

14. prosince 2022

# Algebra I

2022/2023

Zdeněk Kočan

Tento text je studijní opora k předmětu Algebra I pro studenty bakalářských studijních programů v akademickém roce 2022/2023. 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](mailto:zdenek.kocan@math.slu.cz).

## OBSAH

1	Pole	1
2	Matice	1
2.1	Matice	1
2.2	Operace s maticemi	3
2.3	Elementární úpravy a speciální tvary matic	10
2.4	Inverzní matice	14
2.5	Hodnost matice	17
3	Determinant	23
3.1	Permutace	23
3.2	Determinant	23
3.3	Adjungovaná matice	33
4	Soustavy lineárních rovnic	35
4.1	Soustavy lineárních rovnic a jejich řešení	35
4.2	Gaussova eliminační metoda a obecné řešení	38
4.3	Frobeniova věta	41
4.4	Cramerovo pravidlo	42
4.5	Homogenní soustavy lineárních rovnic	43
4.6	Nehomogenní soustavy lineárních rovnic	45
5	Polynomy	47
5.1	Polynomy, algebraické vlastnosti, dělitelnost	47
5.2	Největší společný dělitel	51
5.3	Ireducibilní polynomy	53
5.4	Kořeny a jejich násobnost	54
5.5	Derivace	55
5.6	Polynomy s reálnými koeficienty	56
6	Grupy	57
6.1	Binární operace	57
6.2	Grupy	59
6.3	Podgrupy	60
6.4	Podgrupy aditivní grupy $\mathbb{Z}$	60
6.5	Faktorové grupy	61
6.6	Zbytkové třídy	63
7	Okruhy a pole	65
8	Uspořádání a svazy	69
8.1	Uspořádané množiny	69
8.2	Svazy	70
8.3	Úplné svazy	72
9	Homomorfismy	75
9.1	Homomorfismy a izomorfismy grup	75
9.2	Homomorfismy a izomorfismy polí	77
9.3	Izotonní zobrazení, homomorfismy a izomorfismy svazů	77

## 1. 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

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

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 dvěma 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 racionálních 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 tématu 7.

## 2. MATICE

### 2.1. Matice

**Definice 2.1.1.** Bud'  $P$  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 sloupcu označujeme  $A_j^i$  a matici zapisujeme obvykle

$$A = \begin{pmatrix} A_1^1 & A_2^1 & \dots & A_n^1 \\ A_1^2 & A_2^2 & \dots & A_n^2 \\ \vdots & \vdots & & \vdots \\ A_1^m & A_2^m & \dots & A_n^m \end{pmatrix}$$

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

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  $A_j^i \in P$  a můžeme ho zapsat právě ve tvaru tabulky, která má v  $i$ -tém řádku a  $j$ -tém sloupcu prvek  $A_j^i$ .

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

$$A_{\circ}^i = (A_1^i \quad A_2^i \quad \dots \quad A_n^i)$$

je  $i$ -tý řádek matice  $A$ ; je to tedy matice typu  $1 \times n$ , někdy ji zapisujeme jako uspořádanou  $n$ -tici  $(A_1^i, A_2^i, \dots, A_n^i) \in P^n$ . Nulový řádek označme  $0_\circ$ . Pro pevně zvolené  $j$

$$A_j^\circ = \begin{pmatrix} A_j^1 \\ A_j^2 \\ \vdots \\ A_j^m \end{pmatrix}$$

je  $j$ -tý sloupek matice  $A$ ; je to tedy matice typu  $m \times 1$ , někdy ji zapisujeme jako uspořádanou  $m$ -tici  $(A_j^1, A_j^2, \dots, A_j^m) \in P^m$  nebo  $(A_j^1 \ A_j^2 \ \dots \ A_j^m)^\top$  nebo  $(A_j^1, A_j^2, \dots, A_j^m)^\top$ . Nulový sloupek označme  $0^\circ$ . To, že matice  $A$  je tvořena řádky  $A_\circ^i$ , resp. sloupky  $A_j^\circ$ , budeme někdy zapisovat

$$A = \begin{pmatrix} A_\circ^1 \\ A_\circ^2 \\ \vdots \\ A_\circ^m \end{pmatrix}, \quad \text{resp. } A = (A_1^\circ \ A_2^\circ \ \dots \ A_n^\circ).$$

Matice  $A = (A_j^i)$  a  $B = (B_j^i)$  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  $A_j^i = B_j^i$ .

**Definice 2.1.2.** Matice  $A = (A_j^i)_{m \times n}$  je

- *čtvercová*, jestliže  $m = n$ ,
- *diagonální*, jestliže je čtvercová a  $A_j^i = 0$  pro  $i \neq j$  (prvky  $A_j^i$  se také nazývají *diagonální* a tvoří *hlavní diagonálu*),
- *jednotková*, jestliže je diagonální a  $A_j^i = 1$  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  $A_j^i = 0$  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  $0$  označuje 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  $\text{gl}(n, P)$ .

**Příklad.** (1)

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

(2)

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

(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,  $\begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 2 & 1 \end{pmatrix}$  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)

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

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

## 2.2. Operace s maticemi

### 2.2.1. Součet matic a násobek matice

**Definice 2.2.1.** 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  $i \in \{1, 2, \dots, m\}$ ,  $j \in \{1, 2, \dots, n\}$

$$(A + B)_j^i = A_j^i + B_j^i.$$

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

**Definice 2.2.2.** 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  $i \in \{1, 2, \dots, m\}$ ,  $j \in \{1, 2, \dots, n\}$

$$(cA)_j^i = cA_j^i.$$

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

**Příklad.** Pro

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

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

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

**Cvičení.** Spočítejte

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

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

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

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

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

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

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

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} -1 & -2 \\ -3 & -4 \end{pmatrix}. \quad \triangleright$$

**Tvrzení 2.2.1.** Nechť  $A, B, C$  jsou matice stejného typu nad polem  $P$  a  $c, k \in P$ . Pak

$$(1) A + B = B + A,$$

$$(5) 1A = A,$$

$$(2) A + (B + C) = (A + B) + C,$$

$$(6) c(A + B) = cA + cB,$$

$$(3) A + 0 = A,$$

$$(7) (c + k)A = cA + kA,$$

$$(4) A + (-A) = 0,$$

$$(8) c(kA) = (ck)A.$$

*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  $i \in \{1, 2, \dots, m\}$  a  $j \in \{1, 2, \dots, n\}$  prvek v  $i$ -tém řádku a  $j$ -tém sloupcu matice  $A+(B+C)$  je

$$(A+(B+C))_j^i = A_j^i + (B+C)_j^i = \quad (\text{podle definice součtu matic})$$

$$= A_j^i + (B_j^i + C_j^i) = \quad (\text{podle definice součtu matic})$$

$$= (A_j^i + B_j^i) + C_j^i = \quad (\text{díky asociativitě sčítání v poli})$$

$$= (A+B)_j^i + C_j^i = \quad (\text{podle definice součtu matic})$$

$$= ((A+B)+C)_j^i, \quad (\text{podle definice součtu matic})$$

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

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

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.  $\square$

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

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

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.

### 2.2.2. Součín

**Definice 2.2.4.** Buďte  $A$  matice typu  $m \times n$  a  $B$  matice typu  $n \times p$  nad polem  $P$ . *Součín* 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  $i \in \{1, 2, \dots, m\}$ ,  $j \in \{1, 2, \dots, p\}$

$$(AB)_j^i = A_1^i B_j^1 + A_2^i B_j^2 + \dots + A_n^i B_j^n = \sum_{k=1}^n A_k^i B_j^k.$$

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

$$\begin{aligned} AB &= \begin{pmatrix} A_1^1 B_1^1 + A_2^1 B_1^2 + \dots + A_n^1 B_1^n & \dots & A_1^1 B_p^1 + A_2^1 B_p^2 + \dots + A_n^1 B_p^n \\ A_1^2 B_1^1 + A_2^2 B_1^2 + \dots + A_n^2 B_1^n & \dots & A_1^2 B_p^1 + A_2^2 B_p^2 + \dots + A_n^2 B_p^n \\ \vdots & & \vdots \\ A_1^m B_1^1 + A_2^m B_1^2 + \dots + A_n^m B_1^n & \dots & A_1^m B_p^1 + A_2^m B_p^2 + \dots + A_n^m B_p^n \end{pmatrix} = \\ &= \begin{pmatrix} A_1^1 B_{\circ}^1 + A_2^1 B_{\circ}^2 + \dots + A_n^1 B_{\circ}^n \\ A_1^2 B_{\circ}^1 + A_2^2 B_{\circ}^2 + \dots + A_n^2 B_{\circ}^n \\ \vdots \\ A_1^m B_{\circ}^1 + A_2^m B_{\circ}^2 + \dots + A_n^m B_{\circ}^n \end{pmatrix} = \\ &= (B_1^1 A_{\circ}^1 + B_1^2 A_{\circ}^2 + \dots + B_1^n A_{\circ}^n \quad \dots \quad B_p^1 A_{\circ}^1 + B_p^2 A_{\circ}^2 + \dots + B_p^n A_{\circ}^n). \end{aligned}$$

Čili, první řádek matice  $AB$  získáme tak, že vezmeme  $A_1^1$ -násobek řádku  $B_1^1$ ,  $A_2^1$ -násobek řádku  $B_2^1$ , ...,  $A_n^1$ -násobek řádku  $B_n^1$  a všechny tyto násobky sečteme. Je to tedy lineární kombinace řádků matice  $B$  s koeficienty z prvního řádku matice  $A$ .

Obdobně získáme ostatní řádky matice  $AB$ . Obecně,  $i$ -tý řádek matice  $AB$  získáme tak, že pro každé  $k \in \{1, 2, \dots, n\}$  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  $A$ .

Analogicky, první sloupek matice  $AB$  získáme tak, že vezmeme  $B_1^1$ -násobek sloupku  $A_1^1$ ,  $B_2^1$ -násobek sloupku  $A_2^1$ , ...,  $B_n^1$ -násobek sloupku  $A_n^1$  a všechny tyto násobky sečteme. Je to tedy lineární kombinace sloupků matice  $A$  s koeficienty z prvního sloupku matice  $B$ .

Obdobně získáme ostatní sloupky matice  $AB$ . Obecně,  $j$ -tý sloupek matice  $AB$  získáme tak, že pro každé  $k \in \{1, 2, \dots, n\}$  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  $B$ .

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

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

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

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

(2) Pro

$$A = (1 \ 2), B = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \text{ je}$$

$$AB = (1 \cdot 0 + 2 \cdot 3) = (6),$$

$$BA = \begin{pmatrix} 0 \cdot 1 & 0 \cdot 2 \\ 3 \cdot 1 & 3 \cdot 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 3 & 6 \end{pmatrix}.$$

(3) Pro

$$A = (1 \ 2), B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ je } AB = (2 \ 1), BA \text{ neexistuje.} \quad \blacksquare$$



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

**Cvičení.** Spočtěte

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

▷

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

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

**Tvrzení 2.2.2.** *Nechť  $A, B, C$  jsou matice nad polem  $P$  takové, že níže uvedené operace jsou definovány, a  $c \in P$ . Pak platí*

$$(1) A(BC) = (AB)C,$$

$$(4) (A + B)C = AC + BC,$$

$$(2) AE = EA = A,$$

$$(5) c(AB) = (cA)B = A(cB).$$

$$(3) A(B + C) = AB + AC,$$

*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  $m \times q$ .

$$\begin{aligned}
(A(BC))_j^i &= \sum_{k=1}^n A_k^i (BC)_j^k = && \text{(podle definice součinu matic)} \\
&= \sum_{k=1}^n A_k^i \sum_{l=1}^p (B_l^k C_j^l) = && \text{(podle definice součinu matic)} \\
&= \sum_{k=1}^n \sum_{l=1}^p A_k^i (B_l^k C_j^l) = && \text{(díky distributivnímu zákonu v poli)} \\
&= \sum_{k=1}^n \sum_{l=1}^p (A_k^i B_l^k) C_j^l = && \text{(díky asociativitě součinu v poli)} \\
&= \sum_{l=1}^p \sum_{k=1}^n (A_k^i B_l^k) C_j^l = && \text{(díky komutativitě součtu v poli)} \\
&= \sum_{l=1}^p (AB)_l^i C_j^l = && \text{(podle definice součinu matic)} \\
&= ((AB)C)_j^i. && \text{(podle definice součinu matic)}
\end{aligned}$$

(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  $i \in \{1, 2, \dots, m\}$  a  $j \in \{1, 2, \dots, p\}$  platí

$$\begin{aligned}
(A(B + C))_j^i &= \sum_{k=1}^n A_k^i (B + C)_j^k = && \text{(podle definice součinu matic)} \\
&= \sum_{k=1}^n A_k^i (B_j^k + C_j^k) = && \text{(podle definice součtu matic)} \\
&= \sum_{k=1}^n (A_k^i B_j^k + A_k^i C_j^k) = && \text{(díky distributivnímu zákonu v poli)} \\
&= \sum_{k=1}^n A_k^i B_j^k + \sum_{k=1}^n A_k^i C_j^k = && \text{(díky vlastnostem sčítání v poli)} \\
&= (AB)_j^i + (AC)_j^i = && \text{(podle definice součinu matic)} \\
&= (AB + AC)_j^i. && \text{(podle definice součtu matic)} \quad \square
\end{aligned}$$

### 2.2.3. Transponování

**Definice 2.2.5.** *Transponovaná matice k matici  $A$  typu  $m \times n$  je matice  $A^T$  typu  $n \times m$ , kde  $(A^T)_j^i = A_i^j$  pro všechna  $i, j$ .*

**Příklad.**

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

**Tvrzení 2.2.3.** *Nechť  $A, B$  jsou matice nad polem  $P$  takové, že níže uvedené operace jsou definovány, a  $c \in P$ . Pak platí*

$$\begin{aligned} (1) \quad A &= (A^T)^T, & (3) \quad (cA)^T &= cA^T, \\ (2) \quad (A+B)^T &= A^T + B^T, & (4) \quad (AB)^T &= B^T A^T. \end{aligned}$$

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

$$((A^T)^T)_j^i = (A^T)_i^j = A_j^i.$$

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

$$\begin{aligned} ((AB)^T)_j^i &= (AB)_i^j = \sum_{k=1}^n A_k^j B_i^k = \sum_{k=1}^n B_i^k A_k^j = \sum_{k=1}^n (B^T)_k^i (A^T)_j^k = \\ &= (B^T A^T)_j^i. \end{aligned}$$

Ostatní body jsou ponechány jako cvičení. □

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

## 2.3. Elementární úpravy a speciální tvary matic

### 2.3.1. Elementární úpravy

**Definice 2.3.1.** 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.** Provedte 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 změňme  $i$ -tý řádek na  $(A_1^i + cA_1^j \quad A_2^i + cA_2^j \quad \dots \quad A_n^i + cA_n^j)$  a ostatní řádky zůstanou beze změny.

