Stanislav Palúch, Ida Stankovianska

ALGEBRA
a jej inžinierske aplikácie

VYDALA ŽILINSKÁ UNIVERZITA V ŽILINE
2008

Recenzenti: doc. RNDr. Elena Wisztová, CSc.
doc. RNDr. Roman Frič, CSc.

Tlačová predloha týchto textov bola vytvorená v typografickom systéme LaTeXpod operačným systémom Linux.

ISBN-80-XXXX-XXX-X

Úvod

Moderná algebra je oblasť matematiky, ktorá študuje tzv. algebraické štruktúry. Algebraická štruktúra je základná množina spolu s jednou alebo aj viacerými operáciami. Moderná algebra je zovšeobecnením tzv. elementárnej algebry, ktorá sa zaoberá správnymi pravidlami narábania s výrazmi obsahujúcimi reálne alebo komplexné čísla a premenné zviazané medzi sebou binárnymi operáciami sčítania a násobenia. Na rozdiel od elementárnej algebry prvky základnej množiny v modernej (niekedy tiež abstraktnej) algebre môžu byť okrem čísel aj všeobecné abstraktné objekty – znaky niektorej abecedy, matice, funkcie, zobrazenia a pod.

Rozvoj informačných technológií priniesol so sebou množstvo problémov spojených s ukladaním, prenosom, spracovaním a ochranou informácie. Ukázalo sa, že mnoho z týchto problémov možno formulovať a riešiť ako algebraické problémy tak, že množinu znakov abecedy, (v ktorej informáciu zapisujeme) pokladáme za prvky základnej množiny, na ktorej definujeme isté vhodné operácie. Bez použitia konečných grúp, konečných okruhov, konečných telies, Galoisových telies a ďalších konečných algebraických štruktúr by dnešná kryptografia či teória informácie (najmä pokiaľ ide a kódovanie, kompresiu údajov, zabezpečovacie a samoopravné kódy) vôbec nemohli existovať. Dochádza tak k významnej aplikácii matematických štruktúr, ktoré sa pred niekoľkými desiatkami rokov mohli zdať ako prakticky nepoužiteľné hračky matematikov.

S obrovským vzrastom rýchlosti a pamäťovej kapacity súčasnej výpočtovej techniky stúpol aj význam metód matematického programovania. Z teoretických metód sa tak stali prakticky využiteľné a dostupné algoritmy zabudované v mnohých požívateľských komerčných i voľne dostupných programoch (napr. Excel, Gnumeric, LP-Solve). Aj tieto algoritmy sú založené na výsledkoch modernej algebry – konkrétne na vlastnostiach konečne dimenzionálnych lineárnych priestorov.

Snažili sme sa do tejto učebnice zaradiť tie časti modernej algebry, ktoré majú podľa nášho najlepšieho vedomia a svedomia najširšie a najvýznamnejšie aplikácie v informatike, počítačovom inžinierstve a operačnej analýze.

Ďakujeme RNDr. Alžbete Klaudínyovej a recenzentom doc. RNDr. Elene Wisztovej, CSc. a doc. RNDr. Romanovi Fričovi, CSc. za pozorné prečítanie textu a opravu mnohých, niektorých i veľmi nepríjemných chýb. V neposlednom rade ďakujeme Ing. Milanovi Součkovi, prokuristovi firmy Schenck, za finančnú podporu vydania tejto učebnice.

V Žiline, 21. októbra 2008 Autori

Obsah

Kapitola 1

Binárne relácie

V matematike veľmi často potrebujeme vyjadriť skutočnosť, že dva prvky skúmanej množiny V sú v nejakom vzťahu – relácii. Ak skúmame množinu všetkých priamok v rovine, môžeme skúmať, či dve priamky p, q sú rovnobežné alebo nie. V kladnom prípade píšeme $p \parallel q$. Iný vzťah – kolmosť dvoch priamok vyjadríme ako $p \perp q$. Pri skúmaní množiny prirodzených čísel $\mathbb{N} = \{1, 2, 3, \dots\}$ môžeme študovať deliteľnosť čísel – ak je číslo n deliteľné číslom m, píšeme $m|n$.

