

7. května 2026

Algebra I, II

2025/2026

Zdeněk Kočan

Tento text je studijní opora k předmětům Algebra I a Algebra II pro studenty bakalářských studijních programů v akademickém roce 2025/2026. Máte-li k textu nějaké dotazy, připomínky, náměty, nebo narazíte-li na nějakou chybu, nepřesnost nebo překlep, prosím, napište mi na zdenek.kocan@math.slu.cz.

OBSAH

1	Matice	1
1.1	Matice	1
1.2	Operace s maticemi	4
1.3	Elementární úpravy a speciální tvary matic	13
1.4	Inverzní matice	18
1.5	Hodnost matice	21
2	Determinant	27
2.1	Permutace	27
2.2	Determinant	27
2.3	Adjungovaná matice	38
3	Soustavy lineárních rovnic	41
3.1	Soustavy lineárních rovnic a jejich řešení	41
3.2	Gaussova eliminační metoda a obecné řešení	44
3.3	Frobeniova věta	48
3.4	Cramerovo pravidlo	49
3.5	Homogenní soustavy lineárních rovnic	51
3.6	Nehomogenní soustavy lineárních rovnic	55
4	Polynomy	59
4.1	Polynomy, algebraické vlastnosti, dělitelnost	59
4.2	Největší společný dělitel	64
4.3	Ireducibilní polynomy	67
4.4	Kořeny a jejich násobnost	68
4.5	Polynomy s reálnými koeficienty	70
4.6	Derivace	72
4.7	Hornerovo schéma	73
5	Grupy	75
5.1	Binární operace	75
5.2	Grupy	77
5.3	Podgrupy	78
5.4	Podgrupy aditivní grupy $\mathbb{Z}$	79
5.5	Faktorové grupy	79
5.6	Zbytkové třídy	82
6	Okruhy a pole	85
7	Uspořádání a svazy	89
7.1	Uspořádané množiny	89
7.2	Svazově uspořádané množiny a svazy	91
7.3	Úplné svazy	93
8	Homomorfismy	95
8.1	Homomorfismy a izomorfismy grup	95
8.2	Homomorfismy a izomorfismy polí	97
8.3	Izotonní zobrazení, homomorfismy a izomorfismy svazů	97
9	Vektorové prostory	99
9.1	Definice, příklady, základní vlastnosti	99
9.2	Lineární kombinace, generátory, lineární nezávislost	100
9.3	Báze	106
9.4	Souřadnice	108
9.5	Orientace vektorového prostoru	111
9.6	Přímý součet vektorových prostorů	111
10	Vektorové podprostory	113
10.1	Definice, příklady, základní vlastnosti	113

10.2	Průnik a součet podprostorů	114
10.3	Přímý součet podprostorů	116
10.4	Popis podprostorů P^n homogenními soustavami	118
11	Lineární zobrazení	119
11.1	Definice, příklady	119
11.2	Jádro a obraz	121
11.3	Izomorfismy	123
11.4	Matice lineárního zobrazení	124
11.5	Determinant	128
11.6	Algebraická struktura na množině lineárních zobrazení	129
12	Vlastní vektory	133
12.1	Definice, příklady	133
12.2	Výpočet vlastních čísel a vlastních vektorů	134
12.3	Diagonalizovatelné transformace	137
13	Jordanův kanonický tvar	143
13.1	První rozklad lineární transformace	143
13.2	Druhý rozklad lineární transformace	148
13.3	Jordanův tvar matice a kritérium podobnosti matic	155
14	Skalární součin	157
14.1	Délka (norma) vektoru	158
14.2	Nerovnosti	159
14.3	Odchylka vektorů	161
14.4	Ortogonalita (kolmost)	161
14.5	Souřadnice vzhledem k ortonormální bázi	162
14.6	Kolmost množin	163
14.7	Ortogonální doplněk	164
14.8	Ortogonální projekce	164
14.9	Gramova-Schmidtova ortogonalizace	165
14.10	Vlastnosti ortogonálního doplňku	166
14.11	Shodnosti—ortogonální a unitární transformace a matice	167
15	Bilineární a kvadratické formy	173
15.1	Bilineární formy	173
15.2	Matice bilineární formy	173
15.3	Symetrické a antisymetrické bilineární formy	175
15.4	Kvadratické formy	176
15.5	Kanonické tvary	177
15.6	Pozitivní definitnost	179
16	Tenzory	183

POLE

Uvažujme množinu všech reálných čísel. Reálná čísla sčítáme a násobíme, přičteme-li k reálnému číslu nulu, dostaneme stejné číslo, vynásobíme-li reálné číslo jedničkou, dostaneme stejné číslo, 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 kapitole 6, ale už před tím budeme využívat některé vlastnosti pole, například, že $0 \cdot x = x \cdot 0 = 0$ pro každé x z pole, nebo že součin nenulových prvků pole je také různý od nuly.

1. MATICE

1.1. Matice

Definice 1.1.1. Buď P pole, buďte m, n přirozená čísla. *Matice* typu $m \times n$ nad polem P je tabulka o m řádcích a n sloupcích obsahující na každém místě nějaký prvek pole P (a nic jiného). Máme-li takovou matici A , pak prvek pole P v i -tém řádku a j -tém 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° . To, že matice A je tvořena řádky $A_\circ^i$, resp. sloupky A_j° , budeme někdy zapisovat

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

Definice 1.1.2. 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 1.1.3. 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_i^i jsou také *diagonální* a tvoří *hlavní diagonálu*),
- *jednotková*, jestliže je diagonální a $A_i^i = 1$ pro každé i (označujeme ji E_n nebo jen E),
- *nulová*, jestliže má všechny prvky nulové (označujeme ji $0_{m \times n}$ nebo jen 0),
- *horní* resp. *dolní trojúhelníková* (nebo v *horním* resp. *dolním trojúhelníkovém tvaru*), jestliže je čtvercová a pod resp. nad diagonálou má jen nuly, tedy $A_j^i = 0$ pro $i > j$ resp. pro $i < j$,
- *schodovitá* (nebo ve *schodovitém tvaru* nebo také *odstupňovaném 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 buď nulová, nebo jednotková, nebo rovna matici

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

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

- *blokově diagonální*, jestliže je rovna matici

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix},$$

kde $k > 1$, $A_1, \dots, A_k$ jsou čtvercové matice (bloky) a 0 označují nulové matice příslušných typů.

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

Příklad. (1)

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

(2)

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

(3)

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

(4)

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

(5)

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

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

(6)

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

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

(7)

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

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

(8)

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

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

□

1.2. Operace s maticemi

1.2.1. Součet matic a násobek matice

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

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

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

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

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

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

Příklad. Pro

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

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

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

□

Cvičení. Spočtěte

$$\begin{array}{ll}
 \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix} & \begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \\
 \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ -2 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \\
 \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ -2 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \\
 \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} -1 & -2 \\ -3 & -4 \end{pmatrix}.
 \end{array}
 \quad \square$$

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

- | | |
|-----------------------------------|----------------------------|
| (1) $A + B = B + A$, | (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 sloupku matice $A + (B + C)$ je

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

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

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

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

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

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

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 ji lze formulovat pro sloupky, uspořádané n -tice a matice.

Definice 1.2.3. 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.

Příklad. Mějme

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

Pro $A_{\circ}^1, A_{\circ}^3, A_{\circ}^6$ a $c_1 = 2, c_2 = -1, c_3 = 2$ dostaneme

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

$\square$

1.2.2. Součin

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

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

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

$$\begin{aligned}
 AB &= \begin{pmatrix} A_1^1 B_1^1 + A_2^1 B_1^2 + \cdots + A_n^1 B_1^n & \cdots & A_1^1 B_p^1 + A_2^1 B_p^2 + \cdots + A_n^1 B_p^n \\ A_1^2 B_1^1 + A_2^2 B_1^2 + \cdots + A_n^2 B_1^n & \cdots & A_1^2 B_p^1 + A_2^2 B_p^2 + \cdots + A_n^2 B_p^n \\ \vdots & & \vdots \\ A_1^m B_1^1 + A_2^m B_1^2 + \cdots + A_n^m B_1^n & \cdots & A_1^m B_p^1 + A_2^m B_p^2 + \cdots + A_n^m B_p^n \end{pmatrix} = \\
 &= \begin{pmatrix} A_1^1 B_o^1 + A_2^1 B_o^2 + \cdots + A_n^1 B_o^n \\ A_1^2 B_o^1 + A_2^2 B_o^2 + \cdots + A_n^2 B_o^n \\ \vdots \\ A_1^m B_o^1 + A_2^m B_o^2 + \cdots + A_n^m B_o^n \end{pmatrix} = \\
 &= \begin{pmatrix} A_o^1 B \\ A_o^2 B \\ \vdots \\ A_o^m B \end{pmatrix} = \\
 &= (B_1^1 A_o^1 + B_1^2 A_o^2 + \cdots + B_1^n A_o^n \quad \cdots \quad B_p^1 A_o^1 + B_p^2 A_o^2 + \cdots + B_p^n A_o^n) = \\
 &= (AB_1^o \quad AB_2^o \quad \cdots \quad AB_p^o).
 \end{aligned}$$

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

Obdobně získáme ostatní řádky matice AB . Obecně, i -tý řádek matice AB získáme tak, že pro každé $k \in \{1, 2, \dots, n\}$ 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 , jinými slovy, součin i -tého řádku matice A , řádek je matice typu $1 \times n$, a matice B .

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

Obdobně získáme ostatní sloupky matice AB . Obecně, j -tý sloupek matice AB získáme tak, že pro každé $k \in \{1, 2, \dots, n\}$ 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 , jinými slovy, součin matice A a j -tého sloupku matice B , sloupek je matice typu $n \times 1$.

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

Příklad. (1) Pro

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

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

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

(2) Pro

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

(3) Pro

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

□

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

Cvičení. Spočtete

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

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

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

(3) Součin diagonálních matic je diagonální matice.

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

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

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

i -tý řádek matice A je

$$A_{\circ}^i = (0 \quad \dots \quad 0 \quad A_{i_1}^i \quad \dots \quad A_{i_m}^i \quad 0 \quad \dots \quad 0),$$

čili $A_j^i = 0$ pro $j < i_1$ a $j > i_m$.

j -tý sloupek matice B je

$$B_j^{\circ} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ B_j^{j_1} \\ \vdots \\ B_j^{j_n} \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

čili $B_j^i = 0$ pro $i < j_1$ a $i > j_n$.

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

$$(AB)_j^i = \sum_k A_k^i B_j^k = 0,$$

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

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

$$\begin{array}{ll} (1) \ A(BC) = (AB)C, & (4) \ (A+B)C = AC + BC, \\ (2) \ AE = EA = A, & (5) \ c(AB) = (cA)B = A(cB). \\ (3) \ A(B+C) = AB + AC, \end{array}$$

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 $m \times q$.

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

(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

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

1.2.3. Transponování

Definice 1.2.5. *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.

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

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

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

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) Bud' 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. $\square$

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

Definice 1.2.6. Čtvercová matice A typu $n \times n$ je

- *symetrická*, je-li $A_j^i = A_i^j$ pro libovolné $i, j \in \{1, 2, \dots, n\}$, tedy $A^\top = A$,
- *antisymetrická*, je-li $A_j^i = -A_i^j$ pro libovolné $i, j \in \{1, 2, \dots, n\}$, tedy $A^\top = -A$.

1.3. Elementární úpravy a speciální tvary matic

1.3.1. Elementární úpravy

Definice 1.3.1. Mějme matici nad polem P . *Řádkové elementární úpravy* matice jsou

- (1) přičtení c -násobku j -tého řádku k i -tému řádku, kde $c \in P$ a $i \neq j$,
- (2) vynásobení i -tého řádku nenulovým prvkem $c \in P$,
- (3) vzájemná výměna i -tého řádku a j -tého řádku.

Sloupkové elementární úpravy matice definujeme analogicky.

Cvičení. Proved'te vzájemnou výměnu dvou řádků pomocí konečně mnoha úprav typů (1) a (2). $\square$

Mějme matici A . Přičtením c -násobku j -tého řádku k i -tému řádku změníme 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

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

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

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

Inverzní úpravy ke sloupkovým úpravám jsou obdobné.

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

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

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

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

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

Příklad.

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

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

Důkaz. Cvičení. $\square$

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

Připomeňme si definice z podkapitoly 1.1.

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

Z toho plyne, že v matici ve schodovitém tvaru všechny řádky pod nulovým řádkem jsou nulové.

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

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

Definice 1.3.5. Matice je v *Gaussově kanonickém tvaru*, jestliže je buď nulová, nebo jednotková, nebo rovna matici

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

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

Příklad. (1) Necht

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

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

(2) Každá nulová matice je ve schodovitém tvaru i v Gaussově–Jordanově tvaru i v Gaussově kanonickém tvaru. $\square$

Definice 1.3.6. Mějme nenulovou matici. *Gaussova eliminace* je úprava matice podle následujícího algoritmu.

Buď $i = 1$.

- (1) Uvažujme první 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 sloupek, který má nějaký nenulový prvek v i -tém nebo nižším řádku, vraťme se do bodu (1). Jestliže takový sloupek neexistuje, algoritmus končí.

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

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

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

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

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

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

Definice 1.3.8. Mějme nenulovou matici. *Gaussova–Jordanova eliminace* je úprava matice podle následujícího algoritmu.

Buď $i = 1$.

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

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

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

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

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

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

Důkaz. Pro nulovou matici a jednotkovou matici není co dokazovat. Libovolnou jinou matici lze převést na ekvivalentní matici v Gaussově kanonickém tvaru s použitím řádkových i sloupkových elementárních úprav a pomocí algoritmu, který získáme vhodnou úpravou Gaussovy–Jordanovy eliminace. Podrobnosti ponecháme jako cvičení. $\square$

1.3.3. Elementární matice

Definice 1.3.9. Elementární matice jsou:

(1) pro $i \neq j$

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

(2) pro $c \neq 0$

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

(3) pro $i \neq j$

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

Lemma 1.3.5. Transponované matice k elementárním maticím jsou elementární matice.

Důkaz. Cvičení. $\square$

Tvrzení 1.3.6. Buď A matice typu $m \times n$.

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

Je-li $E^{i,j}(c)$ typu $m \times m$, matice $E^{i,j}(c) \cdot A$ se rovná matici, která vznikne z matice A přičtením c -násobku j -tého řádku k i -tému řádku.

Je-li $E^{i,j}(c)$ typu $n \times n$, matice $A \cdot (E^{i,j}(c))^T$ se rovná matici, která vznikne z matice A přičtením c -násobku j -tého sloupku k i -tému sloupku.

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

Je-li $E^i(c)$ typu $m \times m$, matice $E^i(c) \cdot A$ se rovná matici, která vznikne z matice A vynásobením i -tého řádku prvkem c .

Je-li $E^i(c)$ typu $n \times n$, matice $A \cdot (E^i(c))^T$ se rovná matici, která vznikne z matice A vynásobením i -tého sloupku prvkem c .

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

Je-li $E^{i,j}$ typu $m \times m$, matice $E^{i,j} \cdot A$ se rovná matici, která vznikne z matice A výměnou i -tého řádku a j -tého řádku.

Je-li $E^{i,j}$ typu $n \times n$, matice $A \cdot (E^{i,j})^T$ se rovná matici, která vznikne z matice A výměnou i -tého sloupku a j -tého sloupku.

Důkaz. Cvičení (např. viz komentář za Definicí 1.2.4 součinu matic). □

Důsledek. Buďte A čtvercová matice a Q elementární matice stejného typu. Potom QA znamená provedení příslušné řádkové úpravy matice A a AQ^T znamená provedení stejné sloupkové úpravy matice A .

Důkaz. Cvičení. □

Tvrzení 1.3.7. Buďte A symetrická (antisymetrická) matice a Q elementární matice stejného typu. Potom QAQ^T je symetrická (antisymetrická) matice.

Důkaz. Cvičení. □

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

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

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

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

1.4. Inverzní matice

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

$$AX = XA = E.$$

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

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

(2)

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

(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) Necht

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

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

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

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

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

Tvrzení 1.4.2. Necht $A, A_1, \dots, A_n$ 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 1.4.3. *Nechť A, B jsou čtvercové matice stejného typu 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 čtvercová matice 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 1.4.4. *Matice je invertibilní právě tehdy, když je řádkově ekvivalentní s jednotkovou maticí.*

Důkaz. „ $\Rightarrow$ “ Nechť A je invertibilní matice. Řádkovými elementárními úpravami ji převedeme 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 1.4.3 je A invertibilní a $A^{-1} = Q$. $\square$

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

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

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

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

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

Příklad. Vypočítejme inverzní matici k matici

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

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

Takže A je invertibilní a

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

□

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. □

Cvičení. Pokud existují, spočítejte inverzní matice k maticím

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

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

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

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

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

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

□

1.5. Hodnost matice

1.5.1. Lineární nezávislost

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

Definice 1.5.1. Množina řádků $\{A_{\circ}^{i_1}, A_{\circ}^{i_2}, \dots, A_{\circ}^{i_k}\}$ 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 1.5.1. Množina řádků je lineárně závislá právě tehdy, když aspoň jeden z nich je lineární kombinací ostatních.

Důkaz. Předpokládejme, že množina řádků $\{A_{\circ}^{i_1}, A_{\circ}^{i_2}, \dots, A_{\circ}^{i_k}\}$ 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

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

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. $\square$

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. $\square$

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 $cA_{\circ}^i = 0$, 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. $\square$

1.5.2. Hodnost matice

Definice 1.5.2. *Hodnost* matice je maximální počet prvků lineárně nezávislé množiny 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 poznamenáme 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. $\square$

Cvičení. Spočtěte hodnosti matic

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

$$(6)$$

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

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

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

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

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

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

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

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

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

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

$\square$

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

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

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

Tvrzení 1.5.3. Buďte $A_{\circ}^1, A_{\circ}^2, \dots, A_{\circ}^m$ 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 $\{A_{\circ}^1, A_{\circ}^2, \dots, A_{\circ}^m\}$ vyplývá, že všechny koeficienty poslední lineární kombinace jsou nulové, tj. $c_1 = \dots = c_i = \dots = cc_i + c_j = \dots = c_m = 0$. Z toho dostaneme, že i $c_j = 0$, a množina $\{B_{\circ}^1, B_{\circ}^2, \dots, B_{\circ}^m\}$ 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 $c_1 B_o^1 + \dots + c_m B_o^m = 0_o$. Takže

$$\begin{aligned} c_1 B_o^1 + \dots + c_m B_o^m &= \\ &= (\sum_k c_k A_1^k \dots \sum_k c_k (A_i^k + cA_j^k) \dots \sum_k c_k A_j^k \dots \sum_k c_k A_n^k) = \\ &= (\sum_k c_k A_1^k \dots \sum_k c_k A_i^k + c \sum_k c_k A_j^k \dots \sum_k c_k A_j^k \dots \sum_k c_k A_n^k) = \\ &= (0 \dots 0 \dots 0 \dots 0) \end{aligned}$$

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

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

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

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

(8) *Maximální počet prvků lineárně nezávislých množin sloupků matice je roven maximálnímu počtu prvků lineárně nezávislých množin jejích řádků, tj. 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 1.5.3. 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 1.5.4. Matice je regulární právě tehdy, když je řádkově ekvivalentní s jednotkovou maticí.

Důkaz. Cvičení. □

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

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

(3) Součin regulárních matic je regulární matice.

(4) Vynásobení regulární maticí zleva nemění hodnotu.

(5) Vynásobení regulární maticí zprava nemění hodnotu.

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

Důkaz. „ $\Rightarrow$ “ 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 1.5.6. 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 $\text{rank } S_A S_B \leq \text{rank } S_B = \text{rank } B$. $\square$

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

2. DETERMINANT

2.1. Permutace

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

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

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

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

Nechť $I_n = \{1, 2, \dots, n\}$. 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 2.1.3. Buď $\sigma \in S_n$. Nechť $i, j \in I_n$ jsou takové, že $i < j$ a $\sigma_i > \sigma_j$. Pak dvojice (σ_i, σ_j) tvoří *inverzi* permutace σ .

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

Definice 2.1.4. *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 2.1.2. *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].

2.2. Determinant

2.2.1. Definice a determinanty některých typů matic

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

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

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 σ 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 σ 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:

$$\begin{array}{c} \oplus \quad \ominus \\ \swarrow \quad \searrow \\ \begin{vmatrix} A_1^1 & A_2^1 \\ A_1^2 & A_2^2 \end{vmatrix} \\ \swarrow \quad \searrow \\ \end{vmatrix} = A_1^1 A_2^2 - A_2^1 A_1^2$$

(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):

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

(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. $\square$

Cvičení. Spočítejte determinanty matic

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

$\square$

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

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

Lemma 2.2.2. *Pro matice lišící se pouze v jednom řádku platí*

$$\begin{vmatrix} A_1^1 & \cdots & A_n^1 \\ \vdots & & \vdots \\ A_1^{i-1} & \cdots & A_n^{i-1} \\ A_1^i & \cdots & A_n^i \\ A_1^{i+1} & \cdots & A_n^{i+1} \\ \vdots & & \vdots \\ A_1^n & \cdots & A_n^n \end{vmatrix} + \begin{vmatrix} A_1^1 & \cdots & A_n^1 \\ \vdots & & \vdots \\ A_1^{i-1} & \cdots & A_n^{i-1} \\ B_1^i & \cdots & B_n^i \\ A_1^{i+1} & \cdots & A_n^{i+1} \\ \vdots & & \vdots \\ A_1^n & \cdots & A_n^n \end{vmatrix} = \begin{vmatrix} A_1^1 & \cdots & A_n^1 \\ \vdots & & \vdots \\ A_1^{i-1} & \cdots & A_n^{i-1} \\ A_1^i + B_1^i & \cdots & A_n^i + B_n^i \\ A_1^{i+1} & \cdots & A_n^{i+1} \\ \vdots & & \vdots \\ A_1^n & \cdots & A_n^n \end{vmatrix}.$$

Důkaz. Cvičení. $\square$

Příklad.

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

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

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

Tvrzení 2.2.3. *Determinant trojúhelníkové matice je roven součinu prvků na diagonále.*

Důkaz. Buď A horní trojúhelníková matice typu $n \times n$. Buď σ 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 σ 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 schodovitěm 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.

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

Determinanty elementárních matic jsou nenulové.

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

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

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

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

(3) Jelikož v každém řádku a v každém sloupku matice $E^{i,j}$ je právě jedna jednička a ostatní prvky jsou nuly, existuje jediná permutace τ 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 τ transpozice, takže $\operatorname{sgn} \tau = -1$. Proto

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

Tvrzení 2.2.4. 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 $A_{\sigma_1^{-1}}^1 \cdots A_{\sigma_i^{-1}}^i \cdots A_{\sigma_n^{-1}}^n$, protože σ_i^{-1} -tý činitel v původním součinu je

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

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

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

Tvrzení 2.2.5. 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 σ' je

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

a je tedy opačný k členu odpovídajícímu permutaci σ .

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

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

2.2.2. Elementární úpravy

Tvrzení 2.2.6. (1) *Přičtením násobku jednoho řádku, resp. sloupku k jinému řádku, resp. sloupku se determinant nezmění, čili*

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

při zápisu s použitím elementárních matic

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

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

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

při zápisu s použitím elementárních matic

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

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

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

při zápisu s použitím elementárních matic

$$\det(E^{i,j} \cdot A) = \det(A \cdot E^{i,j}) = -\det A.$$

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

Buďte A čtvercová matice a B upravená matice.

(1) Necht' 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) Necht' 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) Necht' 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 . Buď $\tau_{ij} \in S_n$ transpozice vyměňující i, j , čili $\operatorname{sgn} \tau_{ij} = -1$. Pro každou permutaci $\sigma \in S_n$ označme $\sigma' = \sigma \circ \tau_{ij}$. Pak $\sigma'_i = \sigma_j$, $\sigma'_j = \sigma_i$ a $\sigma'_k = \sigma_k$ pro $k \neq i, j$ a $\operatorname{sgn} \sigma' = \operatorname{sgn} \sigma \cdot \operatorname{sgn} \tau_{ij} = -\operatorname{sgn} \sigma$. Potom

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

protože když σ projde všechny prvky S_n , tak σ' také. □

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

Cvičení. Buď A antisymetrická matice typu $n \times n$. Ukažte, že je-li n liché číslo, pak $\det A = 0$. □

Příklad.

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

Důsledek. *Bud' 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) $\det(E^{i,j}A) = (-1) \cdot \det A = \det E^{i,j} \cdot \det A$. $\square$

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. $\square$

Tvrzení 2.2.7. *Matice je regulární právě tehdy, když má nenulový determinant.*

Důkaz. Buď A regulární matice. Podle Důsledku Tvrzení 1.5.4 $A = Q_1 Q_2 \cdots Q_k$, kde $Q_1, Q_2, \dots, Q_k$ jsou elementární matice. Potom díky Důledku Tvrzení 2.2.6

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

A součin nenulových determinantů elementárních matic není roven nule, viz kapitola 6.

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 opět díky Důledku Tvrzení 2.2.6 a díky tomu, že součin nenulových prvků pole je nenulový,

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

Jelikož B je ve schodovitém tvaru a její determinant je tedy součinem prvků na diagonále, na diagonále není žádná nula, opět viz kapitola 6. 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 2.2.8 (Cauchyova věta). *Bud' 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 Tvzení 1.5.5 je AB také singulární a tedy

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

Cvičení. Pro regulární matici A platí $\det A^{-1} = 1/\det A$. $\square$

Lemma 2.2.9. *Každá čtvercová matice je ekvivalentní matici v trojúhelníkovém tvaru, jejíž determinant je roven determinantu původní matice.*

Důkaz. Na převedení matice na trojúhelníkový tvar stačí pouze dva typy elementárních úprav, přičtení násobku jednoho řádku, nebo sloupku k jinému řádku, resp. sloupku, což nemění determinant, a vzájemná výměna dvou řádků, nebo dvou sloupků, čímž se změní jen znaménko determinantu.

Pokud při takovém převedení matice na trojúhelníkový tvar použijeme sudý počet výměn řádků, nebo sloupků, determinant získané matice v trojúhelníkovém tvaru je roven determinantu původní matice. Pokud použijeme lichý počet takových výměn, vynásobíme jeden řádek získané matice prvkem -1 a determinant této nové matice v trojúhelníkovém tvaru je roven determinantu původní matice. $\square$

Lemma 2.2.10.

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

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.

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

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

2.2.3. Laplaceův rozvoj

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

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

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

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

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

Příklad. Mějme

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

Potom

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

$$\hat{A}_1^1 = (-1)^{1+1} \bar{A}_1^1 = d,$$

$$\hat{A}_2^1 = (-1)^{1+2} \bar{A}_2^1 = -c,$$

$$\hat{A}_1^2 = (-1)^{2+1} \bar{A}_1^2 = -b,$$

$$\hat{A}_2^2 = (-1)^{2+2} \bar{A}_2^2 = a. \quad \square$$

Příklad. Mějme

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

Potom

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

$$\hat{A}_1^1 = (-1)^{1+1} \bar{A}_1^1 = \begin{vmatrix} e & f \\ h & i \end{vmatrix},$$

$$\hat{A}_2^1 = (-1)^{1+2} \bar{A}_2^1 = - \begin{vmatrix} d & f \\ g & i \end{vmatrix},$$

$$\hat{A}_3^1 = (-1)^{1+3} \bar{A}_3^1 = \begin{vmatrix} d & e \\ g & h \end{vmatrix},$$

$$\hat{A}_3^3 = (-1)^{3+3} \bar{A}_3^3 = \begin{vmatrix} a & b \\ d & e \end{vmatrix}. \quad \square$$

Tvrzení 2.2.11 (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.

$$\begin{aligned}
 \det A &= \begin{vmatrix} A_1^1 & \dots & A_{j-1}^1 & A_j^1 & A_{j+1}^1 & \dots & A_n^1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^i & \dots & A_{j-1}^i & A_j^i & A_{j+1}^i & \dots & A_n^i \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^n & \dots & A_{j-1}^n & A_j^n & A_{j+1}^n & \dots & A_n^n \end{vmatrix} = & \quad (\text{Lemma 2.2.2}) \\
 &= \sum_{j=1}^n \begin{vmatrix} A_1^1 & \dots & A_{j-1}^1 & A_j^1 & A_{j+1}^1 & \dots & A_n^1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & A_j^i & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^n & \dots & A_{j-1}^n & A_j^n & A_{j+1}^n & \dots & A_n^n \end{vmatrix} = \\
 &= \sum_{j=1}^n A_j^i \begin{vmatrix} A_1^1 & \dots & A_{j-1}^1 & A_j^1 & A_{j+1}^1 & \dots & A_n^1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_1^n & \dots & A_{j-1}^n & A_j^n & A_{j+1}^n & \dots & A_n^n \end{vmatrix}.
 \end{aligned}$$

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 $\begin{pmatrix} 1 & A_j^1 & \dots & A_j^{i-1} & A_j^{i+1} & \dots & A_j^n \end{pmatrix}^\top$ s předchozími sloupky tak dlouho, až bude prvním sloupkem; k tomu je potřeba $j - 1$ výměn. Takto vzniklý determinant je tedy nutné vynásobit číslem $(-1)^{i-1}(-1)^{j-1} = (-1)^{i+j}$ a navíc, viz Lemma 2.2.10, 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 2.2.4. Vztah v Laplaceově větě je *Laplaceův rozvoj podle i -tého řádku* resp. *podle i -tého sloupku*.

Příklad.

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

$\square$

2.3. Adjungovaná matice

Definice 2.3.1. Buď A čtvercová matice. Označme $\hat{A}$ matici kofaktorů $\hat{A}_j^i$. Matice $\hat{A}^\top$ je matice *adjungovaná* k matici A a značí se $\text{adj } A$. Tedy,

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

Příklad. Mějme

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

Potom

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

Tvrzení 2.3.1. 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

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

Pro $i = j$ podle Laplaceovy věty

$$(A \cdot \text{adj } A)_i^i = \sum_k A_k^i \hat{A}_k^i = \det A.$$

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

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

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 1.4.3 dostaneme uvedený vztah. $\square$

Příklad. Mějme regulární matici

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

Potom

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

Například pro

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

dostaneme

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

□

3. SOUSTAVY LINEÁRNÍCH ROVNIC

3.1. Soustavy lineárních rovnic a jejich řešení

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

Uvedenou lineární rovnici můžeme zapsat

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

Definice 3.1.2. *Řešení rovnice*

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

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 ξ^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. $\square$

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

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

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

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

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

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

Definice 3.1.3. 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 necht' $a_j^i, b^i \in P$, $x^1, x^2, \dots, x^n \notin P$. Potom

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

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

$\vdots$

$$a_1^mx^1 + a_2^mx^2 + \dots + a_n^mx^n = b^m$$

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

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

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

Definice 3.1.5. *Řešení soustavy*

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

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

$\vdots$

$$a_1^m x^1 + a_2^m x^2 + \dots + a_n^m x^n = b^m$$

m lineárních rovnic nad polem P 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 $\xi = (\xi^1 \quad \xi^2 \quad \dots \quad \xi^n)^\top$ taková, že platí rovnost

$$A\xi = b.$$

Součin Ax si můžeme rozepsat

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

a soustavu $Ax = b$ pak můžeme přepsat

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

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

$$a_1 x^1 + a_2 x^2 = b$$

s reálnými koeficienty o dvou neznámých x^1, x^2 jsou uspořádané dvojice (ξ^1, ξ^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. $\square$

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 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 $\emptyset$. $\square$

3.2. Gaussova eliminační metoda a obecné řešení

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

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

Definice 3.2.2. *Elementární úpravy* soustavy lineárních rovnic jsou

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

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

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

Podle následujícího tvrzení elementární úpravy jsou ekvivalentní.

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

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

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

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 ξ je řešením i této nové soustavy, protože je řešením nové i -té rovnice

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

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 ξ je řešením původní soustavy, tedy $A\xi = b$, potom $QA\xi = Qb$ a ξ 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). Je zřejmé, že počet nenulových řádků příslušné upravené matice soustavy není větší než počet neznámých, čili počet sloupků matice soustavy. Jestliže upravená rozšířená matice soustavy má více (o jeden) nenulových řádků než příslušná matice soustavy, soustava (upravená i původní) nemá řešení. Jestliže počty nenulových řádků upravené rozšířené matice soustavy i příslušné matice soustavy se rovnají r ($r \leq n$), tj. rozšířená matice soustavy a matice soustavy mají stejné hodnoty, příslušná soustava rovnic (uvádíme jen ty nenulové) je

$$\begin{aligned} x^{k_1} + \dots + 0 + \dots + 0 + c_{k_r+1}^1 x^{k_r+1} + \dots + c_n^1 x^n &= d^1 \\ &\vdots \\ x^{k_{r-1}} + \dots + 0 + c_{k_r+1}^{r-1} x^{k_r+1} + \dots + c_n^{r-1} x^n &= d^{r-1} \\ x^{k_r} + c_{k_r+1}^r x^{k_r+1} + \dots + c_n^r x^n &= d^r. \end{aligned}$$

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

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

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

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

Takto můžeme postupovat až k první rovnici, ze které vyjádříme x^{k_1} pomocí neznámých $x^{k_1+1}, \dots, x^n$ kromě $x^{k_2}, \dots, x^{k_r}$.

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

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

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

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

Příklad. Mějme soustavu

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

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

$$3x^1 + 4x^2 + 5x^3 = 1$$

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

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

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

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

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

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

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

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

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

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

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

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 $(-1, 1, 0)$, který je dán sloupcem pravých stran soustavy v Gaussově–Jordanově tvaru, se směrovým vektorem $(1, -2, 1)$. Při maticovém zápisu množina všech řešení je

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

Příklad. Mějme soustavu

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

nad polem reálných čísel. Rozšířená matice soustavy je

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

Její Gaussův–Jordanův tvar je

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

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

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

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

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

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

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

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

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

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

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

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

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

a množinu všech řešení soustavy pak můžeme zapsat

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

při maticovém zápisu

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

3.3. Frobeniova věta

Z předchozích pozorování a tvrzení vyplývá následující věta.

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

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

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

Příklad. (1) Soustava

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

má matici soustavy

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

a rozšířenou matici soustavy

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

Jejich 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

$$x = 0$$

$$x = 1$$

má matici soustavy

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

a rozšířenou matici soustavy

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

Hodnota matice soustavy je rovna 1 a hodnota rozšířené matice soustavy je rovna 2, takže podle Frobeniovy věty soustava nemá řešení. $\square$

3.4. Cramerovo pravidlo

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

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

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

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

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

Tvrzení 3.4.2 (Cramerovo pravidlo). *Bud' $Ax = b$ 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 :

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

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

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

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 ξ řešení soustavy $Ax = b$, pak b je lineární kombinací sloupků A_i° s koeficienty $\xi^1, \dots, \xi^n$, tedy

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

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

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

z čehož dostaneme požadovaný vztah. □

Příklad. Mějme soustavu

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

Potom

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

a

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

Proto

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

3.5. Homogenní soustavy lineárních rovnic

Definice 3.5.1. Soustava lineárních rovnic s nulovou pravou stranou je *homogenní*.

Příklad. (1) Soustava

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

je homogenní.

(2) Soustava

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

je homogenní.

(3) Soustava

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

není homogenní. □

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

(2) Každá homogenní soustava má nulové řešení.

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

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

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

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

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

(3) Vyplývá z Tvrzení 3.4.1.

(4) Tvrzení je ekvivalentní předchozímu.

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

Množina všech řešení homogenní soustavy lineárních rovnic má následující vlastnost.

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

Důkaz. Necht' $\xi_1, \xi_2, \dots, \xi_k$ jsou řešení soustavy $Ax = 0$, čili $A\xi_1 = 0, A\xi_2 = 0, \dots, A\xi_k = 0$. Buďte $\alpha_1, \alpha_2, \dots, \alpha_k \in P$. Potom

$$A(\alpha_1\xi_1 + \alpha_2\xi_2 + \dots + \alpha_k\xi_k) = \alpha_1A\xi_1 + \alpha_2A\xi_2 + \dots + \alpha_kA\xi_k = 0$$

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

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

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

Důkaz. Obecné řešení ξ soustavy $Ax = 0$ o n neznámých je vyjádřeno pomocí $n - \text{rank } A$ parametrů $t^1, \dots, t^{n-\text{rank } A}$, tedy $\xi = \xi(t^1, \dots, t^{n-\text{rank } A})$. 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 partikulárních řešení

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

která je lineárně nezávislá a

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

takže obecné řešení, čili každé řešení, soustavy je lineární kombinací těchto partikulárních řešení. $\square$

Příklad. (1) Soustava

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

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

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

množina všech řešení soustavy je

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

a fundamentální systém řešení soustavy je například

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

(2) Soustava

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

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

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

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

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

množina všech řešení soustavy je

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

a fundamentální systém řešení soustavy je například

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

(3) Soustava

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

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

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

množina všech řešení soustavy je

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

a 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 obecné řešení je

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

množina všech řešení soustavy je

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

a fundamentální systém řešení soustavy je $\emptyset$.

(5) Soustava

$$0x = 0$$

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

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

množina všech řešení soustavy je

$$\{t \mid t \in \mathbb{R}\} = \mathbb{R}$$

a fundamentální systém řešení soustavy je například

$$\{1\}.$$

□

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

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

je obecné řešení soustavy a

$$\{t^1 \xi_1 + t^2 \xi_2 + \dots + t^r \xi_r \mid t^1, t^2, \dots, t^r \in P\}$$

je množina všech řešení soustavy.

Homogenní soustava rovnic k zadanému fundamentálnímu systému řešení.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Tedy,

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

$$4a^1 + 3a^2 + 2a^3 + a^4 = 0.$$

Fundamentální systém řešení této soustavy je, například,

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

Zvolíme-li

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

dostaneme soustavu

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

tedy

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

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

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

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

je její obecné řešení a

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

je množina všech řešení soustavy. □

3.6. Nehomogenní soustavy lineárních rovnic

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

Příklad. (1) Soustava

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

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

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

je nehomogenní.

(2) Soustava

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

je nehomogenní. □

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

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

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

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

Důkaz. (1) Má-li soustava právě jedno řešení, potom žádná z neznámých není parametr a homogenizovaná soustava má jen nulové řešení.

(2) Vyplývá z předchozího bodu a z Gaussovy eliminační metody.

(3) Vyplývá z předchozího bodu a z Tvzení 3.5.1.

(4) Zřejmé. $\square$

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

Tvrzení 3.6.2. *Nechť ξ_p je nějaké řešení soustavy $Ax = b$. Potom pro každé řešení ξ této soustavy existuje jediné řešení ξ_0 homogenizované soustavy takové, že $\xi = \xi_p + \xi_0$.*

Na druhou stranu, pro libovolné řešení ξ_0 homogenizované soustavy je $\xi = \xi_p + \xi_0$ řešením soustavy $Ax = b$.

Důkaz. Buďte ξ_p a ξ 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, ξ_0 je řešení homogenizované soustavy a $\xi = \xi_0 + \xi_p$. Jednoznačnost ξ_0 je zřejmá.

Je-li $A\xi_0 = 0$, pak $A\xi = A(\xi_p + \xi_0) = A\xi_p + A\xi_0 = b + 0 = b$. $\square$

Důsledek. (1) *Má-li nehomogenní soustava řešení, potom její obecné řešení je součtem obecného řešení homogenizované soustavy a nějakého partikulárního řešení nehomogenní soustavy.*

(2) *Je-li ξ_p řešení soustavy $Ax = b$, potom množina všech řešení této soustavy je*

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

Cvičení. Rozdíl libovolných dvou řešení nehomogenní soustavy je řešení homogenizované soustavy. $\square$

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

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

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

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

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

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

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

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

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

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

□

4. POLYNOMY

4.1. Polynomy, algebraické vlastnosti, dělitelnost

Definice 4.1.1. Buď P pole, $n \in \mathbb{N}$, $a_0, \dots, a_n \in P$, $x \notin P$. *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*.

Polynom se všemi koeficienty nulovými je *nulový polynom* a označujeme ho 0.

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

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

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

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

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

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

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

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

Definice 4.1.3. *Stupeň* polynomu $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ 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 $\text{lc } f = 6$. $\square$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Speciálně, pokud $f = -1$, pak

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

je polynom *opačný* k polynomu g .

Příklad. Pro

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

je

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

$$fg = 6x^7 - 12x^6 - 3x^5 - 6x^4 + 3x^3 - 12x^2 - 6x. \quad \square$$

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

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

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 $a_n \neq 0$ a $b_m \neq 0$, také $a_n b_m \neq 0$, viz kapitola 6. Ovšem, $a_n b_m$ je $(n+m)$ -tý koeficient součinu fg , takže fg je 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 $\deg(fg) = n+m = \deg f + \deg g$. $\square$

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

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

- | | |
|-----------------------------------|---|
| (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) $f \cdot (g + h) = f \cdot g + f \cdot h$. |

Důkaz. Cvičení. □

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

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

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

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

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

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

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

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

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

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

Příklad. (1) $x \mid x^2 - x$, protože $x^2 - x = x(x - 1)$.

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

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

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

Tvrzení 4.1.5. *Buďte $f, g, h \in P[x]$.*

- (1) $f \mid f$ a $f \mid 0$.
- (2) Jestliže $f \mid g$ a $g \mid h$, pak $f \mid h$.
- (3) Jestliže $f \mid g$ a $f \mid h$, pak $f \mid (g + h)$.
- (4) Jestliže $f \mid g$, pak $f \mid (gh)$.
- (5) Jestliže $fg \mid fh$ a $f \neq 0$, pak $g \mid h$.

Důkaz. Cvičení. □

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

Tvrzení 4.1.6. *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 $f = 0$ nebo $\deg f < \deg g$, dvojice $q = 0$, $r = f$ splňuje podmínky (i) a (ii).

Předpokládejme, že $f \neq 0$ a $\deg f \geq \deg g$. Položme $q_0 = 0$ a $r_0 = f$ a pro $i \in \mathbb{N}$ taková, že $r_i \neq 0$ a $\deg r_i \geq \deg g$, definujme rekurzivně

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

Jelikož stupeň polynomu

$$\frac{\text{lc } r_i}{\text{lc } g} \cdot x^{\deg r_i - \deg g} \cdot g$$

je roven $\deg r_i$ a jeho vedoucí koeficient je roven $\text{lc } r_i$, tak buď $r_{i+1} = 0$ nebo $\deg r_{i+1} < \deg r_i$. Proto existuje i_0 takové, že buď $r_{i_0} = 0$ nebo $\deg r_{i_0} < \deg g$. Navíc, $f = gq_0 + r_0$ a je-li $f = gq_i + r_i$ pro nějaké i , potom také $f = gq_{i+1} + r_{i+1}$. Takže dvojice $q = q_{i_0}$, $r = r_{i_0}$ splňuje podmínky (i) a (ii).

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

$$f = gq_1 + r_1 \quad f = gq_2 + r_2 \quad (1)$$

$$\text{buď } r_1 = 0 \text{ nebo } \deg r_1 < \deg g \quad \text{buď } r_2 = 0 \text{ nebo } \deg r_2 < \deg g. \quad (2)$$

Předpokládejme, že $r_2 - r_1 \neq 0$. Podle (1)

$$gq_1 + r_1 = gq_2 + r_2 \quad \text{tedy } g(q_1 - q_2) = r_2 - r_1 \quad \text{a } \deg g \leq \deg(r_2 - r_1), \quad (3)$$

zatímco z (2) vyplývá, že

$$\deg(r_2 - r_1) < \deg g. \quad (4)$$

Na základě předpokladu $r_2 - r_1 \neq 0$ dostáváme spor, takže $r_2 - r_1 = 0$, čili $r_1 = r_2$. Vzhledem k tomu, že $g \neq 0$, z $g(q_1 - q_2) = 0$ vyplývá, že $q_1 - q_2 = 0$, čili $q_1 = q_2$. □

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

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

Příklad. 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

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

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

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

Tedy

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

Definice 4.1.10. Nenulový polynom, jehož vedoucí koeficient je 1, je *normovaný*.

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 4.1.7. *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.

4.2. Největší společný dělitel

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

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

Zapisujeme $d = D(f, g)$.

Definice 4.2.2. Polynomy, jejichž největší společný dělitel je 1, jsou *nesoudělné*.

Příklad. (1) $D(2x, x^2) = x$.

(2) Polynomy x a $x + 1$ jsou nesoudělné. Oba polynomy jsou stupně 1, proto jejich dělitele jsou stupně buď 1 nebo 0. Lineární dělitele polynomu x jsou cx , kde $c \in P$, ale žádný z nich není dělitelem $x + 1$. Společné dělitele polynomů x a $x + 1$ jsou tedy jen nenulové konstantní polynomy a jelikož největší společný dělitel je navíc normovaný, $D(x, x + 1) = 1$.

(3) Největší společný dělitel polynomů $f = g = 0$ neexistuje.

(4) Pro $f \neq 0$ $D(f, 0) = \bar{f}$. □

Tvrzení 4.2.1 (Eukleidův algoritmus). *Buďte $f, g \in P[x]$ nenulové polynomy. Buď $r_0, r_1, r_2, r_3, \dots$ 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 4.2.2. *Pro libovolné dva polynomy, z nichž aspoň jeden je nenulový, existuje právě jeden jejich největší společný dělitel.*

Důkaz. Buďte $f, g \in P[x]$. Je-li $f \neq 0$ a $g = 0$, $D(f, 0) = \bar{f}$. Předpokládejme, že f, g jsou nenulové, a aplikujme Eukleidův algoritmus. Buď $N \in \mathbb{N}$ takové, že $r_{N-1} \neq 0$ a $r_N = 0$.

Označme $d = \bar{r}_{N-1}$ (normovaný polynom). Zřejmě $d \mid r_{N-1}$ a $d \mid r_N$. Je-li d dělitel polynomů r_{i+1} a r_{i+2} , pak je dělitel i polynomu $r_i = r_{i+1}q_i + r_{i+2}$. Postupně tedy dostaneme, že $d \mid r_i$ pro všechna $i \in \{0, \dots, N\}$, 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 $r_{i+2} = r_i - r_{i+1}q_i$. Takto postupně dostaneme, že $h \mid r_i$ pro všechna $i \in \{0, \dots, N\}$, včetně $h \mid r_{N-1} = d$. Tedy, $d = D(f, g)$.

Buďte d_1, d_2 největší společné dělitele polynomů. Podle definice největšího společného dělitele $d_1 \mid d_2$ a $d_2 \mid d_1$ a jelikož d_1, d_2 jsou normované, $d_1 = d_2$. □

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

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

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

Tvrzení 4.2.3 (Bézoutova věta). *Buďte $f, g \in P[x]$ polynomy, z nichž aspoň jeden je nenulový. Pak existují polynomy $u, v \in P[x]$ takové, že $D(f, g) = fu + gv$.*

Důkaz. Označme $I = \{fu + gv \mid u, v \in P[x]\}$. V množině I existuje normovaný prvek minimálního stupně, označme jej d . Tedy, $d = fu + gv$ pro nějaká $u, v \in P[x]$.

Po dělení se zbytkem dostaneme $f = dq + r$, kde buď $r = 0$ nebo $\deg r < \deg d$. Zároveň $r = f - dq = f - (fu + gv)q = f(1 - uq) + g(-vq) \in I$. Kdyby $r \neq 0$, byl by to nenulový prvek I stupně nižšího než $\deg d$. Takže $r = 0$ a tedy $d \mid f$. Analogicky $d \mid g$.

Buď $h \in P[x]$ společný dělitel f a g . Pak h je dělitel i polynomu $fu + gv = d$. Tedy, $d = D(f, g)$. □

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

Tvrzení 4.2.4 (Rozšířený Eukleidův algoritmus). *Buďte $f, g \in P[x]$ nenulové polynomy. Buďte $r_0, r_1, r_2, \dots, r_{N-1}$ 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

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

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

Důkaz. Podle Eukleidova algoritmu a podle předpokladů

$$r_0 = f, \quad r_1 = g, \quad u_0 = 1, \quad u_1 = 0, \quad v_0 = 0, \quad v_1 = 1$$

a pro $i \in \{0, \dots, N-3\}$

$$r_i = r_{i+1}q_i + r_{i+2}, \quad \text{tedy} \quad r_{i+2} = r_i - r_{i+1}q_i, \quad (5)$$

$$u_i = u_{i+1}q_i + u_{i+2}, \quad \text{tedy} \quad u_{i+2} = u_i - u_{i+1}q_i, \quad (6)$$

$$v_i = v_{i+1}q_i + v_{i+2}, \quad \text{tedy} \quad v_{i+2} = v_i - v_{i+1}q_i. \quad (7)$$

Matematickou indukcí ukážeme, že $r_i = fu_i + gv_i$ pro všechna $i \in \{0, \dots, N-1\}$. Platí

$$r_0 = f = f \cdot 1 + g \cdot 0 = f \cdot u_0 + g \cdot v_0,$$

$$r_1 = g = f \cdot 0 + g \cdot 1 = f \cdot u_1 + g \cdot v_1.$$

Předpokládejme, že pro nějaké k platí

$$r_k = fu_k + gv_k, \quad (8)$$

$$r_{k+1} = fu_{k+1} + gv_{k+1}. \quad (9)$$

Potom

$$\begin{aligned} r_{k+2} &= && \text{(podle (5))} \\ &= r_k - r_{k+1}q_k = && \text{(podle (8), (9))} \\ &= fu_k + gv_k - (fu_{k+1} + gv_{k+1})q_k = \\ &= f(u_k - u_{k+1}q_k) + g(v_k - v_{k+1}q_k) = && \text{(podle (6), (7))} \\ &= fu_{k+2} + gv_{k+2}. \end{aligned}$$

Takže, vztah $r_i = fu_i + gv_i$ platí pro $i = 0, i = 1$ a když platí pro $i = k$ a $i = k+1$, pak platí pro $i = k+2$. Z toho vyplývá, že platí pro každé $i \in \{0, \dots, N-1\}$. Zbytek tvrzení je zřejmý. $\square$

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

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

Už víme, že $D(f, g) = 1$, $N = 4$,

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

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

$$r_2 = -x + 2$$

$$r_3 = 8$$

$$u_0 = 1 \quad v_0 = 0$$

$$u_1 = 0 \quad v_1 = 1.$$

Dále

$$\begin{aligned}
u_0 &= u_1 q_0 + u_2 \\
1 &= 0 \cdot q_0 + u_2 && \text{implikuje } u_2 = 1, \\
v_0 &= v_1 q_0 + v_2 \\
0 &= 1 \cdot q_0 + v_2 && \text{implikuje } v_2 = -q_0 = -x^3 + x^2 - x - 1, \\
u_1 &= u_2 q_1 + u_3 \\
0 &= 1 \cdot q_1 + u_3 && \text{implikuje } u_3 = -q_1 = x + 3, \\
v_1 &= v_2 q_1 + v_3 \\
1 &= -q_0 \cdot q_1 + v_3 && \text{implikuje } v_3 = 1 + q_0 q_1 = -x^4 - 2x^3 + 2x^2 - 4x - 2.
\end{aligned}$$

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

$$\begin{aligned}
u &= \frac{x}{8} + \frac{3}{8} \\
v &= -\frac{x^4}{8} - \frac{x^3}{4} + \frac{x^2}{4} - \frac{x}{2} - \frac{1}{4}
\end{aligned}$$

pak $D(f, g) = 1 = fu + gv$. □

4.3. Ireducibilní polynomy

Definice 4.3.1. Polynom je *reducibilní* nad polem P , jestliže je součinem dvou nekonstantních polynomů nad polem P . Polynom je *ireducibilní* nad polem P , jestliže není konstantní a není reducibilní nad polem P .

Pro polynom z $P[x]$ označením *reducibilní*, resp. *ireducibilní* se myslí *reducibilní nad P* , resp. *ireducibilní nad P* .

Je-li polynom f reducibilní a $f = g \cdot h$, kde g, h jsou nekonstantní polynomy, říká se také, že $g \cdot h$ je *rozklad* polynomu f na součin polynomů g, h nebo také, že $g \cdot h$ je *rozklad* polynomu f na činitele g, h .

Příklad. (1) Každý polynom stupně 1 je ireducibilní, neboť není konstantní a součin dvou nekonstantních polynomů je polynom stupně aspoň 2.

(2) Polynom $x^2 - 1 = (x - 1)(x + 1)$ je reducibilní nad $\mathbb{R}$. Polynomy $x - 1$ a $x + 1$ jsou ireducibilní nad $\mathbb{R}$. □

Cvičení. Normovaný reducibilní polynom je součinem normovaných nekonstantních polynomů. □

Tvrzení 4.3.1. Nechť jsou $f, g \in P[x]$ normované polynomy, g je ireducibilní a $f \mid g$. Potom buď $f = 1$, anebo $f = g$. Je-li f také ireducibilní, pak $f = g$.

Důkaz. Když $f \mid g$, existuje $h \in P[x]$ takové, že $fh = g$. Jelikož g je ireducibilní, právě jeden z polynomů f, h je konstantní. Je-li normovaný polynom f konstantní, pak $f = 1$. Je-li h konstantní a fh je normovaný polynom, pak $h = 1$, tedy $f = g$. Je-li f ireducibilní, pak není konstantní, a zbývá tedy jen $f = g$. □

Lemma 4.3.2. Buďte $g, h_1, \dots, h_n \in P[x]$ normované ireducibilní polynomy a nechť $g \mid h_1 \cdots h_n$. Pak existuje index j takový, že $g = h_j$.