Po vynásobení  $i$ -tého řádku prvkem  $c \in P$   $i$ -tý řádek bude  $(cA_1^i \quad cA_2^i \quad \dots \quad cA_n^i)$  a ostatní řádky zůstanou beze změny.

Po vzájemné výměně  $i$ -tého řádku a  $j$ -tého řádku  $i$ -tý řádek bude  $(A_1^j \quad A_2^j \quad \dots \quad A_n^j)$ ,  $j$ -tý řádek bude  $(A_1^i \quad A_2^i \quad \dots \quad A_n^i)$  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

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

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

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

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

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

**Definice 2.3.2.** 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.**

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

**Tvrzení 2.3.1.** *Ekvivalence matic je relace ekvivalence na množině všech matic stejného typu nad stejným polem.*

*Důkaz.* Cvičení. □

### 2.3.2. Schodovitý, Gaussův–Jordanův a Gaussův kanonický tvar matic

Připomeňme si definice z podkapitoly 2.1.

**Definice 2.3.3.** 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 2.3.4.** 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 sloupcu, ve kterém je první nenulový prvek nějakého řádku, ostatní prvky jsou 0.

**Definice 2.3.5.** *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 v Gaussově–Jordanově tvaru. □

**Definice 2.3.6.** 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 2.3.2.** 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.  $\square$

**Definice 2.3.7.** 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 vydělíme jeho prvním nenulovým prvkem.
- (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.

**Tvrzení 2.3.3.** 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.  $\square$

**Tvrzení 2.3.4.** 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.  $\square$

### 2.3.3. Elementární matice

**Definice 2.3.8.** *Elementární matice* jsou:

(1) pro  $i \neq j$

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

(2) pro  $c \neq 0$

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

(3) pro  $i \neq j$

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

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  $(E^{i,j}(c))_j^i = c$ , zatímco  $E_j^i = 0$ .

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 2.3.5.** *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 2.2.4 součinu matic. Analogicky pro sloupkové úpravy a násobení zprava. Cvičení.  $\square$

**Příklad.** Buďte

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

Potom

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

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

$$B_3 = E^{1,3} \cdot A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} A_{\circ}^3 \\ A_{\circ}^2 \\ A_{\circ}^1 \end{pmatrix}. \quad \blacksquare$$

**Lemma 2.3.6.** *Transponované matice k elementárním maticím jsou elementární matice.*

*Důkaz.* Cvičení. □

## 2.4. Inverzní matice

**Definice 2.4.1.** 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)

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

(3)

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

(4)

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

(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

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

**Tvrzení 2.4.1.** *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 2.4.2.** *Nechť  $A, A_1, \dots, A_n$  jsou invertibilní matice stejného typu. Potom*

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

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

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

**Tvrzení 2.4.3.** *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  $G = Q_k \dots Q_1 A$ , kde  $Q_1, \dots, Q_k$  jsou elementární matice příslušné provedeným úpravám. Pak  $A = Q_1^{-1} \dots Q_k^{-1} G$  a  $AB = Q_1^{-1} \dots Q_k^{-1} GB = E$ . 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  $Q_1^{-1}, \dots, Q_k^{-1}$ ) převést na jednotkovou matici (cvičení). Jelikož  $G$  je v Gaussově–Jordanově tvaru a nemá nulový řádek,  $G = E$ . Pak  $A = Q_1^{-1} \dots Q_k^{-1}$  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 kritérium invertibility.

**Tvrzení 2.4.4.** *Matice je invertibilní právě tehdy, když je řádkově ekvivalentní s jednotkovou maticí.*

*Důkaz.* „ $\Rightarrow$ “ Nechť  $A$  je invertibilní matice. Řádkovými elementárními úpravami ji převedme na Gaussův–Jordanův tvar  $G$ , tedy  $G = Q_k \dots Q_1 A$ , kde  $Q_1, \dots, Q_k$  jsou elementární matice příslušné provedeným úpravám. Každá z matic  $Q_1, \dots, Q_k, A$  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.

„ $\Leftarrow$ “ Předpokládejme, že matice  $A$  je řádkově ekvivalentní s jednotkovou maticí  $E$ , tedy  $Q_k \dots Q_1 A = E$ , kde  $Q_1, \dots, Q_k$  jsou vhodné elementární matice. Označme si  $Q = Q_k \dots Q_2 Q_1$ , tedy  $QA = E$ . Podle Tvrzení 2.4.3 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  $n \times 2n$

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

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

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

**Příklad.** Hledejme inverzní matici k matici

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

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

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

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

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

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

## 2.5. Hodnost matice

### 2.5.1. Lineární nezávislost

Stejně jako v případě lineární kombinace v Definici 2.2.3 následující definice a tvrzení formulujeme pouze pro řádky matice, ale vše lze obdobně formulovat pro sloupky, uspořádané  $n$ -tice a matice.

**Definice 2.5.1.** Množina řádků  $\{A_{\circ}^{i_1}, A_{\circ}^{i_2}, \dots, A_{\circ}^{i_k}\}$  je *lineárně nezávislá*, jestliže pro libovolné  $c_1, c_2, \dots, c_k \in P$  z rovnosti

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

tj. nulový řádek získáme jedinečně takovou lineární kombinací daných řádků, ve které jsou všechny koeficienty rovny nule.

Množina řádků  $\{A_{\circ}^{i_1}, A_{\circ}^{i_2}, \dots, A_{\circ}^{i_k}\}$  je *lineárně závislá*, jestliže není lineárně nezávislá. Tedy, existují  $c_1, c_2, \dots, c_k \in P$  taková, že aspoň jedno z nich je nenulové a přitom

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

**Tvrzení 2.5.1.** Množina řádků je lineárně závislá právě tehdy, když aspoň jeden z nich je lineární kombinací ostatních.

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

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

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

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

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

Potom

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

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

**Příklad.** Mějme

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

Nechť

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

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 jedině, 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

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

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. ■

## 2.5.2. Hodnost matice

**Definice 2.5.2.** *Hodnost* matice je maximální počet prvků lineárně nezávislých množin jejích řádků. Hodnost matice  $A$  značíme  $\text{rank } A$ .

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

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

**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.** Spočítejte hodnosti matic

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

(6)

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

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

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

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

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

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

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

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

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

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

▷

**Tvrzení 2.5.2.** 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  $\text{rank } A \geq p$ . 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  $\text{rank } A = p$ . □

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 2.5.3.** Buďte  $A_{\circ}^1, A_{\circ}^2, \dots, A_{\circ}^m$  řádky. Necht'  $B_{\circ}^1, B_{\circ}^2, \dots, B_{\circ}^m$  jsou řádky, které z řádků  $A_{\circ}^1, A_{\circ}^2, \dots, A_{\circ}^m$  vzniknou provedením jedné řádkové nebo sloupkové elementární úpravy. Potom množina řádků  $\{A_{\circ}^1, A_{\circ}^2, \dots, A_{\circ}^m\}$  je lineárně nezávislá právě tehdy, když množina řádků  $\{B_{\circ}^1, B_{\circ}^2, \dots, B_{\circ}^m\}$  je lineárně nezávislá.

*Důkaz.* (1) Necht' došlo k přičtení  $c$ -násobku  $j$ -tého řádku k  $i$ -tému řádku, kde  $i \neq j$ . Tedy,  $B_{\circ}^i = A_{\circ}^i + cA_{\circ}^j$  a  $B_{\circ}^k = A_{\circ}^k$  pro  $k \neq i$ .

Předpokládejme, že  $\{A_{\circ}^1, A_{\circ}^2, \dots, A_{\circ}^m\}$  je lineárně nezávislá. Buďte  $c_1, \dots, c_m \in P$  takové, že  $c_1 B_{\circ}^1 + \dots + c_m B_{\circ}^m = 0_{\circ}$ . Pak

$$\begin{aligned} 0_{\circ} &= c_1 B_{\circ}^1 + \dots + c_m B_{\circ}^m = \\ &= c_1 A_{\circ}^1 + \dots + c_i (A_{\circ}^i + cA_{\circ}^j) + \dots + c_j A_{\circ}^j + \dots + c_m A_{\circ}^m = \\ &= c_1 A_{\circ}^1 + \dots + c_i A_{\circ}^i + \dots + (c_j + cc_i) A_{\circ}^j + \dots + c_m A_{\circ}^m. \end{aligned}$$

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

Opačná implikace vyplývá z právě dokázané, neboť řádky  $A_o^1, A_o^2, \dots, A_o^m$  vzniknou z řádků  $B_o^1, B_o^2, \dots, B_o^m$  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  $B_i^k = A_i^k + cA_j^k$  a  $B_l^k = A_l^k$  pro  $l \neq i$ . Tedy  $B_o^k = (A_1^k \ \dots \ A_i^k + cA_j^k \ \dots \ A_j^k \ \dots \ A_n^k)$ .

Předpokládejme, že  $\{A_o^1, A_o^2, \dots, A_o^m\}$  je lineárně nezávislá. Buďte  $c_1, \dots, c_m \in P$  takové, že  $c_1B_o^1 + \dots + c_mB_o^m = 0_o$ . Takže

$$\begin{aligned} c_1B_o^1 + \dots + c_mB_o^m &= \\ &= (\sum_k c_k A_1^k \ \dots \ \sum_k c_k (A_i^k + cA_j^k) \ \dots \ \sum_k c_k A_j^k \ \dots \ \sum_k c_k A_n^k) = \\ &= (\sum_k c_k A_1^k \ \dots \ \sum_k c_k A_i^k + c \sum_k c_k A_j^k \ \dots \ \sum_k c_k A_j^k \ \dots \ \sum_k c_k A_n^k) = \\ &= (0 \ \dots \ 0 \ \dots \ 0 \ \dots \ 0) \end{aligned}$$

a z toho dostaneme

$$\sum_k c_k A_1^k = \dots = \sum_k c_k A_i^k = \dots = \sum_k c_k A_j^k = \dots = \sum_k c_k A_n^k = 0.$$

Pak

$$\begin{aligned} (\sum_k c_k A_1^k \ \sum_k c_k A_2^k \ \dots \ \sum_k c_k A_n^k) &= \sum_k c_k (A_1^k \ A_2^k \ \dots \ A_n^k) = \\ &= \sum_k c_k A_o^k = c_1 A_o^1 + \dots + c_m A_o^m = 0_o \end{aligned}$$

a z lineární nezávislosti množiny  $\{A_o^1, A_o^2, \dots, A_o^m\}$  dostaneme  $c_1 = c_2 = \dots = c_m = 0$ . Množina  $\{B_o^1, B_o^2, \dots, B_o^m\}$  je tedy lineárně nezávislá.

Opačná implikace vyplývá z právě dokázané, neboť řádky  $A_o^1, A_o^2, \dots, A_o^m$  vzniknou z řádků  $B_o^1, B_o^2, \dots, B_o^m$  inverzní úpravou, která je stejného typu.

Pro ostatní úpravy je důkaz obdobný a ponecháme ho jako cvičení.  $\square$

**Důsledek.** (1) *Hodnota matice je rovna hodnotě matice z ní vzniklé provedením elementární úpravy.*

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

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

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

(5) *Ekvivalentní matice mají stejnou hodnotu.*

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

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

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

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

**Příklad.** Spočítejme hodnotu 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  $\text{rank } A = 3$ . ■

**Příklad.** Spočítejme hodnotu 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  $\text{rank } A = 2$ . ■

**Definice 2.5.3.** Čtvercová matice je *regulární*, jestliže její hodnota 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 2.5.4.** 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 hodnotu.

(5) Vynásobení regulární maticí zprava nemění hodnotu.

**Tvrzení 2.5.5.** Buďte  $A, B$  čtvercové matice stejného typu. Obě matice  $A, B$  jsou regulární právě tehdy, když matice  $AB$  je regulární.

*Důkaz.* „ $\Rightarrow$ “ Tato implikace je součástí předchozího Důsledku.

„ $\Leftarrow$ “ 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  $Q_1, \dots, Q_k$  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 hodnotu, je také singulární.

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

**Tvrzení 2.5.6.** Buďte  $A$  matice typu  $m \times n$  a  $B$  matice typu  $n \times p$ . Potom  $\text{rank } AB \leq \min\{\text{rank } A, \text{rank } B\}$ .

*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  $S_B^T$  je ve schodovitém tvaru.

Potom  $\text{rank } AB = \text{rank } Q_1^{-1} \cdots Q_k^{-1} S_A S_B P_l^{-1} \cdots P_1^{-1} = \text{rank } S_A S_B$ , 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  $\text{rank } S_A S_B \leq \text{rank } S_A = \text{rank } A$  a  $\text{rank } S_A S_B \leq \text{rank } S_B = \text{rank } B$ . □

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





### 3. DETERMINANT

#### 3.1. Permutace

**Definice 3.1.1.** Buď  $M$  konečná množina. *Permutace* na množině  $M$  je bijekce  $M \rightarrow M$ .

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

**Definice 3.1.2.** *Transpozice* je permutace, při níž se vzájemně vymění dva prvky a ostatní se nezmění.

**Tvrzení 3.1.1.** *Každá permutace je složením konečně mnoha transpozic.*

Nechť  $I_n = \{1, 2, \dots, n\}$ . 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  $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ .

**Definice 3.1.3.** 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  $\text{inv } \sigma$ . Je zřejmé, že  $\text{inv } \sigma = \text{inv } \sigma^{-1}$ .

**Definice 3.1.4.** *Signum (znaménko)* permutace  $\sigma \in S_n$  je  $\text{sgn } \sigma = (-1)^{\text{inv } \sigma}$ . Permutace s  $\text{sgn } \sigma = 1$  je *sudá*, permutace s  $\text{sgn } \sigma = -1$  je *lichá*.

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

**Tvrzení 3.1.2.** *Budte  $\rho, \sigma \in S_n$ . Pak  $\text{sgn}(\pi \circ \rho) = \text{sgn } \pi \cdot \text{sgn } \rho$ .*

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

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

#### 3.2. Determinant

##### 3.2.1. Definice a determinanty některých typů matic

**Definice 3.2.1.** Buď  $A$  matice typu  $n \times n$  nad polem  $P$ . *Determinant* matice  $A$  je

$$\det A = \sum_{\sigma \in S_n} \text{sgn } \sigma \cdot A_{\sigma_1}^1 A_{\sigma_2}^2 \cdots A_{\sigma_n}^n \in P.$$

Číslo  $n$  je *řád* determinantu.

Pro determinant matice  $A$  se používá značení

$$\det A = |A| = \det \begin{pmatrix} A_1^1 & A_2^1 & \cdots & A_n^1 \\ A_1^2 & A_2^2 & \cdots & A_n^2 \\ \vdots & \vdots & & \vdots \\ A_1^n & A_2^n & \cdots & A_n^n \end{pmatrix} = \begin{vmatrix} A_1^1 & A_2^1 & \cdots & A_n^1 \\ A_1^2 & A_2^2 & \cdots & A_n^2 \\ \vdots & \vdots & & \vdots \\ A_1^n & A_2^n & \cdots & A_n^n \end{vmatrix}.$$

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  $A_{\sigma_1}^1 \cdot A_{\sigma_2}^2 \cdots A_{\sigma_n}^n$  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,  $I_1 = \{1\}$ ,  $S_1 = \{\text{id}: \{1\} \rightarrow \{1\}\}$  a  $\text{sgn id} = 1$ . Pro matici  $A = (a)$  je  $\det A = \text{sgn id} \cdot A_{\text{id}_1}^1 = 1 \cdot A_1^1 = a$ .

(2) Nechť  $n = 2$ . Tedy,  $I_2 = \{1, 2\}$ ,  $S_2 = \{\text{id}, \tau\}$ , kde  $\text{id} = (1, 2)$  a  $\tau = (2, 1)$  (viz zápis permutace na  $I_n$ ),  $\text{sgn id} = 1$  a  $\text{sgn } \tau = -1$ . Pro matici

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

je  $\det A = \text{sgn id} \cdot A_{\text{id}_1}^1 A_{\text{id}_2}^2 + \text{sgn } \tau \cdot A_{\tau_1}^1 A_{\tau_2}^2 = 1 \cdot A_1^1 A_2^2 + (-1) \cdot A_2^1 A_1^2 = ad - bc$ . Vzorec pro výpočet determinantu matice druhého řádu je možno odvodit z následujícího obrázku:

$$\begin{array}{c} \oplus \quad \ominus \\ \downarrow \quad \downarrow \\ \left| \begin{array}{cc} A_1^1 & A_2^1 \\ A_1^2 & A_2^2 \end{array} \right| \\ \swarrow \quad \searrow \\ \ominus \quad \oplus \end{array} = A_1^1 A_2^2 - A_2^1 A_1^2$$

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

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

je

$$\begin{aligned} \det A &= \text{sgn id} \cdot A_{\text{id}_1}^1 A_{\text{id}_2}^2 A_{\text{id}_3}^3 + \text{sgn } \sigma_1 \cdot A_{\sigma_1(1)}^1 A_{\sigma_1(2)}^2 A_{\sigma_1(3)}^3 + \\ &\quad + \text{sgn } \sigma_2 \cdot A_{\sigma_2(1)}^1 A_{\sigma_2(2)}^2 A_{\sigma_2(3)}^3 + \text{sgn } \tau_1 \cdot A_{\tau_1(1)}^1 A_{\tau_1(2)}^2 A_{\tau_1(3)}^3 + \\ &\quad + \text{sgn } \tau_2 \cdot A_{\tau_2(1)}^1 A_{\tau_2(2)}^2 A_{\tau_2(3)}^3 + \text{sgn } \tau_3 \cdot A_{\tau_3(1)}^1 A_{\tau_3(2)}^2 A_{\tau_3(3)}^3 = \\ &= 1 \cdot A_1^1 A_2^2 A_3^3 + 1 \cdot A_2^1 A_3^2 A_1^3 + 1 \cdot A_3^1 A_1^2 A_2^3 + \\ &\quad + (-1) \cdot A_1^1 A_3^2 A_2^3 + (-1) \cdot A_3^1 A_2^2 A_1^3 + (-1) \cdot A_2^1 A_1^2 A_3^3 = \\ &= aei + bfg + cdh - afh - ceg - bdi. \end{aligned}$$

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

$$\begin{array}{c} \oplus \quad \oplus \quad \oplus \\ \downarrow \quad \downarrow \quad \downarrow \\ \left| \begin{array}{ccc} A_1^1 & A_2^1 & A_3^1 \\ A_1^2 & A_2^2 & A_3^2 \\ A_1^3 & A_2^3 & A_3^3 \end{array} \right| \\ \swarrow \quad \searrow \quad \swarrow \quad \searrow \\ \oplus \quad \ominus \quad \oplus \quad \ominus \quad \oplus \quad \ominus \\ \downarrow \quad \downarrow \quad \downarrow \\ A_1^1 \quad A_2^1 \quad A_3^1 \\ \swarrow \quad \searrow \\ A_1^2 \quad A_2^2 \quad A_3^2 \end{array} = A_1^1 A_2^2 A_3^3 + A_2^1 A_3^2 A_1^3 + A_3^1 A_1^2 A_2^3 - \\ - A_1^1 A_3^2 A_2^3 - A_3^1 A_2^2 A_1^3 - A_2^1 A_1^2 A_3^3$$

(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{array}{cccc}
 \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \\
 \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} \\
 \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} & \begin{pmatrix} 2 & 6 \\ 2 & 4 \end{pmatrix} & \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} \\
 \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 5 & 6 & 7 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 2 \\ 5 & 6 & 7 \end{pmatrix} & \begin{pmatrix} 2 & 4 & 6 \\ 3 & 4 & 5 \\ 5 & 6 & 7 \end{pmatrix} & \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} & \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 3 \\ 1 & 0 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 3 & 4 \end{pmatrix} & \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} & \begin{pmatrix} 1 & 2 & 1 \\ 3 & 4 & 2 \\ 0 & 0 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix} & \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} & \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 4 & 5 & 6 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 0 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix} & \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} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & -4 & 3 \end{pmatrix} & \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} & \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 4 & 5 & 6 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 4 & 5 & 6 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 4 & 5 & 6 \end{pmatrix} \quad \triangleright
 \end{array}$$

**Tvrzení 3.2.1.** *Determinant matice s nulovým řádkem nebo nulovým sloupcem je roven nule.*

*Důkaz.* Buď  $A$  matice typu  $n \times n$  s nulovým řádkem nebo nulovým sloupcem. Pro každé  $\sigma \in S_n$  je v součinu  $A_{\sigma_1}^1 A_{\sigma_2}^2 \cdots A_{\sigma_n}^n$  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.  $\square$

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

$$\begin{vmatrix} A_1^1 & \dots & A_n^1 \\ \dots & \dots & \dots \\ A_1^i & \dots & A_n^i \\ \dots & \dots & \dots \\ A_1^n & \dots & A_n^n \end{vmatrix} + \begin{vmatrix} A_1^1 & \dots & A_n^1 \\ \dots & \dots & \dots \\ B_1^i & \dots & B_n^i \\ \dots & \dots & \dots \\ A_1^n & \dots & A_n^n \end{vmatrix} = \begin{vmatrix} A_1^1 & \dots & A_n^1 \\ \dots & \dots & \dots \\ A_1^i + B_1^i & \dots & A_n^i + B_n^i \\ \dots & \dots & \dots \\ A_1^n & \dots & A_n^n \end{vmatrix}. \quad \triangleright$$

**Příklad.**

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

**Definice 3.2.2.** Čtvercová matice je (*horní* resp. *dolní*) *trojúhelníková* (nebo v (*horním* resp. *dolním*) *trojúhelníkovém tvaru*), jestliže pod resp. nad diagonálou má jen nuly, tedy  $A_j^i = 0$  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 3.2.2.** *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  $A_{\sigma_i}^i$  je pod diagonálou, tedy  $A_{\sigma_i}^i = 0$  a také  $\text{sgn } \sigma \cdot A_{\sigma_1}^1 \cdots A_{\sigma_i}^i \cdots A_{\sigma_n}^n = 0$ . Jediná permutace  $\sigma$  taková, že  $\sigma_i \geq i$  pro každé  $i$ , je identita. Jelikož  $\text{sgn id} = 1$ ,  $\det A = A_1^1 A_2^2 \cdots A_n^n$ .

Pro dolní trojúhelníkové matice je důkaz analogický.  $\square$

**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.**

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

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

$$\det E^{i,j} = (-1) \cdot (E^{i,j})_{\tau_1}^1 \cdots (E^{i,j})_{\tau_n}^n = -1. \quad \blacksquare$$

**Tvrzení 3.2.3.** *Pro každou čtvercovou matici  $A$  platí  $\det A^T = \det A$ .*

*Důkaz.* Činitele v součinu  $A_1^{\sigma_1} \cdots A_i^{\sigma_i} \cdots A_n^{\sigma_n}$  můžeme uspořádat podle vzrůstajícího řádkového indexu  $A_{\sigma_1}^1 \cdots A_{\sigma_i}^i \cdots A_{\sigma_n}^n$ , protože  $\sigma_i^{-1}$ -tý činitel v původním součinu

je  $A_{\sigma_i^{-1}}^{\sigma_i^{-1}} = A_{\sigma_i^{-1}}^i$ . Potom

$$\begin{aligned} \det A^\top &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot (A^\top)_{\sigma_1}^1 \cdots (A^\top)_{\sigma_i}^i \cdots (A^\top)_{\sigma_n}^n = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot A_1^{\sigma_1} \cdots A_i^{\sigma_i} \cdots A_n^{\sigma_n} = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot A_{\sigma_1^{-1}}^1 \cdots A_{\sigma_i^{-1}}^i \cdots A_{\sigma_n^{-1}}^n = && \text{(přeuspořádání)} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma^{-1} \cdot A_{\sigma_1^{-1}}^1 \cdots A_{\sigma_i^{-1}}^i \cdots A_{\sigma_n^{-1}}^n = && (\operatorname{sgn} \sigma^{-1} = \operatorname{sgn} \sigma) \\ &= \det A, \end{aligned}$$

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

**Tvrzení 3.2.4.** *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  $A_k^i = A_k^j$  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

$$\begin{aligned} \operatorname{sgn} \sigma' \cdot A_{\sigma'_1}^1 \cdots A_{\sigma'_i}^i \cdots A_{\sigma'_j}^j \cdots A_{\sigma'_n}^n &= \\ &= -\operatorname{sgn} \sigma \cdot A_{\sigma_1}^1 \cdots A_{\sigma_j}^i \cdots A_{\sigma_i}^j \cdots A_{\sigma_n}^n = \\ &= -\operatorname{sgn} \sigma \cdot A_{\sigma_1}^1 \cdots A_{\sigma_i}^i \cdots A_{\sigma_j}^j \cdots A_{\sigma_n}^n, && (A_{\sigma_j}^i = A_{\sigma_j}^j \text{ a } A_{\sigma_i}^j = A_{\sigma_i}^i) \end{aligned}$$

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. □

### 3.2.2. Elementární úpravy

**Tvrzení 3.2.5.** (1) *Přičtením násobku jednoho řádku, resp. sloupku k jinému řádku, resp. sloupku se determinant nezmění.*

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

(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.

