14. prosince 2023

# Algebra I

2023/2024

Zdeněk Kočan

Tento text je studijní opora k předmětu Algebra I pro studenty bakalářských studijních programů v akademickém roce 2023/2024. Máte-li k textu nějaké dotazy, připomínky, náměty, nebo narazíte-li na nějakou chybu, nepřesnost nebo překlep, prosím, napište mi na zdenek.kocan@math.slu.cz.

Obsah

# Pole

Uvažujme množinu všech reálných čísel. Reálná čísla sčítáme a násobíme, ke každému reálnému číslu existuje číslo opačné (součet čísla a k němu opačného čísla je roven 0), ke každému nenulovému reálnému číslu existuje číslo inverzní (převrácená hodnota, součin čísla a k němu inverzního čísla je roven 1). Pro libovolná reálná čísla $a, b, c$ navíc platí

$$\begin{aligned} &a+b=b+a, \quad a\cdot b=b\cdot a && \text{(součet a součin jsou komutativní,}\\ &a+(b+c)=(a+b)+c, \quad a\cdot(b\cdot c)=(a\cdot b)\cdot c && \text{asociativní}\\ &a\cdot(b+c)=a\cdot b+a\cdot c && \text{a splňují distributivní zákon)} \end{aligned}$$

Každá množina obsahující aspoň 2 prvky (obvykle označované 0 a 1) s uvedenými operacemi s uvedenými vlastnostmi se nazývá *pole*. Příkladem pole je *pole komplexních čísel*, které značíme $\mathbb{C}$.

Každá podmnožina množiny komplexních čísel, která obsahuje 0 a 1, s každým číslem obsahuje k němu opačné, s každým nenulovým číslem obsahuje k němu inverzní a s libovolnými dvěmi čísly obsahuje jejich součet i součin, se nazývá *číselné pole*.

Příklady číselných polí jsou množina komplexních čísel $\mathbb{C}$, množina reálných čísel $\mathbb{R}$ a množina racionáních čísel $\mathbb{Q}$. Například množina celých čísel $\mathbb{Z}$ a množina přirozených (kladných celých) čísel $\mathbb{N}$ nejsou pole.

Je-li $P$ pole a $n$ přirozené číslo, potom $P^n$ označuje množinu všech uspořádaných $n$-tic prvků pole $P$.

Polím se ještě budeme věnovat později, v kapitole 6.

# 1. Matice

## 1.1. Matice

**Definice 1.1.1.** Buď $P$ pole, buďte $m, n$ přirozená čísla. *Matice* typu $m \times n$ nad polem $P$ je tabulka o $m$ řádcích a $n$ sloupcích obsahující na každém místě nějaký prvek pole $P$ (a nic jiného). Máme-li takovou matici $A$, pak prvek pole $P$ v $i$-tém řádku a $j$-tém sloupku označujeme $A^i_j$ a matici zapisujeme obvykle

$$A = \begin{pmatrix} A^1_1 & A^1_2 & \dots & A^1_n \\ A^2_1 & A^2_2 & \dots & A^2_n \\ \vdots & \vdots & & \vdots \\ A^m_1 & A^m_2 & \dots & A^m_n \end{pmatrix}$$

nebo stručněji $A = (A^i_j)_{m\times n}$ nebo jen $A = (A^i_j)$.

Matici typu $m \times n$ nad polem $P$ je možné definovat také jako zobrazení z kartézského součinu $\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}$ do pole $P$. Takové zobrazení tedy uspořádané dvojici $(i, j)$ přiřazuje $A^i_j \in P$ a můžeme ho zapsat právě ve tvaru tabulky, která má v $i$-tém řádku a $j$-tém sloupku prvek $A^i_j$.

Horním indexům říkáme *řádkové*, dolním indexům říkáme *sloupkové*. Pro pevně zvolené $i$

$$A^i_\circ = \begin{pmatrix} A^i_1 & A^i_2 & \dots & A^i_n \end{pmatrix}$$

je *$i$-tý řádek* matice $A$; je to tedy matice typu $1\times n$, někdy ji zapisujeme jako uspořádanou $n$-tici $(A^i_1, A^i_2, \dots, A^i_n) \in P^n$. Nulový řádek označme $0_\circ$. Pro pevně zvolené $j$

$$A^\circ_j = \begin{pmatrix} A^1_j \\ A^2_j \\ \vdots \\ A^m_j \end{pmatrix}$$

je *$j$-tý sloupek* matice $A$; je to tedy matice typu $m\times 1$, někdy ji zapisujeme jako uspořádanou $m$-tici $(A^1_j, A^2_j, \dots, A^m_j) \in P^m$ nebo $\begin{pmatrix} A^1_j & A^2_j & \dots & A^m_j \end{pmatrix}^\mathsf{T}$ nebo $(A^1_j, A^2_j, \dots, A^m_j)^\mathsf{T}$. Nulový sloupek označme $0^\circ$. To, že matice $A$ je tvořena řádky $A^i_\circ$, resp. sloupky $A^\circ_j$, budeme někdy zapisovat

$$A = \begin{pmatrix} A^1_\circ \\ A^2_\circ \\ \vdots \\ A^m_\circ \end{pmatrix}, \quad \text{resp. } A = \begin{pmatrix} A^\circ_1 & A^\circ_2 & \dots & A^\circ_n \end{pmatrix}.$$

**Definice 1.1.2.** Matice $A = (A^i_j)$ a $B = (B^i_j)$ se vzájemně *rovnají*, jestliže jsou stejného typu a na stejných místech mají stejné prvky, tedy jsou-li typu $m \times n$ a pro každé $i \in \{1, 2, \dots, m\}$ a každé $j \in \{1, 2, \dots, n\}$ platí $A^i_j = B^i_j$.

**Definice 1.1.3.** Matice $A = (A^i_j)_{m\times n}$ je

- *čtvercová*, jestliže $m = n$,
- *diagonální*, jestliže je čtvercová a $A^i_j = 0$ pro $i \neq j$ (prvky $A^i_i$ se také nazývají *diagonální* a tvoří *(hlavní) diagonálu*),
- *jednotková*, jestliže je diagonální a $A^i_i = 1$ pro každé $i$ (označujeme ji $E_n$ nebo jen $E$),
- *nulová*, jestliže má všechny prvky nulové (označujeme ji $0_{m\times n}$ nebo jen 0),
- *horní* resp. *dolní trojúhelníková* (nebo v *horním* resp. *dolním trojúhelníkovém tvaru*), jestliže je čtvercová a pod resp. nad diagonálou má jen nuly, tedy $A^i_j = 0$ pro $i > j$ resp. pro $i < j$,
- *schodovitá* (nebo ve *schodovitém tvaru*), jestliže každý nenulový řádek, kromě prvního, začíná zleva více nulami než řádek předchozí,
- v *Gaussově–Jordanově tvaru*, jestliže
  (i) je ve schodovitém tvaru,
  (ii) první (zleva) nenulové prvky všech nenulových řádků jsou 1,
  (iii) ve sloupcích nad (a nejen pod) prvními nenulovými prvky všech nenulových řádků jsou jen 0,
- v *Gaussově kanonickém tvaru*, jestliže je rovna matici

  $$\begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix},$$

  kde $E$ je jednotková matice a 0 označují nulové matice příslušných typů,

- *blokově diagonální*, jestliže je rovna matici
$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix},$$
kde $k > 1$, $A_1, \ldots, A_k$ jsou čtvercové matice (bloky) a 0 označují nulové matice příslušných typů.

Množinu všech matic typu $m \times n$ nad polem $P$ označujeme $\mathcal{M}_{m\times n}(P)$ nebo $P^{m\times n}$; v případě čtvercových matic také $\mathcal{M}_n(P)$ nebo $\mathrm{gl}(n, P)$.

**Příklad.** (1)

$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ je čtvercová matice, $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ není čtvercová matice.

(2)

$\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$ je diagonální matice, $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ není diagonální není.

(3)

$E_1 = (1), E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ jsou jednotkové matice.

(4)

$0_{2\times 2} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, 0_{2\times 3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ jsou nulové matice.

(5)

$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ je horní trojúhelníková matice,

$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 2 & 1 \end{pmatrix}$ je dolní trojúhelníková matice.

(6)

$\begin{pmatrix} 1 & 2 & 1 & 2 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ je matice ve schodovitém tvaru,

$\begin{pmatrix} 1 & 2 & 1 & 2 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 6 \end{pmatrix}$ není matice ve schodovitém tvaru.

(7)

$$\begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ je matice v Gaussově–Jordanově tvaru,}$$

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ není matice v Gaussově–Jordanově tvaru.}$$

(8)

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 5 & 6 \end{pmatrix} \text{ je blokově diagonální matice,}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 3 \end{pmatrix} \text{ není blokově diagonální matice.} \qquad \square$$

## 1.2. Operace s maticemi

### 1.2.1. Součet matic a násobek matice

**Definice 1.2.1.** Buďte $A, B$ matice typu $m \times n$ nad polem $P$. *Součet* matic $A, B$ je matice $A + B$ typu $m \times n$ nad polem $P$ taková, že pro všechna $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$

$$(A + B)^i_j = A^i_j + B^i_j.$$

Sčítáme tedy jen matice stejného typu. Matice různých typů nelze sčítat.

**Definice 1.2.2.** Buďte $A$ matice typu $m \times n$ nad polem $P$ a $c \in P$. Potom *c-násobek* matice $A$ je matice $cA$ typu $m \times n$ nad polem $P$ taková, že pro všechna $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$

$$(cA)^i_j = cA^i_j.$$

Pro $c = -1$ se matice $(-1)A$ značí $-A$ a nazývá se *opačná* matice k matici $A$.

**Příklad.** Pro

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \text{ a } B = \begin{pmatrix} -1 & 0 & 2 \\ 1 & -3 & 7 \end{pmatrix} \text{ je}$$

$$A + B = \begin{pmatrix} 1 + (-1) & 2 + 0 & 3 + 2 \\ 4 + 1 & 5 + (-3) & 6 + 7 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 5 \\ 5 & 2 & 13 \end{pmatrix},$$

$$6A = \begin{pmatrix} 6 & 12 & 18 \\ 24 & 30 & 36 \end{pmatrix}, \quad -B = \begin{pmatrix} 1 & 0 & -2 \\ -1 & 3 & -7 \end{pmatrix}. \qquad \square$$

**Cvičení.** Spočtěte

$$\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}+\begin{pmatrix}2 & 1\\ 0 & -1\end{pmatrix} \qquad \begin{pmatrix}2 & 1\\ 0 & -1\end{pmatrix}+\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$$
$$\begin{pmatrix}3 & 1\\ 0 & 0\end{pmatrix}+\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} \qquad \begin{pmatrix}0 & 0\\ -2 & 1\end{pmatrix}+\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$$
$$\begin{pmatrix}0 & -1\\ 0 & 1\end{pmatrix}+\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} \qquad \begin{pmatrix}1 & 0\\ -2 & 0\end{pmatrix}+\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$$
$$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} \qquad \begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}+\begin{pmatrix}-1 & -2\\ -3 & -4\end{pmatrix}.$$ □

**Tvrzení 1.2.1.** *Nechť $A, B, C$ jsou matice stejného typu nad polem $P$ a $c, k \in P$. Pak*

*(1)* $A + B = B + A$,
*(2)* $A + (B + C) = (A + B) + C$,
*(3)* $A + 0 = A$,
*(4)* $A + (-A) = 0$,
*(5)* $1A = A$,
*(6)* $c(A + B) = cA + cB$,
*(7)* $(c + k)A = cA + kA$,
*(8)* $c(kA) = (ck)A$.

*Důkaz.* Uvedeme jen důkaz bodů (2) a (6), ostatní ponecháme jako cvičení.

(2) Máme dokázat, že matice $A+(B+C)$ se rovná matici $(A+B)+C$. Předpokládejme, že $A, B, C$ jsou typu $m \times n$. Potom i $B+C$ a $A+B$ jsou typu $m \times n$, a tedy i $A+(B+C)$ a $(A + B) + C$ jsou typu $m \times n$.

Pro každé $i \in \{1, 2, \ldots, m\}$ a $j \in \{1, 2, \ldots, n\}$ prvek v $i$-tém řádku a $j$-tém sloupku matice $A + (B + C)$ je

$$\begin{aligned}
(A + (B + C))^i_j &= && \text{(podle definice součtu matic)}\\
&= A^i_j + (B + C)^i_j = && \text{(podle definice součtu matic)}\\
&= A^i_j + (B^i_j + C^i_j) = && \text{(díky asociativitě sčítání v poli)}\\
&= (A^i_j + B^i_j) + C^i_j = && \text{(podle definice součtu matic)}\\
&= (A + B)^i_j + C^i_j = && \text{(podle definice součtu matic)}\\
&= ((A + B) + C)^i_j,
\end{aligned}$$

což je prvek v $i$-tém řádku a $j$-tém sloupku matice $(A + B) + C$.

Dokázali jsme, že matice $A+(B+C)$ a $(A+B)+C$ jsou stejného typu a na stejných místech mají stejné prvky.

(6) Máme dokázat, že matice $c(A + B)$ se rovná matici $cA + cB$. Předpokládejme, že $A, B$ jsou typu $m \times n$. Potom i $A + B$, $cA$ a $cB$ jsou typu $m \times n$, a tedy i $c(A + B)$ a $cA + cB$ jsou typu $m \times n$.

Pro každé $i \in \{1, 2, \ldots, m\}$ a $j \in \{1, 2, \ldots, n\}$ prvek v $i$-tém řádku a $j$-tém sloupku matice $c(A + B)$ je

$$\begin{aligned}
(c(A + B))^i_j &= && \text{(podle definice } c\text{-násobku matice)}\\
&= c(A + B)^i_j = && \text{(podle definice součtu matic)}\\
&= c(A^i_j + B^i_j) = && \text{(díky distributivnímu zákonu v poli)}\\
&= cA^i_j + cB^i_j = && \text{(podle definice } c\text{-násobku matice)}\\
&= (cA)^i_j + (cB)^i_j = && \text{(podle definice součtu matic)}\\
&= (cA + cB)^i_j,
\end{aligned}$$

což je prvek v $i$-tém řádku a $j$-tém sloupku matice $cA + cB$.

Dokázali jsme, že matice $c(A+B)$ a $cA+cB$ jsou stejného typu a na stejných místech mají stejné prvky. □

Uvedli jsme si, že řádky a sloupky matice chápeme jako matice. Můžeme je tedy také násobit prvky příslušného pole, můžeme sčítat řádky a sčítat sloupky, jsou-li stejného typu a nad stejným polem.

Následující definici formulujeme pouze pro řádky matice, ale obdobně lze formulovat pro sloupky, uspořádané $n$-tice a matice.

**Definice 1.2.3.** Buďte $A^{i_1}_\circ, A^{i_2}_\circ, \dots, A^{i_k}_\circ$ řádky matice nad polem $P$, $c_1, c_2, \dots, c_k \in P$. *Lineární kombinace* řádků $A^{i_1}_\circ, A^{i_2}_\circ, \dots, A^{i_k}_\circ$ s *koeficienty* $c_1, c_2, \dots, c_k$ je řádek

$$c_1 A^{i_1}_\circ + c_2 A^{i_2}_\circ + \cdots + c_k A^{i_k}_\circ = \sum_{j=1}^{k} c_j A^{i_j}_\circ .$$

Máme-li prázdnou množinu řádků (tedy, nemáme žádný řádek), jejich lineární kombinaci definujeme jako nulový řádek. Takže, nulový řádek je lineární kombinací řádků z prázdné množiny.

**Příklad.** Mějme

$$A = \begin{pmatrix} 3 & 2 & 1 & 0 \\ -1 & 0 & 1 & -1 \\ 0 & 2 & -1 & 0 \\ 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 2 \\ 1 & -1 & 2 & 1 \end{pmatrix}, \qquad \text{tedy} \qquad \begin{aligned} A^1_\circ &= \begin{pmatrix} 3 & 2 & 1 & 0 \end{pmatrix} \\ A^2_\circ &= \begin{pmatrix} -1 & 0 & 1 & -1 \end{pmatrix} \\ A^3_\circ &= \begin{pmatrix} 0 & 2 & -1 & 0 \end{pmatrix} \\ A^4_\circ &= \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix} \\ A^5_\circ &= \begin{pmatrix} -1 & 0 & 1 & 2 \end{pmatrix} \\ A^6_\circ &= \begin{pmatrix} 1 & -1 & 2 & 1 \end{pmatrix}. \end{aligned}$$

Pro $A^1_\circ, A^3_\circ, A^6_\circ$ a $c_1 = 2, c_2 = -1, c_3 = 2$ dostaneme

$$\begin{aligned} &c_1 A^1_\circ + c_2 A^3_\circ + c_3 A^6_\circ = \\ &\quad = 2 \cdot \begin{pmatrix} 3 & 2 & 1 & 0 \end{pmatrix} + (-1) \cdot \begin{pmatrix} 0 & 2 & -1 & 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 1 & -1 & 2 & 1 \end{pmatrix} = \\ &\quad = \begin{pmatrix} 6 & 4 & 2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -2 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 2 & -2 & 4 & 2 \end{pmatrix} = \\ &\quad = \begin{pmatrix} 8 & 0 & 7 & 2 \end{pmatrix}. \end{aligned}$$ □

### 1.2.2. Součin

**Definice 1.2.4.** Buďte $A$ matice typu $m \times n$ a $B$ matice typu $n \times p$ nad polem $P$. *Součin* matic $A, B$ (v tomto pořadí) je matice $A \cdot B$ (obvykle označovaná jen $AB$) typu $m \times p$ nad polem $P$ taková, že pro všechna $i \in \{1, 2, \dots, m\}$, $j \in \{1, 2, \dots, p\}$

$$(AB)^i_j = A^i_1 B^1_j + A^i_2 B^2_j + \cdots + A^i_n B^n_j = \sum_{k=1}^{n} A^i_k B^k_j .$$

Matice $B$ má tedy tolik řádků, kolik má matice $A$ sloupků. Prvek matice $AB$ v $i$-tém řádku a $j$-tém sloupku získáme tedy tak, že sečteme součiny prvků v $i$-tém řádku matice

$A$ s odpovídajícími prvky v $j$-tém sloupku matice $B$. Tedy

$$AB = \begin{pmatrix} A_1^1B_1^1 + A_2^1B_1^2 + \cdots + A_n^1B_1^n & \cdots & A_1^1B_p^1 + A_2^1B_p^2 + \cdots + A_n^1B_p^n \\ A_1^2B_1^1 + A_2^2B_1^2 + \cdots + A_n^2B_1^n & \cdots & A_1^2B_p^1 + A_2^2B_p^2 + \cdots + A_n^2B_p^n \\ \vdots & & \vdots \\ A_1^mB_1^1 + A_2^mB_1^2 + \cdots + A_n^mB_1^n & \cdots & A_1^mB_p^1 + A_2^mB_p^2 + \cdots + A_n^mB_p^n \end{pmatrix} =$$

$$= \begin{pmatrix} A_1^1B_\circ^1 + A_2^1B_\circ^2 + \cdots + A_n^1B_\circ^n \\ A_1^2B_\circ^1 + A_2^2B_\circ^2 + \cdots + A_n^2B_\circ^n \\ \vdots \\ A_1^mB_\circ^1 + A_2^mB_\circ^2 + \cdots + A_n^mB_\circ^n \end{pmatrix} =$$

$$= \begin{pmatrix} A_\circ^1B \\ A_\circ^2B \\ \vdots \\ A_\circ^mB \end{pmatrix} =$$

$$= \begin{pmatrix} B_1^1A_1^\circ + B_1^2A_2^\circ + \cdots + B_1^nA_n^\circ & \cdots & B_p^1A_1^\circ + B_p^2A_2^\circ + \cdots + B_p^nA_n^\circ \end{pmatrix} =$$

$$= \begin{pmatrix} AB_1^\circ & AB_2^\circ & \cdots & AB_p^\circ \end{pmatrix}.$$

Čili, první řádek matice $AB$ získáme tak, že vezmeme $A_1^1$-násobek řádku $B_\circ^1$, $A_2^1$-násobek řádku $B_\circ^2$, …, $A_n^1$-násobek řádku $B_\circ^n$ a všechny tyto násobky sečteme. Je to tedy lineární kombinace řádků matice $B$ s koeficienty z prvního řádku matice $A$, jinými slovy, součin prvního řádku matice $A$, řádek je matice typu $1 \times n$, a matice $B$.

Obdobně získáme ostatní řádky matice $AB$. Obecně, $i$-tý řádek matice $AB$ získáme tak, že pro každé $k \in \{1, 2, \ldots, n\}$ prvkem $A_k^i$ vynásobíme $k$-tý řádek matice $B$ a všechny tyto násobky sečteme. Takže $i$-tý řádek matice $AB$ je lineární kombinace řádků matice $B$ s koeficienty z $i$-tého řádku matice $A$, jinými slovy, součin $i$-tého řádku matice $A$, řádek je matice typu $1 \times n$, a matice $B$.

Analogicky, první sloupek matice $AB$ získáme tak, že vezmeme $B_1^1$-násobek sloupku $A_1^\circ$, $B_1^2$-násobek sloupku $A_2^\circ$, …, $B_1^n$-násobek sloupku $A_n^\circ$ a všechny tyto násobky sečteme. Je to tedy lineární kombinace sloupků matice $A$ s koeficienty z prvního sloupku matice $B$, jinými slovy, součin matice $A$ a prvního sloupku matice $B$, sloupek je matice typu $n \times 1$.

Obdobně získáme ostatní sloupky matice $AB$. Obecně, $j$-tý sloupek matice $AB$ získáme tak, že pro každé $k \in \{1, 2, \ldots, n\}$ prvkem $B_j^k$ vynásobíme $k$-tý sloupek matice $A$ a všechny tyto násobky sečteme. Takže $j$-tý sloupek matice $AB$ je lineární kombinace sloupků matice $A$ s koeficienty z $j$-tého sloupku matice $B$, jinými slovy, součin matice $A$ a $j$-tého sloupku matice $B$, sloupek je matice typu $n \times 1$.

Nejsou-li typy matic v uvedeném vztahu (druhá má tolik řádků, kolik má první sloupků), nelze je (v daném pořadí) násobit, příslušný součin neexistuje.

**Příklad.** (1) Pro

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \; B = \begin{pmatrix} -1 & 0 \\ 1 & 2 \end{pmatrix} \text{ je}$$

$$
\begin{aligned}
AB &= \begin{pmatrix} 1 & 4 \\ 1 & 8 \end{pmatrix} = \\
&= \begin{pmatrix} 1\cdot(-1)+2\cdot 1 & 1\cdot 0+2\cdot 2 \\ 3\cdot(-1)+4\cdot 1 & 3\cdot 0+4\cdot 2 \end{pmatrix} = \\
&= \begin{pmatrix} 1\cdot\begin{pmatrix}-1 & 0\end{pmatrix}+2\cdot\begin{pmatrix}1 & 2\end{pmatrix} \\ 3\cdot\begin{pmatrix}-1 & 0\end{pmatrix}+4\cdot\begin{pmatrix}1 & 2\end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix}-1 & 0\end{pmatrix}+\begin{pmatrix}2 & 4\end{pmatrix} \\ \begin{pmatrix}-3 & 0\end{pmatrix}+\begin{pmatrix}4 & 8\end{pmatrix} \end{pmatrix} = \\
&= \begin{pmatrix} \begin{pmatrix}1 & 2\end{pmatrix}\cdot\begin{pmatrix}-1 & 0\\ 1 & 2\end{pmatrix} \\ \begin{pmatrix}3 & 4\end{pmatrix}\cdot\begin{pmatrix}-1 & 0\\ 1 & 2\end{pmatrix} \end{pmatrix} = \\
&= \begin{pmatrix} -1\cdot\begin{pmatrix}1\\3\end{pmatrix}+1\cdot\begin{pmatrix}2\\4\end{pmatrix} & 0\cdot\begin{pmatrix}1\\3\end{pmatrix}+2\cdot\begin{pmatrix}2\\4\end{pmatrix} \end{pmatrix} = \\
&= \begin{pmatrix} \begin{pmatrix}-1\\-3\end{pmatrix}+\begin{pmatrix}2\\4\end{pmatrix} & \begin{pmatrix}0\\0\end{pmatrix}+\begin{pmatrix}4\\8\end{pmatrix} \end{pmatrix} = \\
&= \left( \begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}\cdot\begin{pmatrix}-1\\1\end{pmatrix} \quad \begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}\cdot\begin{pmatrix}0\\2\end{pmatrix} \right),
\end{aligned}
$$

$$
\begin{aligned}
BA &= \begin{pmatrix} -1 & -2 \\ 7 & 10 \end{pmatrix} = \\
&= \begin{pmatrix} (-1)\cdot 1+0\cdot 3 & (-1)\cdot 2+0\cdot 4 \\ 1\cdot 1+2\cdot 3 & 1\cdot 2+2\cdot 4 \end{pmatrix} = \\
&= \begin{pmatrix} -1\cdot\begin{pmatrix}1 & 2\end{pmatrix}+0\cdot\begin{pmatrix}3 & 4\end{pmatrix} \\ 1\cdot\begin{pmatrix}1 & 2\end{pmatrix}+2\cdot\begin{pmatrix}3 & 4\end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix}-1 & -2\end{pmatrix}+\begin{pmatrix}0 & 0\end{pmatrix} \\ \begin{pmatrix}1 & 2\end{pmatrix}+\begin{pmatrix}6 & 8\end{pmatrix} \end{pmatrix} = \\
&= \begin{pmatrix} \begin{pmatrix}-1 & 0\end{pmatrix}\cdot\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix} \\ \begin{pmatrix}1 & 2\end{pmatrix}\cdot\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix} \end{pmatrix} = \\
&= \begin{pmatrix} 1\cdot\begin{pmatrix}-1\\1\end{pmatrix}+3\cdot\begin{pmatrix}0\\2\end{pmatrix} & 2\cdot\begin{pmatrix}-1\\1\end{pmatrix}+4\cdot\begin{pmatrix}0\\2\end{pmatrix} \end{pmatrix} = \\
&= \begin{pmatrix} \begin{pmatrix}-1\\1\end{pmatrix}+\begin{pmatrix}0\\6\end{pmatrix} & \begin{pmatrix}-2\\2\end{pmatrix}+\begin{pmatrix}0\\8\end{pmatrix} \end{pmatrix} = \\
&= \left( \begin{pmatrix}-1 & 0\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}1\\3\end{pmatrix} \quad \begin{pmatrix}-1 & 0\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}2\\4\end{pmatrix} \right).
\end{aligned}
$$

(2) Pro

$$
\begin{aligned}
&A = \begin{pmatrix}1 & 2\end{pmatrix},\ B = \begin{pmatrix}0\\3\end{pmatrix} \text{ je} \\
&AB = \begin{pmatrix}1\cdot 0+2\cdot 3\end{pmatrix} = \begin{pmatrix}6\end{pmatrix}, \\
&BA = \begin{pmatrix}0\cdot 1 & 0\cdot 2\\ 3\cdot 1 & 3\cdot 2\end{pmatrix} = \begin{pmatrix}0 & 0\\ 3 & 6\end{pmatrix}.
\end{aligned}
$$

(3) Pro

$$A = \begin{pmatrix}1 & 2\end{pmatrix},\ B = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \text{ je } AB = \begin{pmatrix}2 & 1\end{pmatrix},\ BA \text{ neexistuje.} \qquad \square$$

Předcházející příklady ukazují, že násobení matic není komutativní, tedy nemusí platit $AB = BA$.

**Cvičení.** Spočtěte

$$\begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}2&1\\0&-1\end{pmatrix} \qquad \begin{pmatrix}2&1\\0&-1\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix}$$

$$\begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}1\\0\end{pmatrix} \qquad \begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}0\\1\end{pmatrix}$$

$$\begin{pmatrix}1&0\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix} \qquad \begin{pmatrix}0&1\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix}$$

$$\begin{pmatrix}0&0\\-2&1\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix} \qquad \begin{pmatrix}3&1\\0&0\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix}$$

$$\begin{pmatrix}0&-1\\0&1\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix} \qquad \begin{pmatrix}1&0\\-2&0\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix}$$

$$\begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}0&-1\\0&1\end{pmatrix} \qquad \begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}1&0\\-2&0\end{pmatrix}$$

$$\begin{pmatrix}0&0\\0&0\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix} \qquad \begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

$$\begin{pmatrix}1&0\\2&3\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix} \qquad \begin{pmatrix}0&1\\2&3\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}$$

$$\begin{pmatrix}2&3\\1&0\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix} \qquad \begin{pmatrix}2&3\\0&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}$$

$$\begin{pmatrix}1&2\\3&4\\5&6\end{pmatrix}\cdot\begin{pmatrix}1&2\\0&3\end{pmatrix} \qquad \begin{pmatrix}1&2\\3&4\\5&6\end{pmatrix}\cdot\begin{pmatrix}0&2\\1&3\end{pmatrix}$$

$$\begin{pmatrix}1&2\\3&4\\5&6\end{pmatrix}\cdot\begin{pmatrix}2&1\\3&0\end{pmatrix} \qquad \begin{pmatrix}1&2\\3&4\\5&6\end{pmatrix}\cdot\begin{pmatrix}2&0\\3&1\end{pmatrix}$$

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix} \qquad \begin{pmatrix}0&1\\1&0\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}$$

$$\begin{pmatrix}1&2\\3&4\\5&6\end{pmatrix}\cdot\begin{pmatrix}1&0\\0&1\end{pmatrix} \qquad \begin{pmatrix}1&2\\3&4\\5&6\end{pmatrix}\cdot\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

$$\begin{pmatrix}1&0&0\\2&3&4\\5&6&7\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix} \qquad \begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}\cdot\begin{pmatrix}1&2&0\\3&4&1\\5&6&0\end{pmatrix}$$

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix} \qquad \begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}\cdot\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\0&4&5\\0&0&6\end{pmatrix}\cdot\begin{pmatrix}3&2&1\\0&6&5\\0&0&4\end{pmatrix} \qquad \begin{pmatrix}1&0&0\\2&3&0\\4&5&6\end{pmatrix}\cdot\begin{pmatrix}6&0&0\\4&5&0\\3&2&1\end{pmatrix}$$

$$\begin{pmatrix}1&0&0\\0&2&3\\0&4&5\end{pmatrix}\cdot\begin{pmatrix}5&0&0\\0&4&3\\0&2&1\end{pmatrix} \qquad \begin{pmatrix}1&2&0\\3&4&0\\0&0&5\end{pmatrix}\cdot\begin{pmatrix}5&4&0\\3&2&0\\0&0&1\end{pmatrix}$$

$$\begin{pmatrix}1&0&0&0\\0&2&3&4\\0&5&6&7\\0&8&9&0\end{pmatrix}\cdot\begin{pmatrix}2&0&0&0\\0&3&4&5\\0&6&7&8\\0&9&0&1\end{pmatrix} \qquad \begin{pmatrix}1&2&0&0\\3&4&0&0\\0&0&5&4\\0&0&3&2\end{pmatrix}\cdot\begin{pmatrix}4&3&0&0\\2&1&0&0\\0&0&1&4\\0&0&2&3\end{pmatrix}$$

$$\begin{pmatrix}1&0&0&0\\0&2&3&0\\0&4&5&0\\0&0&0&6\end{pmatrix}\cdot\begin{pmatrix}2&0&0&0\\0&3&4&0\\0&5&1&0\\0&0&0&6\end{pmatrix} \qquad \begin{pmatrix}1&0&0&0\\0&2&0&0\\0&0&3&0\\0&0&0&4\end{pmatrix}\cdot\begin{pmatrix}5&0&0&0\\0&6&0&0\\0&0&7&0\\0&0&0&8\end{pmatrix}$$

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

$$\begin{pmatrix}0&1\end{pmatrix}\cdot\begin{pmatrix}1\\0\end{pmatrix} \qquad \begin{pmatrix}1\\0\end{pmatrix}\cdot\begin{pmatrix}0&1\end{pmatrix}$$

$$\begin{pmatrix}0&1\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&1\\0&0\end{pmatrix} \qquad \begin{pmatrix}0&1\\1&0\end{pmatrix}\cdot\begin{pmatrix}0&1\\1&0\end{pmatrix}. \qquad \square$$

**Tvrzení 1.2.2.** *(1) Je-li $i$-tý řádek matice $A$ nulový, pak $i$-tý řádek matice $AB$ je nulový.*

*(2) Je-li $j$-tý sloupek matice $B$ nulový, pak $j$-tý sloupek matice $AB$ je nulový.*

*(3) Součin diagonálních matic je diagonální matice.*

*(4) Součin blokově diagonálních matic s bloky stejných typů je blokově diagonální matice s bloky stejných typů.*

*Důkaz.* Uvedeme jen důkaz bodu (4), ostatní ponecháme jako cvičení.

(4) Buďte $A, B$ blokově diagonální matice s bloky $A_1, \dots, A_k$, resp. $B_1, \dots, B_k$ takovými, že pro každé $i$ $A_i, B_i$ jsou stejného typu. $A, B$ jsou tedy čtvercové matice stejného typu a je možné je vzájemně násobit.

$i$-tý řádek matice $A$ je

$$A^i_\circ = \begin{pmatrix}0 & \dots & 0 & A^i_{i_1} & \dots & A^i_{i_m} & 0 & \dots & 0\end{pmatrix},$$

$j$-tý sloupek matice $B$ je

$$B^\circ_j = \begin{pmatrix}0 & \dots & 0 & B^{j_1}_j & \dots & B^{j_n}_j & 0 & \dots & 0\end{pmatrix}^\mathsf{T}.$$

Jsou-li $i, j$ taková, že pozice v $i$-tém řádku a $j$-tém sloupku je mimo bloky $A_1, \dots, A_k$, resp. $B_1, \dots, B_k$, pak buď $i_m > j_1$ nebo $i_1 > j_n$. Jelikož $0 \cdot x = x \cdot 0 = 0$ pro každé $x$ z příslušného pole, viz kapitola 6, v obou případech

$$(AB)^i_j = 0,$$

takže $AB$ je blokově diagonální matice s bloky stejných typů, jakých jsou bloky v maticích $A$ a $B$. $\square$

**Tvrzení 1.2.3.** *Nechť $A, B, C$ jsou matice nad polem $P$ takové, že níže uvedené operace jsou definovány, a $c \in P$. Pak platí*

*(1)* $A(BC) = (AB)C$,
*(2)* $AE = EA = A$,
*(3)* $A(B + C) = AB + AC$,
*(4)* $(A + B)C = AC + BC$,
*(5)* $c(AB) = (cA)B = A(cB)$.

*Důkaz.* Uvedeme jen důkaz bodů (1) a (3), ostatní ponecháme jako cvičení.

(1) Předpokládejme, že $A$ je matice typu $m \times n$, $B$ je matice typu $n \times p$ a $C$ je matice typu $p \times q$. Potom $AB$ je matice typu $m \times p$ a $BC$ je matice typu $n \times q$, takže $A(BC)$ a $(AB)C$ jsou matice typu $m \times q$.

$$
\begin{aligned}
(A(BC))^i_j = & && \text{(podle definice součinu matic)}\\
= \sum_{k=1}^{n} A^i_k (BC)^k_j = & && \text{(podle definice součinu matic)}\\
= \sum_{k=1}^{n} A^i_k \sum_{l=1}^{p} (B^k_l C^l_j) = & && \text{(díky distributivnímu zákonu v poli)}\\
= \sum_{k=1}^{n} \sum_{l=1}^{p} A^i_k (B^k_l C^l_j) = & && \text{(díky asociativitě součinu v poli)}\\
= \sum_{k=1}^{n} \sum_{l=1}^{p} (A^i_k B^k_l) C^l_j = & && \text{(díky komutativitě součtu v poli)}\\
= \sum_{l=1}^{p} \sum_{k=1}^{n} (A^i_k B^k_l) C^l_j = & && \text{(podle definice součinu matic)}\\
= \sum_{l=1}^{p} (AB)^i_l C^l_j = & && \text{(podle definice součinu matic)}\\
= ((AB)C)^i_j. &&
\end{aligned}
$$

(3) Předpokládejme, že $A$ je matice typu $m \times n$ a $B, C$ jsou matice typu $n \times p$. Potom $A(B + C)$ a $AB + AC$ jsou matice typu $m \times p$ a pro každé $i \in \{1, 2, \ldots, m\}$ a $j \in \{1, 2, \ldots, p\}$ platí

$$
\begin{aligned}
(A(B + C))^i_j = & && \text{(podle definice součinu matic)}\\
= \sum_{k=1}^{n} A^i_k (B + C)^k_j = & && \text{(podle definice součtu matic)}\\
= \sum_{k=1}^{n} A^i_k (B^k_j + C^k_j) = & && \text{(díky distributivnímu zákonu v poli)}\\
= \sum_{k=1}^{n} (A^i_k B^k_j + A^i_k C^k_j) = & && \text{(díky komutativitě sčítání v poli)}\\
= \sum_{k=1}^{n} A^i_k B^k_j + \sum_{k=1}^{n} A^i_k C^k_j = & && \text{(podle definice součinu matic)}\\
= (AB)^i_j + (AC)^i_j = & && \text{(podle definice součtu matic)}\\
= (AB + AC)^i_j. && \qquad \square
\end{aligned}
$$

### 1.2.3. Transponování

**Definice 1.2.5.** *Transponovaná* matice k matici $A$ typu $m \times n$ je matice $A^\mathsf{T}$ typu $n \times m$, kde $(A^\mathsf{T})^i_j = A^j_i$ pro všechna $i, j$.

**Příklad.**

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^\mathsf{T} = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$ □

**Tvrzení 1.2.4.** *Nechť $A, B$ jsou matice nad polem $P$ takové, že níže uvedené operace jsou definovány, a $c \in P$. Pak platí*

*(1)* $A = (A^\mathsf{T})^\mathsf{T}$,
*(2)* $(A + B)^\mathsf{T} = A^\mathsf{T} + B^\mathsf{T}$,
*(3)* $(cA)^\mathsf{T} = cA^\mathsf{T}$,
*(4)* $(AB)^\mathsf{T} = B^\mathsf{T}A^\mathsf{T}$.

*Důkaz.* (1) Je-li $A$ typu $m \times n$, potom $A^\mathsf{T}$ je typu $n \times m$ a $(A^\mathsf{T})^\mathsf{T}$ je typu $m \times n$. Navíc pro každé $i \in \{1, 2, \ldots, m\}$ a $j \in \{1, 2, \ldots, n\}$ platí

$$((A^\mathsf{T})^\mathsf{T})^i_j = (A^\mathsf{T})^j_i = A^i_j.$$

(4) Buďte $A$ matice typu $m \times n$ a $B$ matice typu $n \times p$. Pak $A^\mathsf{T}$ je typu $n \times m$, $B^\mathsf{T}$ je typu $p \times n$, $AB$ je typu $m \times p$ a tedy $(AB)^\mathsf{T}$ i $B^\mathsf{T}A^\mathsf{T}$ jsou typu $p \times m$. Pro každé $i \in \{1, 2, \ldots, p\}$ a $j \in \{1, 2, \ldots, m\}$ platí

$$((AB)^\mathsf{T})^i_j = (AB)^j_i = \sum_{k=1}^{n} A^j_k B^k_i = \sum_{k=1}^{n} B^k_i A^j_k = \sum_{k=1}^{n} (B^\mathsf{T})^i_k (A^\mathsf{T})^k_j =$$
$$= (B^\mathsf{T}A^\mathsf{T})^i_j.$$

Ostatní body jsou ponechány jako cvičení. □

**Cvičení.** Ukažte, že pro libovolné $k \in \mathbb{N}$ a libovolné matice $A_1, \ldots, A_k$ vhodných typů platí $(A_1 \cdots A_k)^\mathsf{T} = A_k^\mathsf{T} \cdots A_1^\mathsf{T}$. □

## 1.3. Elementární úpravy a speciální tvary matic

### 1.3.1. Elementární úpravy

**Definice 1.3.1.** Mějme matici nad polem $P$. *Řádkové elementární úpravy* matice jsou
(1) přičtení $c$-násobku $j$-tého řádku k $i$-tému řádku, kde $c \in P$ a $i \neq j$,
(2) vynásobení $i$-tého řádku nenulovým prvkem $c \in P$,
(3) vzájemná výměna $i$-tého řádku a $j$-tého řádku.
*Sloupkové elementární úpravy* matice definujeme analogicky.

**Cvičení.** Proveďte vzájemnou výměnu dvou řádků pomocí konečně mnoha úprav typů (1) a (2). □

Mějme matici $A$. Přičtením $c$-násobku $j$-tého řádku k $i$-tému řádku změníme $i$-tý řádek na $\begin{pmatrix} A^i_1 + cA^j_1 & A^i_2 + cA^j_2 & \dots & A^i_n + cA^j_n \end{pmatrix}$ a ostatní řádky zůstanou beze změny.

Po vynásobení $i$-tého řádku prvkem $c \in P$ $i$-tý řádek bude $\begin{pmatrix} cA^i_1 & cA^i_2 & \dots & cA^i_n \end{pmatrix}$ a ostatní řádky zůstanou beze změny.

Po vzájemné výměně $i$-tého řádku a $j$-tého řádku $i$-tý řádek bude $\begin{pmatrix} A^j_1 & A^j_2 & \dots & A^j_n \end{pmatrix}$, $j$-tý řádek bude $\begin{pmatrix} A^i_1 & A^i_2 & \dots & A^i_n \end{pmatrix}$ a ostatní řádky zůstanou beze změny.

Sloupkové úpravy fungují analogicky pro sloupky.

**Příklad.** (1) Přičtením 3-násobku prvního řádku k druhému řádku upravíme matici

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \quad \text{na matici} \quad \begin{pmatrix} 1 & 2 & 3 \\ 7 & 11 & 15 \end{pmatrix}.$$

(2) Vzájemnou výměnou prvního sloupku a třetího sloupku upravíme matici

$$\begin{pmatrix} 1 & 2 & 3 \\ 7 & 11 & 15 \end{pmatrix} \quad \text{na matici} \quad \begin{pmatrix} 3 & 2 & 1 \\ 15 & 11 & 7 \end{pmatrix}. \qquad \square$$

Ke všem elementárním úpravám existují úpravy inverzní, které jsou také elementární a upravenou matici převedou zpět na původní matici. Inverzní úpravy k řádkovým úpravám jsou

(1) přičtení $-c$-násobku $j$-tého řádku k $i$-tému řádku,
(2) vynásobení $i$-tého řádku prvkem $c^{-1}$,
(3) vzájemná výměna $i$-tého řádku a $j$-tého řádku.

Inverzní úpravy ke sloupkovým úpravám jsou obdobné.

**Příklad.** (1) Přičtením $-3$-násobku prvního řádku k druhému řádku upravíme matici

$$\begin{pmatrix} 1 & 2 & 3 \\ 7 & 11 & 15 \end{pmatrix} \quad \text{na matici} \quad \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

(2) Vzájemnou výměnou prvního sloupku a třetího sloupku upravíme matici

$$\begin{pmatrix} 3 & 2 & 1 \\ 15 & 11 & 7 \end{pmatrix} \quad \text{na matici} \quad \begin{pmatrix} 1 & 2 & 3 \\ 7 & 11 & 15 \end{pmatrix}. \qquad \square$$

**Definice 1.3.2.** Matice $A, B$ jsou *ekvivalentní*, jestliže $B$ může vzniknout z $A$ konečnou posloupností elementárních úprav. Je-li možné toho dosáhnout pomocí pouze řádkových, resp. sloupkových úprav, matice jsou *řádkově*, resp. *sloupkově ekvivalentní*. V každém případě značíme $A \sim B$.

**Příklad.**

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 6 \\ 2 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 0 \\ 2 & 4 & 6 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 2 \\ 6 & 4 & 2 \end{pmatrix}. \qquad \square$$

**Tvrzení 1.3.1.** *Ekvivalence matic je relace ekvivalence na množině všech matic stejného typu nad stejným polem.*

*Důkaz.* Cvičení. $\square$

### 1.3.2. Schodovitý, Gaussův–Jordanův a Gaussův kanonický tvary matic

Připomeňme si definice z podkapitoly 1.1.

**Definice 1.3.3.** Matice je ve *schodovitém tvaru*, jestliže každý nenulový řádek, kromě prvního řádku, začíná zleva více nulami než řádek předchozí.

To znamená, že všechny řádky pod nulovým řádkem jsou nulové.

**Definice 1.3.4.** Matice je v *Gaussově–Jordanově tvaru*, jestliže

(i) je ve schodovitém tvaru,
(ii) v každém nenulovém řádku první (zleva) nenulový prvek je 1,
(iii) v každém sloupku, ve kterém je první nenulový prvek nějakého řádku, ostatní prvky jsou 0.

**Definice 1.3.5.** *Gaussův kanonický tvar* matice je

$$\begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix},$$

kde $E$ je jednotková matice a 0 označuje nulové matice příslušných typů.

**Příklad.** (1) Nechť

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 3 & 2 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Matice $A$ není ve schodovitém tvaru. Matice $B$ je ve schodovitém tvaru, ale není v Gaussově–Jordanově tvaru. Matice $C$ je v Gaussově–Jordanově tvaru.