Důkaz. Označme $d = D(g, h_1)$. Jelikož $d \mid g$ a g je ireducibilní, podle Tvzení 4.3.1 buď $d = g$ anebo $d = 1$. Jestliže $d = g$, pak $g \mid h_1$ a $g = h_1$. Jestliže $d = 1$, pak Tvzení 4.2.3

$$1 = gu + h_1v$$

pro vhodné $u, v \in P[x]$. Vynásobíme-li obě strany polynomem $h_2 \cdots h_n$, dostaneme

$$h_2 \cdots h_n = gh_2 \cdots h_nu + h_1h_2 \cdots h_nv.$$

Podle předpokladu $g \mid h_1 \cdots h_n$, takže pravá strana je dělitelná g , proto i levá strana je dělitelná g , čili $g \mid h_2 \cdots h_n$. Stejným postupem ukážeme, že buď $g = h_2$ anebo $g \mid h_3 \cdots h_n$. Opakováním tohoto postupu najdeme j , $1 \leq j \leq n$, takové, že $g = h_j$. $\square$

Tvrzení 4.3.3. *Každý nekonstantní polynom je součinem konstanty a normovaných ireducibilních polynomů, přičemž všechny činitele jsou určeny jednoznačně až na pořadí.*

Důkaz. Buď $f \in P[x]$ nekonstantní polynom a označme $\bar{f} = \frac{1}{\text{lc } f} \cdot f$. Je-li $\bar{f}$ ireducibilní, pak $f = \text{lc } f \cdot \bar{f}$. Je-li $\bar{f}$ reducibilní, pak je součinem normovaných nekonstantních polynomů nižšího stupně. Každý z těchto polynomů je také buď ireducibilní nebo reducibilní, ve druhém případě je opět součinem normovaných nekonstantních polynomů nižšího stupně. Opakováním tohoto postupu po konečně mnoha krocích dojdeme ke konečnému počtu normovaných ireducibilních polynomů. Jejich počet je shora omezen stupněm polynomu f a jejich součin je roven $\bar{f}$.

Ještě je potřeba dokázat jednoznačnost. Předpokládejme, že $\bar{f} = g_1 \cdots g_n = h_1 \cdots h_m$ a všechny činitele jsou normované ireducibilní polynomy. Jelikož $g_1 \mid h_1 \cdots h_m$, podle předchozího lemmatu existuje index $\varphi(1)$ takový, že $g_1 = h_{\varphi(1)}$. Takže rovnost $g_1 \cdots g_n = h_1 \cdots h_m$ můžeme zkrátit g_1 a na obou stranách rovnosti tedy bude o jednoho činitele méně. Obdobně dostaneme, že existuje index $\varphi(2)$ takový, že $g_2 = h_{\varphi(2)}$, a postupně až že existuje index $\varphi(n)$ takový, že $g_n = h_{\varphi(n)}$.

Navíc, $n \leq m$, protože jinak by $g_{m+1} \cdots g_n = 1$, což není možné, když všechny g_i jsou nekonstantní polynomy. A obdobně dostaneme, že $m \leq n$. Takže $n = m$. $\square$

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. $\square$

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

4.4. Kořeny a jejich násobnost

Pro $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in P[x]$ a $\xi \in P$, označme

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

Tvrzení 4.4.1. *Pro libovolné polynomy $f, g \in P[x]$ a libovolný prvek $\xi \in P$ platí*

$$(f + g)(\xi) = f(\xi) + g(\xi), \quad (-f)(\xi) = -f(\xi), \quad (fg)(\xi) = f(\xi)g(\xi).$$

Důkaz. Cvičení. $\square$

Definice 4.4.1. Prvek $\xi \in P$ je kořen polynomu $f \in P[x]$, jestliže $f(\xi) = 0$.

Tvrzení 4.4.2. *Nechť $f \in P[x]$ a $\xi \in P$. Potom ξ je kořen polynomu f právě tehdy, když $x - \xi$ dělí f .*

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

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

Takže v obou případech r je konstantní polynom a $0 = f(\xi) = (\xi - \xi)q(\xi) + r = r$. Čili $r = 0$, $f = (x - \xi)q$ a $x - \xi$ dělí f .

Předpokládejme, že $x - \xi$ dělí f , tedy $f = (x - \xi)q$ pro nějaké q . Potom $f(\xi) = (\xi - \xi)q(\xi) = 0$, čili ξ je kořen polynomu f . $\square$

Definice 4.4.2. Nechť $f \in P[x]$ a $\xi \in P$. Pokud ξ je kořen f , potom polynom $x - \xi$ je *kořenový činitel* polynomu f .

Definice 4.4.3. Prvek $\xi \in P$ je *k-násobný kořen* polynomu $f \in P[x]$, jestliže $(x - \xi)^k$ dělí f , ale $(x - \xi)^{k+1}$ nedělí f .

Tvrzení 4.4.3. *Budte $\xi_1, \dots, \xi_n \in P$ různé kořeny polynomu $f \in P[x]$ s násobnostmi po řadě $k_1, \dots, k_n$. Potom*

- (1) $(x - \xi_1)^{k_1} \cdots (x - \xi_n)^{k_n} \mid f$;
- (2) $k_1 + \cdots + k_n \leq \deg f$.

Důkaz. Cvičení. $\square$

Tvrzení 4.4.4 (Základní věta algebry). *Každý nekonstantní polynom nad polem $\mathbb{C}$ má aspoň jeden kořen.*

Všechny známé důkazy využívají výsledky matematické analýzy, proto zde důkaz neuvádíme.

Důsledek. *Každý nekonstantní polynom nad polem $\mathbb{C}$ má rozklad na lineární činitele. Kořenů se započtením násobnosti má právě tolik, kolik činí jeho stupeň, a navzájem různých kořenů má nejvýše tolik.*

Předchozí důsledek znamená, že pro každý nekonstantní polynom $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ stupně n s komplexními koeficienty existují čísla $\xi_1, \xi_2, \dots, \xi_n$ (nemusí být po dvou různá), pro která platí

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = a_n (x - \xi_1)(x - \xi_2) \cdots (x - \xi_n).$$

Každé z čísel $\xi_1, \xi_2, \dots, \xi_n$ je kořenem polynomu f .

Tvrzení 4.4.5 (Vlastnosti kořenů (Viètovy vzorce)). *Budte $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{C}[x]$ 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. Polynom f můžeme rozložit na součin jeho kořenových činitelů

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - \xi_1) \dots (x - \xi_n).$$

Po roznásobení pravé strany porovnáním koeficientů s příslušnými koeficienty na levé straně získáme uvedené vztahy. $\square$

Příklad. Kořeny polynomu $x^2 - 5x + 6$ jsou 2 a 3 a

$$a_1 = -(2 + 3) = -5,$$

$$a_0 = (-1)^2 \cdot 2 \cdot 3 = 6. \quad \square$$

4.5. Polynomy s reálnými koeficienty

Komplexní čísla

Komplexní číslo v algebraickém tvaru je číslo $a + bi$, kde a, b jsou reálná čísla a i je imaginární jednotka, čili $i^2 = -1$.

Komplexní čísla $z_1 = a + bi$, $z_2 = c + di$ se rovnají právě tehdy, když $a = c$ a $b = d$.

Pro $z_1 = a + bi$, $z_2 = c + di$

$$z_1 + z_2 = (a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$z_1 - z_2 = (a + bi) - (c + di) = (a - c) + (b - d)i,$$

$$z_1 \cdot z_2 = (a + bi) \cdot (c + di) = (ac + bdi^2) + adi + bci = (ac - bd) + (ad + bc)i,$$

pro $z_2 \neq 0$

$$\frac{z_1}{z_2} = \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2}.$$

Číslo komplexně sdružené k číslu $z = a + bi$ je číslo $a - bi$ a označujeme jej z^* .

Cvičení. Pro komplexní číslo $z = a + bi$

- (1) $(z^*)^* = z$,
- (2) $z = z^*$ právě tehdy, když z je reálné číslo,
- (3) $z + z^* = 2a$, tedy reálné číslo,
- (4) $zz^* = a^2 + b^2$, tedy reálné číslo. □

Cvičení. Pro komplexní čísla z_1, z_2

$$(z_1 + z_2)^* = z_1^* + z_2^*, \quad (z_1 z_2)^* = z_1^* z_2^*, \quad \left(\frac{z_1}{z_2}\right)^* = \frac{z_1^*}{z_2^*}. \quad \square$$

Cvičení. Pro komplexní číslo $z = a + bi$

$$(x - z)(x - z^*) = x^2 - 2ax + a^2 + b^2$$

je polynom s reálnými koeficienty a pokud $z \notin \mathbb{R}$, čili $b \neq 0$, potom diskriminant tohoto polynomu je záporný. □

Absolutní hodnota komplexního čísla $z = a + bi$ je

$$|z| = \sqrt{a^2 + b^2} = \sqrt{zz^*}$$

Polynomy s reálnými koeficienty

Tvrzení 4.5.1. Je-li $\xi \in \mathbb{C}$ kořenem polynomu s reálnými koeficienty, potom $\xi^* \in \mathbb{C}$ je také kořenem tohoto polynomu, a to stejné násobnosti.

Důkaz. Necht' $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ je polynom s reálnými koeficienty a $\xi \in \mathbb{C}$ je jeho kořen, čili $f(\xi) = 0$. Potom

$$\begin{aligned} f(\xi^*) &= a_n (\xi^*)^n + a_{n-1} (\xi^*)^{n-1} + \dots + a_1 \xi^* + a_0 = & (a = a^* \text{ pro } a \in \mathbb{R}) \\ &= a_n^* (\xi^*)^n + a_{n-1}^* (\xi^*)^{n-1} + \dots + a_1^* \xi^* + a_0^* = & (a^* b^* = (ab)^*) \\ &= (a_n \xi^n)^* + (a_{n-1} \xi^{n-1})^* + \dots + (a_1 \xi)^* + a_0^* = & (a^* + b^* = (a + b)^*) \\ &= (a_n \xi^n + a_{n-1} \xi^{n-1} + \dots + a_1 \xi + a_0)^* = \\ &= f(\xi)^* = 0^* = 0. \end{aligned}$$

Na druhou stranu, pokud ξ^* je kořen polynomu f , potom z právě dokázaného vyplývá, že $\xi = (\xi^*)^*$ je také kořen.

Takže, je-li $\xi = a + bi$ kořen f , potom $\xi^* = a - bi$ je také kořen f a

$$f = (x - \xi)(x - \xi^*)h.$$

Díky tomu, že $\xi + \xi^* = 2a$ a $\xi\xi^* = a^2 + b^2$ jsou reálná čísla,

$$(x - \xi)(x - \xi^*) = x^2 - (\xi + \xi^*)x + \xi\xi^*$$

je polynom s reálnými koeficienty, a proto h je také polynom s reálnými koeficienty. Proto, je-li ξ k -násobný kořen f ,

$$f = (x - \xi)^k (x - \xi^*)^k g,$$

kde g je polynom s reálnými koeficienty, jehož kořenem nejsou ani ξ ani ξ^* , takže ξ^* je také k -násobný kořen f . □

Rozklad normovaného polynomu f s reálnými koeficienty na ireducibilní činitele nad $\mathbb{C}$ tedy obsahuje lineární činitele $x - \alpha_i$ s reálnými kořeny α_i a dvojice lineárních činitelů $x - \xi_j$, $x - \xi_j^*$ s dvojicemi komplexně sdružených kořenů ξ_j, ξ_j^* :

$$f = (x - \alpha_1)^{l_1} \dots (x - \alpha_r)^{l_r} (x - \xi_1)^{k_1} (x - \xi_1^*)^{k_1} \dots (x - \xi_s)^{k_s} (x - \xi_s^*)^{k_s}.$$

Takže $\deg f = l_1 + \dots + l_r + 2(k_1 + \dots + k_s)$.

Pokud roznásobíme všechny dvojice $(x - \xi_j), (x - \xi_j^*)$, dostaneme rozklad polynomu f na ireducibilní činitele nad $\mathbb{R}$, který obsahuje lineární činitele $x - \alpha_i$ a kvadratické činitele $x^2 - (\xi_j + \xi_j^*)x + \xi_j \xi_j^*$ se zápornými diskriminanty:

$$f = (x - \alpha_1)^{l_1} \cdots (x - \alpha_r)^{l_r} (x^2 - (\xi_1 + \xi_1^*)x + \xi_1 \xi_1^*)^{k_1} \cdots (x^2 - (\xi_s + \xi_s^*)x + \xi_s \xi_s^*)^{k_s}.$$

Cvičení. (1) Každý polynom s reálnými koeficienty lichého stupně má aspoň jeden reálný kořen.

(2) Každý polynom s reálnými koeficienty stupně většího než 2 je reducibilní nad $\mathbb{R}$. $\square$

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

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

Tvrzení 4.5.2. *Buďte $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 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. Předpokládejme, že $\frac{p}{q}$ je kořenem polynomu f , tedy

$$f\left(\frac{p}{q}\right) = a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \cdots + a_1 \frac{p}{q} + a_0 = 0.$$

Vhodnými úpravami lze získat uvedené vlastnosti. Cvičení. $\square$

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

4.6. Derivace

Definice 4.6.1. Buď

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x].$$

Polynom

$$f' = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1 \in \mathbb{C}[x]$$

je *derivace* polynomu f .

Tvrzení 4.6.1. (1) $(f + g)' = f' + g'$,

(2) $(fg)' = f'g + fg'$,

(3) $(f^k)' = k f^{k-1} f'$.

Důkaz. Cvičení. $\square$

Tvrzení 4.6.2. *Nechť $k \geq 2$, $f \in \mathbb{C}[x]$ je polynom a $\xi \in \mathbb{C}$ je jeho k -násobný kořen. Potom*

(1) ξ je $(k-1)$ -násobný kořen f' ,

(2) ξ je $(k-1)$ -násobný kořen největšího společného dělitele $D(f, f')$.

Důkaz. (1) Předpokládejme, že ξ je k -násobný kořen polynomu f , čili $(x - \xi)^k$ dělí f a $(x - \xi)^{k+1}$ nedělí f . Pro nějaký polynom q tedy $f = (x - \xi)^k q$. 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' , potom $x - \xi$ by dělilo $kq + (x - \xi)q'$ a vzhledem k tomu, že $x - \xi$ dělí $(x - \xi)q'$, muselo by $x - \xi$ dělit také kq , tedy i q . V takovém případě $(x - \xi)^{k+1}$ by dělilo f , což je spor 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 4.6.3. *Budť $f \in \mathbb{C}[x]$ a $\xi \in \mathbb{C}$ jeho kořen. Potom ξ je 1-násobný kořen polynomu*

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

Důkaz. Nechť ξ je k -násobný kořen polynomu f , tedy $f = (x - \xi)^k q$, ale $(x - \xi)^{k+1}$ nedělí f , čili $x - \xi$ nedělí q . Podle předchozího tvrzení $D(f, f') = (x - \xi)^{k-1} r$. Takže

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

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

- (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. $\square$

4.7. Hornerovo schéma

Budť $f \in P[x]$ a $\xi \in P$. Podle Tvrzení 4.1.6 existuje právě jedna dvojice polynomů $q, r \in P[x]$ taková, že

- (i) $f = (x - \xi)q + r$;
- (ii) buď $r = 0$ nebo $\deg r < \deg(x - \xi) = 1$.

Takže r je konstantní polynom a $f(\xi) = r$.

Je-li f konstantní polynom, potom $q = 0$ a $r = f$. Je-li $\deg f \geq 1$, potom $\deg q = \deg f - 1$. Nechť $\deg f = n \geq 1$ a

$$\begin{aligned} f &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \\ q &= b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0. \end{aligned}$$

Potom,

$$\begin{aligned} a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 &= \\ &= (x - \xi)(b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0) + r = \\ &= b_{n-1} x^n + (b_{n-2} - \xi b_{n-1}) x^{n-1} + \cdots + (b_1 - \xi b_2) x^2 + (b_0 - \xi b_1) x + (r - \xi b_0). \end{aligned}$$

Když se polynomy vzájemně rovnají, rovnají se jejich koeficienty u stejných mocnin neurčit x . Díky tomu dostaneme soustavu lineárních rovnic s neznámými $b_{n-1}, \dots, b_1, b_0, r$,

jejíž řešení lze snadno vyjádřit pomocí $a_n, \dots, a_1, a_0$ a ξ .

$$\begin{array}{lll}
 a_n = b_{n-1} & \Rightarrow & b_{n-1} = a_n \\
 a_{n-1} = b_{n-2} - \xi b_{n-1} & \Rightarrow & b_{n-2} = a_{n-1} + \xi b_{n-1} \\
 a_{n-2} = b_{n-3} - \xi b_{n-2} & \Rightarrow & b_{n-3} = a_{n-2} + \xi b_{n-2} \\
 \vdots & \vdots & \vdots \\
 a_2 = b_1 - \xi b_2 & \Rightarrow & b_1 = a_2 + \xi b_2 \\
 a_1 = b_0 - \xi b_1 & \Rightarrow & b_0 = a_1 + \xi b_1 \\
 a_0 = r - \xi b_0 & \Rightarrow & r = a_0 + \xi b_0
 \end{array}$$

Tedy,

$$\begin{aligned}
 b_{n-1} &= a_n \\
 b_{n-2} &= a_{n-1} + \xi a_n \\
 b_{n-3} &= a_{n-2} + \xi(a_{n-1} + \xi a_n) \\
 &\vdots \\
 b_1 &= a_2 + \xi(a_3 + \xi(a_4 + \dots + \xi(a_{n-2} + \xi(a_{n-1} + \xi a_n)) \dots)) \\
 b_0 &= a_1 + \xi(a_2 + \xi(a_3 + \dots + \xi(a_{n-2} + \xi(a_{n-1} + \xi a_n)) \dots)) \\
 r &= a_0 + \xi(a_1 + \xi(a_2 + \dots + \xi(a_{n-2} + \xi(a_{n-1} + \xi a_n)) \dots)).
 \end{aligned}$$

Pro výpočet je praktické uspořádat si koeficienty, jak známé $a_n, \dots, a_1, a_0, \xi$, tak hledané $b_{n-1}, \dots, b_1, b_0, r$, do tabulky (schématu) tak, že v prvním řádku jsou koeficienty polynomu f , do druhého řádku postupně píšeme ξ -násobky vypočítaných koeficientů polynomu q a do třetího řádku napíšeme ξ a potom postupně součty hodnot v příslušných sloupcích v prvních dvou řádcích, tedy koeficienty polynomu q a také hodnotu $r = f(\xi)$.

	a_n	a_{n-1}	a_{n-2}	$\dots$	a_2	a_1	a_0
		ξb_{n-1}	ξb_{n-2}	$\dots$	ξb_2	ξb_1	ξb_0
ξ	a_n $= b_{n-1}$	$a_{n-1} + \xi b_{n-1}$ $= b_{n-2}$	$a_{n-2} + \xi b_{n-2}$ $= b_{n-3}$	$\dots$ $\dots$	$a_2 + \xi b_2$ $= b_1$	$a_0 + \xi b_0$ $= b_0$	$a_0 + \xi b_0$ $= r$

Takto lze tedy spočítat částečný podíl q a zbytek r při dělení polynomu f polynomem $x - \xi$, čili také $f(\xi) = r$, a ověřit tak, například, zda ξ je kořenem polynomu f .

Navíc, Hornerovo schéma lze použít pro nalezení hodnot derivací polynomu f v bodě ξ a k převodu čísla z nadesítkové do desítkové soustavy.

5. GRUPY

5.1. Binární operace

Definice 5.1.1. Binární operace na množině X je libovolné zobrazení $X \times X \rightarrow X$.

Jedná se tedy o zobrazení, které každé uspořádané dvojici prvků z X přiřazuje nějaký 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 součet matic.

(6) Množina $\mathcal{M}_n(P)$ čtvercových matic stejného typu s operací součin matic.

(7) Množina $P[x]$ všech polynomů s operací součet nebo součin 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 $P(X)$. $\square$

Definice 5.1.2. Binární operace $*$ na množině X je *asociativní*, jestliže pro každé $x, y, z \in X$ platí

$$x * (y * z) = (x * y) * z.$$

Můžeme tedy psát bez závorek $x * y * z$.

Definice 5.1.3. Binární operace $*$ na množině X je *komutativní*, jestliže pro každé $x, y \in X$ platí

$$x * y = y * x.$$

Příklad. (1) Součet a součin na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ jsou asociativní i komutativní.

(2) Součet na množině $\mathbb{R}^2$ je asociativní i komutativní.

(3) Součet matic na množině $\mathcal{M}_{m \times n}(P)$ je asociativní i komutativní.

(4) Součin matic na množině $\mathcal{M}_n(P)$ je asociativní, ale není komutativní.

(5) Součet a součin 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. $\square$

Definice 5.1.4. Buď $*$ binární operace na množině X . Prvek $e \in X$ je *neutrální prvek* operace $*$, jestliže pro každý prvek $x \in X$ platí

$$x * e = x = e * x.$$

Tvrzení 5.1.1. Každá binární operace má nejvýše jeden neutrální prvek.

Důkaz. Jsou-li e_1, e_2 neutrální prvky operace $*$, pak $e_2 = e_1 * e_2 = e_1$. $\square$

Příklad. (1) Neutrální prvek operace součet na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je 0.

(2) Neutrální prvek operace součin na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je 1.

(3) Neutrální prvek operace součet na množině $\mathbb{R}^2$ je $(0, 0)$.

(4) Neutrální prvek operace součet matic na množině $\mathcal{M}_{m \times n}(P)$ je nulová matice příslušného typu, tedy $0_{m \times n}$.

(5) Neutrální prvek operace součin matic na množině $\mathcal{M}_n(P)$ je jednotková matice příslušného typu, tedy E_n .

(6) Neutrální prvek operace součet polynomů na množině $P[x]$ je polynom 0.

(7) Neutrální prvek operace součin polynomů na množině $P[x]$ je polynom 1.

(8) Neutrální prvek operace skládání zobrazení na množině X^X je identita 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 $\emptyset$. $\square$

Definice 5.1.5. Buď $*$ binární operace na množině X , $e \in X$ její neutrální prvek. Prvek $x \in X$ je *invertibilní*, jestliže existuje prvek $y \in X$ takový, že

$$x * y = y * x = e.$$

Potom y je *inverzní prvek* nebo *inverze* k prvku x vzhledem k operaci $*$.

Tvrzení 5.1.2. Každý prvek množiny s asociativní binární operací má vzhledem k této operaci nejvýše jeden inverzní prvek.

Důkaz. Je-li e neutrální prvek operace $*$ a jsou-li y_1, y_2 inverzní prvky k prvku x , pak

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

Inverzní prvek k prvku x se obvykle značí x^{-1} . Pouze u operace $+$ se značí $-x$ a říká se mu *opačný*.

Cvičení. Přímou z definice inverzního prvku vyplývá, že

$$e^{-1} = e \quad \text{a} \quad (x^{-1})^{-1} = x. \quad \square$$

Příklad. (1) Inverzní prvek k číslu x vzhledem k operaci součet 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 součin 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 součet je $(-x, -y)$.

- (4) Inverzní prvek k matici A vzhledem k operaci součet matic na množině $\mathcal{M}_{m \times n}(P)$ je opačná matice $-A$.
- (5) Inverzní prvek k matici A vzhledem k operaci součin 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 . $\square$

Příklad. Na množině $\{0, 1, 2\}$ mějme binární operaci $*$ zadanou tabulkou

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	0

Neutrální prvek operace $*$ je 0 a

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

Čili 1 a 2 jsou inverzní prvky k 2. Podle Tvzení 5.1.2 to znamená, že operace $*$ není asociativní. A skutečně, například,

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

5.2. Grupy

Definice 5.2.1. 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 součet je grupa. Stejně tak $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(2) Množina $\mathbb{N}_0$ s operací součet není grupa.

(3) Množina $\mathbb{Q}^*$ s operací součin je grupa. Stejně tak $\mathbb{R}^*, \mathbb{C}^*, \mathbb{R}_+$ (kladná reálná čísla).

(4) Množina $\mathbb{Z} \setminus \{0\}$ s operací součin není grupa. Stejně tak $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(5) Množina $\mathbb{R}^2$ s operací součet je grupa.

(6) Množina $\mathcal{M}_{m \times n}(P)$ s operací součet je grupa.

(7) Množina $\mathcal{M}_n(P)$ s operací součin není grupa.

(8) Množina $\text{GL}_n(P)$ invertibilních matic typu $n \times n$ s operací součin je grupa (nazývá se *obecná lineární grupa*).

- (9) Množina X^X s operací skládání zobrazení není grupa.
 (10) Množina všech bijektivních zobrazení $X \rightarrow X$ s operací skládání je grupa. $\square$

Tvrzení 5.2.1. *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 rovnosti $x * y * y^{-1} * x^{-1} = e$ a (1). $\square$

Poznámka. Bez předpokladu existence inverze ke každému prvku nejde o grupu a implikace v bodě (1) v Tvrzení 5.2.1 nemusí platit, viz následující příklad (1), ale v některých případech i přesto platí, viz následující příklad (2).

Příklad. (1) Označme $I = [0, 1]$ a mějme množinu I^I všech zobrazení $I \rightarrow I$ s operací skládání a neutrálním prvkem id_I . Necht' $f, g \in I^I$ jsou taková, že

$$f(x) = \begin{cases} 2x & \text{pro } x \in [0, \frac{1}{2}], \\ 1 & \text{pro } x \in [\frac{1}{2}, 1], \end{cases} \quad g(x) = \frac{1}{2}x \quad \text{pro } x \in I.$$

Potom sice $f \circ g = \text{id}_I$, ale

$$(g \circ f)(x) = \begin{cases} x & \text{pro } x \in [0, \frac{1}{2}], \\ \frac{1}{2} & \text{pro } x \in [\frac{1}{2}, 1], \end{cases} \quad \text{a } f^{-1}, g^{-1} \text{ neexistují.}$$

(2) Množina $\mathcal{M}_n(P)$ s operací součin sice není grupa, přesto pro libovolné dvě matice z $\mathcal{M}_n(P)$ bod (1) v Tvrzení 5.2.1 platí, viz Tvrzení 1.4.3. $\square$

5.3. Podgrupy

Definice 5.3.1. Bud' $(X, *, e, {}^{-1})$ grupa, bud' $Y \subseteq X$ podmnožina taková, že

- (1) jestliže $y_1, y_2 \in Y$, pak $y_1 * y_2 \in Y$;
 (2) $e \in Y$;
 (3) jestliže $y \in Y$, pak $y^{-1} \in Y$.

Potom Y je *podgrupa* grupy X .

Vlastnosti (1) se někdy říká *uzavřenost množiny vzhledem k operaci*, vlastnosti (3) *uzavřenost množiny vzhledem k inverzi*.

Je-li Y podgrupa grupy $(X, *, e, {}^{-1})$ a je-li $*_Y$ zúžení operace $*$ na podmnožinu $Y \times Y$, pak $(Y, *_Y, e, {}^{-1})$ je grupa. Zúžení operace na podmnožinu se obvykle značí stejně jako původní operace.

Příklad. (1) Každá grupa $(X, *, e, {}^{-1})$ má podgrupy X a $\{e\}$. Tyto podgrupy se nazývají *triviální* podgrupy.

- (2) Aditivní podgrupy $(\mathbb{Z}, +, 0, -) \subset (\mathbb{Q}, +, 0, -) \subset (\mathbb{R}, +, 0, -) \subset (\mathbb{C}, +, 0, -)$.
 (3) Multiplikativní podgrupy $(\mathbb{Q}^*, \cdot, 1, {}^{-1}) \subset (\mathbb{R}^*, \cdot, 1, {}^{-1}) \subset (\mathbb{C}^*, \cdot, 1, {}^{-1})$.
 (4) Množina $\{-1, 1\}$ je podgrupa multiplikativní grupy $\mathbb{R}^*$.
 (5) Množina $\{z \in \mathbb{C} \mid |z| = 1\}$ 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 součet.

(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 součet. $\square$

Tvrzení 5.3.1. (1) Budť X grupa, Y podgrupa X a Z podgrupa Y . Pak Z je podgrupa X .

(2) Budť X grupa a Y, Z její podgrupy. Pak $Y \cap Z$ je podgrupa X .

Důkaz. Cvičení. $\square$

Cvičení. Pokud průnik prázdného systému podmnožin množiny X je množina X , potom průnik libovolného systému podgrup grupy X je podgrupa grupy X . $\square$

5.4. Podgrupy aditivní grupy $\mathbb{Z}$

Najdeme všechny podgrupy aditivní grupy $\mathbb{Z} = (\mathbb{Z}, +, 0, -)$. Pro celé nezáporné číslo $m \in \mathbb{N}_0$ označme

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

Tvrzení 5.4.1. Množiny $m\mathbb{Z}$, $m \in \mathbb{N}_0$, jsou podgrupy aditivní grupy $\mathbb{Z}$ a jiné podgrupy v $\mathbb{Z}$ nejsou.

Důkaz. Budť $m \in \mathbb{N}_0$ libovolné. Ukážeme, že $m\mathbb{Z}$ je podgrupa. Pro libovolné $mk, ml \in m\mathbb{Z}$ platí $mk + ml = m(k + l) \in m\mathbb{Z}$, čímž je dokázána uzavřenost množiny $m\mathbb{Z}$ vzhledem ke sčítání. Množina $m\mathbb{Z}$ obsahuje neutrální prvek 0 grupy $\mathbb{Z}$. Nakonec, pro libovolné $mk \in m\mathbb{Z}$ platí $-(mk) = m(-k) \in m\mathbb{Z}$, čímž je dokázána uzavřenost množiny $m\mathbb{Z}$ vzhledem k inverzi (opačným prvkům).

Budť $B \subseteq \mathbb{Z}$ libovolná podgrupa grupy $\mathbb{Z}$. Ukážeme, že B je rovna některé podgrupě $m\mathbb{Z}$. Jelikož B je podgrupa, obsahuje neutrální prvek 0. Pokud $B = \{0\}$, pak $B = 0\mathbb{Z}$ ($m = 0$). Předpokládejme, že $B \neq \{0\}$, tedy existuje nenulové číslo $b \in B$. Navíc existuje kladné číslo $b_+ \in B$, buď $b_+ = b$, nebo $b_+ = -b$ ($-b \in B$, protože B je podgrupa). Označme m nejmenší kladné číslo v B (v každé neprázdné množině kladných celých čísel existuje nejmenší číslo).

Dokážeme, že toto číslo m je hledané číslo, pro něž $B = m\mathbb{Z}$. Nejdříve ukážeme, že $m\mathbb{Z} \subseteq B$. Již víme, že $0 \in B$ a $m \in B$. Předpokládejme, že $mk \in B$. Potom i $m(k + 1) = mk + m \in B$ a díky matematické indukci dostáváme, že $mk \in B$ pro každé $k \in \mathbb{N}$. A potom i inverzní prvky $-mk$ leží v B , a tím je ukázáno, že všechny prvky množiny $m\mathbb{Z}$ leží v B .

Zbývá dokázat, že $B \subseteq m\mathbb{Z}$. Budť $b \in B$ libovolné a předpokládejme, že $b \notin m\mathbb{Z}$. Pak existují $q, r \in \mathbb{Z}$ taková, že

$$b = mq + r \quad \text{a} \quad 0 < r < m.$$

Tedy, $r = b - mq = b + m(-q)$ je kladný prvek B , menší než m , což je v rozporu s definicí prvku m . Proto $b \in m\mathbb{Z}$. $\square$

5.5. Faktorové grupy

Definice 5.5.1. Relace na množině X je podmnožina kartézského součinu $X \times X$.

Je-li ρ relace, místo „ (x, y) je v relaci ρ “ se obvykle říká „ x je v relaci ρ s y “ a místo $(x, y) \in \rho$ se obvykle píše $x \rho y$.

Definice 5.5.2. Relace ρ na množině X je *relace ekvivalence*, jestliže je

- (1) reflexivní, tj. $x \rho x$ pro každé $x \in X$,
- (2) symetrická, tj. $x \rho y$ implikuje $y \rho x$,
- (3) tranzitivní, tj. $x \rho y, y \rho z$ implikuje $x \rho z$.

Definice 5.5.3. Buďte $\equiv$ relace ekvivalence na množině X a $x, y \in X$. Jestliže $x \equiv y$, potom x je *ekvivalentní y vzhledem k $\equiv$* . Množina

$$\{y \in X \mid x \equiv y\}$$

všech prvků ekvivalentních prvku x je *třída ekvivalence* příslušná x vzhledem k $\equiv$, označujeme ji $[x]_{\equiv}$ nebo jen $[x]$, je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

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

Definice 5.5.4. Buď $\equiv$ relace ekvivalence na množině X . Množina

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

všech příslušných tříd ekvivalence je *faktorová množina* vzhledem k $\equiv$, označujeme ji $\tilde{X}_{\equiv}$ nebo jen $\tilde{X}$, je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

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

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

Definice 5.5.5. Buďte X množina s binární operací $*$ a $\equiv$ relace ekvivalence na množině X . Relace $\equiv$ je *kongruence* na X s $*$, jestliže platí *podmínka kompatibility*, čili implikace

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

nebo ekvivalentně

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

Tvrzení 5.5.1. Buďte $\equiv$ kongruence na množině s asociativní binární operací a x, y invertibilní prvky. Pak platí implikace

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

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 na $\mathbb{Z}$ s $+$, protože součet jakýchkoliv sudých čísel je sudé číslo, součet jakýchkoliv dvou lichých čísel je sudé číslo a součet jakéhokoliv sudého čísla a jakéhokoliv lichého čísla je liché číslo.

(2) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě záporná nebo obě kladná nebo obě nulová, tedy $\tilde{\mathbb{Z}} = \{[-1], [0], [1]\}$. Potom $\equiv$ je relace ekvivalence, platí implikace

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

ale existují $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ taková, že $x_1 \equiv x_2$ a $y_1 \equiv y_2$, ale $x_1 + y_1 \not\equiv x_2 + y_2$. Čili $\equiv$ nesplňuje podmínku kompatibility a není to tedy kongruence na $\mathbb{Z}$ s $+$.

(3) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě záporná nebo obě nezáporná, tedy $\tilde{\mathbb{Z}} = \{[-1], [0]\}$. Potom $\equiv$ je relace ekvivalence, ale existují $x, y \in \mathbb{Z}$ taková, že $x \equiv y$, ale $-x \not\equiv -y$. Podle Tvzení 5.5.1 $\equiv$ není kongruence na $\mathbb{Z}$ s $+$, a nesplňuje tedy podmínku kompatibility. $\square$

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

$$[x]\tilde{*}[y] = [x * y]. \quad (10)$$

Příklad. Mějme grupu $(\mathbb{Z}, +, 0, -)$ a na ní 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 binární operaci $\tilde{+}$ definovanou předpisem (10), tedy $[x]\tilde{+}[y] = [x + y]$. Takže

$$\begin{aligned} [0]\tilde{+}[0] &= [0 + 0] = [2 + 6] = [8 + (-14)] = [0], \\ [0]\tilde{+}[1] &= [0 + 1] = [2 + 7] = [(-6) + 11] = [1], \\ [1]\tilde{+}[0] &= [1 + 0] = [7 + 6] = [17 + (-2)] = [1], \\ [1]\tilde{+}[1] &= [1 + 1] = [3 + 13] = [(-7) + 5] = [0]. \end{aligned}$$

$\square$

Tvrzení 5.5.2. Mějme kongruenci na množině X s binární operací $*$. Bud' $\tilde{*}$ binární operace na $\tilde{X}$ definovaná předpisem (10). 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

$$[x] \tilde{*} [x^{-1}] = [x * x^{-1}] = [e],$$

$$[x^{-1}] \tilde{*} [x] = [x^{-1} * x] = [e],$$

takže $[x^{-1}]$ je inverzní prvek k $[x]$ vzhledem k operaci $\tilde{*}$.

(iv) Z (10) je zřejmé, že je-li $*$ komutativní, pak i $\tilde{*}$ je komutativní. $\square$

Důsledek. Pro každou (komutativní) grupu a každou kongruenci na této grupě příslušná faktorová množina s operací definovanou předpisem (10) je (komutativní) grupa.

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

Jelikož každý prvek množiny s asociativní operací má nejvýše jeden inverzní prvek, viz Tvzení 5.1.2 nebo Tvzení 5.5.1, třída $[x^{-1}]$ je v takovém případě jednoznačně určena třídou $[x]$, čili nezávisí na konkrétním výběru jejího prvku x , a proto je korektní ji označovat $[x]^{-1}$.

Definice 5.5.6. Faktorová množina s operací definovanou předpisem (10) z předchozího Důsledku je *faktorová grupa*.

Příklad. Mějme grupu $(\mathbb{Z}, +, 0, -)$ a na ní 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 $-[0] = [0]$, $-[1] = [-1] = [1]$. $\square$

5.6. Zbytkové třídy

Mějme aditivní grupu $(\mathbb{Z}, +, 0, -)$ a buď m libovolné přirozené (kladné celé) číslo. Definujme relaci $\equiv_m$ na $\mathbb{Z}$ předpisem:

$x \equiv_m y$ právě tehdy, když $x - y$ 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, 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 aditivní grupě $\mathbb{Z}$, čili podmínku kompatibility. Předpokládejme, že $[x_1]_m = [x_2]_m$ a $[y_1]_m = [y_2]_m$. To znamená, že $x_2 \in [x_1]_m$ a $y_2 \in [y_1]_m$, čili $x_2 = x_1 + km$, $y_2 = y_1 + lm$ pro vhodná $k, l \in \mathbb{Z}$. Potom $x_2 + y_2 = x_1 + km + y_1 + lm = x_1 + y_1 + (k+l)m \in [x_1 + y_1]_m$, a tedy $[x_1 + y_1]_m = [x_2 + y_2]_m$.

Na množině $\mathbb{Z}_m$ tedy máme binární operaci $+$ (značí se obvykle stejně jako původní operace) podle (10)

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

a příslušná faktorová grupa $(\mathbb{Z}_m, +, [0]_m, -)$ je komutativní *aditivní grupa zbytkových tříd modulo m* .

Na množině $\mathbb{Z}$ uvažujme operaci $\cdot$, která je asociativní a má neutrální prvek 1. Ověříme podmínku kompatibility pro operaci $\cdot$.

Předpokládejme, že $[x_1]_m = [x_2]_m$ a $[y_1]_m = [y_2]_m$. To znamená, že $x_2 = x_1 + km$, $y_2 = y_1 + lm$ pro vhodná $k, l \in \mathbb{Z}$. Potom $x_2 \cdot y_2 = (x_1 + km) \cdot (y_1 + lm) = x_1 y_1 + (k y_1 + l x_1 + k l m)m \in [x_1 y_1]_m$, a tedy $[x_1 y_1]_m = [x_2 y_2]_m$.

Na $\mathbb{Z}_m$ tedy máme i binární operaci $\cdot$ podle (10)

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

Podle Tvzení 5.5.2 operace $\cdot$ na množině $\mathbb{Z}_m$ je komutativní, asociativní a má neutrální prvek $[1]_m$. Faktorová množina $\mathbb{Z}_m$ s operací $\cdot$ a neutrálním prvkem $[1]_m$ je komutativní *multiplikativní monoid zbytkových tříd modulo m* (*monoid* je množina s asociativní binární operací a neutrálním prvkem). Otázka existence inverzí vzhledem k operaci $\cdot$ není tak jednoduchá jako v případě operace $+$.

Tvrzení 5.6.1. *Prvek $[x]_m \in \mathbb{Z}_m$ má inverzi vzhledem k operaci $\cdot$ právě tehdy, když x a m jsou nesoudělná, tedy jejich největší společný dělitel $D(x, m)$ je 1.*

Důkaz. Předpokládejme, že $[y]_m$ je inverze k $[x]_m$, tedy $[x]_m \cdot [y]_m = [xy]_m = [1]_m$. Takže $xy + km = 1$ pro vhodné $k \in \mathbb{Z}$ a každý společný dělitel čísel x a m je dělitel i čísla 1. Proto $D(x, m) = 1$.

Předpokládejme, že $D(x, m) = 1$. Podle Bézoutovy věty existují čísla $y, k \in \mathbb{Z}$ taková, že $D(x, m) = xy + km$, tedy $1 = xy + km$, takže $[1]_m = [xy]_m = [x]_m \cdot [y]_m$ a $[y]_m$ je inverze k $[x]_m$. $\square$

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
$[2]_5$	$\dots$		-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

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

Příklad. Nechť v některém roce připadá Štědrý den na středu. Není-li následující rok přestupný, potom v něm Štědrý den připadá na čtvrtek, protože $365 = 52 \cdot 7 + 1$, tedy $[365]_7 = [1]_7$. Je-li následující rok přestupný, potom v něm Štědrý den připadá na pátek, protože $366 = 52 \cdot 7 + 2$, tedy $[366]_7 = [2]_7$. □

6. OKRUHY A POLE

Definice 6.0.1. 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 součet a součin jsou pole.

(2) Množina $\mathbb{Z}$ s operacemi součet a součin je okruh, ale není pole.

(3) Množina $\mathbb{N}_0$ s operacemi součet a součin není okruh.

(4) Množina $P[x]$ s operacemi součet a součin polynomů je okruh, ale není pole.

(5) Množina $\mathcal{M}_n(P)$ s operacemi součet a součin matic není okruh.

(6) Pro každé $m \in \mathbb{N}$ množina $\mathbb{Z}_m$ zbytkových tříd s operacemi součet a součin je okruh. Totiž, $\mathbb{Z}_m$ splňuje podmínky (1)–(4) z definice okruhu podle kapitol 5.5 a 5.6 a to, že splňuje i distributivní zákon (5), lze snadno ověřit (cvičení).

(7) Okruh $\mathbb{Z}_m$ zbytkových tříd je pole právě tehdy, když m je prvočíslo (viz Tvzení 6.0.1).

(8) Nechť $P = \{0, 1\}$ a binární operace $+$ a $\cdot$ na P jsou takové, že

$+$	0	1		$\cdot$	0	1
0	0	1	a	0	0	0
1	1	0		1	0	1

Pro operaci $+$ neutrální prvek je 0 a inverzní (opačné) prvky jsou $-0 = 0$ a $-1 = 1$. Pro operaci $\cdot$ neutrální prvek je 1 a inverzní prvek k 1 je 1 ($1^{-1} = 1$), inverzní prvek k 0 neexistuje. Množina $\{0, 1\}$ s těmito operacemi je pole.

(9) Nechť $P = \{0, 1, 2, 3\}$ a binární operace $+$ a $\cdot$ na P jsou takové, že

$+$	0	1	2	3		$\cdot$	0	1	2	3
0	0	1	2	3	a	0	0	0	0	0
1	1	2	3	0		1	0	1	2	3
2	2	3	0	1		2	0	2	0	2
3	3	0	1	2		3	0	3	2	1

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

$-0 = 0$		0^{-1} neexistuje
$-1 = 3$	a	$1^{-1} = 1$
$-2 = 2$		2^{-1} neexistuje
$-3 = 1$		$3^{-1} = 3$

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

Tvrzení 6.0.1. Množina $\mathbb{Z}_m$ zbytkových tříd je pole právě tehdy, když m je prvočíslo.

Důkaz. Podle předchozího Příkladu (6) $\mathbb{Z}_m$ je okruh. Číslo 1 není prvočíslo a $\mathbb{Z}_1$ není pole (cvičení). Buď $m > 1$. 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 Tvzení 5.6.1 každé takové x je nesoudělné s m , tedy m je prvočíslo.

Na druhou stranu, je-li m prvočíslo, pak každé $x \in \mathbb{Z}$ takové, že $[x]_m \neq [0]_m$, je nesoudělné s m . Opět podle Tvzení 5.6.1 $[x]_m$ má inverzi.

Jiný důkaz tohoto tvrzení lze nalézt v [Marvan, 3. Pole]. $\square$

Takže, například, $\mathbb{Z}_4$ není pole. Čtyřprvkové pole ale existuje, viz následující příklad.

Příklad. Necht' $X = \{0, 1, a, b\}$ a binární operace $+$ a $\cdot$ na X jsou takové, že

$+$	0	1	a	b		$\cdot$	0	1	a	b
0	0	1	a	b		0	0	0	0	0
1	1	0	b	a	a	1	0	1	a	b
a	a	b	0	1		a	0	a	b	1
b	b	a	1	0		b	0	b	1	a

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

Poznámka. Buď n libovolné přirozené číslo. Potom existuje n -prvkové pole právě tehdy, když n je mocnina prvočísla, čili $n = p^k$, kde p je prvočíslo a k je přirozené číslo.

Tvrzení 6.0.2. Buď P okruh. Pak pro libovolné prvky $x, y, z \in P$ platí

- (i) $x \cdot 0 = 0$;
- (ii) $x \cdot (-1) = -x$;
- (iii) $x \cdot (y - z) = x \cdot y - x \cdot z$.

Důkaz. (i)

$$\begin{aligned} x \cdot 0 &= x \cdot 0 + 0 = & (0 &= x \cdot 0 + (-(x \cdot 0))) \\ &= x \cdot 0 + x \cdot 0 + (-(x \cdot 0)) = \\ &= x \cdot (0 + 0) + (-(x \cdot 0)) = \\ &= x \cdot 0 + (-(x \cdot 0)) = 0 \end{aligned}$$

(ii)

$$\begin{aligned} x + x \cdot (-1) &= x \cdot 1 + x \cdot (-1) = x \cdot (1 + (-1)) = x \cdot 0 = 0 \\ x \cdot (-1) + x &= x \cdot (-1) + x \cdot 1 = x \cdot (-1 + 1) = x \cdot 0 = 0 \end{aligned}$$

takže $x \cdot (-1) = -x$.

(iii) Cvičení. $\square$

Cvičení. Dokažte, že v každém okruhu platí:

(1) $(-1) \cdot (-1) = 1$,

(2) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$. $\square$

Tvrzení 6.0.3. 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 Tvzení 6.0.2(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 Tvzení 6.0.2(i) dostaneme

$$y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0.$$

(2)

$$\begin{aligned} y &= 1 \cdot y = & (1 &= x^{-1} \cdot x) \\ &= x^{-1} \cdot x \cdot y = & (x \cdot y &= x \cdot z) \\ &= x^{-1} \cdot x \cdot z = & (x^{-1} \cdot x &= 1) \\ &= 1 \cdot z = z \end{aligned}$$

□

Příklad. (1) V příkladu (9) máme okruh, v němž $2 \cdot 2 = 0$ a $2 \cdot 1 = 2 \cdot 3$. To ukazuje, že předchozí tvrzení neplatí pro okruhy.

(2) Pro okruh $P[x]$ ale předchozí tvrzení platí, viz kapitolu o polynomech. □

Obdobně jako v kapitole 5 P^* označuje množinu $P \setminus \{0\}$.

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

Tvrzení 6.0.4. *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 Tvzení 6.0.3(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. □

Stejně jako máme podgrupy grup (a podstruktury dalších algebraických struktur), existují podokruhy okruhů a podpole polí. Zmíníme jen podpole.

Definice 6.0.2. Buď P pole. Buď $Q \subseteq P$ podmnožina taková, že

- (1) $0, 1 \in Q$;
- (2) je-li $x, y \in Q$, pak $x + y \in Q$ a $xy \in Q$;
- (3) je-li $x \in Q$, pak $-x \in Q$;
- (4) je-li $x \in Q$, $x \neq 0$, pak $x^{-1} \in Q$.

Potom Q je *podpole* pole P .

Aby podmnožina pole byla podpole, musí obsahovat neutrální prvky obou binárních operací, musí být uzavřená vzhledem k oběma binárním operacím a musí být uzavřená vzhledem k inverzím vzhledem k oběma binárním operacím.

Každé podpole je pole.

Příklad. (1) Pole $\mathbb{Q}$ je podpole polí $\mathbb{R}$ a $\mathbb{C}$. Pole $\mathbb{R}$ je podpole pole $\mathbb{C}$.

(2) $\mathbb{Z}$ není podpole pole $\mathbb{Q}$, neboť neobsahuje inverzi k 2 vzhledem k operaci $\cdot$.

(3) Množina $\{0, 1\}$ není podpole pole $\mathbb{Q}$ (a samozřejmě ani $\mathbb{R}$ a $\mathbb{C}$), protože $1 + 1 = 2 \notin \{0, 1\}$. Ačkoliv, jak už víme, na množině $\{0, 1\}$ lze definovat operace součet a součin tak, že to je pole. □

Definice 6.0.3. Podpole pole $\mathbb{C}$ je *číselné pole*.

7. USPOŘÁDÁNÍ A SVAZY

7.1. Uspořádané množiny

Definice 7.1.1. Relace ρ 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, ρ) 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 $n = -1$). $\square$

Buď ρ uspořádání na množině X . Inverzní (opačná) relace ρ^{-1} (tj. relace definovaná předpisem „ $x \rho^{-1} y$ právě tehdy, když $y \rho x$ “) je také uspořádání. Nazývá se *duální uspořádání*. Máme-li uspořádání $\leq$, potom duální uspořádání $\leq^{-1}$ se označuje symbolem $\geq$. Podobně je to se symboly $\subseteq$ atp.

Definice 7.1.2. Buď $(X, \leq)$ uspořádaná množina, $Y \subseteq X$. Relace $\leq_Y$ na množině Y zadaná předpisem $x \leq_Y y \Leftrightarrow x \leq y$ je *indukované uspořádání* na množině Y a značí se rovněž $\leq$.

Definice 7.1.3. Prvky x, y uspořádané množiny jsou *srovnatelné*, platí-li $x \leq y$ nebo $y \leq x$. Uspořádaná množina je *řetězec*, jsou-li každé dva její prvky srovnatelné.

Příklad. $(\mathbb{R}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{N}, \leq)$ jsou řetězce. $\square$

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.

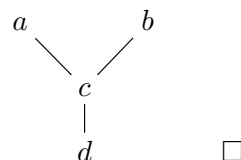
(3) V množině $\mathbb{Q}$ všech racionálních čísel s přirozeným uspořádáním podle velikosti neplatí $x \triangleleft y$ pro žádnou dvojici $x, y \in \mathbb{Q}$. Pro libovolné $x, y \in \mathbb{Q}$ takové, že $x < y$, platí $z = \frac{1}{2}(x + y) \in \mathbb{Q}$ a $x < z$, $z < y$. $\square$

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 7.1.4. Buď $(X, \leq)$ uspořádaná množina, $Y \subseteq X$. Prvek $x \in X$ je

- *dolní závora* množiny Y , je-li $x \leq y$ pro každé $y \in Y$;
- *horní závora* množiny Y , je-li $y \leq x$ pro každé $y \in Y$.

Příklad. V uspořádané množině Y z předchozího příkladu platí:

- c, d jsou dolní závory podmnožiny $\{a, b\}$,
- podmnožina $\{a, b\}$ nemá žádnou horní závoru.

Definice 7.1.5. Buď $(X, \leq)$ uspořádaná množina. Prvek $x \in X$ je

- *nejmenší (minimální)* prvek množiny X , je-li $x \leq y$ pro každé $y \in X$, v takovém případě píšeme $x = \min X$;
- *největší (maximální)* prvek množiny X , je-li $x \geq y$ pro každé $y \in X$, v takovém případě píšeme $x = \max X$.

Příklad. V uspořádané množině Y z předchozího příkladu platí:

- d je její nejmenší prvek,
- její největší prvek neexistuje.

Cvičení. Každá uspořádaná množina má nejvýše jeden největší prvek a nejvýše jeden nejmenší prvek.

Definice 7.1.6. Buď $(X, \leq)$ uspořádaná množina, $Y \subseteq X$. Prvek $x \in X$ je

- *infimum* množiny Y , je-li x největší prvek množiny všech dolních závor množiny Y , v takovém případě píšeme $x = \inf Y$,
- *supremum* množiny Y , je-li x nejmenší prvek množiny všech horních závor množiny Y , v takovém případě píšeme $x = \sup Y$.

Příklad. V uspořádané množině Y z předchozího příkladu platí:

- množina dolních závor podmnožiny $\{a, b\}$ je $\{c, d\}$, její největší prvek je c , a proto $\inf\{a, b\} = c$,
- podmnožina $\{a, b\}$ nemá žádnou horní závoru, čili množina horních závor je prázdná, nemá tedy nejmenší prvek, a proto $\sup\{a, b\}$ neexistuje.

Cvičení. (1) Každá podmnožina má nejvýše jedno supremum a nejvýše jedno infimum.

- (2) Jestliže $x \leq y$, pak $\inf\{x, y\} = x$ a $\sup\{x, y\} = y$.
 (3) Jestliže $\inf\{x, y\} = x$, pak $x \leq y$.
 (4) Jestliže $\sup\{x, y\} = y$, pak $x \leq y$. □

Cvičení. Buď X uspořádaná množina. Supremum prázdné množiny je nejmenší prvek množiny X (pokud existuje) a infimum prázdné množiny je největší prvek množiny X (pokud existuje). □

7.2. Svazově uspořádané množiny a svazy

Definice 7.2.1. Uspořádaná množina je *svazově uspořádaná*, jestliže každá její dvouprvková podmnožina má infimum i supremum.

Každá konečná podmnožina svazově uspořádané množiny má infimum i supremum.