Budte  $A$  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  $B_{\circ}^i = cA_{\circ}^i$  a ostatní řádky matice  $B$  jsou stejné jako řádky matice  $A$ . Potom

$$\begin{aligned} \det B &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot B_{\sigma_1}^1 \dots B_{\sigma_i}^i \dots B_{\sigma_n}^n = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot A_{\sigma_1}^1 \dots cA_{\sigma_i}^i \dots A_{\sigma_n}^n = \\ &= c \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot A_{\sigma_1}^1 \dots A_{\sigma_i}^i \dots A_{\sigma_n}^n = \\ &= c \det A. \end{aligned}$$

(3) Nechť  $B$  vznikne z  $A$  vzájemnou výměnou  $i$ -tého řádku a  $j$ -tého řádku, čili  $B_{\circ}^i = A_{\circ}^j$ ,  $B_{\circ}^j = A_{\circ}^i$  a ostatní řádky matice  $B$  jsou stejné jako řádky matice  $A$ . Bud'  $\tau_{ij} \in S_n$  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

$$\begin{aligned}
 \det B &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot B_{\sigma_1}^1 \dots B_{\sigma_i}^i \dots B_{\sigma_j}^j \dots B_{\sigma_n}^n = \\
 &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot A_{\sigma_1}^1 \dots A_{\sigma_i}^i \dots A_{\sigma_j}^j \dots A_{\sigma_n}^n = \\
 &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot A_{\sigma_1}^1 \dots A_{\sigma_j}^j \dots A_{\sigma_i}^i \dots A_{\sigma_n}^n = \quad (\text{komutativita násobení}) \\
 &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot A_{\sigma'_1}^1 \dots A_{\sigma'_i}^i \dots A_{\sigma'_j}^j \dots A_{\sigma'_n}^n = \\
 &= - \sum_{\sigma \in S_n} \operatorname{sgn} \sigma' \cdot A_{\sigma'_1}^1 \dots A_{\sigma'_i}^i \dots A_{\sigma'_j}^j \dots A_{\sigma'_n}^n = \quad (\operatorname{sgn} \sigma^{-1} = \operatorname{sgn} \sigma) \\
 &= - \det A,
 \end{aligned}$$

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  $A^T = -A$  (taková matice se nazývá *antisymetrická*). Ukažte, že je-li  $n$  liché číslo, pak  $\det A = 0$ . ▷

**Příklad.**

$$\begin{aligned}
 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 4 \end{vmatrix} &= \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 \\ 4 & 4 & 4 & 8 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 3 & 3 & 6 & 6 \\ 4 & 4 & 4 & 8 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 2 & 4 & 4 & 4 \\ 3 & 3 & 6 & 6 \\ 4 & 4 & 4 & 8 \end{vmatrix} \\
 4 \cdot \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 4 \end{vmatrix} &= \begin{vmatrix} 4 & 4 & 4 & 4 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 8 & 8 & 8 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 12 & 12 \\ 0 & 0 & 0 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 16 \end{vmatrix} \\
 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 4 \end{vmatrix} &= (-1) \cdot \begin{vmatrix} 0 & 0 & 0 & 4 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 \\ 1 & 1 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 & 4 \\ 0 & 0 & 3 & 3 \\ 0 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 \end{vmatrix} \quad \blacksquare
 \end{aligned}$$

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

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

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

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  $Q_1, \dots, Q_k$  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.  $\square$

**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 3.2.7** (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 2.5.5 je  $AB$  také singulární a tedy

$$\det AB = 0 = \det A = \det A \cdot \det B. \quad \square$$

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

**Lemma 3.2.8.**

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

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

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

**Příklad.**

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

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



### 3.2.3. Laplaceův rozvoj

**Definice 3.2.3.** Buď  $A$  matice typu  $n \times n$ . Determinant řádu  $n - 1$  matice vzniklé z  $A$  vynecháním jednoho řádku a jednoho sloupku se nazývá *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

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

$$\begin{aligned} \hat{A}_1^1 &= (-1)^{1+1} \bar{A}_1^1 = d, & \hat{A}_2^1 &= (-1)^{1+2} \bar{A}_2^1 = -c, \\ \hat{A}_1^2 &= (-1)^{2+1} \bar{A}_1^2 = -b, & \hat{A}_2^2 &= (-1)^{2+2} \bar{A}_2^2 = a. \end{aligned} \quad \blacksquare$$

**Příklad.** Mějme

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

Potom

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

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

**Tvrzení 3.2.9** (Laplaceova věta o rozvoji determinantu). *Buď  $A$  matice typu  $n \times n$ . Pro každé  $i \in \{1, \dots, n\}$  platí*

$$\begin{aligned} \det A &= A_1^i \hat{A}_1^i + A_2^i \hat{A}_2^i + \dots + A_n^i \hat{A}_n^i = \sum_{j=1}^n A_j^i \hat{A}_j^i = \\ &= A_i^1 \hat{A}_i^1 + A_i^2 \hat{A}_i^2 + \dots + A_i^n \hat{A}_i^n = \sum_{j=1}^n A_i^j \hat{A}_i^j. \end{aligned}$$

*Důkaz.*

$$\begin{aligned}
 \det A &= \begin{vmatrix} A_1^1 & \dots & A_{j-1}^1 & A_j^1 & A_{j+1}^1 & \dots & A_n^1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^i & \dots & A_{j-1}^i & A_j^i & A_{j+1}^i & \dots & A_n^i \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^n & \dots & A_{j-1}^n & A_j^n & A_{j+1}^n & \dots & A_n^n \end{vmatrix} = \\
 &= \sum_{j=1}^n \begin{vmatrix} A_1^1 & \dots & A_{j-1}^1 & A_j^1 & A_{j+1}^1 & \dots & A_n^1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & A_j^i & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^n & \dots & A_{j-1}^n & A_j^n & A_{j+1}^n & \dots & A_n^n \end{vmatrix} = \\
 &= \sum_{j=1}^n A_j^i \begin{vmatrix} A_1^1 & \dots & A_{j-1}^1 & A_j^1 & A_{j+1}^1 & \dots & A_n^1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^n & \dots & A_{j-1}^n & A_j^n & A_{j+1}^n & \dots & A_n^n \end{vmatrix}.
 \end{aligned}$$

Ukažme, že

$$\begin{vmatrix} A_1^1 & \dots & A_{j-1}^1 & A_j^1 & A_{j+1}^1 & \dots & A_n^1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^n & \dots & A_{j-1}^n & A_j^n & A_{j+1}^n & \dots & A_n^n \end{vmatrix} = \hat{A}_j^i.$$

Vyměňujeme  $i$ -tý řádek  $(0 \dots 0 \ 1 \ 0 \dots 0)$  s předchozími řádky tak dlouho, až bude prvním řádkem; k tomu je potřeba  $i - 1$  výměn. Poté vyměňujeme  $j$ -tý sloupek  $(1 \ A_j^1 \dots A_j^{i-1} \ A_j^{i+1} \dots A_j^n)^T$  s předchozími sloupkami 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  $\bar{A}_j^i$ . Proto  $\det A = \sum_{j=1}^n A_j^i \cdot (-1)^{i+j} \bar{A}_j^i = \sum_{j=1}^n A_j^i \hat{A}_j^i$  a máme rozvoj podle  $i$ -tého řádku.

Rozvoj podle  $i$ -tého sloupku získáme analogicky.  $\square$

**Definice 3.2.4.** Vztah v Laplaceově větě se nazývá *Laplaceův rozvoj podle  $i$ -tého řádku* resp. *podle  $i$ -tého sloupku*.

**Příklad.**

$$\begin{aligned}
 \begin{vmatrix} 2 & 1 & 3 & 4 \\ 0 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 \\ 0 & 0 & 3 & 4 \end{vmatrix} &= 2 \cdot (-1)^{1+1} \cdot \begin{vmatrix} 0 & 1 & 2 \\ 2 & 3 & 4 \\ 0 & 3 & 4 \end{vmatrix} + 1 \cdot (-1)^{3+1} \cdot \begin{vmatrix} 1 & 3 & 4 \\ 0 & 1 & 2 \\ 0 & 3 & 4 \end{vmatrix} = \\
 &= 2 \cdot (-1)^{1+1} \cdot 2 \cdot (-1)^{2+1} \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} + 1 \cdot (-1)^{3+1} \cdot 1 \cdot \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 8 + (-2) = 6 \quad \blacksquare
 \end{aligned}$$

### 3.3. Adjungovaná matice

**Definice 3.3.1.** Buď  $A$  čtvercová matice. Označme  $\hat{A}$  matici kofaktorů  $\hat{A}_j^i$ . Matice  $\hat{A}^T$  je matice *adjungovaná* k matici  $A$  a značí se  $\text{adj } A$ . Tedy,

$$\text{adj } A = \hat{A}^T.$$

**Příklad.** Mějme

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

Potom

$$\text{adj } A = \hat{A}^T = \begin{pmatrix} \hat{A}_1^1 & \hat{A}_2^1 \\ \hat{A}_1^2 & \hat{A}_2^2 \end{pmatrix}^T = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}^T = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \quad \blacksquare$$

**Tvrzení 3.3.1.** Pro libovolnou čtvercovou matici  $A$

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

Je-li  $A$  regulární matice, pak

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

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

$$(A \cdot \text{adj } A)_j^i = \sum_k A_k^i (\hat{A}^T)_j^k = \sum_k A_k^i \hat{A}_k^j.$$

Pro  $i = j$  je  $(A \cdot \text{adj } A)_i^i = \sum_k A_k^i \hat{A}_k^i = \det A$  podle Laplaceovy věty.

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

$$\begin{aligned} \sum_k A_k^i \hat{A}_k^j &= \sum_k B_k^i \hat{B}_k^j && (B \text{ se liší od } A \text{ jen v } j\text{-tém řádku}) \\ &= \sum_k B_k^j \hat{B}_k^j && (B_k^i = B_k^j) \\ &= \det B && (\text{podle Laplaceovy věty}) \\ &= 0. && (B \text{ má dva stejné řádky}) \end{aligned}$$

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

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

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

Je-li  $A$  regulární, pak  $\det A \neq 0$ , takže jím můžeme dělit a s použitím Tvrzení 2.4.3 dostaneme uvedený vztah.  $\square$

**Příklad.** Mějme regulární matici

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

Potom

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

Například pro

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

dostaneme

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



## 4. SOUSTAVY LINEÁRNÍCH ROVNIC

### 4.1. Soustavy lineárních rovnic a jejich řešení

**Definice 4.1.1.** Buďte  $n \in \mathbb{N}$ ,  $P$  pole,  $a_1, a_2, \dots, a_n, b \in P$ ,  $x^1, x^2, \dots, x^n \notin P$ . Potom

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

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

Uvedenou lineární rovnici můžeme zapsat

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

**Definice 4.1.2.** *Řešení rovnice*

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

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

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

Při hledání řešení rovnice tedy hledáme prvky  $\xi^1, \xi^2, \dots, \xi^n$  pole  $P$  takové, že po dosazení  $\xi^i$  za  $x^i$  pro každé  $i \in \{1, 2, \dots, n\}$  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 4.1.1.** *Rovnice  $ax = b$  nad polem  $P$  o jedné neznámé  $x$ , kde  $a \neq 0$ , má jediné řešení, a to  $\xi = ba^{-1}$ .*

*Důkaz.* 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. □

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

**Definice 4.1.3.** Buďte  $m, n, i, j \in \mathbb{N}$ ,  $i \in \{1, 2, \dots, m\}$ ,  $j \in \{1, 2, \dots, n\}$ ,  $P$  pole, pro každé  $i, j$  nechť  $a_j^i, b^i \in P$ ,  $x^1, x^2, \dots, x^n \notin P$ . Potom

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

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

Uvedenou soustavu lineárních rovnic můžeme zapsat

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

Označíme-li

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

můžeme soustavu lineárních rovnic psát jako rovnici

$$Ax = b.$$

**Definice 4.1.4.** 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

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

je *rozšířená matice soustavy*.

**Definice 4.1.5.** 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  $\xi = (\xi^1 \ \xi^2 \ \dots \ \xi^n)^T$  taková, že platí rovnost

$$A\xi = b.$$

Součin  $Ax$  si můžeme rozepsat

$$\begin{aligned} Ax &= \begin{pmatrix} a_1^1 & a_2^1 & \dots & a_n^1 \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^m & a_2^m & \dots & a_n^m \end{pmatrix} \begin{pmatrix} x^1 \\ x^2 \\ \vdots \\ x^n \end{pmatrix} = \begin{pmatrix} a_1^1 x^1 + a_2^1 x^2 + \dots + a_n^1 x^n \\ a_1^2 x^1 + a_2^2 x^2 + \dots + a_n^2 x^n \\ \vdots \\ a_1^m x^1 + a_2^m x^2 + \dots + a_n^m x^n \end{pmatrix} = \\ &= x^1 \begin{pmatrix} a_1^1 \\ a_2^1 \\ \vdots \\ a_n^1 \end{pmatrix} + x^2 \begin{pmatrix} a_2^1 \\ a_2^2 \\ \vdots \\ a_2^m \end{pmatrix} + \dots + x^n \begin{pmatrix} a_n^1 \\ a_n^2 \\ \vdots \\ a_n^m \end{pmatrix} = \\ &= x^1 A_1^\circ + x^2 A_2^\circ + \dots + x^n A_n^\circ \end{aligned}$$

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 hodnota rozšířené matice soustavy je rovna hodnotě matice soustavy. Jestliže soustava nemá řešení, tj. sloupek pravých stran není lineární kombinací sloupků matice soustavy, potom hodnota rozšířené matice soustavy je o 1 větší než hodnota 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

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

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

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

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

(3) Soustava

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

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

## 4.2. 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 4.2.1.** *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 4.2.2.** *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 4.2.1.** *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

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

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

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



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.  $\square$

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). 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  $r$ , tj. rozšířená matice soustavy a matice soustavy mají stejné hodnoty, příslušná soustava rovnic (uvádíme jen ty nenulové) je

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

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 4.2.3.** 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 *volné proměnné*) a označujeme je po řadě  $t^1, \dots, t^{n-r}$ .

**Definice 4.2.4.** Řešení soustavy lineárních rovnic o  $n$  neznámých, jejíž rozšířená matice má hodnotu  $r$ , zapsané pomocí  $n - r$  parametrů se nazývá *obecné řešení*. Řešení získané z obecného řešení libovolnou volbou parametrů se nazývá *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.

**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

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

Z druhé rovnice můžeme vyjádřit  $x^2$  pomocí  $x^3$

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

a z první rovnice můžeme vyjádřit  $x^1$  pomocí  $x^3$

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

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

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

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

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

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

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

což je přímka v  $\mathbb{R}^3$  procházející bodem  $(-1, 1, 0)$  se směrovým vektorem  $(1, -2, 1)$ . Při maticovém zápisu je množina všech řešení

$$\left\{ \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \mid t \in \mathbb{R} \right\}.$$

■

### 4.3. Frobeniova věta

Z předchozích pozorování a tvrzení vyplývá následující věta.

