_i} \rangle \mathbf{v_i}$$

se nazývá ortogonální projekce prostoru W na V.

Pozorování 9.7. *Ortogonální projekce je lineární zobrazení.*

Lemma 9.8. *Nechť p_Z je ortogonální projekce prostoru W na V. Potom $\forall \mathbf{u} \in W$ platí:*

$$(\mathbf{u} - p_Z(\mathbf{u})) \perp \mathbf{v_i} \text{ pro } \forall \mathbf{v_i} \in Z.$$

Důkaz.

$$\langle \mathbf{u} - p_Z(\mathbf{u}) | \mathbf{v_i} \rangle = \langle \mathbf{u} - \sum_{j=1}^{n} \langle \mathbf{u} | \mathbf{v_j} \rangle \mathbf{v_j} | \mathbf{v_i} \rangle = \langle \mathbf{u} | \mathbf{v_i} \rangle - \sum_{i=n}^{n} \langle \mathbf{u} | \mathbf{v_j} \rangle \langle \mathbf{v_j} | \mathbf{v_i} \rangle = \langle \mathbf{u} | \mathbf{v_i} \rangle - \langle \mathbf{u} | \mathbf{v_i} \rangle = 0$$

jelikož

$$\langle \mathbf{v_j} | \mathbf{v_i} \rangle = \begin{cases} 1 \text{ pro } i = j, \\ 0 \text{ pro } i \neq j \end{cases}$$

□

Pozorování 9.9. *Projekce $p_Z(\mathbf{u})$ je nejbližší vektor k vektoru $\mathbf{u}$, který leží v prostoru V.*

Definice 9.10. V zápise $\mathbf{u} = \langle \mathbf{u} | \mathbf{v_1} \rangle \mathbf{v_1} + \dots + \langle \mathbf{u} | \mathbf{v_n} \rangle \mathbf{v_n}$ se koeficienty $\langle \mathbf{u} | \mathbf{v_i} \rangle$ nazývají Fourierovy koeficienty.

Algoritmus 9.11. Gram-Schmidtova ortonormalizace je postup, který převede libovolnou bázi $\{\mathbf{u_1}, \dots, \mathbf{u_n}\}$ na ortonormální bázi $\{\mathbf{v_1}, \dots, \mathbf{v_n}\}$.

Postup. Pro i od 1 do n opakuj:

1. $\mathbf{w_i} = \mathbf{u_i} - \sum_{j=1}^{i-1} \langle \mathbf{u_i} | \mathbf{v_j} \rangle \mathbf{v_j}$, neboli odečtení projekce na doposud spočtený lineární obal $\text{span}(\mathbf{v_1}, \dots, \mathbf{v_{i-1}})$.
2. $\mathbf{v_i} = \frac{1}{\|\mathbf{w_i}} \mathbf{w_i}$

Poznámka 9.12. Dokažme korektnost Gram-Schmidtovy ortonormalizace.

1. $\mathbf{v_i} \perp \mathbf{v_j} \forall j < i$, dle Lemmatu 9.8
2. $\|\mathbf{v_i}\| = \|\frac{1}{\|\mathbf{w_i}\|} \mathbf{w_i}\| = \frac{1}{\|\mathbf{w_i}\|} \|\mathbf{w_i}\| = 1$

3. Zůstáváme ve stejném prostoru, neboli:

$$\operatorname{span}(\mathbf{v_1}, \ldots, \mathbf{v_{i-1}}, \mathbf{u_i}, \mathbf{u_{i+1}}, \ldots, \mathbf{u_n}) = \operatorname{span}(\mathbf{v_1}, \ldots, \mathbf{v_i}, \mathbf{u_{i+1}}, \ldots, \mathbf{u_n}),$$

dle Lemmatu 6.15.

Definice 9.13. Nechť V je množina vektorů ve vektorovém prostoru W se skalárním součinem. Ortogonální doplněk V je množina $V^\perp$ definována:

$$V^\perp := \{\mathbf{u} \in W, \forall \mathbf{v} \in V : \mathbf{u} \perp \mathbf{v}\}$$

Poznámka 9.14 (Příklady ortogonálních doplňků v R^3)**.** Doplněk přímky je kolmá rovina. Doplňek roviny je kolmá přímka.

Pozorování 9.15. *Pokud $U \subseteq V$, tak potom $U^\perp \supseteq V^\perp$.*

Důkaz. $\mathbf{u} \in V^\perp \iff \mathbf{u} \perp \mathbf{v}$ pro $\forall \mathbf{v} \in V \implies \mathbf{u} \perp \mathbf{v}$ pro $\forall \mathbf{v} \in U \iff \mathbf{u} \in U^\perp$ □

Věta 9.16. *Nechť V je podprostorem prostoru W se skalárním součinem. Potom platí:*

i. *$V^\perp$ je podprostorem W*

ii. $V \cap V^\perp = \{\mathbf{0}\}$

Pokud je navíc W konečné dimenze, tak platí:

iii. $\dim V + \dim V^\perp = \dim W$

iv. $(V^\perp)^\perp = V$

Důkaz.

i. Je třeba ověřit uzavřenost na sčítání a násobení:

- $\langle \mathbf{u} + \mathbf{v} | \mathbf{w} \rangle = \langle \mathbf{u} | \mathbf{w} \rangle + \langle \mathbf{v} | \mathbf{w} \rangle = 0 + 0 = 0$
- $\langle a\mathbf{u} | \mathbf{w} \rangle = a \cdot \langle \mathbf{u} | \mathbf{w} \rangle = a \cdot 0 = 0$

ii. Pokud $\mathbf{u} \in V \cap V^\perp$, potom $\langle \mathbf{u} | \mathbf{u} \rangle = 0$ a tedy $\mathbf{u} = \mathbf{0}$.

iii.-iv. Sestrojíme ortonormální bázi V a doplníme ji na ortonormální bázi W. To, co jsme přidali, je ortonormální báze $V^\perp$.

□