Vo všeobecnejších prípadoch môžeme skúmať vzťahy medzi prvkami dvoch rôznych množín V, W. Ak V je množina všetkých priamok a W množina všetkých rovín v trojrozmernom priestore, môžeme skúmať, či daná priamka $p \in V$ je kolmá na rovinu $\omega \in W$. Ak áno píšeme $p \perp \omega$. Podobne môžeme skúmať vzťah rovnobežnosti priamky a roviny.

Ako matematicky definovať reláciu ρ medzi prvkami množín V a W, resp. na množine objektov V? Vzťah $u \,\rho\, v$ je úplne a jednoznačne charakterizovaný množinou všetkých usporiadaných dvojíc (u, v), pre ktoré platí $u \,\rho\, v$.

Definícia 1.1. Usporiadaná dvojica (u, v) prvkov u, v z množiny V je taká dvojica, pri ktorej je určené, ktorý z prvkov u, v je na prvom a ktorý na druhom mieste. **Usporiadaná n-tica** prvkov je taká n-tica prvkov $(a_1, a_2, \dots, a_n)$, pri ktorej je určené poradie prvkov.

Definícia 1.2. Karteziánsky súčin $A \times B$ dvoch množín A, B je množina všetkých usporiadaných dvojíc tvaru (a, b), kde $a \in A$, $b \in B$. **Kartezián-**

sky súčin $A_1 \times A_2 \times \cdots \times A_n$ **množín** $A_1, A_2, \ldots, A_n$ je množina všetkých usporiadaných n-tíc $(a_1, a_2, \ldots, a_n)$, kde $a_i \in A_i$ pre $i = 1, 2, \ldots, n$.

Píšeme $A^2 = A \times A$. Podobne A^n je definované vzťahom $A^n = \underbrace{A \times A \times \cdots \times A}_{n\text{-krát}}$.

Karteziánsky súčin $A^p \times A^q$ podľa definície obsahuje všetky usporiadané dvojice tvaru

$$\big((a_1, a_2, \ldots, a_p), (a_{p+1}, a_{p+2}, \ldots, a_{p+q})\big), \tag{1.1}$$

kde $(a_1, a_2, \ldots, a_p) \in A^p$, $(a_{p+1}, a_{p+2}, \ldots, a_{p+q}) \in A^q$. Vo väčšine prípadov stotožníme usporiadanú dvojicu (1.1) s $(p+q)$-ticou

$$(a_1, a_2, \ldots, a_p, a_{p+1}, a_{p+2}, \ldots, a_{p+q}),$$

a preto potom môžeme písať

$$A^p \times A^q = A^{p+q}. \tag{1.2}$$

Pre názornosť je výhodné predstaviť si prvky (a_i, b_j) karteziánskeho súčinu dvoch konečných množín $A = \{a_1, a_2, \ldots, a_m\}$, $B = \{b_1, b_2, \ldots, b_n\}$ usporiadané vo forme tabuľky:

	b_1	b_2	$\ldots$	b_j	$\ldots$	b_n
a_1	(a_1, b_1)	(a_1, b_2)	$\ldots$	(a_1, b_j)	$\ldots$	(a_1, b_n)
a_2	(a_2, b_1)	(a_2, b_2)	$\ldots$	(a_2, b_j)	$\ldots$	(a_2, b_n)
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_i	(a_i, b_1)	(a_i, b_2)	$\ldots$	(a_i, b_j)	$\ldots$	(a_i, b_n)
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_m	(a_m, b_1)	(a_m, b_2)	$\ldots$	(a_m, b_j)	$\ldots$	(a_m, b_n)

Tabuľka 1.1: Prvky karteziánskeho súčinu $A \times B$

Tabuľka obsahuje $m \times n$ usporiadaných dvojíc (a_i, b_j), $a_i \in A$, $b_j \in B$, čo pravdepodobne bolo motívom pre označenie operácie karteziánskeho súčinu znakom $\times$.