**Tvrzení 4.3.1** (Frobeniova věta). *Soustava lineárních rovnic má aspoň jedno řešení právě tehdy, když hodnota matice soustavy se rovná hodnotě rozšířené matice soustavy.*

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

Jestliže se hodnoty matic  $A$  a  $\bar{A}$  rovnají, a rovnají se tedy i hodnoty příslušných matic v Gaussově–Jordanově tvaru, pak použitím postupu z předchozí podkapitoly 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 hodnoty jsou stejné, obě se rovnají 3, takže podle Frobeniovy věty soustava má řešení. Jelikož hodnoty 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

$$(1 \quad -1)$$

a rozšířenou matici soustavy

$$(1 \quad -1 \quad 1).$$

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

(3) Soustava

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

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. ■

#### 4.4. Cramerovo pravidlo

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

**Tvrzení 4.4.1.** *Soustava  $Ax = b$  s regulární maticí  $A$  má právě jedno řešení*

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

*Důkaz.* Buď  $A$  regulární matice, tedy čtvercová, invertibilní, s maximální hodností. Potom podle Frobeniovy věty soustava  $Ax = b$  má řešení. A pro každé řešení  $\xi$  platí  $A\xi = b$ , tedy  $\xi = A^{-1}A\xi = A^{-1}b$ . □

**Tvrzení 4.4.2** (Cramerovo pravidlo). *Buď  $Ax = b$  soustava s regulární maticí  $A$  a řešením  $\xi = (\xi^1 \ \xi^2 \ \dots \ \xi^n)^T$ . 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  $b$ :

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

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

$$\xi = A^{-1}b = \frac{\text{adj } A}{\det A} b = \frac{\hat{A}^T}{\det A} b = \frac{\hat{A}^T b}{\det A}$$

a tedy

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

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

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

z čehož dostaneme požadovaný vztah.  $\square$

**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

$$\begin{aligned}A &= \begin{pmatrix} 1 & 2 & -1 \\ -1 & 1 & 2 \\ 2 & -1 & 1 \end{pmatrix} & A_1 &= \begin{pmatrix} 1 & 2 & -1 \\ 1 & 1 & 2 \\ 1 & -1 & 1 \end{pmatrix} \\ A_2 &= \begin{pmatrix} 1 & 1 & -1 \\ -1 & 1 & 2 \\ 2 & 1 & 1 \end{pmatrix} & A_3 &= \begin{pmatrix} 1 & 2 & 1 \\ -1 & 1 & 1 \\ 2 & -1 & 1 \end{pmatrix}\end{aligned}$$

a

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

Proto

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

## 4.5. Homogenní soustavy lineárních rovnic

**Definice 4.5.1.** Soustava lineárních rovnic s nulovou pravou stranou,  $b = 0$ , se nazývá *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.  $\blacksquare$

**Tvrzení 4.5.1.** Každá homogenní soustava má řešení, nulové.

*Důkaz.* Existence řešení vyplývá z Frobeniovy věty. Je zřejmé, že dosazením nuly za všechny neznámé získáme řešení.  $\square$

Předchozí tvrzení netvrdí, že nulové řešení je jediné.

**Tvrzení 4.5.2.** 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.* Necht'  $\xi_1, \xi_2$  jsou řešení,  $\alpha_1, \alpha_2 \in P$ . Tedy,  $A\xi_1 = 0$  a  $A\xi_2 = 0$ . Potom

$$A(\alpha_1\xi_1 + \alpha_2\xi_2) = \alpha_1A\xi_1 + \alpha_2A\xi_2 = 0$$

a lineární kombinace řešení je tedy také řešení soustavy.  $\square$

**Definice 4.5.2.** *Fundamentální systém řešení* homogenní soustavy je taková množina řešení homogenní soustavy, která je lineárně nezávislá a každé řešení lze vyjádřit jako lineární kombinaci řešení z této množiny.

**Tvrzení 4.5.3.** *Fundamentální systém řešení soustavy rovnic  $Ax = 0$  o  $n$  neznámých má  $n - \text{rank } A$  prvků.*

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

$$(t^1, \dots, t^{n-\text{rank } A}) = (1, 0, \dots, 0),$$

$$(t^1, \dots, t^{n-\text{rank } A}) = (0, 1, \dots, 0),$$

...

$$(t^1, \dots, t^{n-\text{rank } A}) = (0, \dots, 0, 1),$$

dostaneme množinu řešení s požadovanými vlastnostmi.  $\square$

**Příklad.** (1) Soustava

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

má 2 neznámé, matice soustavy má hodnost 1 a množina všech řešení soustavy je  $\{(t, t) \mid t \in \mathbb{R}\} = \{t(1, 1) \mid t \in \mathbb{R}\}$ . Fundamentální systém řešení soustavy je například  $\{(1, 1)\}$ .

(2) Soustava

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

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

$$x^1 + 3x^2 + 6x^3 = 0$$

má 3 neznámé, matice soustavy má hodnost 2 a množina všech řešení soustavy je  $\{(0, -2t, t) \mid t \in \mathbb{R}\} = \{t(0, -2, 1) \mid t \in \mathbb{R}\}$ . 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 a množina všech řešení soustavy je  $\{(s - t, s, t) \mid s, t \in \mathbb{R}\} = \{s(1, 1, 0) - t(-1, 0, 1) \mid s, t \in \mathbb{R}\}$ . Fundamentální systém řešení soustavy je například  $\{(1, 1, 0), (-1, 0, 1)\}$ .

(4) Soustava

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

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

má 2 neznámé, matice soustavy má hodnost 2 a soustava má jediné řešení, čili množina všech řešení soustavy je  $\{(0, 0)\}$ . Fundamentální systém řešení soustavy je  $\emptyset$ .

(5) Soustava

$$0x = 0$$

má 1 neznámou, matice soustavy má hodnost 0 a množina všech řešení soustavy je  $\{t \mid t \in \mathbb{R}\} = \mathbb{R}$ . Fundamentální systém řešení soustavy je například  $\{6\}$ .  $\blacksquare$

## 4.6. Nehomogenní soustavy lineárních rovnic

**Definice 4.6.1.** Soustava lineárních rovnic s nenulovou pravou stranou se nazývá *nehomogenní*. Je-li  $Ax = b$  nehomogenní soustava, potom  $Ax = 0$  se nazývá *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 4.6.1.** Necht'  $\xi_p$  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  $\xi = \xi_p + \xi_0$  řešením 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 řešením 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.** Je-li  $\xi_p$  řešení soustavy  $Ax = b$ , potom množina všech řešení této soustavy je

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

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

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

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

(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

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

je  $\{(2, -1) + (0, 0)\} = \{(2, -1)\}$ . ■





## 5. POLYNOMY

### 5.1. Polynomy, algebraické vlastnosti, dělitelnost

**Definice 5.1.1.** Buď  $P$  pole,  $n \in \mathbb{N}$ ,  $a_0, \dots, a_n \in P$ ,  $x \notin P$ . *Polynom (mnohočlen)* jedné neurčité  $x$  nad polem  $P$  je výraz tvaru

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

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  $a_0, \dots, a_n \in P$  jsou *koeficienty*,  $a_i$  je  *$i$ -tý koeficient*. Koeficient  $a_0$  je *absolutní člen*. 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. Polynom se všemi koeficienty nulovými je *nulový polynom* a označujeme ho 0.

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

**Definice 5.1.2.** Polynomy

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

$$g = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

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

$$f = g, \text{ jestliže } a_0 = b_0, a_1 = b_1, \dots$$

**Definice 5.1.3.** *Stupeň* polynomu  $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  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  $\text{lc } f$ .

Pro nulový polynom nemáme definován ani stupeň ani vedoucí koeficient.

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

**Definice 5.1.4.** 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 5.1.5.** Mějme polynomy

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

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

Označme  $p = \max\{n, m\}$ . *Součet* polynomů  $f$  a  $g$  je polynom

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

*Součin* polynomů  $f$  a  $g$  je polynom

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

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

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

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

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

Speciálně, pokud  $f = -1$ , pak

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

je polynom *opačný* k polynomu  $g$ .

**Příklad.** Pro

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

je

$$\begin{aligned} f + g &= 6x^4 + x^3 + x^2 - x + 6, \\ fg &= 6x^7 - 12x^6 - 3x^5 - 6x^4 + 3x^3 - 12x^2 - 6x. \end{aligned}$$

■

**Tvrzení 5.1.1.** *Budte  $f, g \in P[x]$  nenulové. Potom  $fg$  je nenulový polynom a*

$$\deg(fg) = \deg f + \deg g,$$

$$\text{lc}(fg) = \text{lc } f \cdot \text{lc } g.$$

*Důkaz.* Budte  $f, g$  nenulové polynomy. Nechť  $\deg f = n$ ,  $\deg g = m$ ,  $\text{lc } f = a_n$  a  $\text{lc } g = b_m$ . 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  $\text{lc } fg = a_n b_m = \text{lc } f \cdot \text{lc } g$  a  $\deg(fg) = n + m = \deg f + \deg g$ . □

**Cvičení.** Součin polynomů je nulový právě tehdy, když aspoň jeden z nich je nulový. ▷

**Tvrzení 5.1.2.** *Budte  $f, g, h \in P[x]$ . Potom*

$$\begin{array}{ll} (1) f + g = g + f, & (5) f \cdot g = g \cdot f, \\ (2) f + (g + h) = (f + g) + h, & (6) f \cdot (g \cdot h) = (f \cdot g) \cdot h, \\ (3) f + 0 = f, & (7) f \cdot 1 = f, \\ (4) f + (-f) = 0, & (8) f \cdot (g + h) = f \cdot g + f \cdot h. \end{array}$$

*Důkaz.* Cvičení. □

**Tvrzení 5.1.3.** *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 5.1.6.** Budte  $f, g \in P[x]$ . 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 5.1.4.** *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  $f$ .  $\square$

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

**Definice 5.1.7.** Budte  $f, g \in P[x]$ . 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  $\deg g \leq \deg f$ .  $\triangleright$

**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  $x \cdot h = a_1x^2 + a_0x$ .  $\blacksquare$

**Cvičení.** (1) Ukažte, že  $x - 1 \mid x^n - 1$  pro každé celé  $n > 1$ .

(2) Ukažte, že relace  $\mid$  je reflexivní a tranzitivní.  $\triangleright$

**Tvrzení 5.1.5.** Budte  $f, g, h \in P[x]$ .

- (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.  $\square$

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

**Tvrzení 5.1.6.** Budte  $f, g \in P[x]$ ,  $g \neq 0$ . 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

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

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,

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

$$r_1 = 0 \text{ nebo } \deg r_1 < \deg g \quad (2)$$

$$r_2 = 0 \text{ nebo } \deg r_2 < \deg g. \quad (3)$$

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  $q_1 = q_2$ .  $\square$

**Definice 5.1.8.** V předchozím tvrzení  $q$  je *částečný podíl* (*podíl*, je-li  $r = 0$ ) polynomů  $f$  a  $g$  a  $r$  je *zbytek*.

Je zřejmé, že  $g \mid f$  právě tehdy, když zbytek je roven nule.

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

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

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

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

Čili

$$\begin{array}{ll} q_0 = 0 & r_0 = x^5 + 2x^3 + 2x + 4 \\ q_1 = x^3 & r_1 = -x^4 + 2x + 4 \\ q_2 = x^3 - x^2 & r_2 = x^3 + 2x^2 + 2x + 4 \\ q_3 = x^3 - x^2 + x & r_3 = x^2 + 4 \\ q_4 = x^3 - x^2 + x + 1 & r_4 = -x + 2 \end{array}$$

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

Jelikož  $\deg r_4 = 1 < 2 = \deg g$ ,

$$q = q_4 = x^3 - x^2 + x + 1 \quad \text{a} \quad r = r_4 = -x + 2.$$

Tedy

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

**Definice 5.1.9.** Polynom je *normovaný*, je-li nenulový a jeho vedoucí koeficient je 1.

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

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

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

**Lemma 5.1.7.** Budte  $f, g$  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  $1 = \text{lc } g = \text{lc}(fp) = \text{lc } f \cdot \text{lc } p = 1 \cdot p = p$ . 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.

## 5.2. Největší společný dělitel

**Definice 5.2.1.** Buďte  $f, g \in P[x]$  nenulové. 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.

Zapíšeme  $d = D(f, g)$ .

**Definice 5.2.2.** 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) Pro  $f \neq 0$   $D(f, 0) = \bar{f}$ . ■

**Tvrzení 5.2.1** (Eukleidův algoritmus.). *Buďte  $f, g \in P[x]$  nenulové polynomy. Buď  $r_0, r_1, r_2, r_3, \dots$  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  $\deg g = \deg r_1 > \deg r_2 > \deg r_3 > \dots$  je klesající posloupnost nezáporných celých čísel, existuje  $N \in \mathbb{N}$  takové, že  $r_{N-1} \neq 0$  a  $r_N = 0$ . □

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

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

Tedy  $r_0 = f$ ,  $r_1 = g$  a už víme, že  $f = g \cdot (x^3 - x^2 + x + 1) + (-x + 2)$ , takže

$$r_2 = -x + 2 \quad \text{a} \quad q_0 = x^3 - x^2 + x + 1.$$

Dělením polynomu  $r_1$  polynomem  $r_2$

$$\begin{array}{r} (x^2 + x + 2) : (-x + 2) = -x - 3 + \frac{8}{-x+2} \\ -(x^2 - 2x) \\ \hline 3x + 2 \\ -(-3x - 6) \\ \hline 8 \end{array}$$

dostaneme

$$r_3 = 8 \quad \text{a} \quad q_1 = -x - 3.$$

Dělením polynomu  $r_2$  polynomem  $r_3$

$$\begin{array}{r} (-x + 2) : (8) = -\frac{x}{8} + \frac{2}{8} \\ -(-x) \\ \hline 2 \\ -2 \\ \hline 0 \end{array}$$

dostaneme

$$r_4 = 0 \quad \text{a} \quad q_2 = -\frac{x}{8} + \frac{2}{8}.$$

V tomto případě tedy  $N = 4$ . ■

**Tvrzení 5.2.2.** *Pro libovolné dva polynomy, z nichž aspoň jeden je nenulový, existuje 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  $i \in \{0, \dots, N\}$ , 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  $r_{i+2} = r_i - r_{i+1}q_i$ . Postupně tedy dostaneme, že  $h \mid r_i$  pro všechna  $i \in \{0, \dots, N\}$ , včetně  $h \mid r_{N-1} = d$ . Tedy,  $d = D(f, g)$ .  $\square$

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

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

Už víme, že  $N = 4$  a  $r_3 = 8$ , čili  $D(f, g) = \bar{r}_3 = 1$ .  $\blacksquare$

**Tvrzení 5.2.3.** *Libovolné dva polynomy mají nejvýše jeden největší společný dělitel.*

*Důkaz.* Buďte  $d_1, d_2$  největší společné dělitele. Podle definice  $d_1 \mid d_2$  a  $d_2 \mid d_1$  a jelikož  $d_1, d_2$  jsou normované,  $d_1 = d_2$ .  $\square$

**Tvrzení 5.2.4** (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,  $d = D(f, g)$ .  $\square$

Pomocí Rozšířeného Eukleidova algoritmu lze získat nejen  $D(f, g)$ , ale i polynomy  $u, v$  z předchozího tvrzení.