(2) Každá nulová matice je ve schodovitém tvaru i v Gaussově–Jordanově tvaru. Nulová matice je v Gaussově kanonickém tvaru právě tehdy, když je čtvercová. □

**Definice 1.3.6.** Mějme nenulovou matici. *Gaussova eliminace* je úprava matice podle následujícího algoritmu.
Buď $i = 1$.

(1) Uvažujme první nenulový sloupek, který má nějaký nenulový prvek v $i$-tém nebo nižším řádku.
(2) Není-li v $i$-tém řádku uvažovaného sloupku nenulový prvek, vyměníme $i$-tý řádek s vhodným nižším řádkem.
(3) V uvažovaném sloupku vynulujeme prvky v řádcích pod $i$-tým řádkem přičtením vhodných násobků $i$-tého řádku.
(4) Vezměme $i$ o 1 větší ($i := i+1$). Existuje-li nenulový sloupek, který má nějaký nenulový prvek v $i$-tém nebo nižším řádku, vraťme se do bodu (1). Jestliže takový sloupek neexistuje, algoritmus končí.

**Tvrzení 1.3.2.** *Každá matice je řádkově ekvivalentní matici ve schodovitém tvaru.*

*Důkaz.* Nulová matice je ve schodovitém tvaru. Libovolnou nenulovou matici upravíme pomocí Gaussovy eliminace. Všechny provedené úpravy jsou řádkové elementární úpravy a z postupu při Gaussově eliminaci vyplývá, že každý nenulový řádek, kromě prvního řádku, začíná více nulami než řádek předchozí. □

Z Tvrzení 1.5.2 a 1.5.3 vyplývá, že počet nenulových řádků v matici získané Gaussovou eliminací je určen jednoznačně, nezávisí na tom, jak byla Gaussova eliminace použita, přesněji, k jaké výměně řádků došlo v bodě (2).

**Definice 1.3.7.** Sloupek matice je *bázový*, jestliže není nulový a není lineární kombinací předchozích sloupků.

Bázové sloupky matice jsou právě ty sloupky, které jsou uvažovány v bodě (1) v Gaussově eliminaci.

Pozice (indexy) bázových sloupků v matici jsou maticí určeny jednoznačně.

**Definice 1.3.8.** Mějme nenulovou matici. *Gaussova–Jordanova eliminace* je úprava matice podle následujícího algoritmu.
Buď $i = 1$.

(1) Uvažujme první nenulový sloupek, který má nějaký nenulový prvek v $i$-tém nebo nižším řádku.
(2) Není-li v $i$-tém řádku uvažovaného sloupku nenulový prvek, vyměníme $i$-tý řádek s vhodným nižším řádkem.
(3) $i$-tý řádek vynásobíme převrácenou hodnotou jeho prvního nenulového prvku.
(4) V uvažovaném sloupku vynulujeme prvky mimo $i$-tý řádek přičtením vhodných násobků $i$-tého řádku.
(5) Vezměme $i$ o 1 větší ($i := i + 1$). Existuje-li nenulový sloupek, který má nějaký nenulový prvek v $i$-tém nebo nižším řádku, vraťme se do bodu (1). Jestliže takový sloupek neexistuje, algoritmus končí.

Gaussovu-Jordanovu eliminaci je možné ekvivalentně definovat i tak, že matici upravíme pomocí Gaussovy eliminace (na schodovitý tvar), každý nenulový řádek vynásobíme převrácenou hodnotou jeho prvního nenulového prvku a vynulujeme všechny prvky nad všemi prvními nenulovými prvky řádků.

**Tvrzení 1.3.3.** *Každá matice je řádkově ekvivalentní matici v Gaussově–Jordanově tvaru.*

*Důkaz.* Nulová matice je v Gaussově–Jordanově tvaru. Libovolnou nenulovou matici upravíme pomocí Gaussovy–Jordanovy eliminace. Všechny provedené úpravy jsou řádkové elementární úpravy a z postupu při Gaussově–Jordanově eliminaci vyplývá, že výsledná matice je v Gaussově–Jordanově tvaru. □

Maticí je jednoznačně určena řádkově ekvivalentní matice v Gaussově-Jordanově tvaru, tedy pro každou matici existuje právě jedna matice v Gaussově-Jordanově tvaru řádkově ekvivalentní původní matici.

**Tvrzení 1.3.4.** *Každá nenulová matice je ekvivalentní matici v Gaussově kanonickém tvaru.*

*Důkaz.* S použitím řádkových i sloupkových elementárních úprav a vhodnou úpravou Gaussovy–Jordanovy eliminace získáme algoritmus, který převádí libovolnou nenulovou matici na ekvivalentní matici v Gaussově kanonickém tvaru. Podrobnosti ponecháme jako cvičení. □

### 1.3.3. Elementární matice

**Definice 1.3.9.** *Elementární matice* jsou:

(1) pro $i \neq j$

$$E^{i,j}(c) = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ & \dots & & \dots & & \dots & \\ 0 & \dots & 1 & \dots & c & \dots & 0 \\ & \dots & & \dots & & \dots & \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ & \dots & & \dots & & \dots & \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \begin{matrix} \\ \\ i\text{-tý řádek} \\ \\ j\text{-tý řádek} \\ \\ \\ \end{matrix}$$

(2) pro $c \neq 0$

$$E^{i}(c) = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 \\ & \dots & & \dots & \\ 0 & \dots & c & \dots & 0 \\ & \dots & & \dots & \\ 0 & \dots & 0 & \dots & 1 \end{pmatrix} \begin{matrix} \\ \\ i\text{-tý řádek} \\ \\ \\ \end{matrix}$$

(3) pro $i \neq j$

$$E^{i,j} = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ & \dots & & \dots & & \dots & \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ & \dots & & \dots & & \dots & \\ 0 & \dots & 1 & \dots & 0 & \dots & 0 \\ & \dots & & \dots & & \dots & \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \begin{matrix} \\ \\ i\text{-tý řádek} \\ \\ j\text{-tý řádek} \\ \\ \\ \end{matrix}$$

Každá elementární matice vznikne z jednotkové matice provedením vhodné řádkové nebo sloupkové elementární úpravy.

Matice $E^{i,j}(c)$ vznikne z jednotkové matice $E$ přičtením $c$-násobku $j$-tého řádku k $i$-tému řádku a od jednotkové matice se liší jen tím, že $(E^{i,j}(c))^i_j = c$, zatímco $E^i_j = 0$.

Matice $E^i(c)$ vznikne z jednotkové matice $E$ vynásobením $i$-tého řádku prvkem $c$ a od jednotkové matice se liší jen tím, že $(E^i(c))^i_i = c$, zatímco $E^i_i = 1$.

Matice $E^{i,j}$ vznikne z jednotkové matice $E$ výměnou $i$-tého řádku a $j$-tého řádku a od jednotkové matice liší jen tím, že $i$-tý a $j$-tý řádky jsou vzájemně vyměněny.

**Lemma 1.3.5.** *Buďte $A, B$ matice.*

*(1) Matice $B$ může vzniknout z matice $A$ pomocí jedné řádkové elementární úpravy právě tehdy, když existuje elementární matice $Q$ taková, že $B = QA$.*

*(2) Matice $B$ může vzniknout z matice $A$ pomocí jedné sloupkové elementární úpravy právě tehdy, když existuje elementární matice $Q$ taková, že $B = AQ$.*

*Důkaz.* Přímým výpočtem lze ověřit, že přičtení $c$-násobku $j$-tého řádku k $i$-tému řádku je totéž co vynásobení maticí $E^{i,j}(c)$ zleva, vynásobení $i$-tého řádku prvkem $c \in P$ je totéž co vynásobení maticí $E^i(c)$ zleva a výměna $i$-tého řádku a $j$-tého řádku je totéž co vynásobení maticí $E^{i,j}$ zleva. Viz také komentář za Definicí 1.2.4 součinu matic. Analogicky pro sloupkové úpravy a násobení zprava. Cvičení. □

**Příklad.** Buďte

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix},\ B_1 = \begin{pmatrix} 7 & 6 & 5 \\ 4 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix},\ B_2 = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 4 \\ 6 & 4 & 2 \end{pmatrix},\ B_3 = \begin{pmatrix} 3 & 2 & 1 \\ 4 & 5 & 4 \\ 1 & 2 & 3 \end{pmatrix}.$$

Potom

$$B_1 = E^{1,3}(2) \cdot A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot A^1_\circ + 2 \cdot A^3_\circ \\ A^2_\circ \\ A^3_\circ \end{pmatrix}$$

$$B_2 = E^3(2) \cdot A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} A^1_\circ \\ A^2_\circ \\ 2 \cdot A^3_\circ \end{pmatrix}$$

$$B_3 = E^{1,3} \cdot A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} A^3_\circ \\ A^2_\circ \\ A^1_\circ \end{pmatrix}. \qquad \square$$

**Lemma 1.3.6.** *Transponované matice k elementárním maticím jsou elementární matice.*

*Důkaz.* Cvičení. $\square$

## 1.4. Inverzní matice

**Definice 1.4.1.** Buď $A$ čtvercová matice. Matice $X$ je *inverzní* k matici $A$, je-li stejného typu a platí

$$AX = XA = E.$$

Inverzní matice k matici $A$ se značí $A^{-1}$. Matice je *invertibilní*, existuje-li matice k ní inverzní.

**Příklad.** (1) Každá jednotková matice $E$ je invertibilní a $E^{-1} = E$.

(2)

$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ je invertibilní, protože $A \cdot A = E$, a tedy $A^{-1} = A$.

(3)

$A = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ není invertibilní, protože pro libovolnou matici $X$ typu $2 \times 2$ $AX$ má druhý řádek nulový a není to tedy jednotková matice.

(4)

$A = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}$ není invertibilní, protože pro libovolnou matici $X$ typu $2 \times 2$ $XA$ má první sloupek nulový a není to tedy jednotková matice.

(5) Nechť

$$A = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \quad \text{a} \quad X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Předpokládejme, že $X$ je inverzní k $A$. Pak $AX = E$, tedy

$$\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Z toho dostaneme rovnosti

$$a - c = 1, \quad b - d = 0, \quad a - c = 0, \quad b - d = 1.$$

Ze třetí rovnosti máme $a = c$ a po dosazení do první rovnosti máme $0 = 1$, což je spor. Z toho vyplývá, že neexistuje matice $X$ taková, že $AX = E$, a matice $A$ tedy není invertibilní.

(6) Žádná nulová matice není invertibilní.

(7) Elementární matice jsou invertibilní a přímým výpočtem lze ověřit (cvičení), že

$$(E^{i,j}(c))^{-1} = E^{i,j}(-c), \qquad (E^i(c))^{-1} = E^i(c^{-1}), \qquad (E^{i,j})^{-1} = E^{i,j}. \qquad \square$$

**Tvrzení 1.4.1.** *Ke každé matici existuje nejvýše jedna inverzní matice.*

*Důkaz.* Předpokládejme, že $X', X''$ jsou inverzní matice k matici $A$. Tedy $AX' = X'A = AX'' = X''A = E$. Potom $X' = EX' = X''AX' = X''E = X''$. $\square$

**Tvrzení 1.4.2.** *Nechť $A, A_1, \ldots, A_n$ jsou invertibilní matice stejného typu. Potom*

*(1) $A_1 \cdot \ldots \cdot A_n$ je invertibilní a $(A_1 \cdot \ldots \cdot A_n)^{-1} = A_n^{-1} \cdot \ldots \cdot A_1^{-1}$;*
*(2) $A^{-1}$ je invertibilní a $(A^{-1})^{-1} = A$;*
*(3) $A^\mathsf{T}$ je invertibilní a $(A^\mathsf{T})^{-1} = (A^{-1})^\mathsf{T}$.*

*Důkaz.* (1) $(A_1 \cdot \ldots \cdot A_n) \cdot (A_n^{-1} \cdot \ldots \cdot A_1^{-1}) = E = (A_n^{-1} \cdot \ldots \cdot A_1^{-1}) \cdot (A_1 \cdot \ldots \cdot A_n)$ a podle definice inverzní matice tedy $(A_1 \cdot \ldots \cdot A_n)^{-1} = A_n^{-1} \cdot \ldots \cdot A_1^{-1}$.

(2) $AA^{-1} = A^{-1}A = E$ a podle definice inverzní matice tedy $(A^{-1})^{-1} = A$.

(3) $AA^{-1} = A^{-1}A = E$, tedy $E = E^\mathsf{T} = (A^{-1}A)^\mathsf{T} = A^\mathsf{T}(A^{-1})^\mathsf{T}$ a $E = (AA^{-1})^\mathsf{T} = (A^{-1})^\mathsf{T}A^\mathsf{T}$ a podle definice inverzní matice $(A^\mathsf{T})^{-1} = (A^{-1})^\mathsf{T}$. $\square$

**Tvrzení 1.4.3.** *Nechť $A, B$ jsou čtvercové matice takové, že $AB = E$. Pak $BA = E$, obě matice $A, B$ jsou invertibilní a jsou vzájemně inverzní ($A = B^{-1}$ a $B = A^{-1}$).*

*Důkaz.* Matici $A$ upravme řádkovými elementárními úpravami na Gaussův–Jordanův tvar $G$, tedy $G = Q_k \ldots Q_1 A$, kde $Q_1, \ldots, Q_k$ jsou elementární matice příslušné provedeným úpravám. Pak $A = Q_1^{-1} \ldots Q_k^{-1} G$ a $AB = Q_1^{-1} \ldots Q_k^{-1} GB = E$. Matice $G$ nemá nulový řádek, protože jinak by matice $GB$ také měla nulový řádek a takovou matici nelze pomocí řádkových elementárních úprav (v tomto případě reprezentovaných maticemi $Q_1^{-1}, \ldots, Q_k^{-1}$) převést na jednotkovou matici (cvičení). Jelikož $G$ je v Gaussově–Jordanově tvaru a nemá nunový řádek, $G = E$. Pak $A = Q_1^{-1} \ldots Q_k^{-1}$ je invertibilní matice jakožto součin invertibilních matic a existuje tedy $A^{-1}$.

Potom $BA = EBA = A^{-1}ABA = A^{-1}EA = A^{-1}A = E$. Jelikož $AB = BA = E$, jsou obě matice $A, B$ invertibilní a jsou vzájemně inverzní. $\square$

Nyní zformulujeme důležité kriterium invertibility.

**Tvrzení 1.4.4.** *Matice je invertibilní právě tehdy, když je řádkově ekvivalentní s jednotkovou maticí.*

*Důkaz.* „⇒“ Nechť $A$ je invertibilní matice. Řádkovými elementárními úpravami ji převeďme na Gaussův–Jordanův tvar $G$, tedy $G = Q_k \ldots Q_1 A$, kde $Q_1, \ldots, Q_k$ jsou elementární matice příslušné provedeným úpravám. Každá z matic $Q_1, \ldots, Q_k, A$ je invertibilní a jejich součin $G$ je také invertibilní. Potom $G$, jakožto invertibilní matice nemá nulový řádek a $G = E$, jelikož $G$ je v Gaussově–Jordanově tvaru. Matice $A$ je tedy řádkově ekvivalentní s jednotkovou maticí.

„⇐“ Předpokládejme, že matice $A$ je řádkově ekvivalentní s jednotkovou maticí $E$, tedy $Q_k \ldots Q_1 A = E$, kde $Q_1, \ldots, Q_k$ jsou vhodné elementární matice. Označme si $Q = Q_k \ldots Q_2 Q_1$, tedy $QA = E$. Podle Tvrzení 1.4.3 je $A$ invertibilní a $A^{-1} = Q$. $\square$

Předchozí tvrzení nám nabízí postup pro výpočet inverzní matice. Podle důkazu totiž $A^{-1} = Q = Q_k \dots Q_2 Q_1 = Q_k \dots Q_2 Q_1 E$, což je matice, která vznikne z jednotkové matice provedením řádkových elementárních úprav odpovídajících násobení elementárními maticemi $Q_1, Q_2, \dots, Q_k$. To jsou stejné úpravy (resp. matice), které převedly $A$ na $E$.

**Výpočet inverzní matice.** K matici $A$ typu $n \times n$ zprava připojíme jednotkovou matici stejného typu a vznikne matice typu $n \times 2n$

$$\left(\begin{array}{cccc|cccc} A_1^1 & A_2^1 & \dots & A_n^1 & 1 & 0 & \dots & 0 \\ A_1^2 & A_2^2 & \dots & A_n^2 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^m & A_2^m & \dots & A_n^m & 0 & 0 & \dots & 1 \end{array}\right).$$

Řádkovými elementárními úpravami ji převedeme na matici, která v levé části má matici $B$ v Gaussově–Jordanově tvaru. Mohou nastat dvě možnosti.

(1) $B = E$. Pak $A$ je invertibilní a v pravé části matice vyjde $A^{-1}$.
(2) $B \neq E$ ($B$ má nulový řádek). Pak $A$ není invertibilní.

**Příklad.** Vypočítejme inverzní matici k matici

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

$$\begin{aligned}
(A|E) &= \left(\begin{array}{ccc|ccc} 0 & 1 & 2 & 1 & 0 & 0 \\ 1 & 2 & 3 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 2 & 3 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \end{array}\right) \sim \\
&\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 2 & 2 & 0 & 1 & -1 \\ 0 & 1 & 2 & 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 1 & -1 \\ 0 & 1 & 2 & 1 & 0 & 0 \end{array}\right) \sim \\
&\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 1 & -1 \\ 0 & 0 & 2 & 2 & -1 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 1 & -1 \\ 0 & 0 & 1 & 1 & -\frac{1}{2} & \frac{1}{2} \end{array}\right) \sim \\
&\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & -1 & 1 & -1 \\ 0 & 0 & 1 & 1 & -\frac{1}{2} & \frac{1}{2} \end{array}\right).
\end{aligned}$$

Takže $A$ je invertibilní a

$$A^{-1} = \begin{pmatrix} -1 & \frac{1}{2} & \frac{1}{2} \\ -1 & 1 & -1 \\ 1 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \quad \text{(ověřte).} \qquad \square$$

**Příklad.** Hledejme inverzní matici k matici

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

$$(A|E) = \left(\begin{array}{ccc|ccc} 0 & 1 & 2 & 1 & 0 & 0 \\ 1 & 2 & 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 1 & 0 & 0 \end{array}\right) \sim$$
$$\sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 0 & 1 & 0 \\ 0 & -3 & -6 & 0 & -2 & 1 \\ 0 & 1 & 2 & 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 1 & 2 & 1 & 0 & 0 \end{array}\right) \sim$$
$$\sim \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & 0 & 1 & -\frac{2}{3} & \frac{1}{3} \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & -\frac{1}{3} & \frac{2}{3} \\ 0 & 1 & 2 & 0 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & 0 & 1 & -\frac{2}{3} & \frac{1}{3} \end{array}\right).$$

Matice $A$ tedy není řádkově ekvivalentní s jednotkovou maticí a není invertibilní. □

**Cvičení.** Pokud existují, spočtěte inverzní matice k maticím

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 5 & 6 & 7 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & -4 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

□

## 1.5. Hodnost matice

### 1.5.1. Lineární nezávislost

Stejně jako v případě lineární kombinace v Definici 1.2.3 následující definice a tvrzení formulujeme pouze pro řádky matice, ale vše lze obdobně formulovat pro sloupky, uspořádané $n$-tice a matice.

**Definice 1.5.1.** Množina řádků $\{A_\circ^{i_1}, A_\circ^{i_2}, \ldots, A_\circ^{i_k}\}$ je *lineárně nezávislá*, jestliže pro libovolné $c_1, c_2, \ldots, c_k \in P$ z rovnosti

$$c_1 A_\circ^{i_1} + c_2 A_\circ^{i_2} + \cdots + c_k A_\circ^{i_k} = 0_\circ \qquad \text{vyplývá} \qquad c_1 = c_2 = \cdots = c_k = 0,$$

tj. nulový řádek získáme jedině takovou lineární kombinací daných řádků, ve které jsou všechny koeficienty rovny nule.
Množina řádků $\{A_\circ^{i_1}, A_\circ^{i_2}, \ldots, A_\circ^{i_k}\}$ je *lineárně závislá*, jestliže není lineárně nezávislá. Tedy, existují $c_1, c_2, \ldots, c_k \in P$ taková, že aspoň jedno z nich je nenulové a přitom

$$c_1 A_\circ^{i_1} + c_2 A_\circ^{i_2} + \cdots + c_k A_\circ^{i_k} = 0_\circ.$$

**Tvrzení 1.5.1.** *Množina řádků je lineárně závislá právě tehdy, když aspoň jeden z nich je lineární kombinací ostatních.*

*Důkaz.* Předpokládejme, že množina řádků $\{A_\circ^{i_1}, A_\circ^{i_2}, \ldots, A_\circ^{i_k}\}$ je lineárně závislá. Existují tedy koeficienty $c_1, c_2, \ldots, c_k \in P$ takové, že aspoň jeden z nich je nenulový (například $c_j$) a $c_1 A_\circ^{i_1} + \cdots + c_j A_\circ^{i_j} + \cdots + c_k A_\circ^{i_k} = 0_\circ$. Potom

$$c_j A_\circ^{i_j} = -c_1 A_\circ^{i_1} - \cdots - c_{j-1} A_\circ^{i_{j-1}} - c_{j+1} A_\circ^{i_{j+1}} - \cdots - c_k A_\circ^{i_k},$$
$$A_\circ^{i_j} = -\frac{c_1}{c_j} A_\circ^{i_1} - \cdots - \frac{c_{j-1}}{c_j} A_\circ^{i_{j-1}} - \frac{c_{j+1}}{c_j} A_\circ^{i_{j+1}} - \cdots - \frac{c_k}{c_j} A_\circ^{i_k}$$

a řádek $A_\circ^{i_j}$ je tedy lineární kombinací ostatních řádků.

Předpokládejme, že například řádek $A_\circ^{i_j}$ je lineární kombinací ostatních řádků, tedy

$$A_\circ^{i_j} = c_1 A_\circ^{i_1} + \cdots + c_{j-1} A_\circ^{i_{j-1}} + c_{j+1} A_\circ^{i_{j+1}} + \cdots + c_k A_\circ^{i_k}.$$

Potom

$$c_1 A_\circ^{i_1} + \cdots + c_{j-1} A_\circ^{i_{j-1}} - A_\circ^{i_j} + c_{j+1} A_\circ^{i_{j+1}} + \cdots + c_k A_\circ^{i_k} = 0_\circ$$

a zároveň $c_j = -1$. Takže množina řádků $\{A_\circ^{i_1}, A_\circ^{i_2}, \ldots, A_\circ^{i_k}\}$ je lineárně závislá. □

**Příklad.** Mějme

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

Nechť

$$\begin{aligned} &c_1 \begin{pmatrix} 0 & 1 & 2 \end{pmatrix} + c_2 \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} + c_3 \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} = \\ &\quad = \begin{pmatrix} c_2 + c_3 & c_1 + 2c_2 & 2c_1 + 3c_2 + c_3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Takže

$$\begin{aligned} c_2 + c_3 &= 0 \\ c_1 + 2c_2 &= 0 \\ 2c_1 + 3c_2 + c_3 &= 0 \end{aligned}$$

a to je možné jedině v případě, že $c_1 = c_2 = c_3 = 0$ (vyřešíme soustavu tří rovnic o třech neznámých $c_1, c_2, c_3$ a získáme jediné, nulové řešení).

Množina řádků matice $A$ je tedy lineárně nezávislá. □

**Příklad.** Mějme

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

Nechť

$$\begin{aligned} &c_1 \begin{pmatrix} 0 & 1 & 2 \end{pmatrix} + c_2 \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} + c_3 \begin{pmatrix} 2 & 1 & 0 \end{pmatrix} = \\ &\quad = \begin{pmatrix} c_2 + 2c_3 & c_1 + 2c_2 + c_3 & 2c_1 + 3c_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Soustava

$$\begin{aligned} c_2 + 2c_3 &= 0 \\ c_1 + 2c_2 + c_3 &= 0 \\ 2c_1 + 3c_2 &= 0 \end{aligned}$$

má kromě nulového i nenulová řešení (například $c_1 = 3$, $c_2 = -2$, $c_3 = 1$). Množina řádků matice $A$ je tedy lineárně závislá. □

**Příklad.** (1) Množina řádků jednotkové matice je lineárně nezávislá. Ověřte.

(2) Množina řádků, z nichž aspoň jeden je nulový, je lineárně závislá. Ověřte.

(3) Jednoprvková množina obsahující řádek $A_\circ^i$ je lineárně nezávislá, jestliže z $cA_\circ^i = 0_\circ$ plyne $c = 0$. Tedy, jednoprvková množina obsahující jeden řádek je lineárně nezávislá, jestliže ten řádek je nenulový, a je lineárně závislá, jestliže ten řádek je nulový.

(4) Množina obsahující jen řádky $A_\circ^{i_1}, A_\circ^{i_2}$ je lineárně závislá právě tehdy, když jeden z řádků je násobkem druhého z řádků (existuje $c \in P$ takové, že $A_\circ^{i_1} = cA_\circ^{i_2}$).

(5) Prázdná množina řádků je lineárně nezávislá. □

### 1.5.2. Hodnost matice

**Definice 1.5.2.** *Hodnost* matice je maximální počet prvků lineárně nezávislé množiny jejích řádků. Hodnost matice $A$ značíme $\operatorname{rank} A$.

Mějme matici $A$ typu $m \times n$ s řádky $A^1_\circ, A^2_\circ, \ldots, A^m_\circ$. Vezmeme všechny možné množiny těchto řádků, čili prázdnou množinu $\emptyset$, jednoprvkové množiny $\{A^1_\circ\}, \{A^2_\circ\}, \ldots, \{A^m_\circ\}$, dvouprvkové množiny $\{A^1_\circ, A^2_\circ\}, \ldots, \{A^{m-1}_\circ, A^m_\circ\}$, $\ldots$, až množinu $\{A^1_\circ, A^2_\circ, \ldots, A^m_\circ\}$. Z těchto množin vybereme ty, které jsou lineárně nezávislé. U každé z nich si poznamenáme počet prvků a maximální z těchto počtů je hodnost matice $A$.

Hodnost matice s $m$ řádky je tedy jedno z čísel $0, 1, \ldots, m$.

**Příklad.** (1) Hodnost matice

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

je rovna 3. Ověřte.

(2) Hodnost matice

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

je rovna 2. Ověřte.

(3) Hodnost nulové matice je rovna 0, hodnost nenulové matice je kladná.

(4) Hodnost diagonální matice je rovna počtu jejích nenulových řádků. □

**Cvičení.** Spočtěte hodnosti matic

$$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 6 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \qquad \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \qquad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 5 & 6 & 7 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & -4 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$ □

**Tvrzení 1.5.2.** *Hodnost matice ve schodovitém tvaru je rovna počtu jejích nenulových řádků.*

*Důkaz.* Buď $A$ matice ve schodovitém tvaru, která má $m$ řádků, z nichž $p$ je nenulových. Množina všech nenulových řádků je lineárně nezávislá (cvičení), takže $\operatorname{rank} A \geq p$. Jestliže $m = p$, hodnost větší být nemůže. Jestliže $m > p$, pak každá množina s více než $p$ řádky obsahuje aspoň jeden nulový řádek, a je tedy lineárně závislá, takže i v tomto případě $\operatorname{rank} A = p$. □

Podle následujícího tvrzení je množina řádků lineárně nezávislá právě tehdy, když je lineárně nezávislá množina řádků vzniklá provedením řádkové nebo sloupkové elementární úpravy původní množiny řádků.

**Tvrzení 1.5.3.** *Buďte $A^1_\circ, A^2_\circ, \dots, A^m_\circ$ řádky. Nechť $B^1_\circ, B^2_\circ, \dots, B^m_\circ$ jsou řádky, které z řádků $A^1_\circ, A^2_\circ, \dots, A^m_\circ$ vzniknou provedením jedné řádkové nebo sloupkové elementární úpravy. Potom množina řádků $\{A^1_\circ, A^2_\circ, \dots, A^m_\circ\}$ je lineárně nezávislá právě tehdy, když množina řádků $\{B^1_\circ, B^2_\circ, \dots, B^m_\circ\}$ je lineárně nezávislá.*

*Důkaz.* (1) Nechť došlo k přičtení $c$-násobku $j$-tého řádku k $i$-tému řádku, kde $i \neq j$. Tedy, $B^i_\circ = A^i_\circ + cA^j_\circ$ a $B^k_\circ = A^k_\circ$ pro $k \neq i$.

Předpokládejme, že $\{A^1_\circ, A^2_\circ, \dots, A^m_\circ\}$ je lineárně nezávislá. Buďte $c_1, \dots, c_m \in P$ takové, že $c_1B^1_\circ + \dots + c_mB^m_\circ = 0_\circ$. Pak

$$\begin{aligned} 0_\circ &= c_1B^1_\circ + \dots + c_mB^m_\circ = \\ &= c_1A^1_\circ + \dots + c_i(A^i_\circ + cA^j_\circ) + \dots + c_jA^j_\circ + \dots + c_mA^m_\circ = \\ &= c_1A^1_\circ + \dots + c_iA^i_\circ + \dots + (c_j + cc_i)A^j_\circ + \dots + c_mA^m_\circ. \end{aligned}$$

Z lineární nezávislosti množiny $\{A^1_\circ, A^2_\circ, \dots, A^m_\circ\}$ vyplývá, že všechny koeficienty poslední lineární kombinace jsou nulové, tj. $c_1 = \dots = c_i = \dots = cc_i + c_j = \dots = c_m = 0$. Z toho dostaneme, že i $c_j = 0$, a množina $\{B^1_\circ, B^2_\circ, \dots, B^m_\circ\}$ je lineárně nezávislá.

Opačná implikace vyplývá z právě dokázané, neboť řádky $A^1_\circ, A^2_\circ, \dots, A^m_\circ$ vzniknou z řádků $B^1_\circ, B^2_\circ, \dots, B^m_\circ$ inverzní úpravou, která je stejného typu.

(2) Nechť došlo k přičtení $c$-násobku $j$-tého sloupku k $i$-tému sloupku, kde $i \neq j$. Pak pro každé $k \in \{1, \dots, m\}$ je $B^k_i = A^k_i + cA^k_j$ a $B^k_l = A^k_l$ pro $l \neq i$. Tedy $B^k_\circ = \begin{pmatrix} A^k_1 & \dots & A^k_i + cA^k_j & \dots & A^k_j & \dots & A^k_n \end{pmatrix}$.

Předpokládejme, že $\{A^1_\circ, A^2_\circ, \dots, A^m_\circ\}$ je lineárně nezávislá. Buďte $c_1, \dots, c_m \in P$ takové, že $c_1B^1_\circ + \dots + c_mB^m_\circ = 0_\circ$. Takže

$$\begin{aligned} &c_1B^1_\circ + \dots + c_mB^m_\circ = \\ &= \begin{pmatrix} \sum_k c_kA^k_1 & \dots & \sum_k c_k(A^k_i + cA^k_j) & \dots & \sum_k c_kA^k_j & \dots & \sum_k c_kA^k_n \end{pmatrix} = \\ &= \begin{pmatrix} \sum_k c_kA^k_1 & \dots & \sum_k c_kA^k_i + c\sum_k c_kA^k_j & \dots & \sum_k c_kA^k_j & \dots & \sum_k c_kA^k_n \end{pmatrix} = \\ &= \begin{pmatrix} 0 & \dots & 0 & \dots & 0 & \dots & 0 \end{pmatrix} \end{aligned}$$

a z toho dostaneme

$$\sum_k c_kA^k_1 = \dots = \sum_k c_kA^k_i = \dots = \sum_k c_kA^k_j = \dots = \sum_k c_kA^k_n = 0.$$

Pak

$$\begin{aligned} &\begin{pmatrix} \sum_k c_kA^k_1 & \sum_k c_kA^k_2 & \dots & \sum_k c_kA^k_n \end{pmatrix} = \sum_k c_k \begin{pmatrix} A^k_1 & A^k_2 & \dots & A^k_n \end{pmatrix} = \\ &= \sum_k c_kA^k_\circ = c_1A^1_\circ + \dots + c_mA^m_\circ = 0_\circ \end{aligned}$$

a z lineární nezávislosti množiny $\{A^1_\circ, A^2_\circ, \dots, A^m_\circ\}$ dostaneme $c_1 = c_2 = \dots = c_m = 0$. Množina $\{B^1_\circ, B^2_\circ, \dots, B^m_\circ\}$ je tedy lineárně nezávislá.

Opačná implikace vyplývá z právě dokázané, neboť řádky $A^1_\circ, A^2_\circ, \dots, A^m_\circ$ vzniknou z řádků $B^1_\circ, B^2_\circ, \dots, B^m_\circ$ inverzní úpravou, která je stejného typu.

Pro ostatní úpravy je důkaz obdobný a ponecháme ho jako cvičení. □

**Důsledek.** *(1) Hodnost matice je rovna hodnosti matice z ní vzniklé provedením elementární úpravy.*

*(2) Provedení konečně mnoha elementárních úprav nemění hodnost.*

*(3) Vynásobení konečně mnoha elementárními maticemi zleva nemění hodnost.*

*(4) Vynásobení konečně mnoha elementárními maticemi zprava nemění hodnost.*

*(5) Ekvivalentní matice mají stejnou hodnost.*

*(6) Hodnost matice je rovna počtu nenulových řádků ekvivalentní matice ve schodovitém tvaru.*

*(7) Hodnost matice je rovna počtu nenulových řádků (sloupků) ekvivalentní matice v Gaussově kanonickém tvaru.*

*(8) Maximální počet prvků lineárně nezávislých množin sloupků matice je roven maximálnímu počtu prvků lineárně nezávislých množin jejích řádků, tj. hodnosti matice.*

*(9)* $\operatorname{rank} A = \operatorname{rank} A^T$.

**Příklad.** Spočítejme hodnost matice

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

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 3 \\ 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Takže $\operatorname{rank} A = 3$. □

**Příklad.** Spočítejme hodnost matice

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

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}.$$

Takže $\operatorname{rank} A = 2$. □

**Definice 1.5.3.** Čtvercová matice je *regulární*, jestliže její hodnost je rovna počtu jejích řádků (tedy množina všech jejích řádků je lineárně nezávislá). Čtvercová matice je *singulární*, jestliže není regulární.

**Příklad.** (1) Všechny jednotkové matice jsou regulární.

(2) Všechny elementární matice jsou regulární.

(3) Všechny čtvercové matice s aspoň jedním nulovým řádkem jsou singulární. □

**Tvrzení 1.5.4.** *Matice je regulární právě tehdy, když je řádkově ekvivalentní s jednotkovou maticí.*

*Důkaz.* Cvičení. □

**Důsledek.** *(1) Matice je invertibilní právě tehdy, když je regulární.*

*(2) Regulární matice je součinem konečně mnoha elementárních matic.*

*(3) Součin regulárních matic je regulární matice.*

*(4) Vynásobení regulární maticí zleva nemění hodnost.*

*(5) Vynásobení regulární maticí zprava nemění hodnost.*

**Tvrzení 1.5.5.** *Buďte $A, B$ čtvercové matice stejného typu. Obě matice $A, B$ jsou regulární právě tehdy, když matice $AB$ je regulární.*

*Důkaz.* „⇒“ Tato implikace je součástí předchozího Důsledku.

„⇐“ Dokážeme, že je-li aspoň jedna z matic $A, B$ singulární, pak $AB$ je singulární. Nechť $A$ je singulární. Ekvivalentní matice $S = Q_k \cdots Q_1 A$, kde $Q_1, \ldots, Q_k$ jsou elementární matice, ve schodovitém tvaru, má nulový řádek. Potom matice $SB$ má také nulový řádek, je tedy singulární a řádkově ekvivalentní matice $AB = Q_1^{-1} \cdots Q_k^{-1} SB$, která má stejnou hodnost, je také singulární.

Pro $B$ singulární je důkaz analogický a ponecháme ho jako cvičení. □

**Tvrzení 1.5.6.** *Buďte $A$ matice typu $m \times n$ a $B$ matice typu $n \times p$. Potom* $\operatorname{rank} AB \leq \min\{\operatorname{rank} A, \operatorname{rank} B\}$.

*Důkaz.* Matici $A$ převedeme pomocí řádkových elementárních úprav na schodovitý tvar $S_A = Q_k \cdots Q_1 A$ a matici $B$ převedeme pomocí sloupkových elementárních úprav na tvar $S_B = B P_1 \cdots P_l$ takový, že $S_B^{\mathsf{T}}$ je ve schodovitém tvaru.

Potom $\operatorname{rank} AB = \operatorname{rank} Q_1^{-1} \cdots Q_k^{-1} S_A S_B P_l^{-1} \cdots P_1^{-1} = \operatorname{rank} S_A S_B$, přičemž matice $S_A S_B$ má minimálně tolik nulových řádků, kolik jich má matice $S_A$, a minimálně tolik nulových sloupků, kolik jich má matice $S_B$. Tedy $\operatorname{rank} S_A S_B \leq \operatorname{rank} S_A = \operatorname{rank} A$ a $\operatorname{rank} S_A S_B \leq \operatorname{rank} S_B = \operatorname{rank} B$. □

**Cvičení.** Co se dá říct o $\operatorname{rank}(A + B)$? □

# 2. Determinant

## 2.1. Permutace

**Definice 2.1.1.** Buď $M$ konečná množina. *Permutace* na množině $M$ je bijekce $M \to M$.

Buď $\sigma$ permutace na množině $M$ a $m \in M$. Obraz $\sigma(m)$ prvku $m$ při permutaci $\sigma$ se často značí $\sigma_m$.

**Definice 2.1.2.** *Transpozice* je permutace, při níž se vzájemně vymění dva prvky a ostatní se nezmění.

**Tvrzení 2.1.1.** *Každá permutace je složením konečně mnoha transpozic.*

Nechť $I_n = \{1, 2, \ldots, n\}$. Množinu všech permutací na množině $I_n$ značíme $S_n$. Permutaci $\sigma \in S_n$ můžeme zapisovat jako uspořádanou $n$-tici obrazů prvků množiny $I_n$, tedy $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$.

**Definice 2.1.3.** Buď $\sigma \in S_n$. Nechť $i, j \in I_n$ jsou takové, že $i < j$ a $\sigma_i > \sigma_j$. Pak dvojice $(\sigma_i, \sigma_j)$ tvoří *inverzi* permutace $\sigma$.

Počet inverzí permutace $\sigma$ značíme $\operatorname{inv}\sigma$. Je zřejmé, že $\operatorname{inv}\sigma = \operatorname{inv}\sigma^{-1}$.

**Definice 2.1.4.** *Signum (znaménko)* permutace $\sigma \in S_n$ je $\operatorname{sgn}\sigma = (-1)^{\operatorname{inv}\sigma}$. Permutace s $\operatorname{sgn}\sigma = 1$ je *sudá*, permutace s $\operatorname{sgn}\sigma = -1$ je *lichá*.

Jelikož $\operatorname{inv}\sigma = \operatorname{inv}\sigma^{-1}$, $\operatorname{sgn}\sigma = \operatorname{sgn}\sigma^{-1}$.

**Tvrzení 2.1.2.** *Buďte $\rho, \sigma \in S_n$. Pak* $\operatorname{sgn}(\pi \circ \rho) = \operatorname{sgn}\pi \cdot \operatorname{sgn}\rho$.

**Cvičení.** Ukažte, že každá transpozice je lichá permutace. □

Více o permutacích lze najít například v [Marvan, 4. Permutace].

## 2.2. Determinant

### 2.2.1. Definice a determinanty některých typů matic

**Definice 2.2.1.** Buď $A$ matice typu $n \times n$ nad polem $P$. *Determinant* matice $A$ je

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma \cdot A^1_{\sigma_1} A^2_{\sigma_2} \cdots A^n_{\sigma_n} \in P.$$

Číslo $n$ je *řád* determinantu.

Pro determinant matice $A$ se používá značení

$$\det A = |A| = \det \begin{pmatrix} A^1_1 & A^1_2 & \ldots & A^1_n \\ A^2_1 & A^2_2 & \ldots & A^2_n \\ \vdots & \vdots & & \vdots \\ A^n_1 & A^n_2 & \ldots & A^n_n \end{pmatrix} = \begin{vmatrix} A^1_1 & A^1_2 & \ldots & A^1_n \\ A^2_1 & A^2_2 & \ldots & A^2_n \\ \vdots & \vdots & & \vdots \\ A^n_1 & A^n_2 & \ldots & A^n_n \end{vmatrix}.$$

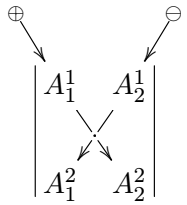
Díky tomu, že $\sigma$ je permutace (bijektivní zobrazení) na množině $I_n$, můžeme ji chápat jako zobrazení z množiny všech řádkových indexů do množiny všech sloupkových indexů

matice $A$. Ke každému řádku je tedy vzájemně jednoznačně přiřazen sloupek a v každém součinu $A^1_{\sigma_1} \cdot A^2_{\sigma_2} \cdots A^n_{\sigma_n}$ je tedy právě jeden prvek z každého řádku a právě jeden prvek z každého sloupku. Determinant matice $A$ je tedy součet všech takovýchto součinů (pro všechny permutace $\sigma$ na množině $I_n$) opatřených buď znaménkem $+$, jde-li o sudou permutaci, nebo znaménkem $-$, jde-li o lichou permutaci.