- Příklad.** (1) Pro libovolnou množinu X je $(\mathcal{P}(X), \subseteq)$ svazově uspořádaná množina, přičemž pro libovolné $Y, Z \in \mathcal{P}(X)$ $\inf\{Y, Z\} = Y \cap Z$ a $\sup\{Y, Z\} = Y \cup Z$.
 (2) $(\mathbb{N}, |)$ je svazově uspořádaná množina, přičemž $\inf\{x, y\}$ je největší společný dělitel čísel x, y , $\sup\{x, y\}$ je nejmenší společný násobek čísel x, y .
 (3) $(\{1, 3, 5, 6, 9, 10, 12\}, |)$ není svazově uspořádaná množina.
 (4) Každý řetězec je svazově uspořádaná množina, přičemž $\inf\{x, y\} = \min\{x, y\}$ je menší z prvků x, y , $\sup\{x, y\} = \max\{x, y\}$ je větší z prvků x, y . □

Definice 7.2.2. Množina X se dvěma binárními operacemi $\wedge$ a $\vee$ je *svaz*, jestliže pro každé $x, y, z \in X$ platí

$$\begin{array}{lll} x \wedge y = y \wedge x, & x \vee y = y \vee x, & (\text{komutativita } \wedge \text{ a } \vee) \\ (x \wedge y) \wedge z = x \wedge (y \wedge z), & (x \vee y) \vee z = x \vee (y \vee z), & (\text{asociativita } \wedge \text{ a } \vee) \\ x \wedge (y \vee x) = x, & x \vee (y \wedge x) = x. & (\text{zákon absorpce}) \end{array}$$

Binární operace $\wedge$ je *průsek*, binární operace $\vee$ je *spojení*.

- Příklad.** (1) Pro libovolnou množinu X množina $\mathcal{P}(X)$ s operacemi $\cap$ a $\cup$ je svaz.
 (2) Množina $\mathbb{N}$ s operacemi D a N , kde $x D y$ je největší společný dělitel čísel x, y a $x N y$ je nejmenší společný násobek čísel x, y , je svaz.
 (3) Množina $\mathbb{R}$ s operacemi $\min$ a $\max$ je svaz.
 (4) Množina $\{0, 1\}$ pravdivostních hodnot s operacemi konjunkce a disjunkce je svaz. □

Tvrzení 7.2.1. Buď $(X, \wedge, \vee)$ svaz. Pro libovolné $x \in X$ platí

$$x \wedge x = x, \quad x \vee x = x. \quad (\text{idempotentnost } \wedge \text{ a } \vee)$$

Důkaz.

$$\begin{array}{ll} x \wedge x = & (\text{zákon absorpce}) \\ = x \wedge (x \vee (y \wedge x)) = & (\text{komutativita } \vee) \\ = x \wedge ((y \wedge x) \vee x) = & (\text{zákon absorpce}) \\ = x. & \end{array}$$

Druhou část tvrzení necháme jako cvičení. □

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

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

Podle následujícího tvrzení každá svazově uspořádaná množina s těmito operacemi je svaz.

Tvrzení 7.2.2. *Svazově uspořádaná množina X s binárními operacemi $\wedge$, $x \wedge y = \inf\{x, y\}$, $\vee$, $x \vee y = \sup\{x, y\}$, je svaz.*

Důkaz. Cvičení.

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

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). $\square$

Podle následujícího tvrzení každý svaz je svazově uspořádaná množina.

Tvrzení 7.2.3. *Buď $(X, \wedge, \vee)$ svaz.*

- (1) *Položme $x \leq_\wedge y$ právě tehdy, když $x \wedge y = x$. Pak $\leq_\wedge$ je uspořádání na X .*
- (2) *Položme $x \leq_\vee y$ právě tehdy, když $x \vee y = y$. Pak $\leq_\vee$ je uspořádání na X .*
- (3) *Uspořádání $\leq_\wedge$ je shodné s uspořádáním $\leq_\vee$ a $(X, \leq_\wedge)$ je svazově uspořádaná množina, přičemž*

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

Důkaz. Cvičení. $\square$

Svazy i svazově uspořádané množiny tedy můžeme chápat jak jako algebraické struktury tak jako uspořádané množiny. Uspořádání totiž jednoznačně určuje algebraickou strukturu a algebraická struktura zase jednoznačně určuje uspořádání.

Buď $(X, \wedge, \vee)$ svaz. Identity v definici svazu jsou symetrické vzhledem k vzájemné záměně $\wedge$ a $\vee$, proto $(X, \vee, \wedge)$ je také svaz. Nazývá se *duální svaz* a značí se X^* .

Cvičení. Ověřte, že duální svaz má duální uspořádání. $\square$

Tvrzení 7.2.4. *Buď X svaz. Pro každé $x, a, b \in X$ platí*

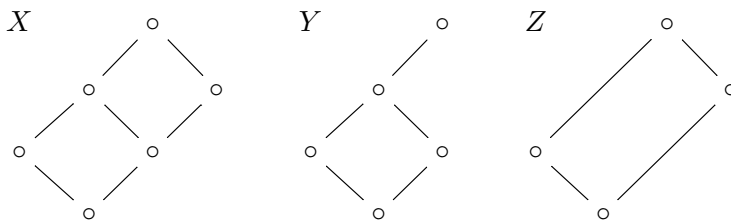
- (i) *jestliže $a \leq b$, pak $a \wedge x \leq b \wedge x$;*
- (ii) *jestliže $a \leq b$, pak $a \vee x \leq b \vee x$;*
- (iii) *jestliže $x \leq a$, $x \leq b$, pak $x \leq a \wedge b$;*
- (iv) *jestliže $x \geq a$, $x \geq b$, pak $x \geq a \vee b$.*

Důkaz. (i) Nechť $a \leq b$, pak $a \wedge b = a$, načež $(a \wedge x) \wedge (b \wedge x) = a \wedge b \wedge x = a \wedge x$; odtud tvrzení. (ii) Cvičení. (iii) a (iv) plynou ihned z definice infima a suprema (cvičení). $\square$

Obsahuje-li podmnožina svazu všechna infima a suprema všech dvojic svých prvků, je to také svaz.

Definice 7.2.3. *Podsvaz svazu $(X, \wedge, \vee)$ je podmnožina $Y \subseteq X$ taková, že pro každé $x, y \in Y$ platí $x \wedge y \in Y$ a $x \vee y \in Y$.*

Příklad. Svaz X a jeho podsvazy Y a Z :



□

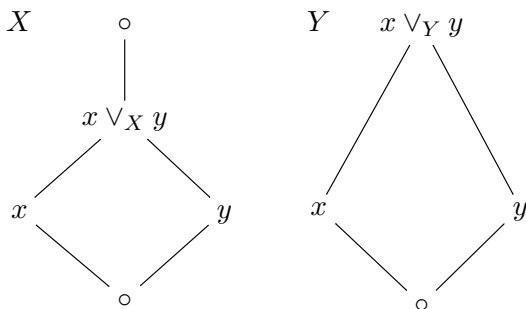
Cvičení. (1) Každá podmnožina řetězce je podsvaz.

(2) Každá podmnožina svazu, která je řetězcem, je podsvaz.

□

Podmnožina svazu může být svazem vzhledem k indukovanému uspořádání, aniž by byla podsvazem.

Příklad. Svaz X a jeho podmnožina Y , která je svazem, ale není podsvazem.



Supremum $x \vee_Y y$ v Y je různé od suprema $x \vee_X y$ v X .

□

7.3. Úplné svazy

Definice 7.3.1. Svaz je *úplný*, má-li každá jeho podmnožina supremum i infimum.

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

(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 7.3.1. Buď X uspořádaná množina, jejíž každá podmnožina má infimum. Pak X je úplný svaz.

Důkaz. Stačí ukázat, že každá podmnožina má supremum. Buď $Y \subseteq X$. Označme Z množinu všech horních závor množiny Y a položme $s = \inf Z$. Dokažme, že $s = \sup Y$.

Každý prvek množiny Z je horní závora množiny Y , takže každý prvek množiny Y je dolní závora množiny Z . Jelikož s je největší dolní závora množiny Z , tak $y \leq s$ pro každé $y \in Y$, čili s je zároveň horní závora množiny Y . A když $s \in Z$ a současně s je (největší) dolní závora množiny Z , je to nejmenší prvek množiny Z , čili nejmenší horní závora množiny Y . □

Příklad. Předpoklad, že každá (i prázdná) podmnožina množiny X má infimum, znamená, že X má největší prvek. Například $(\mathbb{N}, \leq)$ není úplný svaz, přestože každá neprázdná podmnožina má infimum. $\square$

Příklad. Buďte G grupa a $P(G)$ množina všech podgrup grupy G . Pak $(P(G), \subseteq)$ je úplný svaz.

Buď $\{A_\iota \mid \iota \in I\} \subseteq P(G)$, tedy nějaký systém podgrup grupy G . Potom $\bigcap_{\iota \in I} A_\iota$ je také podgrupa (cvičení), která je zároveň $\inf\{A_\iota \mid \iota \in I\}$ (cvičení). Podle předchozího tvrzení je $(P(G), \subseteq)$ úplný svaz. Proto existuje i $\sup\{A_\iota \mid \iota \in I\}$ a je to průnik všech podgrup, které obsahují všechny podgrupy A_ι .

Příklad je zformulován pro grupy, ale jeho analogie platí i pro jiné algebraické struktury. $\square$

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. $\square$

8. HOMOMORFISMY

8.1. Homomorfismy a izomorfismy grup

8.1.1. Homomorfismy grup

Definice 8.1.1. Bud' $(X, *, e_X, {}^{-1})$, $(Y, \diamond, e_Y, {}^{-1})$ 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) Bud' $X = \{0, 1, 2, 3\}$ a $Y = \{0, 1\}$ s binárními operacemi $+$ takovými, že

$+$	0	1	2	3		$+$	0	1
0	0	1	2	3		0	0	1
1	1	2	3	0	a	0	0	1
2	2	3	0	1		1	1	0
3	3	0	1	2				

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. $\square$

Tvrzení 8.1.1. Bud' $(X, *, e_X, {}^{-1})$, $(Y, \diamond, e_Y, {}^{-1})$ 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 $f(x)$. $\square$

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 . $\square$

Tvrzení 8.1.2. *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. Budte $(X, *, e_X, {}^{-1}), (Y, \diamond, e_Y, {}^{-1}), (Z, \cdot, e_Z, {}^{-1})$ grupy. Pro každé $x_1, x_2 \in X$ platí

$$\begin{aligned} (g \circ f)(x_1 * x_2) &= g(f(x_1 * x_2)) = \\ &= g(f(x_1) \diamond f(x_2)) = \\ &= g(f(x_1)) \cdot g(f(x_2)) = \\ &= (g \circ f)(x_1) \cdot (g \circ f)(x_2). \end{aligned}$$

Zbytek vyplývá z předchozího tvrzení. □

8.1.2. Izomorfismy grup

Definice 8.1.2. Bijektivní homomorfismus grup je *izomorfismus grup*.

Tvrzení 8.1.3. *Bud' $f: X \rightarrow Y$ izomorfismus grup. Pak $f^{-1}: Y \rightarrow X$ je izomorfismus grup.*

Důkaz. Budte $(X, *, e_X, {}^{-1}), (Y, \diamond, e_Y, {}^{-1})$ grupy. Inverzní zobrazení je bijektivní. Pro libovolné $y_1, y_2 \in Y$ označme $x_1 = f^{-1}(y_1)$ a $x_2 = f^{-1}(y_2)$. Takže $f(x_1) = y_1$ a $f(x_2) = y_2$. Potom

$$\begin{aligned} f^{-1}(y_1 \diamond y_2) &= f^{-1}(f(x_1) \diamond f(x_2)) = f^{-1}(f(x_1 * x_2)) = x_1 * x_2 = \\ &= f^{-1}(y_1) * f^{-1}(y_2). \end{aligned}$$

Zbytek vyplývá z Tvrzení 8.1.1. □

Příklad. (1) Každá identita je izomorfismus.

(2) Označme $\mathbb{R}_+$ množinu všech kladných reálných čísel. Pak $(\mathbb{R}_+, \cdot, 1, {}^{-1})$ je grupa (cvičení). Zobrazení $\exp: (\mathbb{R}, +, 0, -) \rightarrow (\mathbb{R}_+, \cdot, 1, {}^{-1}), x \mapsto e^x$ 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

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

Definice 8.1.3. Grupy X, Y jsou *izomorfní*, jestliže existuje izomorfismus $X \rightarrow Y$. Zapisujeme $X \cong Y$.

Tvrzení 8.1.4. *Pro libovolné grupy X, Y, Z platí*

- (i) $X \cong X$ (reflexivita),
- (ii) jestliže $X \cong Y$, pak $Y \cong X$ (symetrie),
- (iii) jestliže $X \cong Y$ a $Y \cong Z$, pak $X \cong Z$ (tranzitivita).

Důkaz. Cvičení. □

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

Cvičení. Bud' $h: X \rightarrow Y$ 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: $\tilde{X} \rightarrow \text{Im } h, [x] \mapsto h(x)$. $\square$

8.2. Homomorfismy a izomorfismy polí

Definice 8.2.1. Budťe 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 $f(p^{-1}) = (f(p))^{-1}$.

O zobrazeních polí platí následující tvrzení obdobné Tvrzení 8.1.1 o zobrazeních grup.

Tvrzení 8.2.1. Budťe P, Q pole. Budť $f: P \rightarrow Q$ zobrazení takové, že pro každé $p_1, p_2 \in P$ platí

- (i) $f(p_1 + p_2) = f(p_1) + f(p_2)$,
- (ii) $f(p_1 \cdot p_2) = f(p_1) \cdot f(p_2)$,
- (iii) $f(1) \neq 0$.

Pak f je homomorfismus polí $P \rightarrow Q$.

Důkaz. Cvičení. $\square$

Definice 8.2.2. Bijektivní homomorfismus polí je *izomorfismus polí*. Pole jsou *izomorfní*, jestliže mezi nimi existuje izomorfismus.

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

8.3. Izotonní zobrazení, homomorfismy a izomorfismy svazů

8.3.1. Izotonní zobrazení a izomorfismy uspořádaných množin

Definice 8.3.1. Budťe $(X, \leq), (Y, \leq)$ uspořádané množiny. Zobrazení $f: X \rightarrow Y$ je *izotonní*, jestliže platí implikace

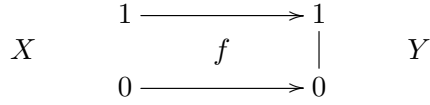
$$x \leq y \Rightarrow f(x) \leq f(y).$$

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 $2 \nmid 3$). $\square$

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



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

Cvičení. Složení izotonních zobrazení je izotonní zobrazení. $\square$

8.3.2. Homomorfismy a izomorfismy svazů

Definice 8.3.2. Buďte $(X, \wedge, \vee)$, $(Y, \wedge, \vee)$ svazy. Zobrazení $f: X \rightarrow Y$ je *homomorfismus svazů*, jestliže pro každé $x_1, x_2 \in X$

$$f(x_1 \wedge x_2) = f(x_1) \wedge f(x_2)$$

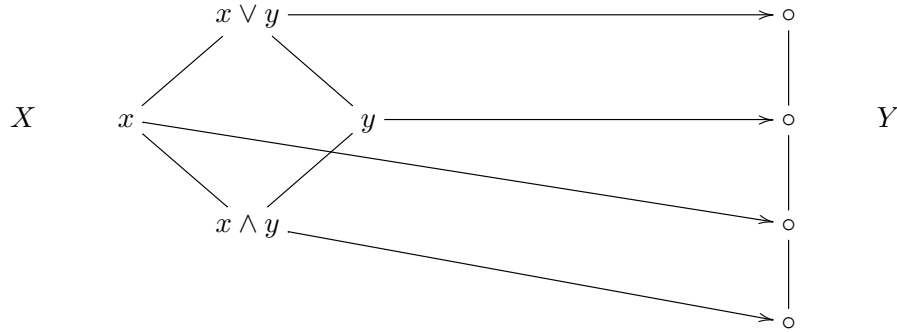
$$f(x_1 \vee x_2) = f(x_1) \vee f(x_2).$$

Tvrzení 8.3.1. Každý homomorfismus svazů je izotonní zobrazení.

Důkaz. Buďte $(X, \wedge, \vee)$, $(Y, \wedge, \vee)$ svazy, $f: X \rightarrow Y$ 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 $f(x_1) \leq f(x_2)$. $\square$

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

$$f(x) \vee f(y) = f(y) \neq f(x \vee y).$$

$\square$

Definice 8.3.3. Bijektivní homomorfismus svazů je *izomorfismus svazů*.

Cvičení. Buď f zobrazení svazů. Dokažte, že následující výroky jsou ekvivalentní:

- (1) f je izomorfismus uspořádaných množin;
- (2) f je izomorfismus svazů.

$\square$

9. VEKTOROVÉ PROSTORY

9.1. Definice, příklady, základní vlastnosti

Vektor je běžně znázorňován v rovině nebo v prostoru jako orientovaná úsečka (šipka), která má počáteční bod a koncový bod. Pokud je možné jeden takový vektor převést na druhý takový vektor rovnoběžným posunutím, říká se, že tyto dva vektory jsou totožné nebo ekvivalentní, nebo že jsou to dvě umístění jednoho vektoru. Takové vektory se sčítají pomocí pravidla rovnoběžníku a násobí se reálným číslem tak, že šipka se příslušně prodlouží nebo zkrátí a při násobení záporným číslem navíc změní směr na opačný.

Obecně definujeme vektor jako prvek vektorového prostoru a vektorový prostor nad nějakým polem jako množinu s operací sčítání a s násobením prvků množiny prvky pole s takovými vlastnostmi, které umožňují představu vektoru jako šipky a představu sčítání vektorů a násobení vektoru prvkem pole, jak je uvedeno v předchozím odstavci.

Definice 9.1.1. Buď V neprázdná množina, P pole. *Vektorový prostor V nad polem P* je množina V spolu s binární operací $+: V \times V \rightarrow V$, $(u, v) \mapsto u + v$, a zobrazením $\cdot: P \times V \rightarrow V$, $(p, v) \mapsto p \cdot v$, takovými, že

- (1) pro každé $u, v, w \in V$ platí $(u + v) + w = u + (v + w)$,
- (2) existuje $0 \in V$ takový, že pro každé $v \in V$ platí $v + 0 = v$,
- (3) pro každé $v \in V$ existuje $-v \in V$ takové, že $v + (-v) = 0$,
- (4) pro každé $u, v \in V$ platí $u + v = v + u$,
- (5) pro každé $v \in V$ platí $1 \cdot v = v$,
- (6) pro každé $p, q \in P$ a $v \in V$ platí $(p \cdot q) \cdot v = p \cdot (q \cdot v)$,
- (7) pro každé $p, q \in P$ a $v \in V$ platí $(p + q) \cdot v = (p \cdot v) + (q \cdot v)$,
- (8) pro každé $p \in P$ a $u, v \in V$ platí $p \cdot (u + v) = (p \cdot u) + (p \cdot v)$.

Prvky množiny V jsou *vektory*, prvky pole P jsou *skaláry*. Binární operace $+$ je *sčítání*, zobrazení $\cdot$ je *násobení skalárem*, vektor $0 \in V$ je *nulový vektor* nebo *nula*, vektor $-v$ je *opačný vektor* k vektoru v .

Podmínky (1)–(8) jsou *axiomy vektorového prostoru*. Podmínky (1)–(4) znamenají, že V s operací $+$ je komutativní grupa.

Jelikož každá binární operace má nejvýše jeden neutrální prvek, ve vektorovém prostoru existuje jediný nulový vektor. Obdobně, jelikož každý prvek má vzhledem k asociativní binární operaci nejvýše jeden inverzní prvek, ke každému vektoru existuje jediný opačný vektor.

Násobení skalárem $\cdot: P \times V \rightarrow V$, $(p, v) \mapsto p \cdot v$, není binární operace (není-li $P = V$), ale nazývá se *vnější operace*, a místo $p \cdot v$ se často píše jen pv . Binární operace se někdy nazývá *vnitřní operace*.

Vektorový prostor nad polem $\mathbb{R}$, nebo $\mathbb{C}$ je *reálný*, resp. *komplexní* vektorový prostor.

Příklad. (1) Vektorový prostor Eukleidovské geometrie, dvojrozměrné i trojrozměrné, kde vektor je třída ekvivalentních šipek a je reprezentován jednotlivými šipkami, jak je uvedeno v prvním odstavci této kapitoly.

Nulový vektor je reprezentován degenerovanou úsečkou nulové délky. Vektorový prostor v rovině resp. prostoru značíme E^2 resp. E^3 .

(2) Buď V jednoprvková množina, P pole. Jediný prvek množiny V označme 0 a položme $0 + 0 = 0$, $-0 = 0$ a $p \cdot 0 = 0$ pro každé $p \in P$. Dostáváme vektorový prostor nazývaný *nulový prostor* nebo *triviální prostor*.

(3) Každé pole je vektorový prostor nad sebou samým. Položíme-li v definici vektorového prostoru $V = P$, budou všechny axiomy vektorového prostoru důsledky axiomů

pole (ověřte). Získáváme tak například vektorový prostor $\mathbb{R}$ nad $\mathbb{R}$, vektorový prostor $\mathbb{C}$ nad $\mathbb{C}$, vektorový prostor $\mathbb{Q}$ nad $\mathbb{Q}$ a vektorový prostor $\mathbb{Z}_2$ nad $\mathbb{Z}_2$.

(4) Každé pole je vektorový prostor nad libovolným svým podpolem. Jediný rozdíl oproti předchozímu příkladu spočívá v tom, že násobení skalárem je dovoleno jen pro skaláry z podpole.

(5) Buď $n \in \mathbb{N}$, P pole. Na množině P^n všech uspořádaných n -tic prvků P zavedme sčítání a násobení skalárem předpisem

$$(u_1, u_2, \dots, u_n) + (v_1, v_2, \dots, v_n) = (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n),$$

$$p(u_1, u_2, \dots, u_n) = (pu_1, pu_2, \dots, pu_n).$$

Vzniká vektorový prostor P^n nad polem P (ověřte). Například řádky a sloupky matic jsou prvky takových vektorových prostorů.

(6) Vektorový prostor P^n nad podpolem $Q \subset P$.

(7) Vektorový prostor matic typu $m \times n$ nad polem P s operacemi sčítání a násobení skalárem. Značí se $P^{m \times n}$ nebo $\mathcal{M}_{m \times n}(P)$ (resp. $\mathcal{M}_m(P)$ nebo $\text{gl}(m, P)$ v případě čtvercových matic).

(8) Vektorový prostor polynomů stupně nejvýše n nad polem P s operacemi sčítání a násobení skalárem.

(9) Vektorový prostor polynomů nad polem P s operacemi sčítání a násobení skalárem.

(10) Vektorový prostor všech řešení homogenní soustavy rovnic.

(11) Buď X množina, P pole. Na množině P^X všech zobrazení $X \rightarrow P$ zavedme sčítání a násobení skalárem předpisem

$$(u + v)(x) = u(x) + v(x),$$

$$(pu)(x) = p \cdot u(x).$$

Vzniká vektorový prostor P^X nad polem P (ověřte). Speciální případy jsou množina všech funkcí z $\mathbb{R}$ do $\mathbb{R}$, množina všech spojitých funkcí na $\mathbb{R}$, množina diferencovatelných funkcí na $\mathbb{R}$, množina všech spojitých funkcí na intervalu $[a, b]$. $\square$

Tvrzení 9.1.1. Buď V vektorový prostor nad polem P . Pak pro každé $u, v \in V$, $p, q \in P$ platí

- (i) $0 \cdot v = 0$,
- (ii) $(-1) \cdot v = -v$,
- (iii) $(p - q) \cdot v = p \cdot v - q \cdot v$,
- (iv) $p \cdot (u - v) = p \cdot u - p \cdot v$,
- (v) Je-li $p \cdot v = 0$, pak buď $p = 0$ nebo $v = 0$.

Důkaz. Cvičení. $\square$

9.2. Lineární kombinace, generátory, lineární nezávislost

Buď V vektorový prostor nad polem P .

Definice 9.2.1. Buďte $n \in \mathbb{N}$, $v_1, v_2, \dots, v_n \in V$ a $p^1, p^2, \dots, p^n \in P$. Lineární kombinace vektorů $v_1, v_2, \dots, v_n$ s koeficienty $p^1, p^2, \dots, p^n$ je vektor

$$p^1 v_1 + p^2 v_2 + \dots + p^n v_n \in V.$$

Lineární kombinace prázdné množiny je nulový vektor $0 \in V$.

Příklad. (1) Součet vektorů u, v je jejich lineární kombinace s koeficienty 1, 1. Opačný vektor k v je jeho lineární kombinace (skalární násobek) s koeficientem -1 :

$$u + v = 1 \cdot u + 1 \cdot v, \quad -v = (-1) \cdot v.$$

(2) Lineární kombinace vektorů $1, 6 \in \mathbb{R}$ s koeficienty $3, 1 \in \mathbb{R}$ je $3 \cdot 1 + 1 \cdot 6 = 9$.

(3) Lineární kombinace vektorů $(1, 2, 0), (2, 3, 1) \in \mathbb{R}^3$ s koeficienty $-3, 2 \in \mathbb{R}$ je

$$(-3) \cdot (1, 2, 0) + 2 \cdot (2, 3, 1) = (1, 0, 2).$$

□

Definice 9.2.2. Buď $U \subseteq V$. *Lineární obal* množiny U je množina $\llbracket U \rrbracket$ všech lineárních kombinací konečně mnoha vektorů množiny U . Pro $U = \{u_1, u_2, \dots, u_n\}$ je

$$\llbracket U \rrbracket = \llbracket u_1, u_2, \dots, u_n \rrbracket = \{p^1 u_1 + p^2 u_2 + \dots + p^n u_n \mid p^1, p^2, \dots, p^n \in P\}.$$

Lineární obal prázdné množiny je $\llbracket \emptyset \rrbracket = \{0\} \subset V$.

Definice 9.2.3. Množina $\{v_1, v_2, \dots, v_n\} \subset V$ *generuje* V , je-li každý vektor $v \in V$ lineární kombinací vektorů $v_1, v_2, \dots, v_n$, to jest, jestliže pro každý vektor $v \in V$ existují skaláry $p^1, p^2, \dots, p^n \in P$ takové, že $v = p^1 v_1 + p^2 v_2 + \dots + p^n v_n$, to jest, jestliže $\llbracket v_1, v_2, \dots, v_n \rrbracket = V$.

V takovém případě také $\{v_1, v_2, \dots, v_n\}$ je *množina generátorů* prostoru V nebo vektory $v_1, v_2, \dots, v_n \in V$ *generují* V nebo V je *generován* vektory $v_1, v_2, \dots, v_n$.

Příklad. (1) Prostor $\mathbb{R}^3$ je generován vektory $(1, 0, 0), (0, 1, 0), (0, 0, 1)$. Skutečně, libovolný vektor $(x, y, z) \in \mathbb{R}^3$ je jejich lineární kombinací s koeficienty x, y, z :

$$(x, y, z) = x \cdot (1, 0, 0) + y \cdot (0, 1, 0) + z \cdot (0, 0, 1).$$

(2) Prostor $\mathbb{R}^3$ je generován vektory $(1, 0, 0), (1, 1, 0), (1, 1, 1)$. Skutečně, libovolný vektor $(x, y, z) \in \mathbb{R}^3$ je jejich lineární kombinací s koeficienty $x - y, y - z, z$:

$$(x, y, z) = (x - y) \cdot (1, 0, 0) + (y - z) \cdot (1, 1, 0) + z \cdot (1, 1, 1).$$

(3) Prostor $\mathbb{R}^3$ je generován vektory $(1, 0, 0), (0, 1, 0), (0, 0, 1), (3, 4, 5)$. Libovolný vektor $(x, y, z) \in \mathbb{R}^3$ je jejich lineární kombinací s koeficienty $x, y, z, 0$:

$$(x, y, z) = x \cdot (1, 0, 0) + y \cdot (0, 1, 0) + z \cdot (0, 0, 1) + 0 \cdot (3, 4, 5).$$

V tomto případě můžeme najít dokonce nekonečně mnoho vyjádření ve tvaru lineární kombinace, pro libovolný parametr $t \in \mathbb{R}$ platí

$$(x, y, z) = (x - 3t) \cdot (1, 0, 0) + (y - 4t) \cdot (0, 1, 0) + (z - 5t) \cdot (0, 0, 1) + t \cdot (3, 4, 5).$$

(4) Prostor $\mathbb{R}^3$ není generován vektory $(1, 2, 0), (3, 4, 0), (5, 6, 0)$. Ověřte.

(5) Vektory $v_1, v_2, \dots, v_n \in \mathbb{R}^m$, kde $v_i = (v_i^1, v_i^2, \dots, v_i^m)$, generují $\mathbb{R}^m$, jestliže soustava

$$\begin{aligned} v_1^1 x^1 + v_2^1 x^2 + \dots + v_n^1 x^n &= v^1 \\ v_1^2 x^1 + v_2^2 x^2 + \dots + v_n^2 x^n &= v^2 \\ &\vdots \\ v_1^m x^1 + v_2^m x^2 + \dots + v_n^m x^n &= v^m \end{aligned}$$

o neznámých $x^1, x^2, \dots, x^n$ má řešení pro každou pravou stranu $v^1, v^2, \dots, v^m$. Soustava je totiž ekvivalentní s podmínkou

$$x^1 \begin{pmatrix} v_1^1 \\ v_1^2 \\ \vdots \\ v_1^m \end{pmatrix} + x^2 \begin{pmatrix} v_2^1 \\ v_2^2 \\ \vdots \\ v_2^m \end{pmatrix} + \dots + x^n \begin{pmatrix} v_n^1 \\ v_n^2 \\ \vdots \\ v_n^m \end{pmatrix} = \begin{pmatrix} v^1 \\ v^2 \\ \vdots \\ v^m \end{pmatrix}.$$

(6) Prostor $\mathbb{R}_2[x]$ polynomů neurčité x s reálnými koeficienty stupně nejvýše 2 je generován vektory $x^2, x+1, 1$. Ověřte. $\square$

Definice 9.2.4. Prostor, který má konečnou množinu generátorů, je *konečněrozměrný*.

Příklad. Vektorový prostor $\mathbb{R}[x]$ všech polynomů s reálnými koeficienty není konečněrozměrný. Pro libovolné $p_1, \dots, p_n \in \mathbb{R}[x]$ existuje přirozené číslo m , které je větší než stupeň kteréhokoliv z polynomů $p_1, \dots, p_n$. Pak polynom $x^m \in \mathbb{R}[x]$ není lineární kombinací polynomů $p_1, \dots, p_n$, takže polynomy $p_1, \dots, p_n$ negenerují $\mathbb{R}[x]$. $\square$

Cvičení. (1) Jestliže $v_1, \dots, v_n$ generují V a v_i je lineární kombinací ostatních, pak $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$ také generují V . Dokažte.

(2) Nechť každý z vektorů $v_1, \dots, v_n$ je lineární kombinací vektorů $u_1, \dots, u_m \in V$. Jestliže $v_1, \dots, v_n$ generují V , pak $u_1, \dots, u_m$ také generují V . Dokažte. $\square$

Definice 9.2.5. (1) Množina vektorů $\{v_1, v_2, \dots, v_n\} \subseteq V$ je *lineárně nezávislá*, jestliže pro libovolné $x^1, x^2, \dots, x^n \in P$ z rovnosti

$$x^1 v_1 + x^2 v_2 + \dots + x^n v_n = 0 \quad \text{plyne} \quad x^1 = x^2 = \dots = x^n = 0.$$

(2) Množina vektorů $\{v_1, v_2, \dots, v_n\} \subseteq V$ je *lineárně závislá*, jestliže není lineárně nezávislá.

Často se zjednodušeně a nepřesně říká, že nějaké vektory jsou lineárně (ne)závislé. Myslí se tím, že příslušná množina vektorů je lineárně (ne)závislá.

Příklad. (1) Množina $\{7\} \subset \mathbb{R}$ je lineárně nezávislá. Je-li $x \cdot 7 = 0$ pro nějaké $x \in \mathbb{R}$, pak $x = 0$ (pro nenulové x uvedená rovnost $x \cdot 7 = 0$ neplatí).

(2) Množina $\{2, 3\} \subset \mathbb{R}$ je lineárně závislá. Lineární kombinace $x^1 \cdot 2 + x^2 \cdot 3$ může být rovna 0, i když je některý z koeficientů x^1, x^2 nenulový, například $x^1 = 3, x^2 = -2$.

(3) Množina $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\} \subset \mathbb{R}^3$ je lineárně nezávislá. Lineární kombinace $x \cdot (1, 0, 0) + y \cdot (0, 1, 0) + z \cdot (0, 0, 1)$ je vektor (x, y, z) , který je roven $(0, 0, 0)$ právě tehdy, když $x = y = z = 0$ (ověřte).

(4) Množina $\{(1, 0, 0), (1, 1, 0), (1, 1, 1)\} \subset \mathbb{R}^3$ je lineárně nezávislá. Lineární kombinace $x \cdot (1, 0, 0) + y \cdot (1, 1, 0) + z \cdot (1, 1, 1)$ je vektor $(x + y + z, y + z, z)$, který je roven $(0, 0, 0)$ právě tehdy, když $x = y = z = 0$ (ověřte).

(5) Množina $\{(1, 0, -1), (0, 1, 2), (2, 1, 0)\} \subset \mathbb{R}^3$ je lineárně závislá. Lineární kombinace $x \cdot (1, 0, -1) + y \cdot (0, 1, 2) + z \cdot (2, 1, 0)$ je vektor $(x + 2z, y + z, -x + 2y)$, který je roven $(0, 0, 0)$ i pro nenulové koeficienty x, y, z , například $x = 2, y = 1, z = -1$. Ověřte.

(6) Libovolná množina vektorů obsahující nulový vektor je lineárně závislá. Lineární kombinace $0 \cdot v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_n + 1 \cdot 0$ je nulový vektor a přitom aspoň jeden koeficient je nenulový.

(7) Množina $\{v_1, \dots, v_n\} \subset \mathbb{R}^m$, kde $v_i = (v_i^1, \dots, v_i^m)$, je lineárně nezávislá právě tehdy, když soustava

$$\begin{aligned} v_1^1 x^1 + v_2^1 x^2 + \dots + v_n^1 x^n &= 0 \\ v_1^2 x^1 + v_2^2 x^2 + \dots + v_n^2 x^n &= 0 \\ &\vdots \\ v_1^m x^1 + v_2^m x^2 + \dots + v_n^m x^n &= 0 \end{aligned}$$

má právě jedno řešení, a to sice $x^1 = x^2 = \dots = x^n = 0$.

(8) Množina $\{x^2, x, 1\} \subset \mathbb{R}_2[x]$ je lineárně nezávislá. Ověřte.

(9) Prázdná množina je lineárně nezávislá, protože všechny koeficienty z prázdné množiny koeficientů jsou nulové. $\square$

Cvičení. (1) Libovolná podmnožina lineárně nezávislé množiny vektorů je lineárně nezávislá. Dokažte.

(2) Jednoprvková množina $\{v\} \subset V$ je lineárně nezávislá právě tehdy, když $v \neq 0$. Dokažte. $\square$

Tvrzení 9.2.1. Množina vektorů $\{v_1, \dots, v_n\}$ je lineárně závislá právě tehdy, když aspoň jeden z nich je lineární kombinací ostatních, tj. právě když existuje index i takový, že vektor v_i je lineární kombinací vektorů $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$.

Důkaz. „ $\Rightarrow$ “ Předpokládejme, že množina $\{v_1, \dots, v_n\}$ je lineárně závislá, tedy že existují koeficienty $a^1, \dots, a^n$ takové, že $a^1 v_1 + \dots + a^i v_i + \dots + a^n v_n = 0$ a aspoň jeden z nich je nenulový (například a^i). Potom

$$v_i = -\frac{a^1}{a^i} v_1 - \dots - \frac{a^{i-1}}{a^i} v_{i-1} - \frac{a^{i+1}}{a^i} v_{i+1} - \dots - \frac{a^n}{a^i} v_n,$$

a vektor v_i je tedy lineární kombinací ostatních.

„ $\Leftarrow$ “ Necht vektor v_i je lineární kombinací vektorů $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$, tedy existují koeficienty $a^1, \dots, a^{i-1}, a^{i+1}, \dots, a^n$ takové, že

$$v_i = a^1 v_1 + \dots + a^{i-1} v_{i-1} + a^{i+1} v_{i+1} + \dots + a^n v_n.$$

Potom

$$a^1 v_1 + \dots + a^{i-1} v_{i-1} - v_i + a^{i+1} v_{i+1} + \dots + a^n v_n = 0$$

s nenulovým koeficientem (-1) u vektoru v_i . Tedy, množina $\{v_1, \dots, v_n\}$ je lineárně závislá. $\square$

Tvrzení 9.2.2. Množina vektorů $\{v_1, \dots, v_n\}$ je lineárně závislá právě tehdy, když aspoň jeden z nich je lineární kombinací předchozích, tj. právě když existuje index i takový, že vektor v_i je lineární kombinací vektorů $v_1, \dots, v_{i-1}$.

Důkaz. „ $\Rightarrow$ “ Postupujeme jako v důkazu předchozího tvrzení, jen nenulový koeficient a^i vybereme s nejvyšším možným indexem. To znamená, že $a^{i+1} = \dots = a^n = 0$ a zbytek je zřejmý.

Jako cvičení rozeberte podrobně případ $i = 1$, kdy bude množina předcházejících vektorů prázdná.

„ $\Leftarrow$ “ Tvrzení je speciálním případem předchozího. $\square$

Definice 9.2.6. *Elementární úprava n -tice vektorů $(v_1, \dots, v_n)$ je:*

- (i) vynásobení vektoru nenulovým skalárem c ;
- (ii) přičtení c -násobku j -tého vektoru k i -tému vektoru, kde $i \neq j$;
- (iii) výměna i -tého vektoru s j -tým vektorem.

Při tom vznikají po řadě n -tice

$$\begin{aligned} &(v_1, \dots, v_{i-1}, cv_i, v_{i+1}, \dots, v_n), \\ &(v_1, \dots, v_{i-1}, v_i + cv_j, v_{i+1}, \dots, v_j, \dots, v_n), \\ &(v_1, \dots, v_{i-1}, v_j, v_{i+1}, \dots, v_{j-1}, v_i, v_{j+1}, \dots, v_n). \end{aligned}$$

Ke každé z těchto úprav existuje úprava inverzní, která je rovněž elementární a stejného typu (ověřte).

Definice 9.2.7. Dvě n -tice vektorů jsou *ekvivalentní*, jestliže jedna vznikne z druhé konečnou posloupností elementárních úprav.

Cvičení. Ukažte, že právě zavedená relace mezi n -ticemi vektorů je reflexivní, symetrická a tranzitivní. $\square$

Příklad. Mějme matici typu $m \times n$ nad polem P . Její řádky jsou uspořádané n -tice prvků pole P , tj. vektory z prostoru P^n . Celá matice je pak m -tice takových n -tic, tedy m -tici vektorů z prostoru P^n . Elementární úpravy této m -tice vektorů jsou právě elementární řádkové úpravy dané matice. $\square$

Tvrzení 9.2.3. *Nechť n -tice $(u_1, \dots, u_n)$ je ekvivalentní s n -ticí $(v_1, \dots, v_n)$. Pak vektory $u_1, \dots, u_n$ generují V právě tehdy, když vektory $v_1, \dots, v_n$ generují V .*

Důkaz. Nechť lze získat n -tici $(v_1, \dots, v_n)$ z n -tice $(u_1, \dots, u_n)$ jednou z elementárních úprav, vybereme si úpravu druhého typu, tedy $v_i = u_i + cu_j$ a $v_k = u_k$ pro $k \neq i$.

Předpokládejme, že $v_1, \dots, v_n$ generují V . Pro libovolný vektor $w \in V$ tedy existují koeficienty $p^1, \dots, p^n$ takové, že $w = p^1 v_1 + \dots + p^n v_n$. Pak

$$\begin{aligned} w &= p^1 u_1 + \dots + p^i (u_i + cu_j) + \dots + p^j u_j + \dots + p^n u_n = \\ &= p^1 u_1 + \dots + p^i u_i + \dots + (p^j + cp^i) u_j + \dots + p^n u_n \end{aligned}$$

je lineární kombinace vektorů $u_1, \dots, u_n$.

Opačná implikace vyplývá z právě dokázané, neboť n -tice $(u_1, \dots, u_n)$ vzniká z n -tice $(v_1, \dots, v_n)$ inverzní úpravou, která je stejného typu.

Pro ostatní úpravy obdobně a výsledek platí i pro libovolnou konečnou posloupnost elementárních úprav. $\square$

Tvrzení 9.2.4. *Nechť n -tice $(u_1, \dots, u_n)$ je ekvivalentní s n -ticí $(v_1, \dots, v_n)$. Pak množina $\{u_1, \dots, u_n\}$ je lineárně nezávislá právě tehdy, když množina $\{v_1, \dots, v_n\}$ je lineárně nezávislá.*

Důkaz. Nechť lze získat n -tici $(v_1, \dots, v_n)$ z n -tice $(u_1, \dots, u_n)$ jednou z elementárních úprav, vybereme si úpravu druhého typu, tedy $v_i = u_i + cu_j$ a $v_k = u_k$ pro $k \neq i$.

Předpokládejme, že $\{u_1, \dots, u_n\}$ je lineárně nezávislá. Buďte $x^1, \dots, x^n \in P$ takové, že $x^1 v_1 + \dots + x^n v_n = 0$. Pak

$$\begin{aligned} 0 &= x^1 v_1 + \dots + x^n v_n = x^1 u_1 + \dots + x^i (u_i + cu_j) + \dots + x^j u_j + \dots + x^n u_n = \\ &= x^1 u_1 + \dots + x^i u_i + \dots + (x^j + cx^i) u_j + \dots + x^n u_n. \end{aligned}$$

Z lineární nezávislosti množiny $\{u_1, \dots, u_n\}$ vyplývá, že všechny koeficienty poslední lineární kombinace jsou nulové, tj. $x^1 = \dots = x^i = \dots = x^j + cx^i = \dots = x^n = 0$. Z toho dostaneme, že $x^j = 0$.

Opačná implikace vyplývá z právě dokázané, neboť n -tice $(u_1, \dots, u_n)$ vzniká z n -tice $(v_1, \dots, v_n)$ inverzní úpravou, která je stejného typu.

Pro ostatní úpravy obdobně a výsledek platí i pro libovolnou konečnou posloupnost elementárních úprav. $\square$

Tvrzení 9.2.5. *Nechť vektory $v_1, \dots, v_n$ generují prostor V a $\{u_1, \dots, u_m\} \subset V$ je lineárně nezávislá. Pak $m \leq n$.*

Důkaz. Každý z vektorů $u_1, \dots, u_m$ je lineární kombinací vektorů $v_1, \dots, v_n$, takže pro každé $i \in \{1, \dots, m\}$ existují koeficienty $a_i^1, \dots, a_i^n$ takové, že $u_i = a_i^1 v_1 + \dots + a_i^n v_n$. Matici

$$A = \begin{pmatrix} a_1^1 & \dots & a_1^n \\ \vdots & & \vdots \\ a_m^1 & \dots & a_m^n \end{pmatrix}$$

upravme pomocí řádkových elementárních úprav na matici A' ve schodovitém tvaru. Provedeme-li stejné elementární úpravy s m -ticí $u_1, \dots, u_m$, dostaneme ekvivalentní m -ticí $u'_1, \dots, u'_m$. Lineární kombinace vektorů $v_1, \dots, v_n$ s koeficienty z jednotlivých řádků matice A' jsou rovny právě vektorům $u'_1, \dots, u'_m$. Z lineární nezávislosti množiny $\{u_1, \dots, u_m\}$ plyne lineární nezávislost množiny $\{u'_1, \dots, u'_m\}$ a také lineární nezávislost, tedy i nenulovost řádků matice A' . Jelikož A' je ve schodovitém tvaru a všechny řádky má nenulové, nemá více řádků než sloupků, tedy $m \leq n$.

Tvrzení je také součástí Tvrzení 9.2.7. $\square$

Lemma 9.2.6 (Lemma o výměně). *Budte $v_1, \dots, v_n \in V$ a $u = a^1 v_1 + \dots + a^n v_n$. Pak pro každé i takové, že $a^i \neq 0$, platí $\llbracket v_1, \dots, v_n \rrbracket = \llbracket v_1, \dots, v_{i-1}, u, v_{i+1}, \dots, v_n \rrbracket$.*

Důkaz. Předpokládejme, že $a^1 \neq 0$ (pro jiné indexy je důkaz stejný). Potom

$$v_1 = \frac{1}{a^1} u - \sum_{i=2}^n \frac{a^i}{a^1} v_i.$$

Bud' $w \in \llbracket v_1, \dots, v_n \rrbracket$. Existují tedy $b^1, b^2, \dots, b^n$ takové, že

$$\begin{aligned} w &= b^1 v_1 + b^2 v_2 + \dots + b^n v_n = \\ &= \frac{b^1}{a^1} u - \sum_{i=2}^n \frac{b^1 a^i}{a^1} v_i + b^2 v_2 + \dots + b^n v_n = \\ &= \frac{b^1}{a^1} u + \sum_{i=2}^n \left(b^i - \frac{b^1 a^i}{a^1} \right) v_i \in \llbracket u, v_2, \dots, v_n \rrbracket. \end{aligned}$$

Bud' $w \in \llbracket u, v_2, \dots, v_n \rrbracket$. Existují tedy $c^1, c^2, \dots, c^n$ takové, že

$$\begin{aligned} w &= c^1 u + c^2 v_2 + \dots + c^n v_n = \\ &= c^1 \sum_{i=1}^n a^i v_i + \sum_{i=2}^n c^i v_i = \\ &= c^1 a^1 v_1 + \sum_{i=2}^n (c^1 a^i + c^i) v_i \in \llbracket v_1, \dots, v_n \rrbracket. \end{aligned}$$

$\square$

Tvrzení 9.2.7 (Steinitzova věta o výměně). *Nechť vektory $v_1, \dots, v_n$ generují prostor V a $\{u_1, \dots, u_m\} \subset V$ je lineárně nezávislá. Pak $m \leq n$ a existují indexy $i_1, \dots, i_{n-m} \in \{1, \dots, n\}$ takové, že*

$$\llbracket v_1, \dots, v_n \rrbracket = \llbracket u_1, \dots, u_m, v_{i_1}, \dots, v_{i_{n-m}} \rrbracket.$$

Důkaz. Množina $\{u_1, \dots, u_m\}$ je lineárně nezávislá, takže všechny u_i jsou nenulové. Vektor u_1 je lineární kombinací vektorů $v_1, \dots, v_n$ s aspoň jedním nenulovým koeficientem a stejně jako v předchozím důkazu předpokládáme, že nenulový koeficient je u v_1 . Z Lemmatu o výměně dostaneme $\llbracket v_1, v_2, \dots, v_n \rrbracket = \llbracket u_1, v_2, \dots, v_n \rrbracket$.

Potom vektor u_2 je lineární kombinací vektorů $u_1, v_2, \dots, v_n$ s aspoň jedním nenulovým koeficientem u vektorů $v_2, \dots, v_n$ (jinak by množina $\{u_1, u_2\}$ byla lineárně závislá). Opět pro jednoduchost předpokládáme, že nenulový koeficient je u v_2 . Z Lemmatu o výměně dostaneme $\llbracket u_1, v_2, \dots, v_n \rrbracket = \llbracket u_1, u_2, v_3, \dots, v_n \rrbracket$.

Takto pokračujeme, dokud buď nepoužijeme všechny vektory $u_1, \dots, u_m$ nebo nevyměníme všechny vektory $v_1, \dots, v_n$ za vektory $u_1, \dots, u_n$. Kdyby bylo $m > n$, vektory $u_{n+1}, \dots, u_m$ by byly lineární kombinace vektorů $u_1, u_2, \dots, u_n$ ve sporu s lineární nezávislostí množiny $\{u_1, \dots, u_m\}$. Takže $m \leq n$ a

$$\llbracket v_1, \dots, v_n \rrbracket = \llbracket u_1, \dots, u_m, v_{i_1}, \dots, v_{i_{n-m}} \rrbracket. \quad \square$$

9.3. Báze

Definice 9.3.1. *Báze vektorového prostoru je libovolná uspořádaná lineárně nezávislá množina jeho generátorů.*

Obvykle tedy budeme bázi vektorového prostoru zapisovat jako uspořádanou n -tici vektorů. Pokud nebude záležet na uspořádání vektorů v bázi, budeme ji někdy zapisovat jen jako množinu vektorů.

Příklad. (1) (6) je báze $\mathbb{R}$.

(2) $((1, 0), (0, 1))$ je báze $\mathbb{R}^2$.

(3) $((1, 0, 0), (1, 1, 0), (1, 1, 1))$ je báze $\mathbb{R}^3$.

(4) Pro každé $i \in \{1, \dots, n\}$ buď e_i vektor z $\mathbb{R}^n$, který má na i -tém místě jedničku a jinde nuly. Potom $(e_1, \dots, e_n)$ je báze $\mathbb{R}^n$ a nazývá se *kanonická* nebo také *standardní*.

(5) $(x^2, x, 1)$ je báze $\mathbb{R}_2[x]$. $\square$

Tvrzení 9.3.1. *Každý konečněrozměrný vektorový prostor má bázi.*

Důkaz. Podle definice konečněrozměrný vektorový prostor má konečnou množinu generátorů. Ukážeme, že v ní existuje lineárně nezávislá podmnožina, která generuje tentýž vektorový prostor a je tedy jeho báze. Buď $\{v_1, \dots, v_n\}$ množina generátorů vektorového prostoru. Z této množiny postupně pro $i = 1, \dots, n$ vyloučíme vektor v_i , je-li lineární kombinací předchozích. Tedy v_1 vyloučíme, pokud $v_1 = 0$. Vektory, které nevyloučíme, označme $v_{i_1}, \dots, v_{i_m}$. Je-li prvek množiny generátorů lineární kombinací ostatních prvků této množiny, po jeho vyloučení z této množiny zůstane opět množina generátorů stejného vektorového prostoru (ověřte). Proto vektory $v_{i_1}, \dots, v_{i_m}$ generují tentýž vektorový prostor.

Díky uvedenému postupu žádný z vektorů $v_{i_1}, \dots, v_{i_m}$ není lineární kombinací předchozích a množina $\{v_{i_1}, \dots, v_{i_m}\}$ je lineárně nezávislá. $\square$

I nulový prostor $\{0\}$ má bázi. Je jí $\emptyset$, jelikož je lineárně nezávislá a $\llbracket \emptyset \rrbracket = \{0\}$.

Tvrzení 9.3.2. Všechny báze jednoho konečněrozměrného vektorového prostoru mají stejný počet prvků.

Důkaz. Buďte $(v_1, \dots, v_n)$ a $(u_1, \dots, u_m)$ báze vektorového prostoru V . Jelikož vektory $v_1, \dots, v_n$ generují V a $\{u_1, \dots, u_m\}$ je lineárně nezávislá množina, podle Tvrzení 9.2.5 $m \leq n$. Obdobně dostaneme, že $n \leq m$. Takže $n = m$. $\square$

Definice 9.3.2. Dimenze vektorového prostoru je počet vektorů (libovolné) jeho báze. Vektorový prostor V dimenze n je n -rozměrný, zapisujeme $\dim V = n$. Nulový vektorový prostor $\{0\}$ je 0-rozměrný.

Příklad. (1) Vektorový prostor P^n nad polem P je n -rozměrný. Jednou z bází je n -tice (kanonická báze) $((1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1))$.

(2) Vektorový prostor $\mathbb{C}$ nad polem $\mathbb{R}$ je dvojrozměrný. Jednou z bází je dvojice $(1, i)$. Vektorový prostor $\mathbb{C}$ nad polem $\mathbb{C}$ je jednorozměrný, jednu z bází tvoří vektor 1. Vidíme, že dva vektorové prostory mohou mít různé dimenze, přestože mají stejné množiny vektorů.

(3) Vektorový prostor $\mathbb{C}^n$ nad polem $\mathbb{R}$ je $2n$ -rozměrný. Jednou z bází je $2n$ -tice

$$\begin{aligned} &((1, 0, \dots, 0), (i, 0, \dots, 0), \\ &(0, 1, 0, \dots, 0), (0, i, 0, \dots, 0), \\ &\dots, \\ &(0, \dots, 0, 1), (0, \dots, 0, i)). \end{aligned}$$

 $\square$

Definice 9.3.3. (1) Minimální množina generátorů vektorového prostoru V je množina generátorů prostoru V , jejíž žádná vlastní podmnožina negeneruje V .
 (2) Maximální lineárně nezávislá množina vektorů vektorového prostoru V je lineárně nezávislá množina vektorů z V , která není vlastní podmnožinou žádné lineárně nezávislé množiny.

Tvrzení 9.3.3. Buďte $v_1, \dots, v_n \in V$. Pak následující podmínky jsou ekvivalentní:

- (1) $\{v_1, \dots, v_n\}$ je báze V ;
- (2) $\{v_1, \dots, v_n\}$ je minimální množina generátorů V ;
- (3) $\{v_1, \dots, v_n\}$ je maximální lineárně nezávislá množina vektorů V .

Důkaz. (1) $\Rightarrow$ (2): Je-li $\{v_1, \dots, v_n\}$ báze, je to množina generátorů a žádný z nich není lineární kombinací ostatních. Tudíž žádná její vlastní podmnožina negeneruje V a $\{v_1, \dots, v_n\}$ je minimální množina generátorů.