**Tvrzení 5.2.5** (Rozšířený Eukleidův algoritmus). *Buďte  $f, g \in P[x]$  nenulové polynomy. Buďte  $r_0, r_1, r_2, \dots, r_{N-1}$  a  $q_0, q_1, q_2, \dots, q_{N-3}$  posloupnosti polynomů z Eukleidova algoritmu. Buďte*

$$\begin{aligned} u_0 &= 1, u_1 = 0, u_2, \dots, u_{N-1}, \\ v_0 &= 0, v_1 = 1, v_2, \dots, v_{N-1}, \end{aligned}$$

*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  $i \in \{0, \dots, N-3\}$ . Potom  $r_{N-1} = fu_{N-1} + gv_{N-1}$  a označíme-li*

$$u = \frac{1}{\text{lc } r_{N-1}} u_{N-1} \quad \text{a} \quad v = \frac{1}{\text{lc } r_{N-1}} v_{N-1},$$

*pak  $D(f, g) = fu + gv$ .*

*Důkaz.*  $\square$

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

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

Už víme, že  $D(f, g) = 1$ ,  $N = 4$ ,

$$r_0 = x^5 + 2x^3 + 2x + 4 \qquad q_0 = x^3 - x^2 + x + 1$$

$$r_1 = x^2 + x + 2 \qquad q_1 = -x - 3$$

$$r_2 = -x + 2$$

$$r_3 = 8$$

$$u_0 = 1$$

$$v_0 = 0$$

$$u_1 = 0$$

$$v_1 = 1.$$

Dále

$$u_0 = u_1 q_0 + u_2$$

$$1 = 0 \cdot q_0 + u_2 \quad \text{implikuje} \quad u_2 = 1,$$

$$v_0 = v_1 q_0 + v_2$$

$$0 = 1 \cdot q_0 + v_2 \quad \text{implikuje} \quad v_2 = -q_0 = -x^3 + x^2 - x - 1,$$

$$u_1 = u_2 q_1 + u_3$$

$$0 = 1 \cdot q_1 + u_3 \quad \text{implikuje} \quad u_3 = -q_1 = x + 3,$$

$$v_1 = v_2 q_1 + v_3$$

$$1 = -q_0 \cdot q_1 + v_3 \quad \text{implikuje} \quad v_3 = 1 + q_0 q_1 = -x^4 - 2x^3 + 2x^2 - 4x - 2.$$

Lze snadno ověřit, že  $r_3 = fu_3 + gv_3$ , a když

$$u = \frac{x}{8} + \frac{3}{8}$$

$$v = -\frac{x^4}{8} - \frac{x^3}{4} + \frac{x^2}{4} - \frac{x}{2} - \frac{1}{4}$$

pak  $D(f, g) = 1 = fu + gv$ . ■

### 5.3. Ireducibilní polynomy

**Definice 5.3.1.** *Reducibilní* polynom je nekonstantní polynom, který je součinem dvou nekonstantních polynomů. *Ireducibilní* polynom je nekonstantní polynom, který není reducibilní.

**Příklad.** Polynom  $x^2 - 1 = (x - 1)(x + 1)$  je reducibilní. Polynomy  $x - 1$  a  $x + 1$  jsou ireducibilní, máte tedy rozklad na normované ireducibilní polynomy. ■

**Cvičení.** Nechtě jsou  $f, g \in P[x]$  normované polynomy, nechtě  $g$  je ireducibilní a  $f \mid g$ . Potom buď  $f = 1$  nebo  $f = g$ . Je-li  $f$  také ireducibilní, pak  $f = g$ . ▷

**Lemma 5.3.1.** *Buděte  $g, h_1, \dots, h_n \in P[x]$  ireducibilní normované polynomy a nechtě  $g \mid h_1 \cdots h_n$ . Pak existuje index  $j$  takový, že  $g = h_j$ .*

*Důkaz.* □

**Tvrzení 5.3.2.** *Budě  $f \in P[x]$  normovaný polynom. Pak existují normované ireducibilní polynomy  $g_1, \dots, g_n$  takové, že  $f = g_1 \cdots g_n$ .*

*Tento rozklad je jediný. Je-li  $f = h_1 \cdots h_m$  jiný rozklad na normované ireducibilní činitele, pak  $m = n$  a po vhodném přechíslování platí  $h_i = g_i$  pro všechna  $i \in \{1, \dots, n\}$ . (Přesněji, existuje bijekce  $\varphi: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  taková, že  $h_i = g_{\varphi(i)}$  pro všechna  $i$ .)*

*Důkaz.* □

**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. ■

Jako důsledek obdržíme jisté zobecnění shora uvedeného lemmatu.

**Důsledek.** *Nechť  $f \in P[x]$ , buďte  $g_1, \dots, g_m \in P[x]$  ireducibilní, normované a po dvou různé, tj.  $g_i \neq g_j$  pro  $i \neq j$ . Jestliže  $g_1^{k_1} \mid f, \dots, g_m^{k_m} \mid f$ , pak  $g_1^{k_1} \cdots g_m^{k_m} \mid f$ .*

## 5.4. Kořeny a jejich násobnost

Když  $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in P[x]$  a  $\xi \in P$ , položme

$$f(\xi) = a_n \xi^n + a_{n-1} \xi^{n-1} + \dots + a_1 \xi + a_0 \in P.$$

**Tvrzení 5.4.1.** *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 5.4.1.** Prvek  $\xi \in P$  je kořen polynomu  $f \in P[x]$ , jestliže  $f(\xi) = 0$ .

**Tvrzení 5.4.2.** *Nechť  $f \in P[x]$  a  $\xi \in P$ . Potom  $\xi$  je kořen polynomu  $f$  právě tehdy, když polynom  $x - \xi$  dělí  $f$ .*

*Důkaz.* Předpokládejme, že  $\xi$  je kořen polynomu  $f$ . Dělením  $f : (x - \xi)$  dostaneme

$$f = (x - \xi)q + r, \quad \text{kde buď } r = 0 \text{ nebo } \deg r = 0 < 1 = \deg(x - \xi).$$

Takže  $r$  je konstantní polynom. Navíc  $0 = f(\xi) = (\xi - \xi)q(\xi) + r = r$ , čili  $f = (x - \xi)q$  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 5.4.2.** Nechť  $f \in P[x]$  a  $\xi \in P$ . Pokud  $(x - \xi) \mid f$ , polynom  $x - \xi$  je kořenový činitel polynomu  $f$ .

**Definice 5.4.3.** 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 5.4.3.** *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)  $k_1 + \dots + k_n \leq \deg f$ .

*Důkaz.* Cvičení. □

**Tvrzení 5.4.4** (Základní věta algebry). *Každý nekonstantní polynom  $f \in \mathbb{C}[x]$  má aspoň jeden kořen.*

**Důsledek.** *Každý nekonstantní polynom  $f \in \mathbb{C}[x]$  má rozklad na lineární ireducibilní činitele. Kořenů má se započtením násobnosti právě tolik, kolik činí jeho stupeň.*



**Tvrzení 5.4.5** (Vlastnosti kořenů (Viètovy vzorce)). *Bud'  $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{C}[x]$  normovaný polynom a  $\xi_1, \xi_2, \dots, \xi_n$  jeho kořeny (nemusí být všechny různé). Potom*

$$\begin{aligned} a_{n-1} &= -(\xi_1 + \xi_2 + \dots + \xi_n) = -\sum_{i=1}^n \xi_i \\ a_{n-2} &= \xi_1\xi_2 + \xi_1\xi_3 + \dots + \xi_1\xi_n + \xi_2\xi_3 + \dots + \xi_2\xi_n + \dots + \xi_{n-1}\xi_n = \\ &= \sum_{\substack{i,j=1 \\ i < j}}^n \xi_i\xi_j \\ a_{n-3} &= -(\xi_1\xi_2\xi_3 + \xi_1\xi_2\xi_4 + \dots + \xi_1\xi_{n-1}\xi_n + \dots + \xi_{n-2}\xi_{n-1}\xi_n) = \\ &= -\sum_{\substack{i,j,k=1 \\ i < j < k}}^n \xi_i\xi_j\xi_k \\ &\vdots \\ a_1 &= (-1)^{n-1}(\xi_1 \dots \xi_{n-2}\xi_{n-1} + \xi_1 \dots \xi_{n-2}\xi_n + \dots \\ &\quad \dots + \xi_1\xi_3 \dots \xi_n + \xi_2 \dots \xi_n) \\ a_0 &= (-1)^n \xi_1\xi_2 \dots \xi_n \end{aligned}$$

*Důkaz.*

$$x^n + \dots + a_0 = (x - \xi_1) \dots (x - \xi_n)$$

□

**Příklad.**  $x^2 - 5x + 6$  ■

Pro polynomy, jejichž koeficienty jsou celá čísla, navíc platí následující tvrzení.

**Tvrzení 5.4.6.** *Bud'  $f = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  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.* Cvičení. Dosazení  $\frac{p}{q}$  do  $f \dots$  □

**Důsledek.** *Celočíselné kořeny polynomu s celočíselnými koeficienty jsou dělitelé absolutního členu.*

## 5.5. Derivace

**Definice 5.5.1.** Bud'  $f = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{C}[x]$ . Polynom  $f' = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1 \in \mathbb{C}[x]$  je *derivace* polynomu  $f$ .

**Tvrzení 5.5.1.** (1)  $(f + g)' = f' + g'$ ,  
 (2)  $(fg)' = f'g + fg'$ ,  
 (3)  $(f^k)' = kf^{k-1}f'$ .

*Důkaz.* Cvičení. □

**Tvrzení 5.5.2.** *Bud'  $k \geq 2$ ,  $f \in \mathbb{C}[x]$  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.  $\square$

**Tvrzení 5.5.3.** *Budte  $f \in \mathbb{C}[x]$  a  $\xi \in \mathbb{C}$  jeho kořen. Potom  $\xi$  je 1-násobný kořen polynomu*

$$\frac{f}{D(f, f')} \in \mathbb{C}[x].$$

*Důkaz.* Buď  $\xi$  je  $k$ -násobný kořen, 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

$$\frac{f}{D(f, f')} = (x - \xi) \frac{q}{r} \quad \text{a jelikož } x - \xi \text{ nedělí } q, \text{ nedělí ani } \frac{q}{r}. \quad \square$$

**Důsledek.** *Bud'  $f \in \mathbb{C}[x]$ .*

- (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.  $\square$

## 5.6. Polynomy s reálnými koeficienty

Mějme polynom  $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{C}[x]$ . Přiřadíme mu polynom  $f^* = a_n^* x^n + \dots + a_1^* x + a_0^* \in \mathbb{C}[x]$ .

- Tvrzení 5.6.1.** (1)  $(f + g)^* = f^* + g^*$ ,  
 (2)  $(fg)^* = f^* g^*$ .

*Důkaz.* Cvičení.  $\square$

**Tvrzení 5.6.2.** *Bud'  $f \in \mathbb{R}[x]$  polynom a  $\xi \in \mathbb{C}$  jeho kořen. Pak komplexně sdružené číslo  $\xi^*$  je též kořen stejné násobnosti.*

*Důkaz.*  $f = (x - \xi)^k q$ . Aplikujeme komplexní sdružení  $f = f^* = (x - \xi^*)^k q^*$  (cvičení). Kdyby  $f = (x - \xi^*)^{k+1} r$ , pak  $f = f^* = (x - \xi)^{k+1} r^*$ .  $\square$

Rozklad polynomu  $f \in \mathbb{R}[x]$  na ireducibilní činitele nad  $\mathbb{C}$  pak obsahuje ...

Vidíme, že  $\deg f =$

**Tvrzení 5.6.3.** *Každý polynom  $f \in \mathbb{R}[x]$  lichého stupně má aspoň jeden reálný kořen.*

*Důkaz.* Cvičení.  $\square$

**Tvrzení 5.6.4.** *Nechť  $\xi \in \mathbb{C} \setminus \mathbb{R}$ . Ukažte, že  $(x - \xi)(x - \xi^*) = x^2 - 2 \operatorname{re} \xi + |\xi|^2$  je kvadratický polynom s reálnými koeficienty a záporným diskriminantem.*

*Důkaz.* Cvičení.

Návod: pište  $\xi = \alpha + \beta i$ , kde  $\alpha, \beta \in \mathbb{R}$ .  $\square$

**Cvičení.** Ukažte, že reálné polynomy řádu  $> 2$  jsou vždy reducibilní nad  $\mathbb{R}$ .  $\triangleright$

**Cvičení.** Rozložte polynom  $x^4 + 1$  na ireducibilní činitele nad polem  $\mathbb{C}$  a nad polem  $\mathbb{R}$ .  $\triangleright$

## 6. GRUPY

### 6.1. Binární operace

**Definice 6.1.1.** *Binární operace* na množině  $X$  je libovolné zobrazení  $X \times X \rightarrow X$ .

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  $\mathbb{N}_0 = \{0, 1, 2, \dots\}$  množina všech celých nezáporných čísel. Zobrazení  $+: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0$ , 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  $X \rightarrow X$  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 6.1.2.** 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 6.1.3.** 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 6.1.4.** 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 6.1.1.** 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  $\text{id}_X$ .

(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 6.1.5.** 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 6.1.2.** 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

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2. \quad \square$$

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  $f: X \rightarrow X$  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

$$1 * 2 = 2 * 1 = 0 \quad \text{a} \quad 2 * 2 = 0.$$

Číli 1 a 2 jsou inverzní prvky k 2. Podle Tvrzení 6.1.2 to znamená, že operace  $*$  není asociativní. A skutečně, například,

$$(1 * 1) * 2 = 2 * 2 = 0 \quad \text{zatímco} \quad 1 * (1 * 2) = 1 * 0 = 1. \quad \blacksquare$$

## 6.2. Grupy

**Definice 6.2.1.** Množina  $G$  s binární operací  $*$ :  $G \times G \rightarrow G$  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  $GL_n(P)$  invertibilních matic typu  $n \times n$  s operací násobení matic je grupa (nazývá se *obecná lineární grupa*). ■

**Tvrzení 6.2.1.** *Bud'  $(G, *, e, ^{-1})$  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  $x * y * y^{-1} * x^{-1} = e$ . □

### 6.3. Podgrupy

**Definice 6.3.1.** Buď  $(X, *, e, {}^{-1})$  grupa, buď  $Y \subset X$  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 inverzím*.