**Příklad.** (1) Nechť $n = 1$. Tedy, $I_1 = \{1\}$, $S_1 = \{\mathrm{id}\colon \{1\} \to \{1\}\}$ a $\operatorname{sgn} \mathrm{id} = 1$. Pro matici $A = \begin{pmatrix} a \end{pmatrix}$ je $\det A = \operatorname{sgn} \mathrm{id} \cdot A^1_{\mathrm{id}_1} = 1 \cdot A^1_1 = a$.
(2) Nechť $n = 2$. Tedy, $I_2 = \{1, 2\}$, $S_2 = \{\mathrm{id}, \tau\}$, kde $\mathrm{id} = (1, 2)$ a $\tau = (2, 1)$ (viz zápis permutace na $I_n$), $\operatorname{sgn} \mathrm{id} = 1$ a $\operatorname{sgn} \tau = -1$. Pro matici

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

je $\det A = \operatorname{sgn} \mathrm{id} \cdot A^1_{\mathrm{id}_1} A^2_{\mathrm{id}_2} + \operatorname{sgn} \tau \cdot A^1_{\tau_1} A^2_{\tau_2} = 1 \cdot A^1_1 A^2_2 + (-1) \cdot A^1_2 A^2_1 = ad - bc$. Vzorec pro výpočet determinantu matice druhého řádu je možno odvodit z následujícího obrázku:




$$= A^1_1 A^2_2 - A^1_2 A^2_1$$

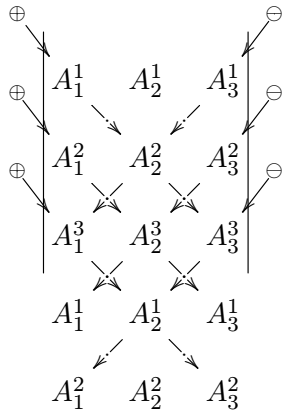
(3) Nechť $n = 3$. Tedy, $I_3 = \{1, 2, 3\}$, $S_3 = \{\mathrm{id}, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$, kde $\mathrm{id} = (1, 2, 3)$, $\sigma_1 = (2, 3, 1)$, $\sigma_2 = (3, 1, 2)$, $\tau_1 = (1, 3, 2)$, $\tau_2 = (3, 2, 1)$, $\tau_3 = (2, 1, 3)$ (viz zápis permutace na $I_n$), $\operatorname{sgn} \mathrm{id} = \operatorname{sgn} \sigma_1 = \operatorname{sgn} \sigma_2 = 1$ a $\operatorname{sgn} \tau_1 = \operatorname{sgn} \tau_2 = \operatorname{sgn} \tau_3 = -1$. Pro matici

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

je

$$\begin{aligned}
\det A = {} & \operatorname{sgn} \mathrm{id} \cdot A^1_{\mathrm{id}_1} A^2_{\mathrm{id}_2} A^3_{\mathrm{id}_3} + \operatorname{sgn} \sigma_1 \cdot A^1_{\sigma_1(1)} A^2_{\sigma_1(2)} A^3_{\sigma_1(3)} + \\
& + \operatorname{sgn} \sigma_2 \cdot A^1_{\sigma_2(1)} A^2_{\sigma_2(2)} A^3_{\sigma_2(3)} + \operatorname{sgn} \tau_1 \cdot A^1_{\tau_1(1)} A^2_{\tau_1(2)} A^3_{\tau_1(3)} + \\
& + \operatorname{sgn} \tau_2 \cdot A^1_{\tau_2(1)} A^2_{\tau_2(2)} A^3_{\tau_2(3)} + \operatorname{sgn} \tau_3 \cdot A^1_{\tau_3(1)} A^2_{\tau_3(2)} A^3_{\tau_3(3)} = \\
= {} & 1 \cdot A^1_1 A^2_2 A^3_3 + 1 \cdot A^1_2 A^2_3 A^3_1 + 1 \cdot A^1_3 A^2_1 A^3_2 + \\
& + (-1) \cdot A^1_1 A^2_3 A^3_2 + (-1) \cdot A^1_3 A^2_2 A^3_1 + (-1) \cdot A^1_2 A^2_1 A^3_3 = \\
= {} & aei + bfg + cdh - afh - ceg - bdi.
\end{aligned}$$

Vzorec pro výpočet determinantu matice třetího řádu lze odvodit z následujího obrázku pomocí *Sarrusova pravidla* (pro matice vyššího řádu žádné takové pravidlo neexistuje):




$$= \quad A_1^1A_2^2A_3^3 + A_2^1A_3^2A_1^3 + A_3^1A_1^2A_2^3 -$$
$$-A_1^1A_3^2A_2^3 - A_3^1A_2^2A_1^3 - A_2^1A_1^2A_3^3$$

(4) Nechť $n = 4$. Na čtyřprvkové množině existují 24 permutace, takže při výpočtu determinantu podle definice dostaneme 24 sčítance. Uvedeme si i jiné způsoby výpočtu determinantu. □

**Cvičení.** Spočtěte determinanty matic

$$\begin{pmatrix}1&2\\3&4\end{pmatrix} \quad \begin{pmatrix}1&3\\2&4\end{pmatrix} \quad \begin{pmatrix}1&2\\3&0\end{pmatrix} \quad \begin{pmatrix}1&2\\0&0\end{pmatrix}$$

$$\begin{pmatrix}1&0\\2&0\end{pmatrix} \quad \begin{pmatrix}1&2\\1&2\end{pmatrix} \quad \begin{pmatrix}1&2\\0&3\end{pmatrix} \quad \begin{pmatrix}1&0\\2&3\end{pmatrix}$$

$$\begin{pmatrix}2&0\\0&3\end{pmatrix} \quad \begin{pmatrix}1&2\\2&2\end{pmatrix} \quad \begin{pmatrix}2&6\\2&4\end{pmatrix} \quad \begin{pmatrix}3&4\\1&2\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\3&4&5\\5&6&7\end{pmatrix} \quad \begin{pmatrix}1&2&3\\2&2&2\\5&6&7\end{pmatrix} \quad \begin{pmatrix}2&4&6\\3&4&5\\5&6&7\end{pmatrix} \quad \begin{pmatrix}3&4&5\\1&2&3\\5&6&7\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\0&0&0\\3&4&5\end{pmatrix} \quad \begin{pmatrix}1&0&1\\2&0&3\\1&0&3\end{pmatrix} \quad \begin{pmatrix}1&0&0\\0&1&2\\0&3&4\end{pmatrix} \quad \begin{pmatrix}1&2&3\\0&1&2\\0&3&4\end{pmatrix}$$

$$\begin{pmatrix}1&2&0\\3&4&0\\0&0&3\end{pmatrix} \quad \begin{pmatrix}1&2&1\\3&4&2\\0&0&3\end{pmatrix} \quad \begin{pmatrix}1&2&3\\4&5&6\\1&2&3\end{pmatrix} \quad \begin{pmatrix}1&2&2\\4&5&5\\7&8&8\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\0&4&5\\0&0&6\end{pmatrix} \quad \begin{pmatrix}1&0&0\\2&3&0\\4&5&6\end{pmatrix} \quad \begin{pmatrix}1&2&0\\0&4&5\\0&0&6\end{pmatrix} \quad \begin{pmatrix}1&2&0\\0&4&0\\0&5&6\end{pmatrix}$$

$$\begin{pmatrix}1&2&0\\0&4&0\\0&0&6\end{pmatrix} \quad \begin{pmatrix}1&0&0\\0&4&0\\0&0&6\end{pmatrix} \quad \begin{pmatrix}1&2&1\\2&1&3\\1&-4&3\end{pmatrix} \quad \begin{pmatrix}1&2&1\\2&1&3\\1&2&3\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\1&0&0\\4&5&6\end{pmatrix} \quad \begin{pmatrix}1&2&3\\0&1&0\\4&5&6\end{pmatrix} \quad \begin{pmatrix}1&2&3\\0&0&1\\4&5&6\end{pmatrix} \quad \begin{pmatrix}1&2&3\\1&1&1\\4&5&6\end{pmatrix}$$

□

**Tvrzení 2.2.1.** *Determinant matice s nulovým řádkem nebo nulovým sloupkem je roven nule.*

*Důkaz.* Buď $A$ matice typu $n \times n$ s nulovým řádkem nebo nulovým sloupkem. Pro každé $\sigma \in S_n$ je v součinu $A^1_{\sigma_1} A^2_{\sigma_2} \cdots A^n_{\sigma_n}$ právě jeden prvek z každého, tedy i nulového řádku a právě jeden prvek z každého, tedy i nulového sloupku. Proto je každý takový součin roven nule. □

**Cvičení.** Dokažte, že pro determinanty lišící se pouze v jednom řádku platí

$$\begin{vmatrix} A^1_1 & \dots & A^1_n \\ & \dots & \\ A^i_1 & \dots & A^i_n \\ & \dots & \\ A^n_1 & \dots & A^n_n \end{vmatrix} + \begin{vmatrix} A^1_1 & \dots & A^1_n \\ & \dots & \\ B^i_1 & \dots & B^i_n \\ & \dots & \\ A^n_1 & \dots & A^n_n \end{vmatrix} = \begin{vmatrix} A^1_1 & \dots & A^1_n \\ & \dots & \\ A^i_1 + B^i_1 & \dots & A^i_n + B^i_n \\ & \dots & \\ A^n_1 & \dots & A^n_n \end{vmatrix}. \qquad \square$$

**Příklad.**

$$\begin{vmatrix} 1 & 2 & 3 \\ 1 & 0 & 0 \\ 4 & 5 & 6 \end{vmatrix} + \begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 4 & 5 & 6 \end{vmatrix} + \begin{vmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 4 & 5 & 6 \end{vmatrix} = 3 + (-6) + 3 = 0 = \begin{vmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 4 & 5 & 6 \end{vmatrix}. \qquad \square$$

**Definice 2.2.2.** Čtvercová matice je (*horní* resp. *dolní*) *trojúhelníková* (nebo v (*horním* resp. *dolním*) *trojúhelníkovém tvaru*), jestliže pod resp. nad diagonálou má jen nuly, tedy $A^i_j = 0$ pro $i > j$ resp. pro $i < j$.

Každá čtvercová matice ve schodovitém tvaru je také v (horním) trojúhelníkovém tvaru a tedy každou čtvercovou matici lze pomocí řádkových elementárních úprav převést na trojúhelníkový tvar.

**Tvrzení 2.2.2.** *Determinant trojúhelníkové matice je roven součinu prvků na diagonále.*

*Důkaz.* Buď $A$ horní trojúhelníková matice typu $n \times n$. Buď $\sigma$ permutace na množině $I_n$. Jestliže pro nějaké $i \in I_n$ platí $\sigma_i < i$, pak $A^i_{\sigma_i}$ je pod diagonálou, tedy $A^i_{\sigma_i} = 0$ a také $\operatorname{sgn}\sigma \cdot A^1_{\sigma_1} \cdots A^i_{\sigma_i} \cdots A^n_{\sigma_n} = 0$. Jediná permutace $\sigma$ taková, že $\sigma_i \geq i$ pro každé $i$, je identita. Jelikož $\operatorname{sgn}\mathrm{id} = 1$, $\det A = A^1_1 A^2_2 \cdots A^n_n$.

Pro dolní trojúhelníkové matice je důkaz analogický. □

**Důsledek.** *(1) Determinant matice ve schodovitém tvaru je roven součinu prvků na diagonále.*

*(2) Determinant diagonální matice je roven součinu prvků na diagonále.*

*(3) Determinant jednotkové matice je roven* 1.

**Příklad.**

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 0 \\ 1 & 2 & 3 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{vmatrix} = 24. \qquad \square$$

Determinanty elementárních matic jsou nenulové.

**Příklad.** (1) $E^{i,j}(c)$ je trojúhelníková matice a na diagonále má jen jedničky, proto

$$\det E^{i,j}(c) = 1.$$

(2) $E^i(c)$ je diagonální matice a na diagonále má jedno $c$ a jinak jen jedničky, proto

$$\det E^i(c) = c.$$

(3) Jelikož v každém řádku a v každém sloupku matice $E^{i,j}$ je právě jedna jednička a ostatní prvky jsou nuly, existuje jediná permutace $\tau$ na $I_n$, pro kterou jsou všechny $(E^{i,j})^1_{\tau_1}, \dots, (E^{i,j})^n_{\tau_n}$ rovny jedné. Pro ostatní permutace je aspoň jeden z těchto prvků nulový. Díky tvaru $E^{i,j}$ je $\tau$ transpozice, takže $\sin\tau = -1$. Proto

$$\det E^{i,j} = (-1)\cdot(E^{i,j})^1_{\tau_1}\cdots(E^{i,j})^n_{\tau_n} = -1. \qquad \square$$

**Tvrzení 2.2.3.** *Pro každou čtvercovou matici $A$ platí* $\det A^{\mathsf{T}} = \det A$.

*Důkaz.* Činitele v součinu $A^{\sigma_1}_1 \dots A^{\sigma_i}_i \dots A^{\sigma_n}_n$ můžeme uspořádat podle vzrůstajícího řádkového indexu $A^1_{\sigma_1^{-1}} \dots A^i_{\sigma_i^{-1}} \dots A^n_{\sigma_n^{-1}}$, protože $\sigma_i^{-1}$-tý činitel v původním součinu je $A^{\sigma_{\sigma_i^{-1}}}_{\sigma_i^{-1}} = A^i_{\sigma_i^{-1}}$. Potom

$$\begin{aligned}
\det A^{\mathsf{T}} &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot (A^{\mathsf{T}})^1_{\sigma_1} \dots (A^{\mathsf{T}})^i_{\sigma_i} \dots (A^{\mathsf{T}})^n_{\sigma_n} = \\
&= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A^{\sigma_1}_1 \dots A^{\sigma_i}_i \dots A^{\sigma_n}_n = && \text{(přeuspořádání)} \\
&= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A^1_{\sigma_1^{-1}} \dots A^i_{\sigma_i^{-1}} \dots A^n_{\sigma_n^{-1}} = && (\operatorname{sgn}\sigma^{-1} = \operatorname{sgn}\sigma) \\
&= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma^{-1} \cdot A^1_{\sigma_1^{-1}} \dots A^i_{\sigma_i^{-1}} \dots A^n_{\sigma_n^{-1}} = \\
&= \det A,
\end{aligned}$$

protože když $\sigma$ projde všechny prvky $S_n$, tak $\sigma^{-1}$ také. $\square$

**Tvrzení 2.2.4.** *Determinant matice, která má buď dva řádky stejné nebo dva sloupky stejné, je roven nule.*

*Důkaz.* Buď $A$ matice typu $n \times n$, která má $i$-tý řádek stejný jako $j$-tý ($i \neq j$), tedy $A^i_k = A^j_k$ pro každé $k \in \{1, 2, \dots, n\}$.

Buď $\tau_{ij} \in S_n$ transpozice vyměňující $i, j$, čili $\operatorname{sgn}\tau_{ij} = -1$. Pro každou permutaci $\sigma \in S_n$ označme $\sigma' = \sigma \circ \tau_{ij}$. Pak $\operatorname{sgn}\sigma' = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau_{ij} = -\operatorname{sgn}\sigma$ a člen determinantu odpovídající permutaci $\sigma'$ je

$$\begin{aligned}
&\operatorname{sgn}\sigma' \cdot A^1_{\sigma'_1} \cdots A^i_{\sigma'_i} \cdots A^j_{\sigma'_j} \cdots A^n_{\sigma'_n} = \\
&\quad = -\operatorname{sgn}\sigma \cdot A^1_{\sigma_1} \cdots A^i_{\sigma_j} \cdots A^j_{\sigma_i} \cdots A^n_{\sigma_n} = && (A^i_{\sigma_j} = A^j_{\sigma_j} \text{ a } A^j_{\sigma_i} = A^i_{\sigma_i}) \\
&\quad = -\operatorname{sgn}\sigma \cdot A^1_{\sigma_1} \cdots A^i_{\sigma_i} \cdots A^j_{\sigma_j} \cdots A^n_{\sigma_n},
\end{aligned}$$

a je tedy opačný k členu odpovídajícímu permutaci $\sigma$.

Množinu $S_n$, která má sudý počet prvků, můžeme rozložit na podmnožiny $\{\sigma, \sigma'\}$, které jsou dvouprvkové, protože $\sigma' \neq \sigma$ a $\sigma'' = \sigma$ (ověřte), a každá z nich přispívá k determinantu nulou. Takže $\det A = 0$.

Když má matice dva stejné sloupky, lze tvrzení dokázat analogicky nebo je možno použít předchozí tvrzení. $\square$

### 2.2.2. Elementární úpravy

**Tvrzení 2.2.5.** *(1) Přičtením násobku jednoho řádku, resp. sloupku k jinému řádku, resp. sloupku se determinant nezmění.*

$$\begin{vmatrix} A_1^1 & A_2^1 & \dots & A_n^1 \\ \vdots & \vdots & & \vdots \\ A_1^i + cA_1^j & A_2^i + cA_2^j & \dots & A_n^i + cA_n^j \\ \vdots & \vdots & & \vdots \\ A_1^n & A_2^n & \dots & A_n^n \end{vmatrix} = \begin{vmatrix} A_1^1 & A_2^1 & \dots & A_n^1 \\ \vdots & \vdots & & \vdots \\ A_1^i & A_2^i & \dots & A_n^i \\ \vdots & \vdots & & \vdots \\ A_1^n & A_2^n & \dots & A_n^n \end{vmatrix}.$$

*(2) Vynásobením jednoho řádku, nebo sloupku prvkem $c$ se determinant vynásobí prvkem $c$.*

$$\begin{vmatrix} A_1^1 & A_2^1 & \dots & A_n^1 \\ \vdots & \vdots & & \vdots \\ cA_1^i & cA_2^i & \dots & cA_n^i \\ \vdots & \vdots & & \vdots \\ A_1^n & A_2^n & \dots & A_n^n \end{vmatrix} = c \begin{vmatrix} A_1^1 & A_2^1 & \dots & A_n^1 \\ \vdots & \vdots & & \vdots \\ A_1^i & A_2^i & \dots & A_n^i \\ \vdots & \vdots & & \vdots \\ A_1^n & A_2^n & \dots & A_n^n \end{vmatrix}.$$

*(3) Vzájemnou výměnou dvou řádků, nebo dvou sloupků determinant změní znaménko.*

$$\begin{vmatrix} A_1^1 & A_2^1 & \dots & A_n^1 \\ \vdots & \vdots & & \vdots \\ A_1^j & A_2^j & \dots & A_n^j \\ \vdots & \vdots & & \vdots \\ A_1^i & A_2^i & \dots & A_n^i \\ \vdots & \vdots & & \vdots \\ A_1^n & A_2^n & \dots & A_n^n \end{vmatrix} = - \begin{vmatrix} A_1^1 & A_2^1 & \dots & A_n^1 \\ \vdots & \vdots & & \vdots \\ A_1^i & A_2^i & \dots & A_n^i \\ \vdots & \vdots & & \vdots \\ A_1^j & A_2^j & \dots & A_n^j \\ \vdots & \vdots & & \vdots \\ A_1^n & A_2^n & \dots & A_n^n \end{vmatrix}.$$

*Důkaz.* Uvedeme pouze důkaz pro řádkové úpravy, pro sloupkové je analogický.

Buďte $A$ čtvercová matice a $B$ upravená matice.

(1) Nechť $B$ vznikne z $A$ přičtením $c$-násobku $j$-tého řádku k $i$-tému řádku, čili $B_\circ^i = A_\circ^i + cA_\circ^j$ a ostatní řádky matice $B$ jsou stejné jako řádky matice $A$. Potom

$$\begin{aligned} \det B &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot B_{\sigma_1}^1 \dots B_{\sigma_i}^i \dots B_{\sigma_j}^j \dots B_{\sigma_n}^n = \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A_{\sigma_1}^1 \dots (A_{\sigma_i}^i + cA_{\sigma_i}^j) \dots A_{\sigma_j}^j \dots A_{\sigma_n}^n = \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A_{\sigma_1}^1 \dots A_{\sigma_i}^i \dots A_{\sigma_j}^j \dots A_{\sigma_n}^n + \\ &\quad + c \underbrace{\sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A_{\sigma_1}^1 \dots A_{\sigma_i}^j \dots A_{\sigma_j}^j \dots A_{\sigma_n}^n}_{\text{determinant matice, kde } i\text{-tý řádek je stejný jako } j\text{-tý}} = \\ &= \det A + c \cdot 0 = \det A. \end{aligned}$$

(2) Nechť $B$ vznikne z $A$ vynásobením $i$-tého řádku prvkem $c$, čili $B^i_\circ = cA^i_\circ$ a ostatní řádky matice $B$ jsou stejné jako řádky matice $A$. Potom

$$\begin{aligned}\det B &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot B^1_{\sigma_1}\dots B^i_{\sigma_i}\dots B^n_{\sigma_n} = \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A^1_{\sigma_1}\dots cA^i_{\sigma_i}\dots A^n_{\sigma_n} = \\ &= c\sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A^1_{\sigma_1}\dots A^i_{\sigma_i}\dots A^n_{\sigma_n} = \\ &= c\det A.\end{aligned}$$

(3) Nechť $B$ vznikne z $A$ vzájemnou výměnou $i$-tého řádku a $j$-tého řádku, čili $B^i_\circ = A^j_\circ$, $B^j_\circ = A^i_\circ$ a ostatní řádky matice $B$ jsou stejné jako řádky matice $A$. Buď $\tau_{ij}\in S_n$ transpozice vyměňující $i,j$, čili $\operatorname{sgn}\tau_{ij} = -1$. Pro každou permutaci $\sigma\in S_n$ označme $\sigma' = \sigma\circ\tau_{ij}$. Pak $\sigma'_i = \sigma_j$, $\sigma'_j = \sigma_i$ a $\sigma'_k = \sigma_k$ pro $k\neq i,j$ a $\operatorname{sgn}\sigma' = \operatorname{sgn}\sigma\cdot\operatorname{sgn}\tau_{ij} = -\operatorname{sgn}\sigma$. Potom

$$\begin{aligned}\det B &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot B^1_{\sigma_1}\dots B^i_{\sigma_i}\dots B^j_{\sigma_j}\dots B^n_{\sigma_n} = \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A^1_{\sigma_1}\dots A^j_{\sigma_i}\dots A^i_{\sigma_j}\dots A^n_{\sigma_n} = \qquad \text{(komutativita násobení)} \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A^1_{\sigma_1}\dots A^i_{\sigma_j}\dots A^j_{\sigma_i}\dots A^n_{\sigma_n} = \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot A^1_{\sigma'_1}\dots A^i_{\sigma'_i}\dots A^j_{\sigma'_j}\dots A^n_{\sigma'_n} = \qquad (\operatorname{sgn}\sigma' = -\operatorname{sgn}\sigma) \\ &= -\sum_{\sigma\in S_n} \operatorname{sgn}\sigma' \cdot A^1_{\sigma'_1}\dots A^i_{\sigma'_i}\dots A^j_{\sigma'_j}\dots A^n_{\sigma'_n} = \\ &= -\det A,\end{aligned}$$

protože když $\sigma$ projde všechny prvky $S_n$, tak $\sigma'$ také. □

**Cvičení.** Jaký je vztah mezi $\det(cA)$ a $\det A$? □

**Cvičení.** Nechť $A$ je matice typu $n\times n$ taková, že $A^\mathsf{T} = -A$ (taková matice se nazývá *antisymetrická*). Ukažte, že je-li $n$ liché číslo, pak $\det A = 0$. □

**Příklad.**

$$\begin{vmatrix}1&1&1&1\\0&2&2&2\\0&0&3&3\\0&0&0&4\end{vmatrix} = \begin{vmatrix}1&1&1&1\\0&2&2&2\\0&0&3&3\\4&4&4&8\end{vmatrix} = \begin{vmatrix}1&1&1&1\\0&2&2&2\\3&3&6&6\\4&4&4&8\end{vmatrix} = \begin{vmatrix}1&1&1&1\\2&4&4&4\\3&3&6&6\\4&4&4&8\end{vmatrix}$$

$$4\cdot\begin{vmatrix}1&1&1&1\\0&2&2&2\\0&0&3&3\\0&0&0&4\end{vmatrix} = \begin{vmatrix}4&4&4&4\\0&2&2&2\\0&0&3&3\\0&0&0&4\end{vmatrix} = \begin{vmatrix}1&1&1&1\\0&8&8&8\\0&0&3&3\\0&0&0&4\end{vmatrix} = \begin{vmatrix}1&1&1&1\\0&2&2&2\\0&0&12&12\\0&0&0&4\end{vmatrix} = \begin{vmatrix}1&1&1&1\\0&2&2&2\\0&0&3&3\\0&0&0&16\end{vmatrix}$$

$$\begin{vmatrix}1&1&1&1\\0&2&2&2\\0&0&3&3\\0&0&0&4\end{vmatrix} = (-1)\cdot\begin{vmatrix}0&0&0&4\\0&2&2&2\\0&0&3&3\\1&1&1&1\end{vmatrix} = \begin{vmatrix}0&0&0&4\\0&0&3&3\\0&2&2&2\\1&1&1&1\end{vmatrix}$$

□

**Důsledek.** *Buďte $Q$ elementární matice a $A$ matice stejného typu. Pak*

$$\det QA = \det Q \cdot \det A.$$

*Důkaz.* (1) $\det(E^{i,j}(c)A) = \det A = 1 \cdot \det A = \det E^{i,j}(c) \cdot \det A$.
(2) $\det(E^{i}(c)A) = c \det A = \det E^{i}(c) \cdot \det A$.
(3) $\det(E^{i,j}A) = (-1) \cdot \det A = \det E^{i,j} \cdot \det A$. □

**Cvičení.** Dokažte, že $\det E^{i,j} = -1$ s využitím předchozího důsledku a toho, že vzájemná výměna dvou řádků je složením konečně mnoha řádkových elementárních úprav ostatních druhů. □

**Tvrzení 2.2.6.** *Matice je regulární právě tehdy, když má nenulový determinant.*

*Důkaz.* Buď $A$ regulární matice, tedy $A = Q_1 \cdots Q_k$, kde $Q_1, \ldots, Q_k$ jsou elementární matice. Potom

$$\begin{aligned}\det A &= \det(Q_1 \cdots Q_k) = \det Q_1 \cdot \det(Q_2 \cdots Q_k) = \cdots = \\ &= \det Q_1 \cdot \det Q_2 \cdots \det Q_k,\end{aligned}$$

což není rovno nule, protože determinanty elementárních matic jsou nenulové.

Nechť $\det A \neq 0$. Pomocí řádkových elementárních úprav převedeme $A$ na schodovitý tvar $B$, tedy $B = Q_k \cdots Q_1 A$, kde $Q_1, \ldots, Q_k$ jsou příslušné elementární matice. Potom

$$\begin{aligned}\det B &= \det(Q_k \cdots Q_1 A) = \det Q_k \det(Q_{k-1} \cdots Q_1 A) = \cdots = \\ &= \det Q_k \det Q_{k-1} \cdots \det Q_1 \det A \neq 0.\end{aligned}$$

Jelikož $B$ je ve schodovitém tvaru a její determinant je tedy součinem prvků na diagonále, na diagonále není žádná nula. To znamená, že $B$ nemá nulový řádek, je tedy regulární a $A$ také. □

**Důsledek.** *Matice je regulární právě tehdy, když má nenulový determinant, a to má právě tehdy, když je invertibilní, a to je právě tehdy, když je ekvivalentní jednotkové matici.*

**Tvrzení 2.2.7** (Cauchyho věta)**.** *Buďte $A, B$ čtvercové matice stejného typu. Pak*

$$\det AB = \det A \cdot \det B.$$

*Důkaz.* (1) Je-li $A$ regulární, tedy součin $Q_1 Q_2 \cdots Q_k$ elementárních matic, pak

$$\begin{aligned}\det AB &= \det(Q_1 \cdots Q_k B) = \det Q_1 \cdot \det(Q_2 \cdots Q_k B) = \cdots = \\ &= \det Q_1 \det Q_2 \cdots \det Q_k \det B = \det(Q_1 Q_2 \cdots Q_k) \det B = \\ &= \det A \det B.\end{aligned}$$

(2) Je-li $A$ singulární, podle Tvrzení 1.5.5 je $AB$ také singulární a tedy

$$\det AB = 0 = \det A = \det A \cdot \det B.$$ □

**Cvičení.** $\det A^{-1} = 1/\det A$. □

**Lemma 2.2.8.**

$$\begin{vmatrix} A_1^1 & \dots & A_k^1 & A_{k+1}^1 & \dots & A_n^1 \\ \vdots & & \vdots & \vdots & & \vdots \\ A_1^k & \dots & A_k^k & A_{k+1}^k & \dots & A_n^k \\ 0 & \dots & 0 & A_{k+1}^{k+1} & \dots & A_n^{k+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & A_{k+1}^n & \dots & A_n^n \end{vmatrix} = \begin{vmatrix} A_1^1 & \dots & A_k^1 \\ \vdots & & \vdots \\ A_1^k & \dots & A_k^k \end{vmatrix} \cdot \begin{vmatrix} A_{k+1}^{k+1} & \dots & A_n^{k+1} \\ \vdots & & \vdots \\ A_{k+1}^n & \dots & A_n^n \end{vmatrix}.$$

Determinant matice $A$ v předchozím tvrzení se *rozpadá na subdeterminanty*: jeden subdeterminant řádu $k$ a jeden subdeterminant řádu $n-k$. Stručně ale výstižně lze toto tvrzení vyjádřit zápisem

$$\begin{vmatrix} A' & X \\ 0 & A'' \end{vmatrix} = \left|A'\right| \cdot \left|A''\right|.$$

**Příklad.**

$$\begin{vmatrix} 2 & 3 & 4 & 5 \\ 0 & 2 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 6 & 7 & 8 \end{vmatrix} = 2 \cdot \begin{vmatrix} 2 & 3 & 0 \\ 1 & 2 & 0 \\ 6 & 7 & 8 \end{vmatrix} = 2 \cdot \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} \cdot 8 = 2 \cdot 1 \cdot 8 = 16$$

$$\begin{vmatrix} 2 & 1 & 3 & 4 \\ 0 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 \\ 0 & 0 & 3 & 4 \end{vmatrix} = (-1) \cdot \begin{vmatrix} 2 & 1 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 3 & 4 \end{vmatrix} = (-1) \cdot \begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix} \cdot \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = (-1) \cdot 3 \cdot (-2) = 6 \quad \square$$

### 2.2.3. Laplaceův rozvoj

**Definice 2.2.3.** Buď $A$ matice typu $n \times n$. Determinant řádu $n-1$ matice vzniklé z $A$ vynecháním jednoho řádku a jednoho sloupku je *minor*. Při vynechání $i$-tého řádku a $j$-tého sloupku příslušný minor označujeme

$$\bar{A}_j^i.$$

*Kofaktor* (nebo *algebraický doplněk*) prvku $A_j^i$ je

$$\hat{A}_j^i = (-1)^{i+j} \bar{A}_j^i.$$

Tedy, kofaktor (algebraický doplněk) prvku $A_j^i$ je $(-1)^{i+j}$-násobek determinantu matice, která vznikne z matice $A$ vynecháním $i$-tého řádku a $j$-tého sloupku.

**Příklad.** Mějme

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Potom

$$\bar{A}_1^1 = d, \quad \bar{A}_2^1 = c, \quad \bar{A}_1^2 = b, \quad \bar{A}_2^2 = a,$$

$$\hat{A}_1^1 = (-1)^{1+1} \bar{A}_1^1 = d, \qquad \hat{A}_2^1 = (-1)^{1+2} \bar{A}_2^1 = -c,$$
$$\hat{A}_1^2 = (-1)^{2+1} \bar{A}_1^2 = -b, \qquad \hat{A}_2^2 = (-1)^{2+2} \bar{A}_2^2 = a. \quad \square$$

**Příklad.** Mějme

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}.$$

Potom

$$\bar{A}^1_1 = \begin{vmatrix} e & f \\ h & i \end{vmatrix}, \quad \bar{A}^1_2 = \begin{vmatrix} d & f \\ g & i \end{vmatrix}, \quad \bar{A}^1_3 = \begin{vmatrix} d & e \\ g & h \end{vmatrix}, \quad \ldots, \quad \bar{A}^3_3 = \begin{vmatrix} a & b \\ d & e \end{vmatrix},$$

$$\hat{A}^1_1 = (-1)^{1+1}\bar{A}^1_1 = \begin{vmatrix} e & f \\ h & i \end{vmatrix}, \qquad \hat{A}^1_2 = (-1)^{1+2}\bar{A}^1_2 = -\begin{vmatrix} d & f \\ g & i \end{vmatrix},$$
$$\hat{A}^1_3 = (-1)^{1+3}\bar{A}^1_3 = \begin{vmatrix} d & e \\ g & h \end{vmatrix}, \qquad \hat{A}^3_3 = (-1)^{3+3}\bar{A}^3_3 = \begin{vmatrix} a & b \\ d & e \end{vmatrix}. \qquad \square$$

**Tvrzení 2.2.9** (Laplaceova věta o rozvoji determinantu)**.** *Buď $A$ matice typu $n \times n$. Pro každé $i \in \{1, \ldots, n\}$ platí*

$$\det A = A^i_1\hat{A}^i_1 + A^i_2\hat{A}^i_2 + \cdots + A^i_n\hat{A}^i_n = \sum_{j=1}^{n} A^i_j\hat{A}^i_j =$$
$$= A^1_i\hat{A}^1_i + A^2_i\hat{A}^2_i + \cdots + A^n_i\hat{A}^n_i = \sum_{j=1}^{n} A^j_i\hat{A}^j_i.$$

*Důkaz.*

$$\det A = \begin{vmatrix} A^1_1 & \ldots & A^1_{j-1} & A^1_j & A^1_{j+1} & \ldots & A^1_n \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A^i_1 & \ldots & A^i_{j-1} & A^i_j & A^i_{j+1} & \ldots & A^i_n \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A^n_1 & \ldots & A^n_{j-1} & A^n_j & A^n_{j+1} & \ldots & A^n_n \end{vmatrix} =$$
$$= \sum_{j=1}^{n} \begin{vmatrix} A^1_1 & \ldots & A^1_{j-1} & A^1_j & A^1_{j+1} & \ldots & A^1_n \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & A^i_j & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A^n_1 & \ldots & A^n_{j-1} & A^n_j & A^n_{j+1} & \ldots & A^n_n \end{vmatrix} =$$
$$= \sum_{j=1}^{n} A^i_j \begin{vmatrix} A^1_1 & \ldots & A^1_{j-1} & A^1_j & A^1_{j+1} & \ldots & A^1_n \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A^n_1 & \ldots & A^n_{j-1} & A^n_j & A^n_{j+1} & \ldots & A^n_n \end{vmatrix}.$$

Ukažme, že

$$\begin{vmatrix} A^1_1 & \ldots & A^1_{j-1} & A^1_j & A^1_{j+1} & \ldots & A^1_n \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A^n_1 & \ldots & A^n_{j-1} & A^n_j & A^n_{j+1} & \ldots & A^n_n \end{vmatrix} = \hat{A}^i_j.$$

Vyměňujme $i$-tý řádek $\begin{pmatrix}0 & \dots & 0 & 1 & 0 & \dots & 0\end{pmatrix}$ s předchozími řádky tak dlouho, až bude prvním řádkem; k tomu je potřeba $i-1$ výměn. Poté vyměňujme $j$-tý sloupek $\begin{pmatrix}1 & A^1_j & \dots & A^{i-1}_j & A^{i+1}_j & \dots & A^n_j\end{pmatrix}^\mathsf{T}$ s předchozími sloupky tak dlouho, až bude prvním sloupkem; k tomu je potřeba $j-1$ výměn. Takto vzniklý determinant je tedy nutné vynásobit číslem $(-1)^{i-1}(-1)^{j-1} = (-1)^{i-1+j-1} = (-1)^{i+j}$ a navíc se rozpadá na subdeterminanty $\det(1)$ a $\bar{A}^i_j$. Proto $\det A = \sum_{j=1}^n A^i_j \cdot (-1)^{i+j}\bar{A}^i_j = \sum_{j=1}^n A^i_j \hat{A}^i_j$ a máme rozvoj podle $i$-tého řádku.

Rozvoj podle $i$-tého sloupku získáme analogicky. □

**Definice 2.2.4.** Vztah v Laplaceově větě je *Laplaceův rozvoj podle $i$-tého řádku* resp. *podle $i$-tého sloupku*.

**Příklad.**

$$\begin{vmatrix}2&1&3&4\\0&0&1&2\\1&2&3&4\\0&0&3&4\end{vmatrix} = 2\cdot(-1)^{1+1}\cdot\begin{vmatrix}0&1&2\\2&3&4\\0&3&4\end{vmatrix} + 1\cdot(-1)^{3+1}\cdot\begin{vmatrix}1&3&4\\0&1&2\\0&3&4\end{vmatrix} =$$

$$= 2\cdot(-1)^{1+1}\cdot 2\cdot(-1)^{2+1}\begin{vmatrix}1&2\\3&4\end{vmatrix} + 1\cdot(-1)^{3+1}\cdot 1\cdot\begin{vmatrix}1&2\\3&4\end{vmatrix} = 8+(-2) = 6 \qquad \square$$

## 2.3. Adjungovaná matice

**Definice 2.3.1.** Buď $A$ čtvercová matice. Označme $\hat{A}$ matici kofaktorů $\hat{A}^i_j$. Matice $\hat{A}^\mathsf{T}$ je matice *adjungovaná* k matici $A$ a značí se $\operatorname{adj} A$. Tedy,

$$\operatorname{adj} A = \hat{A}^\mathsf{T}.$$

**Příklad.** Mějme

$$A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}.$$

Potom

$$\operatorname{adj} A = \hat{A}^\mathsf{T} = \begin{pmatrix}\hat{A}^1_1 & \hat{A}^1_2\\ \hat{A}^2_1 & \hat{A}^2_2\end{pmatrix}^\mathsf{T} = \begin{pmatrix}d & -c\\ -b & a\end{pmatrix}^\mathsf{T} = \begin{pmatrix}d & -b\\ -c & a\end{pmatrix}. \qquad \square$$

**Tvrzení 2.3.1.** *Pro libovolnou čtvercovou matici $A$*

$$\det A\cdot E = A\cdot\operatorname{adj} A = \operatorname{adj} A\cdot A.$$

*Je-li $A$ regulární matice, pak*

$$A^{-1} = \frac{1}{\det A}\operatorname{adj} A.$$

*Důkaz.* V $i$-tém řádku a $j$-tém sloupku matice $A\cdot\operatorname{adj} A$ je

$$(A\cdot\operatorname{adj} A)^i_j = \sum_k A^i_k(\hat{A}^\mathsf{T})^k_j = \sum_k A^i_k\hat{A}^j_k.$$

Pro $i=j$ podle Laplaceovy věty

$$(A\cdot\operatorname{adj} A)^i_i = \sum_k A^i_k\hat{A}^i_k = \det A.$$

Je-li $i \neq j$, buď $B$ matice, která z $A$ vznikne tím, že $j$-tý řádek nahradíme $i$-tým řádkem. Potom

$$\begin{aligned}
(A \cdot \operatorname{adj} A)^i_j &= \sum_k A^i_k \hat{A}^j_k = && (B \text{ se liší od } A \text{ jen v } j\text{-tém řádku}) \\
&= \sum_k B^i_k \hat{B}^j_k = && (B^i_k = B^j_k) \\
&= \sum_k B^j_k \hat{B}^j_k = && (\text{podle Laplaceovy věty}) \\
&= \det B = && (B \text{ má dva stejné řádky}) \\
&= 0.
\end{aligned}$$

Matice $A \cdot \operatorname{adj} A$ je tedy diagonální a všechny prvky na diagonále jsou rovny $\det A$, čili

$$A \cdot \operatorname{adj} A = \det A \cdot E.$$

Rovnost $\operatorname{adj} A \cdot A = \det A \cdot E$ dostaneme analogicky.

Je-li $A$ regulární, pak $\det A \neq 0$, takže jím můžeme dělit a s použitím Tvrzení 1.4.3 dostaneme uvedený vztah. □

**Příklad.** Mějme regulární matici

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Potom

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Například pro

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

dostaneme

$$A^{-1} = \frac{1}{-2} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}.$$ □

# 3. Soustavy lineárních rovnic

## 3.1. Soustavy lineárních rovnic a jejich řešení

**Definice 3.1.1.** Buďte $n \in \mathbb{N}$, $P$ pole, $a_1, a_2, \ldots, a_n, b \in P$, $x^1, x^2, \ldots, x^n \notin P$. Potom

$$a_1x^1 + a_2x^2 + \cdots + a_nx^n = b$$

je *lineární rovnice nad polem $P$ o $n$ neznámých* $x^1, x^2, \ldots, x^n$ (nejsou to mocniny, jen horní indexy). Prvky $a_1, a_2, \ldots, a_n, b \in P$ jsou *koeficienty*.

Uvedenou lineární rovnici můžeme zapsat

$$\sum_{j=1}^{n} a_j x^j = b.$$

**Definice 3.1.2.** *Řešení* rovnice

$$a_1x^1 + a_2x^2 + \cdots + a_nx^n = b$$

je každá uspořádaná $n$-tice $(\xi^1, \xi^2, \ldots, \xi^n)$ prvků pole $P$ taková, že platí rovnost

$$a_1\xi^1 + a_2\xi^2 + \cdots + a_n\xi^n = b.$$

Při hledání řešení rovnice tedy hledáme prvky $\xi^1, \xi^2, \ldots, \xi^n$ pole $P$ takové, že po dosazení $\xi^i$ za $x^i$ pro každé $i \in \{1, 2, \ldots, n\}$ se z rovnice stane rovnost.

**Příklad.** Nechť $P$ je pole reálných čísel $\mathbb{R}$.

$$1 \cdot x^1 + 2 \cdot x^2 + 0 \cdot x^3 + 4 \cdot x^4 = 6$$

je lineární rovnice o čtyřech neznámých $x^1, x^2, x^3, x^4$. Řešení této rovnice jsou například $(6, 0, 1, 0)$, $(2, 2, 7, 0)$, $(-4, 3, 0, 1)$, ale nejsou to zdaleka všechna řešení. □

**Tvrzení 3.1.1.** *Buď $ax = b$ lineární rovnice nad polem $P$ o jedné neznámé $x$.*

*(1) Pokud $a \neq 0$, potom $ax = b$ má právě jedno řešení, a to $\xi = ba^{-1}$.*
*(2) Pokud $a = 0$ a $b \neq 0$, potom $ax = b$ nemá řešení.*
*(3) Pokud $a = b = 0$, potom každý prvek pole $P$ je řešením $ax = b$.*

*Důkaz.* (1) Dosadíme-li $\xi = ba^{-1}$ za $x$, dostaneme $a\xi = aba^{-1} = b$, takže $\xi$ je řešení.

Na druhou stranu, je-li $\xi$ nějaké řešení, tedy $a\xi = b$, pak $\xi = \xi \cdot 1 = \xi(aa^{-1}) = (\xi a)a^{-1} = (a\xi)a^{-1} = ba^{-1}$. Čili každé řešení je rovno $ba^{-1}$ a je tedy jediné.

(2) a (3) Vyplývá z toho, že $0 \cdot x = 0$ pro každé $x \in P$, viz kapitola 6. □

**Příklad.** Rovnice $3x = 6$ nad polem reálných čísel má jediné řešení $6 \cdot 3^{-1} = 2$. □

**Definice 3.1.3.** Buďte $m, n, i, j \in \mathbb{N}$, $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$, $P$ pole, pro každé $i, j$ nechť $a^i_j, b^i \in P$, $x^1, x^2, \ldots, x^n \notin P$. Potom

$$\begin{aligned}
a^1_1x^1 + a^1_2x^2 + \cdots + a^1_nx^n &= b^1 \\
a^2_1x^1 + a^2_2x^2 + \cdots + a^2_nx^n &= b^2 \\
&\vdots \\
a^m_1x^1 + a^m_2x^2 + \cdots + a^m_nx^n &= b^m
\end{aligned}$$

je *soustava $m$ lineárních rovnic nad polem $P$ o $n$ neznámých* $x^1, \ldots, x^n$.

Uvedenou soustavu lineárních rovnic můžeme zapsat

$$\sum_{j=1}^{n} a_j^i x^j = b^i, \quad 1 \le i \le m.$$

Označíme-li

$$A = \begin{pmatrix} a_1^1 & a_2^1 & \dots & a_n^1 \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & & & \\ a_1^m & a_2^m & \dots & a_n^m \end{pmatrix}, \quad b = \begin{pmatrix} b^1 \\ b^2 \\ \vdots \\ b^m \end{pmatrix}, \quad x = \begin{pmatrix} x^1 \\ x^2 \\ \vdots \\ x^n \end{pmatrix},$$

můžeme soustavu lineárních rovnic psát jako rovnici

$$Ax = b.$$

**Definice 3.1.4.** Matice $A = (a_j^i)_{m\times n}$ je *matice soustavy*, $b = (b^i)_{m\times 1}$ je *sloupek pravých stran*, $x = (x^i)_{n\times 1}$ je *sloupek neznámých*. Matice

$$\bar{A} = \begin{pmatrix} a_1^1 & a_2^1 & \dots & a_n^1 & b^1 \\ a_1^2 & a_2^2 & \dots & a_n^2 & b^2 \\ \vdots & & & & \\ a_1^m & a_2^m & \dots & a_n^m & b^m \end{pmatrix}$$

je *rozšířená matice soustavy*. $\bar{A}$ se někdy značí $(A \,|\, b)$ nebo $(a_j^i \,|\, b^i)$.

**Definice 3.1.5.** *Řešení* soustavy $m$ lineárních rovnic o $n$ neznámých je každá uspořádaná $n$-tice $\xi = (\xi^1, \xi^2, \dots, \xi^n)$ prvků pole $P$ taková, že pro každé $i \in \{1, \dots, m\}$ platí rovnost

$$a_1^i \xi^1 + a_2^i \xi^2 + \dots + a_n^i \xi^n = b^i,$$

nebo při maticovém zápisu je to sloupková matice $\xi = \begin{pmatrix} \xi^1 & \xi^2 & \dots & \xi^n \end{pmatrix}^\mathsf{T}$ taková, že platí rovnost

$$A\xi = b.$$

Součin $Ax$ si můžeme rozepsat

$$Ax = \begin{pmatrix} a_1^1 & a_2^1 & \dots & a_n^1 \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & & & \\ a_1^m & a_2^m & \dots & a_n^m \end{pmatrix} \begin{pmatrix} x^1 \\ x^2 \\ \vdots \\ x^n \end{pmatrix} = \begin{pmatrix} a_1^1 x^1 + a_2^1 x^2 + \dots + a_n^1 x^n \\ a_1^2 x^1 + a_2^2 x^2 + \dots + a_n^2 x^n \\ \vdots \\ a_1^m x^1 + a_2^m x^2 + \dots + a_n^m x^n \end{pmatrix} =$$

$$= x^1 \begin{pmatrix} a_1^1 \\ a_1^2 \\ \vdots \\ a_1^m \end{pmatrix} + x^2 \begin{pmatrix} a_2^1 \\ a_2^2 \\ \vdots \\ a_2^m \end{pmatrix} + \dots + x^n \begin{pmatrix} a_n^1 \\ a_n^2 \\ \vdots \\ a_n^m \end{pmatrix} =$$

$$= x^1 A_1^\circ + x^2 A_2^\circ + \dots + x^n A_n^\circ$$

a soustavu $Ax = b$ pak můžeme přepsat

$$x^1 A_1^\circ + x^2 A_2^\circ + \dots + x^n A_n^\circ = b.$$

Tedy, soustava lineárních rovnic $Ax = b$ má řešení právě tehdy, když existuje lineární kombinace sloupků matice $A$, která je rovna sloupku pravých stran $b$. Koeficienty takových lineárních kombinací tvoří jednotlivá řešení soustavy.

Jestliže soustava lineárních rovnic má nějaké řešení, tj. sloupek pravých stran je nějakou lineární kombinací sloupků matice soustavy, potom hodnost rozšířené matice soustavy je rovna hodnosti matice soustavy. Jestliže soustava nemá řešení, tj. sloupek pravých stran není lineární kombinací sloupků matice soustavy, potom hodnost rozšířené matice soustavy je o 1 větší než hodnost matice soustavy.

Množina všech řešení soustavy lineárních rovnic je průnik množin všech řešení jednotlivých rovnic soustavy.

**Příklad.** (1) Řešení lineární rovnice

$$a_1x^1 + a_2x^2 = b$$

s reálnými koeficienty o dvou neznámých $x^1, x^2$ jsou uspořádané dvojice $(\xi^1, \xi^2)$ reálných čísel takové, že po jejich dosazení do rovnice za neznámé dostaneme rovnost. Množina všech řešení takové rovnice je tedy

$$\{(\xi^1, \xi^2) \in \mathbb{R}^2 \,|\, a_1\xi^1 + a_2\xi^2 = b\}$$

a bereme-li uspořádané dvojice jako body v rovině, tato množina je

- prázdná, tj. rovnice nemá řešení — pokud $a_1 = a_2 = 0$ a $b \neq 0$;
- přímka, tj. rovnice má nekonečně mnoho řešení — pokud aspoň jeden z koeficientů $a_1, a_2$ je nenulový;
- celá rovina, tj. rovnice má nekonečně mnoho řešení — pokud $a_1 = a_2 = b = 0$.