(2) $\Rightarrow$ (1): $\{v_1, \dots, v_n\}$ je množina generátorů. Jelikož je minimální, žádný z jejích vektorů není lineární kombinací ostatních, takže je navíc lineárně nezávislá, čili báze.

(1) $\Rightarrow$ (3): Je-li $\{v_1, \dots, v_n\}$ báze, je lineárně nezávislá a každý vektor z V je lineární kombinací vektorů báze. Tudíž každá vlastní nadmnožina je lineárně závislá a tato je tedy maximální.

(3) $\Rightarrow$ (1): Množina $\{v_1, \dots, v_n\}$ je lineárně nezávislá. Jelikož je maximální, po přidání libovolného vektoru z V , dostaneme lineárně závislou množinu a ten přidaný vektor (ty původní to být nemohou) je lineární kombinací předchozích, takže $\{v_1, \dots, v_n\}$ je navíc množina generátorů, čili báze. $\square$

Tvrzení poskytuje dvě alternativní definice báze, které se často používají. Má také důležité důsledky.

Důsledek. *Bud' $n \in \mathbb{N}$. Je-li V n -rozměrný vektorový prostor, pak*

- (1) *libovolná jeho n -prvková lineárně nezávislá podmnožina tvoří jeho bázi;*
- (2) *libovolná jeho n -prvková množina generátorů tvoří jeho bázi.*

Důkaz. (1) Prostor V má n -prvkovou množinu generátorů, takže podle Tvzení 9.2.5 každá n -prvková lineárně nezávislá podmnožina je maximální, tedy báze.

(2) V prostoru V existuje n -prvková lineárně nezávislá množina, takže podle Tvzení 9.2.5 každá n -prvková množina generátorů je minimální, tedy báze. $\square$

Důsledek. *Bud' $\{v_1, \dots, v_k\}$ lineárně nezávislá podmnožina n -rozměrného vektorového prostoru V . Pak ji lze doplnit do báze $(v_1, \dots, v_k, v_{k+1}, \dots, v_n)$.*

Důkaz. V případě, že $v_1, \dots, v_k$ generují V , tvoří bázi. Jinak existuje vektor $v_{k+1} \in V$, který není lineární kombinací vektorů $v_1, \dots, v_k$, načež množina $\{v_1, \dots, v_k, v_{k+1}\}$ je lineárně nezávislá, protože v_{k+1} není lineární kombinací předchozích vektorů.

Po $n - k$ opakováních této úvahy získáme n -prvkovou lineárně nezávislou množinu $\{v_1, \dots, v_k, v_{k+1}, v_{k+2}, \dots, v_n\}$, která je bází podle předchozího důsledku. $\square$

9.4. Souřadnice

Tvrzení 9.4.1. *Bud' $(e_1, \dots, e_n)$ báze vektorového prostoru V . Pak pro každé $v \in V$ existuje právě jedna n -tice skalárů $(x^1, \dots, x^n)$ taková, že $v = x^1 e_1 + \dots + x^n e_n$.*

Důkaz. Bud' $v \in V$. Jelikož $e_1, \dots, e_n$ generují V , existují $x^1, \dots, x^n \in P$ takové, že $v = x^1 e_1 + \dots + x^n e_n$. Jsou-li $y^1, \dots, y^n$ libovolná taková, že $v = y^1 e_1 + \dots + y^n e_n$, pak

$$\begin{aligned} 0 &= v - v = (x^1 e_1 + \dots + x^n e_n) - (y^1 e_1 + \dots + y^n e_n) = \\ &= (x^1 - y^1) e_1 + \dots + (x^n - y^n) e_n. \end{aligned}$$

Z lineární nezávislosti množiny $\{e_1, \dots, e_n\}$ plyne $x^1 - y^1 = \dots = x^n - y^n = 0$, a tedy $x^1 = y^1, \dots, x^n = y^n$. $\square$

Cvičení. Zformulujte a dokažte obrácené tvrzení. $\square$

Definice 9.4.1. Skaláry $x^1, \dots, x^n$ z předchozího tvrzení jsou *souřadnice* vektoru v vzhledem k bázi $(e_1, \dots, e_n)$.

Souřadnice budeme zapisovat buď jako prvky pole $x^1, \dots, x^n$ nebo jako uspořádanou n -tici $x = (x^1, \dots, x^n)$ nebo jako matici typu $n \times 1$

$$x = \begin{pmatrix} x^1 \\ x^2 \\ \vdots \\ x^n \end{pmatrix}.$$

Příklad. (1) Souřadnice vektoru $2 \in \mathbb{R}$ vzhledem k bázi (6) je $\frac{1}{3}$, protože $2 = \frac{1}{3} \cdot 6$.

(2) Souřadnice vektoru $(x, y, z) \in \mathbb{R}^3$ v kanonické bázi jsou x, y, z , protože $(x, y, z) = x \cdot (1, 0, 0) + y \cdot (0, 1, 0) + z \cdot (0, 0, 1)$.

(3) Souřadnice vektoru $(x, y, z) \in \mathbb{R}^3$ v bázi $((1, 0, 0), (1, 1, 0), (1, 1, 1))$ jsou $x - y, y - z, z$, protože $(x, y, z) = (x - y) \cdot (1, 0, 0) + (y - z) \cdot (1, 1, 0) + z \cdot (1, 1, 1)$.

(4) Souřadnice vektoru $z = a + bi \in \mathbb{C}(\mathbb{R})$ vzhledem k bázi $(1, i)$ jsou a, b , protože $z = a \cdot 1 + b \cdot i$.

Souřadnice vektoru $z = a + bi \in \mathbb{C}(\mathbb{C})$ vzhledem k bázi (1) je z , protože $z = z \cdot 1$. $\square$

Souřadnice vektoru závisí na volbě báze. Jeden vektor má v různých bázích různé souřadnice.

Buďte V vektorový prostor, $v \in V$. Buďte $e = (e_1, \dots, e_n)$ a $e' = (e'_1, \dots, e'_n)$ báze V , e nazvěme *stará báze*, e' nazvěme *nová báze*. Souřadnice vektoru v vzhledem ke staré bázi označme $x = (x^1, \dots, x^n)$ a řekjme jim *staré souřadnice*. Souřadnice vektoru v vzhledem k nové bázi označme $x' = (x'^1, \dots, x'^n)$ a řekjme jim *nové souřadnice*. Platí tedy $v = \sum_i x^i e_i = \sum_i x'^i e'_i$.

Definice 9.4.2. Matice, jejíž sloupky jsou tvořeny novými souřadnicemi starých bázevých vektorů, je *matice přechodu* od staré báze k nové bázi.

Matici přechodu od báze α k bázi β značíme $Q_{\alpha\beta}$.

Zobrazení

$$\delta(i, j) = \delta_j^i = \begin{cases} 1, & \text{je-li } i = j, \\ 0 & \text{jinak} \end{cases} \quad \text{je Kroneckerovo delta.}$$

Tvrzení 9.4.2. *Matice přechodu je regulární.*

Důkaz. Buďte $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ a $\beta = (\beta_1, \beta_2, \dots, \beta_n)$ báze jednoho vektorového prostoru. Označme $Q_{\alpha\beta} = (a_i^j)$ matici přechodu od báze α k bázi β a $Q_{\beta\alpha} = (b_i^j)$ matici přechodu od báze β k bázi α . Tedy, $(a_i^1, a_i^2, \dots, a_i^n)$ jsou souřadnice vektoru α_i vzhledem k bázi β , $(b_i^1, b_i^2, \dots, b_i^n)$ jsou souřadnice vektoru β_i vzhledem k bázi α a

$$\alpha_i = \sum_{j=1}^n a_i^j \beta_j \quad \text{a} \quad \beta_i = \sum_{j=1}^n b_i^j \alpha_j \quad \text{pro každé } i = 1, 2, \dots, n.$$

Po dosazení dostaneme

$$\begin{aligned} \alpha_i &= \sum_{j=1}^n a_i^j \beta_j = \\ &= \sum_{j=1}^n a_i^j \left(\sum_{k=1}^n b_j^k \alpha_k \right) = \\ &= \sum_{k=1}^n \left(\sum_{j=1}^n a_i^j b_j^k \right) \alpha_k, \end{aligned}$$

čili

$$\left(\sum_{j=1}^n a_i^j b_j^1, \quad \sum_{j=1}^n a_i^j b_j^2, \quad \dots, \quad \sum_{j=1}^n a_i^j b_j^n \right)$$

jsou souřadnice vektoru α_i vzhledem k bázi α . Tedy,

$$\sum_{j=1}^n a_i^j b_j^k = \delta_k^i = \begin{cases} 1 & \text{je-li } i = k, \\ 0 & \text{jinak.} \end{cases}$$

Ovšem

$$\sum_{j=1}^n a_i^j b_j^k = (Q_{\beta\alpha} Q_{\alpha\beta})_i^k$$

je v k -tém řádku a i -tém sloupku součinu $Q_{\beta\alpha}Q_{\alpha\beta}$, takže $Q_{\beta\alpha}Q_{\alpha\beta} = E$, proto matice $Q_{\beta\alpha}$ a $Q_{\alpha\beta}$ jsou vzájemně inverzní a tedy obě regulární. $\square$

Tvrzení 9.4.3. *Buď $Q_{ee'}$ matice přechodu od staré báze e k nové bázi e' a buďte x a x' staré a nové souřadnice jednoho vektoru. Potom*

$$x' = Q_{ee'} \cdot x.$$

Důkaz. Buď $Q_{ee'} = (q_j^i)$ matice přechodu od staré báze e k nové bázi e' . Tedy

$$e_i = \sum_j q_j^i e'_j.$$

Buď $v = x^1 e_1 + \dots + x^n e_n \in V$. Potom

$$\begin{aligned} v &= x^1 \sum_j q_j^1 e'_j + \dots + x^n \sum_j q_j^n e'_j = \\ &= x^1 (q_1^1 e'_1 + q_1^2 e'_2 + \dots + q_1^n e'_n) + \dots + x^n (q_n^1 e'_1 + q_n^2 e'_2 + \dots + q_n^n e'_n) = \\ &= \left(\sum_j q_j^1 x^j \right) e'_1 + \left(\sum_j q_j^2 x^j \right) e'_2 + \dots + \left(\sum_j q_j^n x^j \right) e'_n. \end{aligned}$$

Tedy

$$x'^i = \sum_j q_j^i x^j \quad \text{a} \quad x' = Q_{ee'} \cdot x. \quad \square$$

Příklad. (1) Mějme $\mathbb{R}$, starou bázi $e = (6)$ a novou bázi $e' = (1)$. Pro $v = 2$ je $x = (\frac{1}{3})$ a $x' = (2)$.

Matice přechodu od staré báze e k nové bázi e' je

$$Q_{ee'} = (6).$$

A skutečně

$$x' = (6) \cdot \left(\frac{1}{3}\right) = (2).$$

(2) Mějme $\mathbb{R}^2$, starou bázi $e = ((1, -1), (1, 1))$ a novou bázi $e' = ((0, 2), (2, 1))$. Pro $v = (2, 0)$ je $x = (1, 1)$ a $x' = (-\frac{1}{2}, 1)$.

Matice přechodu od staré báze e k nové bázi e' je

$$Q_{ee'} = \begin{pmatrix} -\frac{3}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

A skutečně

$$x' = Q_{ee'} \cdot x = \begin{pmatrix} -\frac{3}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} \\ 1 \end{pmatrix}. \quad \square$$

Tvrzení 9.4.4. *Buďte V vektorový prostor nad polem P , $e = (e_1, \dots, e_n)$ jeho báze, $u, v \in V$, $p \in P$, $x = (x^1, \dots, x^n)$ souřadnice vektoru u a $y = (y^1, \dots, y^n)$ souřadnice vektoru v . Pak $x + y = (x^1 + y^1, \dots, x^n + y^n)$ jsou souřadnice vektoru $u + v$ a $px = (px^1, \dots, px^n)$ jsou souřadnice vektoru pu .*

Důkaz. Cvičení. $\square$

9.5. Orientace vektorového prostoru

Definice 9.5.1. Budťe α, β báze jednoho vektorového prostoru. Báze α má stejnou *orientaci* jako báze β , jestliže $\det Q_{\alpha\beta} > 0$.

Relace

$$\alpha \sim \beta \quad \text{právě tehdy, když} \quad \alpha \text{ má stejnou orientaci jako } \beta$$

je relace ekvivalence. (Cvičení.) Tato relace ekvivalence rozděluje množinu všech bází jednoho vektorového prostoru do dvou disjunktních tříd.

Definice 9.5.2. Prohlásíme-li některou z bází vektorového prostoru, a společně s ní i každou bázi se stejnou orientací, za *kladnou* (nebo *kladně orientovanou*), určíme tím *orientaci* vektorového prostoru a vektorový prostor je potom *orientovaný*. Báze, které nejsou kladné, jsou *záporné* (nebo *záporně orientované*).

Příklad. Kanonická báze prostoru P^n je obvykle uvažována jako kladná. □

9.6. Přímý součet vektorových prostorů

Definice 9.6.1. Budťe $V_1, \dots, V_n$ vektorové prostory nad polem P . Na kartézském součinu $V_1 \times \dots \times V_n$ zaveďme sčítání a násobení skalárem předpisem

$$(u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n),$$

$$p(u_1, \dots, u_n) = (pu_1, \dots, pu_n)$$

pro libovolné $(u_1, \dots, u_n), (v_1, \dots, v_n) \in V_1 \times \dots \times V_n$ a $p \in P$.

Na $V_1 \times \dots \times V_n$ tak dostaneme strukturu vektorového prostoru nad polem P , který se značí $V_1 \oplus \dots \oplus V_n$ a je to *přímý součet* vektorových prostorů $V_1, \dots, V_n$.

Cvičení. Ověřte, že $V_1 \oplus \dots \oplus V_n$ je vektorový prostor. □

Tvrzení 9.6.1. Budťe $V_1, \dots, V_n$ konečněrozměrné vektorové prostory. Pak

$$\dim(V_1 \oplus \dots \oplus V_n) = \dim V_1 + \dots + \dim V_n.$$

Důkaz. Pro každé i nechť $(e_1^i, \dots, e_{m_i}^i)$ je báze V_i . Potom

$$((e_1^1, 0, \dots, 0), \dots, (e_{m_1}^1, 0, \dots, 0),$$

$$(0, e_1^2, 0, \dots, 0), \dots, (0, e_{m_2}^2, 0, \dots, 0),$$

$$\dots,$$

$$(0, \dots, 0, e_1^n), \dots, (0, \dots, 0, e_{m_n}^n))$$

je báze $V_1 \oplus \dots \oplus V_n$ (cvičení). □

Příklad. Budť $V_1 = \mathbb{R}$ a $V_2 = \mathbb{R}^2$. Potom $V_1 \times V_2$ je množina $\mathbb{R} \times \mathbb{R}^2$ uspořádaných dvojic (x, y) , kde $x \in \mathbb{R}$ a $y = (y_1, y_2) \in \mathbb{R}^2$, tedy $\mathbb{R} \times \mathbb{R}^2 = \{(x, (y_1, y_2)) \mid x \in \mathbb{R}, (y_1, y_2) \in \mathbb{R}^2\}$. Například

$$(1, (2, 3)) + (2, (1, -1)) = (1 + 2, (2, 3) + (1, -1)) = (3, (3, 2)),$$

$$3 \cdot (2, (1, 4)) = (3 \cdot 2, 3 \cdot (1, 4)) = (6, (3, 12)).$$

Budť $e^1 = (1)$ báze $\mathbb{R}$ a budť $e^2 = (e_1^2, e_2^2) = ((1, 0), (0, 1))$ báze $\mathbb{R}^2$. Potom trojice

$$((e^1, 0), (0, e_1^2), (0, e_2^2)) = ((1, (0, 0)), (0, (1, 0)), (0, (0, 1)))$$

je báze $\mathbb{R} \oplus \mathbb{R}^2$ a $\dim(\mathbb{R} \oplus \mathbb{R}^2) = 3 = \dim \mathbb{R} + \dim \mathbb{R}^2 = 1 + 2$.

□

10. VEKTOROVÉ PODPROSTORY

10.1. Definice, příklady, základní vlastnosti

Definice 10.1.1. Buďte V vektorový prostor nad polem P a $U \subseteq V$. U je *vektorový podprostor* prostoru V , jestliže

- (i) $0 \in U$;
- (ii) $u_1 + u_2 \in U$ pro každé $u_1, u_2 \in U$ (uzavřenost na sčítání);
- (iii) $pu \in U$ pro každé $u \in U$ a každé $p \in P$ (uzavřenost na násobení skalárem).

Podle (iii) pro každý vektor $u \in U$ máme $-u = (-1) \cdot u \in U$, čili s každým vektorem leží v U i vektor k němu opačný. To spolu s (i) a (ii) znamená, že podprostor je podgrupa abelovské grupy $(V, +, 0, -)$.

Axiomy vektorového prostoru jsou splněny na V a tím spíše na U (cvičení). Tudíž, podobně jako u ostatních algebraických podstruktur, podprostor je sám též vektorovým prostorem.

Příklad. (1) V každém vektorovém prostoru je nulový podprostor obsahující jen nulový vektor.

(2) Každý prostor je sám svým podprostorem.

(3) $\mathbb{R}$ je podprostorem vektorového prostoru $\mathbb{C}$ nad polem $\mathbb{R}$ (ověřte).

(4) $\{(a, 0) \mid a \in \mathbb{R}\}$ je podprostor vektorového prostoru $\mathbb{R}^2$ nad polem $\mathbb{R}$ (ověřte). $\square$

Tvrzení 10.1.1. Množina všech řešení homogenní soustavy lineárních rovnic o n neznámých s maticí A nad polem P je podprostor prostoru P^n s dimenzí $n - \text{rank } A$.

Důkaz. Tvrzení vyplývá z kapitoly 3.5. Každá homogenní soustava rovnic má nulové řešení, součet řešení je řešení a skalární násobek řešení je řešení. Množina všech řešení tedy má vlastnosti požadované v definici vektorového podprostoru. Navíc, fundamentální systém řešení má $n - \text{rank } A$ prvků a tvoří bázi prostoru všech řešení. $\square$

Mnoho dalších příkladů můžeme získat jako lineární obaly.

Tvrzení 10.1.2. Buď W podmnožina vektorového prostoru V nad polem P . Potom:

(1) $\llbracket W \rrbracket$ je podprostor prostoru V .

(2) Je-li U podprostor V obsahující W , pak $\llbracket W \rrbracket \subseteq U$.

Důkaz. (1) Ukážeme, že množina $\llbracket W \rrbracket$ splňuje podmínky (i)–(iii) z definice vektorového podprostoru. Podmínka (i): Je-li $W = \emptyset$, potom $\llbracket W \rrbracket = \{0\}$, takže $0 \in \llbracket W \rrbracket$. Je-li $W \neq \emptyset$, potom pro libovolný vektor $v \in W$ je $0 = 0v \in \llbracket W \rrbracket$. Podmínka (ii): Jsou-li $u, v \in \llbracket W \rrbracket$, potom $u = x^1 u_1 + \dots + x^m u_m$ a $v = y^1 v_1 + \dots + y^n v_n$ pro nějaké $x^i, y^j \in P$, $u_i, v_j \in W$ a $m, n \in \mathbb{N}$. Tedy $u + v = x^1 u_1 + \dots + x^m u_m + y^1 v_1 + \dots + y^n v_n \in \llbracket W \rrbracket$. Podmínka (iii): Cvičení.

(2) Buď $w \in \llbracket W \rrbracket$, tedy $w = x^1 w_1 + \dots + x^n w_n$ pro nějaké $x^i \in P$, $w_i \in W$ a $n \in \mathbb{N}$. Jelikož $W \subseteq U$, všechny vektory w_i jsou prvky U , a jelikož U je vektorový podprostor, tedy uzavřený na násobení skalárem a sčítání vektorů, $w \in U$. $\square$

Tudíž, $\llbracket W \rrbracket$ je nejmenší podprostor prostoru V obsahující množinu W .

Tvrzení 10.1.3. Buď V konečněrozměrný prostor a U jeho podprostor. Potom:

(1) U je konečněrozměrný a $\dim U \leq \dim V$.

(2) $\dim U = \dim V$ právě tehdy, když $U = V$.

Důkaz. (1) Je-li U nulový prostor, potom je 0-rozměrný. Jestliže $U \neq \{0\}$, existuje $u_1 \in U \setminus \{0\}$ a je-li $U = \llbracket u_1 \rrbracket$, pak je 1-rozměrný. Takto můžeme pokračovat. Jestliže $U \neq \llbracket u_1, \dots, u_{k-1} \rrbracket$, existuje $u_k \in U \setminus \llbracket u_1, \dots, u_{k-1} \rrbracket$, a je-li $U = \llbracket u_1, \dots, u_k \rrbracket$, pak je k -rozměrný.

Množina $\{u_1, \dots, u_k\}$ je lineárně nezávislá, protože žádný z jejích vektorů není lineární kombinací předchozích. Podle Tvzení 9.2.5 lineárně nezávislá množina nemá více prvků než množina generátorů, takže pro nějaké $m \leq \dim V$ dostaneme $U = \llbracket u_1, \dots, u_m \rrbracket$, čili $\dim U \leq \dim V$.

(2) Podle předchozího bodu U je konečněrozměrný, takže podle Tvzení 9.3.1 má bázi $(u_1, \dots, u_n)$. Jestliže $\dim U = \dim V$, pak $\{u_1, \dots, u_n\}$ je n -prvková lineárně nezávislá množina v n -rozměrném prostoru V , čili podle Důsledku Tvzení 9.3.3 $(u_1, \dots, u_n)$ je také báze prostoru V a $U = V$.

Jestliže $U = V$, pak samozřejmě $\dim U = \dim V$. □

Důsledek. *Vektorový prostor, který má nekonečněrozměrný podprostor, je nekonečněrozměrný.*

Příklad. Prostor $C^r \mathbb{R}$ všech funkcí $\mathbb{R} \rightarrow \mathbb{R}$, spojitých se všemi derivacemi až do řádu r včetně, je nekonečněrozměrný, protože obsahuje podprostor polynomů $\mathbb{R}[x]$, který je nekonečněrozměrný. □

Příklad. (1) Podprostory $\mathbb{R}$.

(2) Podprostory $\mathbb{R}^2$.

(3) Podprostory $\mathbb{R}^3$. □

10.2. Průnik a součet podprostorů

Tvrzení 10.2.1. *Průnik libovolného systému podprostorů jednoho vektorového prostoru je podprostor tohoto prostoru.*

Důkaz. Buďte U_ι , $\iota \in I$, kde I je indexová množina, podprostory vektorového prostoru V . Ukážeme, že množina $\bigcap_{\iota \in I} U_\iota$ splňuje podmínky (i)–(iii) z definice vektorového podprostoru. Podmínka (i): $0 \in \bigcap_{\iota \in I} U_\iota$, protože $0 \in U_\iota$ pro každé $\iota \in I$. Podmínka (ii): Nechť $u_1, u_2 \in \bigcap_{\iota \in I} U_\iota$. Pak $u_1, u_2 \in U_\iota$ pro každé $\iota \in I$, takže $u_1 + u_2 \in U_\iota$ pro každé $\iota \in I$. Tudíž, $u_1 + u_2 \in \bigcap_{\iota \in I} U_\iota$. Podmínka (iii): Cvičení. □

Definice 10.2.1. Buďte $U_1, \dots, U_n$ podprostory V . Množina

$$\{u_1 + \dots + u_n \mid u_1 \in U_1, \dots, u_n \in U_n\}$$

je *součet* podprostorů $U_1, \dots, U_n$. Označujeme jej $U_1 + \dots + U_n$.

Prvky množiny $U_1 + \dots + U_n$ jsou všechny vektory $v \in V$, pro něž existuje vyjádření $v = u_1 + \dots + u_n$, kde $u_1 \in U_1, \dots, u_n \in U_n$.

Tvrzení 10.2.2. *Buďte $U_1, \dots, U_n$ podprostory V . Pak $U_1 + \dots + U_n = \llbracket U_1 \cup \dots \cup U_n \rrbracket$, a je to tedy podprostor V .*

Důkaz. Důkaz, že $U_1 + \dots + U_n = \llbracket U_1 \cup \dots \cup U_n \rrbracket$, necháme jako cvičení. Podle Tvzení 10.1.2 $U_1 + \dots + U_n$ je tedy podprostor V .

Nebo je možné ukázat, že množina $U_1 + \dots + U_n$ splňuje podmínky (i)–(iii) z definice vektorového podprostoru. Podmínka (i): $0 = 0 + \dots + 0 \in U_1 + \dots + U_n$, kde $0 \in U_i$ pro

každé $i \in \{1, \dots, n\}$. Podmínka (ii): Nechť $u, v \in U_1 + \dots + U_n$. Pak $u = u_1 + \dots + u_n$ a $v = v_1 + \dots + v_n$, kde $u_i, v_i \in U_i$ pro každé $i \in \{1, \dots, n\}$, načež $u + v = u_1 + \dots + u_n + v_1 + \dots + v_n = (u_1 + v_1) + \dots + (u_n + v_n) \in U_1 + \dots + U_n$. Podmínka (iii): Cvičení. $\square$

Cvičení. Dokažte, že (1) $U_1, U_2 \subseteq U_1 + U_2$.

(2) Je-li U podprostor ve V takový, že $U_1 \subseteq U$ a $U_2 \subseteq U$, pak $U_1 + U_2 \subseteq U$.

Návod: (1) Je-li $u_1 \in U_1$ libovolný prvek, pak $u_1 = u_1 + 0 \in U_1 + U_2$.

(2) Buď $u_1 + u_2$ obecný vektor z $U_1 + U_2$, $u_1 \in U_1$, $u_2 \in U_2$. Protože $U_1, U_2 \subseteq U$, máme $u_1, u_2 \in U$, načež $u_1 + u_2 \in U$. $\square$

Množina $S(V)$ všech podprostorů vektorového prostoru V je uspořádána inkluzí $\subseteq$. Z dokázaných tvrzení o průnicích a součtech podprostorů plyne, že množina $S(V)$ je svazově uspořádána, přičemž infimum je průnik a supremum je součet podprostorů. Tudíž, $(S(V), \cap, +)$ je svaz.

Cvičení. Pro každé $i \in \{1, \dots, n\}$ nechť U_i je podprostor V a G_i je množina generátorů podprostoru U_i . Potom $\bigcup_{i=1}^n G_i$ je množina generátorů podprostoru $U_1 + \dots + U_n$. $\square$

Tvrzení 10.2.3. *Buďte U_1, U_2 konečněrozměrné podprostory jednoho vektorového prostoru. Pak*

$$\dim U_1 + \dim U_2 = \dim(U_1 + U_2) + \dim(U_1 \cap U_2).$$

Důkaz. Označme $\dim U_1 = n_1$, $\dim U_2 = n_2$ a $\dim(U_1 \cap U_2) = m$. Buď $\{u_1, \dots, u_m\}$ báze v $U_1 \cap U_2$. To je lineárně nezávislá množina vektorů v U_1 i v U_2 a můžeme ji tedy v obou prostorech doplnit do báze vektory $u_1^1, \dots, u_{n_1-m}^1$, resp. $u_1^2, \dots, u_{n_2-m}^2$. Ukažme, že $\{u_1, \dots, u_m, u_1^1, \dots, u_{n_1-m}^1, u_1^2, \dots, u_{n_2-m}^2\}$ je báze v $U_1 + U_2$.

Nejdříve ukážeme, že množina $\{u_1, \dots, u_m, u_1^1, \dots, u_{n_1-m}^1, u_1^2, \dots, u_{n_2-m}^2\}$ je lineárně nezávislá. Nechť

$$c^1 u_1 + \dots + c^m u_m + c_1^1 u_1^1 + \dots + c_1^{n_1-m} u_{n_1-m}^1 + c_2^1 u_1^2 + \dots + c_2^{n_2-m} u_{n_2-m}^2 = 0$$

pro nějaké skaláry $c^1, \dots, c^m, c_1^1, \dots, c_1^{n_1-m}, c_2^1, \dots, c_2^{n_2-m} \in P$. Pak

$$c^1 u_1 + \dots + c^m u_m + c_1^1 u_1^1 + \dots + c_1^{n_1-m} u_{n_1-m}^1 = -c_2^1 u_1^2 - \dots - c_2^{n_2-m} u_{n_2-m}^2,$$

kde na levé straně je prvek z U_1 a na pravé prvek z U_2 , ale protože jsou si rovny, leží v $U_1 \cap U_2$, a lze je jednoznačně vyjádřit jako lineární kombinace vektorů $u_1, \dots, u_m$. Vyjádříme tak vektor na pravé straně: existují skaláry $x^1, \dots, x^m \in P$ takové, že

$$x^1 u_1 + \dots + x^m u_m = -c_2^1 u_1^2 - \dots - c_2^{n_2-m} u_{n_2-m}^2.$$

Z nezávislosti množiny $\{u_1, \dots, u_m, u_1^2, \dots, u_{n_2-m}^2\}$ (je to báze v U_2) plyne, že

$$x^1 = \dots = x^m = c_2^1 = \dots = c_2^{n_2-m} = 0.$$

Odtud

$$c^1 u_1 + \dots + c^m u_m + c_1^1 u_1^1 + \dots + c_1^{n_1-m} u_{n_1-m}^1 = 0,$$

a z nezávislosti množiny $\{u_1, \dots, u_m, u_1^1, \dots, u_{n_1-m}^1\}$ (je to báze v U_1) plyne, že

$$c^1 = \dots = c^m = c_1^1 = \dots = c_1^{n_1-m} = 0.$$

Všechny koeficienty $c^1, \dots, c^m, c_1^1, \dots, c_1^{n_1-m}, c_2^1, \dots, c_2^{n_2-m}$ jsou tedy nulové, takže množina $\{u_1, \dots, u_m, u_1^1, \dots, u_{n_1-m}^1, u_1^2, \dots, u_{n_2-m}^2\}$ je lineárně nezávislá.

Snadno se dokáže, že vektory $u_1, \dots, u_m, u_1^1, \dots, u_{n_1-m}^1, u_1^2, \dots, u_{n_2-m}^2$ generují $U_1 + U_2$ (cvičení).

Máme tedy bázi v $U_1 + U_2$ o $m + (n_1 - m) + (n_2 - m) = n_1 + n_2 - m$ vektorech, takže $\dim(U_1 + U_2) = n_1 + n_2 - m = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$. $\square$

Příklad. V prostoru E^3 buď $U \subset E^3$ nějaká rovina procházející počátkem a $L \subset E^3$ libovolná přímka procházející počátkem a neležící v U . Pak U je podprostor a podobně L je podprostor, přičemž evidentně $U \cap L = \{0\}$. Proto $\dim(U + L) = \dim U + \dim L - \dim(U \cap L) = 2 + 1 - 0 = 3 = \dim E^3$. Tudíž, $E^3 = U + L$ a každý vektor $v \in E^3$ je součtem $v = u + l$, kde $u \in U$ a $l \in L$. Jak najdeme vektory u, l , je-li dán vektor v ? $\square$

Cvičení. Buďte U_1, U_2 podprostory prostoru V takové, že $\dim U_1 + \dim U_2 > \dim V$. Ukažte, že existuje nenulový vektor $u \in U_1 \cap U_2$. $\square$

10.3. Přímý součet podprostorů

Definice 10.3.1. Buď V vektorový prostor nad polem P , buďte $U_1, \dots, U_n$ podprostory V . Součet $U_1 + \dots + U_n$ je *přímý*, jestliže každý vektor $v \in U_1 + \dots + U_n$ lze zapsat právě jedním způsobem jako součet $v = u_1 + \dots + u_n$, kde $u_1 \in U_1, \dots, u_n \in U_n$. Přímý součet zapisujeme s tečkami: $U_1 \dot{+} \dots \dot{+} U_n$.

Příklad. Nechtě $U_1 = \{(x, 0, 0) \mid x \in P\}$, $U_2 = \{(0, y, 0) \mid y \in P\}$, $U_3 = \{(0, 0, z) \mid z \in P\}$. Pak $P^3 = U_1 \dot{+} U_2 \dot{+} U_3$, protože libovolný vektor $u = (x, y, z) \in P^3$ má jediné vyjádření ve tvaru součtu $u = u_1 + u_2 + u_3$, kde $u_1 \in U_1, u_2 \in U_2, u_3 \in U_3$, a sice $(x, y, z) = (x, 0, 0) + (0, y, 0) + (0, 0, z)$. $\square$

Tvrzení 10.3.1. Buďte U_1, U_2 podprostory V . Pak následující podmínky jsou ekvivalentní:

- (i) $V = U_1 \dot{+} U_2$;
- (ii) $V = U_1 + U_2$, $U_1 \cap U_2 = 0$.

Důkaz. (i) $\Rightarrow$ (ii): Je-li $V = U_1 \dot{+} U_2$, pak každý vektor $v \in V$ lze vyjádřit jako součet $v = u_1 + u_2$, kde $u_1 \in U_1$ a $u_2 \in U_2$, čili $V = U_1 + U_2$. Ukažme, že $U_1 \cap U_2 = 0$. Buď $v \in U_1 \cap U_2$. Pak máme dva rozklady vektoru v na sčítance z U_1 a U_2 , a sice $v = 0 + v$ a $v = v + 0$. Totožnost obou rozkladů znamená, že $v = 0$.

(ii) $\Rightarrow$ (i): Je-li $V = U_1 + U_2$, pak každý vektor $v \in V$ lze vyjádřit jako součet $v = u_1 + u_2$, kde $u_1 \in U_1$ a $u_2 \in U_2$. Dokážeme ještě jednoznačnost vektorů u_1, u_2 : Pokud je u'_1, u'_2 libovolná dvojice vektorů taková, že $v = u'_1 + u'_2$, pak

$$0 = v - v = (u_1 - u'_1) + (u_2 - u'_2),$$

a tedy $u_1 - u'_1 = -(u_2 - u'_2)$. Vektor $u_1 - u'_1 \in U_1$ je roven vektoru $-(u_2 - u'_2) \in U_2$, proto leží v průniku $U_1 \cap U_2$, což je nulový prostor. Tudíž, $u_1 - u'_1 = 0$ a $u_2 - u'_2 = 0$. $\square$

Příklad. (1) $V = V \dot{+} 0$ pro libovolný vektorový prostor V .

(2) Prostor E^3 je přímým součtem $U \dot{+} L$, je-li $U \subset E^3$ libovolná rovina procházející počátkem a $L \subset E^3$ libovolná přímka procházející počátkem a neležící v U . $\square$

V případě konečněrozměrných podprostorů máme jednoduché kritérium.

Tvrzení 10.3.2. Buďte U_1, U_2 podprostory konečněrozměrného vektorového prostoru V takové, že $V = U_1 + U_2$. Pak následující podmínky jsou ekvivalentní:

- (i) $V = U_1 \dot{+} U_2$;
- (ii) $\dim V = \dim U_1 + \dim U_2$.

Důkaz. (i) $\Rightarrow$ (ii): $\dim V = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2) = \dim U_1 + \dim U_2$.

(ii) $\Rightarrow$ (i): Necht' $\dim V = \dim U_1 + \dim U_2$. Potom $\dim(U_1 \cap U_2) = \dim U_1 + \dim U_2 - \dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim V = 0$, čili $U_1 \cap U_2 = 0$. $\square$

Cvičení. Buďte $V = U_1 \dot{+} U_2$, $(e_1^1, \dots, e_{m_1}^1)$ báze podprostoru U_1 , $(e_1^2, \dots, e_{m_2}^2)$ báze podprostoru U_2 . Pak $(e_1^1, \dots, e_{m_1}^1, e_1^2, \dots, e_{m_2}^2)$ je báze prostoru V . Dokažte. $\square$

Cvičení. Buď $m < n$, buď $(e_1, \dots, e_m, e_{m+1}, \dots, e_n)$ báze vektorového prostoru V . Pak $V = \llbracket e_1, \dots, e_m \rrbracket \dot{+} \llbracket e_{m+1}, \dots, e_n \rrbracket$. Dokažte. $\square$

Vzniká otázka, jak jednoduše rozeznat přímý součet n podprostorů při $n > 2$. Mohlo by se zdát, že prostor V je přímým součtem podprostorů $U_1, \dots, U_n$, jestliže je jejich součtem a podprostory $U_1, \dots, U_n$ mají po dvou nulový průnik. Následující příklad ukazuje, že to tak není:

Příklad. Prostor E^3 není přímým součtem $L_1 \dot{+} L_2 \dot{+} U$, je-li U rovina procházející počátkem a jsou-li $L_1, L_2 \subset E^3$ různé přímky procházející počátkem, neležící v rovině U .

Skutečně, součet $L_1 + L_2$ je sice přímý, ale má nenulový průnik s rovinou U . Libovolný nenulový vektor $u = l_1 + l_2$ ležící v průniku $(L_1 + L_2) \cap U$ pak má dvojí vyjádření: jako součet $l_1 + l_2 + 0$ a jako součet $0 + 0 + u$. $\square$

Tvrzení 10.3.3. *Buďte $U_1, \dots, U_n \subseteq V$ podprostory takové, že $V = U_1 + \dots + U_n$. Pak následující podmínky jsou ekvivalentní:*

- (i) $V = U_1 \dot{+} U_2 \dot{+} \dots \dot{+} U_n$;
- (ii) $U_1 \cap U_2 = 0, (U_1 + U_2) \cap U_3 = 0, \dots, (U_1 + \dots + U_{n-1}) \cap U_n = 0$.

Je-li navíc prostor V konečněrozměrný, pak je s nimi ekvivalentní i podmínka

- (iii) $\dim V = \dim U_1 + \dots + \dim U_n$.

Důkaz. Cvičení. $\square$

Jsou-li $U_1, \dots, U_n$ podprostory nějakého vektorového prostoru V , pak mohou existovat dva různé přímé součty, $U_1 \dot{+} \dots \dot{+} U_n$ a $U_1 \oplus \dots \oplus U_n$. První z nich je podprostor V , kdežto druhý není. Nicméně, tyto přímé součty jsou izomorfní, což plyne z tvrzení uvedeného později v kapitole o lineárních zobrazeních.

Příklad. Buďte $V = \mathbb{R}^3$, $U_1 = \{(x, 0, 0) \mid x \in \mathbb{R}\}$ a $U_2 = \{(0, y, 0) \mid y \in \mathbb{R}\}$. Potom

$U_1 \dot{+} U_2 = \{(x, y, 0) \mid x, y \in \mathbb{R}\}$ je podprostor $\mathbb{R}^3$,

$\{(1, 0, 0), (0, 1, 0)\}$ je báze $U_1 \dot{+} U_2$ a

$$\dim(U_1 \dot{+} U_2) = 2.$$

$U_1 \oplus U_2 = \{((x, 0, 0), (0, y, 0)) \mid x, y \in \mathbb{R}\}$ není podprostor $\mathbb{R}^3$,

$\{((1, 0, 0), (0, 0, 0)), ((0, 0, 0), (0, 1, 0))\}$ je báze $U_1 \oplus U_2$ a

$$\dim(U_1 \oplus U_2) = 2. \quad \square$$

10.4. Popis podprostorů P^n homogenními soustavami

Každý podprostor prostoru P^n je množina všech řešení homogenní soustavy lineárních rovnic.

Tvrzení 10.4.1. *Každý podprostor $U \subseteq P^n$ je množina všech řešení homogenní soustavy $Ax = 0$, kde A je vhodná matice typu $m \times n$, přičemž $m = n - \dim U$.*

Důkaz. Podprostor U je konečněrozměrný, nechť $U = \llbracket v_1, \dots, v_k \rrbracket$. Je třeba najít matici A takovou, že U je množina všech řešení soustavy $Ax = 0$. Matice A tedy musí mít n sloupků a má platit

$$Av_i = 0 \quad \text{pro každé } i = 1, \dots, k,$$

což je totéž jako

$$AV = 0,$$

kde V je matice s k sloupky $v_1, \dots, v_k$. Transponujeme-li na obou stranách, obdržíme ekvivalentní rovnici

$$V^T A^T = 0.$$

Řádky hledané matice A tedy můžeme získat jako nějaký fundamentální systém řešení homogenní soustavy

$$V^T a = 0, \quad \text{kde } a \text{ je } n\text{-tice (sloupek) neznámých.}$$

Označme Ξ_A , resp. Ξ_{V^T} prostor všech řešení homogenní soustavy $Ax = 0$, resp. $V^T a = 0$. Máme $v_i \in \Xi_A$, odkud $\llbracket v_1, \dots, v_k \rrbracket \subseteq \Xi_A$. Přitom platí $\dim \Xi_A = n - \text{rank } A = n - \dim \Xi_{V^T} = n - (n - \text{rank } V^T) = \text{rank } V^T = \dim \llbracket v_1, \dots, v_k \rrbracket$. Tudíž, $\Xi_A = U$. $\square$

Příklad. Buď $U = \llbracket (1, 0, 2) \rrbracket \subset \mathbb{R}^3$. Najdeme soustavu rovnic, jejíž množina všech řešení je právě U .

Podle důkazu předchozího tvrzení je třeba vyřešit soustavu $V^T a = 0$, tedy rovnici

$$1 \cdot a^1 + 0 \cdot a^2 + 2 \cdot a^3 = 0.$$

Neznámá a^1 je hlavní, neznámé a^2, a^3 jsou parametry. Obecné řešení tedy je

$$a^1 = -2 \cdot t^2, \quad a^2 = t^1, \quad a^3 = t^2$$

a vhodnými volbami parametrů dostaneme fundamentální systém řešení

$$(0, 1, 0), \quad (-2, 0, 1).$$

Tudíž, matice hledané homogenní soustavy je

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

Není obtížné najít součet podprostorů zadaných generátory, resp. průnik podprostorů zadaných homogenními soustavami rovnic:

Cvičení. $\llbracket u_1, \dots, v_i \rrbracket + \llbracket u_{i+1}, \dots, u_n \rrbracket = \llbracket u_1, \dots, v_i, u_{i+1}, \dots, u_n \rrbracket$. $\square$

Cvičení. $\{x \mid A'x = 0\} \cap \{x \mid A''x = 0\} = \{x \mid Ax = 0\}$, kde

$$A = \begin{pmatrix} A' \\ A'' \end{pmatrix}. \quad \square$$

Protože zadání podprostoru generátory umíme převádět na zadání homogenní soustavou rovnic a naopak, umíme najít i součet podprostorů zadaných homogenními soustavami rovnic, resp. průnik podprostorů zadaných generátory.

11. LINEÁRNÍ ZOBRAZENÍ

11.1. Definice, příklady

Definice 11.1.1. Buďte U, V vektorové prostory nad polem P . Zobrazení $f: U \rightarrow V$ je *lineární*, přesněji *lineární nad polem P* , nebo *homomorfismus vektorových prostorů*, jestliže pro každé vektory $u, u_1, u_2 \in U$ a každý skalár $p \in P$ platí

- (i) $f(u_1 + u_2) = f(u_1) + f(u_2)$ (aditivita)
 (ii) $f(pu) = pf(u)$. (homogenita)

Definice 11.1.2. Lineární zobrazení $V \rightarrow V$ je *lineární transformace* vektorového prostoru V nebo také *lineární operátor* na vektorovém prostoru V .

Příklad. (1) Identické zobrazení $\text{id}: U \rightarrow U$, $\text{id}(a) = a$, je lineární.

(2) Nulové zobrazení $0: U \rightarrow U$, $0(a) = 0$, je lineární.

(3) Násobení skalárem $c \in P$: Zobrazení $f_c: U \rightarrow U$, $f_c(a) = ca$, je lineární. Nazývá se *homotetie*. Všimněte si, že předchozí dva příklady jsou speciální případy pro $c = 1$, resp. $c = 0$.

(4) Zobrazení $f: \mathbb{R} \rightarrow \mathbb{R}$ je lineární nad $\mathbb{R}$ právě tehdy, když existuje skalár $c \in \mathbb{R}$ takový, že $f(a) = ca$. Dokažte. Návod: Položte $c = f(1)$.

(5) Zobrazení $f: \mathbb{R}^3 \rightarrow \mathbb{R}^2$, $(x, y, z) \mapsto (3x + 2y + z, x - y)$, je lineární. Ověřte.

(6) Zobrazení $f: \mathbb{R}^2 \rightarrow \mathbb{R}^4$, $(x, y) \mapsto (x + y, x, x - y, y)$, je lineární. Ověřte.

(7) Buď A matice typu $m \times n$ nad polem P . Nechť $f_A: P^n \rightarrow P^m$ je zobrazení takové, že $f_A(x) = Ax$ (přesněji tedy $f_A: P^{n \times 1} \rightarrow P^{m \times 1}$). Čili, obraz n -tice $x = (x^1, \dots, x^n)$ je lineární kombinace sloupků matice A s koeficienty $x^1, \dots, x^n$,

$$f_A(x) = x^1 A_1^\circ + x^2 A_2^\circ + \dots + x^n A_n^\circ.$$

Potom f_A je lineární zobrazení.

(8) Zobrazení $\mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto \bar{z}$, kde $\bar{z}$ je číslo komplexně sdružené k číslu $z \in \mathbb{C}$, je lineární zobrazení vektorových prostorů nad $\mathbb{R}$. Toto zobrazení není lineární zobrazení nad $\mathbb{C}$. Ověřte.

(9) Zobrazení $\text{re}: \mathbb{C} \rightarrow \mathbb{R}$, $z \mapsto \text{re } z = \frac{1}{2}(z + \bar{z})$ (reálná část čísla z) je lineární zobrazení vektorových prostorů nad $\mathbb{R}$.

(10) Je-li $U \subseteq V$ podprostor, pak vložení $\iota_U: U \rightarrow V$, $\iota_U(u) = u$, je lineární zobrazení.

(11) Otáčení. Při otáčení Eukleidovské roviny kolem pevného bodu o úhel α se všechny vektory otáčejí o týž úhel α , nezávisle na jejich umístění. Vzniká zobrazení $\phi_\alpha: E^2 \rightarrow E^2$.

Otáčení převádí součet vektorů na součet vektorů a podobně c -násobek vektoru na c -násobek vektoru. Například aditivita se velmi názorně ověří poukazem na to, že otáčením kolem vrcholu se rovnoběžník převádí v rovnoběžník a délka jeho stran a úhlopříček se přitom nemění.

Podobně otáčení kolem pevné osy v trojrozměrném Eukleidovském prostoru představuje lineární zobrazení vektorů $E^3 \rightarrow E^3$.

(12) Rotace $E^3 \rightarrow E^3$.

(13) Rovnoběžné promítání. Promítání Eukleidovského prostoru E^3 do 2-rozměrného podprostoru (průmětny) R ve zvoleném směru L je zobrazení $E^3 \rightarrow R$. Směrem se rozumí libovolný 1-rozměrný podprostor L takový, že $E^3 = L \dot{+} R$. Průmět do roviny R je sčítanec x_R v (jednoznačném) vyjádření $x = x_L + x_R$, kde $x_L \in L$ a $x_R \in R$.

Promítání $p: E^3 \rightarrow R$ je lineární zobrazení. Aditivita se projevuje v tom, že průmětem rovnoběžníka je rovnoběžník.

(14) Projekce na přímku L procházející počátkem $E^2 \rightarrow L$.

(15) Osová souměrnost podle přímky procházející počátkem, $E^2 \rightarrow E^2$ i $E^3 \rightarrow E^3$.

(16) Zobrazení $U \rightarrow P^{\dim U}$ přiřazující vektorům jejich souřadnice vzhledem ke zvolené bázi, viz Tvzení 9.4.4.

(17) Zobrazení $P^{n \times n} \rightarrow P$, $A \mapsto \text{tr } A$, přiřazující matici A typu $n \times n$ nad polem P její stopu $\text{tr } A = \sum_i A_i^i$ (součet prvků na diagonále).

(18) Zobrazení $P[x] \rightarrow P[x]$, kde $P[x]$ je prostor polynomů, přiřazující polynomu jeho derivaci. Derivace může být například i zobrazení $P_n[x] \rightarrow P_{n-1}[x]$, nebo zobrazení z prostoru diferencovatelných funkcí do prostoru všech funkcí.

(19) Zobrazení z prostoru všech integrovatelných funkcí na uzavřeném intervalu do $\mathbb{R}$ přiřazující funkci její určitý integrál. $\square$

Cvičení. Lineární zobrazení $U \rightarrow V$ je homomorfismus grup $(U, +, 0, -) \rightarrow (V, +, 0, -)$. Speciálně,

$$f(0) = 0 \quad \text{a} \quad f(-u) = -f(u). \quad \square$$

Cvičení. Buď $f: U \rightarrow V$ zobrazení vektorových prostorů. Matematickou indukcí ukažte, že f je lineární právě tehdy, když pro libovolné $n \in \mathbb{N}$, $u_1, \dots, u_n \in U$ a skaláry $p^1, \dots, p^n$ platí

$$f(p^1 u_1 + \dots + p^n u_n) = p^1 f(u_1) + \dots + p^n f(u_n),$$

tedy obraz lineární kombinace je lineární kombinace obrazů. $\square$

Cvičení. Buď $f: V \rightarrow W$ lineární zobrazení. Je-li U podprostor V , potom $f(U)$ je podprostor W . $\square$

Lineární zobrazení je jednoznačně určeno obrazy vektorů libovolné báze:

Tvrzení 11.1.1. *Buďte U, V vektorové prostory nad polem P , $(u_1, \dots, u_n)$ báze U . Pak pro každou n -tici $v_1, \dots, v_n \in V$ existuje právě jedno lineární zobrazení $f: U \rightarrow V$ takové, že $f(u_1) = v_1, \dots, f(u_n) = v_n$.*

Důkaz. Buďte $v_1, \dots, v_n \in V$. Pro $u \in U$ existují $x^1, \dots, x^n \in P$ tak, že $u = x^1 u_1 + \dots + x^n u_n$. Položme $f(u) = x^1 v_1 + \dots + x^n v_n$. Cvičení: ověřte, že $f(u_i) = v_i$, f je lineární a je-li f' zobrazení s těmito vlastnostmi, potom $f' = f$. $\square$

Tvrzení 11.1.2. *Buďte $f: U \rightarrow V$ a $g: V \rightarrow W$ lineární zobrazení. Pak $g \circ f: U \rightarrow W$ je lineární zobrazení.*

Důkaz. Buďte U, V, W vektorové prostory nad polem P . Pro libovolná $u_1, u_2 \in U$ máme

$$\begin{aligned} (g \circ f)(u_1 + u_2) &= g(f(u_1 + u_2)) = \\ &= g(f(u_1) + f(u_2)) = \\ &= g(f(u_1)) + g(f(u_2)) = \\ &= (g \circ f)(u_1) + (g \circ f)(u_2). \end{aligned}$$

Pro libovolné $u \in U$ a $p \in P$ máme

$$\begin{aligned} (g \circ f)(pu) &= g(f(pu)) = \\ &= g(pf(u)) = \\ &= pg(f(u)) = \\ &= p(g \circ f)(u). \end{aligned} \quad \square$$

11.2. Jádro a obraz

Definice 11.2.1. Buď $f: U \rightarrow V$ lineární zobrazení. Množina

$$\text{Ker } f = \{u \in U \mid f(u) = 0\}$$

je *jádro* zobrazení f a množina

$$\text{Im } f = f(U) = \{f(u) \mid u \in U\}$$

je *obraz* zobrazení f .

Tvrzení 11.2.1. Buď $f: U \rightarrow V$ lineární zobrazení. Pak

- (1) $\text{Ker } f$ je podprostor U ,
- (2) $\text{Im } f$ je podprostor V .

Důkaz. (1) (i) $f(0) = 0$, takže $0 \in \text{Ker } f$. (ii) Pro $u_1, u_2 \in \text{Ker } f$ platí $f(u_1 + u_2) = f(u_1) + f(u_2) = 0 + 0 = 0$, takže $u_1 + u_2 \in \text{Ker } f$. (iii) Pro $u \in \text{Ker } f$ a $p \in P$ platí $f(pu) = pf(u) = p \cdot 0 = 0$, takže $pu \in \text{Ker } f$.

(2) (i) $f(0) = 0$, takže $0 \in \text{Im } f$. (ii) Pro $v_1, v_2 \in \text{Im } f$ existují $u_1, u_2 \in U$ takové, že $f(u_1) = v_1$ a $f(u_2) = v_2$. Potom $f(u_1 + u_2) = f(u_1) + f(u_2) = v_1 + v_2$, takže $v_1 + v_2 \in \text{Im } f$. (iii) Buďte $v \in \text{Im } f$ a $p \in P$. Potom existuje $u \in U$ takové, že $f(u) = v$, a $f(pu) = pf(u) = pv$, takže $pv \in \text{Im } f$. $\square$

Příklad. (1) Pro lineární zobrazení re z příkladu (9) platí:

$$\text{Im } \text{re} = \mathbb{R}, \quad \text{Ker } \text{re} = \mathbb{R}i = \{ri \mid r \in \mathbb{R}\}.$$

(2) Při rovnoběžném promítání $p: E^3 \rightarrow E^2$ je podprostor $\text{Ker } p$ totožný se směrem promítání, kdežto $\text{Im } p = E^2$.

(3) Při otáčení $\phi_\alpha: E^2 \rightarrow E^2$ o úhel $\alpha \neq 2k\pi$ je $\text{Im } \phi_\alpha = E^2$, zatímco $\text{Ker } \phi_\alpha$ je nulový podprostor. $\square$

Tvrzení 11.2.2. Lineární zobrazení f je injektivní právě tehdy, když $\text{Ker } f = \{0\}$.