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  $\{z \in \mathbb{C} \mid |z| = 1\}$  je podgrupa multiplikativní grupy  $\mathbb{C}^*$ .

(6) Množina  $\{(x, 2x) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$  je podgrupa grupy  $\mathbb{R}^2$  s operací sčítání.

(7) Množiny  $\{(x, 1) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$  a  $\{(x, y) \in \mathbb{R}^2 \mid x, y \in \mathbb{R}, x^2 + y^2 \leq 1\}$  nejsou podgrupy grupy  $\mathbb{R}^2$  s operací sčítání. ■

**Tvrzení 6.3.1.** (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  $X$ . ▷

### 6.4. 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

$$m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, 2m, \dots\}.$$

**Tvrzení 6.4.1.** 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  $m\mathbb{Z}$  na 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  $m\mathbb{Z}$  na inverzní (opačné) prvky.

Ukážeme, že každá podgrupa  $B \subset \mathbb{Z}$  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  $m\mathbb{Z} \subset B$ . Již víme, že  $0 \in B$  a  $m \in B$ . Matematickou indukcí se snadno dokáže, že  $mk = m(k-1) + m \in B$  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  $B \subset m\mathbb{Z}$ . 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  $b \in m\mathbb{Z}$ .  $\square$

## 6.5. Faktorové grupy

**Definice 6.5.1.** *Relace* na množině  $X$  je podmnožina kartézského součinu  $X \times X$ .

Je-li  $\rho$  relace, místo  $(x, y) \in \rho$  často píšeme  $x \rho y$ .

**Definice 6.5.2.** 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  $x \rho z$ .

Buďte  $\equiv$  relace ekvivalence na množině  $X$  a  $x \in X$ . Množina všech prvků ekvivalentních prvku  $x$  je *třída ekvivalence* příslušná  $x$  a označujeme ji  $[x]_{\equiv}$  nebo jen  $[x]$ , je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

$$[x]_{\equiv} = \{y \in X \mid x \equiv y\},$$

a množina všech tříd ekvivalence je *faktorová množina* a označujeme ji  $\tilde{X}_{\equiv}$  nebo jen  $\tilde{X}$ , tedy

$$\tilde{X}_{\equiv} = \{[x]_{\equiv} \mid x \in X\}.$$

Poznamenejme, že  $\tilde{X}$  je rozklad množiny  $X$ , čili množiny  $[x]$  jsou neprázdné, po dvou disjunktní a jejich sjednocení je  $X$ .

**Definice 6.5.3.** Buďte  $X$  množina s binární operací  $*$  a  $\equiv$  relace ekvivalence na množině  $X$ . Relace  $\equiv$  je *kongruence* na  $X$  s  $*$ , jestliže platí implikace (*podmínka kompatibility*)

$$\text{jestliže } x_1 \equiv x_2 \text{ a } y_1 \equiv y_2, \text{ pak } x_1 * y_1 \equiv x_2 * y_2, \tag{4}$$

nebo ekvivalentně zapsáno

$$\text{jestliže } [x_1] = [x_2] \text{ a } [y_1] = [y_2], \text{ pak } [x_1 * y_1] = [x_2 * y_2].$$

**Tvrzení 6.5.1.** *Buďte  $\equiv$  kongruence na množině s asociativní binární operací a  $x, y$  invertibilní prvky. Pak platí implikace*

$$\text{jestliže } x \equiv y, \text{ pak } x^{-1} \equiv y^{-1}$$

nebo ekvivalentně zapsáno

$$\text{jestliže } [x] = [y], \text{ pak } [x^{-1}] = [y^{-1}].$$

*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  $y^{-1} \equiv x^{-1}$ .  $\square$

**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 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  $\equiv$  nespĺňuje podmínku kompatibility a není to tedy kongruence na  $\mathbb{Z}$ . ■

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

$$[x]\tilde{*}[y] = [x * y]. \quad (5)$$

**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 (5), 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 6.5.2.** *Mějme kongruenci na množině  $X$  s binární operací  $*$ . Bud'  $\tilde{*}$  binární operace na  $\tilde{X}$  definovaná předpisem (5). 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 operace  $*$ , 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 (5) 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 (5) je (komutativní) grupa.*



*Důkaz.* Tvzení je jednoduchým důsledkem předchozího Tvzení.  $\square$

Jelikož každý prvek množiny s asociativní operací má nejvýše jeden inverzní prvek, viz Tvzení 6.1.2 nebo Tvzení 6.5.1, 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 6.5.4.** Faktorová množina s operací definovanou předpisem (5) 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  $-[0] = [0]$ ,  $-[1] = [-1] = [1]$ .  $\blacksquare$

## 6.6. 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

$$\begin{aligned} & \vdots \\ [-2]_m &= \{-2 + km \mid k \in \mathbb{Z}\} = \{\dots, -2 - 2m, -2 - m, -2, -2 + m, -2 + 2m, \dots\}, \\ [-1]_m &= \{-1 + km \mid k \in \mathbb{Z}\} = \{\dots, -1 - 2m, -1 - m, -1, -1 + m, -1 + 2m, \dots\}, \\ [0]_m &= \{km \mid k \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, 2m, \dots\}, \\ [1]_m &= \{1 + km \mid k \in \mathbb{Z}\} = \{\dots, 1 - 2m, 1 - m, 1, 1 + m, 1 + 2m, \dots\}, \\ [2]_m &= \{2 + km \mid k \in \mathbb{Z}\} = \{\dots, 2 - 2m, 2 - m, 2, 2 + m, 2 + 2m, \dots\}, \\ & \vdots \\ [i]_m &= \{i + km \mid k \in \mathbb{Z}\} = \{\dots, i - 2m, i - m, i, i + m, i + 2m, \dots\}, \\ & \vdots \end{aligned}$$

Pro  $i \in \{0, \dots, m-1\}$  třída ekvivalence  $[i]_m$  obsahuje právě ta celá čísla  $z$ , po jejichž celočíselném dělení číslem  $m$  číslo  $i$  je zbytek. Třídám  $[i]_m$ , kde  $i \in \{0, \dots, m-1\}$ , se proto říká *zbytkové třídy*. Při dělení číslem  $m$  všechny možné zbytky jsou právě  $0, 1, \dots, m-1$ , takže každé celé číslo leží v právě jedné ze zbytkových tříd  $[0]_m, [1]_m, \dots, [m-1]_m$ . Příslušná faktorová množina  $\tilde{\mathbb{Z}}_{\equiv_m}$  se značí  $\mathbb{Z}_m$ , tedy

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}.$$

Ověříme, zda  $\equiv_m$  je kongruence na  $\mathbb{Z}$ , čili podmínku kompatibility (4). 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 (5)

$$[x]_m + [y]_m = [x + y]_m$$

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 (4) 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  $[x_2 y_2]_m = [x_1 y_1]_m$ .

Na  $\mathbb{Z}_m$  tedy máme i binární operaci  $\cdot$  podle (5)

$$[x]_m \cdot [y]_m = [x \cdot y]_m.$$

Podle Tvzení 6.5.2 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 6.6.1.** *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  $D(x, m) = yx + km$ . V našem případě  $1 = xy + km$ , takže  $[1]_m = [xy]_m = [x]_m \cdot [y]_m$  a  $[y]_m$  je inverze k  $[x]_m$ .  $\square$

**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	
$[2]_5$	...	-3	2	7
$[3]_5$		-2	3	8
$[4]_5$		-1	4	9

Aditivní grupa  $\mathbb{Z}_5$  resp. multiplikativní monoid  $\mathbb{Z}_5$  mají tabulky

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$		$\cdot$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$		$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$		$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	resp.	$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$		$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$		$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

## 7. OKRUHY A POLE

**Definice 7.0.1.** Množina  $P$  se dvěma 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

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \text{a} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Neutrální prvek operace  $+$  je  $0$  a inverzní (opačné) prvky jsou  $-0 = 0$  a  $-1 = 1$ . Neutrální prvek operace  $\cdot$  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

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array} \quad \text{a} \quad \begin{array}{c|cccc} \cdot & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 0 & 2 \\ 3 & 0 & 3 & 2 & 1 \end{array}$$

Potom neutrální prvek operace  $+$  je  $0$ , neutrální prvek operace  $\cdot$  je  $1$  a

$$\begin{array}{cc} -0 = 0 & 0^{-1} \text{ neexistuje} \\ -1 = 3 & 1^{-1} = 1 \\ -2 = 2 & 2^{-1} \text{ neexistuje} \\ -3 = 1 & 3^{-1} = 3 \end{array} \quad \text{a}$$

Množina  $\{0, 1, 2, 3\}$  s těmito operacemi je okruh, ale není pole. ■

**Tvrzení 7.0.1.** *Bud'  $P$  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 7.0.2.** *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 7.0.1(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 7.0.1(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 6  $P^*$  označuje množinu  $P \setminus \{0\}$ .

Je-li  $P$  okruh, pak  $P$  s operací  $+$  je komutativní grupa. Pro pole máme navíc následující tvrzení.

**Tvrzení 7.0.3.** *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 7.0.2(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 7.0.4.** *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 6.5 a 6.6  $\mathbb{Z}_m$  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 6.6.1 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 6.6.1  $[x]_m$  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		$\cdot$	0	1	a	b
0	0	1	a	b	$a$	0	0	0	0	0
1	1	0	b	a	$a$	1	0	1	a	b
a	a	b	0	1	$a$	a	0	a	b	1
b	b	a	1	0	$a$	b	0	b	1	a

Množina  $X$  s těmito operacemi  $+$  a  $\cdot$  je pole. ■

**Poznámka.** Pro libovolné přirozené číslo  $n$  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 7.0.2.** Buď  $P$  pole. Buď  $Q \subset P$  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 7.0.3.** Podpole pole  $\mathbb{C}$  je *číselné pole*.



## 8. USPOŘÁDÁNÍ A SVAZY

### 8.1. Uspořádané množiny

**Definice 8.1.1.** 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.  $x | y$  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  $x | y$  a  $y | x$ , 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  $x = x \cdot 1 = y$ .

Upozorníme, že obdobně definovaná relace dělitelnosti na  $\mathbb{Z}$  není antisymetrická, protože  $1 \neq -1$ , přestože  $1 | -1$  a  $-1 | 1$  (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 8.1.2.** 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 8.1.3.** 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 zavedme označení  $x \triangleleft y$ , jestliže  $x < y$  a neexistuje  $z \in X$  takové, že  $x < z, z < y$ . Je-li  $x \triangleleft y$ , 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  $1 \triangleleft 2$ ,  $1 < 3$ , ale neplatí  $1 \triangleleft 3$ .

(2) V množině  $\mathbb{N}$  s relací dělitelnosti 6 pokrývá 3.

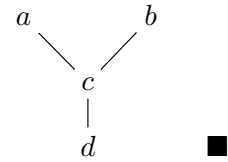
(3) V množině  $\mathbb{Q}$  všech racionálních čísel s přirozeným uspořádáním podle velikosti neplatí  $x \triangleleft y$  pro žádnou dvojici  $x, y \in \mathbb{Q}$ . Pro libovolné  $x, y \in \mathbb{Q}$  takové, že  $x < y$ , platí  $z = \frac{1}{2}(x + y) \in \mathbb{Q}$  a  $x < z, z < y$ . ■

Konečnou uspořádanou množinu  $(X, \leq)$  můžeme znázornit diagramem. Prvky množiny  $X$  znázorníme jako body v rovině. Prvky  $x, y$  splňující  $x \triangleleft y$  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:

- $d \triangleleft c$ ,  $c \triangleleft a$ ,  $c \triangleleft b$ ,
- $d < a$ , ale nikoliv  $d \triangleleft a$ ,
- prvky  $a, b$  nejsou srovnatelné.



**Definice 8.1.4.** Buď  $(X, \leq)$  uspořádaná množina. Prvek  $x \in X$  je

- *nejmenší*, je-li  $x \leq y$  pro každé  $y \in X$ ;
- *největší*, je-li  $x \geq y$  pro každé  $y \in X$ ;
- *minimální*, neexistuje-li  $y \in X$  takové, že  $y < x$ ;
- *maximální*, neexistuje-li  $y \in X$  takové, že  $x < y$ .

**Příklad.** V uspořádané množině  $Y$  z předchozího příkladu platí:

- $d$  je nejmenší prvek a zároveň jediný minimální prvek,
- $a, b$  jsou maximální prvky, ale největší prvek neexistuje. ■

**Definice 8.1.5.** 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  $y \in Y$ ,
- *infimum* množiny  $Y$ , je-li  $x$  největší prvek množiny všech dolních závor množiny  $Y$ ; píšeme  $x = \inf Y$ ,
- *supremum* množiny  $Y$ , je-li  $x$  nejmenší prvek množiny všech horních závor množiny  $Y$ ; píšeme  $x = \sup Y$ .

**Příklad.** V uspořádané množině  $Y$  z předchozího příkladu platí:

- podmnožina  $\{a, b\}$  má dolní závory  $c, d$ , z nich největší je  $c$ , a proto  $\inf\{a, b\} = c$ ,
- podmnožina  $a, b$  nemá žádnou horní závoru, a proto  $\sup\{a, b\}$  neexistuje (množina horních závor je prázdná, a proto nemá největší prvek). ■

**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). ▷

## 8.2. Svazy

**Definice 8.2.1.** Buď  $X$  uspořádaná množina. Nechť pro každé  $x, y \in X$  existují infimum  $\inf\{x, y\}$  a supremum  $\sup\{x, y\}$ . Pak  $X$  je *svazově uspořádaná množina*.