Je-li to přímka procházející dvěma body $u = (u_1, u_2), v = (v_1, v_2)$ a označíme-li $w = u - v$, můžeme ji zapsat také parametricky

$$\begin{aligned}\{u + tw \,|\, t \in \mathbb{R}\} &= \{(u_1, u_2) + t(w_1, w_2) \,|\, t \in \mathbb{R}\} = \\ &= \{(u_1 + tw_1, u_2 + tw_2) \,|\, t \in \mathbb{R}\}.\end{aligned}$$

(2) Množina všech řešení soustavy lineárních rovnic o dvou neznámých je průnik množin všech řešení jednotlivých rovnic. Taková množina je tedy

- prázdná — pokud buď aspoň jedna rovnice nemá řešení, nebo množiny všech řešení dvou rovnic jsou rovnoběžné přímky, nebo množiny všech řešení tří rovnic jsou přímky s prázdným průnikem;
- jednoprvková — pokud množiny všech řešení dvou rovnic jsou přímky s jednoprvkovým průnikem, jehož prvek je řešením i všech ostatních rovnic soustavy;
- přímka — pokud to není celá rovina a všechny množiny všech řešení jednotlivých rovnic různé od celé roviny jsou tatáž přímka, tedy všechny rovnice jsou násobky jedné z nich;
- celá rovina — pokud všechny rovnice mají všechny koeficienty i pravé strany nulové, tedy $a_1^i = a_2^i = b^i = 0$ pro každé $i$.

(3) Řešení lineární rovnice o třech neznámých jsou uspořádané trojice, po jejichž dosazení do rovnice dostaneme rovnost, a bereme-li uspořádané trojice jako body v trojrozměrném prostoru, množina všech řešení je

- prázdná — pokud $a_1 = a_2 = a_3 = 0$ a $b \neq 0$;
- rovina — pokud aspoň jeden z koeficientů $a_1, a_2, a_3$ je nenulový;
- celý trojrozměrný prostor — pokud $a_1 = a_2 = a_3 = b = 0$.

A také rovinu v prostoru můžeme vyjádřit parametricky.

(4) Množina všech řešení soustavy lineárních rovnic o třech neznámých může být

- prázdná;
- jednoprvková;
- přímka;
- rovina;
- celý trojrozměrný prostor.

(5) Řešení lineární rovnice o $n$ neznámých jsou uspořádané $n$-tice a množina všech řešení je

- prázdná;
- „$(n-1)$-rozměrná rovina“, nazývá se *nadrovina* v $n$-rozměrném prostoru;
- celý $n$-rozměrný prostor.

Množina všech řešení soustavy lineárních rovnic o $n$ neznámých je tedy případně průnik nadrovin v $n$-rozměrném prostoru. □

**Příklad.** (1) Soustava

$$\begin{aligned} x^1 + 2x^2 - \ x^3 &= 1 \\ -x^1 + \ x^2 + 2x^3 &= 1 \\ 2x^1 - \ x^2 + \ x^3 &= 1 \end{aligned}$$

má právě jedno řešení, $(0{,}5, 0{,}5, 0{,}5)$, tj. $\xi^1 = \xi^2 = \xi^3 = 0{,}5$. Množina všech řešení je $\{(0{,}5, 0{,}5, 0{,}5)\}$.

(2) Mějme soustavu

$$x - y = 1,$$

tedy jednu rovnici o dvou neznámých $x, y$. Každá uspořádaná dvojice $(t, t-1)$, kde $t$ je libovolné reálné číslo, je řešení soustavy, tj. $\xi^1 = t$, $\xi^2 = t - 1$ pro libovolné $t \in \mathbb{R}$. Soustava má tedy nekonečně mnoho řešení a množina všech řešení je $\{(t, t-1) \,|\, t \in \mathbb{R}\}$.

(3) Soustava

$$\begin{aligned} x &= 0 \\ x &= 1 \end{aligned}$$

nemá žádné řešení, množina všech řešení je tedy prázdná množina $\emptyset$. □

## 3.2. Gaussova eliminační metoda a obecné řešení

Řešit soustavu lineárních rovnic, tj. hledat množinu všech jejích řešení, je možné tak, že soustavu upravíme na takový tvar, ze kterého všechna řešení vyčteme. Je ovšem nutné používat pouze takové úpravy, po jejichž provedení množina všech řešení nové soustavy je stejná jako množina všech řešení původní soustavy.

**Definice 3.2.1.** *Ekvivalentní úprava* soustavy lineárních rovnic je úprava, jejíž provedením vznikne soustava lineárních rovnic s množinou všech řešení rovnou množině všech řešení původní soustavy.
Soustavy lineárních rovnic, jejichž množiny všech řešení se vzájemně rovnají, jsou *ekvivalentní*.

**Definice 3.2.2.** *Elementární úpravy* soustavy lineárních rovnic jsou

(i) přičtení nějakého násobku jedné rovnice k jiné rovnici,
(ii) vynásobení některé rovnice nenulovým prvkem pole,
(iii) vzájemná výměna dvou rovnic.

Ke každé elementární úpravě soustavy existuje elementární úprava (stejného typu), která soustavu převede do původního stavu.

Je zřejmé, že provedení řádkové elementární úpravy rozšířené matice soustavy je totéž co provedení obdobné elementární úpravy soustavy.

Podle následujícího tvrzení elementární úpravy jsou ekvivalentní.

**Tvrzení 3.2.1.** *Elementární úpravy soustavy lineárních rovnic jsou ekvivalentní.*

*Důkaz.* Mějme soustavu lineárních rovnic o $n$ neznámých $x^1, x^2, \dots, x^n$ a buď $\xi = (\xi^1, \xi^2, \dots, \xi^n)$ její řešení, tj. pro každé $i$ platí rovnost

$$a_1^i\xi^1 + a_2^i\xi^2 + \cdots + a_n^i\xi^n = b^i.$$

Zvolme si jednu elementární úpravu, přičtení $c$-násobku $j$-té rovnice k $i$-té rovnici, kde $i \neq j$ (pro zbylé dvě úpravy je důkaz analogický). Po této úpravě dostaneme novou soustavu, která se od té původní liší jen v $i$-té rovnici, ta v nové soustavě je

$$(a_1^i + ca_1^j)x^1 + \cdots + (a_n^i + ca_n^j)x^n = b^i + cb^j.$$

Je zřejmé, že $\xi$ je řešením i této nové soustavy, protože je řešením nové $i$-té rovnice

$$\begin{aligned}(a_1^i + ca_1^j)\xi^1 + \cdots + (a_n^i + ca_n^j)\xi^n &= \\ = (a_1^i\xi^1 + \cdots + a_n^i\xi^n) + c(a_1^j\xi^1 + \cdots + a_n^j\xi^n) &= \\ = b^i + cb^j\end{aligned}$$

i všech ostatních, nezměněných rovnic soustavy. To znamená, že každé řešení původní soustavy je řešením i upravené soustavy.

Při maticovém zápisu můžeme tvrzení dokázat s využitím toho, že řádková elementární úprava matice je totéž co vynásobení elementární maticí zleva. Úpravou soustavy $Ax = b$ dostaneme soustavu $QAx = Qb$. Jestliže $\xi$ je řešením původní soustavy, tedy $A\xi = b$, potom $QA\xi = Qb$ a $\xi$ je řešením i upravené soustavy.

Vzhledem k tomu, že upravenou soustavu můžeme převést na tu původní opět pomocí jedné z elementárních úprav, každé řešení upravené soustavy je také řešením původní soustavy. Celkově tedy množina všech řešení upravené soustavy je rovna množině všech řešení původní soustavy. □

Tvary soustavy lineárních rovnic, ze kterých lze snadno vyčíst všechna řešení soustavy, jsou ty, jejichž rozšířené matice jsou ve schodovitém a ještě lépe v Gaussově–Jordanově tvaru.

**Gaussova eliminační metoda.** Řádkovými elementárními úpravami upravme rozšířenou matici soustavy na Gaussův–Jordanův tvar (stačil by i schodovitý). Je zřejmé, že počet nenulových řádků příslušné upravené matice soustavy není větší než počet neznámých, čili počet sloupků matice soustavy. Jestliže upravená rozšířená matice soustavy má více (o jeden) nenulových řádků než příslušná matice soustavy, soustava (upravená i původní) nemá řešení. Jestliže počty nenulových řádků upravené rozšířené matice soustavy i příslušné matice soustavy se rovnají $r$ ($r \leq n$), tj. rozšířená matice soustavy a matice soustavy mají stejné hodnosti, příslušná soustava rovnic (uvádíme jen ty nenulové) je

$$\begin{aligned}x^1 + \cdots + \ 0\ + \cdots + \ 0\ + c_{k_r+1}^1 x^{k_r+1} + \cdots + \quad c_n^1 x^n &= d^1 \\ &\vdots \\ x^{k_{r-1}} + \cdots + \ 0\ + c_{k_r+1}^{r-1} x^{k_r+1} + \cdots + c_n^{r-1} x^n &= d^{r-1} \\ x^{k_r} + c_{k_r+1}^r x^{k_r+1} + \cdots + \quad c_n^r x^n &= d^r.\end{aligned}$$

Z poslední rovnice můžeme pomocí $x^{k_r+1}, \dots, x^n$ vyjádřit

$$x^{k_r} = d^r - c_{k_r+1}^r x^{k_r+1} - \cdots - c_n^r x^n.$$

Z předposlední rovnice můžeme pomocí $x^{k_{r-1}+1}, \dots, x^{k_r-1}, x^{k_r+1}, \dots, x^n$ vyjádřit

$$x^{k_{r-1}} = d^{r-1} - c_{k_{r-1}+1}^{r-1} x^{k_{r-1}+1} - \cdots - c_{k_r-1}^{r-1} x^{k_r-1} - c_{k_r+1}^{r-1} x^{k_r+1} - \cdots - c_n^{r-1} x^n.$$

Takto můžeme postupovat až k první rovnici, ze které vyjádříme $x^1$ ($k_1 = 1$) pomocí všech ostatních neznámých kromě $x^{k_2}, \dots, x^{k_r}$.

Získáme tak vyjádření $r$ neznámých $x^{k_1}, x^{k_2}, \dots, x^{k_r}$ pomocí $n-r$ neznámých $x^i$ s $i \in \{1, 2, \dots, n\} \setminus \{k_1, k_2, \dots, k_r\}$. Když za neznámé $x^i$, $i \in \{1, 2, \dots, n\} \setminus \{k_1, k_2, \dots, k_r\}$, zvolíme libovolné prvky pole $P$, které pak dosadíme do získaných vztahů pro neznámé $x^{k_1}, x^{k_2}, \dots, x^{k_r}$ a tyto hodnoty dopočítáme, dostaneme řešení soustavy $Ax = b$.

**Definice 3.2.3.** Neznámé $x^{k_1}, x^{k_2}, \dots, x^{k_r}$ z předchozího odstavce jsou *hlavní* (nebo *bázové* nebo *bázické*), neznámé $x^i$, kde $i \in \{1, 2, \dots, n\} \setminus \{k_1, k_2, \dots, k_r\}$, jsou *parametry* (nebo *nebázické neznámé* nebo *volné proměnné*) a označujeme je po řadě $t^1, \dots, t^{n-r}$.

**Definice 3.2.4.** Řešení soustavy lineárních rovnic o $n$ neznámých, jejíž rozšířená matice má hodnost $r$, zapsané pomocí $n - r$ parametrů je *obecné řešení*. Řešení získané z obecného řešení libovolnou volbou parametrů je *partikulární řešení*.

Je zřejmé, že každé řešení soustavy lineárních rovnic lze získat z obecného řešení vhodnou volbou parametrů. Takže množina všech řešení získaných z obecného řešení všemi možnými volbami parametrů je rovna množině všech řešení soustavy a obecné řešení reprezentuje všechna řešení soustavy.

**Příklad.** Mějme soustavu

$$\begin{aligned} x^1 + 2x^2 + 3x^3 &= 1 \\ 2x^1 + 3x^2 + 4x^3 &= 1 \\ 3x^1 + 4x^2 + 5x^3 &= 1 \end{aligned}$$

nad polem reálných čísel. Rozšířená matice soustavy je

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

Její Gaussův–Jordanův tvar je

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

a hodnost matice soustavy i hodnost rozšířené matice soustavy se rovnají 2. Uvedený Gaussův–Jordanův tvar reprezentuje soustavu

$$\begin{aligned} x^1 \qquad - x^3 &= -1 \\ x^2 + 2x^3 &= 1. \end{aligned}$$

Z první rovnice můžeme vyjádřit $x^1$ pomocí $x^3$

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

a z druhé rovnice můžeme vyjádřit $x^2$ pomocí $x^3$

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

Máme tedy 2 (= hodnost matice) neznámé vyjádřeny pomocí jedné ($= 3 - 2$) neznámé. Neznámé $x^1$ a $x^2$ jsou hlavní, neznámá $x^3$ je parametr a můžeme za ni dosadit libovolné reálné číslo a hlavní neznámé dopočítat. Označíme-li parametr $t$, dostaneme, že

$$\xi(t) = (-1 + t, 1 - 2t, t), \quad t \in \mathbb{R},$$

je obecné řešení soustavy. Při volbě $t = 0$ získáme partikulární řešení $\xi(0) = (-1, 1, 0)$. Množina všech řešení soustavy je

$$\{(-1 + t, 1 - 2t, t) \,|\, t \in \mathbb{R}\}.$$

Uspořádanou trojici $(-1 + t, 1 - 2t, t)$ můžeme zapsat

$$\begin{aligned}(-1 + t, 1 - 2t, t) &= (-1, 1, 0) + (t, -2t, t) = \\ &= (-1, 1, 0) + t(1, -2, 1)\end{aligned}$$

a množinu všech řešení soustavy pak můžeme zapsat

$$\{(-1, 1, 0) + t(1, -2, 1) \,|\, t \in \mathbb{R}\},$$

což je přímka v $\mathbb{R}^3$ procházející bodem $(-1, 1, 0)$, který je dán sloupcem pravých stran soustavy v Gaussově–Jordanově tvaru, se směrovým vektorem $(1, -2, 1)$. Při maticovém zápisu množina všech řešení je

$$\left\{ \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \,\middle|\, t \in \mathbb{R} \right\}. \qquad \square$$

**Příklad.** Mějme soustavu

$$\begin{aligned} x^1 + 2x^2 + 3x^3 + 4x^4 &= 1 \\ 2x^1 + 3x^2 + 4x^3 + 5x^4 &= 1 \\ 3x^1 + 4x^2 + 5x^3 + 6x^4 &= 1 \\ 4x^1 + 5x^2 + 6x^3 + 7x^4 &= 1 \end{aligned}$$

nad polem reálných čísel. Rozšířená matice soustavy je

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 6 & 1 \\ 4 & 5 & 6 & 7 & 1 \end{pmatrix}.$$

Její Gaussův–Jordanův tvar je

$$\begin{pmatrix} 1 & 0 & -1 & -2 & -1 \\ 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

a hodnost matice soustavy i hodnost rozšířené matice soustavy se rovnají 2. Uvedený Gaussův–Jordanův tvar reprezentuje soustavu

$$\begin{aligned} x^1 \qquad - x^3 - 2x^4 &= -1 \\ x^2 + 2x^3 + 3x^4 &= 1. \end{aligned}$$

Z první rovnice můžeme vyjádřit $x^1$ pomocí $x^3$ a $x^4$

$$x^1 = -1 + x^3 + 2x^4$$

a z druhé rovnice můžeme vyjádřit $x^2$ pomocí $x^3$ a $x^4$

$$x^2 = 1 - 2x^3 - 3x^4.$$

Máme tedy 2 (= hodnost matice) neznámé vyjádřeny pomocí dvou (= $4 - 2$) neznámých. Neznámé $x^1$ a $x^2$ jsou hlavní, neznámé $x^3$ a $x^4$ jsou parametry a můžeme za ně dosadit libovolná reálná čísla a hlavní neznámé dopočítat. Označíme-li parametry $t^1$ a $t^2$, dostaneme, že

$$\xi(t^1, t^2) = (-1 + t^1 + 2t^2, 1 - 2t^1 - 3t^2, t^1, t^2), \quad t^1, t^2 \in \mathbb{R},$$

je obecné řešení soustavy. Při volbě $t^1 = 1, t^2 = 0$ získáme partikulární řešení $\xi(1,0) = (0,-1,1,0)$, při volbě $t^1 = 0, t^2 = 1$ získáme partikulární řešení $\xi(0,1) = (1,-2,0,1)$. Množina všech řešení soustavy je

$$\{(-1+t^1+2t^2, 1-2t^1-3t^2, t^1, t^2) \,|\, t^1, t^2 \in \mathbb{R}\}.$$

Uspořádanou čtveřici $(-1+t^1+2t^2, 1-2t^1-3t^2, t^1, t^2)$ můžeme zapsat

$$\begin{aligned}(-1+t^1+2t^2, 1-2t^1-3t^2, t^1, t^2) &= \\ &= (-1,1,0,0) + (t^1,-2t^1,t^1,0) + (2t^2,-3t^2,0,t^2) = \\ &= (-1,1,0,0) + t^1(1,-2,1,0) + t^2(2,-3,0,1)\end{aligned}$$

a množinu všech řešení soustavy pak můžeme zapsat

$$\{(-1,1,0,0) + t^1(1,-2,1,0) + t^2(2,-3,0,1) \,|\, t^1, t^2 \in \mathbb{R}\},$$

při maticovém zápisu

$$\left\{ \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t^1 \begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix} + t^2 \begin{pmatrix} 2 \\ -3 \\ 0 \\ 1 \end{pmatrix} \,\middle|\, t^1, t^2 \in \mathbb{R} \right\}. \qquad \square$$

## 3.3. Frobeniova věta

Z předchozích pozorování a tvrzení vyplývá následující věta.

**Tvrzení 3.3.1** (Frobeniova věta)**.** *Soustava lineárních rovnic má aspoň jedno řešení právě tehdy, když hodnost matice soustavy se rovná hodnosti rozšířené matice soustavy.*

*Důkaz.* Jestliže soustava $Ax = b$ má nějaké řešení, pak sloupek $b$ pravých stran je lineární kombinací sloupků matice $A$ a rozšířením matice $A$ o takový sloupek se hodnost nezmění. Takže matice $A$ a $\bar{A}$ mají stejné hodnosti.

Jestliže se hodnosti matic $A$ a $\bar{A}$ rovnají, a rovnají se tedy i hodnosti příslušných matic v Gaussově–Jordanově tvaru, pak použitím Gaussovy eliminační metody a libovolnou volbou parametrů získáme řešení soustavy. $\square$

**Příklad.** (1) Soustava

$$\begin{aligned} x^1 + 2x^2 - \ x^3 &= 1 \\ -x^1 + \ x^2 + 2x^3 &= 1 \\ 2x^1 - \ x^2 + \ x^3 &= 1 \end{aligned}$$

má matici soustavy

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

a rozšířenou matici soustavy

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

Jejich hodnosti jsou stejné, obě se rovnají 3, takže podle Frobeniovy věty soustava má řešení. Jelikož hodnosti jsou rovny počtu neznámých, všechny neznámé jsou hlavní, žádná není parametr a soustava má právě jedno řešení.

(2) Soustava

$$x - y = 1$$

má matici soustavy

$$\begin{pmatrix} 1 & -1 \end{pmatrix}$$

a rozšířenou matici soustavy

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

Jejich hodnosti jsou stejné, obě se rovnají 1, takže podle Frobeniovy věty soustava má řešení. Jelikož hodnosti jsou nižší než počet neznámých, jedna neznámá je hlavní, jedna neznámá je parametr a soustava má nekonečně mnoho řešení.

(3) Soustava

$$x = 0$$
$$x = 1$$

má matici soustavy

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

a rozšířenou matici soustavy

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

Hodnost matice soustavy je rovna 1 a hodnost rozšířené matice soustavy je rovna 2, takže podle Frobeniovy věty soustava nemá řešení. □

## 3.4. Cramerovo pravidlo

Podle Frobeniovy věty soustava s regulární maticí má řešení. Podle následující věty má právě jedno řešení.

**Tvrzení 3.4.1.** *Buď $Ax = b$ soustava se čtvercovou maticí $A$. Potom $A$ je regulární právě tehdy, když $Ax = b$ má právě jedno řešení, a to*

$$\xi = A^{-1}b.$$

*Důkaz.* „⇒“ Nechť $A$ je regulární matice, tedy invertibilní, s maximální hodností. Potom podle Frobeniovy věty soustava $Ax = b$ má řešení. A pro každé řešení $\xi$ platí $A\xi = b$, tedy $\xi = A^{-1}A\xi = A^{-1}b$, čili řešení je jediné.

„⇐“ Nechť $A$ není regulární matice, tedy je singulární, s hodností menší než počet jejích řádků, který se rovná počtu neznámých. Pokud hodnost rozšířené matice soustavy je větší než hodnost matice soustavy, soustava nemá řešení. Pokud hodnost rozšířené matice soustavy je stejná jako hodnost matice soustavy, potom v obecném řešení soustavy vystupuje aspoň jeden parametr, za který lze dosadit libovolný prvek pole. Vzhledem k tomu, že pole obsahuje více než jeden prvek, soustava má více než jedno řešení. □

**Tvrzení 3.4.2** (Cramerovo pravidlo)**.** *Buď $Ax = b$ soustava s regulární maticí $A$ a řešením $\xi = \begin{pmatrix} \xi^1 & \xi^2 & \dots & \xi^n \end{pmatrix}^T$. Pak pro každé $i \in \{1, 2, \dots, n\}$*

$$\xi^i = \frac{\det A_i}{\det A},$$

*kde $A_i$ je matice vzniklá z matice $A$ výměnou $i$-tého sloupku za sloupek pravých stran $b$:*

$$A_i = \begin{pmatrix} a_1^1 & \dots a_{i-1}^1 & b^1 & a_{i+1}^1 & \dots & a_n^1 \\ \vdots & & & & & \\ a_1^n & \dots a_{i-1}^n & b^n & a_{i+1}^n & \dots & a_n^n \end{pmatrix}.$$

*Důkaz.* Při rozvoji podle $i$-tého sloupku dostáváme $\det A_i = \sum_j \hat{A}_i^j b^j$. Dále

$$\xi = A^{-1}b = \frac{1}{\det A}(\operatorname{adj} A)\cdot b = \frac{1}{\det A}\hat{A}^{\mathsf{T}} b$$

a tedy

$$\xi^i = \frac{\sum_j (\hat{A}^{\mathsf{T}})_j^i b^j}{\det A} = \frac{\sum_j \hat{A}_i^j b^j}{\det A} = \frac{\sum_j (\hat{A}_i)_i^j b^j}{\det A} = \frac{\det A_i}{\det A}.$$

Tvrzení můžeme dokázat také takto: Je-li $\xi$ řešení soustavy $Ax = b$, pak $b$ je lineární kombinací sloupků $A_i^\circ$ s koeficienty $\xi^1, \dots, \xi^n$, tedy

$$b = \xi^1 A_1^\circ + \xi^2 A_2^\circ + \dots + \xi^n A_n^\circ = \sum_j \xi^j A_j^\circ$$

a matice $A_i$ má v $i$-tém sloupku tuto lineární kombinaci všech sloupků matice $A$. Potom

$$\begin{aligned}
\det A_i &= \det\begin{pmatrix} A_1^\circ & \dots & A_{i-1}^\circ & b & A_{i+1}^\circ & \dots & A_n^\circ \end{pmatrix} = \\
&= \det\begin{pmatrix} A_1^\circ & \dots & A_{i-1}^\circ & \sum_j \xi^j A_j^\circ & A_{i+1}^\circ & \dots & A_n^\circ \end{pmatrix} = \\
&= \sum_j \det\begin{pmatrix} A_1^\circ & \dots & A_{i-1}^\circ & \xi^j A_j^\circ & A_{i+1}^\circ & \dots & A_n^\circ \end{pmatrix} = \\
&= \sum_j \xi^j \det\begin{pmatrix} A_1^\circ & \dots & A_{i-1}^\circ & A_j^\circ & A_{i+1}^\circ & \dots & A_n^\circ \end{pmatrix} = \\
&= \xi^i \det\begin{pmatrix} A_1^\circ & \dots & A_{i-1}^\circ & A_i^\circ & A_{i+1}^\circ & \dots & A_n^\circ \end{pmatrix} = \\
&= \xi^i \det A,
\end{aligned}$$

z čehož dostaneme požadovaný vztah. □

**Příklad.** Mějme soustavu

$$\begin{aligned}
x^1 + 2x^2 - x^3 &= 1 \\
-x^1 + x^2 + 2x^3 &= 1 \\
2x^1 - x^2 + x^3 &= 1.
\end{aligned}$$

Potom

$$A = \begin{pmatrix} 1 & 2 & -1 \\ -1 & 1 & 2 \\ 2 & -1 & 1 \end{pmatrix} \qquad A_1 = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 1 & 2 \\ 1 & -1 & 1 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 1 & 1 & -1 \\ -1 & 1 & 2 \\ 2 & 1 & 1 \end{pmatrix} \qquad A_3 = \begin{pmatrix} 1 & 2 & 1 \\ -1 & 1 & 1 \\ 2 & -1 & 1 \end{pmatrix}$$

a

$$\det A = 14 \qquad \det A_1 = 7 \qquad \det A_2 = 7 \qquad \det A_3 = 7.$$

Proto

$$\xi^1 = \xi^2 = \xi^3 = \frac{\det A_1}{\det A} = \frac{\det A_2}{\det A} = \frac{\det A_3}{\det A} = \frac{7}{14} = \frac{1}{2}.$$

□

## 3.5. Homogenní soustavy lineárních rovnic

**Definice 3.5.1.** Soustava lineárních rovnic s nulovou pravou stranou, $b = 0$, je *homogenní.*

**Příklad.** (1) Soustava

$$\begin{aligned} x^1 + 2x^2 - \ x^3 &= 0 \\ -x^1 + \ x^2 + 2x^3 &= 0 \\ 2x^1 - \ x^2 + \ x^3 &= 0 \end{aligned}$$

je homogenní.

(2) Soustava

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

je homogenní.

(3) Soustava

$$\begin{aligned} x &= 0 \\ x &= 1 \end{aligned}$$

není homogenní. □

**Tvrzení 3.5.1.** *(1) Každá homogenní soustava má řešení.*

*(2) Každá homogenní soustava má nulové řešení.*

*(3) Homogenní soustava se čtvercovou maticí má pouze nulové řešení právě tehdy, když matice soustavy je regulární.*

*(4) Homogenní soustava se čtvercovou maticí má nenulové řešení právě tehdy, když determinant matice soustavy je roven nule.*

*(5) Homogenní soustava, ve které je méně rovnic než neznámých, má nenulové řešení.*

*Důkaz.* (1) Existence řešení homogenní soustavy vyplývá z Frobeniovy věty i z následujícího bodu (2).

(2) Vzhledem k tomu, že $0 \cdot p = p \cdot 0 = 0$ pro každé $p$ z příslušného pole, viz kapitola 6, je zřejmé, že homogenní soustava má nulové řešení.

(3) Vyplývá z Tvrzení 3.4.1.

(4) Tvrzení je ekvivalentní předchozímu.

(5) V tomto případě při použití Gaussovy eliminační metody kladný počet neznámých jsou parametry a vhodnou volbou libovolného parametru získáme nenulové řešení. □

Množina všech řešení homogenní soustavy lineárních rovnic má následující vlastnost.

**Tvrzení 3.5.2.** *Lineární kombinace řešení homogenní soustavy je také řešení té soustavy. Speciálně, nulový sloupek je řešení, součet řešení je řešení a c-násobek řešení je řešení.*

*Důkaz.* Nechť $\xi_1, \xi_2, \ldots, \xi_k$ jsou řešení, $\alpha_1, \alpha_2, \ldots, \alpha_k \in P$. Tedy, $A\xi_1 = 0, A\xi_2 = 0, \ldots, A\xi_k = 0$. Potom

$$A(\alpha_1\xi_1 + \alpha_2\xi_2 + \cdots + \alpha_k\xi_k) = \alpha_1 A\xi_1 + \alpha_2 A\xi_2 + \cdots + \alpha_k A\xi_k = 0$$

a lineární kombinace řešení je tedy také řešení soustavy. □

**Definice 3.5.2.** *Fundamentální systém řešení* homogenní soustavy je taková množina řešení té soustavy, která je lineárně nezávislá a každé řešení lze vyjádřit jako lineární kombinaci řešení z této množiny.

**Tvrzení 3.5.3.** *Fundamentální systém řešení soustavy rovnic $Ax = 0$ o $n$ neznámých má $n - \operatorname{rank} A$ prvků.*

*Důkaz.* Obecné řešení $\xi$ soustavy $Ax = 0$ o $n$ neznámých je vyjádřeno pomocí $n - \operatorname{rank} A$ parametrů $t^1, \dots, t^{n-\operatorname{rank} A}$, tedy $\xi = \xi(t^1, \dots, t^{n-\operatorname{rank} A})$. Provedeme-li $n - \operatorname{rank} A$ voleb parametrů

$$\begin{aligned}
&(t^1, \dots, t^{n-\operatorname{rank} A}) = (1, 0, \dots, 0),\\
&(t^1, \dots, t^{n-\operatorname{rank} A}) = (0, 1, \dots, 0),\\
&\dots\\
&(t^1, \dots, t^{n-\operatorname{rank} A}) = (0, \dots, 0, 1),
\end{aligned}$$

dostaneme množinu partikulárních řešení

$$\{\xi(1, 0, \dots, 0), \xi(0, 1, \dots, 0), \dots, \xi(0, \dots, 0, 1)\},$$

která je lineárně nezávislá a

$$\xi(t^1, \dots, t^{n-\operatorname{rank} A}) = t^1\xi(1, 0, \dots, 0) + t^2\xi(0, 1, \dots, 0) + \dots + t^{n-\operatorname{rank} A}\xi(0, \dots, 0, 1),$$

takže obecné řešení, čili každé řešení, soustavy je lineární kombinací těchto partikulárních řešení. □

**Příklad.** (1) Soustava

$$x^1 - x^2 = 0$$

má 2 neznámé, matice soustavy má hodnost 1, obecné řešení je

$$\xi(t) = (t, t), \quad t \in \mathbb{R},$$

množina všech řešení soustavy je

$$\{(t, t) \mid t \in \mathbb{R}\} = \{t(1, 1) \mid t \in \mathbb{R}\}$$

a fundamentální systém řešení soustavy je například

$$\{(1, 1)\}.$$

(2) Soustava

$$\begin{aligned}
x^1 + \ x^2 + 2x^3 &= 0\\
-x^1 + \ x^2 + 2x^3 &= 0\\
x^1 + 3x^2 + 6x^3 &= 0
\end{aligned}$$

má 3 neznámé, matice soustavy má hodnost 2, obecné řešení je

$$\xi(t) = (0, -2t, t), \quad t \in \mathbb{R},$$

množina všech řešení soustavy je

$$\{(0, -2t, t) \mid t \in \mathbb{R}\} = \{t(0, -2, 1) \mid t \in \mathbb{R}\}$$

a fundamentální systém řešení soustavy je například

$$\{(0, -2, 1)\}.$$

(3) Soustava

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

má 3 neznámé, matice soustavy má hodnost 1, obecné řešení je

$$\xi(t^1, t^2) = (t^1 - t^2, t^1, t^2), \quad t^1, t^2 \in \mathbb{R},$$

množina všech řešení soustavy je

$$\{(t^1 - t^2, t^1, t^2) \,|\, t^1, t^2 \in \mathbb{R}\} = \{t^1(1,1,0) - t^2(-1,0,1) \,|\, t^1, t^2 \in \mathbb{R}\}$$

a fundamentální systém řešení soustavy je například

$$\{(1,1,0), (-1,0,1)\}.$$

(4) Soustava

$$\begin{aligned} x^1 + 2x^2 &= 0 \\ 3x^1 + 4x^2 &= 0 \end{aligned}$$

má 2 neznámé, matice soustavy má hodnost 2 a soustava má jediné řešení, čili obecné řešení je

$$\xi = (0,0),$$

množina všech řešení soustavy je

$$\{(0,0)\}$$

a fundamentální systém řešení soustavy je $\emptyset$.

(5) Soustava

$$0x = 0$$

má 1 neznámou, matice soustavy má hodnost 0, obecné řešení je

$$\xi(t) = t, \quad t \in \mathbb{R},$$

množina všech řešení soustavy je

$$\{t \,|\, t \in \mathbb{R}\} = \mathbb{R}$$

a fundamentální systém řešení soustavy je například

$$\{1\}.$$

□

**Poznámka.** Je-li $\{\xi_1, \xi_2, \ldots, \xi_r\}$ fundamentální systém řešení nějaké soustavy, potom

$$t^1\xi_1 + t^2\xi_2 + \cdots + t^r\xi_r, \quad t^1, t^2, \ldots, t^r \in P,$$

je obecné řešení soustavy a

$$\{t^1\xi_1 + t^2\xi_2 + \cdots + t^r\xi_r \,|\, t^1, t^2, \ldots, t^r \in P\}$$

je množina všech řešení soustavy.

**Homogenní soustava rovnic k zadanému fundamentálnímu systému řešení.** Pro libovolnou lineárně nezávislou množinu $\{\xi_1, \xi_2, \ldots, \xi_r\} \subset P^n$ existuje homogenní soustava lineárních rovnic taková, že $\{\xi_1, \xi_2, \ldots, \xi_r\}$ je její fundamentální systém řešení. Takových soustav, vzájemně ekvivalentních, existuje více. Uvedeme postup nalezení jedné z nich.

Množina $\{\xi_1, \xi_2, \ldots, \xi_r\}$ uspořádaných $n$-tic prvků pole $P$ má být fundamentální systém řešení soustavy, takže hledáme homogenní soustavu

$$\begin{aligned} a_1^1 x^1 + \quad & a_2^1 x^2 + \cdots + \quad a_n^1 x^n = 0 \\ a_1^2 x^1 + \quad & a_2^2 x^2 + \cdots + \quad a_n^2 x^n = 0 \\ & \vdots \\ a_1^{n-r} x^1 + a_2^{n-r} x^2 + \cdots + a_n^{n-r} x^n &= 0 \end{aligned} \qquad \text{resp.} \quad Ax = 0$$

lineárních rovnic nad polem $P$ o $n$ neznámých $x^1, x^2, \ldots, x^n$, jejíž matice $A = (a_j^i)$ má hodnost $n - r$. Je tedy potřeba najít vhodné koeficienty $a_j^i$.

Jednotlivé uspořádané $n$-tice $\xi_1, \xi_2, \ldots, \xi_r$ mají být řešení soustavy $Ax = 0$, takže po jejich dosazení za $x$ dostaneme $r \cdot (n - r)$ homogenních rovnic o celkem $n \cdot (n - r)$ neznámých $a_j^i$, $i \in \{1, \ldots, n - r\}$, $j \in \{1, \ldots, n\}$. Ovšem, pro každé $k \in \{1, \ldots, r\}$ dosazením $\xi_k$ za $x$ dostaneme $A\xi_k = 0$, což představuje $n - r$ rovnic

$$\begin{aligned} \xi_k^1 a_1^1 + \quad & \xi_k^2 a_2^1 + \cdots + \quad \xi_k^n a_n^1 = 0 \\ \xi_k^1 a_1^2 + \quad & \xi_k^2 a_2^2 + \cdots + \quad \xi_k^n a_n^2 = 0 \\ & \vdots \\ \xi_k^1 a_1^{n-r} + \xi_k^2 a_2^{n-r} + \cdots + \xi_k^n a_n^{n-r} &= 0, \end{aligned}$$

z nichž každá má jiných $n$ neznámých $a_1^j, \ldots, a_n^j$, $j \in \{1, \ldots, n - r\}$, ale všechny mají stejné koeficienty $\xi_k^1, \ldots, \xi_k^n$, takže všechny mají stejnou množinu všech řešení a stačí pro každé $k \in \{1, \ldots, r\}$ uvažovat jen jednu rovnici

$$\xi_k^1 a^1 + \xi_k^2 a^2 + \cdots + \xi_k^n a^n = 0$$

s neznámými $a^1, a^2, \ldots, a^n$. Dosazením všech $\xi_1, \xi_2, \ldots, \xi_r$ tak dostaneme homogenní soustavu

$$\begin{aligned} \xi_1^1 a^1 + \xi_1^2 a^2 + \cdots + \xi_1^n a^n &= 0 \\ \xi_2^1 a^1 + \xi_2^2 a^2 + \cdots + \xi_2^n a^n &= 0 \\ & \vdots \\ \xi_r^1 a^1 + \xi_r^2 a^2 + \cdots + \xi_r^n a^n &= 0 \end{aligned}$$

$r$ lineárních rovnic o $n$ neznámých $a^1, a^2, \ldots, a^n$ s maticí $\Xi$, jejíž řádky jsou tvořeny uspořádanými $n$-ticemi $\xi_1, \xi_2, \ldots, \xi_r$. Hodnost matice $\Xi$ je tedy rovna $r$, fundamentální systém řešení má $n - r$ prvků $(a_1^1, a_2^1, \ldots, a_n^1), (a_1^2, a_2^2, \ldots, a_n^2), \ldots, (a_1^{n-r}, a_2^{n-r}, \ldots, a_n^{n-r})$ a toto jsou řádky hledané matice $A$.

**Příklad.** Nechť $\xi_1 = (1, 2, 3, 4), \xi_2 = (4, 3, 2, 1) \in \mathbb{R}^4$. Najdeme homogenní soustavu lineárních rovnic nad polem $\mathbb{R}$, jejímž fundamentálním systémem řešení je

$$\{\xi_1, \xi_2\}.$$

Hledáme tedy soustavu $Ax = 0$ dvou rovnic o čtyřech neznámých. Sestavíme soustavu $\Xi \cdot a = 0$, kde

$$\Xi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \text{a} \quad a = \begin{pmatrix} a^1 \\ a^2 \\ a^3 \\ a^4 \end{pmatrix}.$$

Tedy,

$$\begin{aligned} a^1 + 2a^2 + 3a^3 + 4a^4 &= 0 \\ 4a^1 + 3a^2 + 2a^3 + a^4 &= 0. \end{aligned}$$

Fundamentální systém řešení této soustavy je, například,

$$\{(2, -3, 0, 1), (1, -2, 1, 0)\}.$$

Zvolíme-li

$$A = \begin{pmatrix} a_1^1 & a_2^1 & a_3^1 & a_4^1 \\ a_1^2 & a_2^2 & a_3^2 & a_4^2 \end{pmatrix} = \begin{pmatrix} 2 & -3 & 0 & 1 \\ 1 & -2 & 1 & 0 \end{pmatrix},$$

dostaneme soustavu

$$\begin{pmatrix} 2 & -3 & 0 & 1 \\ 1 & -2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x^1 \\ x^2 \\ x^3 \\ x^4 \end{pmatrix} = 0$$

tedy

$$\begin{aligned} 2x^1 - 3x^2 + x^4 &= 0 \\ x^1 - 2x^2 + x^3 &= 0. \end{aligned}$$

Potom $\{(1, 2, 3, 4), (4, 3, 2, 1)\}$ je fundamentální systém řešení této soustavy,

$$t^1(1, 2, 3, 4) + t^2(4, 3, 2, 1), \quad t^1, t^2 \in \mathbb{R},$$

je její obecné řešení a

$$\{t^1(1, 2, 3, 4) + t^2(4, 3, 2, 1) \mid t^1, t^2 \in \mathbb{R}\}$$

je množina všech řešení soustavy. □

## 3.6. Nehomogenní soustavy lineárních rovnic

**Definice 3.6.1.** Soustava lineárních rovnic s nenulovou pravou stranou je *nehomogenní*. Je-li $Ax = b$ nehomogenní soustava, potom $Ax = 0$ je *homogenizovaná soustava*.

**Příklad.** (1) Soustava

$$\begin{aligned} x^1 + 2x^2 - x^3 &= 1 \\ -x^1 + x^2 + 2x^3 &= 0 \\ 2x^1 - x^2 + x^3 &= 3 \end{aligned}$$

je nehomogenní.

(2) Soustava

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

je nehomogenní. □

**Tvrzení 3.6.1.** *(1) Pokud nehomogenní soustava lineárních rovnic má právě jedno řešení, potom homogenizovaná soustava má jen nulové řešení.*

*(2) Nehomogenní soustava lineárních rovnic se čtvercovou maticí má právě jedno řešení právě tehdy, když homogenizovaná soustava má jen nulové řešení.*

*(3) Nehomogenní soustava lineárních rovnic se čtvercovou maticí má právě jedno řešení právě tehdy, když matice soustavy je regulární.*

*(4) Nehomogenní soustava lineárních rovnic nemá nulové řešení.*

*Důkaz.* (1) Má-li soustava právě jedno řešení, potom žádná z neznámých není parametr a homogenizovaná soustava má jen nulové řešení.
(2) Vyplývá z předchozího bodu a z Gaussovy eliminační metody.
(3) Vyplývá z předchozího bodu a z Tvrzení 3.5.1.
(4) Zřejmé. □

Množina všech řešení nehomogenní soustavy nemá vlastnosti uvedené v Tvrzení 3.5.2, které má množina všech řešení homogenní soustavy. Totiž, součet řešení nehomogenní soustavy není její řešení, $c$-násobek řešení nehomogenní soustavy, kde $c \neq 1$, není její řešení a lineární kombinace řešení nehomogenní soustavy není její řešení.

**Tvrzení 3.6.2.** *Nechť $\xi_p$ je nějaké řešení soustavy $Ax = b$. Potom pro každé řešení $\xi$ této soustavy existuje jediné řešení $\xi_0$ homogenizované soustavy takové, že $\xi = \xi_p + \xi_0$.*
*Na druhou stranu, pro libovolné řešení $\xi_0$ homogenizované soustavy je $\xi = \xi_p + \xi_0$ řešení soustavy $Ax = b$.*

*Důkaz.* Buďte $\xi_p$ a $\xi$ řešení soustavy. Položme $\xi_0 = \xi - \xi_p$. Potom $A\xi_0 = A(\xi - \xi_p) = A\xi - A\xi_p = b - b = 0$. Tedy, $\xi_0$ je řešení homogenizované soustavy a $\xi = \xi_0 + \xi_p$. Jednoznačnost $\xi_0$ je zřejmá.
Je-li $A\xi_0 = 0$, pak $A\xi = A(\xi_p + \xi_0) = A\xi_p + A\xi_0 = b + 0 = b$. □

**Důsledek.** *(1) Má-li nehomogenní soustava řešení, potom její obecné řešení je součtem obecného řešení homogenizované soustavy a nějakého partikulárního řešení nehomogenní soustavy.*
*(2) Je-li $\xi_p$ řešení soustavy $Ax = b$, potom množina všech řešení této soustavy je*

$$\{\xi_p + \xi_0 \,|\, \xi_0 \text{ je řešení homogenizované soustavy } Ax = 0\}.$$

**Cvičení.** Rozdíl libovolných dvou řešení nehomogenní soustavy je řešení homogenizované soustavy. □

**Příklad.** (1) Jedno z řešení soustavy

$$x^1 - x^2 = 1$$

je $(1, 0)$. Množina všech řešení homogenizované soustavy

$$x^1 - x^2 = 0$$

je $\{(t, t) \,|\, t \in \mathbb{R}\}$. Množina všech řešení nehomogenní soustavy

$$x^1 - x^2 = 1$$

je $\{(1, 0) + (t, t) \,|\, t \in \mathbb{R}\} = \{(1 + t, t) \,|\, t \in \mathbb{R}\}$.
(2) Soustava

$$\begin{aligned} x^1 + 2x^2 &= 0 \\ 3x^1 + 4x^2 &= 2 \end{aligned}$$

má řešení $(2, -1)$. Množina všech řešení homogenizované soustavy

$$\begin{aligned} x^1 + 2x^2 &= 0 \\ 3x^1 + 4x^2 &= 0 \end{aligned}$$

je $\{(0,0)\}$. Množina všech řešení nehomogenní soustavy

$$x^1 + 2x^2 = 0$$
$$3x^1 + 4x^2 = 2$$

je $\{(2,-1)+(0,0)\} = \{(2,-1)\}$. □

# 4. Polynomy

## 4.1. Polynomy, algebraické vlastnosti, dělitelnost

**Definice 4.1.1.** Buď $P$ pole, $n \in \mathbb{N}$, $a_0, \ldots, a_n \in P$, $x \notin P$. *Polynom* (*mnohočlen*) jedné neurčité $x$ nad polem $P$ je výraz tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Zde $x^i$ jsou mocniny, nejedná se o horní indexy. Mocninu $x^0$ klademe rovnu $1 \in P$, takže $a_0 = a_0 \cdot 1 = a_0 x^0$. Množinu všech polynomů neurčité $x$ nad polem $P$ označujeme $P[x]$.
Prvky $a_0, \ldots, a_n \in P$ jsou *koeficienty*, $a_i$ je *$i$-tý koeficient*. Koeficient $a_0$ je *absolutní člen*.
Polynom se všemi koeficienty nulovými je *nulový polynom* a označujeme ho 0.