Definícia 1.3. Binárna relácia ρ **z množiny** V **do množiny** W je ľubovoľná podmnožina karteziánskeho súčinu $V \times W$.

Veľmi často skúmame vzťahy medzi prvkami tej istej množiny, t. j. $V = W$. Takéto relácie špecifikuje nasledujúca definícia.

Definícia 1.4. Binárna relácia ρ na množine V je podmnožina karteziánskeho súčinu $V \times V$. Všeobecnejšie: Ľubovoľnú podmnožinu karteziánskeho súčinu V^n nazveme **n-árnou reláciou na množine** V.

Pre $n = 1$ hovoríme o **unárnej relácii**, pre $n = 2$ o binárnej a pre $n = 3$ o **ternárnej relácii**.
Ak je ρ binárnou operáciou na V a $(u, v) \in \rho$, hovoríme, že **prvok u je v relácii ρ s prvkom** v a píšeme $u \,\rho\, v$.

Príklad 1.1. Príklady binárnych relácií na množine prirodzených čísel $\mathbb{N}$.

$$P = \{(n, k.n) \mid k, n \in \mathbb{N}\} \qquad Q = \{(m, n) \mid m, n \in \mathbb{N} \quad \exists k \in \mathbb{N} \quad m + k = n\}$$

Potom $a \,P\, b$ práve vtedy, keď $a|b$, $a \,Q\, b$ práve vtedy, keď $a < b$.

Definícia 1.5. Hovoríme, že binárna relácia ρ na množine V je
reflexívna, ak pre každé $v \in V$ platí $v \,\rho\, v$,
antireflexívna, ak pre žiadne $v \in V$ neplatí $v \,\rho\, v$,
symetrická, ak pre každé $u, v \in V$ z platnosti $u \,\rho\, v$ vyplýva platnosť $v \,\rho\, u$,
antisymetrická, ak pre každé $u, v \in V$ z platnosti $u \,\rho\, v$ a $v \,\rho\, u$ vyplýva $u = v$,
tranzitívna, ak pre každé $u, v, w \in V$ z platnosti $u \,\rho\, v$ a $v \,\rho\, w$ vyplýva $u \,\rho\, w$.

Príklad 1.2. Predstave o binárnych reláciách môže pomôcť tabuľka binárnej relácie ρ. Je to tabuľka podobná tabuľke 1.1, ktorá však na mieste (a_i, b_j) má znak $\bullet$, ak $a_i \,\rho\, b_j$, inak je toto miesto prázdne. Uvedieme tabuľky pre niekoľko binárnych relácií na množine $V = \{1, 2, 3, 4, 5, 6\}$.

	1	2	3	4	5	6
1	•					
2		•				
3			•			
4				•		
5					•	
6						•

a)

	1	2	3	4	5	6
1	•					
2	•	•				
3	•	•	•			
4	•	•	•	•		
5	•	•	•	•	•	
6	•	•	•	•	•	•

b)

	1	2	3	4	5	6
1			•		•	•
2		•	•		•	
3	•	•	•			
4						
5	•	•			•	
6	•					•

c)

Tabuľka a) je tabuľkou binárnej relácie $u = v$, tabuľka b) prislúcha relácii $u \leq v$, tabuľka c) je tabuľkou symetrickej binárnej relácie ρ, ktorá nie je reflexívna. Vidíme, že tabuľka reflexívnej relácie má prvkami $\bullet$ obsadenú celú hlavnú diagonálu, tabuľka antireflexívnej relácie má celú hlavnú diagonálu voľnú. Tabuľka symetrickej relácie je symetrická podľa svojej hlavnej diagonály, tabuľka

antisymetrickej relácie nemá obsadené prvkami • žiadne dve rôzne políčka symetrické podľa hlavnej diagonály. Tranzitivitu binárnej relácie už tak ľahko na prvý pohľad z jej tabuľky nevidno.