Důkaz. Buď f injektivní. Zřejmě $0 \in \text{Ker } f$. Je-li $u \in \text{Ker } f$, pak $f(u) = f(0) = 0$, a díky injektivitě $u = 0$. Čili $\text{Ker } f = \{0\}$.

Nechť $\text{Ker } f = \{0\}$. Je-li $f(u_1) = f(u_2)$, pak $f(u_1 - u_2) = f(u_1) - f(u_2) = 0$, takže $u_1 - u_2 \in \text{Ker } f$, čili $u_1 - u_2 = 0$ a $u_1 = u_2$. $\square$

Cvičení. Buď $f: U \rightarrow V$ lineární zobrazení. Potom f je injektivní právě tehdy, když pro každou lineárně nezávislou množinu $\{u_1, \dots, u_n\} \subset U$ je $\{f(u_1), \dots, f(u_n)\}$ lineárně nezávislá množina. $\square$

Tvrzení 11.2.3. Buď $f: U \rightarrow V$ lineární zobrazení, kde U je konečněrozměrný prostor. Potom f je injektivní právě tehdy, když existuje báze $(u_1, \dots, u_n)$ prostoru U taková, že $\{f(u_1), \dots, f(u_n)\}$ lineárně nezávislá množina.

Důkaz. „ $\Rightarrow$ “ Nechť f je injektivní. Jelikož U je konečněrozměrný, podle Tvrzení 9.3.1 má bázi, označme ji $(u_1, \dots, u_n)$. Jestliže

$$x^1 f(u_1) + \dots + x^n f(u_n) = 0,$$

potom díky linearitě f

$$f(x^1 u_1 + \dots + x^n u_n) = 0, \quad \text{tj.} \quad x^1 u_1 + \dots + x^n u_n \in \text{Ker } f.$$

Podle Tvrzení 11.2.2 $\text{Ker } f = \{0\}$, takže

$$x^1 u_1 + \dots + x^n u_n = 0.$$

Z lineární nezávislosti množiny $\{u_1, \dots, u_n\}$ plyne $x^1 = \dots = x^n = 0$. Tedy, množina $\{f(u_1), \dots, f(u_n)\}$ je lineárně nezávislá.

„ $\Leftarrow$ “ Necht U má bázi $(u_1, \dots, u_n)$ takovou, že $\{f(u_1), \dots, f(u_n)\}$ je lineárně nezávislá množina. Budte

$$u = x^1 u_1 + \dots + x^n u_n, \quad v = y^1 u_1 + \dots + y^n u_n$$

takové, že

$$\sum_{i=1}^n x^i f(u_i) = f\left(\sum_{i=1}^n x^i u_i\right) = f(u) = f(v) = f\left(\sum_{i=1}^n y^i u_i\right) = \sum_{i=1}^n y^i f(u_i).$$

Potom

$$(x^1 - y^1)f(u_1) + \dots + (x^n - y^n)f(u_n) = 0$$

a z lineární nezávislosti množiny $\{f(u_1), \dots, f(u_n)\}$ plyne

$$x^1 - y^1 = \dots = x^n - y^n = 0 \quad \text{čili} \quad x^1 = y^1, \dots, x^n = y^n \quad \text{a} \quad u = v.$$

Takže f je injektivní. $\square$

Tvrzení 11.2.4. *Bud $f: U \rightarrow V$ lineární zobrazení, kde U je konečněrozměrný prostor. Potom f je surjektivní právě tehdy, když existuje báze $(u_1, \dots, u_n)$ prostoru U taková, že $\{f(u_1), \dots, f(u_n)\}$ generuje V .*

Důkaz. „ $\Rightarrow$ “ Necht f je surjektivní. Jelikož U je konečněrozměrný, podle Tvrzení 9.3.1 má bázi, označme ji $(u_1, \dots, u_n)$. Bud $v \in V$. Jelikož f je surjektivní, existuje

$$u = x^1 u_1 + \dots + x^n u_n \in U$$

takové, že

$$v = f(u) = f(x^1 u_1 + \dots + x^n u_n) = x^1 f(u_1) + \dots + x^n f(u_n).$$

Tedy, $\{f(u_1), \dots, f(u_n)\}$ generuje V .

„ $\Leftarrow$ “ Necht U má bázi $(u_1, \dots, u_n)$ takovou, že $\{f(u_1), \dots, f(u_n)\}$ generuje V . Bud $v \in V$. Potom

$$v = x^1 f(u_1) + \dots + x^n f(u_n) = f(x^1 u_1 + \dots + x^n u_n).$$

Tedy, f je surjektivní. $\square$

Cvičení. Bud $f: U \rightarrow V$ lineární zobrazení, kde U je konečněrozměrný prostor. Potom f je surjektivní právě tehdy, když pro každou množinu generátorů $\{u_1, \dots, u_n\}$ prostoru U množina $\{f(u_1), \dots, f(u_n)\}$ generuje prostor V . $\square$

Jsou-li oba prostory U, V konečněrozměrné, pak číslo $\dim \text{Ker } f$ se nazývá *defekt* a číslo $\dim \text{Im } f$ *hodnota* lineárního zobrazení. Platí o nich následující tvrzení.

Tvrzení 11.2.5. *Budte U, V konečněrozměrné vektorové prostory a $f: U \rightarrow V$ lineární zobrazení. Pak*

$$\dim \text{Ker } f + \dim \text{Im } f = \dim U.$$

Důkaz. Bud $(u_1, \dots, u_m)$ báze podprostoru $\text{Ker } f$ a doplňme ji vektory $u_{m+1}, \dots, u_n$ do báze $(u_1, \dots, u_m, u_{m+1}, \dots, u_n)$ prostoru U .

Potom množina $\{f(u_1), \dots, f(u_m), f(u_{m+1}), \dots, f(u_n)\}$ generuje $f(U) = \text{Im } f$ (viz Tvrzení 11.2.4). Jelikož $f(u_1) = \dots = f(u_m) = 0$, tak i množina $\{f(u_{m+1}), \dots, f(u_n)\}$ generuje $\text{Im } f$.

Jestliže

$$x^{m+1} f(u_{m+1}) + \dots + x^n f(u_n) = 0,$$

díky linearitě f tedy

$$f(x^{m+1} u_{m+1} + \dots + x^n u_n) = 0, \quad \text{tj.} \quad x^{m+1} u_{m+1} + \dots + x^n u_n \in \text{Ker } f,$$

potom pro vhodné koeficienty $x^1, \dots, x^m$

$$x^{m+1}u_{m+1} + \dots + x^n u_n = x^1 u_1 + \dots + x^m u_m$$

tedy

$$x^1 u_1 + \dots + x^m u_m - x^{m+1} u_{m+1} - \dots - x^n u_n = 0.$$

Z lineární nezávislosti množiny $\{u_1, \dots, u_m, u_{m+1}, \dots, u_n\}$ vyplývá, že všechny koeficienty $x^1, \dots, x^m, x^{m+1}, \dots, x^n$ jsou nulové, takže množina $\{f(u_{m+1}), \dots, f(u_n)\}$ je lineárně nezávislá.

Tedy, $(f(u_{m+1}), \dots, f(u_n))$ je báze podprostoru $\text{Im } f$, takže $\dim \text{Im } f = n - m = \dim U - \dim \text{Ker } f$. $\square$

11.3. Izomorfismy

Stejně jako u jiných algebraických struktur, bijektivní homomorfismy se nazývají izomorfismy.

Definice 11.3.1. *Izomorfismus* vektorových prostorů je bijektivní lineární zobrazení. Vektorové prostory U, V jsou *izomorfní*, existuje-li mezi nimi izomorfismus. Zapisujeme $U \cong V$.

Příklad. (1) Homotetie $f_c: a \mapsto ca$ z příkladu (3) je izomorfismus právě tehdy, když $c \neq 0$.

(2) Homomorfismus $z \mapsto \bar{z}$ z příkladu (8) je izomorfismus $\mathbb{C} \cong \mathbb{C}$.

(3) Homomorfismus re z příkladu (9) není izomorfismus (není injektivní).

(4) Otáčení je izomorfismus.

(5) Rovnoběžné promítání $E^3 \rightarrow E^2$ není izomorfismus. $\square$

Tvrzení 11.3.1. *Buď $f: U \rightarrow V$ lineární zobrazení, kde U je konečněrozměrný prostor. Potom f je izomorfismus právě tehdy, když existuje báze $(u_1, \dots, u_n)$ prostoru U taková, že $(f(u_1), \dots, f(u_n))$ je báze prostoru V .*

Důkaz. Tvrzení vyplývá z Tvrzení 11.2.3 a 11.2.4. $\square$

Cvičení. Buď $f: U \rightarrow V$ lineární zobrazení, kde U je konečněrozměrný prostor. Potom f je izomorfismus právě tehdy, když pro každou bázi $(u_1, \dots, u_n)$ prostoru U je $(f(u_1), \dots, f(u_n))$ báze prostoru V . $\square$

Tvrzení 11.3.2. *Buď $f: U \rightarrow V$ izomorfismus. Pak $f^{-1}: V \rightarrow U$ je také izomorfismus.*

Důkaz. Zobrazení f je bijektivní, takže k němu existuje inverzní zobrazení f^{-1} , a to je také bijektivní. Zbývá dokázat, že je lineární. Buďte $v_1, v_2 \in V$. Díky bijektivnosti zobrazení f existují $u_1, u_2 \in U$ takové, že $f(u_1) = v_1$ a $f(u_2) = v_2$. Potom

$$\begin{aligned} f^{-1}(v_1 + v_2) &= f^{-1}(f(u_1) + f(u_2)) = \\ &= f^{-1}(f(u_1 + u_2)) = \\ &= u_1 + u_2 = \\ &= f^{-1}(v_1) + f^{-1}(v_2). \end{aligned}$$

Důkaz homogenity necháme jako cvičení. $\square$

Cvičení. Dokažte, že relace „být izomorfní“ je relace ekvivalence (reflexivní, symetrická, tranzitivní). $\square$

Izomorfní prostory se z hlediska lineární algebry liší jen v označení prvků a operací, není mezi nimi žádný rozdíl odhalitelný prostředky lineární algebry.

V konečněrozměrném případě je situace obzvlášť příjemná: každý prostor je izomorfní s některým prostorem P^n .

Tvrzení 11.3.3. *Každý konečněrozměrný vektorový prostor U nad polem P je izomorfní s prostorem $P^{\dim U}$.*

Důkaz. Zobrazení $U \rightarrow P^{\dim U}$, které vektorům přiřazuje jejich souřadnice vzhledem k pevně zvolené bázi, je izomorfismus (ověřte podrobně). $\square$

Počítání se souřadnicemi vektorů z U je tedy počítání v izomorfním prostoru $P^{\dim U}$. Na druhé straně, tento izomorfismus závisí na volbě báze, a to je důvod, proč není vhodné prostory U a $P^{\dim U}$ ztotožňovat.

Tvrzení 11.3.4. *Konečněrozměrné vektorové prostory nad stejným polem jsou izomorfní právě tehdy, když mají stejnou dimenzi.*

Důkaz. Buď $f: U \rightarrow V$ izomorfismus (tedy, mimo jiné, injekce a surjekce). Potom $\dim \operatorname{Ker} f = 0$ (viz Tvrzení 11.2.2) a $\dim \operatorname{Im} f = \dim V$, a proto díky Tvrzení 11.2.5 $\dim U = \dim \operatorname{Ker} f + \dim \operatorname{Im} f = \dim V$.

Jestliže $\dim U = \dim V$, pak $U \cong P^{\dim U} = P^{\dim V} \cong V$. $\square$

11.3.1. Přímé součty vektorových (pod)prostorů

Už známe přímý součet prostorů a přímý součet podprostorů. Jsou-li $U_1, \dots, U_n$ podprostory vektorového prostoru U , pak mohou existovat dva různé přímé součty, $U_1 + \dots + U_n$ a $U_1 \oplus \dots \oplus U_n$. První z nich je podprostor prostoru U , kdežto druhý není. Nicméně, podle následujícího tvrzení tyto přímé součty jsou izomorfní.

Tvrzení 11.3.5. *Buďte $U_1, \dots, U_n$ podprostory konečněrozměrného vektorového prostoru U . Pak následující výroky jsou ekvivalentní:*

- (1) *součet $U_1 + \dots + U_n$ je přímý;*
- (2) *$U_1 + \dots + U_n \cong U_1 \oplus \dots \oplus U_n$.*

Důkaz. Předpokládejme, že součet $U_1 + \dots + U_n$ je přímý. Buď $p: U_1 \oplus \dots \oplus U_n \rightarrow U_1 + \dots + U_n$, $(u_1, \dots, u_n) \mapsto u_1 + \dots + u_n$. Zobrazení p je lineární (cvičení). Jelikož součet $U_1 + \dots + U_n$ je přímý, každé $u \in U_1 + \dots + U_n$ lze zapsat právě jedním způsobem jako $u = u_1 + \dots + u_n$, kde $u_i \in U_i$ pro každé $i = 1, \dots, n$. Můžeme tedy definovat zobrazení $U_1 \oplus \dots \oplus U_n \rightarrow U_1 + \dots + U_n$, $u \mapsto (u_1, \dots, u_n)$. Toto zobrazení je inverzní k p , tudíž p je bijekce, a tedy izomorfismus.

Předpokládejme, že $U_1 + \dots + U_n \cong U_1 \oplus \dots \oplus U_n$. Potom $\dim(U_1 + \dots + U_n) = \dim(U_1 \oplus \dots \oplus U_n) = \dim U_1 + \dots + \dim U_n$ a podle Tvrzení 10.3.3 součet $U_1 + \dots + U_n$ je přímý. $\square$

Cvičení. Dokažte, že zobrazení p z předchozího důkazu je lineární. $\square$

Cvičení. Pro každé $i = 1, \dots, n$ zobrazení $\pi_i: U_1 \oplus \dots \oplus U_n \rightarrow U_i$ zadané předpisem $(u_1, \dots, u_n) \mapsto u_i$ se nazývá *i-tá projekce*.

Pro každé $i = 1, \dots, n$ zobrazení $\iota_i: U_i \rightarrow U_1 \oplus \dots \oplus U_n$ zadané předpisem $u \mapsto (0, \dots, 0, u, 0, \dots, 0)$, kde u stojí na *i-tém* místě, se nazývá *vložení i-tého sčítance*.

Ukažte, že projekce π_i a vložení ι_i jsou lineární zobrazení. Spočtete $\pi_i \circ \iota_j$. $\square$

11.4. Matice lineárního zobrazení

V příkladu (7) v 11.1 pro každou matici A typu $m \times n$ nad polem P je $f_A: P^n \rightarrow P^m$, $x \mapsto Ax$, lineární zobrazení.

Na druhou stranu, pro každé lineární zobrazení $f: P^n \rightarrow P^m$ existuje jediná matice A taková, že $f = f_A$. Pro každé $i \in \{1, \dots, n\}$ buď e_i i -tý vektor kanonické báze P^n , tedy $e_i = (0, \dots, 0, 1, 0, \dots, 0)$, kde 1 je na i -tém místě. Potom pro libovolné $x = (x^1, \dots, x^n) \in P^n$ platí

$$f(x) = f(x^1 e_1 + \dots + x^n e_n) = x^1 f(e_1) + \dots + x^n f(e_n).$$

Čili pro matici A , jejíž sloupky jsou $f(e_1), \dots, f(e_n)$, platí $f(x) = Ax$ a $f = f_A$.

Obdobně lze libovolnému lineárnímu zobrazení mezi konečněrozměrnými vektorovými prostory přiřadit matici, která toto zobrazení popisuje, a to sice matici reprezentující příslušné lineární zobrazení mezi prostory souřadnic vektorů vzhledem ke zvoleným bázím vektorových prostorů.

Definice 11.4.1. Buďte U, V vektorové prostory, $\mathbf{u} = (u_1, \dots, u_n)$ báze U , $\mathbf{v} = (v_1, \dots, v_m)$ báze V a $f: U \rightarrow V$ lineární zobrazení. Matice A typu $m \times n$, jejíž i -tý sloupek je tvořen souřadnicemi vektoru $f(u_i)$ vzhledem k bázi $\mathbf{v}$, je *matice lineárního zobrazení f vzhledem k bázím $\mathbf{u}$ a $\mathbf{v}$* .
Jestliže f je lineární transformace, tedy $U = V$, a $\mathbf{u} = \mathbf{v}$, potom A je *matice lineární transformace f vzhledem k bázi $\mathbf{v}$* .

Přesněji, A_i^j je j -tá souřadnice obrazu $f(u_i)$ vzhledem k bázi $\mathbf{v}$. Platí tedy

$$f(u_i) = \sum_j A_i^j v_j.$$

Tvrzení 11.4.1. *Buďte U, V konečněrozměrné vektorové prostory, $\mathbf{u}$ báze U , $\mathbf{v}$ báze V , $f: U \rightarrow V$ lineární zobrazení, $u \in U$, A matice f , x souřadnice u , y souřadnice $f(u)$ vzhledem ke zvoleným bázím. Potom*

$$y = Ax.$$

Je-li B matice taková, že $y = Bx$, potom $B = A$.

Důkaz. Necht $\mathbf{u} = (u_1, \dots, u_n)$, $\mathbf{v} = (v_1, \dots, v_m)$, $x = (x^1, \dots, x^n)$ a $y = (y^1, \dots, y^m)$. Jelikož $u = \sum_i x^i u_i$, tak

$$\begin{aligned} f(u) &= f\left(\sum_i x^i u_i\right) = \sum_i f(x^i u_i) = \sum_i x^i f(u_i) = \sum_i x^i \sum_j A_i^j v_j = \\ &= \sum_j \sum_i x^i A_i^j v_j = \left(\sum_i x^i A_i^1\right) v_1 + \dots + \left(\sum_i x^i A_i^m\right) v_m. \end{aligned}$$

Čili j -tá souřadnice vektoru $f(u)$ vzhledem k bázi $\mathbf{v}$ je $y^j = \sum_i x^i A_i^j = \sum_i A_i^j x^i$, což je právě hodnota získaná na j -tém řádku součinu matic $A \cdot x$, a tedy $y = Ax$.

Buď B matice taková, že $y = Bx$. Potom B má n sloupků, aby součin Bx mohl existovat, a m řádků, aby se součin Bx mohl rovnat y . Čili B je typu $m \times n$ stejně jako A . Pro $i \in \{1, 2, \dots, n\}$ označme $x_i = (x_i^1, \dots, x_i^n)$ souřadnice vektoru u_i vzhledem k bázi $\mathbf{u}$ a $y_i = (y_i^1, \dots, y_i^m)$ souřadnice vektoru $f(u_i)$ vzhledem k bázi $\mathbf{v}$. Potom $x_i = (0, \dots, 0, 1, 0, \dots, 0)$, kde 1 je na i -tém místě, a $y_i = Bx_i = B_i^\circ$. Podle definice matice lineárního zobrazení zároveň $y_i = A_i^\circ$, takže $B = A$. $\square$

Příklad. Mějme $\alpha: \mathbb{R}_2[x] \rightarrow \mathbb{R}_1[x]$, $f \mapsto f'$. Je to tedy zobrazení z prostoru polynomů stupně nejvýše 2 do prostoru polynomů stupně nejvýše 1, které polynomu přiřazuje jeho derivaci. Ověřte, že se jedná o lineární zobrazení.

V $\mathbb{R}_2[x]$ uvažujme bázi $(1, x, x^2)$ a v $\mathbb{R}_1[x]$ bázi $(1, x)$. Ověřte, že jsou to báze. Najdeme obrazy vektorů báze $(1, x, x^2)$ při zobrazení α a jejich souřadnice v bázi $(1, x)$.

$$\begin{aligned}\alpha(1) &= 0, & \text{souřadnice vektoru } 0 \text{ v bázi } (1, x) \text{ jsou } (0, 0); \\ \alpha(x) &= 1, & \text{souřadnice vektoru } 1 \text{ v bázi } (1, x) \text{ jsou } (1, 0); \\ \alpha(x^2) &= 2x, & \text{souřadnice vektoru } 2x \text{ v bázi } (1, x) \text{ jsou } (0, 2).\end{aligned}$$

Matice zobrazení α vzhledem k bázím $(1, x, x^2)$ a $(1, x)$ tedy je

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

Například, $\alpha(3x^2 + 2x + 7) = 6x + 2$. Vektor $3x^2 + 2x + 7$ má v bázi $(1, x, x^2)$ souřadnice $x = (7, 2, 3)$ a vektor $6x + 2$ má v bázi $(1, x)$ souřadnice $y = (2, 6)$. Ověřte. A platí

$$A \cdot x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 6 \end{pmatrix} = y. \quad \square$$

Příklad. Matice identického zobrazení $\text{id}: U \rightarrow U$, $\text{id}(u) = u$, vzhledem k bázím $\mathfrak{e}$ a $\mathfrak{e}'$ (v tomto pořadí) je matice přechodu od báze $\mathfrak{e}$ k bázi $\mathfrak{e}'$. $\square$

Tvrzení 11.4.2. *Bud' U, V, W vektorové prostory, $\mathfrak{u}$ báze U , $\mathfrak{v}$ báze V , $\mathfrak{w}$ báze W . Bud' $\alpha: U \rightarrow V$, $\beta: V \rightarrow W$ lineární zobrazení. Bud' A matice zobrazení α vzhledem k bázím $\mathfrak{u}$ a $\mathfrak{v}$, bud' B matice zobrazení β vzhledem k bázím $\mathfrak{v}$ a $\mathfrak{w}$. Potom BA je matice zobrazení $\beta \circ \alpha$ vzhledem k bázím $\mathfrak{u}$ a $\mathfrak{w}$.*

Důkaz. Nechť $\mathfrak{u} = (u_1, \dots, u_m)$, $\mathfrak{v} = (v_1, \dots, v_n)$ a $\mathfrak{w} = (w_1, \dots, w_p)$. Jelikož $\alpha(u_i) = \sum_j A_i^j v_j$ a $\beta(v_j) = \sum_k B_j^k w_k$, tak

$$\begin{aligned}(\beta \circ \alpha)(u_i) &= \beta(\alpha(u_i)) = \beta\left(\sum_j A_i^j v_j\right) = \sum_j A_i^j \beta(v_j) = \sum_j A_i^j \sum_k B_j^k w_k = \\ &= \sum_{j,k} A_i^j B_j^k w_k = \sum_k \sum_j A_i^j B_j^k w_k = \\ &= \left(\sum_j A_i^j B_j^1\right) w_1 + \dots + \left(\sum_j A_i^j B_j^p\right) w_p.\end{aligned}$$

Čili v k -tém řádku i -tého sloupku matice zobrazení $\beta \circ \alpha$ je $\sum_j A_i^j B_j^k = \sum_j B_j^k A_i^j$, což je totéž, co dostaneme na stejném místě v součinu $B \cdot A$. $\square$

Tvrzení 11.4.3. *Bud' α izomorfismus a A jeho matice vzhledem k nějakým bázím. Pak A je invertibilní a A^{-1} je matice inverzního izomorfismu α^{-1} .*

Důkaz. Bud' $\alpha: U \rightarrow V$ a bud' B matice lineárního zobrazení $\alpha^{-1}: V \rightarrow U$ vzhledem k příslušným bázím. Matice lineárního zobrazení $\alpha^{-1} \circ \alpha = \text{id}_U$ vzhledem k bázi prostoru U je jednotková matice E a podle předchozího tvrzení je to matice BA . Čili, $BA = E$, A je tedy invertibilní a $A^{-1} = B$. $\square$

Důsledek. *Každá matice přechodu od báze k bázi je invertibilní.*

Důkaz. Podle uvedených definic matice přechodu je totéž co matice identity, což je izomorfismus. $\square$

Tvrzení 11.4.4. *Bud' U vektorový prostor s bázemi $\mathfrak{u}$ a $\mathfrak{u}'$, bud' Q matice přechodu od báze $\mathfrak{u}$ k bázi $\mathfrak{u}'$. Bud' V vektorový prostor s bázemi $\mathfrak{v}$ a $\mathfrak{v}'$, bud' R matice přechodu od báze $\mathfrak{v}$ k bázi $\mathfrak{v}'$. Bud' $\alpha: U \rightarrow V$ lineární zobrazení, bud' A matice zobrazení α vzhledem k bázím $\mathfrak{u}$ a $\mathfrak{v}$ a bud' A' matice zobrazení α vzhledem k bázím $\mathfrak{u}'$ a $\mathfrak{v}'$. Pak*

$$A' = RAQ^{-1}.$$

Důkaz. Necht' $\mathbf{u} = (u_1, \dots, u_n)$, $\mathbf{u}' = (u'_1, \dots, u'_n)$, $\mathbf{v} = (v_1, \dots, v_m)$ a $\mathbf{v}' = (v'_1, \dots, v'_m)$. Situaci můžeme znázornit diagramem

$$\begin{array}{ccc} \boxed{\begin{array}{c} \mathbf{U} \\ (u_1, \dots, u_n) \end{array}} & \xrightarrow[\mathbf{A}]{\alpha} & \boxed{\begin{array}{c} \mathbf{V} \\ (v_1, \dots, v_m) \end{array}} \\ \text{id}_U \downarrow \mathbf{Q} & & \text{id}_V \downarrow \mathbf{R} \\ \boxed{\begin{array}{c} \mathbf{U} \\ (u'_1, \dots, u'_n) \end{array}} & \xrightarrow[\mathbf{A}']{\alpha} & \boxed{\begin{array}{c} \mathbf{V} \\ (v'_1, \dots, v'_m) \end{array}} \end{array}$$

V rozích stojí vektorové prostory s vyznačenými bázemi, šipky označují lineární zobrazení a jsou u nich uvedeny také matice těchto zobrazení. Platí $\alpha \circ \text{id}_U = \text{id}_V \circ \alpha$ a také $\alpha = \text{id}_V \circ \alpha \circ \text{id}_U^{-1}$. Podle Tvzení 11.4.2 o matici složeného zobrazení potom

$$\mathbf{A}'\mathbf{Q} = \mathbf{R}\mathbf{A} \quad \text{a také} \quad \mathbf{A}' = \mathbf{R}\mathbf{A}\mathbf{Q}^{-1}. \quad \square$$

Příklad. Mějme $\alpha: \mathbb{R}_2[x] \rightarrow \mathbb{R}_1[x]$, $f \mapsto f'$. Je to tedy zobrazení z prostoru polynomů stupně nejvýše 2 do prostoru polynomů stupně nejvýše 1, které polynomu přiřazuje jeho derivaci.

(1) Nejprve uvažujme (staré) báze $(1, x, x^2)$ v $\mathbb{R}_2[x]$ a $(1, x)$ v $\mathbb{R}_1[x]$. Ověřte, že jsou to báze. Najdeme obrazy vektorů báze $(1, x, x^2)$ při zobrazení α a jejich souřadnice v bázi $(1, x)$.

$$\begin{array}{ll} \alpha(1) = 0, & \text{souřadnice vektoru } 0 \text{ v bázi } (1, x) \text{ jsou } (0, 0); \\ \alpha(x) = 1, & \text{souřadnice vektoru } 1 \text{ v bázi } (1, x) \text{ jsou } (1, 0); \\ \alpha(x^2) = 2x, & \text{souřadnice vektoru } 2x \text{ v bázi } (1, x) \text{ jsou } (0, 2). \end{array}$$

Matice zobrazení α vzhledem k bázím $(1, x, x^2)$ a $(1, x)$ tedy je

$$\mathbf{A}_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

(2) Nyní uvažujme (nové) báze $(x^2, x+1, x)$ v $\mathbb{R}_2[x]$ a $(x+1, 1)$ v $\mathbb{R}_1[x]$. Ověřte, že jsou to báze. Najdeme obrazy vektorů báze $(x^2, x+1, x)$ při zobrazení α a jejich souřadnice v bázi $(x+1, 1)$.

$$\begin{array}{ll} \alpha(x^2) = 2x, & \text{souřadnice vektoru } 2x \text{ v bázi } (x+1, 1) \text{ jsou } (2, -2); \\ \alpha(x+1) = 1, & \text{souřadnice vektoru } 1 \text{ v bázi } (x+1, 1) \text{ jsou } (0, 1); \\ \alpha(x) = 1, & \text{souřadnice vektoru } 1 \text{ v bázi } (x+1, 1) \text{ jsou } (0, 1). \end{array}$$

Matice zobrazení α vzhledem k bázím $(x^2, x+1, x)$ a $(x+1, 1)$ tedy je

$$\mathbf{A}_2 = \begin{pmatrix} 2 & 0 & 0 \\ -2 & 1 & 1 \end{pmatrix}.$$

Například, $\alpha(3x^2+2x+7) = 6x+2$. Vektor $3x^2+2x+7$ má staré souřadnice $a = (7, 2, 3)$ a nové souřadnice $a' = (3, 7, -5)$. Vektor $6x+2$ má staré souřadnice $b = (2, 6)$ a nové souřadnice $b' = (6, -4)$. Ověřte. A platí

$$\mathbf{A}_1 \cdot a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 6 \end{pmatrix} = b$$

a

$$A_2 \cdot a' = \begin{pmatrix} 2 & 0 & 0 \\ -2 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 7 \\ -5 \end{pmatrix} = \begin{pmatrix} 6 \\ -4 \end{pmatrix} = b'.$$

Matice přechodu od staré báze $(1, x, x^2)$ k nové bázi $(x^2, x+1, x)$ v $\mathbb{R}_2[x]$ je

$$Q_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ -1 & 1 & 0 \end{pmatrix}.$$

Matice přechodu od staré báze $(1, x)$ k nové bázi $(x+1, 1)$ v $\mathbb{R}_1[x]$ je

$$Q_2 = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}.$$

A platí

$$\begin{aligned} Q_2 \cdot A_1 \cdot Q_3^{-1} &= \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \\ &= \begin{pmatrix} 0 & 0 & 2 \\ 0 & 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ -2 & 1 & 1 \end{pmatrix} = A_2. \end{aligned} \quad \square$$

Poznámka. Pokud ve Tvzení 11.4.4 $U = V$, $u = v$ a $u' = v'$, tedy $Q = R$ a α je lineární transformace $V \rightarrow V$, potom

$$A' = Q A Q^{-1}.$$

Definice 11.4.2. Matice A je *podobná* matici B , jestliže existuje invertibilní matice Q taková, že $B = Q^{-1} A Q$. Zapisujeme $A \approx B$.
Zobrazení $A \mapsto Q^{-1} A Q$ je *podobnostní transformace*.

Cvičení. Dokažte, že relace $\approx$ je relace ekvivalence na množině všech čtvercových matic stejného typu nad stejným polem. $\square$

Příklad. Matice jedné lineární transformace vzhledem k různým bázím jsou podobné. $\square$

11.5. Determinant

Je-li $A = (A_j^i)$ čtvercová matice typu $n \times n$ nad polem P , potom $|\det A|$ je objem n -rozměrného rovnoběžnostěnu v P^n určeného vektory (vrcholy)

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} A_1^1 \\ A_1^2 \\ \vdots \\ A_1^n \end{pmatrix}, \begin{pmatrix} A_2^1 \\ A_2^2 \\ \vdots \\ A_2^n \end{pmatrix}, \dots, \begin{pmatrix} A_n^1 \\ A_n^2 \\ \vdots \\ A_n^n \end{pmatrix}.$$

Nechť $f_A: P^n \rightarrow P^n$, $f_A(x) = Ax$ (viz Příklad (7) v podkapitole 11.1). Buď $(e_1, \dots, e_n)$ kanonická báze v P^n . Potom pro každé $i \in \{1, 2, \dots, n\}$ $f_A(e_i) = Ae_i = A_i^\circ$, čili obraz i -tého vektoru kanonické báze je i -tý sloupec matice A , A je tedy matice lineární transformace f_A vzhledem ke kanonické bázi, a obraz jednotkové krychle dané vrcholy $0, e_1, \dots, e_n$, jejíž objem je roven 1, je rovnoběžnostěn daný vrcholy $0, A_1^\circ, \dots, A_n^\circ$ o objemu $|\det A|$.

Volbou jiné báze dostaneme matici podobnou matici A se stejným determinanem.

Tvrzení 11.5.1. *Podobné matice mají stejné determinanty.*

Důkaz. Necht' A, B jsou podobné matice, tedy $B = Q^{-1}AQ$. Potom

$$\begin{aligned}\det B &= \det(Q^{-1}AQ) = \det Q^{-1} \cdot \det A \cdot \det Q = \\ &= \frac{1}{\det Q} \cdot \det A \cdot \det Q = \det A.\end{aligned}\quad \square$$

11.6. Algebraická struktura na množině lineárních zobrazení

Definice 11.6.1. Bud' U, V vektorové prostory nad polem P a $f, g: U \rightarrow V$ zobrazení.

- (1) Zobrazení $f + g: U \rightarrow V$, zadané předpisem

$$(f + g)(u) = f(u) + g(u)$$
 pro libovolný vektor $u \in U$, je *součet* zobrazení f a g .
- (2) Bud' $c \in P$. Zobrazení $cf: U \rightarrow V$, zadané předpisem

$$(cf)(u) = c \cdot f(u)$$
 pro libovolný vektor $u \in U$, je *c-násobek* zobrazení f .

Tvrzení 11.6.1. *Bud' U, V vektorové prostory nad polem P , $f, g: U \rightarrow V$ lineární zobrazení a $c \in P$. Pak zobrazení $f + g$, cf jsou lineární.*

Důkaz. Cvičení. $\square$

Bud' U, V vektorové prostory nad polem P . Množinu všech lineárních zobrazení z U do V označme $\text{Hom}_P(U, V)$. Tedy

$$\text{Hom}_P(U, V) = \{f: U \rightarrow V \mid f \text{ je lineární zobrazení nad polem } P\}.$$

Tvrzení 11.6.2. *Bud' U, V vektorové prostory nad polem P . Pak množina $\text{Hom}_P(U, V)$ s operacemi sčítání zobrazení a násobení zobrazení skalárem je vektorový prostor nad polem P .*

Důkaz. Cvičení. $\square$

Tvrzení 11.6.3. *Bud' U, V vektorové prostory nad polem P , $c \in P$, $f, g: U \rightarrow V$ lineární zobrazení a A, B jejich matice vzhledem ke zvoleným bázím. Pak*

- (1) $A + B$ je matice lineárního zobrazení $f + g$ vzhledem ke stejným bázím,
- (2) cA je matice lineárního zobrazení cf vzhledem ke stejným bázím.

Důkaz. Cvičení. $\square$

Tvrzení 11.6.4. *Bud' U, V konečněrozměrné vektorové prostory nad polem P , $\dim U = n$ a $\dim V = m$. Pak vektorový prostor $\text{Hom}_P(U, V)$ je izomorfní s prostorem $P^{m \times n}$ všech matic typu $m \times n$ nad polem P .*

Důkaz. Tvrzení dokážeme tak, že najdeme příslušný izomorfismus. Bud' u báze U , v báze V a $\varphi: \text{Hom}_P(U, V) \rightarrow P^{m \times n}$ zobrazení, které každému lineárnímu zobrazení $f: U \rightarrow V$ přiřadí jeho matici vzhledem k bázím u a v .

Potom φ je bijekce, protože každá matice typu $m \times n$ je maticí právě jednoho lineárního zobrazení $U \rightarrow V$ vzhledem k uvedeným bázím (ověřte podrobně). Navíc, podle předchozího tvrzení φ je lineární, protože matice zobrazení $f + g$ je součet matic jednotlivých zobrazení f a g a matice zobrazení cf je c -násobek matice zobrazení f . $\square$

Na množině $\text{Hom}_P(V, V)$ můžeme navíc uvažovat binární operaci o skládání lineárních transformací s neutrálním prvkem id_V (množina s asociativní binární operací s neutrálním prvkem je *monoid*).

Tvrzení 11.6.5. *Bud' V vektorový prostor nad polem P . Pak pro libovolná $f, g, h \in \text{Hom}_P(V, V)$ a $c \in P$ platí*

$$\begin{aligned} f \circ (g + h) &= f \circ g + f \circ h, \\ (f + g) \circ h &= f \circ h + g \circ h, \\ f \circ (cg) &= (cf) \circ g = c(f \circ g). \end{aligned}$$

Důkaz. Cvičení. □

Algebraická struktura, která je současně monoid i vektorový prostor nad polem P a platí pro ni identity uvedené v předchozím tvrzení, je *asociativní P -algebra*. Tudíž, $\text{Hom}_P(V, V)$ je asociativní P -algebra.

Jiný příklad asociativní P -algebry je množina $P^{n \times n} (= \text{gl}(n, P))$ všech čtvercových matic typu $n \times n$ nad polem P vzhledem k binárním operacím násobení a sčítání matic a k operaci násobení skalárem (ověřte).

Podle předchozích tvrzení v konečněrozměrném případě P -algebra $\text{Hom}_P(V, V)$ je izomorfní P -algebře $\text{gl}(n, P)$.

Pro libovolné celé nezáporné číslo k zavedme lineární transformaci $f^k: V \rightarrow V$ předpisem

$$f^k(v) = \underbrace{f(f(\cdots f(v)\cdots))}_k \text{ pro libovolné } v \in V, \text{ tj. } f^k = \underbrace{f \circ \cdots \circ f}_k.$$

Tedy, $f^0 = \text{id}_V$, $f^1 = f$, $f^2 = f \circ f$ a $f^{n+1} = f \circ f^n$.

Definice 11.6.2. Bud' $p = a_m x^m + \cdots + a_1 x + a_0 \in P[x]$ polynom. Bud' $f: V \rightarrow V$ lineární transformace vektorového prostoru V nad polem P a A čtvercová matice nad polem P . Položme

$$\begin{aligned} p(f) &= a_m f^m + \cdots + a_1 f + a_0 \text{id}_V, \\ p(A) &= a_m A^m + \cdots + a_1 A + a_0 E, \end{aligned}$$

kde E je jednotková matice stejného rozměru jako matice A .

Lineární transformace $p(f)$, resp. matice $p(A)$ vznikla *dosazením lineární transformace f , resp. matice A do polynomu p .*

Hodnota transformace $p(f)$ ve vektoru $v \in V$ se zapisuje $p(f)(v)$.

Příklad. Necht' $p = x^2 - 2x + 2$. Pak pro libovolnou lineární transformaci $f: V \rightarrow V$ máme $p(f) = f^2 - 2f + 2\text{id}$ a pro libovolný vektor $v \in V$ máme $p(f)(v) = f(f(v)) - 2f(v) + 2v$. □

Tvrzení 11.6.6. *Bud' p polynom a bud' A matice lineární transformace f vzhledem k nějaké bázi. Pak $p(A)$ je matice lineární transformace $p(f)$ vzhledem k téže bázi.*

Důkaz. Cvičení. □

Tvrzení 11.6.7. *Bud' p, q polynomy. Pro libovolnou lineární transformaci f a libovolnou čtvercovou matici A platí*

$$\begin{aligned} (p+q)(f) &= p(f) + q(f), & (pq)(f) &= p(f) \circ q(f), \\ (p+q)(A) &= p(A) + q(A), & (pq)(A) &= p(A)q(A). \end{aligned}$$

Důkaz. Cvičení. □

Důsledek. *Budťe p, q polynomy. Pro libovolnou lineární transformaci f a pro libovolnou čtvercovou matici A platí*

$$p(f) \circ q(f) = q(f) \circ p(f), \qquad p(A)q(A) = q(A)p(A)$$

(říkáme, že $p(f)$ a $q(f)$ komutují a $p(A)$ a $q(A)$ komutují).

12. VLASTNÍ VEKTORY

Mějme lineární transformaci $f: V \rightarrow V$ a její matici A vzhledem k nějaké bázi. Obraz vektoru v při lineární transformaci f^n můžeme najít pomocí toho, že spočteme jeho souřadnice, a to tak že souřadnice vektoru v vynásobíme maticí A^n , protože to je matice transformace f^n (vše samozřejmě vzhledem ke zvolené bázi). Je tedy žádoucí volit bázi prostoru tak, aby matice transformace byla co nejjednodušší, pokud možno diagonální, protože potom se její mocnina počítá velice jednoduše.

12.1. Definice, příklady

Při lineární transformaci $V \rightarrow V$ se každý vektor z prostoru V zobrazí na některý vektor opět z prostoru V . Může se tedy stát, že vektor se zobrazí na nějaký svůj skalární násobek.

Definice 12.1.1. Buď $f: V \rightarrow V$ lineární transformace vektorového prostoru V nad polem P . Skalár $\lambda \in P$ je *vlastní hodnota* (v případě číselného pole P *vlastní číslo*) transformace f , jestliže existuje nenulový vektor $v \in V$ takový, že

$$f(v) = \lambda v.$$

Je-li λ je vlastní hodnota transformace f , potom každý vektor $v \in V$ takový, že $f(v) = \lambda v$, je *vlastní vektor* transformace f příslušný vlastní hodnotě λ .

Analogicky jsou definovány vlastní vektory a vlastní hodnoty (čísla) čtvercové matice.

Definice 12.1.2. Buď A čtvercová matice řádu n nad polem P . Skalár $\lambda \in P$ je *vlastní hodnota* (*vlastní číslo*) matice A , jestliže existuje nenulový vektor (uspořádaná n -tice, sloupcová matice) $x \in P^n$ takový, že

$$Ax = \lambda x.$$

Je-li λ je vlastní hodnota matice A , potom každý vektor $x \in P^n$ takový, že $Ax = \lambda x$, je *vlastní vektor* matice A příslušný vlastní hodnotě λ .

Tedy, aby skalár λ byl vlastní hodnotou lineární transformace nebo čtvercové matice, musí existovat nenulový vektor, který se zobrazí tou lineární transformací, resp. čtvercovou maticí na svůj λ -násobek. V takovém případě i nulový vektor je vlastní vektor příslušný vlastní hodnotě λ .

Příklad. (1) Je-li V netriviální prostor (obsahuje nenulový vektor), pak pro identickou transformaci $\text{id}: V \rightarrow V$, $\text{id}(v) = v$, každý vektor $v \in V$ je vlastní s vlastní hodnotou 1, protože $\text{id}(v) = 1 \cdot v$.

(2) Je-li V netriviální prostor, pak pro nulovou transformaci $0: V \rightarrow V$, $0(v) = 0$, každý vektor $v \in V$ je vlastní s vlastní hodnotou 0, protože $0(v) = 0 \cdot v$.

(3) Je-li V netriviální prostor a c skalár, pak pro transformaci $f_c: V \rightarrow V$, $f_c(v) = cv$, každý vektor $v \in V$ je vlastní s vlastní hodnotou c .

(4) Pro rovnoběžné promítání $E^3 \rightarrow E^3$ podél vektoru $v \neq 0$ na rovinu $U \subset E^3$ procházející počátkem, kde $v \notin U$, vektor v a všechny jeho násobky jsou vlastní vektory s vlastním číslem 0, každý vektor $z \in U$ je vlastní vektor s vlastním číslem 1 a jiné vlastní vektory tato transformace nemá.

(5) Pro rotaci $E^2 \rightarrow E^2$ o úhel $0 \leq \varphi < 2\pi$:

(a) je-li $\varphi = 0$, pak jde o identickou transformaci a každý vektor je vlastní s vlastním číslem 1;

(b) je-li $\varphi = \pi$, pak jde o středovou symetrii $v \mapsto -v = (-1)v$ a každý vektor je vlastní s vlastním číslem -1 ;

(c) v ostatních případech neexistuje žádný vlastní vektor.

(6) Rotace $E^3 \rightarrow E^3$ o úhel $0 < \varphi < 2\pi$ kolem zvolené pevné osy L procházející počátkem. Označme $L^\perp$ rovinu procházející počátkem kolmo k L (tzv. ortogonální doplněk).

(a) Je-li $\varphi = 0$, pak jde o identickou transformaci a každý vektor je vlastní s vlastním číslem 1 ;

(b) je-li $\varphi = \pi$, pak každý vektor z L je vlastní s vlastním číslem 1 , každý vektor z $L^\perp$ je vlastní s vlastním číslem -1 a žádný jiný vlastní vektor tato transformace nemá;

(c) v ostatních případech každý vektor z L je vlastní vektor s vlastním číslem 1 a žádný jiný vlastní vektor neexistuje.

(7) Buď V vektorový prostor všech hladkých funkcí $\mathbb{R} \rightarrow \mathbb{R}$ (mají spojitě derivace všech řádů) a buď $\delta: V \rightarrow V$, $\delta(f) = f'$ transformace, která funkci f přiřadí její derivaci f' . Z matematické analýzy víme, že pro libovolné $\lambda \in \mathbb{R}$ platí $(e^{\lambda x})' = \lambda e^{\lambda x}$, čili funkce $e^{\lambda x}$ a každý její skalární násobek jsou vlastní vektory transformace δ s vlastním číslem λ .

Buď $f \in V$ libovolná funkce s vlastností $f' = \lambda f$. Potom

$$(f(x)e^{-\lambda x})' = \lambda f(x)e^{-\lambda x} - f(x)\lambda e^{-\lambda x} = 0,$$

čili funkce $f(x)e^{-\lambda x}$ je konstantní. Označíme-li $f(x)e^{-\lambda x} = c$, dostaneme $f(x) = ce^{\lambda x}$, takže každá funkce s vlastností $f' = \lambda f$ je skalární násobek funkce $e^{\lambda x}$. To znamená, že každé reálné číslo λ je vlastní číslo transformace δ a příslušné vlastní vektory jsou všechny skalární násobky funkce $e^{\lambda x}$. $\square$

Cvičení. Určete všechny vlastní vektory následujících lineárních transformací vektorového prostoru $\mathbb{C}$ nad $\mathbb{R}$. Návod: Pomozte si geometrickou interpretací v Gaussově rovině.

(1) Zobrazení $\mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto \bar{z}$, kde $\bar{z}$ je číslo komplexně sdružené k číslu z .

(2) Zobrazení $\text{re}: \mathbb{C} \rightarrow \mathbb{R}$, $z \mapsto \text{re } z = \frac{1}{2}(z + \bar{z})$ (reálná část čísla z). $\square$

12.2. Výpočet vlastních čísel a vlastních vektorů

Tvrzení 12.2.1. Buď $f: V \rightarrow V$ lineární transformace. Potom

- (1) skalár λ je vlastní hodnota transformace f právě tehdy, když $f - \lambda \text{id}_V$ není injektivní;
- (2) množina všech vlastních vektorů příslušných vlastní hodnotě λ transformace f je $\text{Ker}(f - \lambda \text{id}_V)$, tedy podprostor prostoru V .

Důkaz. Buďte $v \in V$ a λ skalár. Následující vztahy jsou ekvivalentní:

$$f(v) = \lambda v$$

$$f(v) - \lambda v = 0$$

$$f(v) - (\lambda \text{id}_V)(v) = 0$$

$$(f - \lambda \text{id}_V)(v) = 0$$

$$v \in \text{Ker}(f - \lambda \text{id}_V)$$

Takže λ je vlastní hodnota právě tehdy, když v $\text{Ker}(f - \lambda \text{id}_V)$ existuje nenulový vektor, což podle Tvrzení 11.2.2 je právě tehdy, když $f - \lambda \text{id}_V$ není injektivní.

Z uvedeného navíc vyplývá, že množina všech vlastních vektorů příslušných vlastní hodnotě λ transformace f je $\text{Ker}(f - \lambda \text{id}_V)$, což je podprostor prostoru V . $\square$

Obdobné tvrzení platí i pro vlastní hodnoty a vlastní vektory matice.

Tvrzení 12.2.2. Buď A matice typu $n \times n$ nad polem P . Potom

- (1) skalár λ je vlastní hodnota matice A právě tehdy, když $\det(A - \lambda E_n) = 0$;
 (2) množina všech vlastních vektorů příslušných vlastní hodnotě λ matice A je podprostor prostoru P^n .

Důkaz. Buďte $x \in P^n$ a λ skalár. Následující vztahy jsou ekvivalentní:

$$\begin{aligned} Ax &= \lambda x \\ Ax - \lambda x &= 0 \\ Ax - \lambda E_n x &= 0 \\ (A - \lambda E_n)x &= 0 \\ x &\in \text{Ker}(A - \lambda E_n) \end{aligned}$$

Takže λ je vlastní hodnota právě tehdy, když v $\text{Ker}(A - \lambda E_n)$ existuje nenulový vektor, tedy homogenní soustava $(A - \lambda E_n)x = 0$ má nenulové řešení, a to má právě tehdy, když matice $A - \lambda E_n$ je singulární, čili $\det(A - \lambda E_n) = 0$.

Z uvedeného navíc vyplývá, že množina všech vlastních vektorů příslušných vlastní hodnotě λ matice A je množina všech řešení homogenní soustavy rovnic o n neznámých, což je podprostor prostoru P^n . $\square$

Definice 12.2.1. Nechť f (resp. A) je lineární transformace konečněrozměrného vektorového prostoru (resp. čtvercová matice) a λ je její vlastní hodnota. *Geometrická násobnost* vlastní hodnoty λ je dimenze podprostoru vlastních vektorů transformace f (resp. matice A) příslušných vlastní hodnotě λ .

Tvrzení 12.2.3. *Vlastní hodnoty trojúhelníkové matice jsou prvky na diagonále matice.*

Důkaz. Cvičení. $\square$

Tvrzení 12.2.4. *Buď A matice typu $n \times n$ nad polem P . Potom $\det(A - \lambda E_n)$ je polynom neurčitě λ stupně n s koeficienty z pole P .*

Důkaz. Cvičení. $\square$

Definice 12.2.2. Buď A čtvercová matice. Polynom

$$\chi_A = \det(A - \lambda E)$$

je *charakteristický polynom* matice A a rovnice

$$\det(A - \lambda E) = 0$$

je *charakteristická rovnice* matice A .

Cvičení. Buď $\chi_A = c_n \lambda^n + c_{n-1} \lambda^{n-1} + \dots + c_0$ charakteristický polynom matice A typu $n \times n$. Ukažte, že $c_n = (-1)^n$, $c_{n-1} = (-1)^{n-1} \text{tr } A$ a $c_0 = \det A$. $\square$

Podle Tvrzení 12.2.2 je λ vlastní hodnota matice A právě tehdy, když je kořenem příslušného charakteristického polynomu. Vlastní vektory příslušné vlastní hodnotě λ získáme jako řešení soustavy lineárních rovnic $(A - \lambda E)x = 0$.

Tvrzení 12.2.5. *Matice typu $n \times n$ má nejvýše n vlastních hodnot.*

Důkaz. Vlastní hodnoty jsou kořeny polynomu stupně n a polynom stupně n má nejvýše n kořenů. $\square$

Tvrzení 12.2.6. *Buďte V konečněrozměrný vektorový prostor nad polem P , $f: V \rightarrow V$ lineární transformace a A matice transformace f vzhledem k nějaké bázi prostoru V . Potom $\lambda \in P$ je vlastní hodnota transformace f právě tehdy, když λ je vlastní hodnota matice A .*

Důkaz. Tvzení vyplývá z toho, že vektorům z V jsou jednoznačně přiřazeny jejich souřadnice (zobrazení přiřazující vektorům jejich souřadnice je izomorfismus), transformace f je určena svou maticí A a souřadnice obrazu $f(v)$ vektoru v o souřadnicích x jsou rovny součinu matic Ax , vše vzhledem k jedné bázi. $\square$

Vlastní hodnoty lineární transformace f tedy získáváme jako vlastní hodnoty matice A transformace f vzhledem k nějaké bázi, tedy jako kořeny charakteristického polynomu matice A . Při volbě jiné báze dostaneme jinou matici A' transformace f , jejíž vztah k A je $A' = QAQ^{-1}$, kde Q je matice přechodu mezi bázemi. Je otázkou, zda matice A a A' mají stejné charakteristické polynomy a tedy stejné vlastní hodnoty.

Tvrzení 12.2.7. *Podobné matice mají stejné charakteristické polynomy.*

Důkaz. Necht A, B jsou podobné matice, tedy $B = Q^{-1}AQ$. Potom

$$\begin{aligned}\chi_B &= \det(B - \lambda E) = \det(Q^{-1}AQ - \lambda E) = \det(Q^{-1}AQ - Q^{-1}\lambda EQ) = \\ &= \det(Q^{-1}(A - \lambda E)Q) = \det Q^{-1} \cdot \det(A - \lambda E) \cdot \det Q = \\ &= \frac{1}{\det Q} \cdot \det(A - \lambda E) \cdot \det Q = \det(A - \lambda E) = \chi_A.\end{aligned}\quad \square$$

Díky předchozímu tvrzení můžeme pomocí charakteristického polynomu matice definovat charakteristický polynom lineární transformace konečněrozměrného prostoru.

Definice 12.2.3. Buď $f: V \rightarrow V$ lineární transformace konečněrozměrného vektorového prostoru V . *Charakteristický polynom* χ_f transformace f je roven charakteristickému polynomu χ_A matice A transformace f vzhledem k libovolné bázi.

Díky Tvrzení 12.2.7 je předchozí definice korektní a kořeny charakteristického polynomu transformace f jsou všechny vlastní hodnoty transformace f .

Tvrzení 12.2.8. *Lineární transformace n -rozměrného vektorového prostoru má nejvýše n vlastních hodnot.*

Důkaz. Charakteristický polynom je stupně n a má tedy nejvýše n kořenů. $\square$

Definice 12.2.4. Necht f (resp. A) je lineární transformace konečněrozměrného vektorového prostoru (resp. čtvercová matice) a λ je její vlastní hodnota. *Algebraická násobnost* vlastní hodnoty λ je její násobnost jako kořene charakteristického polynomu transformace f (resp. matice A).