Sčítance $a_i x^i$ s nulovými koeficienty $a_i$ se v zápisu polynomu obvykle neuvádí, ty s nenulovými koeficienty se samozřejmě uvádí a neuvedené koeficienty $a_i$ jsou tedy nulové.

Vyjádření „polynom nad polem $P$“ tedy znamená, že se jedná o „polynom s koeficienty z pole $P$“.

**Příklad.** $6x^4 + 0x^3 + 3x^2 + 1x + 6 \in \mathbb{R}[x]$, $a_0 = 6$, $a_1 = 1$, $a_2 = 3$, $a_3 = 0$, $a_4 = 6$, pro $i > 4$ $a_i = 0$. □

**Definice 4.1.2.** Polynomy $f, g \in P[x]$,

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$
$$g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

se sobě *rovnají*, jestliže se rovnají jejich příslušné koeficienty. Tedy,

$$f = g, \text{ jestliže } a_i = b_i \text{ pro všechna nezáporná celá } i.$$

**Definice 4.1.3.** *Stupeň* polynomu $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ je největší číslo $s$ takové, že $a_s \neq 0$, označujeme ho $\deg f$. Koeficient $a_s$, kde $s$ je stupeň, je *vedoucí koeficient* polynomu $f$, označujeme ho $\operatorname{lc} f$.

Pro nulový polynom nemáme definován ani stupeň ani vedoucí koeficient.

**Příklad.** Pro $f = 6x^4 + 3x^2 + x + 6$ je $\deg f = 4$ a $\operatorname{lc} f = 6$. □

**Definice 4.1.4.** Nulový polynom a polynomy stupně 0 jsou *konstantní*, polynomy stupně 1 jsou *lineární*, polynomy stupně 2 jsou *kvadratické*, polynomy stupně 3 jsou *kubické*, polynomy stupně 4 jsou *bikvadratické*.

**Definice 4.1.5.** Pro polynomy $f, g \in P[x]$,

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$
$$g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0,$$

označme $p = \max\{n, m\}$. *Součet* polynomů $f$ a $g$ je polynom $f + g \in P[x]$,

$$f + g = (a_p + b_p) x^p + (a_{p-1} + b_{p-1}) x^{p-1} + \cdots + (a_1 + b_1) x + a_0 + b_0.$$

**Definice 4.1.6.** *Součin* polynomů $f, g \in P[x]$,

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$
$$g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

je polynom $fg \in P[x]$,

$$\begin{aligned} fg &= \sum_{k=0}^{n+m} \Big( \sum_{i+j=k} a_i b_j \Big) x^k = \\ &= a_n b_m x^{n+m} + \\ &\quad + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \\ &\quad \vdots \\ &\quad + (a_2 b_0 + a_1 b_1 + a_0 b_2) x^2 + \\ &\quad + (a_1 b_0 + a_0 b_1) x + \\ &\quad + a_0 b_0. \end{aligned}$$

Tedy, pro $k \in \{0, 1, \ldots, n+m\}$ $k$-tý koeficient polynomu $fg$ je

$$\sum_{i+j=k} a_i b_j = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k.$$

Je-li například $f$ konstantní polynom, $f = a_0$, pak

$$fg = a_0 g = a_0 b_m x^m + a_0 b_{m-1} x^{m-1} + \cdots + a_0 b_1 x + a_0 b_0.$$

Speciálně, pokud $f = -1$, pak

$$fg = -g = -b_m x^m - b_{m-1} x^{m-1} - \cdots - b_1 x - b_0$$

je polynom *opačný* k polynomu $g$.

**Příklad.** Pro

$$f = 6x^4 + 3x^2 + 6, \qquad g = x^3 - 2x^2 - x$$

je

$$f + g = 6x^4 + x^3 + x^2 - x + 6,$$
$$fg = 6x^7 - 12x^6 - 3x^5 - 6x^4 + 3x^3 - 12x^2 - 6x. \qquad \square$$

**Tvrzení 4.1.1.** *Buďte $f, g \in P[x]$ nenulové. Potom*

*(1) $fg$ je nenulový polynom,*
*(2)* $\deg(fg) = \deg f + \deg g$,
*(3)* $\operatorname{lc}(fg) = \operatorname{lc} f \cdot \operatorname{lc} g$.

*Důkaz.* Buďte $f, g$ nenulové polynomy. Nechť $\deg f = n$, $\deg g = m$, $\operatorname{lc} f = a_n$ a $\operatorname{lc} g = b_m$. Jelikož $a_n \neq 0$, $b_m \neq 0$ a $(n+m)$-tý koeficient součinu $fg$ je roven $a_n b_m$, je $fg$ nenulový polynom. Pro $k > n + m$ je $k$-tý koeficient roven nule, takže $\operatorname{lc} fg = a_n b_m = \operatorname{lc} f \cdot \operatorname{lc} g$ a $\deg(fg) = n + m = \deg f + \deg g$. $\square$

**Cvičení.** Součin polynomů je nulový právě tehdy, když aspoň jeden z nich je nulový. $\square$

**Tvrzení 4.1.2.** *Buďte $f, g, h \in P[x]$. Potom*

*(1)* $f+g=g+f$,
*(2)* $f+(g+h)=(f+g)+h$,
*(3)* $f+0=f$,
*(4)* $f+(-f)=0$,
*(5)* $f\cdot g=g\cdot f$,
*(6)* $f\cdot(g\cdot h)=(f\cdot g)\cdot h$,
*(7)* $f\cdot 1=f$,
*(8)* $f\cdot(g+h)=f\cdot g+f\cdot h$.

*Důkaz.* Cvičení. □

**Tvrzení 4.1.3.** *Nechť* $f,g,h\in P[x]$, $fg=fh$ *a* $f\neq 0$. *Pak* $g=h$.

*Důkaz.* Jestliže $fg=fh$, pak $f(g-h)=0$ a aspoň jeden z polynomů $f$ a $g-h$ je nulový. Podle předpokladu $f\neq 0$, takže $g-h=0$ a $g=h$. □

Podobně jako v případě matic nebo v případě prvků nějakého pole je možné definovat inverzní polynom.

**Definice 4.1.7.** Buďte $f,g\in P[x]$. Polynom $g$ je *inverzní* k polynomu $f$, jestliže $fg=gf=1$. Inverzní polynom k polynomu $f$ značíme $f^{-1}$. Polynom, ke kterému existuje polynom inverzní, je *invertibilní*. Množina všech invertibilních prvků $P[x]$ nebo $P$ se značí $P[x]^*$, resp. $P^*$.

**Tvrzení 4.1.4.** *Invertibilní polynomy jsou právě nenulové konstantní polynomy (tedy polynomy stupně* 0*).*

*Důkaz.* Existuje-li k polynomu $f$ inverze $f^{-1}$, potom $ff^{-1}=1$ a oba polynomy $f, f^{-1}$ jsou nenulové. Dále $\deg f\leq \deg f+\deg f^{-1}=\deg(ff^{-1})=\deg 1=0$. Takže $\deg f=0$ a $f$ je tedy nenulový konstantní polynom.

Na druhou stranu, pokud $f$ je nenulový konstantní polynom, můžeme ho ztotožnit s příslušným prvkem pole, ke kterému díky vlastnostem pole existuje prvek inverzní a ten zase můžeme ztotožnit s příslušným polynomem, který je tedy inverzní k $f$. □

Nyní se budeme věnovat dělitelnosti polynomů. Teorie dělitelnosti polynomů a teorie dělitelnosti celých čísel si jsou dosti podobné.

**Definice 4.1.8.** Buďte $f,g\in P[x]$. Polynom $g$ *dělí* polynom $f$, jestliže existuje polynom $h\in P[x]$ takový, že $f=gh$. Pak také polynom $g$ je *dělitel* polynomu $f$ a polynom $f$ je *dělitelný* polynomem $g$. Zapisujeme $g\mid f$.

**Cvičení.** Jestliže $g\mid f$ a $f\neq 0$, pak $\deg g\leq\deg f$. □

**Příklad.** (1) $x\mid x^2-x$, protože $x^2-x=x(x-1)$.
(2) $x$ nedělí $x^2+1$. Aby $x\cdot h$ byl polynom stupně 2, $h$ musí být stupně 1, ale pro jakýkoliv polynom $h=a_1x+a_0$ stupně 1 platí $x\cdot h=a_1x^2+a_0x$. □

**Cvičení.** (1) Ukažte, že $x-1\mid x^n-1$ pro každé celé $n>1$.
(2) Ukažte, že relace $\mid$ je reflexivní a tranzitivní. □

**Tvrzení 4.1.5.** *Buďte* $f,g,h\in P[x]$.
*(1)* $f\mid f$ *a* $f\mid 0$.
*(2) Jestliže* $f\mid g$ *a* $g\mid h$, *pak* $f\mid h$.
*(3) Jestliže* $f\mid g$ *a* $f\mid h$, *pak* $f\mid(g+h)$.
*(4) Jestliže* $f\mid g$, *pak* $f\mid(gh)$.
*(5) Jestliže* $fg\mid fh$ *a* $f\neq 0$, *pak* $g\mid h$.

*Důkaz.* Cvičení. □

Podobně jako v případě celých čísel i v případě polynomů existuje dělení se zbytkem (nebo neúplné dělení).

**Tvrzení 4.1.6.** *Buďte $f, g \in P[x]$, $g \neq 0$. Pak existuje právě jedna dvojice $q, r \in P[x]$ taková, že*

*(i)* $f = gq + r$;
*(ii)* *buď* $r = 0$ *nebo* $\deg r < \deg g$.

*Důkaz.* Jestliže $f = 0$, tak pro dvojici $q = 0$, $r = 0$ jsou splněny podmínky (i) a (ii).

Předpokládejme, že $f \neq 0$. Položme $q_0 = 0$ a $r_0 = f$ a definujme rekurzivně

$$q_{i+1} = q_i + \frac{\operatorname{lc} r_i}{\operatorname{lc} g} \cdot x^{\deg r_i - \deg g}, \qquad r_{i+1} = r_i - \frac{\operatorname{lc} r_i}{\operatorname{lc} g} \cdot x^{\deg r_i - \deg g} \cdot g.$$

Potom pro každé $i$ platí $f = gq_i + r_i$ a buď $r_{i+1} = 0$ nebo $\deg r_{i+1} < \deg r_i$. Proto pro nějaké $i$ buď $r_i = 0$ nebo $\deg r_i < \deg g$. V takovém případě v rekurzi nepokračujeme a poslední dvojice $q_i, r_i$ je hledaná dvojice $q, r$.

Ještě je třeba dokázat jednoznačnost. Předpokládejme, že pro dvojice $q_1, r_1$ a $q_2, r_2$ jsou splněny podmínky (i) a (ii). Tedy,

$$f = gq_1 + r_1 = gq_2 + r_2, \text{ čili } g(q_1 - q_2) = r_2 - r_1 \text{ a } g \mid r_2 - r_1 \tag{1}$$

$$r_1 = 0 \text{ nebo } \deg r_1 < \deg g \tag{2}$$

$$r_2 = 0 \text{ nebo } \deg r_2 < \deg g. \tag{3}$$

Kdyby $r_2 - r_1 \neq 0$, tak z (1) vyplývá, že $\deg g \leq \deg(r_2 - r_1)$, zatímco z (2) a (3) vyplývá, že $\deg(r_2 - r_1) < \deg g$. Dostáváme spor, takže $r_2 - r_1 = 0$, čili $r_1 = r_2$. Vzhledem k tomu, že $g \neq 0$, z $g(q_1 - q_2) = 0$ vyplývá, že $q_1 - q_2 = 0$, čili $q_1 = q_2$. □

**Definice 4.1.9.** V předchozím tvrzení $q$ je *částečný podíl* (*podíl*, je-li $r = 0$) polynomů $f$ a $g$ (v tomto pořadí) a $r$ je příslušný *zbytek*.

Je zřejmé, že $g \mid f$ právě tehdy, když zbytek při (částečném) podílu polynomů $f$ a $g$ je roven nule.

**Příklad.** Buďte $f, g \in \mathbb{R}[x]$,

$$f = x^5 + 2x^3 + 2x + 4 \qquad \text{a} \qquad g = x^2 + x + 2.$$

Tedy $q_0 = 0$, $r_0 = f$ a polynomy $q_1, \ldots, q_4$ a $r_1, \ldots, r_4$ je možné získat pomocí schématu

$$\begin{array}{l}
(x^5 + 2x^3 + 2x + 4) : (x^2 + x + 2) = \underbrace{x^3}_{q_1} \underbrace{- x^2}_{q_2} \underbrace{+ x}_{q_3} \underbrace{+ 1 + \frac{-x+2}{x^2+x+2}}_{q_4} \\
\underline{-(x^5 + x^4 + 2x^3)} \\
r_1 = -x^4 + 2x + 4 \\
\quad \underline{-(-x^4 - x^3 - 2x^2)} \\
r_2 = x^3 + 2x^2 + 2x + 4 \\
\quad \underline{-(x^3 + x^2 + 2x)} \\
r_3 = x^2 + 4 \\
\quad \underline{-(x^2 + x + 2)} \\
r_4 = -x + 2
\end{array}$$

Čili

$$q_0 = 0 \qquad r_0 = x^5 + 2x^3 + 2x + 4$$
$$q_1 = x^3 \qquad r_1 = -x^4 + 2x + 4$$
$$q_2 = x^3 - x^2 \qquad r_2 = x^3 + 2x^2 + 2x + 4$$
$$q_3 = x^3 - x^2 + x \qquad r_3 = x^2 + 4$$
$$q_4 = x^3 - x^2 + x + 1 \qquad r_4 = -x + 2$$

a je snadné ověřit, že $f = gq_i + r_i$ pro každé $i \in \{0, 1, 2, 3, 4\}$.

Jelikož $\deg r_4 = 1 < 2 = \deg g$,

částečný podíl $q = q_4 = x^3 - x^2 + x + 1$ a zbytek $r = r_4 = -x + 2$.

Tedy

$$f = x^5 + 2x^3 + 2x + 4 = gq + r = (x^2 + x + 2) \cdot (x^3 - x^2 + x + 1) + (-x + 2). \quad \square$$

**Definice 4.1.10.** *Normovaný* polynom je nenulový polynom, jehož vedoucí koeficient je 1.

Je-li $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ nenulový polynom s $\operatorname{lc} f = a_n \neq 0$, pak

$$\bar{f} = \frac{1}{\operatorname{lc} f} f = x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \cdots + \frac{a_1}{a_n}x + \frac{a_0}{a_n}$$

je normovaný polynom. Polynomy $f, \bar{f}$ jsou z hlediska dělitelnosti rovnocenné ($f \mid \bar{f}$ a $\bar{f} \mid f$).

**Lemma 4.1.7.** *Buďte $f, g$ normované polynomy takové, že $f \mid g$ a $g \mid f$. Potom $f = g$.*

*Důkaz.* Předpokládejme, že $f \mid g$ a zároveň $g \mid f$. Potom existují polynomy $p, q \in P[x]$ tak, že $g = fp$ a $f = gq$. Máme $f = fpq$ a tedy $1 = pq$. Polynomy $p, q$ jsou tedy nenulové konstantní polynomy a $1 = \operatorname{lc} g = \operatorname{lc}(fp) = \operatorname{lc} f \cdot \operatorname{lc} p = 1 \cdot p = p$. Takže $g = fp = f$. $\square$

Relace dělitelnosti mezi normovanými polynomy je tedy navíc antisymetrická, čili je to uspořádání a máme uspořádanou množinu všech normovaných polynomů.

## 4.2. Největší společný dělitel

**Definice 4.2.1.** Buďte $f, g \in P[x]$. Polynom $d \in P[x]$ je *největší společný dělitel* polynomů $f, g$, jestliže

(1) $d \mid f$ a $d \mid g$;
(2) když $h \in P[x]$, $h \mid f$ a $h \mid g$, pak $h \mid d$;
(3) $d$ je normovaný.

Zapisujeme $d = D(f, g)$.

**Definice 4.2.2.** Polynomy, jejichž největší společný dělitel je 1, jsou *nesoudělné*.

**Příklad.** (1) $D(2x, x^2) = x$.

(2) Polynomy $x$ a $x + 1$ jsou nesoudělné. Oba polynomy jsou stupně 1, proto jejich dělitele jsou stupně buď 1 nebo 0. Lineární dělitele polynomu $x$ jsou $cx$, kde $c \in P$, ale žádný z nich není dělitelem $x + 1$. Společné dělitele polynomů $x$ a $x + 1$ jsou tedy jen nenulové konstantní polynomy a jelikož největší společný dělitel je navíc normovaný, $D(x, x + 1) = 1$.

(3) Pokud $f = g = 0$, pak neexistuje jejich největší společný dělitel.
(4) Pro $f \neq 0$ $D(f, 0) = \bar{f}$. □

**Tvrzení 4.2.1** (Eukleidův algoritmus)**.** *Buďte $f, g \in P[x]$ nenulové polynomy. Buď $r_0, r_1, r_2, r_3, \ldots$ posloupnost polynomů taková, že $r_0 = f$, $r_1 = g$ a jsou-li známy $r_i, r_{i+1}$, pak $r_{i+2}$ získáme neúplným dělením polynomu $r_i$ polynomem $r_{i+1}$:*

$$r_i = r_{i+1}q_i + r_{i+2}, \quad \text{buď } r_{i+2} = 0 \text{ nebo } \deg r_{i+2} < \deg r_{i+1}.$$

*Potom existuje index $N$ takový, že $r_{N-1} \neq 0$ a $r_N = 0$.*

*Důkaz.* Jelikož $\deg g = \deg r_1 > \deg r_2 > \deg r_3 > \ldots$ je klesající posloupnost nezáporných celých čísel, existuje $N \in \mathbb{N}$ takové, že $r_{N-1} \neq 0$ a $r_N = 0$. □

**Příklad.** Buďte $f, g \in \mathbb{R}[x]$,

$$f = x^5 + 2x^3 + 2x + 4 \qquad \text{a} \qquad g = x^2 + x + 2.$$

Tedy $r_0 = f$, $r_1 = g$ a už víme, že $f = g \cdot (x^3 - x^2 + x + 1) + (-x + 2)$, takže

$$r_2 = -x + 2 \qquad \text{a} \qquad q_0 = x^3 - x^2 + x + 1.$$

Dělením polynomu $r_1$ polynomem $r_2$

$$\begin{array}{r} (x^2 + \ x + 2) : (-x + 2) = -x - 3 + \frac{8}{-x+2} \\ \underline{-(x^2 - 2x)} \\ 3x + 2 \\ \underline{-(-3x - 6)} \\ 8 \end{array}$$

dostaneme

$$r_3 = 8 \qquad \text{a} \qquad q_1 = -x - 3.$$

Dělením polynomu $r_2$ polynomem $r_3$

$$\begin{array}{r} (-x + 2) : (8) = -\frac{x}{8} + \frac{2}{8} \\ \underline{-(-x)} \\ 2 \\ \underline{-2} \\ 0 \end{array}$$

dostaneme

$$r_4 = 0 \qquad \text{a} \qquad q_2 = -\frac{x}{8} + \frac{2}{8}.$$

V tomto případě tedy $N = 4$. □

**Tvrzení 4.2.2.** *Pro libovolné dva polynomy, z nichž aspoň jeden je nenulový, existuje právě jeden jejich největší společný dělitel.*

*Důkaz.* Buďte $f, g \in P[x]$. Je-li $f \neq 0$ a $g = 0$, $D(f, 0) = \bar{f}$. Předpokládejme, že $f, g$ jsou nenulové, a aplikujme Eukleidův algoritmus. Buď $N \in \mathbb{N}$ takové, že $r_{N-1} \neq 0$ a $r_N = 0$.

Označme $d = \bar{r}_{N-1}$ (normovaný polynom). Zřejmě $d \mid r_{N-1}$ a $d \mid r_N$. Je-li $d$ dělitel polynomů $r_{i+1}$ a $r_{i+2}$, pak je dělitel i polynomu $r_i = r_{i+1}q_i + r_{i+2}$. Postupně tedy dostaneme, že $d \mid r_i$ pro všechna $i \in \{0, \ldots, N\}$, včetně $d \mid r_1 = g$ a $d \mid r_0 = f$.

Buď $h \in P[x]$ takové, že $h \mid f = r_0$ a $h \mid g = r_1$. Je-li $h$ dělitel polynomů $r_i$ a $r_{i+1}$, pak je dělitel i polynomu $r_{i+2} = r_i - r_{i+1}q_i$. Takto postupně dostaneme, že $h \mid r_i$ pro všechna $i \in \{0, \ldots, N\}$, včetně $h \mid r_{N-1} = d$. Tedy, $d = D(f, g)$.

Buďte $d_1, d_2$ největší společné dělitele polynomů. Podle definice největšího společného dělitele $d_1 \mid d_2$ a $d_2 \mid d_1$ a jelikož $d_1, d_2$ jsou normované, $d_1 = d_2$. □

**Příklad.** Buďte $f, g \in \mathbb{R}[x]$,

$$f = x^5 + 2x^3 + 2x + 4 \qquad \text{a} \qquad g = x^2 + x + 2.$$

Už víme, že $N = 4$ a $r_3 = 8$, čili $D(f, g) = \bar{r}_3 = 1$. □

**Tvrzení 4.2.3** (Bézoutova věta)**.** *Buďte $f, g \in P[x]$ polynomy, z nichž aspoň jeden je nenulový. Pak existují polynomy $u, v \in P[x]$ takové, že $D(f, g) = fu + gv$.*

*Důkaz.* Označme $I = \{fu + gv \mid u, v \in P[x]\}$. V množině $I$ existuje normovaný prvek minimálního stupně, označme jej $d$. Tedy, $d = fu + gv$ pro nějaká $u, v \in P[x]$.

Po dělení se zbytkem dostaneme $f = dq + r$, kde buď $r = 0$ nebo $\deg r < \deg d$. Zároveň $r = f - dq = f - (fu + gv)q = f(1 - uq) + g(-vq) \in I$. Kdyby $r \neq 0$, byl by to nenulový prvek $I$ stupně nižšího než $\deg d$. Takže $r = 0$ a tedy $d \mid f$. Analogicky $d \mid g$.

Buď $h \in P[x]$ společný dělitel $f$ a $g$. Pak $h$ je dělitel i polynomu $fu + gv = d$. Tedy, $d = D(f, g)$. □

Pomocí Rozšířeného Eukleidova algoritmu lze získat nejen $D(f, g)$, ale i polynomy $u, v$ z předchozího tvrzení.

**Tvrzení 4.2.4** (Rozšířený Eukleidův algoritmus)**.** *Buďte $f, g \in P[x]$ nenulové polynomy. Buďte $r_0, r_1, r_2, \ldots, r_{N-1}$ a $q_0, q_1, q_2, \ldots, q_{N-3}$ posloupnosti polynomů z Eukleidova algoritmu. Buďte*

$$u_0 = 1, u_1 = 0, u_2, \ldots, u_{N-1},$$
$$v_0 = 0, v_1 = 1, v_2, \ldots, v_{N-1},$$

*posloupnosti polynomů takové, že $u_i = u_{i+1}q_i + u_{i+2}$ a $v_i = v_{i+1}q_i + v_{i+2}$ pro všechna $i \in \{0, \ldots, N-3\}$. Potom $r_{N-1} = fu_{N-1} + gv_{N-1}$ a označíme-li*

$$u = \frac{1}{\operatorname{lc} r_{N-1}} u_{N-1} \qquad a \qquad v = \frac{1}{\operatorname{lc} r_{N-1}} v_{N-1},$$

*pak $D(f, g) = fu + gv$.*

*Důkaz.* Podle Eukleidova algoritmu a podle předpokladů

$$r_0 = f, \quad r_1 = g, \qquad u_0 = 1, \quad u_1 = 0, \qquad v_0 = 0, \quad v_1 = 1$$

a pro $i \in \{0, \ldots, N-3\}$

$$r_i = r_{i+1}q_i + r_{i+2}, \qquad \text{tedy} \quad r_{i+2} = r_i - r_{i+1}q_i, \tag{4}$$
$$u_i = u_{i+1}q_i + u_{i+2}, \qquad \text{tedy} \quad u_{i+2} = u_i - u_{i+1}q_i, \tag{5}$$
$$v_i = v_{i+1}q_i + v_{i+2}, \qquad \text{tedy} \quad v_{i+2} = v_i - v_{i+1}q_i. \tag{6}$$

Matematickou indukcí ukážeme, že $r_i = fu_i + gv_i$ pro všechna $i \in \{0, \ldots, N-1\}$. Platí

$$r_0 = f = f \cdot 1 + g \cdot 0 = f \cdot u_0 + g \cdot v_0,$$
$$r_1 = g = f \cdot 0 + g \cdot 1 = f \cdot u_1 + g \cdot v_1.$$

Předpokládejme, že pro nějaké $k$ platí

$$r_k = fu_k + gv_k, \tag{7}$$
$$r_{k+1} = fu_{k+1} + gv_{k+1}. \tag{8}$$

Potom

$$\begin{aligned} r_{k+2} &= && \text{(podle (4))}\\ &= r_k - r_{k+1}q_k = && \text{(podle (7), (8))}\\ &= fu_k + gv_k - (fu_{k+1} + gv_{k+1})q_k =\\ &= f(u_k - u_{k+1}q_k) + g(v_k - v_{k+1}q_k) = && \text{(podle (5), (6))}\\ &= fu_{k+2} + gv_{k+2}. \end{aligned}$$

Takže, vztah $r_i = fu_i + gv_i$ platí pro $i = 0, i = 1$ a když platí pro $i = k$ a $i = k+1$, pak platí pro $i = k+2$. Z toho vyplývá, že platí pro každé $i \in \{0, \ldots, N-1\}$. Zbytek tvrzení je zřejmý. □

**Příklad.** Buďte $f, g \in \mathbb{R}[x]$,

$$f = x^5 + 2x^3 + 2x + 4 \qquad \text{a} \qquad g = x^2 + x + 2.$$

Už víme, že $D(f, g) = 1$, $N = 4$,

$$\begin{aligned} r_0 &= x^5 + 2x^3 + 2x + 4 & q_0 &= x^3 - x^2 + x + 1\\ r_1 &= x^2 + x + 2 & q_1 &= -x - 3\\ r_2 &= -x + 2\\ r_3 &= 8 \end{aligned}$$

$$\begin{aligned} u_0 &= 1 & v_0 &= 0\\ u_1 &= 0 & v_1 &= 1. \end{aligned}$$

Dále

$$\begin{aligned} u_0 &= u_1q_0 + u_2\\ 1 &= 0 \cdot q_0 + u_2 && \text{implikuje} && u_2 = 1,\\ v_0 &= v_1q_0 + v_2\\ 0 &= 1 \cdot q_0 + v_2 && \text{implikuje} && v_2 = -q_0 = -x^3 + x^2 - x - 1,\\ u_1 &= u_2q_1 + u_3\\ 0 &= 1 \cdot q_1 + u_3 && \text{implikuje} && u_3 = -q_1 = x + 3,\\ v_1 &= v_2q_1 + v_3\\ 1 &= -q_0 \cdot q_1 + v_3 && \text{implikuje} && v_3 = 1 + q_0q_1 = -x^4 - 2x^3 + 2x^2 - 4x - 2. \end{aligned}$$

Lze snadno ověřit, že $r_3 = fu_3 + gv_3$, a když

$$\begin{aligned} u &= \frac{x}{8} + \frac{3}{8}\\ v &= -\frac{x^4}{8} - \frac{x^3}{4} + \frac{x^2}{4} - \frac{x}{2} - \frac{1}{4} \end{aligned}$$

pak $D(f, g) = 1 = fu + gv$. □

## 4.3. Ireducibilní polynomy

**Definice 4.3.1.** Polynom je *reducibilní* nad polem $P$, jestliže je součinem dvou nekonstantních polynomů nad polem $P$. Polynom je *ireducibilní* nad polem $P$, jestliže není konstantní a není reducibilní nad polem $P$.

Pro polynom z $P[x]$ označením *reducibilní*, resp. *ireducibilní* se myslí *reducibilní nad* $P$, resp. *ireducibilní nad* $P$.

Je-li polynom $f$ reducibilní a $f = g \cdot h$, kde $g, h$ jsou nekonstantní polynomy, říká se také, že $g \cdot h$ je *rozklad* polynomu $f$ na součin polynomů $g, h$ nebo také, že $g \cdot h$ je *rozklad* polynomu $f$ na činitele $g, h$.

**Příklad.** (1) Každý polynom stupně 1 je ireducibilní, neboť není konstantní a součin dvou nekonstantních polynomů je polynom stupně aspoň 2.

(2) Polynom $x^2 - 1 = (x-1)(x+1)$ je reducibilní nad $\mathbb{R}$. Polynomy $x-1$ a $x+1$ jsou ireducibilní nad $\mathbb{R}$. □

**Cvičení.** Normovaný reducibilní polynom je součinem normovaných nekonstantních polynomů. □

**Tvrzení 4.3.1.** *Nechť jsou $f, g \in P[x]$ normované polynomy, $g$ je ireducibilní a $f \mid g$. Potom buď $f = 1$, anebo $f = g$. Je-li $f$ také ireducibilní, pak $f = g$.*

*Důkaz.* Když $f \mid g$, existuje $h \in P[x]$ takové, že $fh = g$. Jelikož $g$ je ireducibilní, právě jeden z polynomů $f, h$ je konstantní. Je-li normovaný polynom $f$ konstantní, pak $f = 1$. Je-li $h$ konstantní a $fh$ je normovaný polynom, pak $h = 1$, tedy $f = g$. Je-li $f$ ireducibilní, pak není konstantní, a zbývá tedy jen $f = g$. □

**Lemma 4.3.2.** *Buďte $g, h_1, \ldots, h_n \in P[x]$ normované ireducibilní polynomy a nechť $g \mid h_1 \cdots h_n$. Pak existuje index $j$ takový, že $g = h_j$.*

*Důkaz.* Označme $d = D(g, h_1)$. Jelikož $d \mid g$ a $g$ je ireducibilní, podle Tvrzení 4.3.1 buď $d = g$ anebo $d = 1$. Jestliže $d = g$, pak $g \mid h_1$ a $g = h_1$. Jestliže $d = 1$, pak Tvrzení 4.2.3

$$1 = gu + h_1 v$$

pro vhodné $u, v \in P[x]$. Vynásobíme-li obě strany polynomem $h_2 \cdots h_n$, dostaneme

$$h_2 \cdots h_n = g h_2 \cdots h_n u + h_1 h_2 \cdots h_n v.$$

Podle předpokladu $g \mid h_1 \cdots h_n$, takže pravá strana je dělitelná $g$, proto i levá strana je dělitelná $g$, čili $g \mid h_2 \cdots h_n$. Stejným postupem ukážeme, že buď $g = h_2$ anebo $g \mid h_3 \cdots h_n$. Opakováním tohoto postupu najdeme $j$, $1 \leq j \leq n$, takové, že $g = h_j$. □

**Tvrzení 4.3.3.** *Každý nekonstantní polynom je součinem konstanty a normovaných ireducibilních polynomů, přičemž všechny činitele jsou určeny jednoznačně až na pořadí.*

*Důkaz.* Buď $f \in P[x]$ nekonstantní polynom a označme $\bar{f} = \frac{1}{\operatorname{lc} f} \cdot f$. Je-li $\bar{f}$ ireducibilní, pak $f = \operatorname{lc} f \cdot \bar{f}$. Je-li $\bar{f}$ reducibilní, pak je součinem normovaných nekonstantních polynomů nižšího stupně. Každý z těchto polynomů je také buď ireducibilní nebo reducibilní, ve druhém případě je opět součinem normovaných nekonstantních polynomů nižšího stupně. Opakováním tohoto postupu po konečně mnoha krocích dojdeme ke konečnému počtu normovaných ireducibilních polynomů. Jejich počet je shora omezen stupněm polynomu $f$ a jejich součin je roven $\bar{f}$.

Ještě je potřeba dokázat jednoznačnost. Předpokládejme, že $\bar{f} = g_1 \cdots g_n = h_1 \cdots h_m$ a všechny činitele jsou normované ireducibilní polynomy. Jelikož $g_1 \mid h_1 \cdots h_m$, podle předchozího lemmatu existuje index $\varphi(1)$ takový, že $g_1 = h_{\varphi(1)}$. Takže rovnost $g_1 \cdots g_n = h_1 \cdots h_m$ můžeme zkrátit $g_1$ a na obou stranách rovnosti tedy bude o jednoho činitele méně. Obdobně dostaneme, že existuje index $\varphi(2)$ takový, že $g_2 = h_{\varphi(2)}$, a postupně až že existuje index $\varphi(n)$ takový, že $g_n = h_{\varphi(n)}$.

Navíc, $n \leq m$, protože jinak by $g_{m+1} \cdots g_n = 1$, což není možné, když všechny $g_i$ jsou nekonstantní polynomy. A obdobně dostaneme, že $m \leq n$. Takže $n = m$. □

**Příklad.** Polynom $x^2+1$ je reducibilní nad polem $\mathbb{C}$, protože $x^2+1=(x+i)(x-i)$. Tentýž polynom je ireducibilní nad polem $\mathbb{R}$, protože jakýkoliv jeho hypotetický rozklad $x^2+1=(x+\xi)(x+\eta)$, $\xi,\eta\in\mathbb{R}$ je současně rozkladem nad $\mathbb{C}$ různým od $x^2+1=(x+i)(x-i)$, ve sporu s jednoznačností rozkladu. □

**Důsledek.** *Buď $f\in P[x]$ a buďte $g_1,\dots,g_m\in P[x]$ normované ireducibilní a po dvou různé, tj. $g_i\neq g_j$ pro $i\neq j$. Jestliže $g_1^{k_1}\mid f$, …, $g_m^{k_m}\mid f$, pak $g_1^{k_1}\cdots g_m^{k_m}\mid f$.*

## 4.4. Kořeny a jejich násobnost

Pro $f=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in P[x]$ a $\xi\in P$, označme

$$f(\xi)=a_n\xi^n+a_{n-1}\xi^{n-1}+\cdots+a_1\xi+a_0\in P.$$

**Tvrzení 4.4.1.** *Pro libovolné polynomy $f,g\in P[x]$ a libovolný prvek $\xi\in P$ platí*

$$(f+g)(\xi)=f(\xi)+g(\xi),\quad (-f)(\xi)=-f(\xi),\quad (fg)(\xi)=f(\xi)g(\xi).$$

*Důkaz.* Cvičení. □

**Definice 4.4.1.** Prvek $\xi\in P$ je *kořen* polynomu $f\in P[x]$, jestliže $f(\xi)=0$.

**Tvrzení 4.4.2.** *Nechť $f\in P[x]$ a $\xi\in P$. Potom $\xi$ je kořen polynomu $f$ právě tehdy, když $x-\xi$ dělí $f$.*

*Důkaz.* Předpokládejme, že $\xi$ je kořen polynomu $f$. Dělením $f:(x-\xi)$ dostaneme

$$f=(x-\xi)q+r,\quad \text{kde buď } r=0 \text{ nebo } \deg r<\deg(x-\xi)=1,\ \text{čili } \deg r=0.$$

Takže v obou případech $r$ je konstantní polynom a $0=f(\xi)=(\xi-\xi)q(\xi)+r=r$. Čili $r=0$, $f=(x-\xi)q$ a $x-\xi$ dělí $f$.

Předpokládejme, že $x-\xi$ dělí $f$, tedy $f=(x-\xi)q$ pro nějaké $q$. Potom $f(\xi)=(\xi-\xi)q(\xi)=0$, čili $\xi$ je kořen polynomu $f$. □

**Definice 4.4.2.** Nechť $f\in P[x]$ a $\xi\in P$. Pokud $\xi$ je kořen $f$, potom polynom $x-\xi$ je *kořenový činitel* polynomu $f$.

**Definice 4.4.3.** Prvek $\xi\in P$ je *$k$-násobný kořen* polynomu $f\in P[x]$, jestliže $(x-\xi)^k$ dělí $f$, ale $(x-\xi)^{k+1}$ nedělí $f$.

**Tvrzení 4.4.3.** *Buďte $\xi_1,\dots,\xi_n\in P$ různé kořeny polynomu $f\in P[x]$ s násobnostmi po řadě $k_1,\dots,k_n$. Potom*

*(1)* $(x-\xi_1)^{k_1}\cdots(x-\xi_n)^{k_n}\mid f$;
*(2)* $k_1+\cdots+k_n\le\deg f$.

*Důkaz.* Cvičení. □

**Tvrzení 4.4.4** (Základní věta algebry)**.** *Každý nekonstantní polynom nad polem $\mathbb{C}$ má aspoň jeden kořen.*

Všechny známé důkazy využívají výsledky matematické analýzy, proto zde důkaz neuvádíme.

**Důsledek.** *Každý nekonstantní polynom nad polem $\mathbb{C}$ má rozklad na lineární činitele. Kořenů se započtením násobnosti má právě tolik, kolik činí jeho stupeň.*

Předchozí důsledek znamená, že pro každý nekonstantní polynom $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ stupně $n$ s komplexními koeficienty existují čísla $\xi_1, \xi_2, \ldots, \xi_n$ (nemusí být po dvou různá), pro která platí

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = a_n(x - \xi_1)(x - \xi_2)\ldots(x - \xi_n).$$

Každé z čísel $\xi_1, \xi_2, \ldots, \xi_n$ je kořenem polynomu $f$.

**Důsledek.** *Každý nekonstantní polynom stupně $n$ s komplexními koeficienty má nejvýše $n$ navzájem různých kořenů.*

**Tvrzení 4.4.5** (Vlastnosti kořenů (Viètovy vzorce))**.** *Buďte $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ a $\xi_1, \xi_2, \ldots, \xi_n$ jeho kořeny (nemusí být všechny různé). Potom*

$$\begin{aligned}
a_{n-1} &= -(\xi_1 + \xi_2 + \cdots + \xi_n) = -\sum_{i=1}^{n} \xi_i \\
a_{n-2} &= \xi_1\xi_2 + \xi_1\xi_3 + \cdots + \xi_1\xi_n + \xi_2\xi_3 + \cdots + \xi_2\xi_n + \cdots + \xi_{n-1}\xi_n = \\
&= \sum_{\substack{i,j=1 \\ i<j}}^{n} \xi_i\xi_j \\
a_{n-3} &= -(\xi_1\xi_2\xi_3 + \xi_1\xi_2\xi_4 + \cdots + \xi_1\xi_{n-1}\xi_n + \cdots + \xi_{n-2}\xi_{n-1}\xi_n) = \\
&= -\sum_{\substack{i,j,k=1 \\ i<j<k}}^{n} \xi_i\xi_j\xi_k \\
&\vdots \\
a_1 &= (-1)^{n-1}(\xi_1\cdots\xi_{n-2}\xi_{n-1} + \xi_1\cdots\xi_{n-2}\xi_n + \cdots \\
&\qquad \cdots + \xi_1\xi_3\cdots\xi_n + \xi_2\cdots\xi_n) \\
a_0 &= (-1)^n\xi_1\xi_2\cdots\xi_n
\end{aligned}$$

*Důkaz.* Polynom $f$ můžeme rozložit na součin jeho kořenových činitelů

$$x^n + \ldots + a_0 = (x - \xi_1)\ldots(x - \xi_n).$$

Po roznásobení pravé strany porovnáním koeficientů s příslušnými koeficienty na levé straně získáme uvedené vztahy. □

**Příklad.** Kořeny polynomu $x^2 - 5x + 6$ jsou 2 a 3 a

$$\begin{aligned}
a_1 &= -(2 + 3) = -5, \\
a_0 &= (-1)^2 \cdot 2 \cdot 3 = 6.
\end{aligned}$$

□

## 4.5. Polynomy s reálnými koeficienty

### Komplexní čísla

*Komplexní číslo* je číslo $a + bi$, kde $a, b$ jsou reálná čísla a $i$ je *imaginární jednotka*, čili $i^2 = -1$.

Komplexní čísla $z_1 = a + bi$, $z_2 = c + di$ se rovnají právě tehdy, když $a = c$ a $b = d$.

Pro $z_1 = a + bi$, $z_2 = c + di$

$$z_1 + z_2 = (a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$z_1 - z_2 = (a + bi) - (c + di) = (a - c) + (b - d)i,$$
$$z_1 \cdot z_2 = (a + bi) \cdot (c + di) = (ac + bdi^2) + adi + bci = (ac - bd) + (ad + bc)i.$$

*Číslo komplexně sdružené k číslu* $z = a + bi$ je číslo $a - bi$ a označujeme jej $z^*$.

**Cvičení.** Pro komplexní číslo $z = a + bi$ platí

(1) $(z^*)^* = z$,
(2) $z = z^*$ právě tehdy, když $z$ je reálné číslo,
(3) $z + z^* = 2a$, tedy reálné číslo,
(4) $zz^* = a^2 + b^2$, tedy reálné číslo. □

**Cvičení.** Pro komplexní čísla $z_1, z_2$ platí

(1) $(z_1 + z_2)^* = z_1^* + z_2^*$,
(2) $(z_1 z_2)^* = z_1^* z_2^*$. □

**Cvičení.** Pro komplexní číslo $z = a + bi$

$$(x - z)(x - z^*) = x^2 - 2ax + a^2 + b^2$$

je polynom s reálnými koeficienty a pokud $z \notin \mathbb{R}$, čili $b \neq 0$, potom diskriminant tohoto polynomu je záporný. □

### Polynomy s reálnými koeficienty

**Tvrzení 4.5.1.** *Je-li $\xi \in \mathbb{C}$ kořenem polynomu s reálnými koeficienty, potom $\xi^* \in \mathbb{C}$ je také kořenem tohoto polynomu, a to stejné násobnosti.*

*Důkaz.* Nechť $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ je polynom s reálnými koeficienty a $\xi \in \mathbb{C}$ je jeho kořen, čili $f(\xi) = 0$. Potom

$$\begin{aligned}
f(\xi^*) &= a_n(\xi^*)^n + a_{n-1}(\xi^*)^{n-1} + \cdots + a_1\xi^* + a_0 = && (a = a^* \text{ pro } a \in \mathbb{R}) \\
&= a_n^*(\xi^*)^n + a_{n-1}^*(\xi^*)^{n-1} + \cdots + a_1^*\xi^* + a_0^* = && (a^*b^* = (ab)^*) \\
&= (a_n\xi^n)^* + (a_{n-1}\xi^{n-1})^* + \cdots + (a_1\xi)^* + a_0^* = && (a^* + b^* = (a+b)^*) \\
&= (a_n\xi^n + a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0)^* = \\
&= f(\xi)^* = 0^* = 0.
\end{aligned}$$

Na druhou stranu, pokud $\xi^*$ je kořen polynomu $f$, potom z právě dokázaného vyplývá, že $\xi = (\xi^*)^*$ je také kořen.

Takže, je-li $\xi = a + bi$ kořen $f$, potom $\xi^* = a - bi$ je také kořen $f$ a

$$f = (x - \xi)(x - \xi^*)h.$$

Díky tomu, že $\xi + \xi^* = 2a$ a $\xi\xi^* = a^2 + b^2$ jsou reálná čísla,

$$(x - \xi)(x - \xi^*) = x^2 - (\xi + \xi^*)x + \xi\xi^*$$

je polynom s reálnými koeficienty, a proto $h$ je také polynom s reálnými koeficienty. Proto, je-li $\xi$ $k$-násobný kořen $f$,

$$f = (x - \xi)^k(x - \xi^*)^k g,$$

kde $g$ je polynom s reálnými koeficienty, jehož kořenem nejsou ani $\xi$ ani $\xi^*$, takže $\xi^*$ je také $k$-násobný kořen $f$. □

Rozklad normovaného polynomu $f$ s reálnými koeficienty na ireducibilní činitele nad $\mathbb{C}$ tedy obsahuje lineární činitele $x-\alpha_i$ s reálnými kořeny $\alpha_i$ a dvojice lineárních činitelů $x-\xi_j$, $x-\xi_j^*$ s dvojicemi komplexně sdružených kořenů $\xi_j, \xi_j^*$:

$$f = (x-\alpha_1)^{l_1}\cdots(x-\alpha_r)^{l_r}(x-\xi_1)^{k_1}(x-\xi_1^*)^{k_1}\cdots(x-\xi_s)^{k_s}(x-\xi_s^*)^{k_s}.$$

Takže $\deg f = l_1+\cdots+l_r+2(k_1+\cdots+k_s)$.