Príklad 1.3. Na množine celých čísel $\mathbb{Z}$ je relácia $\leq$ reflexívna, antisymetrická a tranzitívna. Relácia $<$ je na množine $\mathbb{Z}$ antireflexívna a tranzitívna, nie je antisymetrická.

Príklad 1.4. Relácia $\parallel$ na množine priamok v rovine je reflexívna, symetrická a tranzitívna. Relácia $\perp$ je symetrická, antireflexívna, nie je tranzitívna ani reflexívna.

Príklad 1.5. Vezmime za V množinu všetkých podmnožín niektorej množiny, $A, B \in V$. Potom relácia $A \subseteq B$ je reflexívna, antisymetrická a tranzitívna.

Definícia 1.6. Zobrazenie $F : X \to Y$ je taká binárna relácia z X do Y, že pre každé $x \in X$ existuje nanajvýš jedno $y \in Y$ také, že $x\,F\,y$. (Vtedy namiesto $x\,F\,y$ píšeme $y = F(x)$.)
Definujme množiny $\mathcal{D}_F \subseteq X$, $\mathcal{H}_F \subseteq Y$

$$\mathcal{D}_F = \{x \mid x \in X, \quad \exists y \in Y \; x\,F\,y\} \tag{1.3}$$
$$\mathcal{H}_F = \{y \mid y \in Y, \quad \exists x \in X \; x\,F\,y\} \tag{1.4}$$

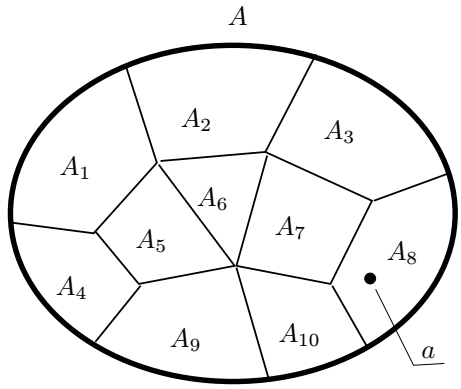
Množinu $\mathcal{D}_F$ nazveme **definičný obor zobrazenia** F a množinu $\mathcal{H}_F$ budeme volať **obor hodnôt zobrazenia** F. Ak je obor hodnôt zobrazenia F podmnožinou množiny všetkých reálnych čísel $\mathbb{R}$, t. j. $\mathcal{H}_F \subseteq \mathbb{R}$, hovoríme, že F je **funkcia**.

Konečne matematicky presná definícia funkcie! Funkcia je teda špeciálnym typom binárnej relácie.

1.1 Ekvivalencia a rozklad množiny

Definícia 1.7. Ekvivalencia alebo **relácia ekvivalencie** na množine V je binárna relácia na V ktorá je reflexívna, symetrická a tranzitívna.

Definícia 1.8. Rozkladom množiny V nazveme systém neprázdnych podmnožín $A_i \subseteq V$, $i \in I$, taký, že $A_i \cap A_j = \emptyset$ pre $i, j \in I$, $i \neq j$, a každý prvok $v \in V$ leží v nejakej množine A_i, t. j. $\bigcup_{i \in I} A_i = V$. Množiny A_i, $i \in I$, nazveme **triedami rozkladu**.



Obr. 1.1: Rozklad množiny A
Každá trieda rozkladu môže byť reprezentovaná svojím ľubovoľným prvkom a.

Definícia 1.9. Nech P je relácia ekvivalencie na množine V, nech $a \in V$. **Triedou ekvivalencie P k prvku** a nazveme množinu

$$[a] = \{v \mid v \in V,\ v\,P\,a\}. \tag{1.5}$$

Prvok a nazveme reprezentantom triedy $[a]$.