Tvrzení 12.2.9. *Geometrická násobnost vlastní hodnoty je menší nebo rovna její algebraické násobnosti.*

Důkaz. Buď $f: V \rightarrow V$ lineární transformace n -rozměrného vektorového prostoru V nad polem P a λ_0 její vlastní hodnota s geometrickou násobností k . Buď $(v_1, \dots, v_k)$ báze podprostoru vlastních vektorů transformace f příslušných vlastní hodnotě λ_0 . Doplňme ji na bázi $(v_1, \dots, v_k, v_{k+1}, \dots, v_n)$ prostoru V . Jelikož vektory $v_1, \dots, v_k$ jsou vlastní vektory s vlastní hodnotou λ_0 , tedy $f(v_i) = \lambda_0 v_i$ pro každé $i \in \{1, \dots, k\}$, matice

transformace f vzhledem k bázi $(v_1, \dots, v_k, v_{k+1}, \dots, v_n)$ je blokově diagonální matice

$$A = \begin{pmatrix} \lambda_0 & 0 & \dots & 0 & A_{k+1}^1 & \dots & A_n^1 \\ 0 & \lambda_0 & \dots & 0 & A_{k+1}^2 & \dots & A_n^2 \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \lambda_0 & A_{k+1}^k & \dots & A_n^k \\ 0 & 0 & \dots & 0 & A_{k+1}^{k+1} & \dots & A_n^{k+1} \\ 0 & 0 & \dots & 0 & A_{k+1}^{k+2} & \dots & A_n^{k+2} \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & A_{k+1}^n & \dots & A_n^n \end{pmatrix}$$

a charakteristický polynom transformace f je $\chi_f = \chi_A = \det(A - \lambda E)$, tedy

$$\begin{aligned} \chi_f &= \begin{vmatrix} \lambda_0 - \lambda & 0 & \dots & 0 & A_{k+1}^1 & \dots & A_n^1 \\ 0 & \lambda_0 - \lambda & \dots & 0 & A_{k+1}^2 & \dots & A_n^2 \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \lambda_0 - \lambda & A_{k+1}^k & \dots & A_n^k \\ 0 & 0 & \dots & 0 & A_{k+1}^{k+1} - \lambda & \dots & A_n^{k+1} \\ 0 & 0 & \dots & 0 & A_{k+1}^{k+2} & \dots & A_n^{k+2} \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & A_{k+1}^n & \dots & A_n^n - \lambda \end{vmatrix} = \\ &= (\lambda_0 - \lambda)^k \cdot \begin{vmatrix} A_{k+1}^{k+1} - \lambda & \dots & A_n^{k+1} \\ A_{k+1}^{k+2} & \dots & A_n^{k+2} \\ \vdots & & \vdots \\ A_{k+1}^n & \dots & A_n^n - \lambda \end{vmatrix}. \end{aligned}$$

To znamená, že λ_0 je kořen polynomu χ_f s násobností aspoň k , takže algebraická násobnost vlastní hodnoty λ_0 je větší nebo rovna její geometrické násobnosti. $\square$

12.3. Diagonalizovatelné transformace

Definice 12.3.1. Lineární transformace konečněrozměrného prostoru je *diagonalizovatelná*, jestliže její matice vzhledem k nějaké bázi je diagonální.

Tvrzení 12.3.1. Buď $f: V \rightarrow V$ lineární transformace konečněrozměrného vektorového prostoru V , $(v_1, \dots, v_n)$ báze prostoru V a A matice transformace f vzhledem k uvedené bázi. Potom

$$A = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

právě tehdy, když $\lambda_1, \dots, \lambda_n$ jsou vlastní hodnoty transformace f a pro každé $i \in \{1, \dots, n\}$ vektor v_i je vlastní vektor příslušný vlastní hodnotě λ_i .

Důkaz. Cvičení. $\square$

Důsledek. Lineární transformace konečněrozměrného prostoru je diagonalizovatelná právě tehdy, když existuje báze prostoru tvořená vlastními vektory transformace.

Definice 12.3.2. Matice je *diagonalizovatelná*, jestliže je podobná diagonální matici.

Tvrzení 12.3.2. Matice A typu $n \times n$ nad polem P je diagonalizovatelná právě tehdy, když existuje báze prostoru P^n tvořená vlastními vektory matice A .

Důkaz. Cvičení. □

Tvrzení 12.3.3. Lineární transformace konečněrozměrného vektorového prostoru je diagonalizovatelná právě tehdy, když její matice vzhledem k libovolné bázi je diagonalizovatelná.

Důkaz. Buď $f: V \rightarrow V$ lineární transformace konečněrozměrného vektorového prostoru V , $(v_1, \dots, v_n)$ báze prostoru V a A matice transformace f vzhledem k uvedené bázi.

Předpokládejme, že transformace f je diagonalizovatelná, tedy že vzhledem k nějaké bázi má diagonální matici B . Potom B je podobná A , tedy A je diagonalizovatelná.

Předpokládejme, že A je diagonalizovatelná, čili je podobná diagonální matici B a existuje tedy regulární matice Q taková, že $B = QAQ^{-1}$. Potom vektory z V , jejichž souřadnice vzhledem k bázi $(v_1, \dots, v_n)$ jsou právě sloupky matice Q , tvoří bázi prostoru V , vzhledem k níž je matice transformace f právě diagonální matice B . Tedy, f je diagonalizovatelná transformace. □

Tvrzení 12.3.4. Buďte $v_1, \dots, v_n$ nenulové vlastní vektory jedné lineární transformace příslušné po řadě různým vlastním hodnotám $\lambda_1, \dots, \lambda_n$. Potom $\{v_1, \dots, v_n\}$ je lineárně nezávislá množina.

Důkaz. Buďte $f: V \rightarrow V$ lineární transformace a $v_1, \dots, v_n$ její nenulové vlastní vektory příslušné po řadě různým vlastním hodnotám $\lambda_1, \dots, \lambda_n$. Tvrzení dokážeme matematickou indukcí podle n . Pro $n = 1$ tvrzení platí, protože $v_1 \neq 0$. Buď $n > 1$ a předpokládejme, že tvrzení platí pro $n - 1$, tedy že množina $\{v_1, \dots, v_{n-1}\}$ je lineárně nezávislá. Buďte $x^1, \dots, x^{n-1}, x^n$ skaláry takové, že

$$x^1 v_1 + \dots + x^{n-1} v_{n-1} + x^n v_n = 0. \quad (11)$$

Zobrazíme-li obě strany v (11) lineární transformací $f - \lambda_n \text{id}_V$, s využitím toho, že $f(v_i) = \lambda_i v_i$, dostaneme

$$\begin{aligned} (f - \lambda_n \text{id}_V)(x^1 v_1 + \dots + x^{n-1} v_{n-1} + x^n v_n) &= \\ &= x^1 (f - \lambda_n \text{id}_V)(v_1) + \dots + x^{n-1} (f - \lambda_n \text{id}_V)(v_{n-1}) + x^n (f - \lambda_n \text{id}_V)(v_n) = \\ &= x^1 (\lambda_1 - \lambda_n) v_1 + \dots + x^{n-1} (\lambda_{n-1} - \lambda_n) v_{n-1} + x^n (\lambda_n - \lambda_n) v_n = \\ &= x^1 (\lambda_1 - \lambda_n) v_1 + \dots + x^{n-1} (\lambda_{n-1} - \lambda_n) v_{n-1} = 0 = (f - \lambda_n \text{id}_V)(0). \end{aligned}$$

Podle indukčního předpokladu množina $\{v_1, \dots, v_{n-1}\}$ je lineárně nezávislá, takže

$$x^1 (\lambda_1 - \lambda_n) = \dots = x^{n-1} (\lambda_{n-1} - \lambda_n) = 0.$$

Jelikož vlastní hodnoty $\lambda_1, \dots, \lambda_n$ jsou navzájem různé, tedy $\lambda_i - \lambda_n \neq 0$ pro všechna $i \in \{1, \dots, n-1\}$, dostáváme

$$x^1 = \dots = x^{n-1} = 0.$$

Po dosazení do (11) dostaneme $x^n v_n = 0$ a tedy také $x^n = 0$, protože v_n je nenulový vektor. Takže množina $\{v_1, \dots, v_n\}$ je lineárně nezávislá. □

Důsledek. Má-li lineární transformace n -rozměrného prostoru n vlastních hodnot, je diagonalizovatelná.

Důkaz. Jsou-li $\lambda_1, \dots, \lambda_n$ navzájem různé vlastní hodnoty transformace $f: V \rightarrow V$, potom pro každé $i \in \{1, \dots, n\}$ existuje nenulový vlastní vektor v_i příslušný λ_i . Množina $\{v_1, \dots, v_n\}$ je lineárně nezávislá a tvoří tedy bázi prostoru V . Matice transformace f vzhledem k bázi tvořené vlastními vektory je diagonální, takže f je diagonalizovatelná transformace. □

Důsledek. Má-li matice typu $n \times n$ n vlastních hodnot, je diagonalizovatelná.

Příklad. Mějme $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $f(x^1, x^2) = (2x^1 + x^2, 3x^1 + 4x^2)$ (ověřte, že f je lineární) a na $\mathbb{R}^2$ uvažujme kanonickou bázi.

Matici zobrazení získáme tak, že do sloupků budeme psát souřadnice obrazů vektorů báze (v tomto případě souřadnice jsou stejné jako vektory).

Obrazy báze jsou $f(1, 0) = (2, 3)$, $f(0, 1) = (1, 4)$, takže matice zobrazení f je

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

Charakteristický polynom je

$$\begin{vmatrix} 2 - \lambda & 1 \\ 3 & 4 - \lambda \end{vmatrix} = (\lambda - 1)(\lambda - 5)$$

a jeho kořeny, tedy vlastní čísla jsou $\lambda_1 = 1$, $\lambda_2 = 5$, obě s algebraickou násobností 1.

Podle předchozích tvrzení je matice A podobná matici

$$A' = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix},$$

tedy diagonalizovatelná.

Vlastní vektory získáme jako řešení soustavy lineárních rovnic $(A - \lambda E)x = 0$ pro jednotlivé vlastní hodnoty.

Pro $\lambda_1 = 1$ řešíme soustavu

$$\begin{pmatrix} 1 & 1 \\ 3 & 3 \end{pmatrix} \cdot \begin{pmatrix} x^1 \\ x^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{tedy} \quad \begin{matrix} 1x^1 + 1x^2 = 0 \\ 3x^1 + 3x^2 = 0 \end{matrix}.$$

Množina všech řešení této soustavy je $\llbracket(1, -1)\rrbracket$ a příslušné vlastní vektory jsou tedy všechny skalární násobky vektoru $v_1 = (1, -1)$. Vektor v_1 se skutečně zobrazí na svůj 1-násobek, $f(1, -1) = (1, -1)$. Geometrická násobnost vlastního čísla $\lambda_1 = 1$ je tedy 1, stejná jako jeho algebraická násobnost.

Pro $\lambda_2 = 5$ řešíme soustavu

$$\begin{pmatrix} -3 & 1 \\ 3 & -1 \end{pmatrix} \cdot \begin{pmatrix} x^1 \\ x^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{tedy} \quad \begin{matrix} -3x^1 + 1x^2 = 0 \\ 3x^1 - 1x^2 = 0 \end{matrix}.$$

Množina všech řešení této soustavy je $\llbracket(1, 3)\rrbracket$ a příslušné vlastní vektory jsou tedy všechny skalární násobky vektoru $v_2 = (1, 3)$. Vektor v_2 se skutečně zobrazí na svůj 5-násobek, $f(1, 3) = (5, 15)$. Geometrická násobnost vlastního čísla $\lambda_2 = 5$ je tedy také 1, také stejná jako jeho algebraická násobnost.

Součet algebraických násobností, stejně jako součet geometrických násobností vlastních čísel $\lambda_1 = 1$ a $\lambda_2 = 5$ je roven 2, tedy dimenzi prostoru $\mathbb{R}^2$.

Podle Tvrzení 12.3.4 vektory v_1, v_2 tvoří „novou“ bázi prostoru $\mathbb{R}^2$.

Matice přechodu Q od kanonické báze k nové bázi (ve sloupcích jsou nové souřadnice vektorů kanonické báze) a matice k ní inverzní Q^{-1} , tedy matice přechodu od nové báze ke kanonické bázi (ve sloupcích jsou kanonické souřadnice vektorů nové báze) jsou

$$Q = \begin{pmatrix} 3/4 & -1/4 \\ 1/4 & 1/4 \end{pmatrix} \quad \text{a} \quad Q^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}.$$

A skutečně

$$A' = Q \cdot A \cdot Q^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}.$$

Poznámka. Při hledání vlastních vektorů tedy hledáme jádra lineárních transformací $f - \lambda \cdot \text{id}$ pro jednotlivé hodnoty λ .

Pro $\lambda_1 = 1$ je $(f - \text{id})(x^1, x^2) = (x^1 + x^2, 3x^1 + 3x^2)$ a jádro tohoto zobrazení je

$$\text{Ker}(f - \text{id}) = \llbracket (1, -1) \rrbracket.$$

Pro $\lambda_2 = 5$ je $(f - 5 \text{id})(x^1, x^2) = (-3x^1 + x^2, 3x^1 - x^2)$ a jádro tohoto zobrazení je

$$\text{Ker}(f - 5 \text{id}) = \llbracket (1, 3) \rrbracket. \quad \square$$

Příklad. Mějme $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $f(x^1, x^2) = (2x^1, 2x^2)$ (ověřte, že f je lineární) a na $\mathbb{R}^2$ uvažujme kanonickou bázi.

Matici zobrazení získáme tak, že do sloupků budeme psát souřadnice obrazů vektorů báze (v tomto případě souřadnice jsou stejné jako vektory).

Obrazy báze jsou $f(1, 0) = (2, 0)$, $f(0, 1) = (0, 2)$, takže matice zobrazení f je

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

Matice A je diagonální, matice transformace f vzhledem k libovolné bázi je rovna matici A , čili diagonalizovatelná.

Charakteristický polynom je

$$\begin{vmatrix} 2 - \lambda & 0 \\ 0 & 2 - \lambda \end{vmatrix} = (2 - \lambda)^2,$$

$\lambda = 2$ je jeho dvojnásobný kořen, tedy jediné vlastní číslo, a jeho algebraická násobnost je 2, stejná jako dimenze prostoru $\mathbb{R}^2$.

Vlastní vektory, přesněji jejich souřadnice, které jsou však v tomto případě stejné jako vektory, získáme jako řešení soustavy lineárních rovnic $(A - 2E)x = 0$.

Řešíme soustavu

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x^1 \\ x^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{tedy} \quad \begin{matrix} 0x^1 + 0x^2 = 0 \\ 0x^1 + 0x^2 = 0 \end{matrix}.$$

Množina všech řešení této soustavy je $\llbracket (1, 0), (0, 1) \rrbracket = \mathbb{R}^2$, příslušné vlastní vektory jsou tedy všechny prvky $\mathbb{R}^2$ a každá lineárně nezávislá dvojice vlastních vektorů tvoří bázi $\mathbb{R}^2$. Geometrická násobnost vlastního čísla $\lambda = 2$ je tedy 2, stejná jako jeho algebraická násobnost, stejná jako dimenze prostoru $\mathbb{R}^2$.

Prostor příslušných vlastních vektorů je v tomto případě jádro nulové lineární transformace $f - 2 \cdot \text{id}$, $(f - 2 \cdot \text{id})(x^1, x^2) = (0, 0)$, tedy

$$\text{Ker}(f - 2 \cdot \text{id}) = \llbracket (1, 0), (0, 1) \rrbracket. \quad \square$$

Příklad. Mějme $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $f(x^1, x^2) = (2x^1 + x^2, 2x^2)$ (ověřte, že f je lineární) a na $\mathbb{R}^2$ uvažujme kanonickou bázi.

Matici zobrazení získáme tak, že do sloupků budeme psát souřadnice obrazů vektorů báze (v tomto případě souřadnice jsou stejné jako vektory).

Obrazy báze jsou $f(1, 0) = (2, 0)$, $f(0, 1) = (1, 2)$, takže matice zobrazení f je

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

Charakteristický polynom je

$$\begin{vmatrix} 2 - \lambda & 1 \\ 0 & 2 - \lambda \end{vmatrix} = (\lambda - 2)^2,$$

$\lambda = 2$ je jeho dvojnásobný kořen, tedy jediné vlastní číslo, a jeho algebraická násobnost je 2, stejná jako dimenze prostoru $\mathbb{R}^2$.

Vlastní vektory, přesněji jejich souřadnice, které jsou však v tomto případě stejné jako vektory, získáme jako řešení soustavy lineárních rovnic $(A - 2E)x = 0$.

Řešíme soustavu

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x^1 \\ x^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{tedy} \quad \begin{matrix} 0x^1 + 1x^2 = 0 \\ 0x^1 + 0x^2 = 0 \end{matrix}.$$

Množina všech řešení této soustavy je $\llbracket(1, 0)\rrbracket$ a příslušné vlastní vektory jsou tedy všechny skalární násobky vektoru $v = (1, 0)$. Vektor v se skutečně zobrazí na svůj 2-násobek, $f(1, 0) = (2, 0)$. Geometrická násobnost vlastního čísla $\lambda = 2$ je tedy 1, je menší než jeho algebraická násobnost a dimenze prostoru $\mathbb{R}^2$.

Jinak formulováno, opět, při hledání vlastních vektorů tedy hledáme jádro lineární transformace $f - 2 \cdot \text{id}$, $(f - 2 \cdot \text{id})(x^1, x^2) = (x^2, 0)$ a to je

$$\text{Ker}(f - 2 \cdot \text{id}) = \llbracket(1, 0)\rrbracket.$$

Z vlastních vektorů tedy nelze sestavit bázi prostoru $\mathbb{R}^2$ a podle Důsledku Tvzení 12.3.1 transformace f není diagonalizovatelná. $\square$

Příklad. Mějme $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $f(x^1, x^2, x^3) = (-x^2, x^1, x^3)$ (ověřte, že f je lineární) a na $\mathbb{R}^3$ uvažujme kanonickou bázi.

Matici zobrazení získáme tak, že do sloupků budeme psát souřadnice obrazů vektorů báze (v tomto případě souřadnice jsou stejné jako vektory).

Obrazy báze jsou $f(1, 0, 0) = (0, 1, 0)$, $f(0, 1, 0) = (-1, 0, 0)$, $f(0, 0, 1) = (0, 0, 1)$, takže matice zobrazení f je

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

Charakteristický polynom je

$$\begin{vmatrix} -\lambda & -1 & 0 \\ 1 & -\lambda & 0 \\ 0 & 0 & 1 - \lambda \end{vmatrix} = (\lambda^2 + 1)(1 - \lambda),$$

$\lambda = 1$ je jeho jediný reálný kořen, tedy jediné vlastní číslo, a jeho algebraická násobnost je 1, menší než dimenze prostoru $\mathbb{R}^3$.

Vlastní vektory, přesněji jejich souřadnice, které jsou však v tomto případě stejné jako vektory, získáme jako řešení soustavy lineárních rovnic $(A - E)x = 0$.

Řešíme soustavu

$$\begin{pmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x^1 \\ x^2 \\ x^3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{tedy} \quad \begin{matrix} -x^1 - x^2 + 0x^3 = 0 \\ x^1 - x^2 + 0x^3 = 0 \\ 0x^1 + 0x^2 + 0x^3 = 0 \end{matrix}.$$

Množina všech řešení této soustavy je $\llbracket(0, 0, 1)\rrbracket$ a příslušné vlastní vektory jsou tedy všechny skalární násobky vektoru $v = (0, 0, 1)$. Vektor v se skutečně zobrazí na svůj 1-násobek, $f(0, 0, 1) = (0, 0, 1)$. Geometrická násobnost vlastního čísla $\lambda = 1$ je tedy 1, je stejná jako jeho algebraická násobnost, ale menší než dimenze prostoru $\mathbb{R}^3$.

Prostor příslušných vlastních vektorů je v tomto případě jádro lineární transformace $f - \text{id}$, $(f - \text{id})(x^1, x^2, x^3) = (-x^2 - x^1, x^1 - x^2, 0)$ a to je

$$\text{Ker}(f - \text{id}) = \llbracket(0, 0, 1)\rrbracket.$$

Z vlastních vektorů tedy nelze sestavit bázi prostoru $\mathbb{R}^3$ a podle Důsledku Tvzení 12.3.1 transformace f není diagonalizovatelná. $\square$

Tvrzení 12.3.5. *Lineární transformace f n -rozměrného vektorového prostoru (resp. matice A typu $n \times n$) je diagonalizovatelná právě tehdy, když součet algebraických násobností jejích vlastních hodnot je n a geometrická násobnost každé vlastní hodnoty je rovna její algebraické násobnosti.*

Důkaz.

□

13. JORDANŮV KANONICKÝ TVAR

Úmluva. V této kapitole V je vektorový prostor (obvykle konečněrozměrný) nad polem P a $f: V \rightarrow V$ je lineární transformace.

13.1. První rozklad lineární transformace

13.1.1. Anulující polynom a minimální polynom

Definice 13.1.1. Nechť $p \in P[x]$, $p \neq 0$. Polynom p je *anulující polynom* čtvercové matice A (resp. lineární transformace f), jestliže $p(A) = 0$ (resp. $p(f) = 0$).

Tvrzení 13.1.1 (Cayleyho-Hamiltonova věta). *Charakteristický polynom matice je její anulující polynom.*

Důkaz. Podle Tvrzení 2.3.1 pro libovolnou čtvercovou matici B platí $B \cdot \text{adj } B = \det B \cdot E$. Tedy, i pro matici $A - xE$

$$(A - xE) \cdot \text{adj}(A - xE) = \det(A - xE) \cdot E = \chi_A \cdot E. \quad (12)$$

Je-li matice A typu $n \times n$, pak její charakteristický polynom χ_A je polynom stupně n , označme

$$\chi_A = c_n x^n + \cdots + c_1 x + c_0.$$

Podle Definice 2.3.1 prvky v adjungované matici $\text{adj}(A - xE)$ jsou polynomy neurčité x stupně nejvýše $n - 1$. Takže, matici $\text{adj}(A - xE)$ můžeme vyjádřit

$$\text{adj}(A - xE) = C_{n-1}x^{n-1} + \cdots + C_1x + C_0,$$

kde C_i jsou čtvercové matice typu $n \times n$.

Po dosazení do (12) máme

$$(A - xE) \cdot (C_{n-1}x^{n-1} + \cdots + C_1x + C_0) = (c_n x^n + \cdots + c_1 x + c_0) \cdot E,$$

tj.

$$\begin{aligned} & -C_{n-1}x^n + (AC_{n-1} - C_{n-2})x^{n-1} + \cdots + (AC_1 - C_0)x + AC_0 = \\ & = c_n E x^n + \cdots + c_1 E x + c_0 E. \end{aligned}$$

Porovnáním koeficientů u stejných mocnin x obdržíme $n + 1$ rovností

$$\begin{aligned} -C_{n-1} &= c_n E, \\ AC_{n-1} - C_{n-2} &= c_{n-1} E, \\ &\vdots \\ AC_1 - C_0 &= c_1 E, \\ AC_0 &= c_0 E. \end{aligned}$$

Jestliže pro každé $i \in \{1, \dots, n + 1\}$ i -tou rovnost vynásobíme zleva $(n + 1 - i)$ -tou mocninou A^{n+1-i} matice A , dostaneme

$$\begin{aligned} -A^n C_{n-1} &= c_n A^n, \\ A^n C_{n-1} - A^{n-1} C_{n-2} &= c_{n-1} A^{n-1}, \\ &\vdots \\ A^2 C_1 - A C_0 &= c_1 A, \\ AC_0 &= c_0 E. \end{aligned}$$

Když tyto rovnosti sečteme, dostaneme

$$0 = c_n A^n + c_{n-1} A^{n-1} + \cdots + c_1 A + c_0 E,$$

což se mělo dokázat. $\square$

Důsledek. *Charakteristický polynom lineární transformace je její anulující polynom.*

Příklad. Matice

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

má charakteristický polynom $\chi_A = x^3 - x^2 - x + 1 = (x+1)(x-1)^2$, ale $q = x^2 - 1 = (x+1)(x-1)$ je také anulující polynom matice A (ověřte). $\square$

Poslední příklad ukazuje, že charakteristický polynom může mít netriviálního dělitele, který je rovněž anulujícím polynomem. Ukažme, že mezi anulujícími polynomy existuje jeden, který dělí všechny ostatní.

Definice 13.1.2. Anulující polynom je *minimální polynom*, je-li normovaný a nejmenšího stupně ze všech anulujících polynomů.

Tvrzení 13.1.2. *Každý anulující polynom je dělitelný minimálním polynomem.*

Důkaz. Buď f anulující polynom matice A , buď g minimální polynom matice A . Dělme se zbytkem: $f = qg + r$, kde buď $r = 0$ nebo $\deg r < \deg g$. Do rovnosti dosadíme A a dostaneme

$$0 = f(A) = q(A)g(A) + r(A) = r(A),$$

protože f a g jsou anulující polynomy. Kdyby $r \neq 0$, byl by to anulující polynom nižšího stupně než minimální polynom g , což je spor, a proto $r = 0$ a g je dělitelem f . $\square$

Důsledek. *Ke každé lineární transformaci konečněrozměrného vektorového prostoru resp. ke každé čtvercové matici existuje minimální polynom a je jediný.*

Cvičení. Dokažte jednoznačnost minimálního polynomu. $\square$

13.1.2. Invariantní podprostory

Je-li $U \subseteq V$ podprostor, pak symbolem fU označujeme jeho obraz při zobrazení f , to jest, podprostor $\{f(u) \mid u \in U\}$.

Definice 13.1.3. Podprostor $U \subseteq V$ je *invariantní* vzhledem k lineární transformaci f , jestliže $fU \subseteq U$, tj. když pro každé $u \in U$ je $f(u) \in U$.

Je-li U invariantní podprostor, pak zobrazení $U \rightarrow U$, zadané předpisem $u \mapsto f(u)$, nazýváme *restrikce* (česky *ohraničení* nebo *zúžení*) lineárního zobrazení f na invariantní podprostor U . Značí se $f|_U: U \rightarrow U$ a je zřejmě opět lineární (ověřte).

Příklad. (1) Celý prostor V a nulový podprostor jsou invariantní podprostory vzhledem ke každé lineární transformaci.

(2) Je-li $f: v \mapsto cv$, pak je každý podprostor invariantní.

(3) Je-li u vlastní vektor s vlastní hodnotou c , pak $\llbracket u \rrbracket$ je invariantní podprostor a $f|_{\llbracket u \rrbracket}$ je zobrazení $v \mapsto cv$.

(4) Mějme rotaci $\varphi: E^3 \rightarrow E^3$ kolem zvolené pevné osy L procházející počátkem 0 o úhel $\alpha \in (0, 2\pi)$. Invariantní podprostory jsou nulový podprostor $\{0\}$, osa rotace L , její ortogonální doplněk $L^\perp$ (rovina procházející počátkem kolmo k L) a celý prostor E^3 . Libovolný vektor $u \in L$ se zobrazí sám na sebe, proto $\varphi|_L$ je identické zobrazení id_L . Libovolný vektor $v \in L^\perp$ zůstane v rovině $L^\perp$ a $\varphi|_{L^\perp}$ je otáčení roviny $L^\perp$ o úhel α .

(5) Mějme zrcadlení ζ v prostoru E^3 vzhledem k rovině U procházející počátkem 0. Invariantní podprostory jsou nulový podprostor $\{0\}$, rovina U a každý její podprostor $V \subseteq U$, ortogonální doplněk $U^\perp$ (přímka procházející počátkem kolmo k U) a celý prostor E^3 . Zobrazení $\zeta|_V$ je identické zobrazení id_V . Zobrazení $\zeta|_{U^\perp}$ je zrcadlení přímky $U^\perp$ vzhledem k počátku 0. $\square$

Cvičení. (1) Jednorozměrný podprostor $\llbracket u \rrbracket$, $u \neq 0$, je invariantní právě tehdy, když u je vlastní vektor. Dokažte.

(2) Průnik a součet invariantních podprostorů jsou invariantní podprostory. Dokažte.

(3) $\text{Ker } f$ je invariantní podprostor. Dokažte. Co je $f|_{\text{Ker } f}$?

(4) $\text{Im } f$ je invariantní podprostor. Dokažte.

(5) Buď $v \in V$ libovolný vektor. Dokažte, že $\llbracket v, f(v), f(f(v)), f(f(f(v))), \dots \rrbracket$ je invariantní podprostor.

(6) Necht' lineární transformace $f, g: V \rightarrow V$ komutují, to jest, $f \circ g = g \circ f$. Buď $U \subseteq V$ invariantní podprostor vzhledem k transformaci f . Pak gU je též invariantní podprostor vzhledem k transformaci f . $\square$

13.1.3. První rozklad lineární transformace

Tvrzení 13.1.3. Buď q anulující polynom lineární transformace $f: V \rightarrow V$ a necht' existuje rozklad $q = q_1 \cdots q_n$, kde $q_1, \dots, q_n$ jsou po dvou nesoudělné ($D(q_i, q_j) = 1$ pro $i \neq j$). Pro $i \in \{1, \dots, n\}$ označme $U_i = \text{Ker } q_i(f)$. Pak platí:

(1) každý podprostor U_i je invariantní;

(2) $V = U_1 \dot{+} \cdots \dot{+} U_n$;

(3) pro každé $i \in \{1, \dots, n\}$ polynom q_i je anulujícím polynomem transformace $f|_{U_i}$.

Důkaz. (1) Necht' $u \in U_i$, tj. $q_i(f)(u) = 0$. Potom

$$q_i(f)(f(u)) = (q_i(f) \circ f)(u) = (f \circ q_i(f))(u) = f(q_i(f)(u)) = f(0) = 0$$

(použili jsme to, že f a $q_i(f)$ spolu komutují podle Důsledku Tvrzení 11.6.7). Tudíž, $f(u) \in U_i$.

(2) Nejdříve případ $n = 2$. Necht' $q = q_1 q_2$ a $D(q_1, q_2) = 1$. Pak existují polynomy p_1, p_2 takové, že $1 = q_1 p_1 + q_2 p_2$. Dosazením f získáváme rovnost

$$\text{id} = q_1(f) \circ p_1(f) + q_2(f) \circ p_2(f),$$

takže pro libovolný vektor $v \in V$ platí

$$v = q_1(f)(p_1(f)(v)) + q_2(f)(p_2(f)(v)). \quad (13)$$

Ukažme, že první sčítanec $q_1(f)(p_1(f)(v))$ z (13) leží v U_2 . Označíme-li $w = p_1(f)(v)$, stačí ověřit, že $q_1(f)(w) \in \text{Ker } q_2(f)$:

$$q_2(f)(q_1(f)(w)) = (q_2(f) \circ q_1(f))(w) = (q_2 q_1)(f)(w) = q(f)(w) = 0,$$

protože q je anulující polynom pro f . Podobně se ukáže, že druhý ze sčítanců leží v U_1 . Tudíž, $v \in U_1 + U_2$. Protože v byl libovolný vektor z V , máme $V = U_1 + U_2$.

Ukažme ještě, že $U_1 \cap U_2 = 0$. Necht' tedy $v \in U_1 \cap U_2$, tj. $q_1(f)(v) = 0$ a $q_2(f)(v) = 0$. Rovnost (13) platí i po záměně $p \leftrightarrow q$ (protože $p_i(f)$ a $q_i(f)$ spolu komutují podle

Důsledku Tvzení 11.6.7), načež

$$v = p_1(f)(q_1(f)(v)) + p_2(f)(q_2(f)(v)) = p_1(f)(0) + p_2(f)(0) = 0,$$

protože $p_1(f), p_2(f)$ jsou lineární zobrazení. Dokázali jsme tedy, že $V = U_1 \dot{+} U_2$.

Obsahující případ $n > 2$ se dokáže indukcí (cvičení).

(3) Polynom q_i je anulujícím polynomem transformace $f|_{U_i}$, protože $\text{Ker } q_i(f) = U_i$, načež

$$\text{Ker } q_i(f|_{U_i}) = \text{Ker}(q_i(f)|_{U_i}) = U_i \cap \text{Ker } q_i(f) = U_i, \text{ a tedy } q_i(f|_{U_i}) = 0. \quad \square$$

Tvrzení 13.1.4. *Nechť existuje přímý rozklad $V = U_1 \dot{+} U_2$, kde U_1, U_2 jsou invariantní podprostory vzhledem k lineární transformaci f . Zvolme nějakou bázi $(e_1, \dots, e_m)$ podprostoru U_1 a nějakou bázi $(e_{m+1}, \dots, e_n)$ podprostoru U_2 . Pak $(e_1, \dots, e_n)$ je báze prostoru V a transformace f v ní má matici tvaru*

$$A = \begin{pmatrix} A_1^1 & \dots & A_m^1 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ A_1^m & \dots & A_m^m & 0 & \dots & 0 \\ 0 & \dots & 0 & A_{m+1}^{m+1} & \dots & A_n^{m+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & A_{m+1}^n & \dots & A_n^n \end{pmatrix}.$$

Označíme-li

$$A_1 = \begin{pmatrix} A_1^1 & \dots & A_m^1 \\ \vdots & & \vdots \\ A_1^m & \dots & A_m^m \end{pmatrix}, \quad A_2 = \begin{pmatrix} A_{m+1}^{m+1} & \dots & A_n^{m+1} \\ \vdots & & \vdots \\ A_{m+1}^n & \dots & A_n^n \end{pmatrix},$$

pak A_i je matice lineární transformace $f|_{U_i}$.

Důkaz. Ověřte, že $(e_1, \dots, e_n)$ je báze prostoru V .

Prvních m sloupků matice A je tvořeno souřadnicemi vektorů $f(e_1), \dots, f(e_m)$ v bázi $(e_1, \dots, e_n)$. Vektory $f(e_1), \dots, f(e_m)$ ovšem leží v U_1 s bázi $(e_1, \dots, e_m)$, takže koeficienty u vektorů $e_{m+1}, \dots, e_n$ v příslušné lineární kombinaci budou nulové.

Ověřte, že A_1 je matice lineární transformace $f|_{U_1}$ vzhledem k bázi $(e_1, \dots, e_m)$.

Zbytek analogicky. $\square$

O shora uvedené matici A říkáme, že je v *blokově diagonálním tvaru* s bloky A_1, A_2 na diagonále. Stručně zapisujeme

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

Říkáme též, že A je *přímý součet submatic* A_1 a A_2 .

Podobně se v případě přímého součtu $V = U_1 \dot{+} \dots \dot{+} U_n$ invariantních podprostorů $U_1, \dots, U_n$ matice zobrazení f rozpadá na přímý součet submatic $A_1, \dots, A_n$ odpovídajících lineárním zobrazením $f|_{U_1}, \dots, f|_{U_n}$:

$$A = \begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & A_n \end{pmatrix}.$$

O matici A rovněž pravíme, že je *blokově diagonální*.

V ideálním případě lze prostor V rozložit na přímý součet jednorozměrných invariantních podprostorů, generovaných vlastními vektory, což je nám již známý případ diagonalizovatelné matice.

Příklad. Nechť

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

Charakteristický polynom je $x^3 - 5x^2 + 9x - 5 = (x-1)(x^2 - 4x + 5)$ (ověřte). Vidíme, že polynom χ_A je součinem nesoudělných polynomů $q_1 = x - 1$ a $q_2 = x^2 - 4x + 5$.

Matice A představuje lineární zobrazení $\alpha: \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $u \mapsto Au$. Počítejme $U_1 = \text{Ker } q_1(\alpha) = \text{Ker}(\alpha - \text{id})$. Jádro $\text{Ker}(\alpha - \text{id})$ vypočteme řešením rovnice $(\alpha - \text{id})(u) = 0$, což je homogenní soustava s maticí

$$q_1(A) = A - E = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & -1 \\ -1 & 0 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 1 \\ 0 & 1 & -1 \\ -1 & 0 & 1 \end{pmatrix}$$

a fundamentálním řešením $e_1 = (1, 1, 1)$ (ověřte). Dostáváme jednorozměrný invariantní podprostor

$$U_1 = \text{Ker } q_1(\alpha) = \llbracket (1, 1, 1) \rrbracket.$$

Podobně $U_2 = \text{Ker } q_2(\alpha) = \text{Ker}(\alpha^2 - 4\alpha + 5\text{id})$. Toto jádro vypočteme řešením rovnice

$$(\alpha^2 - 4\alpha + 5\text{id})(u) = 0,$$

což je homogenní soustava s maticí

$$q_2(A) = A^2 - 4A + 5E = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

a fundamentálním řešením $e_2 = (0, 0, 1)$, $e_3 = (1, -1, 0)$ (ověřte). Dostáváme dvojrozměrný invariantní podprostor

$$U_2 = \text{Ker } q_2(\alpha) = \llbracket (0, 0, 1), (1, -1, 0) \rrbracket.$$

Získali jsme (a) přímý rozklad $\mathbb{R}^3 = U_1 \dot{+} U_2$ na invariantní podprostory U_1 a U_2 ; (b) „novou“ bázi (e_1, e_2, e_3) . Matici přechodu od „staré“ kanonické báze k „nové“ bázi označme Q . Inverzní matice Q^{-1} je matice přechodu od „nové“ báze ke kanonické bázi. Tedy

$$Q = \begin{pmatrix} 1/2 & 1/2 & 0 \\ -1/2 & -1/2 & 1 \\ 1/2 & -1/2 & 0 \end{pmatrix} \quad \text{a} \quad Q^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Matice zobrazení α vzhledem k „nové“ bázi je tedy blokově diagonální matice

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

□

Příklad. Nechť $\alpha: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ je lineární zobrazení, jehož matice vzhledem ke kanonické („staré“) bázi $((1, 0, 0), (0, 1, 0), (0, 0, 1))$ je

$$A = \begin{pmatrix} 1 & -1 & 2 \\ 3 & -3 & 6 \\ 2 & -2 & 4 \end{pmatrix}.$$

Charakteristický polynom matice A je $\chi_A = -x^2(x - 2)$ a můžeme jej zapsat jako součin nesoudělných polynomů $q_1 = -x^2$ a $q_2 = x - 2$. Vlastní čísla jsou $\lambda_1 = 0$ a $\lambda_2 = 2$.

Tedy

$$q_1(A) = -A^2 = \begin{pmatrix} -2 & 2 & -4 \\ -6 & 6 & -12 \\ -4 & 4 & -8 \end{pmatrix} \quad \text{a} \quad q_2(A) = A - 2E = \begin{pmatrix} -1 & -1 & 2 \\ 3 & -5 & 6 \\ 2 & -2 & 2 \end{pmatrix}.$$

Potom $U_1 = \text{Ker } q_1(A) = \text{Ker}(-A^2)$ je množina všech řešení homogenní soustavy lineárních rovnic s maticí $-A^2$ a $U_2 = \text{Ker } q_2(A) = \text{Ker}(A - 2E)$ je množina všech řešení homogenní soustavy lineárních rovnic s maticí $A - 2E$. Tedy $U_1 = \llbracket (-2, 0, 1), (1, 1, 0) \rrbracket$ a $U_2 = \llbracket (1, 3, 2) \rrbracket$.

Takže prostor $\mathbb{R}^3$ je přímým součtem invariantních podprostorů U_1, U_2 a vektory $(-2, 0, 1), (1, 1, 0), (1, 3, 2)$ tvoří „novou“ bázi prostoru $\mathbb{R}^3$. Matice přechodu od „staré“ báze k „nové“ bázi je

$$Q = \begin{pmatrix} -1 & 1 & -1 \\ -3/2 & 5/2 & -3 \\ 1/2 & -1/2 & 1 \end{pmatrix}, \quad Q^{-1} = \begin{pmatrix} -2 & 1 & 1 \\ 0 & 1 & 3 \\ 1 & 0 & 2 \end{pmatrix}$$

a matice zobrazení α vzhledem k „nové“ bázi je

$$A' = Q \cdot A \cdot Q^{-1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}. \quad \square$$

13.2. Druhý rozklad lineární transformace

Úmluva. Všude $P = \mathbb{C}$.

V přednášce o vlastních vektorech jsme se seznámili s diagonalizovatelnými transformacemi. V bázi složené z vlastních vektorů v_i mají diagonální matice s vlastními čísly λ_i na diagonále.

Obecná lineární transformace nemusí mít bázi složenou z vlastních vektorů. Nicméně, jak ukážeme, lze zkonstruovat jinou významnou bázi — Jordanovu. Matice lineární transformace v Jordanově bázi je tzv. Jordanova matice. Opět má na diagonále vlastní čísla, ale může obsahovat i nenulové prvky v řadě sousedící s diagonálou (všechny ovšem rovny 1).

Východiskem pro nalezení Jordanovy báze bude první rozklad, příslušný rozkladu charakteristického polynomu (nebo libovolného jiného anulujícího polynomu) χ_f na nesoudělné součinitele. Při $P = \mathbb{C}$ ovšem existuje rozklad na kořenové činitele

$$\chi_f = (x - \xi_1)^{k_1} \cdots (x - \xi_s)^{k_s}, \quad \xi_i \neq \xi_j \text{ pro } i \neq j,$$

a pro $i \neq j$ jsou polynomy $(x - \xi_i)^{k_i}$ a $(x - \xi_j)^{k_j}$ nesoudělné. Invariantní podprostory prvního rozkladu pak jsou

$$U_i = \text{Ker}(f - \xi_i \text{id})^{k_i}.$$

Na jednotlivých invariantních podprostorech vznikají restrikce $f|_{U_i}: U_i \rightarrow U_i$. Označíme-li $g_i = f - \xi_i \text{id}$, pak $\text{Ker } g_i^{k_i} = U_i$, a tedy $(g|_{U_i})^{k_i} = 0$.

Má tedy smysl studovat transformace $f: U \rightarrow U$ takové, že pro některé číslo ξ transformace $g = f - \xi \text{id}$ splňuje $g^k = 0$. Výsledky použijeme pro $U = U_i$ a $g = f|_{U_i} - \xi_i \text{id}_{U_i}$, $i = 1, \dots, s$.

13.2.1. Rozklad na součet cyklických podprostorů

Definice 13.2.1. Transformace $g: U \rightarrow U$ (resp. čtvercová matice B) je *nilpotentní*, jestliže existuje celé číslo $k \geq 1$ takové, že $g^k = 0$ (resp. $B^k = 0$).

Cvičení. Transformace g je nilpotentní právě tehdy, když je její matice B (v libovolné bázi) nilpotentní. $\square$

Definice 13.2.2. Podprostor $T \subseteq U$ je *cyklický* vzhledem k transformaci $g: U \rightarrow U$, jestliže má bázi $(e_1, e_2, \dots, e_n)$ takovou, že

$$g(e_1) = e_2, \quad g(e_2) = e_3, \quad \dots, \quad g(e_{n-1}) = e_n, \quad g(e_n) = 0.$$

Báze $(e_1, e_2, \dots, e_n)$ je *cyklická báze*.

Schematicky,

$$e_1 \xrightarrow{g} e_2 \xrightarrow{g} \dots e_{n-1} \xrightarrow{g} e_n \xrightarrow{g} 0.$$

Definice 13.2.3. Matice

$$J_1(\xi) = (\xi), \quad J_2(\xi) = \begin{pmatrix} \xi & 0 \\ 1 & \xi \end{pmatrix}, \quad J_3(\xi) = \begin{pmatrix} \xi & 0 & 0 \\ 1 & \xi & 0 \\ 0 & 1 & \xi \end{pmatrix},$$

$$J_4(\xi) = \begin{pmatrix} \xi & 0 & 0 & 0 \\ 1 & \xi & 0 & 0 \\ 0 & 1 & \xi & 0 \\ 0 & 0 & 1 & \xi \end{pmatrix}, \quad \text{atd.}$$

se nazývají *Jordanovy bloky* (též *Jordanovy buňky*).

Tvrzení 13.2.1. Buď T cyklický podprostor nilpotentní transformace g , buď $f = g + \xi \text{id}$. Pak

- (1) T je invariantní vzhledem k lineárním transformacím g i f ;
- (2) $g|_T$ má v cyklické bázi matici $J_n(0)$;
- (3) $f|_T$ má v cyklické bázi matici $J_n(\xi)$.

Důkaz. Cvičení. $\square$

Často se setkáváme s jinou definicí Jordanových buněk — jedničky stojí v řadě těsně nad diagonálou. To odpovídá opačnému pořadí vektorů cyklické báze, tj. $(e_n, \dots, e_2, e_1)$.

Lemma 13.2.2. Buď $h: U \rightarrow V$ lineární zobrazení mezi konečněrozměrnými vektorovými prostory. Zvolme libovolně bázi v $\text{Ker } h$ a doplňme ji do báze v U nějakými vektory $e_1, \dots, e_m$. Pak vektory $h(e_1), \dots, h(e_m)$ tvoří bázi v $\text{Im } h$.

Důkaz. Cvičení (viz důkaz formule $\dim U = \dim \text{Ker } h + \dim \text{Im } h$ v Tvrzení 11.2.5). $\square$

Tvrzení 13.2.3. Buď $g: U \rightarrow U$ nilpotentní transformace. Pak existují cyklické podprostory $T_1, \dots, T_r \subseteq U$ takové, že $U = T_1 \dot{+} \dots \dot{+} T_r$.

Důkaz. Tvrzení dokážeme uvedením praktického algoritmu pro nalezení cyklických podprostorů a jejich cyklickýchází. Popis algoritmu tvoří věty psané kurzívou.

Máme $U = \text{Ker } g^k$ pro jisté k (protože g je nilpotentní). Bez újmy na obecnosti je číslo k minimální, to jest, $g^{k-1} \neq 0$, a tudíž $\text{Ker } g^{k-1} \neq U$.

1. Zvolíme libovolně bázi v $\text{Ker } g^{k-1}$ a doplníme ji do báze v $U = \text{Ker } g^k$ nějakými vektory $e_1, \dots, e_{m_1}$.

Podle lemmatu vektory $g^{k-1}(e_1), \dots, g^{k-1}(e_{m_1})$ tvoří bázi v $\text{Im } g^{k-1}$ a jsou tedy lineárně nezávislé. Navíc, jelikož $g^k = 0$, máme $g(e_1), \dots, g(e_{m_1}) \in \text{Ker } g^{k-1}$.

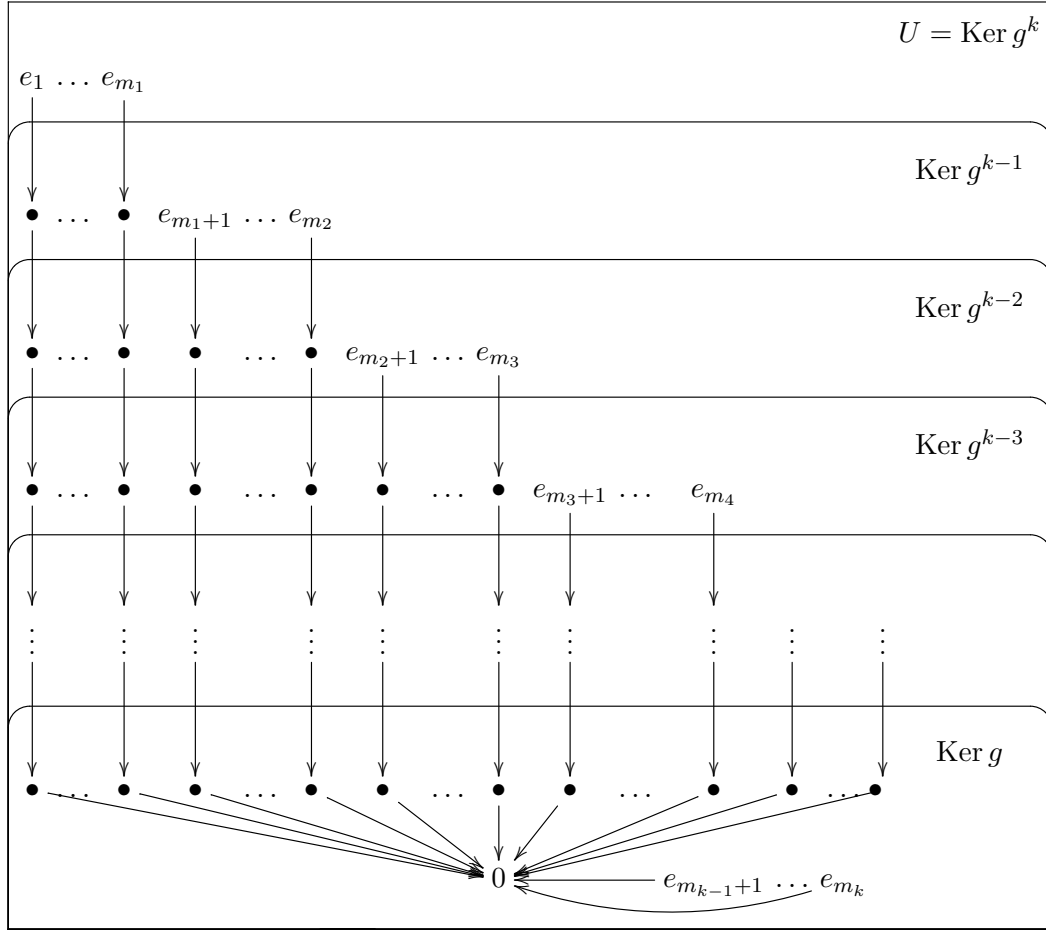
2. Zvolíme libovolně bázi v $\text{Ker } g^{k-2}$ a přidáme k ní vektory $g(e_1), \dots, g(e_{m_1}) \in \text{Ker } g^{k-1}$. Tato sestava je lineárně nezávislá. Skutečně, vezmeme si lineární kombinaci všech vektorů z této sestavy, která je rovna nulovému vektoru. Máme tedy skaláry $c_1, \dots, c_{m_1}$, takové, že $c_1 g(e_1) + \dots + c_{m_1} g(e_{m_1}) \in \text{Ker } g^{k-2}$. Pak ovšem $0 = g^{k-2}(c_1 g(e_1) + \dots + c_{m_1} g(e_{m_1})) = c_1 g^{k-1}(e_1) + \dots + c_{m_1} g^{k-1}(e_{m_1})$, a tedy $c_1 = \dots = c_{m_1} = 0$, protože vektory $g^{k-1}(e_1), \dots, g^{k-1}(e_{m_1})$ jsou lineárně nezávislé (viz výše). A potom také ostatní koeficienty v uvažované lineární kombinaci jsou nulové, protože příslušné vektory tvoří bázi.

Sestavu doplníme do báze v $\text{Ker } g^{k-1}$ nějakými vektory $e_{m_1+1}, \dots, e_{m_2}$.

Tím se vlastně báze v $\text{Ker } g^{k-2}$ doplní do báze v $\text{Ker } g^{k-1}$ vektory $g(e_1), \dots, g(e_{m_1}), e_{m_1+1}, \dots, e_{m_2}$. Z lemmatu potom vyplývá, že vektory $g^{k-1}(e_1), \dots, g^{k-1}(e_{m_1}), g^{k-2}(e_{m_1+1}), \dots, g^{k-2}(e_{m_2})$ tvoří bázi v $\text{Im}(g^{k-2}|_{\text{Ker } g^{k-1}})$ a jsou tedy lineárně nezávislé.

3. Zvolíme libovolně bázi v $\text{Ker } g^{k-3}$ a připojíme k ní vektory $g^2(e_1), \dots, g^2(e_{m_1}), g(e_{m_1+1}), \dots, g(e_{m_2}) \in \text{Ker } g^{k-2}$.

Tato sestava je lineárně nezávislá. Skutečně, vezmeme si lineární kombinaci všech vektorů z této sestavy, která je rovna nulovému vektoru. Máme tedy skaláry $c_1, \dots, c_{m_1}, c_{m_1+1}, \dots, c_{m_2}$, takové, že $c_1 g^2(e_1) + \dots + c_{m_1} g^2(e_{m_1}) + c_{m_1+1} g(e_{m_1+1}) + \dots + c_{m_2} g(e_{m_2}) \in \text{Ker } g^{k-3}$. Pak ovšem $0 = g^{k-3}(c_1 g^2(e_1) + \dots + c_{m_1} g^2(e_{m_1}) + c_{m_1+1} g(e_{m_1+1}) + \dots + c_{m_2} g(e_{m_2})) = c_1 g^{k-1}(e_1) + \dots + c_{m_1} g^{k-1}(e_{m_1}) + c_{m_1+1} g^{k-2}(e_{m_1+1}) + \dots + c_{m_2} g^{k-2}(e_{m_2})$, a tedy $c_1 = \dots = c_{m_1} = c_{m_1+1} = \dots = c_{m_2} = 0$, protože vektory $g^{k-1}(e_1), \dots, g^{k-1}(e_{m_1}), g^{k-2}(e_{m_1+1}), \dots, g^{k-2}(e_{m_2})$ jsou lineárně nezávislé (viz výše). A potom také ostatní koeficienty v uvažované lineární kombinaci jsou nulové, protože příslušné vektory tvoří bázi.



Sestavu doplníme do báze v $\text{Ker } g^{k-2}$ nějakými vektory $e_{m_2+1}, \dots, e_{m_3}$.