Pokud roznásobíme všechny dvojice $(x-\xi_j),(x-\xi_j^*)$, dostaneme rozklad polynomu $f$ na ireducibilní činitele nad $\mathbb{R}$, který obsahuje lineární činitele $x-\alpha_i$ a kvadratické činitele $x^2-(\xi_j+\xi_j^*)x+\xi_j\xi_j^*$ se zápornými diskriminanty:

$$f = (x-\alpha_1)^{l_1}\cdots(x-\alpha_r)^{l_r}(x^2-(\xi_1+\xi_1^*)x+\xi_1\xi_1^*)^{k_1}\cdots(x^2-(\xi_s+\xi_s^*)x+\xi_s\xi_s^*)^{k_s}.$$

**Cvičení.** (1) Každý polynom s reálnými koeficienty lichého stupně má aspoň jeden reálný kořen.

(2) Každý polynom s reálnými koeficienty stupně většího než 2 je reducibilní nad $\mathbb{R}$. □

**Cvičení.** Rozložte polynom $x^4+1$ na ireducibilní činitele nad $\mathbb{C}$ a nad $\mathbb{R}$. □

Pro polynomy, jejichž koeficienty jsou celá čísla, navíc platí následující tvrzení.

**Tvrzení 4.5.2.** *Buďte $f = a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ polynom s celočíselnými koeficienty a $p,q$ nesoudělná celá čísla. Jestliže $\frac{p}{q}$ je kořenem polynomu $f$, potom $a_0$ je dělitelné $p$ a $a_n$ je dělitelné $q$.*

*Důkaz.* Položíme $f(\frac{p}{q})$ rovno nule a po vhodných úpravách získáme uvedené vlastnosti. Cvičení. □

**Důsledek.** *Celočíselné kořeny polynomu s celočíselnými koeficienty jsou dělitelé absolutního členu.*

## 4.6. Derivace

**Definice 4.6.1.** Buď $f = a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \in \mathbb{C}[x]$. Polynom $f' = na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1 \in \mathbb{C}[x]$ je *derivace* polynomu $f$.

**Tvrzení 4.6.1.** *(1)* $(f+g)' = f'+g'$,
*(2)* $(fg)' = f'g+fg'$,
*(3)* $(f^k)' = kf^{k-1}f'$.

*Důkaz.* Cvičení. □

**Tvrzení 4.6.2.** *Nechť $k \geq 2$, $f \in \mathbb{C}[x]$ je polynom a $\xi \in \mathbb{C}$ je jeho $k$-násobný kořen. Potom*

*(1) $\xi$ je $(k-1)$-násobný kořen $f'$,*
*(2) $\xi$ je $(k-1)$-násobný kořen největšího společného dělitele $D(f,f')$.*

*Důkaz.* (1) $(x-\xi)^k \mid f$, tedy $f = (x-\xi)^k q$ a $(x-\xi)^{k+1}$ nedělí $f$. Potom

$$f' = k(x-\xi)^{k-1}q + (x-\xi)^k q' = (x-\xi)^{k-1}(kq + (x-\xi)q').$$

Takže, $(x-\xi)^{k-1}$ dělí $f'$. Kdyby $(x-\xi)^k$ dělilo $f'$, pak by $(x-\xi) \mid (kq + (x-\xi)q')$, načež $(x-\xi) \mid kq$, tedy $(x-\xi) \mid q$ a $(x-\xi)^{k+1} \mid f$ ve sporu s předpokladem.

(2) $(x-\xi)^{k-1}$ je dělitel $f$ i $f'$, takže $(x-\xi)^{k-1} \mid D(f,f')$. Kdyby $(x-\xi)^k$ dělilo $D(f,f')$, pak by $(x-\xi)^k \mid f'$ ve sporu s předchozím bodem. □

**Tvrzení 4.6.3.** *Buďte $f \in \mathbb{C}[x]$ a $\xi \in \mathbb{C}$ jeho kořen. Potom $\xi$ je 1-násobný kořen polynomu*

$$\frac{f}{D(f,f')} \in \mathbb{C}[x].$$

*Důkaz.* Nechť $\xi$ je $k$-násobný kořen polynomu $f$, tedy $f = (x-\xi)^k q$, ale $(x-\xi)^{k+1}$ nedělí $f$, čili $x-\xi$ nedělí $q$. Podle předchozího tvrzení $D(f,f') = (x-\xi)^{k-1}r$. Takže

$$\frac{f}{D(f,f')} = (x-\xi)\frac{q}{r} \quad \text{a jelikož } x-\xi \text{ nedělí } q, \text{ nedělí ani } \frac{q}{r}.$$ □

**Důsledek.** *Buď $f \in \mathbb{C}[x]$.*

*(1) Množina všech kořenů polynomu $f/D(f,f')$ je rovna množině všech kořenů polynomu $f$.*

*(2) Všechny kořeny polynomu $f/D(f,f')$ jsou 1-násobné.*

*Důkaz.* Cvičení. □

# 5. Grupy

## 5.1. Binární operace

**Definice 5.1.1.** *Binární operace* na množině $X$ je libovolné zobrazení $X \times X \to X$.

Jedná se tedy o zobrazení, které libovolné dvojici $(x, y)$ prvků z $X$ přiřazuje nějaký jednoznačně určený prvek z $X$. Binární operace se často označují symboly $*, +, \cdot, \circ$ a hodnota takového zobrazení označeného například $*$ v bodě $(x, y)$ se označuje $x * y$ (místo $*(x, y)$).

**Příklad.** (1) Buď $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ množina všech celých nezáporných čísel. Zobrazení $+ \colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, které uspořádané dvojici $(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0$ celých nezáporných čísel přiřadí jejich součet $x + y \in \mathbb{N}_0$, je binární operace na $\mathbb{N}_0$.

(2) Součet a součin na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(3) Na množině $\mathbb{R}^2$ všech uspořádaných dvojic reálných čísel binární operace sčítání:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2).$$

(4) Na konečné množině lze zadat binární operaci tabulkou. Například nechť $X = \{0, 1, 2\}$ a binární operace $+$ na $X$ je zadána takto

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

tedy například $1 + 2 = 0$.

(5) Množina $\mathcal{M}_{m\times n}(P)$ matic stejného typu s operací sčítání matic.

(6) Množina $\mathcal{M}_n(P)$ čtvercových matic stejného typu s operací násobení matic.

(7) Množina $P[x]$ všech polynomů s operací sčítání nebo násobení polynomů.

(8) Množina $X^X$ všech zobrazení $X \to X$ s operací $\circ$ skládání zobrazení.

(9) Buď $X$ množina. Označme $P(X)$ množinu všech podmnožin množiny $X$. Sjednocení, průnik a symetrický rozdíl množin jsou binární operace na množině $P(X)$. □

**Definice 5.1.2.** Binární operace $*$ na množině $X$ je *asociativní*, jestliže pro každé $x, y, z \in X$ platí

$$x * (y * z) = (x * y) * z.$$

Můžeme tedy psát bez závorek $x * y * z$.

**Definice 5.1.3.** Binární operace $*$ na množině $X$ je *komutativní*, jestliže pro každé $x, y \in X$ platí

$$x * y = y * x.$$

**Příklad.** (1) Sčítání i násobení na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ jsou asociativní i komutativní.

(2) Sčítání na množině $\mathbb{R}^2$ je asociativní i komutativní.

(3) Sčítání matic na množině $\mathcal{M}_{m\times n}(P)$ je asociativní i komutativní.

(4) Násobení matic na množině $\mathcal{M}_n(P)$ je asociativní, ale není komutativní.

(5) Sčítání i násobení polynomů na množině $P[x]$ jsou asociativní i komutativní.

(6) Skládání zobrazení na množině $X^X$ je asociativní. Komutativní je právě tehdy, když $X$ je jednoprvková množina (cvičení).

(7) Sjednocení, průnik a symetrický rozdíl množin na množině $P(X)$ jsou asociativní i komutativní. □

**Definice 5.1.4.** Buď $*$ binární operace na množině $X$. Prvek $e \in X$ je *neutrální prvek* operace $*$, jestliže pro každý prvek $x \in X$ platí

$$x * e = x = e * x.$$

**Tvrzení 5.1.1.** *Každá binární operace má nejvýše jeden neutrální prvek.*

*Důkaz.* Jsou-li $e_1, e_2$ neutrální prvky operace $*$, pak $e_2 = e_1 * e_2 = e_1$. □

**Příklad.** (1) Neutrální prvek operace sčítání na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je 0.

(2) Neutrální prvek operace násobení na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je 1.

(3) Neutrální prvek operace sčítání na množině $\mathbb{R}^2$ je $(0, 0)$.

(4) Neutrální prvek operace sčítání matic na množině $\mathcal{M}_{m\times n}(P)$ je nulová matice příslušného typu, tedy $0_{m\times n}$.

(5) Neutrální prvek operace násobení matic na množině $\mathcal{M}_n(P)$ je jednotková matice příslušného typu, tedy $E_n$.

(6) Neutrální prvek operace sčítání polynomů na množině $P[x]$ je polynom 0.

(7) Neutrální prvek operace násobení polynomů na množině $P[x]$ je polynom 1.

(8) Neutrální prvek operace skládání zobrazení na množině $X^X$ je identita $\mathrm{id}_X$.

(9) Neutrální prvek operace sjednocení množin na množině $P(X)$ je $\emptyset$.

(10) Neutrální prvek operace průnik množin na množině $P(X)$ je $X$.

(11) Neutrální prvek operace symetrický rozdíl množin na množině $P(X)$ je $\emptyset$. □

**Definice 5.1.5.** Buď $*$ binární operace na množině $X$, $e \in X$ její neutrální prvek. Prvek $x \in X$ je *invertibilní*, jestliže existuje prvek $y \in X$ takový, že

$$x * y = y * x = e.$$

Potom $y$ je *inverzní prvek* nebo *inverze* k prvku $x$ vzhledem k operaci $*$.

**Tvrzení 5.1.2.** *Každý prvek množiny s asociativní binární operací má vzhledem k této operaci nejvýše jeden inverzní prvek.*

*Důkaz.* Je-li $e$ neutrální prvek operace $*$ a jsou-li $y_1, y_2$ inverzní prvky k prvku $x$, pak

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2.$$ □

Inverzní prvek k prvku $x$ se obvykle značí $x^{-1}$. Pouze u operace $+$ se značí $-x$ a říká se mu *opačný*.

Přímo z definice inverzního prvku vyplývá, že

$$e^{-1} = e \quad \text{a} \quad (x^{-1})^{-1} = x.$$

**Příklad.** (1) Inverzní prvek k číslu $x$ vzhledem k operaci sčítání na množinách $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ je číslo opačné $-x$ (pokud v příslušné množině existuje).

(2) Inverzní prvek k číslu $x$ vzhledem k operaci násobení na množinách $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ je převrácená hodnota $x^{-1}$ (pokud v příslušné množině existuje).

(3) Inverzní prvek k dvojici $(x, y) \in \mathbb{R}^2$ vzhledem k operaci sčítání je $(-x, -y)$.

(4) Inverzní prvek k matici $A$ vzhledem k operaci sčítání matic na množině $\mathcal{M}_{m\times n}(P)$ je opačná matice $-A$.

(5) Inverzní prvek k matici $A$ vzhledem k operaci násobení matic na množině $\mathcal{M}_n(P)$ je inverzní matice $A^{-1}$ (je-li $A$ invertibilní).

(6) Inverzní prvek k zobrazení $f\colon X \to X$ vzhledem k operaci skládání zobrazení na množině $X^X$ je inverzní zobrazení $f^{-1}$, pokud toto inverzní zobrazení existuje.

(7) Inverzní prvek k množině $Y \in P(X)$ vzhledem k operaci symetrický rozdíl množin na množině $P(X)$ je $Y$. □

**Příklad.** Na množině $\{0, 1, 2\}$ mějme binární operaci $*$ zadanou tabulkou

| $*$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 0 |

Neutrální prvek operace $*$ je 0 a

$$1 * 2 = 2 * 1 = 0 \quad \text{a} \quad 2 * 2 = 0.$$

Čili 1 a 2 jsou inverzní prvky k 2. Podle Tvrzení 5.1.2 to znamená, že operace $*$ není asociativní. A skutečně, například,

$$(1 * 1) * 2 = 2 * 2 = 0 \quad \text{zatímco} \quad 1 * (1 * 2) = 1 * 0 = 1.$$ □

## 5.2. Grupy

**Definice 5.2.1.** Množina $G$ s binární operací $*\colon G \times G \to G$ je *grupa*, jestliže

(1) operace $*$ je asociativní,
(2) v množině $G$ je neutrální prvek operace $*$,
(3) množina $G$ s každým prvkem obsahuje také prvek k němu inverzní vzhledem k operaci $*$.

Je-li navíc operace $*$ komutativní, grupa $G$ je také *komutativní*.

Grupa $G$ s binární operací $*$, neutrálním prvkem $e$ a označením inverzního prvku $^{-1}$ se někdy zapisuje $(G, *, e, ^{-1})$, někdy jen $(G, *)$ a je-li z kontextu zřejmé, o jakou operaci se jedná, někdy se hovoří jen o grupě $G$.

Grupa s binární operací označenou $+$ se nazývá *aditivní* (používá se pouze u komutativních grup). Grupa s binární operací označenou $\cdot$ se nazývá *multiplikativní*.

Označme $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ a obdobně v případech $\mathbb{R}^*, \mathbb{C}^*$.

**Příklad.** (1) Množina $\mathbb{Z}$ s operací sčítání je grupa. Stejně tak $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(2) Množina $\mathbb{N}_0$ s operací sčítání není grupa.

(3) Množina $\mathbb{Q}^*$ s násobením je grupa. Stejně tak $\mathbb{R}^*, \mathbb{C}^*$, $\mathbb{R}_+$ (kladná reálná čísla).

(4) Množina $\mathbb{Z} \setminus \{0\}$ s operací násobení není grupa. Stejně tak $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(5) Množina $\mathbb{R}^2$ s operací sčítání je grupa.

(6) Množina $\mathcal{M}_{m\times n}(P)$ s operací sčítání matic je grupa.

(7) Množina $\mathcal{M}_n(P)$ s operací násobení matic není grupa.

(8) Množina $\mathrm{GL}_n(P)$ invertibilních matic typu $n \times n$ s operací násobení matic je grupa (nazývá se *obecná lineární grupa*). □

**Tvrzení 5.2.1.** *Buď $(G, *, e, ^{-1})$ grupa. Pak pro libovolná $x, y \in G$ platí:*

*(1) Jestliže $x * y = e$, pak $y = x^{-1}$, $x = y^{-1}$.*

*(2) $(x * y)^{-1} = y^{-1} * x^{-1}$.*

*Důkaz.* (1) Jestliže $x * y = e$, pak $y = e * y = x^{-1} * x * y = x^{-1} * e = x^{-1}$. Podobně druhá rovnost (cvičení).

(2) Plyne z (1) a rovnosti $x * y * y^{-1} * x^{-1} = e$. □

## 5.3. Podgrupy

**Definice 5.3.1.** Buď $(X, *, e, ^{-1})$ grupa, buď $Y \subseteq X$ podmnožina taková, že

(1) jestliže $y_1, y_2 \in Y$, pak $y_1 * y_2 \in Y$;

(2) $e \in Y$;

(3) jestliže $y \in Y$, pak $y^{-1} \in Y$.

Potom $Y$ je *podgrupa* grupy $X$.

Vlastnosti (1) se někdy říká *uzavřenost množiny vzhledem k operaci*, vlastnosti (3) *uzavřenost množiny vzhledem k inverzi.*

Je-li $Y$ podgrupa grupy $(X, *, e, ^{-1})$ a je-li $*_Y$ zúžení operace $*$ na podmnožinu $Y \times Y$, pak $(Y, *_Y, e, ^{-1})$ je grupa. Zúžení operace na podmnožinu se obvykle značí stejně jako původní operace.

**Příklad.** (1) Každá grupa $(X, *, e, ^{-1})$ má podgrupy $X$ a $\{e\}$. Tyto podgrupy se nazývají *triviální* podgrupy.

(2) Aditivní podgrupy $(\mathbb{Z}, +, 0, -) \subset (\mathbb{Q}, +, 0, -) \subset (\mathbb{R}, +, 0, -) \subset (\mathbb{C}, +, 0, -)$.

(3) Multiplikativní podgrupy $(\mathbb{Q}^*, \cdot, 1, ^{-1}) \subset (\mathbb{R}^*, \cdot, 1, ^{-1}) \subset (\mathbb{C}^*, \cdot, 1, ^{-1})$.

(4) Množina $\{-1, 1\}$ je podgrupa multiplikativní grupy $\mathbb{R}^*$.

(5) Množina $\{z \in \mathbb{C} \,|\, |z| = 1\}$ je podgrupa multiplikativní grupy $\mathbb{C}^*$.

(6) Množina $\{(x, 2x) \in \mathbb{R}^2 \,|\, x \in \mathbb{R}\}$ je podgrupa grupy $\mathbb{R}^2$ s operací sčítání.

(7) Množiny $\{(x, 1) \in \mathbb{R}^2 \,|\, x \in \mathbb{R}\}$ a $\{(x, y) \in \mathbb{R}^2 \,|\, x, y \in \mathbb{R}, x^2 + y^2 \leq 1\}$ nejsou podgrupy grupy $\mathbb{R}^2$ s operací sčítání. □

**Tvrzení 5.3.1.** *(1) Buďte $X$ grupa, $Y$ podgrupa $X$ a $Z$ podgrupa $Y$. Pak $Z$ je podgrupa $X$.*

*(2) Buďte $X$ grupa a $Y, Z$ její podgrupy. Pak $Y \cap Z$ je podgrupa $X$.*

*Důkaz.* Cvičení. □

**Cvičení.** Pokud průnik prázdného systému podmnožin množiny $X$ je množina $X$, potom průnik libovolného systému podgrup grupy $X$ je podgrupa grupy $X$. □

## 5.4. Podgrupy aditivní grupy $\mathbb{Z}$

Najdeme všechny podgrupy aditivní grupy $\mathbb{Z} = (\mathbb{Z}, +, 0, -)$. Pro celé nezáporné číslo $m \in \mathbb{N}_0$ označme

$$m\mathbb{Z} = \{mk \,|\, k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}.$$

**Tvrzení 5.4.1.** *Množiny $m\mathbb{Z}$, $m \in \mathbb{N}_0$, jsou podgrupy aditivní grupy $\mathbb{Z}$ a jiné podgrupy v $\mathbb{Z}$ nejsou.*

*Důkaz.* Buď $m \in \mathbb{N}_0$ libovolné. Ukážeme, že $m\mathbb{Z}$ je podgrupa. Pro libovolné $mk, ml \in m\mathbb{Z}$ platí $mk+ml = m(k+l) \in m\mathbb{Z}$, čímž je dokázána uzavřenost množiny $m\mathbb{Z}$ vzhledem ke sčítání. Množina $m\mathbb{Z}$ obsahuje neutrální prvek 0 grupy $\mathbb{Z}$. Nakonec, pro libovolné $mk \in m\mathbb{Z}$ platí $-(mk) = m(-k) \in m\mathbb{Z}$, čímž je dokázána uzavřenost množiny $m\mathbb{Z}$ vzhledem k inverzi (opačným prvkům).

Buď $B \subseteq \mathbb{Z}$ libovolná podgrupa grupy $\mathbb{Z}$. Ukážeme, že $B$ je rovna některé podgrupě $m\mathbb{Z}$. Jelikož $B$ je podgrupa, obsahuje neutrální prvek 0. Pokud $B = \{0\}$, pak $B = 0\mathbb{Z}$ ($m = 0$). Předpokládejme, že $B \neq \{0\}$, tedy existuje nenulové číslo $b \in B$. Navíc existuje *kladné* číslo $b_+ \in B$, buď $b_+ = b$, nebo $b_+ = -b$ ($-b \in B$, protože $B$ je podgrupa). Označme $m$ *nejmenší kladné číslo* v $B$ (v každé neprázdné množině kladných celých čísel existuje nejmenší číslo).

Dokážeme, že toto číslo $m$ je hledané číslo, pro něž $B = m\mathbb{Z}$. Nejdříve ukážeme, že $m\mathbb{Z} \subseteq B$. Již víme, že $0 \in B$ a $m \in B$. Předpokládejme, že $mk \in B$. Potom i $m(k+1) = mk+m \in B$ a díky matematické indukci dostáváme, že $mk \in B$ pro každé $k \in \mathbb{N}$. A potom i inverzní prvky $-mk$ leží v $B$, a tím je ukázáno, že všechny prvky množiny $m\mathbb{Z}$ leží v $B$.

Zbývá dokázat, že $B \subseteq m\mathbb{Z}$. Buď $b \in B$ libovolné a předpokládejme, že $b \notin m\mathbb{Z}$. Pak existují $q, r \in \mathbb{Z}$ taková, že

$$b = mq + r \quad \text{a} \quad 0 < r < m.$$

Potom $r = b - mq = b + m(-q)$ je kladný prvek $B$, menší než $m$, což je v rozporu s definicí prvku $m$. Proto $b \in m\mathbb{Z}$. □

## 5.5. Faktorové grupy

**Definice 5.5.1.** *Relace* na množině $X$ je podmnožina kartézského součinu $X \times X$.

Je-li $\rho$ relace, místo „$(x, y)$ je v relaci $\rho$“ se obvykle říká „$x$ je v relaci $\rho$ s $y$“ a místo $(x, y) \in \rho$ se obvykle píše $x \,\rho\, y$.

**Definice 5.5.2.** Relace $\rho$ na množině $X$ je *relace ekvivalence*, jestliže je
(1) reflexivní, tj. $x \,\rho\, x$ pro každé $x \in X$,
(2) symetrická, tj. $x \,\rho\, y$ implikuje $y \,\rho\, x$,
(3) tranzitivní, tj. $x \,\rho\, y$, $y \,\rho\, z$ implikuje $x \,\rho\, z$.

**Definice 5.5.3.** Buďte $\equiv$ relace ekvivalence na množině $X$ a $x, y \in X$. Jestliže $x \equiv y$, potom $x$ je *ekvivalentní* $y$ vzhledem k $\equiv$. Množina

$$\{y \in X \mid x \equiv y\}$$

všech prvků ekvivalentních prvku $x$ je *třída ekvivalence* příslušná $x$ vzhledem k $\equiv$, označujeme ji $[x]_\equiv$ nebo jen $[x]$, je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

$$[x]_\equiv = \{y \in X \mid x \equiv y\}.$$

**Definice 5.5.4.** Buď $\equiv$ relace ekvivalence na množině $X$. Množina

$$\{[x]_{\equiv} \mid x \in X\}$$

všech příslušných tříd ekvivalence je *faktorová množina* vzhledem k $\equiv$, označujeme ji $\tilde{X}_{\equiv}$ nebo jen $\tilde{X}$, je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

$$\tilde{X}_{\equiv} = \{[x]_{\equiv} \mid x \in X\}.$$

Poznamenejme, že $\tilde{X}$ je *rozklad množiny* $X$, to znamená, že množiny $[x]$ jsou neprázdné, po dvou disjunktní a jejich sjednocení je $X$.

**Definice 5.5.5.** Buďte $X$ množina s binární operací $*$ a $\equiv$ relace ekvivalence na množině $X$. Relace $\equiv$ je *kongruence* na $X$ s $*$, jestliže platí *podmínka kompatibility*, čili implikace

$$\text{jestliže } x_1 \equiv x_2 \text{ a } y_1 \equiv y_2, \text{ pak } x_1 * y_1 \equiv x_2 * y_2,$$

nebo ekvivalentně

$$\text{jestliže } [x_1] = [x_2] \text{ a } [y_1] = [y_2], \text{ pak } [x_1 * y_1] = [x_2 * y_2].$$

**Tvrzení 5.5.1.** *Buďte $\equiv$ kongruence na množině s asociativní binární operací a $x, y$ invertibilní prvky. Pak platí implikace*

$$\textit{jestliže } x \equiv y, \textit{ pak } x^{-1} \equiv y^{-1}$$

*nebo ekvivalentně zapsáno*

$$\textit{jestliže } [x] = [y], \textit{ pak } [x^{-1}] = [y^{-1}].$$

*Důkaz.* Nechť $x \equiv y$. Jelikož $x^{-1} \equiv x^{-1}$ a $y^{-1} \equiv y^{-1}$, z podmínky kompatibility dostaneme $x * x^{-1} \equiv y * x^{-1}$, tedy $e \equiv y * x^{-1}$, a $y^{-1} * e \equiv y^{-1} * y * x^{-1}$, tedy $y^{-1} \equiv x^{-1}$. □

**Příklad.** (1) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když $x, y$ jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$. Potom $\equiv$ je kongruence, protože součet jakýchkoliv sudých čísel je sudé číslo, součet jakýchkoliv dvou lichých čísel je sudé číslo a součet jakéhokoliv sudého čísla a jakéhokoliv lichého čísla je liché číslo.

(2) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když $x, y$ jsou obě záporná nebo obě kladná nebo obě nulová, tedy $\tilde{\mathbb{Z}} = \{[-1], [0], [1]\}$. Potom $\equiv$ je relace ekvivalence, platí implikace

$$\text{jestliže } x \equiv y, \text{ pak } -x \equiv -y,$$

ale existují $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ taková, že $x_1 \equiv x_2$ a $y_1 \equiv y_2$, ale $x_1 + y_1 \not\equiv x_2 + y_2$. Čili $\equiv$ nesplňuje podmínku kompatibility a není to tedy kongruence na $\mathbb{Z}$.

(3) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když $x, y$ jsou obě záporná nebo obě nezáporná, tedy $\tilde{\mathbb{Z}} = \{[-1], [0]\}$. Potom $\equiv$ je relace ekvivalence, ale existují $x, y \in \mathbb{Z}$ taková, že $x \equiv y$, ale $-x \not\equiv -y$. Podle Tvrzení 5.5.1 $\equiv$ není kongruence na $\mathbb{Z}$, a nesplňuje tedy podmínku kompatibility. □

Máme-li kongruenci a třídy $[x], [y]$, pak díky podmínce kompatibility třída $[x * y]$ je jednoznačně určena třídami $[x], [y]$, čili nezávisí na konkrétním výběru jejich prvků $x, y$ (*reprezentantů*). Na množině $\tilde{X}$ tedy můžeme zavést binární operaci $\tilde{*}$ předpisem

$$[x]\tilde{*}[y] = [x * y]. \tag{9}$$

**Příklad.** Mějme grupu $(\mathbb{Z}, +, 0, -)$ a kongruenci $\equiv$ danou předpisem: $x \equiv y$ právě tehdy, když $x, y$ jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$.

Na $\tilde{\mathbb{Z}}$ máme binární operaci $\tilde{+}$ definovanou předpisem (9), tedy $[x]\tilde{+}[y] = [x + y]$. Takže

$$\begin{aligned}
&[0]\tilde{+}[0] = [0 + 0] = [2 + 6] = [8 + (-14)] = [0],\\
&[0]\tilde{+}[1] = [0 + 1] = [2 + 7] = [(-6) + 11] = [1],\\
&[1]\tilde{+}[0] = [1 + 0] = [7 + 6] = [17 + (-2)] = [1],\\
&[1]\tilde{+}[1] = [1 + 1] = [3 + 13] = [(-7) + 5] = [0].
\end{aligned}$$

□

**Tvrzení 5.5.2.** *Mějme kongruenci na množině $X$ s binární operací $*$. Buď $\tilde{*}$ binární operace na $\tilde{X}$ definovaná předpisem (9). Potom*

*(i) je-li $*$ asociativní, pak $\tilde{*}$ je asociativní;*
*(ii) je-li $e$ neutrální prvek $*$, pak $[e]$ je neutrální prvek $\tilde{*}$;*
*(iii) je-li $x^{-1}$ inverze k $x$ vzhledem k $*$, pak $[x^{-1}]$ je inverze k $[x]$ vzhledem k $\tilde{*}$;*
*(iv) je-li $*$ komutativní, pak $\tilde{*}$ je komutativní.*

*Důkaz.* (i) Jestliže $*$ je asociativní, potom pro libovolné třídy $[x], [y], [z] \in \tilde{X}$ platí

$$\begin{aligned}
[x]\tilde{*}([y]\tilde{*}[z]) &= [x]\tilde{*}[y * z] =\\
&= [x * (y * z)] =\\
&= [(x * y) * z] =\\
&= [x * y]\tilde{*}[z] =\\
&= ([x]\tilde{*}[y])\tilde{*}[z],
\end{aligned}$$

takže $\tilde{*}$ je asociativní.

(ii) Jestliže $e$ je neutrální prvek oparace $*$, potom pro libovolnou třídu $[x] \in \tilde{X}$ platí

$$\begin{aligned}
&[x]\tilde{*}[e] = [x * e] = [x],\\
&[e]\tilde{*}[x] = [e * x] = [x],
\end{aligned}$$

takže $[e]$ je neutrální prvek operace $\tilde{*}$.

(iii) Jestliže $x^{-1}$ je inverzní prvek k $x$ vzhledem k $*$, pak

$$\begin{aligned}
&[x]\tilde{*}[x^{-1}] = [x * x^{-1}] = [e],\\
&[x^{-1}]\tilde{*}[x] = [x^{-1} * x] = [e],
\end{aligned}$$

takže $[x^{-1}]$ je inverzní prvek k $[x]$ vzhledem k operaci $\tilde{*}$.

(iv) Z (9) je zřejmé, že je-li $*$ komutativní, pak i $\tilde{*}$ je komutativní. □

**Důsledek.** *Pro každou (komutativní) grupu a každou kongruenci na této grupě příslušná faktorová množina s operací definovanou předpisem (9) je (komutativní) grupa.*

*Důkaz.* Tvrzení je jednoduchým důsledkem předchozího tvrzení. □

Jelikož každý prvek množiny s asociativní operací má nejvýše jeden inverzní prvek, viz Tvrzení 5.1.2 nebo Tvrzení 5.5.1, třída $[x^{-1}]$ je v takovém případě jednoznačně určena třídou $[x]$, čili nezávisí na konkrétním výběru jejího prvku $x$, a proto je korektní ji označovat $[x]^{-1}$.

**Definice 5.5.6.** Faktorová množina s operací definovanou předpisem (9) z předchozího Důsledku je *faktorová grupa*.

**Příklad.** Mějme grupu $(\mathbb{Z}, +, 0, -)$ a kongruenci danou předpisem: $x \equiv y$ právě tehdy, když $x, y$ jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$.

Na $\tilde{\mathbb{Z}}$ máme asociativní binární operaci $\tilde{+}$: $[x]\tilde{+}[y] = [x + y]$, neutrální prvek operace $\tilde{+}$ je $[0]$ a opačný prvek $-[x]$ k prvku $[x]$ je $[-x]$, čili $-[0] = [0]$, $-[1] = [-1] = [1]$. □

## 5.6. Zbytkové třídy

Mějme aditivní grupu $(\mathbb{Z}, +, 0, -)$ a buď $m$ libovolné přirozené (kladné celé) číslo. Definujme relaci $\equiv_m$ na $\mathbb{Z}$ předpisem:

$$x \equiv_m y \text{ právě tehdy, když } x - y \text{ je celočíselný násobek čísla } m$$

(čili $m \mid (x - y)$ a existuje tedy $k \in \mathbb{Z}$ takové, že $x - y = km$ a $x = y + km$).

Potom $\equiv_m$ je relace ekvivalence (cvičení), příslušné třídy ekvivalence $[i]_{\equiv_m}$ se značí $[i]_m$ a

$$\begin{aligned}
&\vdots\\
[-2]_m &= \{-2 + km \mid k \in \mathbb{Z}\} = \{\ldots, -2 - 2m, -2 - m, -2, -2 + m, -2 + 2m, \ldots\},\\
[-1]_m &= \{-1 + km \mid k \in \mathbb{Z}\} = \{\ldots, -1 - 2m, -1 - m, -1, -1 + m, -1 + 2m, \ldots\},\\
[0]_m &= \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\},\\
[1]_m &= \{1 + km \mid k \in \mathbb{Z}\} = \{\ldots, 1 - 2m, 1 - m, 1, 1 + m, 1 + 2m, \ldots\},\\
[2]_m &= \{2 + km \mid k \in \mathbb{Z}\} = \{\ldots, 2 - 2m, 2 - m, 2, 2 + m, 2 + 2m, \ldots\},\\
&\vdots\\
[i]_m &= \{i + km \mid k \in \mathbb{Z}\} = \{\ldots, i - 2m, i - m, i, i + m, i + 2m, \ldots\},\\
&\vdots
\end{aligned}$$

Pro $i \in \{0, \ldots, m-1\}$ třída ekvivalence $[i]_m$ obsahuje právě ta celá čísla $z$, po jejichž celočíselném dělení číslem $m$ číslo $i$ je zbytek. Třídám $[i]_m$, kde $i \in \{0, \ldots, m-1\}$, se proto říká *zbytkové třídy*. Při dělení číslem $m$ všechny možné zbytky jsou právě $0, 1, \ldots, m-1$, takže každé celé číslo leží v právě jedné ze zbytkových tříd $[0]_m, [1]_m, \ldots, [m-1]_m$. Příslušná faktorová množina $\tilde{\mathbb{Z}}_{\equiv_m}$ se značí $\mathbb{Z}_m$, tedy

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Ověříme, zda $\equiv_m$ je kongruence na $\mathbb{Z}$, čili podmínku kompatibility. Předpokládejme, že $[x_1]_m = [x_2]_m$ a $[y_1]_m = [y_2]_m$. To znamená, že $x_2 \in [x_1]_m$ a $y_2 \in [y_1]_m$, čili $x_2 = x_1 + km$, $y_2 = y_1 + lm$ pro vhodná $k, l \in \mathbb{Z}$. Potom $x_2 + y_2 = x_1 + km + y_1 + lm = x_1 + y_1 + (k + l)m \in [x_1 + y_1]_m$, a tedy $[x_1 + y_1]_m = [x_2 + y_2]_m$.

Na množině $\mathbb{Z}_m$ tedy máme binární operaci $+$ (značí se obvykle stejně jako původní operace) podle (9)

$$[x]_m + [y]_m = [x + y]_m$$

a příslušná faktorová grupa $(\mathbb{Z}_m, +, [0]_m, -)$ je komutativní *aditivní grupa zbytkových tříd modulo m*.

Na množině $\mathbb{Z}$ uvažujme operaci $\cdot$, která je asociativní a má neutrální prvek 1. Ověříme podmínku kompatibility pro operaci $\cdot$.

Předpokládejme, že $[x_1]_m = [x_2]_m$ a $[y_1]_m = [y_2]_m$. To znamená, že $x_2 = x_1 + km$, $y_2 = y_1 + lm$ pro vhodná $k, l \in \mathbb{Z}$. Potom $x_2 \cdot y_2 = (x_1 + km) \cdot (y_1 + lm) = x_1 y_1 + (ky_1 + lx_1 + klm)m \in [x_1 y_1]_m$, a tedy $[x_1 y_1]_m = [x_2 y_2]_m$.

Na $\mathbb{Z}_m$ tedy máme i binární operaci $\cdot$ podle (9)

$$[x]_m \cdot [y]_m = [x \cdot y]_m.$$

Podle Tvrzení 5.5.2 operace $\cdot$ na množině $\mathbb{Z}_m$ je komutativní, asociativní a má neutrální prvek $[1]_m$. Faktorová množina $\mathbb{Z}_m$ s operací $\cdot$ a neutrálním prvkem $[1]_m$ je komutativní *multiplikativní monoid zbytkových tříd modulo* $m$ (*monoid* je množina s asociativní binární operací a neutrálním prvkem). Otázka existence inverzí vzhledem k operaci $\cdot$ není tak jednoduchá jako v případě operace $+$.

**Tvrzení 5.6.1.** *Prvek $[x]_m \in \mathbb{Z}_m$ má inverzi vzhledem k operaci $\cdot$ právě tehdy, když $x$ a $m$ jsou nesoudělná, tedy jejich největší společný dělitel $D(x, m)$ je 1.*

*Důkaz.* Předpokládejme, že $[y]_m$ je inverze k $[x]_m$, tedy $[x]_m \cdot [y]_m = [xy]_m = [1]_m$. Takže $xy + km = 1$ pro vhodné $k \in \mathbb{Z}$ a každý společný dělitel čísel $x$ a $m$ je dělitel i čísla 1. Proto $D(x, m) = 1$.

Předpokládejme, že $D(x, m) = 1$. Podle Bézoutovy věty existují čísla $y, k \in \mathbb{Z}$ taková, že $D(x, m) = xy + km$, tedy $1 = xy + km$, takže $[1]_m = [xy]_m = [x]_m \cdot [y]_m$ a $[y]_m$ je inverze k $[x]_m$. □

**Příklad.** Nechť $m = 5$. Následující tabulka naznačuje rozložení množiny všech celých čísel do pěti tříd:

| | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $[0]_5$ | | | -5 | | | | | 0 | | | | | 5 | | | | | | | | | |
| $[1]_5$ | | | | | -4 | | | | | 1 | | | | | 6 | | | | | | | |
| $[2]_5$ | $\cdots$ | | | | | -3 | | | | | 2 | | | | | 7 | | | | | | $\cdots$ |
| $[3]_5$ | | | | | | | -2 | | | | | 3 | | | | | 8 | | | | | |
| $[4]_5$ | | | | | | | | -1 | | | | | 4 | | | | | 9 | | | | |

Aditivní grupa $\mathbb{Z}_5$ resp. multiplikativní monoid $\mathbb{Z}_5$ mají tabulky

| $+$ | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ |
|---|---|---|---|---|---|
| $[0]_5$ | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ |
| $[1]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ | $[0]_5$ |
| $[2]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ | $[0]_5$ | $[1]_5$ |
| $[3]_5$ | $[3]_5$ | $[4]_5$ | $[0]_5$ | $[1]_5$ | $[2]_5$ |
| $[4]_5$ | $[4]_5$ | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ |

resp.

| $\cdot$ | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ |
|---|---|---|---|---|---|
| $[0]_5$ | $[0]_5$ | $[0]_5$ | $[0]_5$ | $[0]_5$ | $[0]_5$ |
| $[1]_5$ | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ |
| $[2]_5$ | $[0]_5$ | $[2]_5$ | $[4]_5$ | $[1]_5$ | $[3]_5$ |
| $[3]_5$ | $[0]_5$ | $[3]_5$ | $[1]_5$ | $[4]_5$ | $[2]_5$ |
| $[4]_5$ | $[0]_5$ | $[4]_5$ | $[3]_5$ | $[2]_5$ | $[1]_5$ |

□

# 6. Okruhy a pole

**Definice 6.0.1.** Množina $P$ se dvěmi binárními operacemi + a $\cdot$ je *okruh*, jestliže

(1) + a $\cdot$ jsou asociativní a komutativní operace,
(2) + má neutrální prvek, značíme ho 0,
(3) $\cdot$ má neutrální prvek různý od 0, značíme ho 1,
(4) ke každému prvku $x$ existuje inverzní prvek vzhledem k operaci +,
(5) pro libovolné $x, y, z \in P$ platí $x \cdot (y + z) = x \cdot y + x \cdot z$.

Pokud navíc

(6) ke každému prvku $x \neq 0$ existuje inverzní prvek vzhledem k operaci $\cdot$,

množina $P$ s operacemi + a $\cdot$ je *pole*.

Inverzní prvek k $x$ vzhledem k operaci + se nazývá *opačný* k $x$ a značí se $-x$. Inverzní prvek k $x$ vzhledem k operaci $\cdot$ se značí $x^{-1}$.

Podmínka (5) v předchozí definici je *distributivní zákon*.

**Příklad.** (1) Množiny $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ s operacemi sčítání a násobení jsou pole.

(2) Množina $\mathbb{Z}$ s operacemi sčítání a násobení je okruh, ale není pole.

(3) Množina $\mathbb{N}_0$ s operacemi sčítání a násobení není okruh.

(4) Množina $P[x]$ s operacemi sčítání a násobení polynomů je okruh, ale není pole.

(5) Množina $\mathcal{M}_n(P)$ s operacemi sčítání a násobení matic není okruh.

(6) Nechť $P = \{0, 1\}$ a binární operace + a $\cdot$ na $P$ jsou takové, že

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

a

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Pro operaci + neutrální prvek je 0 a inverzní (opačné) prvky jsou $-0 = 0$ a $-1 = 1$. Pro operaci $\cdot$ neutrální prvek je 1 a inverzní prvek k 1 je 1 ($1^{-1} = 1$), inverzní prvek k 0 neexistuje. Množina $\{0, 1\}$ s těmito operacemi je pole.

(7) Nechť $P = \{0, 1, 2, 3\}$ a binární operace + a $\cdot$ na $P$ jsou takové, že

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

a

| $\cdot$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

Potom neutrální prvek operace + je 0, neutrální prvek operace $\cdot$ je 1 a

| | | |
|---|---|---|
| $-0 = 0$ | a | $0^{-1}$ neexistuje |
| $-1 = 3$ | | $1^{-1} = 1$ |
| $-2 = 2$ | | $2^{-1}$ neexistuje |
| $-3 = 1$ | | $3^{-1} = 3$ |

Množina $\{0, 1, 2, 3\}$ s těmito operacemi je okruh, ale není pole. □

**Tvrzení 6.0.1.** *Buď $P$ okruh. Pak pro libovolné prvky $x, y, z \in P$ platí*

*(i)* $x \cdot 0 = 0$;
*(ii)* $x \cdot (-1) = -x$;
*(iii)* $x \cdot (y - z) = x \cdot y - x \cdot z$.

*Důkaz.* (i) Platí

$$\begin{aligned} x \cdot 0 &= x \cdot (0+0) = \\ &= x \cdot 0 + x \cdot 0 \end{aligned}$$

a po přičtení $-(x \cdot 0)$ k oběma stranám rovnosti dostaneme $0 = x \cdot 0$.

(ii) Platí

$$\begin{aligned} 0 = x \cdot 0 = x \cdot (1 + (-1)) = x \cdot 1 + x \cdot (-1) = \\ = x + x \cdot (-1) \end{aligned}$$

a po přičtení $-x$ k oběma stranám rovnosti dostaneme $-x = x \cdot (-1)$.

(iii) Cvičení. □

**Cvičení.** Dokažte, že v každém okruhu platí:

(1) $(-1) \cdot (-1) = 1$,

(2) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$. □

**Tvrzení 6.0.2.** *Buď $P$ pole a buďte $x, y, z \in P$.*

*(1) $x \cdot y = 0$ právě tehdy, když $x = 0$ nebo $y = 0$.*

*(2) Jestliže $x \cdot y = x \cdot z$ a $x \neq 0$, pak $y = z$.*

*Důkaz.* (1) Jestliže $x = 0$ nebo $y = 0$, pak podle Tvrzení 6.0.1(i) také $x \cdot y = 0$.

Nechť $x \cdot y = 0$. Předpokládejme, že jeden z prvků $x, y$ je nenulový, například $x \neq 0$. Potom s využitím Tvrzení 6.0.1(i) dostaneme

$$y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0.$$

(2)

| | |
|---|---|
| $xy = xz$ | k oběma stranám přičteme $-xz$ |
| $xy - xz = 0$ | použijeme (iii) z předchozího tvrzení |
| $x(y-z) = 0$ | použijeme první část tvrzení a $x \neq 0$ |
| $y - z = 0$ | k oběma stranám přičteme $z$ |
| $y = z$ | |

□

**Příklad.** (1) V příkladu (7) máme okruh, v němž $2 \cdot 2 = 0$ a $2 \cdot 1 = 2 \cdot 3$. To ukazuje, že předchozí tvrzení neplatí pro okruhy.

(2) Pro okruh $P[x]$ ale předchozí tvrzení platí, viz kapitolu o polynomech. □

Obdobně jako v kapitole 5 $P^*$ označuje množinu $P \setminus \{0\}$.

Je-li $P$ okruh, pak $P$ s operací $+$ je komutativní grupa. Pro pole máme navíc následující tvrzení.

**Tvrzení 6.0.3.** *Je-li $P$ pole, pak $P^*$ s operací $\cdot$ je komutativní grupa.*

*Důkaz.* Buďte $x, y \in P^*$, tedy $x \neq 0$ a $y \neq 0$. Podle Tvrzení 6.0.2(i) $x \cdot y \neq 0$, tedy $x \cdot y \in P^*$, a množina $P^*$ je uzavřená vzhledem k operaci $\cdot$. Zbytek tvrzení plyne z toho, že operace $\cdot$ je asociativní a komutativní, $1 \in P^*$ je neutrální prvek, každý nenulový prvek je invertibilní a příslušné inverze jsou nenulové. □

**Tvrzení 6.0.4.** *Množina $\mathbb{Z}_m$ zbytkových tříd je pole právě tehdy, když $m$ je prvočíslo.*

*Důkaz.* Číslo 1 není prvočíslo a $\mathbb{Z}_1$ není pole (cvičení). Buď $m > 1$. Podle kapitol 5.5 a 5.6 $\mathbb{Z}_m$ splňuje podmínky (1)–(4) z definice okruhu a pole. Ověření, že platí distributivní zákon (5), ponecháme jako cvičení. Zbývá ukázat, že ke každému prvku $[x]_m \neq [0]_m$ existuje inverzní prvek vzhledem k operaci $\cdot$ právě tehdy, když $m$ je prvočíslo.

Předpokládejme, že ke každému prvku $[x]_m \neq [0]_m$ existuje inverze. Podle Tvrzení 5.6.1 každé takové $x$ je nesoudělné s $m$, tedy $m$ je prvočíslo.

Na druhou stranu, je-li $m$ prvočíslo, pak každé $x \in \mathbb{Z}$ takové, že $[x]_m \neq [0]_m$, je nesoudělné s $m$. Opět podle Tvrzení 5.6.1 $[x]_m$ má inverzi.