Veta 1.1. *Nech P je ekvivalencia na množine V. Potom všetky triedy ekvivalencie P tvoria rozklad množiny V.*

Dôkaz:
Najprv ukážeme, že ak $[a] \cap [b] \neq \emptyset$, potom $[a] = [b]$. Nech $s \in [a] \cap [b]$. Nech $x \in [a]$. Potom podľa definície $[a]$, $[b]$ je

$$s\,P\,a, \quad \text{zo symetrie } P \text{ je aj} \quad a\,P\,s, \tag{1.6}$$
$$s\,P\,b, \tag{1.7}$$
$$x\,P\,a. \tag{1.8}$$

Ak napíšeme za sebou vzťahy (1.8), (1.6), (1.7), dostávame $x\,P\,a$, $a\,P\,s$, $s\,P\,b$. Z posledného vzťahu s využitím tranzitívnosti ekvivalencie P máme $x\,P\,b$. Je teda $[a] \subseteq [b]$. Analogicky sa dokáže opačná inklúzia.

Keďže pre každý prvok $a \in V$ $a \in [a]$ (lebo $a\,P\,a$), dáva zjednotenie všetkých tried ekvivalencie P celú množinu V. ■

Z dôkazu predchádzajúcej vety tiež vidíme, že ak $b \in [a]$, potom $[a] = [b]$. Nezáleží teda na výbere reprezentanta triedy.

Veta 1.2. *Nech $\mathcal{P} = \{A_i \mid i \in I\}$ je rozklad množiny V. Potom existuje práve jedna relácia ekvivalencie P taká, že triedy ekvivalencie P sú triedami rozkladu $\mathcal{P}$.*

DÔKAZ:
Definujme reláciu P tak, že dva prvky u, v množiny V budú v relácii P práve vtedy, keď ležia v jednej triede rozkladu $\mathcal{P}$. Formálne zapísané

$$u\,P\,v \quad \text{práve vtedy, keď existuje } A_i \in \mathcal{P} \text{ také, že} \quad u \in A_i,\ v \in A_i. \tag{1.9}$$

Reflexivita a symetria relácie P vyplývajú priamo z definície.

Ukážeme tranzitivitu. Nech $u\,P\,v$, $v\,P\,w$. Potom existujú $A_i, A_j \in \mathcal{P}$, také, že $u, v \in A_i$ a $v, w \in A_j$. Pretože $v \in A_i \cap A_j \neq \emptyset$, je $A_i = A_j$ a preto $u, w \in A_i$, z čoho máme $v\,P\,w$. Relácia P je tranzitívna.
Jedinečnosť relácie P vyplýva zo skutočnosti, že dvom rôznym ekvivalenciám prislúchajú rôzne rozklady na triedy ekvivalencií. ■

Príklad 1.6. Rovnosť "=" prvkov akejkoľvek množiny je reflexívna, symetrická a tranzitívna relácia. Každá trieda ekvivalencie obsahuje práve jeden prvok.

Príklad 1.7. Vezmime za základnú množinu množinu $\mathbb{Z}$ celých čísel a definujme binárnu reláciu P predpisom:

$$m\,P\,n \quad \text{práve vtedy, keď} \quad |m| = |n|. \tag{1.10}$$

Triedy ekvivalencie P sú $[0] = \{0\}$, $[1] = \{-1, 1\}$, $[2] = \{-2, 2\}$, $[3] = \{-3, 3\}$, ...

Rozklad na triedy ekvivalencie je silným nástrojom na presné matematické definovanie nových pojmov. K tomu uvedieme niekoľko príkladov.