Tím jsme tedy bázi v $\text{Ker } g^{k-3}$ doplnili do báze v $\text{Ker } g^{k-2}$ vektory $g^2(e_1), \dots, g^2(e_{m_1}), g(e_{m_1+1}), \dots, g(e_{m_2}), e_{m_2+1}, \dots, e_{m_3}$. A potom vektory $g^{k-1}(e_1), \dots, g^{k-1}(e_{m_1}), g^{k-2}(e_{m_1+1}), \dots, g^{k-2}(e_{m_2}), g^{k-3}(e_{m_2+1}), \dots, g^{k-3}(e_{m_3})$ tvoří podle lematu bázi v $\text{Im}(g^{k-3}|_{\text{Ker } g^{k-2}})$ a jsou tedy lineárně nezávislé.

Podobných kroků provedeme k (v posledním kroku doplňujeme bázi podprostoru $\text{Ker } g^0 = \text{Ker id} = \{0\}$ do báze v podprostoru $\text{Ker } g$).

Z uvedeného postupu vyplývá, že celkově získáme bázi

$$\begin{aligned}
 &e_1, \dots, e_{m_1}, \\
 &g(e_1), \dots, g(e_{m_1}), e_{m_1+1}, \dots, e_{m_2}, \\
 &g^2(e_1), \dots, g^2(e_{m_1}), g(e_{m_1+1}), \dots, g(e_{m_2}), e_{m_2+1}, \dots, e_{m_3}, \\
 &\dots \\
 &g^{k-1}(e_1), \dots, g^{k-1}(e_{m_1}), g^{k-2}(e_{m_1+1}), \dots, g^{k-2}(e_{m_2}), \\
 &g^{k-3}(e_{m_2+1}), \dots, g^{k-3}(e_{m_3}), \dots, e_{m_{k-1}+1}, \dots, e_{m_k}
 \end{aligned}$$

v prostoru U . Podprostory

$$\begin{aligned} & \llbracket e_1, g(e_1), \dots, g^{k-1}(e_1) \rrbracket, \dots, \llbracket e_{m_1}, g(e_{m_1}), \dots, g^{k-1}(e_{m_1}) \rrbracket, \\ & \llbracket e_{m_1+1}, g(e_{m_1+1}), \dots, g^{k-2}(e_{m_1+1}) \rrbracket, \dots, \llbracket e_{m_2}, g(e_{m_2}), \dots, g^{k-2}(e_{m_2}) \rrbracket, \\ & \dots \\ & \llbracket e_{m_{k-1}+1}, \dots, e_{m_k} \rrbracket \end{aligned}$$

jsou pak cyklické podprostory s příslušnými cyklickými bázemi.

Označíme-li počet těchto cyklických podprostorů $r := \sum_{j=1}^k m_j$ a jednotlivé podprostory T_i pro $i = 1, \dots, r$, dostáváme $U = T_1 + \dots + T_r$. Jelikož $\dim T_1 + \dots + \dim T_r = \dim(T_1 + \dots + T_r)$, podle Tvzení 10.3.3 se jedná o přímý součet podprostorů. $\square$

Nalezli jsme cyklické podprostory a v každém z nich cyklickou bázi. Situaci můžeme znázornit diagramem, jehož vrcholy jsou vektory cyklických bází a šipky znamenají zobrazení g :

$$\begin{array}{cccccccccccccccc} \bullet & \bullet & \bullet & & & & & & & & & & & & & & & \\ \downarrow & \downarrow & \downarrow & & & & & & & & & & & & & & & \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & & & & & & & & & & & \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & & & & & & & & & & \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \end{array} \quad (14)$$

Sloupky znamenají jednotlivé cyklické podprostory. Vektory spodní řady se zobrazují na nulový vektor. Tvoří vlastně bázi v $\text{Ker } g = \text{Ker}(f - \xi \text{id}) = V_\xi$, což je prostor vlastních vektorů s vlastním číslem ξ . Tudíž, počet sloupků = počet cyklických podprostorů = $\dim V_\xi$.

Vektory dolních j řádků tvoří bázi v $\text{Ker } g^j$. V j -tém řádku zdola je proto právě

$$n_j = \dim \text{Ker } g^j - \dim \text{Ker } g^{j-1} = \sum_{i=1}^{k+1-j} m_i \quad (15)$$

bodů, kde m_i jsou koeficienty z důkazu předchozího tvrzení. Čísla $n_1 \geq n_2 \geq \dots \geq n_k$ jednoznačně určují délky řádků diagramu, a tím i počty cyklických podprostorů příslušných dimenzí.

Formule (15) ukazuje, že čísla $n_1 \geq n_2 \geq \dots \geq n_k$ závisí jen a jen na nilpotentní transformaci g a nikoliv na konkrétním postupu, kterým byly získány jednotlivé cyklické báze. Jsou to *invarianty lineární transformace g* .

Důsledek. *Bud' $g: U \rightarrow U$ nilpotentní transformace. Pak existuje báze prostoru U taková, že*

- (1) *transformace g má blokově diagonální matici, která je přímým součtem Jordanových bloků $J_s(0)$;*
- (2) *transformace $f = g + \xi \text{id}$ má blokově diagonální matici, která je přímým součtem Jordanových bloků $J_s(\xi)$.*

Důkaz. Báze sestavená z cyklických bází cyklických podprostorů v důkazu předchozího tvrzení má požadované vlastnosti. $\square$

Příklad. Uvažujme lineární transformaci $\mathbb{C}^5 \rightarrow \mathbb{C}^5$, $v \mapsto Av$, kde

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

Anulující polynom nejmenšího stupně je $x^3 + 6x^2 + 12x + 8 = (x+2)^3$, s jediným kořenem -2 , což je současně jediná vlastní hodnota matice A . První rozklad má proto jediného sčítance $U = \mathbb{C}^5$ a

$$B = A + 2E = \begin{pmatrix} 2 & 1 & 1 & -2 & 0 \\ -3 & -2 & -4 & 3 & 0 \\ 3 & 1 & 2 & -3 & 3 \\ 4 & 1 & 1 & -4 & 4 \\ 1 & 0 & 0 & -1 & 2 \end{pmatrix}$$

je nilpotentní matice, $B^3 = 0$. Spočítáme

$$B^2 = \begin{pmatrix} -4 & -1 & -2 & 4 & -5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -4 & -1 & -2 & 4 & -5 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

načez $\text{Ker } B^2 = \llbracket (5, 0, 0, 0, -4), (0, 5, 0, 0, -1), (0, 0, 5, 0, -2), (0, 0, 0, 5, 4) \rrbracket$. Tento čtyřrozměrný podprostor můžeme doplnit do báze v $\mathbb{C}^5$ libovolným vektorem, který v něm neleží, zvolme například

$$e_1 = (0, 0, 0, 0, 1).$$

Tím je ukončen první krok. Ve druhém kroku spočítáme

$$\text{Ker } B = \llbracket (1, 0, 0, 1, 0), (0, -5, 1, -2, -1) \rrbracket,$$

a přidáme vektor

$$Be_1 = (0, 0, 3, 4, 2).$$

Získanou sestavu tří lineárně nezávislých vektorů je třeba doplnit do báze ve čtyřrozměrném $\text{Ker } B^2$ jedním vektorem; zvolme například

$$e_2 = (0, 0, 0, 5, 4)$$

(mohli jsme zvolit kterýkoliv ze shora uvedených generátorů podprostoru $\text{Ker } B^2$). Tím je ukončen druhý krok. Ve třetím kroku je $\text{Ker } B^0 = \text{Ker } E = 0$ a doplňujeme tedy dva vektory

$$B^2e_1 = (-5, 0, 0, -5, 0) \quad \text{a} \quad Be_2 = (-10, 15, -3, -4, 3)$$

do báze v dvojrozměrném $\text{Ker } B$, což ovšem nevyžaduje žádný doplňující vektor a jsme hotovi.

Hledaná báze prostoru $\mathbb{C}^5$ je proto $(e_1, Be_1, B^2e_1, e_2, Be_2)$. Příslušný diagram je



a jeho dva sloupky odpovídají dvěma Jordanovým blokům rozměrů 3 a 2. Dostáváme blokově diagonální matice

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

(při obráceném pořadí vektorů v cyklických bázích by jedničky stály nad diagonálou; odlišné může být i pořadí Jordanových bloků). $\square$

13.2.2. Druhý rozklad a Jordanův tvar matice

Vraťme se nyní k obecné transformaci $f: V \rightarrow V$ a prvnímu rozkladu $V = U_1 \dot{+} \dots \dot{+} U_s$ podle některého anulujícího polynomu. Pro každý z prostorů U_l , $l = 1, \dots, s$ dostáváme rozklad na cyklické podprostory $T_{l,i}$, kde $i = 1, \dots, k_l$, celkem tedy

$$V = T_{1,1} \dot{+} \dots \dot{+} T_{1,k_1} \dot{+} \dots \dot{+} T_{s,1} \dot{+} \dots \dot{+} T_{s,k_s}.$$

Definice 13.2.4. Tento rozklad je *druhý rozklad* prostoru lineární transformace.

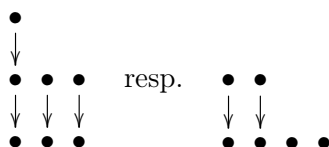
Připomeňme, že cyklické podprostory $T_{i,j}$ jsou invariantní a zobrazení $f|_{T_{i,j}}$ mají v cyklické bázi matici tvaru $J_r(\xi)$, $r = \dim T_{i,j}$.

Definice 13.2.5. Matice, která je přímým součtem Jordanových bloků, je *matice v Jordanově tvaru*.

Příklad. Matice

$$\left(\begin{array}{ccc|ccc|cccc|cccc|cccc|cccc} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \end{array} \right)$$

je v Jordanově tvaru. Bloky prvního rozkladu jsou vyznačeny dvojitou čarou. Blokům druhého rozkladu odpovídají diagramy



Šipky zde znamenají zobrazení $f - 2 \text{id}$ resp. $f - 3 \text{id}$. Délky spodních řádků jsou dimenze prostorů vlastních vektorů s vlastními hodnotami 2 resp. 3. $\square$

Důsledek. Bud' $f: V \rightarrow V$ lineární transformace. Pak existuje báze prostoru V , vzhledem k níž f má matici v Jordanově tvaru.

Definice 13.2.6. Báze z předchozího důsledku je *Jordanova báze* a získáme ji sjednocením cyklických bází v jednotlivých cyklických podprostorech $T_{i,j}$.

Při praktickém převodu na Jordanův tvar nejdříve nalezneme invariantní podprostory $U = \text{Ker } g^k = \text{Ker}(f - \xi \text{id})^k$ prvního rozkladu, pro každou vlastní hodnotu ξ zvlášť. V každém z nich pak hledáme cyklické podprostory a cyklické báze postupem uvedeným v důkazu Tvzení 13.2.3.

Zbývá rozhodnout, nakolik je Jordanův tvar matice lineární transformace určen jednoznačně. Postup k nalezení Jordanovy báze, který jsme popsali, udává jednoznačně všechny Jordanovy buňky $J_r(\xi)$. Číslo ξ probíhá všechny vlastní hodnoty, rozměr r je

určen prostřednictvím diagramů (14) a počet buněk s daným rozměrem je určen prostřednictvím čísel $n_1 \geq n_2 \geq \dots \geq n_k$, která jsou zase jednoznačně určena formulí (15), kde $g = f - \xi \text{ id}$. Neurčeno pak zůstává pouze pořadí Jordanových buněk.

Cvičení. Spočítejte Jordanův tvar transponované matice A^T . (Výsledek: je týž.) $\square$

13.2.3. Minimální polynom

Minimální polynom můžeme jednoduše stanovit z Jordanova tvaru jako polynom

$$(x - \xi_1)^{\mu_1} \cdots (x - \xi_s)^{\mu_s},$$

kde $\xi_1, \dots, \xi_s$ jsou vlastní hodnoty lineární transformace, resp. matice a $\mu_1, \dots, \mu_s$ jsou výšky (maximální délky sloupků) diagramů (14) pro jednotlivé vlastní hodnoty $\xi_1, \dots, \xi_s$. (Dokažte jako cvičení.)

Příklad. Matice z posledního příkladu má minimální polynom $(x - 2)^3(x - 3)^2$. $\square$

13.3. Jordanův tvar matice a kritérium podobnosti matic

Připomeňme, že dvě čtvercové matice A, B jsou podobné, jestliže existuje invertibilní matice Q taková, že $B = QAQ^{-1}$. Zapisujeme $A \approx B$. Dále připomeňme, že matice jedné a téže lineární transformace v různých bázích jsou si podobné (maticí Q je v tomto případě matice přechodu mezi bázemi).

Tvrzení 13.3.1. *Každá čtvercová komplexní matice je podobná matici v Jordanově tvaru.*

Důkaz. Buď A čtvercová komplexní matice typu $n \times n$. Potom A je maticí lineární transformace $f: \mathbb{C}^n \rightarrow \mathbb{C}^n$, $u \mapsto Au$. V Jordanově bázi má transformace f matici B v Jordanově tvaru. Pak $B \approx A$. $\square$

Definice 13.3.1. Matice B z předchozího důkazu je *Jordanův tvar matice A* .

Jordanův tvar je určen jednoznačně až na pořadí bloků a rozhoduje o podobnosti matic:

Tvrzení 13.3.2. *Matice jsou si podobné právě tehdy, když mají stejný Jordanův tvar až na pořadí Jordanových bloků.*

Důkaz. Jsou-li si matice A', A'' podobné, pak zobrazení $u \mapsto A'u$, $u \mapsto A''u$ mají stejné charakteristické polynomy, stejné vlastní hodnoty a stejné jsou i dimenze a počty invariantních podprostorů určené diagramy (14) a formulí (15) (cvičení). Proto jsou stejné i Jordanovy tvary.

Naopak, buďte $B' \approx A'$ a $B'' \approx A''$ Jordanovy tvary matic A' a A'' . Jestliže se B' a B'' liší jen pořadím Jordanových bloků, pak jsou si podobné (cvičení), načež $A' \approx B' \approx B'' \approx A''$. $\square$

Cvičení. Dokažte, že pro libovolnou čtvercovou matici platí $A \approx A^T$.

Návod: Dokažte postupně

- (i) $J \approx J^T$ pro libovolnou Jordanovu matici J (stačí zpřeházet vektory v Jordanově bázi);
- (ii) je-li $A \approx J$, pak $A^T \approx J^T$. $\square$

14. SKALÁRNÍ SOUČIN

Označení. Číslo komplexně sdružené k číslu z označujeme $\bar{z}$. Je-li $A = (A_j^i)$ matice, označujeme $\bar{A} = (\bar{A}_j^i)$.

Definice 14.0.1. Buď V vektorový prostor nad P , kde $P = \mathbb{R}$ nebo $P = \mathbb{C}$. Zobrazení $g: V \times V \rightarrow P$ je *skalární součin* na V , jestliže pro libovolné $u, v, w \in V$ a $p \in P$ platí

- (1) $g(u + v, w) = g(u, w) + g(v, w)$;
- (2) $g(pu, v) = pg(u, v)$;
- (3) $g(u, v) = \overline{g(v, u)}$;
- (4) $g(v, v) > 0$ pro $v \neq 0$.

Číslo $g(v, v)$ je reálné pro každý vektor v , i v případě, že $P = \mathbb{C}$ (cvičení). Díky tomu lze ve čtvrté vlastnosti porovnávat $g(v, v)$ s 0.

První dvě vlastnosti znamenají, že skalární součin je *lineární v prvním argumentu*, třetí vlastnost je v reálném případě *symetrie*, v komplexním případě *kosá symetrie*, čtvrtá vlastnost je *pozitivní definitnost*.

Definice 14.0.2. Vektorový prostor nad P se skalárním součinem je *prostor se skalárním součinem*. Pokud $P = \mathbb{R}$, skalární součin je *eukleidovský* a prostor je *eukleidovský*. Pokud $P = \mathbb{C}$, skalární součin je *hermiteovský* a prostor je *hermiteovský* nebo *unitární*.

Označení. Nemůže-li dojít k nedorozumění, místo $g(u, v)$ píšeme jen (u, v) .

Tvrzení 14.0.1. Buď V prostor se skalárním součinem nad P . Pro libovolné $u, v, w \in V$ a $p \in P$ platí

- (1) $(u, v + w) = (u, v) + (u, w)$;
- (2) $(u, pv) = \overline{p}(u, v)$;
- (3) $(0, v) = (v, 0) = 0$;
- (4) $(v, v) = 0 \Leftrightarrow v = 0$.

Důkaz. (1)

$$(u, v + w) = \overline{(v + w, u)} = \overline{(v, u) + (w, u)} = \overline{(v, u)} + \overline{(w, u)} = (u, v) + (u, w).$$

(2)

$$(u, pv) = \overline{(pv, u)} = \overline{p(v, u)} = \overline{p} \overline{(v, u)} = \overline{p}(u, v).$$

(3)

$$(0, v) = (0 \cdot v, v) = 0 \cdot (v, v) = 0 \quad \text{a} \quad (v, 0) = \overline{(0, v)} = 0.$$

(4) Důsledek podmínky (4) v definici skalárního součinu a předchozího bodu (3). $\square$

Podle (1) a (2) v předchozím tvrzení Eukleidovský skalární součin je lineární i v druhém argumentu.

Příklad. (1) Standardní skalární součin na $\mathbb{R}^n$. Pro $x, y \in \mathbb{R}^n$, $x = (x^1, \dots, x^n)$, $y = (y^1, \dots, y^n)$,

$$(x, y) = x^1 y^1 + \dots + x^n y^n.$$

(2) Standardní skalární součin na $\mathbb{C}^n$. Pro $x, y \in \mathbb{C}^n$, $x = (x^1, \dots, x^n)$, $y = (y^1, \dots, y^n)$,

$$(x, y) = x^1 \overline{y^1} + \dots + x^n \overline{y^n}.$$

(3) Buďte $a_1, \dots, a_n$ kladná reálná čísla. Zobrazení $\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$, které vektorům $x = (x^1, \dots, x^n), y = (y^1, \dots, y^n) \in \mathbb{R}^n$ přiřadí číslo

$$(x, y) = a_1 x^1 y^1 + \dots + a_n x^n y^n,$$

je skalární součin na $\mathbb{R}^n$.

(4) Buďte $a_1, \dots, a_n$ kladná reálná čísla. Zobrazení $\mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}$, které vektorům $x = (x^1, \dots, x^n), y = (y^1, \dots, y^n) \in \mathbb{C}^n$ přiřadí číslo

$$(x, y) = a_1 x^1 \overline{y^1} + \dots + a_n x^n \overline{y^n},$$

je skalární součin na $\mathbb{C}^n$.

(5) Zobrazení, které maticím $A, B \in \mathbb{R}^{m \times n}$ přiřadí číslo

$$(A, B) = \sum_{i=1}^m \sum_{j=1}^n A_j^i B_j^i,$$

je skalární součin na $\mathbb{R}^{m \times n}$.

(6) Zobrazení, které maticím $A, B \in \mathbb{C}^{m \times n}$ přiřadí číslo

$$(A, B) = \sum_{i=1}^m \sum_{j=1}^n A_j^i \overline{B_j^i},$$

je skalární součin na $\mathbb{C}^{m \times n}$.

(7) Zobrazení, které spojitým reálným funkcím f, g na intervalu $[0, 2\pi]$ přiřadí reálné číslo

$$(f, g) = \int_0^{2\pi} f(x)g(x)dx,$$

je skalární součin na prostoru všech spojitých reálných funkcí na intervalu $[0, 2\pi]$. $\square$

14.1. Délka (norma) vektoru

Připomeňme, že $(v, v) \in \mathbb{R}$ a $(v, v) \geq 0$ pro každé v .

Definice 14.1.1. Buď V prostor se skalárním součinem, $v \in V$. *Délka* nebo *norma* vektoru v je číslo

$$\|v\| = \sqrt{(v, v)}.$$

Definice 14.1.2. Vektor délky 1 je *jednotkový* nebo *normovaný*.

Délka vektoru tedy závisí na skalárním součinu, a tak uvedené značení lze použít jen, je-li jasné, který skalární součin je uvažován a nemůže dojít k nedorozumění.

Příklad. (1) Mějme standardní skalární součin na $\mathbb{R}^2$. Délka vektoru $(1, 2)$ je $\sqrt{5}$.

(2) Na $\mathbb{R}^2$ mějme skalární součin $((x^1, x^2), (y^1, y^2)) = x^1 y^1 + 2x^2 y^2$. Délka vektoru $(1, 2)$ je 3.

(3) Na prostoru všech spojitých reálných funkcí na intervalu $[0, 1]$ mějme skalární součin

$$(f, g) = \int_0^1 f(x)g(x)dx.$$

Takže délka (norma) funkce f je

$$\|f\| = \sqrt{\int_0^1 (f(x))^2 dx}.$$

Pokud, například, $f(x) = x$, potom

$$\|f\| = \sqrt{\int_0^1 x^2 dx} = \frac{1}{\sqrt{3}}.$$

□

Tvrzení 14.1.1. *Bud' V prostor se skalárním součinem nad P . Pro libovolné $v \in V$ a $p \in P$ platí*

- (1) $\|v\| \geq 0$, navíc $\|v\| = 0$ právě tehdy, když $v = 0$,
- (2) $\|pv\| = |p|\|v\|$,
- (3) jestliže $v \neq 0$, pak

$$\left\| \frac{v}{\|v\|} \right\| = 1.$$

Důkaz. (1) Jednoduchý důsledek definice skalárního součinu a Tvrzení 14.0.1.

$$(2) \|pv\| = \sqrt{(pv, pv)} = \sqrt{p\overline{p}(v, v)} = \sqrt{|p|^2 \|v\|^2} = |p|\|v\|.$$

(3) Cvičení.

□

Lemma 14.1.2. (1) $\operatorname{re}(u, v) = \frac{1}{2}(\|u + v\|^2 - \|u\|^2 - \|v\|^2)$

$$(2) \operatorname{im}(u, v) = \frac{1}{2}(\|u + iv\|^2 - \|u\|^2 - \|v\|^2)$$

Důkaz. (1)

$$\begin{aligned} \|u + v\|^2 &= (u + v, u + v) = \\ &= (u, u) + (u, v) + (v, u) + (v, v) = \\ &= (u, u) + (u, v) + \overline{(u, v)} + (v, v) = \\ &= \|u\|^2 + 2\operatorname{re}(u, v) + \|v\|^2 \end{aligned}$$

Z toho dostaneme

$$\operatorname{re}(u, v) = \frac{1}{2}(\|u + v\|^2 - \|u\|^2 - \|v\|^2)$$

(2)

$$\begin{aligned} \|u + iv\|^2 &= (u + iv, u + iv) = \\ &= (u, u) + (u, iv) + (iv, u) + (iv, iv) = \\ &= (u, u) - i(u, v) + i\overline{(u, v)} + (v, v) = \\ &= \|u\|^2 + 2\operatorname{im}(u, v) + \|v\|^2 \end{aligned}$$

Z toho dostaneme

$$\operatorname{im}(u, v) = \frac{1}{2}(\|u + iv\|^2 - \|u\|^2 - \|v\|^2)$$

□

14.2. Nerovnosti

Tvrzení 14.2.1 (Cauchyova-Bunjakovského-Schwarzova nerovnost). *Nechť V je prostor se skalárním součinem a $u, v \in V$. Pak*

$$|(u, v)| \leq \|u\|\|v\|.$$

Rovnost nastává právě tehdy, když $\{u, v\}$ je lineárně závislá množina.

Důkaz. Předpokládejme, že $\{u, v\}$ je lineárně závislá. Pokud $u = 0$ nebo $v = 0$, pak $|(u, v)| = \|u\|\|v\| = 0$. Jsou-li u, v nenulové, existuje $p \in P$ takové, že $u = pv$ a

$$|(u, v)| = |(pv, v)| = |p|(v, v) = |p|\|v\|^2 = |p|\|v\|\|v\| = \|pv\|\|v\| = \|u\|\|v\|.$$

Je-li $\{u, v\}$ lineárně nezávislá, pak u, v jsou nenulové a pro každé $p \in P$ je $u - pv \neq 0$.
Pro

$$p = \frac{(u, v)}{(v, v)}$$

platí

$$0 = (u, v) - p(v, v) = (u, v) - (pv, v) = (u - pv, v).$$

Tedy

$$\begin{aligned} 0 &< \|u - pv\|^2 = (u - pv, u - pv) = \\ &= (u - pv, u) - \overline{p}(u - pv, v) = && ((u - pv, v) = 0) \\ &= \|u\|^2 - p(v, u) = && (p = (u, v)/\|v\|^2) \\ &= \|u\|^2 - \frac{(u, v)}{\|v\|^2} \cdot \overline{(u, v)} = \\ &= \|u\|^2 - \frac{|(u, v)|^2}{\|v\|^2}. \end{aligned}$$

Čili

$$\begin{aligned} 0 &< \|u\|^2 - \frac{|(u, v)|^2}{\|v\|^2} && (\text{obě strany vynásobíme } \|v\|^2) \\ 0 &< \|u\|^2\|v\|^2 - |(u, v)|^2 \\ |(u, v)|^2 &< \|u\|^2\|v\|^2 && (\text{obě strany odmocníme}) \\ |(u, v)| &< \|u\|\|v\|. \end{aligned}$$

□

Důležitý důsledek Cauchyovy–Bunjakovského–Schwarzovy nerovnosti je následující tvrzení, které je známé jako trojúhelníková nerovnost.

Tvrzení 14.2.2 (Trojúhelníková nerovnost). *Nechť V je prostor se skalárním součinem a $u, v \in V$. Pak*

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

Rovnost nastává právě tehdy, když $\{u, v\}$ je lineárně závislá množina.

Důkaz.

$$\begin{aligned} \|u + v\|^2 &= && (\text{důkaz Lemmatu 14.1.2}) \\ &= \|u\|^2 + 2\operatorname{re}(u, v) + \|v\|^2 \leq && (\operatorname{re}(u, v) \leq |(u, v)|) \\ &\leq \|u\|^2 + 2|(u, v)| + \|v\|^2 \leq && (\text{Tvrzení 14.2.1}) \\ &\leq \|u\|^2 + 2\|u\|\|v\| + \|v\|^2 = \\ &= (\|u\| + \|v\|)^2 \end{aligned}$$

Zbytek důkazu je jednoduché cvičení.

□

14.3. Odchylka vektorů

Pro nenulové vektory u, v můžeme Cauchyovu–Bunjakovského–Schwarzovu nerovnost zapsat ve tvaru

$$\frac{|(u, v)|}{\|u\| \|v\|} \leq 1$$

a v eukleidovském případě

$$-1 \leq \frac{(u, v)}{\|u\| \|v\|} \leq 1.$$

Funkce $\cos$ zúžená na interval $[0, \pi]$ je injektivní a tento interval zobrazuje vzájemně jednoznačně na interval $[-1, 1]$. Pro každou dvojici nenulových vektorů u, v tedy existuje právě jedno reálné číslo $\varphi \in [0, \pi]$ takové, že

$$\cos \varphi = \frac{(u, v)}{\|u\| \|v\|}.$$

Definice 14.3.1. Buďte V eukleidovský prostor a $u, v \in V$ nenulové. *Odchylka* vektorů u, v (nebo *úhel* mezi vektory u, v) je číslo $\varphi \in [0, \pi]$ takové, že

$$\cos \varphi = \frac{(u, v)}{\|u\| \|v\|}.$$

Pro libovolný eukleidovský skalární součin tedy platí

$$(u, v) = \|u\| \|v\| \cos \varphi.$$

Tvrzení 14.3.1 (Kosinová věta). *Buďte V eukleidovský prostor, $u, v \in V$ nenulové a φ úhel mezi nimi. Potom*

$$\|u - v\|^2 = \|u\|^2 + \|v\|^2 - 2\|u\| \|v\| \cos \varphi.$$

Důkaz.

$$\begin{aligned} \|u - v\|^2 &= (u - v, u - v) = (u, u) - 2(u, v) + (v, v) = \\ &= \|u\|^2 + \|v\|^2 - 2\|u\| \|v\| \cos \varphi. \end{aligned}$$

□

14.4. Ortogonalita (kolmost)

Definice 14.4.1. Buď V prostor se skalárním součinem. Vektory $u, v \in V$ jsou *kolmé* (nebo *ortogonální*), jestliže $(u, v) = 0$. Zapisujeme $u \perp v$.

Dva nenulové vektory v eukleidovském prostoru jsou tedy kolmé právě tehdy, když jejich odchylka je $\pi/2$.

Díky tomu, že $(u, v) = \overline{(v, u)}$, kolmost vektorů nezávisí na jejich pořadí. Jelikož pro každý vektor $v \in V$ platí $(v, 0) = 0$, nulový vektor je kolmý ke každému vektoru. Z toho, že $(pu, qv) = p\overline{q}(u, v)$ pro každé $p, q \in P$, vyplývá, že libovolné skalární násobky kolmých vektorů jsou také kolmé.

Definice 14.4.2. Buď V prostor se skalárním součinem. Množina $U \subset V$ je *ortogonální*, jestliže $u \perp v$ pro libovolné různé $u, v \in U$. Ortogonální množina normovaných vektorů je *ortonormální*.

Když v ortogonální množině nenulových vektorů každý vektor vynásobíme převrácenou hodnotou jeho délky (každý vektor znormujeme), dostaneme ortonormální množinu.

Tvrzení 14.4.1. *Každá ortogonální množina nenulových vektorů je lineárně nezávislá.*

Důkaz. Buď $\{v_1, \dots, v_n\}$ ortogonální množina nenulových vektorů. Nechť

$$p^1 v_1 + \dots + p^n v_n = 0.$$

Když pro libovolné $i \in \{1, \dots, n\}$ obě strany této rovnosti skalárně vynásobíme zprava vektorem v_i , dostaneme

$$\begin{aligned} (p^1 v_1 + \dots + p^n v_n, v_i) &= (0, v_i) && \text{(linearita v prvním argumentu)} \\ p^1 (v_1, v_i) + \dots + p^n (v_n, v_i) &= 0 && \text{(kolmost)} \\ p^i (v_i, v_i) &= 0 && (v_i \neq 0 \text{ a } (v_i, v_i) > 0) \\ p^i &= 0. \end{aligned}$$

Takže $p^i = 0$ pro každé $i \in \{1, \dots, n\}$ a množina $\{v_1, \dots, v_n\}$ je lineárně nezávislá. $\square$

Důsledek. *Každá n -prvková ortogonální množina nenulových vektorů v n -rozměrném prostoru je báze tohoto prostoru.*

Příklad. (1) Mějme $\mathbb{R}^n$ se standardním skalárním součinem. Kanonická báze je ortonormální.

(2) Mějme prostor všech spojitých reálných funkcí na intervalu $[0, 2\pi]$ se skalárním součinem

$$(f, g) = \int_0^{2\pi} f(x)g(x)dx.$$

Množina $\{1, \sin x, \cos x, \sin(2x), \cos(2x), \dots\}$ je ortogonální. $\square$

Tvrzení 14.4.2 (Pythagorova věta). *Budť V prostor se skalárním součinem a $u, v \in V$ kolmé. Pak*

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2.$$

Důkaz.

$$\begin{aligned} \|u + v\|^2 &= (u + v, u + v) = \\ &= (u, u) + (u, v) + (v, u) + (v, v) = && (u \perp v) \\ &= (u, u) + (v, v) = \|u\|^2 + \|v\|^2. \end{aligned} \quad \square$$

Cvičení. Buď $\{v_1, \dots, v_n\}$ ortogonální množina. Ukažte, že

$$\|v_1 + \dots + v_n\|^2 = \|v_1\|^2 + \dots + \|v_n\|^2. \quad \square$$

14.5. Souřadnice vzhledem k ortonormální bázi

Tvrzení 14.5.1. *Nechť V je prostor se skalárním součinem, $(e_1, \dots, e_n)$ jeho ortogonální báze a $v \in V$. Pak*

$$v = \frac{(v, e_1)}{(e_1, e_1)} e_1 + \dots + \frac{(v, e_n)}{(e_n, e_n)} e_n,$$

čili i -tá souřadnice vektoru v vzhledem k uvedené bázi je

$$x^i = \frac{(v, e_i)}{(e_i, e_i)} = \frac{(v, e_i)}{\|e_i\|^2}.$$

Je-li $(e_1, \dots, e_n)$ navíc ortonormální báze, pak

$$v = (v, e_1)e_1 + \dots + (v, e_n)e_n,$$

čili i -tá souřadnice vektoru v vzhledem k uvedené bázi je

$$x^i = (v, e_i).$$

Důkaz. Necht $v = x^1 e_1 + \dots + x^n e_n$. Pro každé $i \in \{1, \dots, n\}$

$$\begin{aligned} x^i &= (e_i \neq 0 \text{ a } (e_i, e_i) \neq 0) \\ &= x^i \frac{(e_i, e_i)}{(e_i, e_i)} = ((e_i, e_j) = 0 \text{ pro } i \neq j) \\ &= x^1 \frac{(e_1, e_i)}{(e_i, e_i)} + \dots + x^i \frac{(e_i, e_i)}{(e_i, e_i)} + \dots + x^n \frac{(e_n, e_i)}{(e_i, e_i)} = \\ &= \frac{1}{(e_i, e_i)} (x^1(e_1, e_i) + \dots + x^n(e_n, e_i)) = \\ &= \frac{1}{(e_i, e_i)} (x^1 e_1 + \dots + x^n e_n, e_i) = \\ &= \frac{(v, e_i)}{(e_i, e_i)} = \frac{(v, e_i)}{\|e_i\|^2}. \end{aligned}$$

Pokud $(e_1, \dots, e_n)$ je ortonormální báze, pak zřejmě $x^i = (v, e_i)$. $\square$

Tvrzení 14.5.2. Necht V je prostor se skalárním součinem, $(e_1, \dots, e_n)$ jeho ortonormální báze, $u, v \in V$, $x = (x^1, \dots, x^n)$ souřadnice vektoru u a $y = (y^1, \dots, y^n)$ souřadnice vektoru v vzhledem k uvedené bázi. Potom

$$(u, v) = x^T \bar{y} = x^1 \bar{y}^1 + \dots + x^n \bar{y}^n.$$

Důkaz.

$$\begin{aligned} (u, v) &= \left(\sum_{i=1}^n x^i e_i, \sum_{i=1}^n y^i e_i \right) = \sum_{i=1}^n \sum_{j=1}^n (x^i e_i, y^j e_j) = \\ &= \sum_{i=1}^n \sum_{j=1}^n x^i \bar{y}^j (e_i, e_j) = \sum_{i=1}^n x^i \bar{y}^i. \end{aligned} \quad \square$$

14.6. Kolmost množin

Definice 14.6.1. Buď V prostor se skalárním součinem, $v \in V$ a $M, N \subseteq V$. Vektor v je kolmý na množinu M , jestliže v je kolmý na každý vektor $z \in M$, zapisujeme $v \perp M$. Množina M je kolmá na množinu N , jestliže každý vektor množiny M je kolmý na každý vektor množiny N , zapisujeme $M \perp N$.

Cvičení. V průniku kolmých množin může být jen nulový vektor. $\square$

Například, dvě roviny v $\mathbb{R}^3$ nejsou vzájemně kolmé.

Tvrzení 14.6.1. Buď V prostor se skalárním součinem a $M, N \subseteq V$. Potom $M \perp N$ právě tehdy, když $\llbracket M \rrbracket \perp N$, a to je právě tehdy, když $\llbracket M \rrbracket \perp \llbracket N \rrbracket$.

Důkaz. Předpokládejme, že $M \perp N$. Buď $u \in \llbracket M \rrbracket$ a $v \in N$, čili $u = p^1 u_1 + \dots + p^n u_n$ pro nějaké $n \in \mathbb{N}$, skaláry $p^1, \dots, p^n$ a vektory $u_1, \dots, u_n \in M$. Potom

$$\begin{aligned} (u, v) &= (p^1 u_1 + \dots + p^n u_n, v) = \\ &= p^1 (u_1, v) + \dots + p^n (u_n, v) = 0. \end{aligned}$$

Takže $\llbracket M \rrbracket^\perp \subseteq N$.

Opačná implikace a druhá ekvivalence jsou zřejmé. $\square$

Chceme-li ověřit, zda vektor $v \in V$ je kolmý na podprostor $U \subseteq V$, díky předcházejícímu tvrzení stačí ověřit, zda vektor v je kolmý na všechny vektory z libovolné množiny generátorů podprostoru U .

14.7. Ortogonální doplněk

Definice 14.7.1. Nechť V je prostor se skalárním součinem a $U \subseteq V$. *Ortogonální doplněk* $U^\perp$ množiny U je množina všech vektorů z V kolmých na každý vektor z U , tedy

$$U^\perp = \{v \in V \mid v \perp u \text{ pro všechna } u \in U\}.$$

Množina $U^\perp$ je tedy největší množina kolmá na U .

Tvrzení 14.7.1. *Buď V prostor se skalárním součinem, $U, U_1, U_2 \subseteq V$. Pak*

- (1) *jestliže $U_1 \subseteq U_2$, pak $U_2^\perp \subseteq U_1^\perp$,*
- (2) *$U^\perp = \llbracket U \rrbracket^\perp$,*
- (3) *$U^\perp$ je podprostor V .*

Důkaz. (1) Je-li $U_1 \subseteq U_2$ a $v \in U_2^\perp$, tedy $v \perp U_2$, potom $v \perp U_1$ a $v \in U_1^\perp$.

(2) Pro $v \in V$ podle Tvrzení 14.6.1 $v \in U^\perp$ právě tehdy, když $v \in \llbracket U \rrbracket^\perp$.

(3) Zřejmě $0 \in U^\perp$. Pro libovolné $v_1, v_2 \in U^\perp$ a $u \in U$ platí $(v_1 + v_2, u) = (v_1, u) + (v_2, u) = 0$, takže $v_1 + v_2 \in U^\perp$. Pro libovolný skalár p , $v \in U^\perp$ a $u \in U$ platí $(pv, u) = p(v, u) = 0$, takže $pv \in U^\perp$. $\square$

14.8. Ortogonální projekce

Definice 14.8.1. Buď V prostor se skalárním součinem, $v \in V$ a U podprostor V . Vektor $u \in U$ je *ortogonální projekce (kolmý průmět) vektoru v do podprostoru U* , jestliže $(v - u) \perp U$, tedy $v - u \in U^\perp$. Označujeme $u = v_U$ nebo $u = \text{pr}_U(v)$.

Z definice vyplývá, že je-li $v \in U$, potom $v_U = v$.

Tvrzení 14.8.1. *Buď V prostor se skalárním součinem, U podprostor V a $v \in V$. Pak pro každý vektor $u \in U$, $u \neq v_U$, platí*

$$\|v - v_U\| < \|v - u\|.$$

Ortogonální projekce vektoru do podprostoru je určena jednoznačně, pokud existuje.

Důkaz. Podle definice $v_U \in U$ a $(v - v_U) \perp U$, takže pro každé $u \in U$ platí $(v - v_U) \perp (v_U - u)$. Pro $u \neq v_U$ navíc

$$\begin{aligned} \|v - v_U\|^2 &< & (\|v_U - u\| > 0) \\ &< \|v - v_U\|^2 + \|v_U - u\|^2 = & (\text{Pythagorova věta}) \\ &= \|(v - v_U) + (v_U - u)\|^2 = \\ &= \|v - u\|^2. \end{aligned}$$

Nechť $u_1, u_2 \in U$ jsou ortogonální projekce vektoru v do podprostoru U . Předpokládejme, že $u_1 \neq u_2$. Potom podle právě dokázaného

$$\|v - u_1\| < \|v - u_2\| \quad \text{a zároveň} \quad \|v - u_2\| < \|v - u_1\|.$$

Dostáváme spor, takže $u_1 = u_2$ a ortogonální projekce je tedy určena jednoznačně. $\square$

Tvrzení 14.8.2. *Buďte V prostor se skalárním součinem, U jeho konečněrozměrný podprostor a $(e_1, \dots, e_m)$ ortogonální báze podprostoru U . Pak pro každé $v \in V$ platí*

$$\text{pr}_U(v) = \frac{(v, e_1)}{(e_1, e_1)}e_1 + \dots + \frac{(v, e_m)}{(e_m, e_m)}e_m.$$

Je-li $(e_1, \dots, e_m)$ navíc ortonormální báze, pak

$$\text{pr}_U(v) = (v, e_1)e_1 + \dots + (v, e_m)e_m.$$

Důkaz. Vektor $u = u^1e_1 + \dots + u^me_m \in U$ je ortogonální projekce vektoru v do podprostoru $U = \llbracket e_1, \dots, e_m \rrbracket$ právě tehdy, když vektor $v - u$ je kolmý ke každému vektoru z U , což je právě tehdy, když $v - u$ je kolmý ke každému e_i , to je právě tehdy, když pro každé $i \in \{1, \dots, m\}$

$$\begin{aligned} 0 &= (v - u, e_i) = (v, e_i) - (u, e_i) = \\ &= (v, e_i) - (u^1e_1 + \dots + u^me_m, e_i) = \\ &= (v, e_i) - u^1(e_1, e_i) - \dots - u^m(e_m, e_i) = \\ &= (v, e_i) - u^i(e_i, e_i) \end{aligned}$$

a to je právě tehdy, když $u^i = \frac{(v, e_i)}{(e_i, e_i)}$, jelikož $(e_i, e_i) \neq 0$.

Pokud $(e_1, \dots, e_n)$ je ortonormální báze, pak zřejmě $u^i = (v, e_i)$. $\square$

14.9. Gramova-Schmidtova ortogonalizace

Tvrzení 14.9.1. *V každém konečněrozměrném prostoru se skalárním součinem existuje ortonormální báze.*

Důkaz. Existenci ortonormální báze dokážeme pomocí *Gramovy-Schmidtovy ortogonalizace*.

Buďte V konečněrozměrný prostor se skalárním součinem a $(v_1, \dots, v_n)$ jeho báze. Ukažme, že existuje jeho ortogonální báze.

- (1) Položme $e_1 = v_1$. Potom vektor e_1 je nenulový, $\{e_1\}$ je lineárně nezávislá množina a $\llbracket e_1 \rrbracket = \llbracket v_1 \rrbracket$.
- (2) Postupně pro $k = 1, \dots, n - 1$ předpokládejme, že máme $\{e_1, \dots, e_k\}$ ortogonální množinu nenulových vektorů (tedy lineárně nezávislou množinu) takovou, že $\llbracket e_1, \dots, e_k \rrbracket = \llbracket v_1, \dots, v_k \rrbracket$. Označme $U_k = \llbracket e_1, \dots, e_k \rrbracket$. Vektor e_{k+1} získáme tak, že od vektoru v_{k+1} odečteme jeho ortogonální projekci do podprostoru U_k . Tedy

$$e_{k+1} = v_{k+1} - \text{pr}_{U_k}(v_{k+1}) = v_{k+1} - \sum_{i=1}^k \frac{(v_{k+1}, e_i)}{(e_i, e_i)}e_i.$$

Podle definice ortogonální projekce vektor e_{k+1} je kolmý na U_k , tedy na všechny vektory z U_k , včetně $e_1, \dots, e_k$. Množina $\{e_1, \dots, e_k, e_{k+1}\}$ je tedy ortogonální.

Jelikož báze je lineárně nezávislá, vektor v_{k+1} není prvkem podprostoru U_k a nerovná se tedy své ortogonální projekci $\text{pr}_{U_k}(v_{k+1})$ do tohoto podprostoru. Proto e_{k+1} je nenulový vektor a množina $\{e_1, \dots, e_k, e_{k+1}\}$ je lineárně nezávislá.

K tomu, $\llbracket e_1, \dots, e_{k+1} \rrbracket = \llbracket v_1, \dots, v_{k+1} \rrbracket$. Platí $e_1 = v_1$ a $e_i, i \in \{2, \dots, k+1\}$, je lineární kombinace vektorů $e_1, \dots, e_{i-1}, v_i$, proto $\llbracket e_1, \dots, e_{k+1} \rrbracket \subseteq \llbracket v_1, \dots, v_{k+1} \rrbracket$. Na druhou stranu, v_i pro $i \in \{1, \dots, k+1\}$ je lineární kombinace vektorů $e_1, \dots, e_i$, proto $\llbracket v_1, \dots, v_{k+1} \rrbracket \subseteq \llbracket e_1, \dots, e_{k+1} \rrbracket$.

Takže pro každé $k \in \{1, \dots, n\}$ ($e_1, \dots, e_k$) je ortogonální báze prostoru U_k a $U_n = V$.

Nakonec,

$$\left(\frac{e_1}{\|e_1\|}, \dots, \frac{e_n}{\|e_n\|} \right)$$

je ortonormální báze prostoru V . □

V předchozím důkazu je možné vždy po získání e_k tento vektor normovat a dostat tak ortonormální bázi prostoru U_k . V takovém případě se zjednoduší výpočet ortogonální projekce do podprostoru U_k a tedy i výpočet vektoru e_{k+1} .

14.10. Vlastnosti ortogonálního doplňku

Tvrzení 14.10.1. *Nechť V je prostor se skalárním součinem a U jeho konečněrozměrný podprostor. Pak*

- (1) $U^{\perp\perp} = U$,
- (2) $V = U \dot{+} U^{\perp}$,
- (3) *je-li V konečněrozměrný, potom $\dim U^{\perp} = \dim V - \dim U$.*

Důkaz. (1) Každý vektor z U je kolmý na $U^{\perp}$, takže $U \subseteq U^{\perp\perp}$. Buď $v \in U^{\perp\perp}$. Tedy v je kolmý na každý vektor z $U^{\perp}$. Jelikož podprostor U je konečněrozměrný, existuje v_U . Podle definice ortogonální projekce $v_U \in U$ a $v - v_U \in U^{\perp}$, čili $v_U \perp (v - v_U)$ a zároveň $v \perp (v - v_U)$. Takže

$$\|v - v_U\|^2 = (v - v_U, v - v_U) = (v, v - v_U) - (v_U, v - v_U) = 0 - 0 = 0,$$

proto $v = v_U \in U$, čili $U^{\perp\perp} \subseteq U$ a celkově $U^{\perp\perp} = U$.

(2) Opět, podprostor U je konečněrozměrný, takže ke každému vektoru $v \in V$ existuje jeho ortogonální projekce do U , přičemž $v_U \in U$, $v - v_U \in U^{\perp}$ a $v = v_U + (v - v_U)$. Takže $V = U + U^{\perp}$. Jelikož U a $U^{\perp}$ jsou vzájemně kolmé, v jejich průniku je jen nulový vektor. Z toho vyplývá, že $V = U \dot{+} U^{\perp}$.

(3) Z předchozího bodu a Tvrzení 10.3.2 dostaneme $\dim V = \dim U + \dim U^{\perp}$. □

Tvrzení 14.10.2. *Nechť V je prostor se skalárním součinem, U_1, U_2 jeho konečněrozměrné podprostory. Potom*

$$(U_1 + U_2)^{\perp} = U_1^{\perp} \cap U_2^{\perp} \subseteq U_1^{\perp} + U_2^{\perp} = (U_1 \cap U_2)^{\perp}.$$

Důkaz.

$$\begin{aligned} U_1, U_2 \subseteq U_1 + U_2 &\Rightarrow (U_1 + U_2)^{\perp} \subseteq U_1^{\perp}, U_2^{\perp} \Rightarrow (U_1 + U_2)^{\perp} \subseteq U_1^{\perp} \cap U_2^{\perp} \\ U_1 \cap U_2 \subseteq U_1, U_2 &\Rightarrow U_1^{\perp}, U_2^{\perp} \subseteq (U_1 \cap U_2)^{\perp} \Rightarrow U_1^{\perp} + U_2^{\perp} \subseteq (U_1 \cap U_2)^{\perp} \end{aligned}$$

V právě dokázaných vztazích místo U_1, U_2 použijeme $U_1^{\perp}, U_2^{\perp}$ a dostaneme

$$\begin{aligned} (U_1^{\perp} + U_2^{\perp})^{\perp} &\subseteq U_1^{\perp\perp} \cap U_2^{\perp\perp} = U_1 \cap U_2 \Rightarrow (U_1 \cap U_2)^{\perp} \subseteq U_1^{\perp} + U_2^{\perp} \\ U_1 + U_2 &= U_1^{\perp\perp} + U_2^{\perp\perp} \subseteq (U_1^{\perp} \cap U_2^{\perp})^{\perp} \Rightarrow U_1^{\perp} \cap U_2^{\perp} \subseteq (U_1 + U_2)^{\perp} \end{aligned}$$

Nakonec, zřejmě

$$U_1^{\perp} \cap U_2^{\perp} \subseteq U_1^{\perp} + U_2^{\perp}. \quad \square$$

Cvičení. Najděte V, U_1, U_2 takové, že $(U_1 \cap U_2)^{\perp} \not\subseteq U_1^{\perp} \cap U_2^{\perp}$. □

14.11. Shodnosti—ortogonální a unitární transformace a matice

14.11.1. Shodnosti—ortogonální a unitární transformace

Shodnost je lineární transformace, která zachovává skalární součin.

Definice 14.11.1. Buď V prostor se skalárním součinem. Lineární transformace $f: V \rightarrow V$ je *shodnost*, jestliže pro každé $u, v \in V$

$$(f(u), f(v)) = (u, v).$$

V eukleidovském případě se shodnost nazývá také *ortogonální transformace*, v hermiteovském případě se shodnost nazývá také *unitární transformace*.

Když shodnost zachovává skalární součin, zachovává i normu, kolmost a v eukleidovském případě i odchylku vektorů, což jsou pojmy zavedené pomocí skalárního součinu. Platí i některé opačné implikace.

Tvrzení 14.11.1. Buď f lineární transformace prostoru V se skalárním součinem. Následující tvrzení jsou ekvivalentní:

- (1) f je shodnost;
- (2) f zachovává délky vektorů, tj. $\|f(v)\| = \|v\|$ pro každé $v \in V$;
- (3) f zobrazuje jednotkové vektory na jednotkové vektory;
- (4) f zachovává ortonormalitu, tj. $f(U)$ je ortonormální množina pro každou ortonormální množinu U .

Důkaz. (1) $\Rightarrow$ (2) Je-li f shodnost, pro každé $v \in V$

$$\|f(v)\| = \sqrt{(f(v), f(v))} = \sqrt{(v, v)} = \|v\|.$$

(2) $\Rightarrow$ (1) Předpokládejme, že f zachovává délky vektorů. Potom

$$\begin{aligned} \operatorname{re}(f(u), f(v)) &= && \text{(Lemma 14.1.2)} \\ &= \frac{1}{2}(\|f(u) + f(v)\|^2 - \|f(u)\|^2 - \|f(v)\|^2) = && \text{(linearita } f) \\ &= \frac{1}{2}(\|f(u + v)\|^2 - \|f(u)\|^2 - \|f(v)\|^2) = && (f \text{ zachovává délky}) \\ &= \frac{1}{2}(\|u + v\|^2 - \|u\|^2 - \|v\|^2) = && \text{(Lemma 14.1.2)} \\ &= \operatorname{re}(u, v) \end{aligned}$$

$$\begin{aligned} \operatorname{im}(f(u), f(v)) &= && \text{(Lemma 14.1.2)} \\ &= \frac{1}{2}(\|f(u) + if(v)\|^2 - \|f(u)\|^2 - \|f(v)\|^2) = && \text{(linearita } f) \\ &= \frac{1}{2}(\|f(u + iv)\|^2 - \|f(u)\|^2 - \|f(v)\|^2) = && (f \text{ zachovává délky}) \\ &= \frac{1}{2}(\|u + iv\|^2 - \|u\|^2 - \|v\|^2) = && \text{(Lemma 14.1.2)} \\ &= \operatorname{im}(u, v). \end{aligned}$$

Tedy,

$$(f(u), f(v)) = (u, v).$$

(2) $\Rightarrow$ (3) Zřejmé.

(3) $\Rightarrow$ (2) Necht f zobrazuje jednotkové vektory na jednotkové vektory. Jelikož $f(0) = 0$, $\|f(0)\| = \|0\|$. Buď $v \in V$, $v \neq 0$. Potom $\|v\| \neq 0$ a

$$\begin{aligned}\|f(v)\| &= \left\| f\left(\frac{\|v\|}{\|v\|}v\right) \right\| = & (f \text{ je lineární}) \\ &= \left\| \|v\| f\left(\frac{v}{\|v\|}\right) \right\| = & (\text{Lemma 14.1.1}) \\ &= \|v\| \left\| f\left(\frac{v}{\|v\|}\right) \right\| = & \left(\left\| \frac{v}{\|v\|} \right\| = 1 \Rightarrow \left\| f\left(\frac{v}{\|v\|}\right) \right\| = 1 \right) \\ &= \|v\|.\end{aligned}$$

(1) $\Rightarrow$ (4) Necht f je shodnost. Buď U ortonormální množina. Potom pro $f(u), f(v) \in f(U)$, $f(u) \neq f(v)$, platí

$$(f(u), f(v)) = (u, v) = 0 \quad \text{a} \quad \|f(u)\| = \|u\| = 1.$$

Čili, $f(U)$ je ortonormální množina.

(4) $\Rightarrow$ (3) Zřejmé. □

Příklad. (1) V eukleidovském prostoru E^2 : rotace kolem nulového vektoru, osová souměrnost.