Jiný důkaz tohoto tvrzení lze nalézt v [Marvan, 3. Pole]. □

Takže, například, $\mathbb{Z}_4$ není pole. Čtyřprvkové pole ale existuje.

**Příklad.** Nechť $X = \{0, 1, a, b\}$ a binární operace + a $\cdot$ na $X$ jsou takové, že

| + | 0 | 1 | a | b |
|---|---|---|---|---|
| 0 | 0 | 1 | a | b |
| 1 | 1 | 0 | b | a |
| a | a | b | 0 | 1 |
| b | b | a | 1 | 0 |

a

| · | 0 | 1 | a | b |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | a | b |
| a | 0 | a | b | 1 |
| b | 0 | b | 1 | a |

Množina $X$ s těmito operacemi + a $\cdot$ je pole. □

**Poznámka.** Buď $n$ libovolné přirozené číslo. Potom existuje $n$-prvkové pole právě tehdy, když $n$ je mocnina prvočísla, čili $n = p^k$, kde $p$ je prvočíslo a $k$ je přirozené číslo.

Stejně jako máme podgrupy grup (a podstruktury dalších algebraických struktur), existují podokruhy okruhů a podpole polí. Zmíníme jen podpole.

**Definice 6.0.2.** Buď $P$ pole. Buď $Q \subseteq P$ podmnožina taková, že
(1) $0, 1 \in Q$;
(2) je-li $x, y \in Q$, pak $x + y \in Q$ a $xy \in Q$;
(3) je-li $x \in Q$, pak $-x \in Q$;
(4) je-li $x \in Q$, $x \neq 0$, pak $x^{-1} \in Q$.
Potom $Q$ je *podpole* pole $P$.

Aby podmnožina pole byla podpole, musí obsahovat neutrální prvky obou binárních operací, musí být uzavřená vzhledem k oběma binárním operacím a musí být uzavřená vzhledem k inverzím vzhledem k oběma binárním operacím.

Každé podpole je pole.

**Příklad.** (1) Pole $\mathbb{Q}$ je podpole polí $\mathbb{R}$ a $\mathbb{C}$. Pole $\mathbb{R}$ je podpole pole $\mathbb{C}$.

(2) $\mathbb{Z}$ není podpole pole $\mathbb{Q}$, neboť neobsahuje inverzi k 2 vzhledem k operaci $\cdot$.

(3) Množina $\{0, 1\}$ není podpole pole $\mathbb{Q}$ (a samozřejmě ani $\mathbb{R}$ a $\mathbb{C}$), protože $1 + 1 = 2 \notin \{0, 1\}$. Ačkoliv, jak už víme, na množině $\{0, 1\}$ lze definovat operace sčítání a násobení tak, že to je pole. □

**Definice 6.0.3.** Podpole pole $\mathbb{C}$ je *číselné pole.*

# 7. Uspořádání a svazy

## 7.1. Uspořádané množiny

**Definice 7.1.1.** Relace $\rho$ na množině $X$ je *uspořádání*, jestliže je
(1) reflexivní, tj. $x \rho x$ pro každé $x \in X$,
(2) antisymetrická, tj. $x \rho y$, $y \rho x$ implikuje $x = y$,
(3) tranzitivní, tj. $x \rho y$, $y \rho z$ implikuje $x \rho z$.
Potom dvojice $(X, \rho)$ je *uspořádaná množina*.

**Příklad.** (1) Pro libovolnou množinu $X$ relace $=$ je uspořádání.

(2) $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$ $(\mathbb{R}, \leq)$, kde $\leq$ je obvyklé uspořádání podle velikosti, jsou uspořádané množiny.

(3) Buďte $X$ množina a $\mathcal{P}(X)$ množina všech podmnožin množiny $X$. Inkluze $\subseteq$ je uspořádání na $\mathcal{P}(X)$.

(4) Relace $|$ (dělí) na množině $\mathbb{N}$ (tj. $x \mid y$ právě tehdy, když existuje $n \in \mathbb{N}$ takové, že $x \cdot n = y$) je uspořádání, nazývá se *relace dělitelnosti*. Je zřejmé, že tato relace je reflexivní a tranzitivní.

Ukážeme, že $|$ je i antisymetrická relace. Předpokládejme, že $x \mid y$ a $y \mid x$, tedy existují $m, n \in \mathbb{N}$ taková, že $xm = y$ a $yn = x$. Potom $xmn = x$ a jelikož $x \neq 0$, $mn = 1$. V přirozených číslech to lze jedině tak, že $m = 1$ a $n = 1$. Tedy $x = x \cdot 1 = y$.

Upozorňeme, že obdobně definovaná relace dělitelnosti na $\mathbb{Z}$ není antisymetrická, protože $1 \neq -1$, přestože $1 \mid -1$ a $-1 \mid 1$ (rovnice $mn = 1$ má v celých číslech další řešení $m = -1$ a $n = -1$). □

Buď $\rho$ uspořádání na množině $X$. Inverzní (opačná) relace $\rho^{-1}$ (tj. relace definovaná předpisem „$x \rho^{-1} y$ právě tehdy, když $y \rho x$“) je také uspořádání. Nazývá se *duální uspořádání*. Máme-li uspořádání $\leq$, potom duální uspořádání $\leq^{-1}$ se označuje symbolem $\geq$. Podobně je to se symboly $\subseteq$ atp.

**Definice 7.1.2.** Buď $(X, \leq)$ uspořádaná množina, $Y \subseteq X$. Relace $\leq_Y$ na množině $Y$ zadaná předpisem $x \leq_Y y \Leftrightarrow x \leq y$ je uspořádání na množině $Y$. Nazývá se *indukované uspořádání* a značí se rovněž $\leq$.

**Definice 7.1.3.** Prvky $x, y$ uspořádané množiny jsou *srovnatelné*, platí-li $x \leq y$ nebo $y \leq x$. Uspořádaná množina je *řetězec*, jsou-li každé dva její prvky srovnatelné.

**Příklad.** $(\mathbb{R}, \leq)$, $(\mathbb{Z}, \leq)$ $(\mathbb{N}, \leq)$ jsou řetězce. □

Buď $\leq$ uspořádání na $X$. Označme $x < y$, jestliže $x \leq y$ a zároveň $x \neq y$. Dále zaveďme označení $x \lhd y$, jestliže $x < y$ a neexistuje $z \in X$ takové, že $x < z$, $z < y$. Je-li $x \lhd y$, pak říkáme, že $x$ je *bezprostředním předchůdcem* $y$, nebo $y$ *pokrývá* $x$.

**Příklad.** (1) V množině $\mathbb{N}$ s přirozeným uspořádáním podle velikosti platí $1 < 2$ a $1 \lhd 2$, $1 < 3$, ale neplatí $1 \lhd 3$.

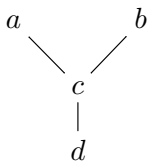
(2) V množině $\mathbb{N}$ s relací dělitelnosti 6 pokrývá 3.

(3) V množině $\mathbb{Q}$ všech racionálních čísel s přirozeným uspořádáním podle velikosti neplatí $x \lhd y$ pro žádnou dvojici $x, y \in \mathbb{Q}$. Pro libovolné $x, y \in \mathbb{Q}$ takové, že $x < y$, platí $z = \frac{1}{2}(x + y) \in \mathbb{Q}$ a $x < z$, $z < y$. □

Konečnou uspořádanou množinu $(X, \leq)$ můžeme znázornit diagramem. Prvky množiny $X$ znázorníme jako body v rovině. Prvky $x, y$ splňující $x \lhd y$ vyznačíme tak, že $x$ leží níže než $y$ a spojíme je úsečkou.

Z diagramu pak můžeme určit uspořádání množiny $X$: $x \leq y$ právě tehdy, když $x$ leží níže než $y$ a existuje zdola nahoru směřující konečná posloupnost na sebe navazujících úseček z bodu $x$ do bodu $y$.

**Příklad.** V uspořádané množině $Y = \{a, b, c, d\}$ s diagramem vpravo platí:




- $d \lhd c$, $c \lhd a$, $c \lhd b$,
- $d < a$, ale nikoliv $d \lhd a$,
- prvky $a, b$ nejsou srovnatelné. □

**Definice 7.1.4.** Buď $(X, \leq)$ uspořádaná množina, $Y \subseteq X$. Prvek $x \in X$ je
- *dolní závora* množiny $Y$, je-li $x \leq y$ pro každé $y \in Y$;
- *horní závora* množiny $Y$, je-li $y \leq x$ pro každé $y \in Y$.

**Příklad.** V uspořádané množině $Y$ z předchozího příkladu platí:
- $c, d$ jsou dolní závory podmnožiny $\{a, b\}$,
- podmnožina $\{a, b\}$ nemá žádnou horní závoru. □

**Definice 7.1.5.** Buď $(X, \leq)$ uspořádaná množina. Prvek $x \in X$ je
- *nejmenší* (*minimální*) prvek množiny $X$, je-li $x \leq y$ pro každé $y \in X$, v takovém případě píšeme $x = \min X$;
- *největší* (*maximální*) prvek množiny $X$, je-li $x \geq y$ pro každé $y \in X$, v takovém případě píšeme $x = \max X$.

**Příklad.** V uspořádané množině $Y$ z předchozího příkladu platí:
- $d$ je její nejmenší prvek,
- její největší prvek neexistuje. □

**Cvičení.** Každá uspořádaná množina má nejvýše jeden největší prvek a nejvýše jeden nejmenší prvek. □

**Definice 7.1.6.** Buď $(X, \leq)$ uspořádaná množina, $Y \subseteq X$. Prvek $x \in X$ je
- *infimum* množiny $Y$, je-li $x$ největší prvek množiny všech dolních závor množiny $Y$, v takovém případě píšeme $x = \inf Y$,
- *supremum* množiny $Y$, je-li $x$ nejmenší prvek množiny všech horních závor množiny $Y$, v takovém případě píšeme $x = \sup Y$.

**Příklad.** V uspořádané množině $Y$ z předchozího příkladu platí:
- množina dolních závor podmnožiny $\{a, b\}$ je $\{c, d\}$, její největší prvek je $c$, a proto $\inf\{a, b\} = c$,
- podmnožina $\{a, b\}$ nemá žádnou horní závoru, čili množina horních závor je prázdná, nemá tedy největší prvek, a proto $\sup\{a, b\}$ neexistuje. □

**Cvičení.** (1) Každá podmnožina má nejvýše jedno supremum a nejvýše jedno infimum.

(2) Jestliže $x \leq y$, pak $\inf\{x, y\} = x$ a $\sup\{x, y\} = y$.

(3) Jestliže $\inf\{x, y\} = x$, pak $x \leq y$.

(4) Jestliže $\sup\{x, y\} = y$, pak $x \leq y$. □

**Cvičení.** Buď $X$ uspořádaná množina. Supremum prázdné množiny je nejmenší prvek množiny $X$ (pokud existuje) a infimum prázdné množiny je největší prvek množiny $X$ (pokud existuje). □

## 7.2. Svazově uspořádané množiny a svazy

**Definice 7.2.1.** Uspořádaná množina je *svazově uspořádaná*, jestliže každá její dvouprvková podmnožina má infimum i supremum.

Každá konečná podmnožina svazově uspořádané množiny má infimum i supremum.

**Příklad.** (1) Pro libovolnou množinu $X$ je $(\mathcal{P}(X), \subseteq)$ svazově uspořádaná množina, přičemž pro libovolné $Y, Z \in \mathcal{P}(X)$ $\inf\{Y, Z\} = Y \cap Z$ a $\sup\{Y, Z\} = Y \cup Z$.

(2) $(\mathbb{N}, |)$ je svazově uspořádaná množina, přičemž $\inf\{x, y\}$ je největší společný dělitel čísel $x, y$, $\sup\{x, y\}$ je nejmenší společný násobek čísel $x, y$.

(3) $(\{1, 3, 5, 6, 9, 10, 12\}, |)$ není svazově uspořádaná množina.

(4) Každý řetězec je svazově uspořádaná množina, přičemž $\inf\{x, y\} = \min\{x, y\}$ je menší z prvků $x, y$, $\sup\{x, y\} = \max\{x, y\}$ je větší z prvků $x, y$. □

**Definice 7.2.2.** Množina $X$ se dvěma binárními operacemi $\wedge$ a $\vee$ je *svaz*, jestliže pro každé $x, y, z \in X$ platí

| | | |
|---|---|---|
| $x \wedge y = y \wedge x$, | $x \vee y = y \vee x$, | (komutativita $\wedge$ a $\vee$) |
| $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, | $(x \vee y) \vee z = x \vee (y \vee z)$, | (asociativita $\wedge$ a $\vee$) |
| $x \wedge (y \vee x) = x$, | $x \vee (y \wedge x) = x$. | (zákon absorpce) |

Binární operace $\wedge$ je *průsek*, binární operace $\vee$ je *spojení*.

**Příklad.** (1) Pro libovolnou množinu $X$ množina $\mathcal{P}(X)$ s operacemi $\cap$ a $\cup$ je svaz.

(2) Množina $\mathbb{N}$ s operacemi $\mathrm{D}$ a $\mathrm{N}$, kde $x \,\mathrm{D}\, y$ je největší společný dělitel čísel $x, y$ a $x \,\mathrm{N}\, y$ je nejmenší společný násobek čísel $x, y$, je svaz.

(3) Množina $\mathbb{R}$ s operacemi min a max je svaz.

(4) Množina $\{0, 1\}$ pravdivostních hodnot s operacemi konjunkce a disjunkce je svaz. □

**Tvrzení 7.2.1.** *Buď $(X, \wedge, \vee)$ svaz. Pro libovolné $x \in X$ platí*

$$x \wedge x = x, \qquad x \vee x = x. \qquad \textit{(idempotentnost } \wedge \textit{ a } \vee\textit{)}$$

*Důkaz.*

$$\begin{aligned} x \wedge x &= && \text{(zákon absorpce)} \\ &= x \wedge (x \vee (y \wedge x)) = && \text{(komutativita } \vee\text{)} \\ &= x \wedge ((y \wedge x) \vee x) = && \text{(zákon absorpce)} \\ &= x. \end{aligned}$$

Druhou část tvrzení necháme jako cvičení. □

Ve svazově uspořádané množině $X$ pro každé $x, y$ existují $\inf\{x, y\}$ a $\sup\{x, y\}$ a jsou jednoznačně určena, proto můžeme na $X$ definovat binární operace $\wedge$ a $\vee$:

$$x \wedge y := \inf\{x, y\}, \quad x \vee y := \sup\{x, y\}.$$

Podle následujícího tvrzení každá svazově uspořádaná množina s těmito operacemi je svaz.

**Tvrzení 7.2.2.** *Svazově uspořádaná množina $X$ s binárními operacemi $\wedge$, $x \wedge y = \inf\{x, y\}$, a $\vee$, $x \vee y = \sup\{x, y\}$, je svaz.*

*Důkaz.* Cvičení.
Asociativita $\vee$: Návod: Ukažte, že $x \vee (y \vee z) = \sup\{x, y, z\} = (x \vee y) \vee z$. □

**Cvičení.** Dokažte, že $x_1 \vee x_2 \vee \cdots \vee x_n = \sup\{x_1, x_2, \ldots, x_n\}$. (Vlevo nezáleží na uzávorkování). □

Podle následujícího tvrzení každý svaz je svazově uspořádaná množina.

**Tvrzení 7.2.3.** *Buď $(X, \wedge, \vee)$ svaz.*

*(1) Položme $x \leq_\wedge y$ právě tehdy, když $x \wedge y = x$. Pak $\leq_\wedge$ je uspořádání na $X$.*

*(2) Položme $x \leq_\vee y$ právě tehdy, když $x \vee y = y$. Pak $\leq_\vee$ je uspořádání na $X$.*

*(3) Uspořádání $\leq_\wedge$ je shodné s uspořádáním $\leq_\vee$ a $(X, \leq_\wedge)$ je svazově uspořádaná množina, přičemž*

$$\inf\{x, y\} = x \wedge y, \quad \sup\{x, y\} = x \vee y.$$

*Důkaz.* Cvičení. □

Svazy i svazově uspořádané množiny tedy můžeme chápat jak jako algebraické struktury tak jako uspořádané množiny. Uspořádání totiž jednoznačně určuje algebraickou strukturu a algebraická struktura zase jednoznačně určuje uspořádání.

Buď $(X, \wedge, \vee)$ svaz. Identity v definici svazu jsou symetrické vzhledem k vzájemné záměně $\wedge$ a $\vee$, proto $(X, \vee, \wedge)$ je také svaz. Nazývá se *duální svaz* a značí se $X^*$.

**Cvičení.** Ověřte, že duální svaz má duální uspořádání. □

**Tvrzení 7.2.4.** *Buď $X$ svaz. Pro každé $x, a, b \in X$ platí*

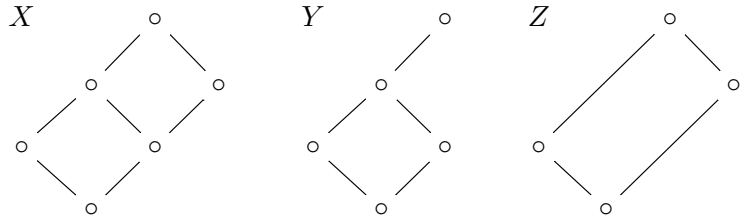
*(i) jestliže $a \leq b$, pak $a \wedge x \leq b \wedge x$;*
*(ii) jestliže $a \leq b$, pak $a \vee x \leq b \vee x$;*
*(iii) jestliže $x \leq a$, $x \leq b$, pak $x \leq a \wedge b$;*
*(iv) jestliže $x \geq a$, $x \geq b$, pak $x \geq a \vee b$.*

*Důkaz.* (i) Nechť $a \leq b$, pak $a \wedge b = a$, načež $(a \wedge x) \wedge (b \wedge x) = a \wedge b \wedge x = a \wedge x$; odtud tvrzení. (ii) Cvičení. (iii) a (iv) plynou ihned z definice infima a suprema (cvičení). □

Obsahuje-li podmnožina svazu všechna infima a suprema všech dvojic svých prvků, je to také svaz.

**Definice 7.2.3.** *Podsvaz* svazu $(X, \wedge, \vee)$ je podmnožina $Y \subseteq X$ taková, že pro každé $x, y \in Y$ platí $x \wedge y \in Y$ a $x \vee y \in Y$.

**Příklad.** Svaz $X$ a jeho podsvazy $Y$ a $Z$:



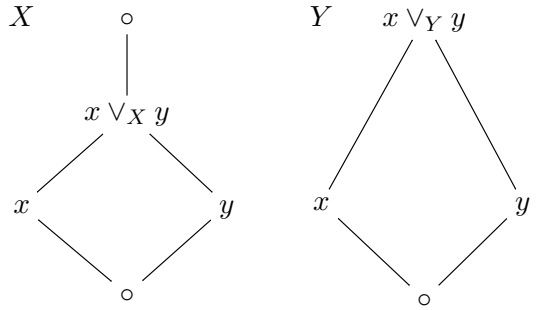

□

**Cvičení.** (1) Každá podmnožina řetězce je podsvaz.

(2) Každá podmnožina svazu, která je řetězcem, je podsvaz. □

Podmnožina svazu může být svazem vzhledem k indukovanému uspořádání, aniž by byla podsvazem.

**Příklad.** Svaz $X$ a jeho podmnožina $Y$, která je svazem, ale není podsvazem.




Supremum $x \vee_Y y$ v $Y$ je různé od suprema $x \vee_X y$ v $X$. □

## 7.3. Úplné svazy

**Definice 7.3.1.** Svaz je *úplný*, má-li každá jeho podmnožina supremum i infimum.

**Příklad.** (1) Každý konečný svaz je úplný a platí $\inf\{x_1, x_2, \ldots, x_n\} = x_1 \wedge x_2 \wedge \ldots \wedge x_n$, $\sup\{x_1, x_2, \ldots, x_n\} = x_1 \vee x_2 \vee \ldots \vee x_n$.

(2) Svaz $(\mathcal{P}(M), \subseteq)$ je úplný. Infima jsou průniky, suprema jsou sjednocení.

(3) Svaz $(\mathbb{N}, \leq)$ není úplný. Schází například supremum celé množiny $\mathbb{N}$. □

Každý úplný svaz má největší prvek, je to jeho supremum, i nejmenší prvek, je to jeho infimum.

**Tvrzení 7.3.1.** *Buď $X$ uspořádaná množina, jejíž každá podmnožina má infimum. Pak $X$ je úplný svaz.*

*Důkaz.* Stačí ukázat, že každá podmnožina má supremum. Buď $Y \subseteq X$. Označme $Z$ množinu všech horních závor množiny $Y$ a položme $s = \inf Z$. Dokažme, že $s = \sup Y$.

Každý prvek množiny $Z$ je horní závora množiny $Y$, takže každý prvek množiny $Y$ je dolní závora množiny $Z$. Jelikož $s$ je největší dolní závora množiny $Z$, tak $y \leq s$ pro každé $y \in Y$, čili $s$ je zároveň horní závora množiny $Y$. A když $s \in Z$ a současně $s$ je (největší) dolní závora množiny $Z$, je to nejmenší prvek množiny $Z$, čili nejmenší horní závora množiny $Y$. □

**Příklad.** Předpoklad, že každá (i prázdná) podmnožina množiny $X$ má infimum, znamená, že $X$ má největší prvek. Například $(\mathbb{N}, \leq)$ není úplný svaz, přestože každá *neprázdná* podmnožina má infimum. □

**Příklad.** Buď $G$ grupa. Označme $P(G)$ množinu všech podgrup grupy $G$. Pak $(P(G), \subseteq)$ je úplný svaz.

Buď $\{A_\iota \mid \iota \in I\} \subseteq P(G)$, tedy nějaký systém podgrup grupy $G$. Potom $\bigcap_{\iota \in I} A_\iota$ je také podgrupa (cvičení), která je zároveň $\inf\{A_\iota \mid \iota \in I\}$ (cvičení). Podle předchozího tvrzení je $(P(G), \subseteq)$ úplný svaz. Proto existuje i $\sup\{A_\iota \mid \iota \in I\}$ a je to průnik všech podgrup, které obsahují všechny podgrupy $A_\iota$.

Příklad je zformulován pro grupy, ale jeho analogie platí i pro jiné algebraické struktury. □

**Cvičení.** Označme $E(X)$ množinu všech relací ekvivalence na množině $X$. Protože $E(X) \subset \mathcal{P}(X \times X)$, vzniká na $E(X)$ indukované uspořádání. Dokažte, že $E(X)$ je úplný svaz. □

# 8. Homomorfismy

## 8.1. Homomorfismy a izomorfismy grup

### 8.1.1. Homomorfismy grup

**Definice 8.1.1.** Buďte $(X,\ *, e_X, {}^{-1})$, $(Y,\ \diamond, e_Y, {}^{-1})$ grupy. Zobrazení $f\colon X \to Y$ je *homomorfismus grup*, jestliže

(i) pro každé $x_1, x_2 \in X$ platí $f(x_1 * x_2) = f(x_1) \diamond f(x_2)$,
(ii) $f(e_X) = e_Y$,
(iii) pro každé $x \in X$ platí $f(x^{-1}) = (f(x))^{-1}$.

Značí se $f\colon (X,\ *, e_X, {}^{-1}) \to (Y,\ \diamond, e_Y, {}^{-1})$.

**Příklad.** (1) $f_2\colon (\mathbb{Z},\ +, 0, -) \to (\mathbb{Z},\ +, 0, -)$, $n \mapsto 2n$, je homomorfismus grup.

(2) Buď $X$ grupa, $\tilde{X}$ faktorová grupa. Potom zobrazení $X \to \tilde{X}$, $x \mapsto [x]$ (faktorová projekce) je homomorfismus grup.

(3) Buďte $X = \{0, 1, 2, 3\}$ a $Y = \{0, 1\}$ s binárními operacemi $+$ takovými, že

| $+$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

a

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

Potom množiny $X$ a $Y$ s těmito operacemi jsou grupy. Zobrazení $X \to Y$, $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 0$, $3 \mapsto 1$, je homomorfismus těchto grup. □

**Tvrzení 8.1.1.** *Buďte $(X,\ *, e_X, {}^{-1}), (Y,\ \diamond, e_Y, {}^{-1})$ grupy. Buď $f\colon X \to Y$ zobrazení takové, že pro každé $x_1, x_2 \in X$ platí $f(x_1 * x_2) = f(x_1) \diamond f(x_2)$. Pak $f$ je homomorfismus grup $(X,\ *, e_X, {}^{-1}) \to (Y,\ \diamond, e_Y, {}^{-1})$.*

*Důkaz.* Podmínka (i) z definice homomorfismu grup je podle předpokladu splněna.

Ukažme, že $f(e_X) = e_Y$.

$$\begin{aligned} f(e_X) &= f(e_X) \diamond e_Y = \\ &= f(e_X) \diamond f(e_X) \diamond (f(e_X))^{-1} = \\ &= f(e_X * e_X) \diamond (f(e_X))^{-1} = \\ &= f(e_X) \diamond (f(e_X))^{-1} = \\ &= e_Y. \end{aligned}$$

Ukažme, že $f(x^{-1}) = (f(x))^{-1}$ pro každé $x \in X$.

$$f(x^{-1}) \diamond f(x) = f(x^{-1} * x) = f(e_X) = e_Y,$$
$$f(x) \diamond f(x^{-1}) = f(x * x^{-1}) = f(e_X) = e_Y.$$

Takže $f(x^{-1})$ je inverze k $f(x)$. □

**Cvičení.** Buď $f\colon X \to Y$ homomorfismus grup. Označme

$$\operatorname{Im} f = \{f(x) \mid x \in X\}.$$

Pak $\operatorname{Im} f$ je podgrupa v $Y$. □

**Tvrzení 8.1.2.** *Buďte $f\colon X \to Y$ a $g\colon Y \to Z$ homomorfismy grup. Pak jejich složení $g \circ f\colon X \to Z$ je homomorfismus grup.*

*Důkaz.* Buďte $(X,\ *, e_X, {}^{-1}), (Y,\ \diamond, e_Y, {}^{-1}), (Z,\ \cdot, e_Z, {}^{-1})$ grupy. Pro každé $x_1, x_2 \in X$ platí

$$\begin{aligned}(g \circ f)(x_1 * x_2) &= g(f(x_1 * x_2)) = \\ &= g(f(x_1) \diamond f(x_2)) = \\ &= g(f(x_1)) \cdot g(f(x_2)) = \\ &= (g \circ f)(x_1) \cdot (g \circ f)(x_2).\end{aligned}$$

Zbytek vyplývá z předchozího tvrzení. □

### 8.1.2. Izomorfismy grup

**Definice 8.1.2.** *Izomorfismus grup* je homomorfismus grup, který je bijektivní.

**Tvrzení 8.1.3.** *Buď $f\colon X \to Y$ izomorfismus grup. Pak $f^{-1}\colon Y \to X$ je izomorfismus grup.*

*Důkaz.* Buďte $(X,\ *, e_X, {}^{-1}), (Y,\ \diamond, e_Y, {}^{-1})$ grupy. Inverzní zobrazení je bijektivní. Pro libovolné $y_1, y_2 \in Y$ označme $x_1 = f^{-1}(y_1)$ a $x_2 = f^{-1}(y_2)$. Takže $f(x_1) = y_1$ a $f(x_2) = y_2$. Potom

$$\begin{aligned}f^{-1}(y_1 \diamond y_2) = f^{-1}(f(x_1) \diamond f(x_2)) = f^{-1}(f(x_1 * x_2)) = x_1 * x_2 = \\ = f^{-1}(y_1) * f^{-1}(y_2).\end{aligned}$$

Zbytek vyplývá z Tvrzení 8.1.1. □

**Příklad.** (1) Každá identita je izomorfismus.

(2) Označme $\mathbb{R}_+$ množinu všech kladných reálných čísel. Pak $(\mathbb{R}_+, \cdot, 1, {}^{-1})$ je grupa (cvičení). Zobrazení $\exp\colon (\mathbb{R},\ +, 0, -) \to (\mathbb{R}_+,\ \cdot, 1, {}^{-1})$, $x \mapsto \mathrm{e}^x$ je homomorfismus grup, protože pro libovolná $x, y \in \mathbb{R}$ platí $\exp(x + y) = \mathrm{e}^{x+y} = \mathrm{e}^x \mathrm{e}^y = (\exp x) \cdot (\exp y)$. Tento homomorfismus je bijektivní, tedy i izomorfismus.

Inverzní izomorfismus je logaritmus

$$\ln\colon (\mathbb{R}_+,\ \cdot, 1, {}^{-1}) \to (\mathbb{R},\ +, 0, -).$$ □

**Definice 8.1.3.** Dvě grupy $X, Y$ jsou *izomorfní*, jestliže existuje izomorfismus $X \to Y$. Zapisujeme $X \cong Y$.

**Tvrzení 8.1.4.** *Pro libovolné grupy $X, Y, Z$ platí*

*(i) $X \cong X$ (reflexivita),*
*(ii) jestliže $X \cong Y$, pak $Y \cong X$ (symetrie),*
*(iii) jestliže $X \cong Y$ a $Y \cong Z$, pak $X \cong Z$ (tranzitivita).*

*Důkaz.* Cvičení. □

**Příklad.** $(\mathbb{R},\ +, 0, -) \cong (\mathbb{R}_+,\ \cdot, 1, {}^{-1})$. Pro libovolné $a \in \mathbb{R}_+, a \neq 1$, zobrazení $\mathbb{R} \to \mathbb{R}_+$, $x \mapsto a^x$ je izomorfismus $(\mathbb{R},\ +, 0, -) \to (\mathbb{R}_+,\ \cdot, 1, {}^{-1})$. Ověřte. □

**Cvičení.** Buď $h\colon X \to Y$ homomorfismus grup.

(1) Ukažte, že relace $\sim$ zadaná předpisem

$$x_1 \sim x_2 \Leftrightarrow h(x_1) = h(x_2)$$

je kongruence na grupě $X$.

(2) Ukažte, že faktorová grupa $\tilde{X}$ podle kongruence $\sim$ je izomorfní podgrupě $\operatorname{Im} h$. Návod: $\tilde{X} \to \operatorname{Im} h$, $[x] \mapsto h(x)$. □

## 8.2. Homomorfismy a izomorfismy polí

**Definice 8.2.1.** Buďte $P, Q$ pole. Zobrazení $f\colon P \to Q$ je *homomorfismus polí*, jestliže

(i) pro každé $p_1, p_2 \in P$ platí $f(p_1 + p_2) = f(p_1) + f(p_2)$,
(ii) $f(0) = 0$,
(iii) pro každé $p \in P$ platí $f(-p) = -f(p)$,
(iv) pro každé $p_1, p_2 \in P$ platí $f(p_1 \cdot p_2) = f(p_1) \cdot f(p_2)$,
(v) $f(1) = 1$,
(vi) pro každé $p \in P$, $p \neq 0$, platí $f(p^{-1}) = (f(p))^{-1}$.

**Definice 8.2.2.** Je-li homomorfismus polí navíc bijektivní, je to *izomorfismus polí*. Pole, mezi nimiž existuje izomorfismus, jsou *izomorfní*.

**Příklad.** Dvouprvkové pole $\{0, 1\}$ je izomorfní s polem $\mathbb{Z}_2$. Izomorfismem je zobrazení $0 \mapsto [0]_2, 1 \mapsto [1]_2$. □

## 8.3. Izotonní zobrazení, homomorfismy a izomorfismy svazů

### 8.3.1. Izotonní zobrazení a izomorfismy uspořádaných množin

**Definice 8.3.1.** Buďte $(X, \leq)$, $(Y, \leq)$ uspořádané množiny. Zobrazení $f\colon X \to Y$ je *izotonní*, jestliže platí implikace

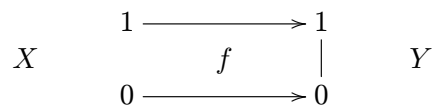
$$x \leq y \Rightarrow f(x) \leq f(y).$$

Je-li zobrazení $f$ bijektivní a $f$ i $f^{-1}$ jsou izotonní, pak $f$ je *izomorfismus uspořádaných množin* a uspořádané množiny $(X, \leq)$, $(Y, \leq)$ jsou *izomorfní*.

**Příklad.** Identické zobrazení $\mathrm{id}\colon (\mathbb{N}, |) \to (\mathbb{N}, \leq)$ je izotonní. Skutečně, jestliže $a \mid b$, pak $b = na$ pro nějaké $n \in \mathbb{N}$, ale $n \geq 1$, a proto $b = na \geq a$.

Inverzní zobrazení $\mathrm{id}\colon (\mathbb{N}, \leq) \to (\mathbb{N}, |)$ není izotonní, protože neplatí implikace $x \leq y \Rightarrow x \mid y$ (například $2 \leq 3$, ale $2 \nmid 3$). □

**Příklad.** Buďte $X = Y = \{0, 1\}$ s uspořádáními a zobrazením $f$ podle obrázku:




Tedy $f\colon X \to Y$ je identické zobrazení. Pak $f$ je izotonní bijekce, jejíž inverze $f^{-1}$ není izotonní. □

**Cvičení.** Složení izotonních zobrazení je izotonní zobrazení. □

### 8.3.2. Homomorfismy a izomorfismy svazů

**Definice 8.3.2.** Buďte $(X, \wedge, \vee)$, $(Y, \wedge, \vee)$ svazy. Zobrazení $f\colon X \to Y$ je *homomorfismus svazů*, jestliže pro každé $x_1, x_2 \in X$

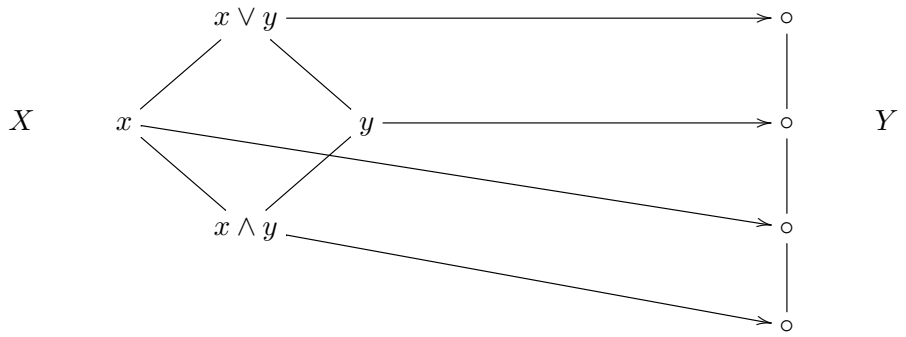
$$f(x_1 \wedge x_2) = f(x_1) \wedge f(x_2)$$
$$f(x_1 \vee x_2) = f(x_1) \vee f(x_2).$$

**Tvrzení 8.3.1.** *Každý homomorfismus svazů je izotonní zobrazení.*

*Důkaz.* Buďte $(X, \wedge, \vee)$, $(Y, \wedge, \vee)$ svazy, $f\colon X \to Y$ homomorfismus a $x_1, x_2 \in X$ takové, že $x_1 \leq x_2$, tedy $x_1 \wedge x_2 = x_1$. Potom $f(x_1) \wedge f(x_2) = f(x_1 \wedge x_2) = f(x_1)$, tedy $f(x_1) \leq f(x_2)$. □

Izotonní zobrazení svazů však nemusí být homomorfismus svazů:

**Příklad.** Buď $f$ zobrazení podle obrázku:




Pak $f$ je izotonní zobrazení svazů, ale není homomorfismus svazů, protože

$$f(x) \vee f(y) = f(y) \neq f(x \vee y).$$ □

**Definice 8.3.3.** *Izomorfismus svazů* je homomorfismus svazů, který je bijektivní.

**Cvičení.** Buď $f$ zobrazení svazů. Dokažte, že následující výroky jsou ekvivalentní:

(1) $f$ je izomorfismus uspořádaných množin;
(2) $f$ je izomorfismus svazů. □

# 9. Vektorové prostory

## 9.1. Definice, příklady, základní vlastnosti

Vektor je běžně znázorňován v rovině nebo v prostoru jako orientovaná úsečka (šipka), která má počáteční bod a koncový bod. Pokud je možné jeden takový vektor převést na druhý takový vektor rovnoběžným posunutím, říká se, že tyto dva vektory jsou totožné nebo ekvivalentní, nebo že jsou to dvě umístění jednoho vektoru. Takové vektory se sčítají pomocí pravidla rovnoběžníku a násobí se reálným číslem tak, že šipka se příslušně prodlouží nebo zkrátí a při násobení záporným číslem navíc změní směr na opačný.

Obecně definujeme vektor jako prvek vektorového prostoru a vektorový prostor nad nějakým polem jako množinu s operací sčítání a s násobením prvků množiny prvky pole s takovými vlastnostmi, které umožňují představu vektoru jako šipky a představu sčítání vektorů a násobení vektoru prvkem pole, jak je uvedeno v předchozím odstavci.

**Definice 9.1.1.** Buď $V$ neprázdná množina, $P$ pole. *Vektorový prostor $V$ nad polem $P$* je množina $V$ spolu s binární operací $+\colon V \times V \to V$, $(u, v) \mapsto u + v$, a zobrazením $\cdot\colon P \times V \to V$, $(p, v) \mapsto p \cdot v$, takovými, že

(1) pro každé $u, v, w \in V$ platí $(u + v) + w = u + (v + w)$,
(2) existuje $0 \in V$ takový, že pro každé $v \in V$ platí $v + 0 = v$,
(3) pro každé $v \in V$ existuje $-v \in V$ takové, že $v + (-v) = 0$,
(4) pro každé $u, v \in V$ platí $u + v = v + u$,
(5) pro každé $v \in V$ platí $1 \cdot v = v$,
(6) pro každé $p, q \in P$ a $v \in V$ platí $(p \cdot q) \cdot v = p \cdot (q \cdot v)$,
(7) pro každé $p, q \in P$ a $v \in V$ platí $(p + q) \cdot v = (p \cdot v) + (q \cdot v)$,
(8) pro každé $p \in P$ a $u, v \in V$ platí $p \cdot (u + v) = (p \cdot u) + (p \cdot v)$.

Prvky množiny $V$ jsou *vektory*, prvky pole $P$ jsou *skaláry*. Binární operace $+$ se nazývá *sčítání*, zobrazení $\cdot$ se nazývá *násobení skalárem*, vektor $0 \in V$ je *nulový vektor* nebo *nula*, vektor $-v$ je *opačný vektor* k vektoru $v$.

Podmínky (1)–(8) jsou *axiomy vektorového prostoru*. Podmínky (1)–(4) znamenají, že $V$ s operací $+$ je komutativní grupa.

Jelikož každá binární operace má nejvýše jeden neutrální prvek, ve vektorovém prostoru existuje jediný nulový vektor. Obdobně, jelikož každý prvek má vzhledem k asociativní binární operaci nejvýše jeden inverzní prvek, ke každému vektoru existuje jediný opačný vektor.

Násobení skalárem $\cdot\colon P \times V \to V$, $(p, v) \mapsto p \cdot v$, není binární operace (není-li $P = V$), ale nazývá se *vnější operace*, a místo $p \cdot v$ se často píše jen $pv$. Binární operace se někdy nazývá *vnitřní operace*.

Vektorový prostor nad polem $\mathbb{R}$, resp. $\mathbb{C}$ se nazývá *reálný*, resp. *komplexní* vektorový prostor.

**Příklad.** (1) Vektorový prostor Eukleidovské geometrie, dvojrozměrné i trojrozměrné, kde vektor je třída ekvivalentních šipek a je reprezentován jednotlivými šipkami, jak je uvedeno v prvním odstavci této kapitoly.

Nulový vektor je reprezentován degenerovanou úsečkou nulové délky. Vektorový prostor v rovině resp. prostoru značíme $E^2$ resp. $E^3$.

(2) Buď $V$ jednoprvková množina, $P$ pole. Jediný prvek množiny $V$ označme 0 a položme $0 + 0 = 0$, $-0 = 0$ a $p \cdot 0 = 0$ pro každé $p \in P$. Dostáváme vektorový prostor nazývaný *nulový prostor* nebo *triviální prostor*.

(3) Každé pole je vektorový prostor nad sebou samým. Položíme-li v definici vektorového prostoru $V = P$, budou všechny axiomy vektorového prostoru důsledky axiomů pole (ověřte). Získáváme tak například vektorový prostor $\mathbb{R}$ nad $\mathbb{R}$, vektorový prostor $\mathbb{C}$ nad $\mathbb{C}$, vektorový prostor $\mathbb{Q}$ nad $\mathbb{Q}$ a vektorový prostor $\mathbb{Z}_2$ nad $\mathbb{Z}_2$.

(4) Každé pole je vektorový prostor nad libovolným svým podpolem. Jediný rozdíl oproti předchozímu příkladu spočívá v tom, že násobení skalárem je dovoleno jen pro skaláry z podpole.

(5) Buď $n \in \mathbb{N}$, $P$ pole. Na množině $P^n$ všech uspořádaných $n$-tic prvků $P$ zaveďme sčítání a násobení skalárem předpisem

$$(u_1, u_2, \ldots, u_n) + (v_1, v_2, \ldots, v_n) = (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n),$$
$$p(u_1, u_2, \ldots, u_n) = (pu_1, pu_2, \ldots, pu_n).$$

Vzniká vektorový prostor $P^n$ nad polem $P$ (ověřte). Například řádky a sloupky matic jsou prvky takových vektorových prostorů.

(6) Vektorový prostor $P^n$ nad podpolem $Q \subset P$.

(7) Vektorový prostor matic typu $m \times n$ nad polem $P$ s operacemi sčítání a násobení skalárem. Značí se $P^{m\times n}$ nebo $\mathcal{M}_{m\times n}(P)$ (resp. $\mathcal{M}_m(P)$ nebo $\mathrm{gl}(m, P)$ v případě čtvercových matic).

(8) Vektorový prostor polynomů stupně nejvýše $n$ nad polem $P$ s operacemi sčítání a násobení skalárem.

(9) Vektorový prostor polynomů nad polem $P$ s operacemi sčítání a násobení skalárem.

(10) Vektorový prostor všech řešení homogenní soustavy rovnic.

(11) Buď $X$ množina, $P$ pole. Na množině $P^X$ všech zobrazení $X \to P$ zaveďme sčítání a násobení skalárem předpisem

$$(u + v)(x) = u(x) + v(x),$$
$$(pu)(x) = p \cdot u(x).$$

Vzniká vektorový prostor $P^X$ nad polem $P$ (ověřte). Speciální případy jsou množina všech funkcí z $\mathbb{R}$ do $\mathbb{R}$, množina všech spojitých funkcí na $\mathbb{R}$, množina diferencovatelných funkcí na $\mathbb{R}$, množina všech spojitých funkcí na intervalu $[a, b]$. □

**Tvrzení 9.1.1.** *Buď $V$ vektorový prostor nad polem $P$. Pak pro každé $u, v \in V$, $p, q \in P$ platí*

*(i)* $0 \cdot v = 0$,
*(ii)* $(-1) \cdot v = -v$,
*(iii)* $(p - q) \cdot v = p \cdot v - q \cdot v$,
*(iv)* $p \cdot (u - v) = p \cdot u - p \cdot v$,
*(v) Je-li* $p \cdot v = 0$, *pak buď* $p = 0$ *nebo* $v = 0$.

*Důkaz.* Cvičení. □

## 9.2. Lineární kombinace, generátory, lineární nezávislost

Buď $V$ vektorový prostor nad polem $P$.

**Definice 9.2.1.** Buďte $n \in \mathbb{N}$, $v_1, v_2, \ldots, v_n \in V$ a $p^1, p^2, \ldots, p^n \in P$. *Lineární kombinace* vektorů $v_1, v_2, \ldots, v_n$ s koeficienty $p^1, p^2, \ldots, p^n$ je vektor

$$p^1 v_1 + p^2 v_2 + \cdots + p^n v_n \in V.$$

Lineární kombinace prázdné množiny vektorů, tedy $n = 0$, je nulový vektor $0 \in V$.

**Příklad.** (1) Součet vektorů $u, v$ je jejich lineární kombinace s koeficienty $1, 1$. Opačný vektor k $v$ je jeho lineární kombinace (skalární násobek) s koeficientem $-1$:

$$u + v = 1 \cdot u + 1 \cdot v, \quad -v = (-1) \cdot v.$$

(2) Lineární kombinace vektorů $1, 6 \in \mathbb{R}$ s koeficienty $3, 1 \in \mathbb{R}$ je $3 \cdot 1 + 1 \cdot 6 = 9$.

(3) Lineární kombinace vektorů $(1, 2, 0), (2, 3, 1) \in \mathbb{R}^3$ s koeficienty $-3, 2 \in \mathbb{R}$ je

$$(-3) \cdot (1, 2, 0) + 2 \cdot (2, 3, 1) = (1, 0, 2). \qquad \square$$

**Definice 9.2.2.** Buď $U \subseteq V$. *Lineární obal* množiny $U$ je množina $[\![U]\!]$ všech lineárních kombinací konečně mnoha vektorů množiny $U$. Pro $U = \{u_1, u_2, \ldots, u_n\}$ je

$$[\![U]\!] = [\![u_1, u_2, \ldots, u_n]\!] = \{p^1 u_1 + p^2 u_2 + \cdots + p^n u_n |\ p^1, p^2, \ldots, p^n \in P\}.$$

Lineární obal prázdné množiny je $[\![\emptyset]\!] = \{0\}$.