Príklad 1.8. V analytickej geometrii (v rovine) je bod $\mathbf{x}$ dvojicou reálnych čísel $\mathbf{x} = (x_1, x_2)$. Orientovaná úsečka je určená usporiadanou dvojicou bodov $(\mathbf{a}, \mathbf{b})$. Dve orientované úsečky $(\mathbf{a}, \mathbf{b})$, $(\mathbf{c}, \mathbf{d})$ majú rovnakú veľkosť a rovnaký smer práve vtedy, keď $b_1 - a_1 = d_1 - c_1$ a $b_2 - a_2 = d_2 - c_2$. Vektor sa potom definuje ako množina všetkých orientovaných úsečiek rovnakej veľkosti a rovnakého smeru. Použitím predchádzajúcich výsledkov teórie binárnych relácií možno spresniť definíciu vektora takto. Relácia „mať rovnakú veľkosť a rovnaký smer“

je reflexívna, symetrická a tranzitívna – je to relácia ekvivalencie na množine všetkých orientovaných úsečiek. **Vektor** potom možno definovať ako triedu ekvivalencie „mať rovnakú veľkosť a rovnaký smer“.

Príklad 1.9. Rozšírenie množiny celých čísel $\mathbb{Z}$ o racionálne čísla. Usporiadanú dvojicu celých čísel (p, q) budeme v tomto špeciálnom prípade zapisovať ako $\frac{p}{q}$. Na podmnožine všetkých usporiadaných dvojíc celých čísel $\frac{p}{q}$ takých, že $q \neq 0$ – je to vlastne množina $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ – zavedieme operácie $+$ a $.$ predpisom:

$$\frac{a}{b} + \frac{c}{d} = \frac{a.d + c.b}{d.b} \qquad \frac{a}{b}.\frac{c}{d} = \frac{a.c}{b.d} \tag{1.11}$$

Na množine $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ zavedieme reláciu $\equiv$ predpisom:

$$\frac{a}{b} \equiv \frac{c}{d} \quad \text{práve vtedy, keď} \quad a.d = c.b \tag{1.12}$$

Ľahko sa ukáže, že relácia $\equiv$ je reflexívna, symetrická a tranzitívna. Triedy ekvivalencie $\equiv$ nazveme **racionálnymi číslami**. Na množine všetkých tried ekvivalencie $\equiv$ zavedieme binárne operácie $+$ a $.$ predpisom:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{a.d + c.b}{d.b}\right] \qquad \left[\frac{a}{b}\right] . \left[\frac{c}{d}\right] = \left[\frac{a.c}{b.d}\right] \tag{1.13}$$

t. j. súčet dvoch tried je trieda, ktorá má za reprezentanta súčet reprezentantov sčítancov. Treba ešte dokázať, že operácie z (1.13) sú korektne definované, t. j. že ich výsledok nezáleží na výbere reprezentantov tried $\left[\frac{a}{b}\right]$, $\left[\frac{c}{d}\right]$. Potom už stačí stotožniť každý prvok $c \in \mathbb{Z}$ s prvkom $\left[\frac{c}{1}\right]$, a rozšírenie okruhu celých čísel na teleso racionálnych čísel máme hotové.

1.2 Usporiadanie

Definícia 1.10. Hovoríme, že relácia $\preceq$ je **usporiadanie** na množine V, ak $\preceq$ je reflexívna, tranzitívna a antisymetrická relácia. Dvojicu $(V, \preceq)$, kde $\preceq$ je usporiadanie na V voláme **čiastočne usporiadaná množina** .
Nech $\preceq$ je usporiadanie na množine V, nech pre prvky $u \in V,\ v \in V$ neplatí ani $u \preceq v$, ani $v \preceq u$. Potom hovoríme, že prvky u, v sú **neporovnateľné**.

Lineárne usporiadanie je také usporiadanie $\preceq$ na V, že pre každú dvojicu prvkov $u, v \in V$ je $u \preceq v$ alebo $v \preceq u$. Dvojicu $(V, \preceq)$, kde P je lineárne usporiadanie na V, voláme **lineárne usporiadaná množina** alebo **reťazec**.