**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) 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  $x, y$ . ■

Jelikož ve svazově uspořádané množině  $X$  pro každé  $x, y$  existují  $\inf\{x, y\}$  a  $\sup\{x, y\}$  a jsou jednoznačně určena, můžeme na  $X$  definovat binární operace  $\wedge$  a  $\vee$ :

$$x \wedge y := \inf\{x, y\}, \quad x \vee y := \sup\{x, y\}.$$

**Tvrzení 8.2.1.** *Bud'  $X$  svazově uspořádaná množina. Pro libovolná  $x, y, z \in X$  platí*

$$\begin{aligned} x \wedge x &= x, & x \vee x &= x, \\ x \wedge y &= y \wedge x, & x \vee y &= y \vee x, \\ x \wedge (y \wedge z) &= (x \wedge y) \wedge z, & x \vee (y \vee z) &= (x \vee y) \vee z, \\ x \wedge (y \vee x) &= x, & x \vee (y \wedge x) &= x. \end{aligned} \tag{6}$$

*Důkaz.* Cvičení.

Asociativita  $\vee$ : Návod: Ukažte, že  $x \vee (y \vee z) = \sup\{x, y, z\} = (x \vee y) \vee z$ . □

**Cvičení.** Dokažte, že  $x_1 \vee x_2 \vee \dots \vee x_n = \sup\{x_1, x_2, \dots, x_n\}$ . (Vlevo nezáleží na uzávkování). ▷

**Definice 8.2.2.** Množina  $X$  (bez jakéhokoliv uvažovaného uspořádání) se dvěma binárními operacemi  $\wedge$  a  $\vee$  s vlastnostmi (6) se nazývá *svaz*. Binární operace  $\wedge$  se nazývá *průsek*, binární operace  $\vee$  se nazývá *spojení*.

Podle předcházejícího tvrzení tedy každá svazově uspořádaná množina je svaz. Podle následujícího cvičení platí však i obráceně, že každý svaz je svazově uspořádaná množina.

**Cvičení.** (1) Bud'  $(X, \wedge, \vee)$  svaz.

- (a) Položme  $x \leq_{\wedge} y$  právě tehdy, když  $x \wedge y = x$ . Pak  $\leq_{\wedge}$  je uspořádání na  $X$ .
- (b) Položme  $x \leq_{\vee} y$  právě tehdy, když  $x \vee y = y$ . Pak  $\leq_{\vee}$  je uspořádání na  $X$ .
- (c) Uspořádání  $\leq_{\wedge}$  je shodné s uspořádáním  $\leq_{\vee}$  a je svazové, přičemž

$$\inf\{x, y\} = x \wedge y, \quad \sup\{x, y\} = x \vee y.$$

(2) Bud'  $(X, \wedge, \vee)$  svaz. Ukažte, že  $(X, \vee, \wedge)$  je také svaz (identity (6) definující svaz jsou symetrické vzhledem k vzájemné záměně  $\wedge$  a  $\vee$ ). Nazývá se *duální svaz* a značí se  $X^*$ . Ověřte, že duální svaz má duální uspořádání. ▷

Budeme používat termín svaz i pro svazově uspořádané množiny. Svazy budeme chápat i jako algebraické struktury i jako uspořádané množiny současně. Uspořádání totiž jednoznačně určuje algebraickou strukturu a algebraická struktura zase jednoznačně určuje uspořádání.

**Tvrzení 8.2.2.** *Bud'  $X$  svaz. Pro každé  $x, a, b \in X$  platí*

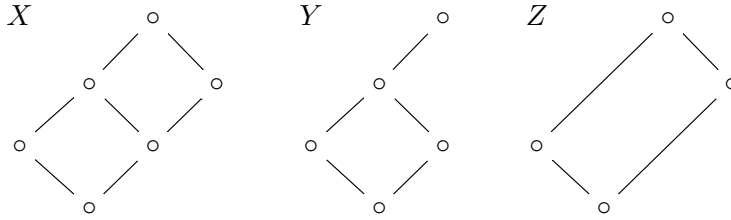
- (i) *jestliže  $a \leq b$ , pak  $a \wedge x \leq b \wedge x$ ;*
- (ii) *jestliže  $a \leq b$ , pak  $a \vee x \leq b \vee x$ ;*
- (iii) *jestliže  $x \leq a$ ,  $x \leq b$ , pak  $x \leq a \wedge b$ ;*
- (iv) *jestliže  $x \geq a$ ,  $x \geq b$ , pak  $x \geq a \vee b$ .*

*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 8.2.3.** *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  $Z$ :



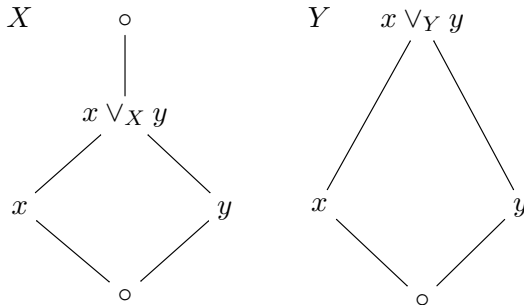
■

**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  $X$ . ■

### 8.3. Úplné svazy

**Definice 8.3.1.** Svaz je *úplný*, má-li každá jeho podmnožina supremum i infimum.

**Příklad.** (1) Každý konečný svaz je úplný a platí  $\inf\{x_1, x_2, \dots, x_n\} = x_1 \wedge x_2 \wedge \dots \wedge x_n$ ,  $\sup\{x_1, x_2, \dots, x_n\} = x_1 \vee x_2 \vee \dots \vee x_n$ .

(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 8.3.1.** *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 podgroupy  $A_\iota$ .

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. ▷



## 9. HOMOMORFISMY

### 9.1. Homomorfismy a izomorfismy grup

#### 9.1.1. Homomorfismy grup

**Definice 9.1.1.** Budte  $(X, *, e_X, {}^{-1})$ ,  $(Y, \diamond, e_Y, {}^{-1})$  grupy. Zobrazení  $f: X \rightarrow Y$  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  $f: (X, *, e_X, {}^{-1}) \rightarrow (Y, \diamond, e_Y, {}^{-1})$ .

**Příklad.** (1)  $f_2: (\mathbb{Z}, +, 0, -) \rightarrow (\mathbb{Z}, +, 0, -)$ ,  $n \mapsto 2n$ , je homomorfismus grup.

(2) Buď  $X$  grupa,  $\tilde{X}$  faktorová grupa. Potom zobrazení  $X \rightarrow \tilde{X}$ ,  $x \mapsto [x]$  (faktorová projekce) je homomorfismus grup.

(3) Budte  $X = \{0, 1, 2, 3\}$  a  $Y = \{0, 1\}$  s binárními operacemi  $+$  takovými, že

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array} \quad \text{a} \quad \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

Potom množiny  $X$  a  $Y$  s těmito operacemi jsou grupy. Zobrazení  $X \rightarrow Y$ ,  $0 \mapsto 0$ ,  $1 \mapsto 1$ ,  $2 \mapsto 0$ ,  $3 \mapsto 1$ , je homomorfismus těchto grup. ■

**Tvrzení 9.1.1.** Budte  $(X, *, e_X, {}^{-1})$ ,  $(Y, \diamond, e_Y, {}^{-1})$  grupy. Buď  $f: X \rightarrow Y$  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  $(X, *, e_X, {}^{-1}) \rightarrow (Y, \diamond, e_Y, {}^{-1})$ .

*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  $x \in X$ .

$$\begin{aligned} f(x^{-1}) \diamond f(x) &= f(x^{-1} * x) = f(e_X) = e_Y, \\ f(x) \diamond f(x^{-1}) &= f(x * x^{-1}) = f(e_X) = e_Y. \end{aligned}$$

Takže  $f(x^{-1})$  je inverze k  $f(x)$ . □

**Cvičení.** Buď  $f: X \rightarrow Y$  homomorfismus grup. Označme

$$\text{Im } f = \{f(x) \mid x \in X\}.$$

Pak  $\text{Im } f$  je podgrupa v  $Y$ . ▷

**Tvrzení 9.1.2.** Budte  $f: X \rightarrow Y$  a  $g: Y \rightarrow Z$  homomorfismy grup. Pak jejich složení  $g \circ f: X \rightarrow Z$  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.  $\square$

### 9.1.2. Izomorfismy grup

**Definice 9.1.2.** *Izomorfismus grup* je homomorfismus grup, který je bijektivní.

**Tvrzení 9.1.3.** *Buď  $f: X \rightarrow Y$  izomorfismus grup. Pak  $f^{-1}: Y \rightarrow X$  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 9.1.1.  $\square$

**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  $\exp: (\mathbb{R}, +, 0, -) \rightarrow (\mathbb{R}_+, \cdot, 1, {}^{-1}), x \mapsto e^x$  je homomorfismus grup, protože pro libovolná  $x, y \in \mathbb{R}$  platí  $\exp(x + y) = e^{x+y} = e^x e^y = (\exp x) \cdot (\exp y)$ . Tento homomorfismus je bijektivní, tedy i izomorfismus.

Inverzní izomorfismus je logaritmus

$$\ln: (\mathbb{R}_+, \cdot, 1, {}^{-1}) \rightarrow (\mathbb{R}, +, 0, -). \quad \blacksquare$$

**Definice 9.1.3.** Dvě grupy  $X, Y$  jsou *izomorfní*, jestliže existuje izomorfismus  $X \rightarrow Y$ . Zapisujeme  $X \cong Y$ .

**Tvrzení 9.1.4.** *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.  $\square$

**Příklad.**  $(\mathbb{R}, +, 0, -) \cong (\mathbb{R}_+, \cdot, 1, {}^{-1})$ . Pro libovolné  $a \in \mathbb{R}_+, a \neq 1$ , zobrazení  $\mathbb{R} \rightarrow \mathbb{R}_+, x \mapsto a^x$  je izomorfismus  $(\mathbb{R}, +, 0, -) \rightarrow (\mathbb{R}_+, \cdot, 1, {}^{-1})$ . Ověřte.  $\blacksquare$

**Cvičení.** Buď  $h: X \rightarrow Y$  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  $\text{Im } h$ .

Návod:  $\tilde{X} \rightarrow \text{Im } h, [x] \mapsto h(x)$ .  $\triangleright$

## 9.2. Homomorfismy a izomorfismy polí

**Definice 9.2.1.** Buďte  $P, Q$  pole. Zobrazení  $f: P \rightarrow Q$  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 9.2.2.** Je-li homomorfismus polí navíc bijektivní, je to *izomorfismus polí*. Pole, mezi nimiž existuje izomorfismus, jsou *izomorfní*.

**Příklad.** Dvoupvkové pole  $\{0, 1\}$  je izomorfní s polem  $\mathbb{Z}_2$ . Izomorfismem je zobrazení  $0 \mapsto [0]_2, 1 \mapsto [1]_2$ . ■

## 9.3. Izotonní zobrazení, homomorfismy a izomorfismy svazů

### 9.3.1. Izotonní zobrazení a izomorfismy uspořádaných množin

**Definice 9.3.1.** Buďte  $(X, \leq), (Y, \leq)$  uspořádané množiny. Zobrazení  $f: X \rightarrow Y$  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  $\text{id}: (\mathbb{N}, |) \rightarrow (\mathbb{N}, \leq)$  je izotonní. Skutečně, jestliže  $a | b$ , pak  $b = na$  pro nějaké  $n \in \mathbb{N}$ , ale  $n \geq 1$ , a proto  $b = na \geq a$ .

Inverzní zobrazení  $\text{id}: (\mathbb{N}, \leq) \rightarrow (\mathbb{N}, |)$  není izotonní, protože neplatí implikace  $x \leq y \Rightarrow x | y$  (například  $2 \leq 3$ , ale  $2 \nmid 3$ ). ■

**Příklad.** Buďte  $X = Y = \{0, 1\}$  s uspořádáními a zobrazením  $f$  podle obrázku:

$$\begin{array}{ccc} X & \begin{array}{ccc} 1 & \xrightarrow{\quad} & 1 \\ & f & | \\ 0 & \xrightarrow{\quad} & 0 \end{array} & Y \end{array}$$

Tedy  $f: X \rightarrow Y$  je identické zobrazení. Pak  $f$  je izotonní bijekce, jejíž inverze  $f^{-1}$  není izotonní. ■

**Cvičení.** Složení izotonních zobrazení je izotonní zobrazení. ▷

### 9.3.2. Homomorfismy a izomorfismy svazů

Buďte  $(X, \wedge, \vee), (Y, \wedge, \vee)$  svazy. Zobrazení  $f: X \rightarrow Y$  je *homomorfismus svazů*, jestliže pro každé  $x_1, x_2 \in X$

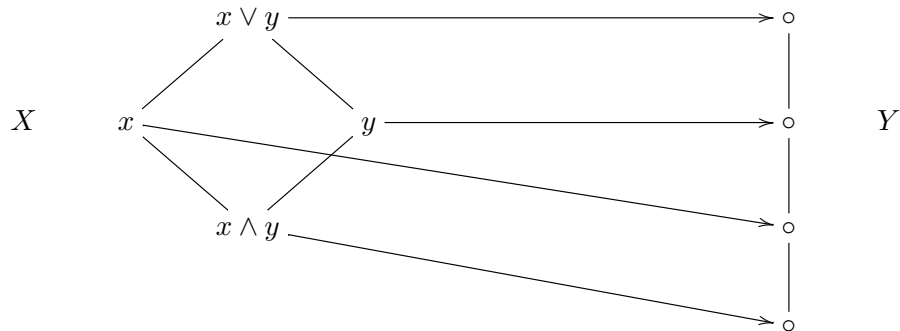
$$\begin{aligned} f(x_1 \wedge x_2) &= f(x_1) \wedge f(x_2) \\ f(x_1 \vee x_2) &= f(x_1) \vee f(x_2). \end{aligned}$$

**Tvrzení 9.3.1.** Každý homomorfismus svazů je izotonní zobrazení.

*Důkaz.* Buďte  $(X, \wedge, \vee), (Y, \wedge, \vee)$  svazy,  $f: X \rightarrow Y$  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 9.3.2.** *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.

▷

## 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>.