**Definice 9.2.3.** Vektory $v_1, v_2, \ldots, v_n \in V$ *generují* $V$, je-li každý vektor $v \in V$ jejich lineární kombinací, to jest, jestliže pro každý vektor $v \in V$ existují skaláry $p^1, p^2, \ldots, p^n \in P$ takové, že $v = p^1 v_1 + p^2 v_2 + \cdots + p^n v_n$, to jest, jestliže $[\![v_1, v_2, \ldots, v_n]\!] = V$.
V takovém případě také množina $\{v_1, v_2, \ldots, v_n\}$ *generuje* $V$ nebo je *množina generátorů* prostoru $V$ nebo $V$ je *generován* vektory $v_1, v_2, \ldots, v_n$.

**Příklad.** (1) Prostor $\mathbb{R}^3$ je generován vektory $(1, 0, 0), (0, 1, 0), (0, 0, 1)$. Skutečně, libovolný vektor $(x, y, z) \in \mathbb{R}^3$ je jejich lineární kombinací s koeficienty $x, y, z$:

$$(x, y, z) = x \cdot (1, 0, 0) + y \cdot (0, 1, 0) + z \cdot (0, 0, 1).$$

(2) Prostor $\mathbb{R}^3$ je generován vektory $(1, 0, 0), (1, 1, 0), (1, 1, 1)$. Skutečně, libovolný vektor $(x, y, z) \in \mathbb{R}^3$ je jejich lineární kombinací s koeficienty $x - y, y - z, z$:

$$(x, y, z) = (x - y) \cdot (1, 0, 0) + (y - z) \cdot (1, 1, 0) + z \cdot (1, 1, 1).$$

(3) Prostor $\mathbb{R}^3$ je generován vektory $(1, 0, 0), (0, 1, 0), (0, 0, 1), (3, 4, 5)$. Libovolný vektor $(x, y, z) \in \mathbb{R}^3$ je jejich lineární kombinací s koeficienty $x, y, z, 0$:

$$(x, y, z) = x \cdot (1, 0, 0) + y \cdot (0, 1, 0) + z \cdot (0, 0, 1) + 0 \cdot (3, 4, 5).$$

V tomto případě můžeme najít dokonce nekonečně mnoho vyjádření ve tvaru lineární kombinace, pro libovolný parametr $t \in \mathbb{R}$ platí

$$(x, y, z) = (x - 3t) \cdot (1, 0, 0) + (y - 4t) \cdot (0, 1, 0) + (z - 5t) \cdot (0, 0, 1) + t \cdot (3, 4, 5).$$

(4) Prostor $\mathbb{R}^3$ není generován vektory $(1, 2, 0), (3, 4, 0), (5, 6, 0)$. Ověřte.

(5) Vektory $v_1, v_2, \ldots, v_n \in \mathbb{R}^m$, kde $v_i = (v_i^1, v_i^2, \ldots, v_i^m)$, generují $\mathbb{R}^m$, jestliže soustava

$$\begin{aligned}
&v_1^1 x^1 + v_2^1 x^2 + \cdots + v_n^1 x^n = v^1 \\
&v_1^2 x^1 + v_2^2 x^2 + \cdots + v_n^2 x^n = v^2 \\
&\vdots \\
&v_1^m x^1 + v_2^m x^2 + \cdots + v_n^m x^n = v^m
\end{aligned}$$

o neznámých $x^1, x^2, \ldots, x^n$ má řešení pro každou pravou stranu $v^1, v^2, \ldots, v^m$. Soustava je totiž ekvivalentní s podmínkou

$$x^1 \begin{pmatrix} v_1^1 \\ v_1^2 \\ \vdots \\ v_1^m \end{pmatrix} + x^2 \begin{pmatrix} v_2^1 \\ v_2^2 \\ \vdots \\ v_2^m \end{pmatrix} + \cdots + x^n \begin{pmatrix} v_n^1 \\ v_n^2 \\ \vdots \\ v_n^m \end{pmatrix} = \begin{pmatrix} v^1 \\ v^2 \\ \vdots \\ v^m \end{pmatrix}.$$

(6) Prostor $\mathbb{R}_2[x]$ polynomů neurčité $x$ s reálnými koeficienty stupně nejvýše 2 je generován vektory $x^2, x+1, 1$. Ověřte. □

**Definice 9.2.4.** Prostor, který má konečnou množinu generátorů, je *konečněrozměrný*.

**Příklad.** Vektorový prostor $\mathbb{R}[x]$ všech polynomů s reálnými koeficienty není konečněrozměrný. Pro libovolné $p_1, \dots, p_n \in \mathbb{R}[x]$ existuje přirozené číslo $m$, které je větší než stupeň kteréhokoliv z polynomů $p_1, \dots, p_n$. Pak polynom $x^m \in \mathbb{R}[x]$ není lineární kombinací polynomů $p_1, \dots, p_n$, takže polynomy $p_1, \dots, p_n$ negenerují $\mathbb{R}[x]$. □

**Cvičení.** (1) Jestliže $v_1, \dots, v_n$ generují $V$ a $v_i$ je lineární kombinací ostatních, pak $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$ také generují $V$. Dokažte.

(2) Nechť každý z vektorů $v_1, \dots, v_n$ je lineární kombinace vektorů $u_1, \dots, u_m \in V$. Jestliže $v_1, \dots, v_n$ generují $V$, pak $u_1, \dots, u_m$ také generují $V$. Dokažte. □

**Definice 9.2.5.** Buď $V$ vektorový prostor nad polem $P$.

(1) Množina vektorů $\{v_1, v_2, \dots, v_n\} \subseteq V$ je *lineárně nezávislá*, jestliže z rovnosti

$$x^1 v_1 + x^2 v_2 + \cdots + x^n v_n = 0, \text{ kde } x^1, x^2, \dots, x^n \in P,$$

plyne $x^1 = x^2 = \cdots = x^n = 0$.

(2) Množina vektorů $\{v_1, v_2, \dots, v_n\} \subseteq V$ je *lineárně závislá*, jestliže není lineárně nezávislá.

Často se zjednodušeně a nepřesně říká, že nějaké vektory jsou lineárně (ne)závislé. Myslí se tím, že příslušná množina vektorů je lineárně (ne)závislá.

**Příklad.** (1) Množina $\{7\} \subset \mathbb{R}$ je lineárně nezávislá. Je-li $x \cdot 7 = 0$ pro nějaké $x \in \mathbb{R}$, pak $x = 0$ (pro nenulové $x$ uvedená rovnost $x \cdot 7 = 0$ neplatí).

(2) Množina $\{2, 3\} \subset \mathbb{R}$ je lineárně závislá. Lineární kombinace $x^1 \cdot 2 + x^2 \cdot 3$ může být rovna 0, i když je některý z koeficientů $x^1, x^2$ nenulový, například $x^1 = 3, x^2 = -2$.

(3) Množina $\{(1,0,0), (0,1,0), (0,0,1)\} \subset \mathbb{R}^3$ je lineárně nezávislá. Lineární kombinace $x \cdot (1,0,0) + y \cdot (0,1,0) + z \cdot (0,0,1)$ je vektor $(x, y, z)$, který je roven $(0,0,0)$ právě tehdy, když $x = y = z = 0$ (ověřte).

(4) Množina $\{(1,0,0), (1,1,0), (1,1,1)\} \subset \mathbb{R}^3$ je lineárně nezávislá. Lineární kombinace $x \cdot (1,0,0) + y \cdot (1,1,0) + z \cdot (1,1,1)$ je vektor $(x+y+z, y+z, z)$, který je roven $(0,0,0)$ právě tehdy, když $x = y = z = 0$ (ověřte).

(5) Množina $\{(1,0,-1), (0,1,2), (2,1,0)\} \subset \mathbb{R}^3$ je lineárně závislá. Lineární kombinace $x \cdot (1,0,-1) + y \cdot (0,1,2) + z \cdot (2,1,0)$ je vektor $(x+2z, y+z, -x+2y)$, který je roven $(0,0,0)$ i pro nenulové koeficienty $x, y, z$, například $x = 2, y = 1, z = -1$. Ověřte.

(6) Libovolná množina vektorů obsahující nulový vektor je lineárně závislá. Lineární kombinace $0 \cdot v_1 + 0 \cdot v_2 + \cdots + 0 \cdot v_n + 1 \cdot 0$ je nulový vektor a přitom aspoň jeden koeficient je nenulový.

(7) Množina $\{v_1, \dots, v_n\} \subset \mathbb{R}^m$, kde $v_i = (v_i^1, \dots, v_i^m)$, je lineárně nezávislá právě tehdy, když soustava

$$\begin{aligned} v_1^1 x^1 + v_2^1 x^2 + \cdots + v_n^1 x^n &= 0 \\ v_1^2 x^1 + v_2^2 x^2 + \cdots + v_n^2 x^n &= 0 \\ &\vdots \\ v_1^m x^1 + v_2^m x^2 + \cdots + v_n^m x^n &= 0 \end{aligned}$$

má právě jedno řešení, a to sice $x^1 = x^2 = \cdots = x^n = 0$.

(8) Množina $\{x^2, x, 1\} \subset \mathbb{R}_2[x]$ je lineárně nezávislá. Ověřte.

(9) Prázdná množina je lineárně nezávislá, protože všechny koeficienty z prázdné množiny koeficientů jsou nulové. □

**Cvičení.** (1) Libovolná podmnožina lineárně nezávislé množiny vektorů je lineárně nezávislá. Dokažte.

(2) Jednoprvková monžina $\{v\} \subset V$ je lineárně nezávislá právě tehdy, když $v \neq 0$. Dokažte. □

**Tvrzení 9.2.1.** *Množina vektorů $\{v_1, \dots, v_n\}$ je lineárně závislá právě tehdy, když aspoň jeden z nich je lineární kombinací ostatních, tj. právě když existuje index $i$ takový, že vektor $v_i$ je lineární kombinací vektorů $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$.*

*Důkaz.* „⇒“ Předpokládejme, že množina $\{v_1, \dots, v_n\}$ je lineárně závislá, tedy že existují koeficienty $a^1, \dots, a^n$ takové, že $a^1 v_1 + \cdots + a^i v_i + \cdots + a^n v_n = 0$ a aspoň jeden z nich je nenulový (například $a^i$). Potom

$$v_i = -\frac{a^1}{a^i} v_1 - \cdots - \frac{a^{i-1}}{a^i} v_{i-1} - \frac{a^{i+1}}{a^i} v_{i+1} - \cdots - \frac{a^n}{a^i} v_n,$$

a vektor $v_i$ je tedy lineární kombinací ostatních.

„⇐“ Nechť vektor $v_i$ je lineární kombinací vektorů $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$, tedy existují koeficienty $a^1, \dots, a^{i-1}, a^{i+1}, \dots, a^n$ takové, že

$$v_i = a^1 v_1 + \cdots + a^{i-1} v_{i-1} + a^{i+1} v_{i+1} + \cdots + a^n v_n.$$

Potom

$$a^1 v_1 + \cdots + a^{i-1} v_{i-1} - v_i + a^{i+1} v_{i+1} + \cdots + a^n v_n = 0$$

s nenulovým koeficientem $(-1)$ u vektoru $v_i$. Tedy, množina $\{v_1, \dots, v_n\}$ je lineárně závislá. □

**Tvrzení 9.2.2.** *Množina vektorů $\{v_1, \dots, v_n\}$ je lineárně závislá právě tehdy, když aspoň jeden z nich je lineární kombinací předchozích, tj. právě když existuje index $i$ takový, že vektor $v_i$ je lineární kombinací vektorů $v_1, \dots, v_{i-1}$.*

*Důkaz.* „⇒“ Postupujeme jako v důkazu předchozího tvrzení, jen nenulový koeficient $a^i$ vybereme s nejvyšším možným indexem. To znamená, že $a^{i+1} = \cdots = a^n = 0$ a zbytek je zřejmý.

Jako cvičení rozeberte podrobně případ $i = 1$, kdy bude množina předcházejících vektorů prázdná.

„⇐“ Tvrzení je speciálním případem předchozího. □

**Definice 9.2.6.** *Elementární úprava* $n$-tice vektorů $(v_1, \dots, v_n)$ z vektorového prostoru $V$ nad polem $P$ je:

(i) vynásobení vektoru nenulovým skalárem $c$;
(ii) přičtení $c$-násobku $j$-tého vektoru k $i$-tému vektoru, kde $i \neq j$;
(iii) výměna $i$-tého vektoru s $j$-tým vektorem.

Při tom vznikají po řadě $n$-tice

$$(v_1, \dots, v_{i-1}, cv_i, v_{i+1}, \dots, v_n),$$
$$(v_1, \dots, v_{i-1}, v_i + cv_j, v_{i+1}, \dots, v_j, \dots, v_n),$$
$$(v_1, \dots, v_{i-1}, v_j, v_{i+1}, \dots, v_{j-1}, v_i, v_{j+1}, \dots, v_n).$$

Ke každé z těchto úprav existuje úprava inverzní, která je rovněž elementární a stejného typu (ověřte).

**Definice 9.2.7.** Dvě $n$-tice vektorů jsou *ekvivalentní*, jestliže jedna vznikne z druhé konečnou posloupností elementárních úprav.

**Cvičení.** Ukažte, že právě zavedená relace mezi $n$-ticemi vektorů je reflexivní, symetrická a tranzitivní. □

**Příklad.** Mějme matici typu $m \times n$ nad polem $P$. Její řádky jsou uspořádané $n$-tice prvků pole $P$, tj. vektory z prostoru $P^n$. Celá matice je pak $m$-tice takových $n$-tic, tedy $m$-ticí vektorů z prostoru $P^n$. Elementární úpravy této $m$-tice vektorů jsou právě elementární řádkové úpravy dané matice. □

**Tvrzení 9.2.3.** *Nechť $n$-tice $(u_1, \dots, u_n)$ je ekvivalentní s $n$-ticí $(v_1, \dots, v_n)$. Pak vektory $u_1, \dots, u_n$ generují $V$ právě tehdy, když vektory $v_1, \dots, v_n$ generují $V$.*

*Důkaz.* Nechť lze získat $n$-tici $(v_1, \dots, v_n)$ z $n$-tice $(u_1, \dots, u_n)$ jednou z elementárních úprav, vybereme si úpravu druhého typu, tedy $v_i = u_i + cu_j$ a $v_k = u_k$ pro $k \neq i$.

Předpokládejme, že $v_1, \dots, v_n$ generují $V$. Pro libovolný vektor $w \in V$ tedy existují koeficienty $p^1, \dots, p^n$ takové, že $w = p^1v_1 + \cdots + p^nv_n$. Pak

$$w = p^1u_1 + \cdots + p^i(u_i + cu_j) + \cdots + p^ju_j + \cdots + p^nu_n =$$
$$= p^1u_1 + \cdots + p^iu_i + \cdots + (p^j + cp^i)u_j + \cdots + p^nu_n$$

je lineární kombinace vektorů $u_1, \dots, u_n$.

Opačná implikace vyplývá z právě dokázané, neboť $n$-tice $(u_1, \dots, u_n)$ vzniká z $n$-tice $(v_1, \dots, v_n)$ inverzní úpravou, která je stejného typu.

Pro ostatní úpravy obdobně a výsledek platí i pro libovolnou konečnou posloupnost elementárních úprav. □

**Tvrzení 9.2.4.** *Nechť $n$-tice $(u_1, \dots, u_n)$ je ekvivalentní s $n$-ticí $(v_1, \dots, v_n)$. Pak množina $\{u_1, \dots, u_n\}$ je lineárně nezávislá právě tehdy, když množina $\{v_1, \dots, v_n\}$ je lineárně nezávislá.*

*Důkaz.* Nechť lze získat $n$-tici $(v_1, \dots, v_n)$ z $n$-tice $(u_1, \dots, u_n)$ jednou z elementárních úprav, vybereme si úpravu druhého typu, tedy $v_i = u_i + cu_j$ a $v_k = u_k$ pro $k \neq i$.

Předpokládejme, že $\{u_1, \dots, u_n\}$ je lineárně nezávislá. Buďte $x^1, \dots, x^n \in P$ takové, že $x^1v_1 + \cdots + x^nv_n = 0$. Pak

$$0 = x^1v_1 + \cdots + x^nv_n = x^1u_1 + \cdots + x^i(u_i + cu_j) + \cdots + x^ju_j + \cdots + x^nu_n =$$
$$= x^1u_1 + \cdots + x^iu_i + \cdots + (x^j + cx^i)u_j + \cdots + x^nu_n.$$

Z lineární nezávislosti množiny $\{u_1, \dots, u_n\}$ vyplývá, že všechny koeficienty poslední lineární kombinace jsou nulové, tj. $x^1 = \cdots = x^i = \cdots = x^j + cx^i = \cdots = x^n = 0$. Z toho dostaneme, že i $x^j = 0$.

Opačná implikace vyplývá z právě dokázané, neboť $n$-tice $(u_1, \dots, u_n)$ vzniká z $n$-tice $(v_1, \dots, v_n)$ inverzní úpravou, která je stejného typu.

Pro ostatní úpravy obdobně a výsledek platí i pro libovolnou konečnou posloupnost elementárních úprav. □

**Tvrzení 9.2.5.** *Nechť vektory $v_1, \dots, v_n$ generují prostor $V$ a $\{u_1, \dots, u_m\} \subset V$ je lineárně nezávislá. Pak $m \leq n$.*

*Důkaz.* Každý z vektorů $u_1, \dots, u_m$ je lineární kombinací vektorů $v_1, \dots, v_n$, takže pro každé $i \in \{1, \dots, m\}$ existují koeficienty $a_i^1, \dots, a_i^n$ takové, že $u_i = a_i^1 v_1 + \cdots + a_i^n v_n$. Matici

$$A = \begin{pmatrix} a_1^1 & \dots & a_1^n \\ \vdots & & \\ a_m^1 & \dots & a_m^n \end{pmatrix}$$

upravme pomocí řádkových elementárních úprav na matici $A'$ ve schodovitém tvaru. Provedeme-li stejné elementární úpravy s $m$-ticí $u_1, \dots, u_m$, dostaneme ekvivalentní $m$-tici $u'_1, \dots, u'_m$. Lineární kombinace vektorů $v_1, \dots, v_n$ s koeficienty z jednotlivých řádků matice $A'$ jsou rovny právě vektorům $u'_1, \dots, u'_m$. Z lineární nezávislosti množiny $\{u_1, \dots, u_m\}$ plyne lineární nezávislost množiny $\{u'_1, \dots, u'_m\}$ a také lineární nezávislost, tedy i nenulovost řádků matice $A'$. Jelikož $A'$ je ve schodovitém tvaru a všechny řádky má nenulové, nemá více řádků než sloupků, tedy $m \leq n$.

Tvrzení je také součástí Tvrzení 9.2.7. □

**Lemma 9.2.6** (Lemma o výměně)**.** *Buďte $v_1, \dots, v_n \in V$ a $u = a^1 v_1 + \cdots + a^n v_n$. Pak pro každé $i$ takové, že $a^i \neq 0$, platí $[\![v_1, \dots, v_n]\!] = [\![v_1, \dots, v_{i-1}, u, v_{i+1}, \dots, v_n]\!]$.*

*Důkaz.* Předpokládejme, že $a^1 \neq 0$ (pro jiné indexy je důkaz stejný). Potom

$$v_1 = \frac{1}{a^1} u - \sum_{i=2}^{n} \frac{a^i}{a^1} v_i.$$

Buď $w \in [\![v_1, \dots, v_n]\!]$. Existují tedy $b^1, b^2, \dots, b^n$ takové, že

$$\begin{aligned} w &= b^1 v_1 + b^2 v_2 + \cdots + b^n v_n = \\ &= \frac{b^1}{a^1} u - \sum_{i=2}^{n} \frac{b^1 a^i}{a^1} v_i + b^2 v_2 + \cdots + b^n v_n = \\ &= \frac{b^1}{a^1} u + \sum_{i=2}^{n} \left( b^i - \frac{b^1 a^i}{a^1} \right) v_i \in [\![u, v_2, \dots, v_n]\!]. \end{aligned}$$

Buď $w \in [\![u, v_2, \dots, v_n]\!]$. Existují tedy $c^1, c^2, \dots, c^n$ takové, že

$$\begin{aligned} w &= c^1 u + c^2 v_2 + \cdots + c^n v_n = \\ &= c^1 \sum_{i=1}^{n} a^i v_i + \sum_{i=2}^{n} c^i v_i = \\ &= c^1 a^1 v_1 + \sum_{i=2}^{n} (c^1 a^i + c^i) v_i \in [\![v_1, \dots, v_n]\!]. \end{aligned}$$

□

**Tvrzení 9.2.7** (Steinitzova věta o výměně). *Nechť vektory $v_1, \ldots, v_n$ generují prostor $V$ a $\{u_1, \ldots, u_m\} \subset V$ je lineárně nezávislá. Pak $m \leq n$ a existují indexy $i_1, \ldots, i_{n-m} \in \{1, \ldots, n\}$ takové, že*

$$[\![v_1, \ldots, v_n]\!] = [\![u_1, \ldots, u_m, v_{i_1}, \ldots, v_{i_{n-m}}]\!].$$

*Důkaz.* Množina $\{u_1, \ldots, u_m\}$ je lineárně nezávislá, takže všechny $u_i$ jsou nenulové. Vektor $u_1$ je lineární kombinací vektorů $v_1, \ldots, v_n$ s aspoň jedním nenulovým koeficientem a stejně jako v předchozím důkazu předpokládejme, že nenulový koeficient je u $v_1$. Z Lemmatu o výměně dostaneme $[\![v_1, v_2, \ldots, v_n]\!] = [\![u_1, v_2, \ldots, v_n]\!]$.

Potom vektor $u_2$ je lineární kombinací vektorů $u_1, v_2, \ldots, v_n$ s aspoň jedním nenulovým koeficientem u vektorů $v_2, \ldots, v_n$ (jinak by byla množina $\{u_1, u_2\}$ lineárně závislá). Opět pro jednoduchost předpokládejme, že nenulový koeficient je u $v_2$. Z Lemmatu o výměně dostaneme $[\![u_1, v_2, \ldots, v_n]\!] = [\![u_1, u_2, v_3, \ldots, v_n]\!]$.

Takto pokračujeme, dokud buď nepoužijeme všechny vektory $u_1, \ldots, u_m$ nebo nevyměníme všechny vektory $v_1, \ldots, v_n$ za vektory $u_1, \ldots, u_n$. Kdyby bylo $m > n$, vektory $u_{n+1}, \ldots, u_m$ by byly lineární kombinace vektorů $u_1, u_2, \ldots, u_n$ ve sporu s lineární nezávislostí množiny $\{u_1, \ldots, u_m\}$. Takže $m \leq n$ a $[\![v_1, \ldots, v_n]\!] = [\![u_1, \ldots, u_m, v_{i_1}, \ldots, v_{i_{n-m}}]\!]$. □

## 9.3. Báze

**Definice 9.3.1.** *Báze* vektorového prostoru je libovolná uspořádaná lineárně nezávislá množina jeho generátorů.

Obvykle tedy budeme bázi vektorového prostoru zapisovat jako uspořádanou $n$-tici vektorů. Pokud nebude záležet na uspořádání vektorů v bázi, budeme ji někdy zapisovat jen jako množinu vektorů.

**Příklad.** (1) (6) je báze $\mathbb{R}$.

(2) $((1,0),(0,1))$ je báze $\mathbb{R}^2$.

(3) $((1,0,0),(1,1,0),(1,1,1))$ je báze $\mathbb{R}^3$.

(4) Pro každé $i \in \{1, \ldots, n\}$ buď $e_i$ vektor z $\mathbb{R}^n$, který má na $i$-tém místě jedničku a jinde nuly. Potom $(e_1, \ldots, e_n)$ je báze $\mathbb{R}^n$ a nazývá se *kanonická* nebo také *standardní*.

(5) $(x^2, x, 1)$ je báze $\mathbb{R}_2[x]$. □

**Tvrzení 9.3.1.** *Každý konečněrozměrný vektorový prostor má bázi.*

*Důkaz.* Podle definice konečněrozměrný vektorový prostor má konečnou množinu generátorů. Ukážeme, že v ní existuje lineárně nezávislá podmnožina, která generuje tentýž vektorový prostor a je tedy jeho báze. Buď $\{v_1, \ldots, v_n\}$ množina generátorů vektorového prostoru. Z této množiny postupně pro $i = 1, \ldots, n$ vylučme vektor $v_i$, je-li lineární kombinací předchozích. Tedy $v_1$ vyloučíme, pokud $v_1 = 0$. Vektory, které nevyloučíme, označme $v_{i_1}, \ldots, v_{i_m}$. Je-li prvek množiny generátorů lineární kombinací ostatních prvků této množiny, po jeho vyloučení z této množiny zůstane opět množina generátorů stejného vektorového prostoru (ověřte). Proto vektory $v_{i_1}, \ldots, v_{i_m}$ generují tentýž vektorový prostor.

Díky uvedenému postupu žádný z vektorů $v_{i_1}, \ldots, v_{i_m}$ není lineární kombinací předchozích a množina $\{v_{i_1}, \ldots, v_{i_m}\}$ je lineárně nezávislá. □

I nulový prostor $\{0\}$ má bázi. Je jí $\emptyset$, jelikož je lineárně nezávislá a $[\![\emptyset]\!] = \{0\}$.

**Tvrzení 9.3.2.** *Všechny báze jednoho konečněrozměrného vektorového prostoru mají stejný počet prvků.*

*Důkaz.* Buďte $(v_1, \dots, v_n)$ a $(u_1, \dots, u_m)$ báze vektorového prostoru $V$. Jelikož vektory $v_1, \dots, v_n$ generují $V$ a $\{u_1, \dots, u_m\}$ je lineárně nezávislá množina, podle Tvrzení 9.2.5 $n \geq m$. Obdobně dostaneme, že $m \geq n$. Takže $n = m$. □

**Definice 9.3.2.** *Dimenze* vektorového prostoru je počet vektorů (libovolné) jeho báze. Vektorový prostor $V$ dimenze $n$ je *$n$-rozměrný*, zapisujeme $\dim V = n$. Nulový vektorový prostor $\{0\}$ je *0-rozměrný*.

**Příklad.** (1) Vektorový prostor $P^n$ nad polem $P$ je $n$-rozměrný. Jednou z bází je $n$-tice (*kanonická báze*) $((1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1))$.

(2) Vektorový prostor $\mathbb{C}$ nad polem $\mathbb{R}$ je dvojrozměrný. Jednou z bází je dvojice $(1, i)$. Vektorový prostor $\mathbb{C}$ nad polem $\mathbb{C}$ je jednorozměrný, jednu z bází tvoří vektor 1. Vidíme, že dva vektorové prostory mohou mít *různé* dimenze, přestože mají *stejné* množiny vektorů.

(3) Vektorový prostor $\mathbb{C}^n$ nad polem $\mathbb{R}$ je $2n$-rozměrný. Jednou z bází je $2n$-tice

$$\begin{aligned}&((1, 0, \dots, 0), (i, 0, \dots, 0),\\ &(0, 1, 0, \dots, 0), (0, i, 0, \dots, 0),\\ &\dots,\\ &(0, \dots, 0, 1), (0, \dots, 0, i)).\end{aligned}$$

□

**Definice 9.3.3.** (1) *Minimální množina generátorů* vektorového prostoru $V$ je množina generátorů prostoru $V$, jejíž žádná vlastní podmnožina negeneruje $V$.

(2) *Maximální lineárně nezávislá množina vektorů* vektorového prostoru $V$ je lineárně nezávislá množina vektorů z $V$, která není vlastní podmnožinou žádné lineárně nezávislé množiny.

**Tvrzení 9.3.3.** *Buďte $v_1, \dots, v_n \in V$. Pak následující podmínky jsou ekvivalentní:*

*(1) $\{v_1, \dots, v_n\}$ je báze $V$;*
*(2) $\{v_1, \dots, v_n\}$ je minimální množina generátorů $V$;*
*(3) $\{v_1, \dots, v_n\}$ je maximální lineárně nezávislá množina vektorů $V$.*

*Důkaz.* (1) ⇒ (2): Je-li $\{v_1, \dots, v_n\}$ báze, je to množina generátorů a žádný z nich není lineární kombinací ostatních. Tudíž žádná její vlastní podmnožina negeneruje $V$ a $\{v_1, \dots, v_n\}$ je minimální množina generátorů.

(2) ⇒ (1): $\{v_1, \dots, v_n\}$ je množina generátorů. Jelikož je minimální, žádný z jejích vektorů není lineární kombinací ostatních, takže je navíc lineárně nezávislá, čili báze.

(1) ⇒ (3): Je-li $\{v_1, \dots, v_n\}$ báze, je lineárně nezávislá a každý vektor z $V$ je lineární kombinací vektorů báze. Tudíž každá vlastní nadmnožina je lineárně závislá a tato je tedy maximální.

(3) ⇒ (1): Množina $\{v_1, \dots, v_n\}$ je lineárně nezávislá. Jelikož je maximální, po přidání libovolného vektoru z $V$, dostaneme lineárně závislou množinu a ten přidaný vektor (ty původní to být nemohou) je lineární kombinací předchozích, takže $\{v_1, \dots, v_n\}$ je navíc množina generátorů, čili báze. □

Tvrzení poskytuje dvě alternativní definice báze, které se často používají. Má také důležité důsledky.

**Důsledek.** *Buď $V$ $n$-rozměrný vektorový prostor. Pak*

*(1) libovolná jeho $n$-prvková lineárně nezávislá podmnožina tvoří bázi $V$;*
*(2) libovolných $n$ jeho generátorů tvoří bázi $V$.*

*Důkaz.* (1) Prostor $V$ má $n$-prvkovou množinu generátorů, takže podle Tvrzení 9.2.5 každá $n$-prvková lineárně nezávislá podmnožina je maximální, tedy báze.

(2) V prostoru $V$ existuje $n$-prvková lineárně nezávislá množina, takže podle Tvrzení 9.2.5 každá $n$-prvková množina generátorů je minimální, tedy báze. □

**Důsledek.** *Buď $\{v_1, \dots, v_k\}$ lineárně nezávislá podmnožina $n$-rozměrného vektorového prostoru $V$. Pak ji lze doplnit do báze $(v_1, \dots, v_k, v_{k+1}, \dots, v_n)$.*

*Důkaz.* V případě, že $v_1, \dots, v_k$ generují $V$, tvoří bázi. Jinak existuje vektor $v_{k+1} \in V$, který není lineární kombinací vektorů $v_1, \dots, v_k$, načež množina $\{v_1, \dots, v_k, v_{k+1}\}$ je lineárně nezávislá, protože $v_{k+1}$ není lineární kombinací předchozích vektorů.

Po $n - k$ opakováních téže úvahy získáme $n$-prvkovou lineárně nezávislou množinu $\{v_1, \dots, v_k, v_{k+1}, v_{k+2}, \dots, v_n\}$, která je bází podle předchozího důsledku. □

## 9.4. Souřadnice

**Tvrzení 9.4.1.** *Buď $(e_1, \dots, e_n)$ báze vektorového prostoru $V$. Pak pro každé $v \in V$ existuje právě jedna $n$-tice skalárů $(x^1, \dots, x^n)$ taková, že $v = x^1 e_1 + \cdots + x^n e_n$.*

*Důkaz.* Buď $v \in V$. Jelikož $e_1, \dots, e_n$ generují $V$, existují $x^1, \dots, x^n \in P$ takové, že $v = x^1 e_1 + \cdots + x^n e_n$. Jsou-li $y^1, \dots, y^n$ libovolná taková, že $v = y^1 e_1 + \cdots + y^n e_n$, pak

$$\begin{aligned} 0 = v - v &= (x^1 e_1 + \cdots + x^n e_n) - (y^1 e_1 + \cdots + y^n e_n) = \\ &= (x^1 - y^1)e_1 + \cdots + (x^n - y^n)e_n. \end{aligned}$$

Z lineární nezávislosti množiny $\{e_1, \dots, e_n\}$ plyne $x^1 - y^1 = \cdots = x^n - y^n = 0$, a tedy $x^1 = y^1, \dots, x^n = y^n$. □

**Cvičení.** Zformulujte a dokažte obrácené tvrzení. □

**Definice 9.4.1.** Skaláry $x^1, \dots, x^n$ z předchozího tvrzení jsou *souřadnice* vektoru $v$ vzhledem k bázi $(e_1, \dots, e_n)$.

Souřadnice budeme zapisovat buď jako prvky pole $x^1, \dots, x^n$ nebo jako uspořádanou $n$-tici $x = (x^1, \dots, x^n)$ nebo jako matici typu $n \times 1$

$$x = \begin{pmatrix} x^1 \\ x^2 \\ \vdots \\ x^n \end{pmatrix}.$$

**Příklad.** (1) Souřadnice vektoru $2 \in \mathbb{R}$ vzhledem k bázi (6) je $\frac{1}{3}$, protože $2 = \frac{1}{3} \cdot 6$.

(2) Souřadnice vektoru $(x, y, z) \in \mathbb{R}^3$ v kanonické bázi jsou $x, y, z$, protože $(x, y, z) = x \cdot (1, 0, 0) + y \cdot (0, 1, 0) + z \cdot (0, 0, 1)$.

(3) Souřadnice vektoru $(x, y, z) \in \mathbb{R}^3$ v bázi $((1, 0, 0), (1, 1, 0), (1, 1, 1))$ jsou $x-y, y-z, z$, protože $(x, y, z) = (x - y) \cdot (1, 0, 0) + (y - z) \cdot (1, 1, 0) + z \cdot (1, 1, 1)$.

(4) Souřadnice vektoru $z = a + bi \in \mathbb{C}(\mathbb{R})$ vzhledem k bázi $(1, i)$ jsou $a, b$, protože $z = a \cdot 1 + b \cdot i$.

Souřadnice vektoru $z = a + bi \in \mathbb{C}(\mathbb{C})$ vzhledem k bázi $(1)$ je $z$, protože $z = z \cdot 1$. □

Souřadnice vektoru závisí na volbě báze. Jeden vektor má v různých bázích různé souřadnice.

Buďte $V$ vektorový prostor, $v \in V$. Buďte $e = (e_1, \ldots, e_n)$ a $e' = (e'_1, \ldots, e'_n)$ báze $V$, $e$ nazvěme *stará báze*, $e'$ nazvěme *nová báze*. Souřadnice vektoru $v$ vzhledem ke staré bázi označme $x = (x^1, \ldots, x^n)$ a říkejme jim *staré souřadnice*. Souřadnice vektoru $v$ vzhledem k nové bázi označme $x' = (x'^1, \ldots, x'^n)$ a říkejme jim *nové souřadnice*. Platí tedy $v = \sum_i x^i e_i = \sum_i x'^i e'_i$.

**Definice 9.4.2.** Matice, jejíž sloupky jsou tvořeny novými souřadnicemi starých bázových vektorů, je *matice přechodu* od staré báze k nové bázi.

Matici přechodu od báze $\alpha$ k bázi $\beta$ budeme značit $Q_{\alpha\beta}$.

Zobrazení

$$\delta(i,j) = \delta^i_j = \begin{cases} 1 & \text{je-li } i = j, \\ 0 & \text{jinak} \end{cases} \qquad \text{je Kroneckerovo delta.}$$

**Tvrzení 9.4.2.** *Matice přechodu je regulární.*

*Důkaz.* Buďte $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ a $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ báze jednoho vektorového prostoru. Označme $Q_{\alpha\beta} = (a^j_i)$ matici přechodu od báze $\alpha$ k bázi $\beta$ a $Q_{\beta\alpha} = (b^j_i)$ matici přechodu od báze $\beta$ k bázi $\alpha$. Tedy, $(a^1_i, a^2_i, \ldots, a^n_i)$ jsou souřadnice vektoru $\alpha_i$ vzhledem k bázi $\beta$, $(b^1_i, b^2_i, \ldots, b^n_i)$ jsou souřadnice vektoru $\beta_i$ vzhledem k bázi $\alpha$ a

$$\alpha_i = \sum_{j=1}^{n} a^j_i \beta_j \qquad \text{a} \qquad \beta_i = \sum_{j=1}^{n} b^j_i \alpha_j \quad \text{pro každé} \quad i = 1, 2, \ldots, n.$$

Po dosazení dostaneme

$$\begin{aligned} \alpha_i &= \sum_{j=1}^{n} a^j_i \beta_j = \\ &= \sum_{j=1}^{n} a^j_i \left( \sum_{k=1}^{n} b^k_j \alpha_k \right) = \\ &= \sum_{k=1}^{n} \left( \sum_{j=1}^{n} a^j_i b^k_j \right) \alpha_k, \end{aligned}$$

čili

$$\left( \sum_{j=1}^{n} a^j_i b^1_j, \quad \sum_{j=1}^{n} a^j_i b^2_j, \quad \ldots, \quad \sum_{j=1}^{n} a^j_i b^n_j \right)$$

jsou souřadnice vektoru $\alpha_i$ vzhledem k bázi $\alpha$. Tedy,

$$\sum_{j=1}^{n} a^j_i b^k_j = \delta^i_k = \begin{cases} 1 & \text{je-li } i = k, \\ 0 & \text{jinak.} \end{cases}$$

Ovšem

$$\sum_{j=1}^{n} a^j_i b^k_j = (Q_{\beta\alpha} Q_{\alpha\beta})^k_i$$

je v $k$-tém řádku a $i$-tém sloupku součinu $Q_{\beta\alpha}Q_{\alpha\beta}$, takže $Q_{\beta\alpha}Q_{\alpha\beta} = E$, proto matice $Q_{\beta\alpha}$ a $Q_{\alpha\beta}$ jsou vzájemně inverzní a tedy obě regulární. □

**Tvrzení 9.4.3.** *Buď $Q_{ee'}$ matice přechodu od staré báze $e$ k nové bázi $e'$ a buďte $x$ a $x'$ staré a nové souřadnice jednoho vektoru. Potom*

$$x' = Q_{ee'} \cdot x.$$

*Důkaz.* Buď $Q_{ee'} = (q_j^i)$ matice přechodu od staré báze $e$ k nové bázi $e'$. Tedy

$$e_i = \sum_j q_i^j e'_j.$$

Buď $v = x^1 e_1 + \cdots + x^n e_n \in V$. Potom

$$\begin{aligned} v &= x^1 \textstyle\sum_j q_1^j e'_j + \cdots + x^n \sum_j q_n^j e'_j = \\ &= x^1(q_1^1 e'_1 + q_1^2 e'_2 + \cdots + q_1^n e'_n) + \cdots + x^n(q_n^1 e'_1 + q_2^2 e'_2 + \cdots + q_n^n e'_n) = \\ &= \left(\textstyle\sum_j q_j^1 x^j\right) e'_1 + \left(\sum_j q_j^2 x^j\right) e'_2 + \cdots + \left(\sum_j q_j^n x^j\right) e'_n. \end{aligned}$$

Tedy

$$x'^i = \sum_j q_j^i x^j \qquad \text{a} \qquad x' = Q_{ee'} \cdot x.$$ □

**Příklad.** (1) Mějme $\mathbb{R}$, starou bázi $e = (6)$ a novou bázi $e' = (1)$. Pro $v = 2$ je $x = (\frac{1}{3})$ a $x' = (2)$.

Matice přechodu od staré báze $e$ k nové bázi $e'$ je

$$Q_{ee'} = \begin{pmatrix} 6 \end{pmatrix}.$$

A skutečně

$$x' = (6) \cdot (\tfrac{1}{3}) = (2).$$

(2) Mějme $\mathbb{R}^2$, starou bázi $e = ((1,-1),(1,1))$ a novou bázi $e' = ((0,2),(2,1))$. Pro $v = (2,0)$ je $x = (1,1)$ a $x' = (-\frac{1}{2}, 1)$.

Matice přechodu od staré báze $e$ k nové bázi $e'$ je

$$Q_{ee'} = \begin{pmatrix} -\frac{3}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

A skutečně

$$x' = Q_{ee'} \cdot x = \begin{pmatrix} -\frac{3}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} \\ 1 \end{pmatrix}.$$ □

**Tvrzení 9.4.4.** *Buďte $V$ vektorový prostor nad polem $P$, $e = (e_1, \ldots, e_n)$ jeho báze, $u, v \in V$, $p \in P$, $x = (x^1, \ldots, x^n)$ souřadnice vektoru $u$ a $y = (y^1, \ldots, y^n)$ souřadnice vektoru $v$. Pak $x + y = (x^1 + y^1, \ldots, x^n + y^n)$ jsou souřadnice vektoru $u + v$ a $px = (px^1, \ldots, px^n)$ jsou souřadnice vektoru $pu$.*

*Důkaz.* Cvičení. □

## 9.5. Orientace vektorového prostoru

**Definice 9.5.1.** Buďte $\alpha$, $\beta$ báze jednoho vektorového prostoru. Báze $\alpha$ má stejnou *orientaci* jako báze $\beta$, jestliže $\det Q_{\alpha\beta} > 0$.

Relace

$$\alpha \sim \beta \quad \text{právě tehdy, když} \quad \alpha \text{ má stejnou orientaci jako } \beta$$

je relace ekvivalence. (Cvičení.) Tato relace ekvivalence rozděluje množinu všech bází jednoho vektorového prostoru do dvou disjunktních tříd.

**Definice 9.5.2.** Prohlásíme-li některou z bází vektorového prostoru, a společně s ní i každou bázi se stejnou orientací, za *kladnou* (nebo *kladně orientovanou*), určíme tím *orientaci* vektorového prostoru a vektorový prostor je potom *orientovaný*. Báze, které nejsou kladné, jsou *záporné* (nebo *záporně orientované*).

**Příklad.** Kanonická báze prostoru $P^n$ je obvykle uvažována jako kladná. □

## 9.6. Přímý součet vektorových prostorů

**Definice 9.6.1.** Buďte $V_1, \dots, V_n$ vektorové prostory nad polem $P$. Na kartézském součinu $V_1 \times \cdots \times V_n$ zaveďme sčítání a násobení skalárem předpisem

$$(u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n),$$
$$p(u_1, \dots, u_n) = (pu_1, \dots, pu_n)$$

pro libovolné $(u_1, \dots, u_n), (v_1, \dots, v_n) \in V_1 \times \cdots \times V_n$ a $p \in P$.
Na $V_1 \times \cdots \times V_n$ tak dostaneme strukturu vektorového prostoru nad polem $P$, který se značí $V_1 \oplus \cdots \oplus V_n$ a je to *přímý součet* vektorových prostorů $V_1, \dots, V_n$.

**Cvičení.** Ověřte, že $V_1 \oplus \cdots \oplus V_n$ je vektorový prostor. □

**Tvrzení 9.6.1.** *Buďte $V_1, \dots, V_n$ konečněrozměrné vektorové prostory. Pak*

$$\dim(V_1 \oplus \cdots \oplus V_n) = \dim V_1 + \cdots + \dim V_n.$$

*Důkaz.* Pro každé $i$ nechť $(e^i_1, \dots, e^i_{m_i})$ je báze $V_i$. Potom

$$((e^1_1, 0, \dots, 0), \dots, (e^1_{m_1}, 0, \dots, 0),$$
$$(0, e^2_1, 0, \dots, 0), \dots, (0, e^2_{m_2}, 0, \dots, 0),$$
$$\dots,$$
$$(0, \dots, 0, e^n_1), \dots, (0, \dots, 0, e^n_{m_n}))$$

je báze $V_1 \oplus \cdots \oplus V_n$ (cvičení). □

**Příklad.** Buď $V_1 = \mathbb{R}$ a $V_2 = \mathbb{R}^2$. Potom $V_1 \times V_2$ je množina $\mathbb{R} \times \mathbb{R}^2$ uspořádaných dvojic $(x, y)$, kde $x \in \mathbb{R}$ a $y = (y_1, y_2) \in \mathbb{R}^2$, tedy $\mathbb{R} \times \mathbb{R}^2 = \{(x, (y_1, y_2)) \,|\, x \in \mathbb{R}, (y_1, y_2) \in \mathbb{R}^2\}$. Například

$$(1, (2, 3)) + (2, (1, -1)) = (1 + 2, (2, 3) + (1, -1)) = (3, (3, 2)),$$
$$3 \cdot (2, (1, 4)) = (3 \cdot 2, 3 \cdot (1, 4)) = (6, (3, 12)).$$

Buď $e^1 = (1)$ báze $\mathbb{R}$ a buď $e^2 = (e^2_1, e^2_2) = ((1, 0), (0, 1))$ báze $\mathbb{R}^2$. Potom trojice

$$((e^1, 0), (0, e^2_1), (0, e^2_2)) = ((1, (0, 0)), (0, (1, 0)), (0, (0, 1)))$$

je báze $\mathbb{R} \oplus \mathbb{R}^2$ a $\dim(\mathbb{R} \oplus \mathbb{R}^2) = 3 = \dim \mathbb{R} + \dim \mathbb{R}^2 = 1 + 2$. □

## Literatura

[Marvan] M. Marvan, Algebra I a II, Učební texty Matematického ústavu v Opavě, Slezská univerzita v Opavě, dostupné na https://www.slu.cz/math/cz/knihovnaucebnitextymu.