(2) V eukleidovském prostoru E^3 : rotace kolem osy, rovinová souměrnost (zrcadlení), středová souměrnost. □

Na druhou stranu, když lineární transformace zachovává kolmost nebo zachovává odchylky vektorů, ještě to neznamená, že to je shodnost.

Cvičení. Uveďte příklady zobrazení, která zachovávají kolmost nebo zachovávají odchylky vektorů, ale nejsou to shodnosti. □

Tvrzení 14.11.2. Buď V konečněrozměrný prostor se skalárním součinem, $(e_1, \dots, e_n)$ jeho ortonormální báze a f jeho lineární transformace. Pak f je shodnost právě tehdy, když $(f(e_1), \dots, f(e_n))$ je ortonormální báze V .

Důkaz. Implikace „ $\Rightarrow$ “ je snadné cvičení.

Necht $(f(e_1), \dots, f(e_n))$ je ortonormální báze. Buďte $u, v \in V$, $u = \sum x^i e_i$, $v = \sum y^i e_i$, $x = (x^1, \dots, x^n)$ a $y = (y^1, \dots, y^n)$. Potom $f(u) = \sum x^i f(e_i)$, $f(v) = \sum y^i f(e_i)$ a podle Tvrzení 14.5.2

$$(u, v) = x^T \bar{y} = (f(u), f(v)). \quad \square$$

Tvrzení 14.11.3. Každá shodnost konečněrozměrného vektorového prostoru se skalárním součinem je izomorfismus.

Důkaz. Shodnost je lineární zobrazení. Je tedy potřeba dokázat již jen bijektivnost. Buď $u \in \text{Ker } f$, tedy $f(u) = 0$. Potom $\|u\| = \|f(u)\| = 0$ a $u = 0$. Takže, $\text{Ker } f = \{0\}$ a f je injektivní.

Dále $\dim \text{Im } f = \dim V - \dim \text{Ker } f = \dim V$, proto $\text{Im } f = V$ a f je surjektivní. □

Tvrzení 14.11.4. Složení shodností je shodnost.

Důkaz. Cvičení. □

14.11.2. Ortogonální a unitární matice

Definice 14.11.2. Čtvercová matice A nad $\mathbb{R}$ (resp. $\mathbb{C}$) typu $n \times n$ je *ortogonální* (resp. *unitární*), jestliže $(Au, Av) = (u, v)$ pro každé $u, v \in \mathbb{R}^n$ (resp. $\mathbb{C}^n$), kde $(\ , \)$ je standardní skalární součin na $\mathbb{R}^n$ (resp. $\mathbb{C}^n$).

Připomeňme značení: Pro matici $A = (A_j^i)$ označujeme $\bar{A} = (\overline{A_j^i})$.

Tvrzení 14.11.5. *Bud' A čtvercová matice nad $\mathbb{R}$ (resp. $\mathbb{C}$) typu $n \times n$. Následující tvrzení jsou ekvivalentní:*

- (1) A je ortogonální (resp. unitární);
- (2) množina sloupků matice A je ortonormální v $\mathbb{R}^n$ (resp. $\mathbb{C}^n$) se standardním skalárním součinem;
- (3) $A^T A = E$ (resp. $\overline{A}^T A = E$);
- (4) $AA^T = E$ (resp. $A\overline{A}^T = E$);
- (5) množina řádků matice A je ortonormální v $\mathbb{R}^n$ (resp. $\mathbb{C}^n$) se standardním skalárním součinem;
- (6) A^T je ortogonální (resp. unitární).

Důkaz. Jen pro reálný případ.

(1) $\Rightarrow$ (2) Bud' $(e_1, \dots, e_n)$ kanonická báze $\mathbb{R}^n$. Potom $Ae_i = A_i^\circ$ je i -tý sloupek matice A a platí

$$(A_i^\circ, A_j^\circ) = (Ae_i, Ae_j) = (e_i, e_j) = \delta_i^j,$$

takže množina sloupků matice A je ortonormální.

(2) $\Leftrightarrow$ (3)

$$(A^T A)_j^i = \sum_{k=1}^n (A^T)_k^i A_j^k = \sum_{k=1}^n A_i^k A_j^k = (A_i^\circ, A_j^\circ).$$

(3) $\Rightarrow$ (1) Jestliže $A^T A = E$, potom pro každé $u, v \in \mathbb{R}^n$

$$(Au, Av) = (Au)^T (Av) = u^T A^T Av = u^T E v = u^T v = (u, v).$$

(3) $\Leftrightarrow$ (4) Jestliže $A^T A = E$, potom $A^T = A^{-1}$ a $AA^T = AA^{-1} = E$. Obdobně druhá implikace.

(4) $\Leftrightarrow$ (5)

$$(AA^T)_j^i = \sum_{k=1}^n A_k^i (A^T)_j^k = \sum_{k=1}^n A_k^i A_k^j = (A_i^\circ, A_j^\circ).$$

(4) $\Rightarrow$ (6) Jestliže $AA^T = E$, potom pro každé $u, v \in \mathbb{R}^n$

$$(A^T u, A^T v) = (A^T u)^T (A^T v) = u^T AA^T v = u^T E v = u^T v = (u, v).$$

(6) $\Rightarrow$ (5) Bud' $(e_1, \dots, e_n)$ kanonická báze $\mathbb{R}^n$. Potom $A^T e_i = (A^T)_i^\circ = A_i^\circ$ je i -tý řádek matice A a platí

$$(A_i^\circ, A_j^\circ) = (A^T e_i, A^T e_j) = (e_i, e_j) = \delta_i^j,$$

takže množina řádků matice A je ortonormální. $\square$

Důsledek. *Je-li A ortogonální (resp. unitární) matice, pak je regulární a $A^{-1} = A^T$ (resp. $A^{-1} = \overline{A}^T$).*

Důkaz. Je-li A ortogonální (resp. unitární) matice, pak podle Tvrzení 14.11.5 $A^T A = E$ (resp. $\overline{A}^T A = E$), takže $A^T = A^{-1}$ (resp. $\overline{A}^T = A^{-1}$). $\square$

Tvrzení 14.11.6. *Je-li A ortogonální (resp. unitární) matice, pak $\det A = \pm 1$ (resp. $|\det A| = 1$).*

Důkaz.

$$1 = \det E = \det(\overline{A}^T A) = \det \overline{A}^T \det A = \overline{\det A} \det A = |\det A|^2$$

Je-li $\det A \in \mathbb{R}$, potom $\det A = \pm 1$. $\square$

Cvičení. Dokažte, že $\det \overline{A}^T = \overline{\det A}$. $\square$

Tvrzení 14.11.7. *Součin ortogonálních (resp. unitárních) matic je ortogonální (resp. unitární) matice.*

Důkaz. Buďte A, B ortogonální (resp. unitární) matice, čili $A^\top A = E$ a $B^\top B = E$ (resp. $\overline{A}^\top A = E$ a $\overline{B}^\top B = E$). Potom

$$(AB)^\top AB = B^\top A^\top AB = B^\top B = E \quad (\text{resp. } \overline{AB}^\top AB = \overline{B}^\top \overline{A}^\top AB = \overline{B}^\top B = E). \square$$

14.11.3. Ortogonální transformace a ortogonální matice

Tvrzení 14.11.8. *Buď f lineární transformace konečněrozměrného prostoru se skalárním součinem a A její matice vzhledem k ortonormální bázi. Pak f je shodnost právě tehdy, když matice A je ortogonální.*

Důkaz. Buď V prostor se skalárním součinem, $(e_1, \dots, e_n)$ jeho ortonormální báze. Sloupky A_i° matice A jsou souřadnice vektorů $f(e_i)$ vzhledem k bázi $(e_1, \dots, e_n)$, čili

$$f(e_i) = \sum_{k=1}^n A_i^k e_k.$$

Podle Tvrzení 14.11.2 f je shodnost právě tehdy, když $(f(e_1), \dots, f(e_n))$ je ortonormální báze, a to je právě tehdy, když pro každé $i, j \in \{1, \dots, n\}$

$$(f(e_i), f(e_j)) = \delta_i^j, \text{ kde } \delta_j^i \text{ je Kroneckerovo delta.}$$

Ale

$$\begin{aligned} (f(e_i), f(e_j)) &= \left(\sum_{k=1}^n A_i^k e_k, \sum_{l=1}^n A_j^l e_l \right) = \sum_{k=1}^n \sum_{l=1}^n A_i^k \overline{A_j^l} (e_k, e_l) = \\ &= \sum_{k=1}^n \sum_{l=1}^n A_i^k \overline{A_j^l} \delta_k^l = \sum_{k=1}^n A_i^k \overline{A_j^k} = \sum_{k=1}^n A_i^k (\overline{A}^\top)_k^j = \\ &= (\overline{A}^\top A)_i^j, \end{aligned}$$

čili f je shodnost právě tehdy, když $\overline{A}^\top A = E$, tedy když A je ortogonální. $\square$

14.11.4. Matice přechodu mezi ortonormálními bázemi

Tvrzení 14.11.9. *Matice přechodu od ortonormální báze k ortonormální bázi prostoru se skalárním součinem je ortogonální (resp. unitární).*

Důkaz. Buď V prostor se skalárním součinem, $\mathfrak{e} = (e_1, \dots, e_n)$ a $\mathfrak{f} = (f_1, \dots, f_n)$ jeho ortonormální báze, Q matice přechodu od báze $\mathfrak{e}$ k bázi $\mathfrak{f}$. Podle Tvrzení 14.5.1

$$e_i = \sum_{k=1}^n (e_i, f_k) f_k, \quad \text{čili} \quad Q_i^k = (e_i, f_k).$$

Potom

$$\begin{aligned} (\overline{Q}^\top Q)_j^i &= \sum_{k=1}^n (\overline{Q}^\top)_j^i Q_k^k = \sum_{k=1}^n \overline{Q}_i^k Q_j^k = \sum_{k=1}^n \overline{(e_i, f_k)} (e_j, f_k) = \sum_{k=1}^n (e_j, (e_i, f_k) f_k) = \\ &= \left(e_j, \sum_{k=1}^n (e_i, f_k) f_k \right) = (e_j, e_i) = \delta_j^i, \end{aligned}$$

takže

$$\overline{Q}^\top Q = E \quad \text{a matice } Q \text{ je ortogonální (resp. unitární).} \quad \square$$

Důsledek. *Bud' Q matice přechodu od ortonormální báze k ortonormální bázi eukleidovského prostoru. Potom*

$$\det Q = \begin{cases} 1, & \text{jestliže uvedené báze mají stejnou orientaci,} \\ -1, & \text{jestliže uvedené báze nemají stejnou orientaci.} \end{cases}$$

Důkaz. Tvrzení vyplývá z Tvrzení 14.11.9 a 14.11.6. □

15. BILINEÁRNÍ A KVADRATICKÉ FORMY

V celé kapitole $P = \mathbb{R}$ nebo $P = \mathbb{C}$ a vektorové prostory jsou nad P .

15.1. Bilineární formy

Definice 15.1.1. Buď V vektorový prostor nad P , kde $P = \mathbb{R}$ nebo $P = \mathbb{C}$. *Bilineární forma* na prostoru V je zobrazení $\beta: V \times V \rightarrow P$ takové, že pro libovolné $u, v, w \in V$ a $a \in P$

$$\begin{aligned}\beta(u + v, w) &= \beta(u, w) + \beta(v, w), & \beta(au, w) &= a\beta(u, w), \\ \beta(u, v + w) &= \beta(u, v) + \beta(u, w), & \beta(u, aw) &= a\beta(u, w),\end{aligned}$$

(linearita v prvním a druhém argumentu).

Příklad. (1) Eukleidovský skalární součin je bilineární forma.

(2) Zobrazení $\beta: \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$,

$$\beta\left(\begin{pmatrix} x^1 \\ x^2 \end{pmatrix}, \begin{pmatrix} y^1 \\ y^2 \end{pmatrix}\right) = \det \begin{pmatrix} x^1 & y^1 \\ x^2 & y^2 \end{pmatrix}$$

je bilineární forma na $\mathbb{R}^2$.

(3) Buď B čtvercová matice typu $n \times n$ nad $\mathbb{R}$. Potom zobrazení $\beta_B: \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$,

$$\beta_B(x, y) = x^T B y = \sum_{i=1}^n x^i \sum_{j=1}^n B_j^i y^j = \sum_{i=1}^n \sum_{j=1}^n B_j^i x^i y^j$$

je bilineární forma na $\mathbb{R}^n$.

Například, pro

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

$$\beta_B(x, y) = x^T B y = \begin{pmatrix} x^1 & x^2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} y^1 \\ y^2 \end{pmatrix} = x^1 y^1 + 2x^1 y^2 + 3x^2 y^1 + 4x^2 y^2. \quad \square$$

15.2. Matice bilineární formy

Definice 15.2.1. Buď V n -rozměrný vektorový prostor nad P , $(v_1, \dots, v_n)$ jeho báze a β bilineární forma na V . Matice, která v i -tém řádku a j -tém sloupku má $\beta(v_i, v_j)$, je *matice bilineární formy β vzhledem k bázi $(v_1, \dots, v_n)$* .

Tvrzení 15.2.1. Buď V n -rozměrný vektorový prostor nad P , $\mathbf{v} = (v_1, \dots, v_n)$ jeho báze, $u, v \in V$, $(x^1, \dots, x^n)$, resp. $(y^1, \dots, y^n)$ jejich souřadnice vzhledem k bázi $\mathbf{v}$, β bilineární forma na V a B matice formy β vzhledem k bázi $\mathbf{v}$. Potom

$$\beta(u, v) = x^T B y = \sum_{i=1}^n \sum_{j=1}^n B_j^i x^i y^j.$$

Důkaz.

$$\begin{aligned}\beta(u, v) &= \beta \left(\sum_{i=1}^n x^i v_i, \sum_{j=1}^n y^j v_j \right) = \sum_{i=1}^n \sum_{j=1}^n x^i y^j \beta(v_i, v_j) = \\ &= \sum_{i=1}^n \sum_{j=1}^n x^i y^j B_j^i = x^T B y.\end{aligned}\quad \square$$

Tvrzení 15.2.2. *Bud' V n -rozměrný vektorový prostor nad P , $\mathbf{v} = (v_1, \dots, v_n)$ jeho báze a B matice typu $n \times n$ nad P . Zobrazení $\beta: V \times V \rightarrow P$,*

$$\beta(u, v) = x^T B y \quad \text{pro každé } u, v \in V,$$

kde x, y jsou souřadnice vektorů u , resp. v vzhledem k bázi $\mathbf{v}$, je bilineární forma na V a její matice vzhledem k bázi $\mathbf{v}$ je B .

Důkaz. Pro libovolné $u, v, w \in V$, jejich souřadnice x, y, z vzhledem k bázi $\mathbf{v}$ a $a \in P$ platí

$$\begin{aligned}\beta(u + v, w) &= (x + y)^T B z = (x^T + y^T) B z = x^T B z + y^T B z = \\ &= \beta(u, w) + \beta(v, w) \\ \beta(a u, v) &= (a x)^T B y = a x^T B y = \\ &= a \beta(u, v).\end{aligned}$$

Linearita ve druhém argumentu se ověří obdobně (cvičení).

Dále,

$$\beta(v_i, v_j) = e_i^T B e_j = B_j^i,$$

kde e_i, e_j jsou i -tý a j -tý vektory kanonické báze $\mathbb{R}^n$, čili B je matice bilineární formy β vzhledem k bázi $\mathbf{v}$. $\square$

Obdobně jako u matice lineární transformace změnou báze se mění i matice bilineární formy.

Tvrzení 15.2.3. *Bud' V n -rozměrný vektorový prostor, $\mathbf{u} = (u_1, \dots, u_n)$, $\mathbf{v} = (v_1, \dots, v_n)$ jeho báze, $Q_{\mathbf{vu}}$ matice přechodu od báze $\mathbf{v}$ k bázi $\mathbf{u}$, β bilineární forma na V , $B_{\mathbf{u}}$ matice formy β vzhledem k bázi $\mathbf{u}$ a $B_{\mathbf{v}}$ matice formy β vzhledem k bázi $\mathbf{v}$. Potom*

$$(B_{\mathbf{v}})_j^i = \sum_{k=1}^n \sum_{l=1}^n (Q_{\mathbf{vu}})_i^k (Q_{\mathbf{vu}})_j^l (B_{\mathbf{u}})_l^k,$$

a

$$B_{\mathbf{v}} = Q_{\mathbf{vu}}^T B_{\mathbf{u}} Q_{\mathbf{vu}}.$$

Důkaz. Pro přehlednost zápisu označme $Q = Q_{\mathbf{vu}}$. Potom

$$v_i = \sum_{k=1}^n Q_i^k u_k \quad \text{a} \quad v_j = \sum_{l=1}^n Q_j^l u_l,$$

takže

$$\begin{aligned}(B_{\mathbf{v}})_j^i &= \beta(v_i, v_j) = \beta \left(\sum_{k=1}^n Q_i^k u_k, \sum_{l=1}^n Q_j^l u_l \right) = \\ &= \sum_{k=1}^n \sum_{l=1}^n Q_i^k Q_j^l \beta(u_k, u_l) = \sum_{k=1}^n \sum_{l=1}^n Q_i^k Q_j^l (B_{\mathbf{u}})_l^k = \\ &= \sum_{k=1}^n \sum_{l=1}^n (Q^T)_k^i (B_{\mathbf{u}})_l^k Q_j^l = (Q^T B_{\mathbf{u}} Q)_j^i\end{aligned}\quad \square$$

Cvičení. Dokažte, že $B_u = Q_{uv}^T B_v Q_{uv}$. □

Definice 15.2.2. Matice A, B jsou *kongruentní*, jestliže existuje regulární matice Q taková, že $A = Q^T B Q$.

Je-li Q ortogonální matice, tedy $Q^T = Q^{-1}$, potom jsou matice A, B podobné i kongruentní.

Kongruentní matice vyjadřují jednu a tutéž bilineární formu v různých bázích.

Tvrzení 15.2.4. *Kongruentnost čtvercových matic je relace ekvivalence.*

Důkaz. Cvičení. □

Tvrzení 15.2.5. *Matice kongruentní se symetrickou (antisymetrickou) maticí je symetrická (antisymetrická).*

Důkaz. Cvičení. □

Tvrzení 15.2.6. *Řádkovou elementární úpravou čtvercové matice a stejnou sloupkovou elementární úpravou takto získané matice, dostaneme matici kongruentní s původní maticí.*

Důkaz. Buď A čtvercová matice. Řádkovou elementární úpravou matice A získáme matici QA , kde Q je vhodná elementární matice. Stejnou sloupkovou elementární úpravou matice A získáme matici AQ^T . Těmito dvěma úpravami tedy dostaneme matici QAQ^T , což je matice kongruentní s maticí A , protože elementární matice jsou regulární. □

15.3. Symetrické a antisymetrické bilineární formy

Definice 15.3.1. Bilineární forma β na vektorovém prostoru V je

- *symetrická*, jestliže $\beta(u, v) = \beta(v, u)$ pro libovolné $u, v \in V$,
- *antisymetrická*, jestliže $\beta(u, v) = -\beta(v, u)$ pro libovolné $u, v \in V$.

Příklad. (1) Eukleidovský skalární součin je symetrická bilineární forma.

(2) Zobrazení $\beta: \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$,

$$\beta \left(\begin{pmatrix} x^1 \\ x^2 \end{pmatrix}, \begin{pmatrix} y^1 \\ y^2 \end{pmatrix} \right) = \det \begin{pmatrix} x^1 & y^1 \\ x^2 & y^2 \end{pmatrix}$$

je antisymetrická bilineární forma na $\mathbb{R}^2$. □

Tvrzení 15.3.1. *Buď β bilineární forma na konečněrozměrném vektorovém prostoru. Potom*

- (1) *β je symetrická právě tehdy, když její matice vzhledem k libovolné bázi je symetrická,*
- (2) *β je antisymetrická právě tehdy, když její matice vzhledem k libovolné bázi je antisymetrická.*

Důkaz. Buď V n -rozměrný vektorový prostor nad P , $(v_1, \dots, v_n)$ jeho báze, β bilineární forma na V a B matice formy β vzhledem k bázi $(v_1, \dots, v_n)$.

- (1) Je-li β symetrická, pak $B_j^i = \beta(v_i, v_j) = \beta(v_j, v_i) = B_i^j$, takže B je symetrická. Je-li B symetrická, pak pro libovolné $u, v \in V$ a jejich souřadnice x , resp. y platí

$$\begin{aligned}\beta(u, v) &= x^T B y = & (B = B^T) \\ &= x^T B^T y = & (x^T B^T y \text{ je matice typu } 1 \times 1) \\ &= (x^T B^T y)^T = \\ &= y^T B x = \\ &= \beta(v, u),\end{aligned}$$

takže β je symetrická.

- (2) Druhou část tvrzení lze dokázat obdobně. $\square$

Tvrzení 15.3.2. Buď V vektorový prostor nad P a β bilineární forma na V . Potom existuje právě jedna symetrická bilineární forma β_s a právě jedna antisymetrická bilineární forma β_a takové, že $\beta = \beta_s + \beta_a$. A to sice

$$\beta_s(u, v) = \frac{1}{2}(\beta(u, v) + \beta(v, u)) \quad a \quad \beta_a(u, v) = \frac{1}{2}(\beta(u, v) - \beta(v, u)).$$

Důkaz. Bilineární forma β_s definovaná vztahem

$$\beta_s(u, v) = \frac{1}{2}(\beta(u, v) + \beta(v, u))$$

je symetrická (cvičení), bilineární forma β_a definovaná vztahem

$$\beta_a(u, v) = \frac{1}{2}(\beta(u, v) - \beta(v, u))$$

je antisymetrická (cvičení) a

$$\beta(u, v) = \beta_s(u, v) + \beta_a(u, v).$$

Buďte γ_s symetrická bilineární forma a γ_a antisymetrická bilineární forma takové, že $\beta = \gamma_s + \gamma_a$. Potom pro libovolné $u, v \in V$

$$\beta(u, v) = \gamma_s(u, v) + \gamma_a(u, v)$$

$$\beta(v, u) = \gamma_s(v, u) + \gamma_a(v, u) = \gamma_s(u, v) - \gamma_a(u, v).$$

Součtem těchto dvou rovnic dostaneme

$$\gamma_s(u, v) = \frac{1}{2}(\beta(u, v) + \beta(v, u)) = \beta_s(u, v),$$

odečtením druhé rovnice od první dostaneme

$$\gamma_a(u, v) = \frac{1}{2}(\beta(u, v) - \beta(v, u)) = \beta_a(u, v). \quad \square$$

Poznámka. Množina všech bilineárních forem na vektorovém prostoru s operacemi sčítání forem a násobení formy skalárem tvoří vektorový prostor. Množina všech symetrických bilineárních forem a množina všech antisymetrických bilineárních forem jsou podprostory tohoto prostoru. Podle předchozího tvrzení prostor všech bilineárních forem na jednom prostoru je přímým součtem těchto dvou podprostorů.

15.4. Kvadratické formy

V geometrii i fyzice se často vyskytují kvadratické formy. Mezi nimi a symetrickými bilineárními formami je jednoznačná korespondence.

Definice 15.4.1. Buď $\beta: V \times V \rightarrow P$ bilineární forma. Zobrazení $\bar{\beta}: V \rightarrow P$, $\bar{\beta}(v) = \beta(v, v)$, je *kvadratická forma* příslušná bilineární formě β .

Příklad. Pro eukleidovský skalární součin příslušná kvadratická forma je zobrazení, které každému vektoru u z příslušného vektorového prostoru přiřadí $(u, u) = \|u\|^2$. $\square$

Kvadratická forma je dána symetrickou částí bilineární formy.

Lemma 15.4.1. *Bud' β bilineární forma. Potom β_s je jediná symetrická bilineární forma taková, že $\bar{\beta} = \bar{\beta}_s$. Navíc,*

$$\beta_s(u, v) = \frac{1}{2}(\bar{\beta}(u + v) - \bar{\beta}(u) - \bar{\beta}(v)).$$

Důkaz.

$$\begin{aligned} \bar{\beta}(v) &= \beta(v, v) = \beta_s(v, v) + \beta_a(v, v) = & (\beta_a(v, v) = 0) \\ &= \beta_s(v, v) = \bar{\beta}_s(v). \end{aligned}$$

Bud' γ symetrická bilineární forma taková, že $\bar{\beta} = \bar{\gamma}$. Potom

$$\begin{aligned} \bar{\gamma}(u + v) &= \gamma(u + v, u + v) = \gamma(u, u) + 2\gamma(u, v) + \gamma(v, v) = \\ &= \bar{\gamma}(u) + 2\gamma(u, v) + \bar{\gamma}(v). \end{aligned}$$

Z toho dostaneme

$$\begin{aligned} \gamma(u, v) &= \frac{1}{2}(\bar{\gamma}(u + v) - \bar{\gamma}(u) - \bar{\gamma}(v)) = \frac{1}{2}(\bar{\beta}(u + v) - \bar{\beta}(u) - \bar{\beta}(v)) = \\ &= \frac{1}{2}(\beta_s(u + v, u + v) - \beta_s(u, u) - \beta_s(v, v)) = \\ &= \frac{1}{2}(\beta_s(u, u) + \beta_s(u, v) + \beta_s(v, u) + \beta_s(v, v) - \beta_s(u, u) - \beta_s(v, v)) = \\ &= \frac{1}{2}2\beta_s(u, v) = \beta_s(u, v). \end{aligned} \quad \square$$

Definice 15.4.2. Bud' β bilineární forma. Bilineární forma β_s je *polarizace* kvadratické formy $\bar{\beta}$.

Tvrzení 15.4.2. *Bud' β, γ bilineární formy. Potom $\bar{\beta} = \bar{\gamma}$ právě tehdy, když $\beta_s = \gamma_s$.*

Důkaz. Vyplyvá z Lemmatu 15.4.1. $\square$

Příklad. Mějme kvadratickou formu $\bar{\beta}$ na $\mathbb{R}^2$

$$\bar{\beta}(x^1, x^2) = a(x^1)^2 + bx^1x^2 + c(x^2)^2.$$

Potom

$$\beta_s((x^1, x^2), (y^1, y^2)) = ax^1y^1 + \frac{1}{2}bx^1y^2 + \frac{1}{2}by^1x^2 + cx^2y^2. \quad \square$$

15.5. Kanonické tvary

Tvrzení 15.5.1. *Každá symetrická matice nad P je kongruentní s diagonální maticí.*

Důkaz. Bud' A symetrická matice typu $n \times n$. Jelikož případ nulové matice je zřejmý, předpokládejme, že A je nenulová. Převedeme ji na diagonální matici v n krocích, v i -tém kroku vynulujeme prvky v i -tém řádku a i -tém sloupku mimo diagonálu, a to pomocí konečně mnoha dvojic úprav, přičemž každá dvojice úprav sestává z řádkové elementární úpravy a stejné sloupkové elementární úpravy. Pro jednoduchost budeme matici po provedení dvojice úprav označovat také A . i -tý krok vypadá následovně.

1. Je-li i -tý sloupek nulový (a tedy i i -tý řádek nulový), v i -tém kroku neděláme nic.
2. Jestliže $A_i^i = 0$, přičteme c -násobek j -tého řádku k i -tému řádku a pak přičteme c -násobek j -tého sloupku k i -tému sloupku, kde $j > i$ je takové, že $A_i^j \neq 0$, a c volíme takové, že $c \neq 0$ a $2A_j^i + cA_j^j \neq 0$. Potom $A_i^i = c(2A_j^i + cA_j^j) \neq 0$.

3. Pro každé $j \neq i$ takové, že $A_i^j \neq 0$, přičteme $(-A_i^j/A_i^i)$ -násobek i -tého řádku k j -tému řádku a pak přičteme $(-A_j^i/A_i^i)$ -násobek i -tého sloupku k j -tému sloupku. Potom $A_j^i = 0$ pro každé $j \neq i$.

Po i -tém kroku máme blokově diagonální matici

$$\begin{pmatrix} D_i & 0 \\ 0 & C_i \end{pmatrix},$$

kde D_i je diagonální matice typu $i \times i$ s prvky $d_1, \dots, d_i$ na diagonále.

Provedením k dvojic úprav (vždy řádková a stejná sloupková úprava) dostaneme matici

$$B_k = P_k \cdots P_1 A P_1^T \cdots P_k^T = P_k \cdots P_1 A (P_k \cdots P_1)^T,$$

kde $P_1, \dots, P_k$ jsou vhodné elementární matice. Matice B_k je tedy symetrická matice kongruentní s původní maticí A (viz Tvzení 15.2.5 a 15.2.6).

Po n -tém kroku máme diagonální matici D s prvky $d_1, \dots, d_n$ na diagonále, přičemž

$$D = P_m \cdots P_1 A P_1^T \cdots P_m^T = P_m \cdots P_1 A (P_m \cdots P_1)^T,$$

kde $P_1, \dots, P_m$ jsou vhodné elementární matice. Označíme-li $Q = (P_m \cdots P_1)^T$, potom $D = Q^T A Q$ a matici Q můžeme získat tak, že začneme s jednotkovou maticí a provádíme jen uvedené sloupkové úpravy. $\square$

Tvrzení 15.5.2. *Buď A symetrická matice nad P .*

- (1) *Jestliže $P = \mathbb{R}$, potom A je kongruentní s diagonální maticí D takovou, že $D_i^i \in \{0, 1, -1\}$ pro každé i .*
- (2) *Jestliže $P = \mathbb{C}$, potom A je kongruentní s diagonální maticí D takovou, že $D_i^i \in \{0, 1\}$ pro každé i .*

Důkaz. Podle předchozího tvrzení A je kongruentní s diagonální maticí, která má na diagonále prvky $d_1, \dots, d_n$.

- (1) Pro každé i takové, že $d_i \neq 0$, provedeme dvojici úprav: i -tý řádek vynásobíme $1/\sqrt{|d_i|}$ a i -tý sloupek vynásobíme $1/\sqrt{|d_i|}$. Na místě (i, i) potom bude $d_i/|d_i| = \pm 1$, takže na diagonále budou jen prvky množiny $\{0, 1, -1\}$.
- (2) Pro každé i takové, že $d_i \neq 0$, provedeme dvojici úprav: i -tý řádek vynásobíme z_i a i -tý sloupek vynásobíme z_i , čili na místě (i, i) potom bude $d_i z_i^2$, a tak $z_i \in \mathbb{C}$ volíme takové, aby $d_i z_i^2 = 1$. Na diagonále pak budou jen prvky množiny $\{0, 1\}$. $\square$

Definice 15.5.1. Buď A symetrická matice nad P . Diagonální matice D kongruentní s maticí A taková, že $D_i^i \in \{0, 1, -1\}$ (resp. $D_i^i \in \{0, 1\}$) pro každé i , je *kanonický tvar symetrické matice A vzhledem ke kongruentnosti*.

Poznámka. Počet nenulových prvků v diagonální matici je roven počtu jejích nenulových řádků, tedy její hodnoti. Hodnota matice se nemění elementárními úpravami, tedy ani násobením regulární maticí, takže kongruentní matice mají stejnou hodnotu a počty nenulových prvků v kongruentních diagonálních maticích jsou stejné.

Takže diagonální matice D z důkazu Tvzení 15.5.1 sice není určena jednoznačně, ale všechny diagonální matice kongruentní s maticí A , včetně všech jejích kanonických tvarů, mají stejný počet nenulových prvků na diagonále.

Tvrzení 15.5.3. *Pro každou symetrickou bilineární formu na konečněrozměrném vektorovém prostoru nad P existuje báze tohoto prostoru taková, že matice dané bilineární formy vzhledem k této bázi je v kanonickém tvaru vzhledem ke kongruentnosti.*

Důkaz. Důsledek Tvzení 15.5.1 a 15.5.2. □

Počet nenulových prvků diagonální matice symetrické bilineární formy nezávisí na volbě báze příslušného prostoru. Dokonce, v případě vektorového prostoru nad $\mathbb{R}$ a symetrické bilineární formy na něm počet jedniček a minus jedniček v její matici, která je diagonální, nezávisí na volbě báze.

Tvrzení 15.5.4 (Sylvesterův zákon setrvačnosti). *Počet jedniček a minus jedniček v matici symetrické bilineární formy na konečněrozměrném reálném vektorovém prostoru nezávisí na volbě báze.*

Důkaz. Buď β symetrická bilineární forma na konečněrozměrném reálném vektorovém prostoru V . Buďte $\mathbf{u} = (u_1, \dots, u_n)$, $\mathbf{v} = (v_1, \dots, v_n)$ báze prostoru V takové, že matice formy β vzhledem k těmto bázím, označme je $B_{\mathbf{u}}$ a $B_{\mathbf{v}}$, jsou v kanonickém tvaru. Bez ztráty obecnosti pro jednoduchost předpokládejme, že matice $B_{\mathbf{u}}$ je diagonální matice, která má na diagonále nejdříve k_1 jedniček, potom l_1 minus jedniček a ostatní prvky nulové, a matice $B_{\mathbf{v}}$ je diagonální matice, která má na diagonále nejdříve k_2 jedniček, potom l_2 minus jedniček a ostatní prvky nulové. Čili,

$$B_{\mathbf{u}} = \begin{pmatrix} E_{k_1} & 0 & 0 \\ 0 & -E_{l_1} & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{a} \quad B_{\mathbf{v}} = \begin{pmatrix} E_{k_2} & 0 & 0 \\ 0 & -E_{l_2} & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

kde E_i je jednotková matice typu $i \times i$.

Předpokládejme, že $k_1 > k_2$. Označme $U_1 = \llbracket u_1, \dots, u_{k_1} \rrbracket$ a $U_2 = \llbracket v_{k_2+1}, \dots, v_n \rrbracket$. Potom

$$\begin{aligned} \dim(U_1 \cap U_2) &= \\ &= \dim U_1 + \dim U_2 - \dim(U_1 + U_2) \geq \quad (\dim(U_1 + U_2) \leq n) \\ &\geq k_1 + (n - k_2) - n > 0, \end{aligned}$$

takže existuje nenulový vektor $v \in U_1 \cap U_2$. Označme x a y souřadnice vektoru v vzhledem k bázím $\mathbf{u}$, resp. $\mathbf{v}$. Jelikož $v \in U_1$ a zároveň $v \in U_2$,

$$x = (x^1, \dots, x^{k_1}, \underbrace{0, \dots, 0}_{n-k_1}) \quad \text{a} \quad y = (\underbrace{0, \dots, 0}_{k_2}, y^{k_2+1}, \dots, y^n).$$

Jelikož v je nenulový vektor, aspoň jedna souřadnice $x^1, \dots, x^{k_1}$ je nenulová a zároveň aspoň jedna souřadnice $y^{k_2+1}, \dots, y^n$ je nenulová. Takže,

$$\beta(v, v) = \bar{\beta}(v) = x^T B_{\mathbf{u}} x = (x^1)^2 + \dots + (x^{k_1})^2 > 0$$

a zároveň

$$\beta(v, v) = \bar{\beta}(v) = y^T B_{\mathbf{v}} y = -(y^{k_2+1})^2 - \dots - (y^{k_2+l_2})^2 \leq 0,$$

což je spor. Obdobně bychom došli ke sporu s předpokladem, že $k_2 > k_1$. Proto $k_1 = k_2$ a v důsledku toho také $l_1 = l_2$.

Jiný důkaz tohoto tvrzení lze nalézt v [Marvan, 17. Bilineární a kvadratické formy]. □

15.6. Pozitivní definitnost

Definice 15.6.1. Symetrická bilineární forma β na reálném vektorovém prostoru V je *pozitivně definitní*, jestliže $\beta(v, v) = \bar{\beta}(v) > 0$ pro každý nenulový vektor $v \in V$.

Tvrzení 15.6.1. *Symetrická bilineární forma na konečněrozměrném reálném vektorovém prostoru je pozitivně definitní právě tehdy, když její matice vzhledem k nějaké bázi je jednotková.*

Důkaz. Buď β symetrická bilineární forma na konečněrozměrném reálném vektorovém prostoru V . Podle Tvzení 15.5.3 existuje báze $\mathbf{v} = (v_1, \dots, v_n)$ prostoru V taková, že matice B formy β vzhledem k této bázi je v kanonickém tvaru, čili B je diagonální matice s $d_1, \dots, d_n \in \{0, 1, -1\}$ na diagonále. Pro každé $v \in V$ tedy $\beta(v, v) = \beta(v) = x^T Bx = d_1(x^1)^2 + \dots + d_n(x^n)^2$, kde $x = (x^1, \dots, x^n)$ jsou souřadnice vektoru v vzhledem k bázi $\mathbf{v}$.

Předpokládejme, že β je pozitivní definitní, tedy $\beta(v, v) > 0$ pro každé nenulové $v \in V$. Potom pro každé i $\beta(v_i, v_i) = e_i^T B e_i = d_i > 0$, takže každé $d_i = 1$ a B je jednotková matice.

Je-li B jednotková matice, potom pro každý nenulový vektor $v \in V$ $\beta(v, v) = x^T E x = (x^1)^2 + \dots + (x^n)^2 > 0$, čili β je pozitivně definitní. $\square$

Definice 15.6.2. Symetrická reálná matice A typu $n \times n$ je *pozitivně definitní*, jestliže $x^T A x > 0$ pro všechna nenulová $x \in \mathbb{R}^n$.

Tvrzení 15.6.2. Symetrická bilineární forma na konečněrozměrném reálném vektorovém prostoru je pozitivně definitní právě tehdy, když její matice vzhledem k libovolné bázi je pozitivně definitní.

Důkaz. Buď β symetrická bilineární forma na konečněrozměrném reálném vektorovém prostoru V , $\mathbf{v}$ libovolná báze V a B je matice formy β vzhledem k bázi $\mathbf{v}$.

Předpokládejme, že pro každé $v \in V \setminus \{0\}$ $\beta(v, v) > 0$. Pro libovolné nenulové $x \in \mathbb{R}^n$ buď v vektor z V , jehož souřadnice vzhledem k bázi $\mathbf{v}$ jsou x . Potom $x^T B x = \beta(v, v) > 0$.

Předpokládejme, že pro každé nenulové $x \in \mathbb{R}^n$ $x^T B x > 0$. Pro libovolné nenulové $v \in V$ nechť x jsou jeho souřadnice vzhledem k bázi $\mathbf{v}$. Potom $\beta(v, v) = x^T B x > 0$. $\square$

Důsledek. Symetrická reálná matice je pozitivně definitní právě tehdy, když je kongruentní s jednotkovou maticí.

Důkaz. Důsledek Tvzení 15.6.1 a 15.6.2. $\square$

Definice 15.6.3. Buď A matice typu $n \times n$. Pro $i \in \{1, \dots, n\}$ determinant matice typu $i \times i$ vzniklé z A vynecháním posledních $n - i$ řádků a posledních $n - i$ sloupků je *hlavní minor*.

Tvrzení 15.6.3. Symetrická reálná matice je pozitivně definitní právě tehdy, když všechny její hlavní minory jsou kladné.

Důkaz. Buď B symetrická reálná matice typu $n \times n$. Pro $i \in \{1, \dots, n\}$ označme B_i matici typu $i \times i$, která z matice B vznikne vynecháním posledních $n - i$ řádků a posledních $n - i$ sloupků (např. $B_n = B$), a označme $D_i = \det B_i$.

Předpokládejme, že B je pozitivně definitní. Podle předchozího Důsledku B je kongruentní s jednotkovou maticí, čili existuje regulární matice Q taková, že $B = Q^T E Q = Q^T Q$. Proto $\det B = \det(Q^T Q) = (\det Q)^2 > 0$.

Buď $i \in \{1, \dots, n - 1\}$. Pro libovolné nenulové $y = (y^1, \dots, y^i) \in \mathbb{R}^i$ označme $y_0 = (y^1, \dots, y^i, 0, \dots, 0) \in \mathbb{R}^n$. Potom $y^T B_i y = y_0^T B y_0 > 0$, čili B_i je pozitivně definitní a podle předchozího odstavce $\det B_i > 0$.

Předpokládejme, že všechny hlavní minory matice B jsou kladné, čili $D_i > 0$ pro $i \in \{1, \dots, n\}$. Převeďme B na kanonický tvar pomocí dvojic symetrických elementárních úprav, jak je popsáno v důkazech Tvzení 15.5.1 a 15.5.2. Protože $B_1^1 = D_1 > 0$, při čítání vhodných násobků prvního řádku k ostatním řádkům a vhodných násobků prvního sloupku k ostatním sloupkům vynulujeme všechny prvky prvního sloupku a všechny prvky prvního řádku kromě B_1^1 . Vzniklou matici označme $\bar{B}$. Provedené úpravy nemění

hodnotu determinantu, proto hlavní minory matice $\bar{B}$ jsou také rovny $D_1, \dots, D_n$. Čili $B_1^1 \bar{B}_2^2 = D_2 > 0$, takže $\bar{B}_2^2 > 0$ a přičítáním vhodných násobků druhého řádku k ostatním řádkům a vhodných násobků druhého sloupku k ostatním sloupkům vynulujeme všechny prvky druhého sloupku a všechny prvky druhého řádku kromě $\bar{B}_2^2$. Vzniklou matici označme $\bar{\bar{B}}$ a její hlavní minory jsou také rovny $D_1, \dots, D_n$. Čili $D_2 \bar{\bar{B}}_3^3 = D_3 > 0$, takže $\bar{\bar{B}}_3^3 > 0$ a takto můžeme pokračovat, až dostaneme diagonální matici s kladnými prvky na diagonále. Převodem na kanonický tvar dostaneme jednotkovou matici. Matice B je tedy kongruentní s jednotkovou maticí a podle předchozího Důsledku je tedy pozitivně definitní. $\square$

16. TENZORY

Zobecněním bilineární formy jsou multilineární formy. Nazývají se též kovariantní tenzory. Hojně se vyskytují ve fyzice spolu s tenzory kontravariantními a smíšenými. Omezíme se na reálný případ. Používáme Einsteinovu sumační konvenci.

Definice 16.0.1. Buď V vektorový prostor nad polem $\mathbb{R}$. Buď p přirozené číslo, označme $V^p = V \times \cdots \times V$ (p -krát). Zobrazení $f: V^p \rightarrow \mathbb{R}$, splňující pro libovolné vektory $u_i, u'_i, u''_i \in V$, libovolný skalár $a \in \mathbb{R}$ a každý index $i = 1, \dots, p$ podmínky

$$\begin{aligned} f(u_1, \dots, u_{i-1}, u'_i + u''_i, u_{i+1}, \dots, u_p) &= \\ &= f(u_1, \dots, u_{i-1}, u'_i, u_{i+1}, \dots, u_p) + f(u_1, \dots, u_{i-1}, u''_i, u_{i+1}, \dots, u_p), \\ f(u_1, \dots, u_{i-1}, au_i, u_{i+1}, \dots, u_p) &= af(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_p) \end{aligned}$$

(linearita v i -tém argumentu), je p -lineární forma nebo též kovariantní tenzor řádu p na V .

1-lineární forma je lineární zobrazení $V \rightarrow \mathbb{R}$, 2-lineární forma je bilineární forma.

Příklad. Necht' $V = \mathbb{R}^n$. Pro vektory $x_1 = (x_1^1, \dots, x_1^n), \dots, x_n = (x_n^1, \dots, x_n^n) \in \mathbb{R}^n$ položme

$$\epsilon(x_1, \dots, x_n) = \begin{vmatrix} x_1^1 & \dots & x_n^1 \\ \vdots & & \vdots \\ x_1^n & \dots & x_n^n \end{vmatrix}.$$

Z vlastností determinantu vyplývá, že ϵ je n -linerární forma na $\mathbb{R}^n$ (cvičení). $\square$

Definice 16.0.2. Buď V konečněrozměrný vektorový prostor s bází $(e_1, \dots, e_n)$, buď f p -lineární forma na V . Čísla $f_{i_1 \dots i_p} := f(e_{i_1}, \dots, e_{i_p})$ jsou složky formy f vzhledem k bázi $(e_1, \dots, e_n)$.

Příklad. Složky bilineární formy f jsou právě prvky její matice: $B_j^i = f(e_i, e_j)$. $\square$

Cvičení. Složky n -formy ϵ zadané determinantem jsou (ve standardní bázi prostoru $\mathbb{R}^n$)

$$\epsilon_{i_1 \dots i_n} = \begin{cases} \text{sgn}(i_1, \dots, i_n) & \text{jsou-li } i_1, \dots, i_n \text{ po dvou různá čísla,} \\ 0 & \text{jinak.} \end{cases} \quad \square$$

Tvrzení 16.0.1. Buďte V konečněrozměrný vektorový prostor, $(e_1, \dots, e_n)$ jeho báze, f p -lineární forma na V , $u_1, \dots, u_p \in V$ a $(x_1^1, \dots, x_1^n), \dots, (x_p^1, \dots, x_p^n)$ jejich souřadnice vzhledem k bázi $(e_1, \dots, e_n)$. Pak platí

$$f(u_1, \dots, u_p) = f_{i_1 \dots i_p} x_1^{i_1} \cdots x_p^{i_p}. \quad (16)$$

Důkaz.

$$\begin{aligned} f(u_1, \dots, u_p) &= f(x_1^{i_1} e_{i_1}, \dots, x_p^{i_p} e_{i_p}) = x_1^{i_1} \cdots x_p^{i_p} f(e_{i_1}, \dots, e_{i_p}) = \\ &= f_{i_1 \dots i_p} x_1^{i_1} \cdots x_p^{i_p} \end{aligned} \quad \square$$

Při změně báze $(e_1, \dots, e_n)$ se mění i složky $f_{i_1 \dots i_p}$.

Tvrzení 16.0.2. Buď Q matice přechodu od báze $(e_1, \dots, e_n)$ k bázi $(e'_1, \dots, e'_n)$. Složky p -lineární formy f vzhledem k bázi $(e_1, \dots, e_n)$ buďte $f_{i_1 \dots i_p}$, složky téže formy vzhledem k bázi $(e'_1, \dots, e'_n)$ buďte $f'_{i_1 \dots i_p}$. Pak platí

$$f'_{i_1 \dots i_p} = Q_{i_1}^{j_1} \cdots Q_{i_p}^{j_p} f_{j_1 \dots j_p}. \quad (17)$$

Důkaz. Cvičení. □

Ve fyzice se obvykle zavádí kovariantní tenzorové pole jako soubor n^p funkcí $f_{i_1 \dots i_p}$, jež se při změně báze transformují podle formule (17). Takový soubor funkcí určuje p -lineární zobrazení vztahem (16).

Množinu všech p -lineárních forem na vektorovém prostoru V označujeme $T_p V$. Zavedme algebraické operace s p -lineárními formami.

Definice 16.0.3. Budťe f a g p -lineární formy a $a \in \mathbb{R}$. *Součet* forem f a g je zobrazení $f + g: V^p \rightarrow \mathbb{R}$ zadané předpisem

$$(f + g)(u_1, \dots, u_p) = f(u_1, \dots, u_p) + g(u_1, \dots, u_p),$$

a -násobek formy f je zobrazení $af: V^p \rightarrow \mathbb{R}$ zadané předpisem

$$(af)(u_1, \dots, u_p) = af(u_1, \dots, u_p).$$

Snadno se ověří (cvičení), že $f + g$ a af jsou zase p -lineární formy. Dokonce jsou splněny axiomy vektorového prostoru:

Důsledek. *Množina $T_p V$ všech p -lineárních forem na prostoru V je vektorový prostor vzhledem ke sčítání forem a násobení skalárem.*

Definice 16.0.4. *Tenzorový součin* forem $f \in T_p V$ a $g \in T_q V$ je zobrazení $f \otimes g: V^{p+q} \rightarrow \mathbb{R}$ zadané předpisem

$$(f \otimes g)(u_1, \dots, u_{p+q}) = f(u_1, \dots, u_p) \cdot g(u_{p+1}, \dots, u_{p+q}).$$

Snadno se ověří (cvičení), že tenzorový součin p -lineární formy a q -lineární formy je $(p + q)$ -lineární forma.

Tvrzení 16.0.3. *Nechť $f \in T_p V$, $g \in T_q V$, $h \in T_r V$, $a \in \mathbb{R}$. Pak platí:*

- (1) $(f \otimes g) \otimes h = f \otimes (g \otimes h)$;
- (2) $(f + g) \otimes h = f \otimes h + g \otimes h$;
- (3) $f \otimes (g + h) = f \otimes g + f \otimes h$;
- (4) $(af) \otimes h = a(f \otimes h) = f \otimes (ah)$.

Důkaz. Cvičení. □

Obečně však tenzorový součin není komutativní: $f \otimes g \neq g \otimes f$.

Cvičení. Dokažte formule pro složky:

$$\begin{aligned} (f + g)_{i_1 \dots i_p} &= f_{i_1 \dots i_p} + g_{i_1 \dots i_p}, \\ (f \otimes g)_{i_1 \dots i_{p+q}} &= f_{i_1 \dots i_p} \cdot g_{i_{p+1} \dots i_{p+q}}. \end{aligned}$$

□

Prostor $T_1 V$ se alternativně označuje V^* a nazývá se *duální* prostor k prostoru V . Ukážeme, že s každou bází prostoru V je spojena jistá báze prostoru V^* .

Buď $(e_1, \dots, e_n)$ nějaká báze prostoru V . Souřadnice vektoru $x \in V$ vzhledem k bázi $(e_1, \dots, e_n)$ označme $(x^1, \dots, x^n)$ (pak platí $x = x^j e_j$). Pro $1 \leq i \leq n$ zavedme zobrazení $e^i: V \rightarrow \mathbb{R}$ předpisem $x \mapsto x^i$. To jest,

$$e^i(x^j e_j) = x^i.$$

Zobrazení e^i jsou lineární (cvičení), a proto $e^i \in V^*$. Máme

$$e^i(e_j) = \delta_j^i,$$

kde δ_j^i je známé Kroneckerovo delta:

$$\delta_j^i = \begin{cases} 1 & \text{pro } i = j, \\ 0 & \text{jinak.} \end{cases}$$

Tvrzení 16.0.4. *Bud' $(e_1, \dots, e_n)$ báze prostoru V , bud' $f \in V^*$ libovolná 1-forma se složkami $f_i = f(e_i)$. Pak*

$$f = f_i e^i.$$

Důkaz. Podle formule (16) je $f(x) = f(x^i e_i) = x^i f_i = f_i e^i(x) = (f_i e^i)(x)$. $\square$

Tvrzení 16.0.5. *Bud' $(e_1, \dots, e_n)$ báze prostoru V . Pak formy $e^1, \dots, e^n$ tvoří bázi prostoru V^* .*

Důkaz. Podle předchozího tvrzení každá 1-forma f je lineární kombinací 1-forem e^i (koeficienty jsou složky f_i). Tudíž, formy e^i generují V^* .

Zároveň množina $\{e^1, \dots, e^n\}$ je lineárně nezávislá: Necht' $c_i e^i = 0$ pro nějaké koeficienty $c_i \in \mathbb{R}$. Dosazením e_j obdržíme $0 = c_i e^i(e_j) = c_j$. $\square$

Báze $(e^1, \dots, e^n)$ se nazývá *duální* k bázi $(e_1, \dots, e_n)$.

Důsledek. *Je-li prostor V konečněrozměrný, pak $\dim V^* = \dim V$.*

Podobně najdeme báze v prostorech $T_p V$.

Tvrzení 16.0.6. *Bud' $(e_1, \dots, e_n)$ báze prostoru V , bud' $f \in T_p V$ libovolná p -forma se složkami $f_{i_1 \dots i_p} = f(e_{i_1}, \dots, e_{i_p})$. Pak*

$$f = f_{i_1 \dots i_p} e^{i_1} \otimes \dots \otimes e^{i_p}.$$

Důkaz. Podle formule (16) je opět

$$\begin{aligned} f(x_1, \dots, x_p) &= f(x_1^{i_1} e_{i_1}, \dots, x_p^{i_p} e_{i_p}) = x_1^{i_1} \dots x_p^{i_p} f_{i_1 \dots i_p} = \\ &= f_{i_1 \dots i_p} e^{i_1}(x_1) \dots e^{i_p}(x_p) = \\ &= (f_{i_1 \dots i_p} e^{i_1} \otimes \dots \otimes e^{i_p})(x_1, \dots, x_p). \end{aligned} \quad \square$$

Tvrzení 16.0.7. *Bud' $(e_1, \dots, e_n)$ báze prostoru V . Pak formy $e^{i_1} \otimes \dots \otimes e^{i_p}$ tvoří bázi prostoru $T_p V$.*

Důkaz. Podle předchozího tvrzení každá p -forma f je lineární kombinací p -forem $e^{i_1} \otimes \dots \otimes e^{i_p}$ (koeficienty jsou složky $f_{i_1 \dots i_p}$). Tudíž, formy $e^{i_1} \otimes \dots \otimes e^{i_p}$ generují $T_p V$.

Zároveň jsou nezávislé: Necht' $c_{i_1 \dots i_p} e^{i_1} \otimes \dots \otimes e^{i_p} = 0$ pro nějaké koeficienty $c_{i_1 \dots i_p} \in \mathbb{R}$. Dosazením $e_{j_1}, \dots, e_{j_p}$ obdržíme $0 = c_{i_1 \dots i_p} e^{i_1}(e_{j_1}) \dots e^{i_p}(e_{j_p}) = c_{j_1 \dots j_p}$. $\square$

Důsledek. *Je-li prostor V konečněrozměrný, pak $\dim T_p V = (\dim V)^p$.*

REFERENCE

- [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>.