Príklad 1.10. Relácia inklúzie $\subseteq$ je usporiadaním na množine všetkých podmnožín nejakej základnej množiny A. Nech množina A má aspoň dva rôzne prvky a, b, $a \neq b$, t. j. $|A| \geq 2$. Potom existujú dve neprázdne disjunktné podmnožiny množiny A (totiž $\{a\}$, $\{b\}$), ktoré sú neporovnateľné v čiastočnom usporiadaní $\subseteq$. Usporiadanie $\subseteq$ preto nie je lineárnym usporiadaním na množine všetkých podmnožín množiny A takej, že $|A| \geq 2$.

Príklad 1.11. Relácia $k|n$ (číslo n je deliteľné číslom k) je usporiadaním na množine všetkých prirodzených čísel $\mathbb{N}$. Ak máme dve rôzne prvočísla p, q, potom neplatí $p|q$, ani $q|p$, preto usporiadanie $k|n$ nie je lineárnym usporiadaním.

Príklad 1.12. Relácia $n \leq k$ je lineárnym usporiadaním na množine všetkých celých čísel $\mathbb{Z}$.

Definícia 1.11. Nech $(V, \preceq)$ je čiastočne usporiadaná množina. Hovoríme, že $w \in V$ je **maximálny prvok** množiny V, ak neexistuje prvok $x \in V$, $x \neq w$ taký, že $w \preceq x$. Hovoríme, že w je **najväčší prvok** množiny V, ak pre všetky $x \in V$ platí $x \preceq w$.
Hovoríme, že $v \in V$ je **minimálny prvok** množiny V, ak neexistuje prvok $y \in V$, $y \neq v$ taký, že $y \preceq v$. Hovoríme, že v je **najmenší prvok** množiny V, ak pre všetky $y \in V$ platí $v \preceq y$.

Čiastočne usporiadaná množina $(V, \preceq)$ môže mať viac maximálnych, resp. minimálnych prvkov, avšak najviac jeden najväčší a jeden najmenší prvok. Ak je $w \in V$ najväčším prvkom usporiadanej množiny V s usporiadaním $\preceq$, potom w je aj maximálnym prvkom množiny V. Toto tvrdenie sa však nedá obrátiť – ak je w maximálnym prvkom množiny V, ešte nemusí byť jej najväčším prvkom.

Môže sa stať, že usporiadaná množina nemá žiaden maximálny (resp. minimálny) prvok – príkladom je množina celých čísel $\mathbb{Z}$ s usporiadaním $\leq$. Množina prirodzených čísel $\mathbb{N} = \{1, 2, 3, \dots\}$ s usporiadaním $\leq$ má najmenší prvok 1 a nemá žiaden maximálny prvok. Ak označíme V množinu všetkých podmnožín neprázdnej množiny A, potom V s usporiadaním $\subseteq$ má najmenší prvok $v = \emptyset$ a najväčší prvok $w = A$.

Príklad 1.13. Nech $V = (0, 1) \subset \mathbb{R}$ je otvorený interval. Potom V s usporiadaním $\leq$ nemá ani najmenší ani najväčší prvok.

Kapitola 2

Algebraické štruktúry

V celej tejto publikácii budeme používať nasledujúcu symboliku

$\mathbb{N}$ – množina prirodzených čísel, t. j. $\mathbb{N} = \{1, 2, 3, \dots\}$

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, t. j. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

$\mathbb{Z}$ – množina všetkých celých čísel

$\mathbb{Q}$ – množina všetkých racionálnych čísel

$\mathbb{R}$ – množina všetkých reálnych čísel

$\mathbb{C}$ – množina všetkých komplexných čísel

2.1 Grupy

Na množine celých čísel je známe sčítanie dvoch celých čísel. Čo to znamená sčítať dve čísla $a, b \in \mathbb{Z}$? Znamená to k usporiadanej dvojici (a, b) dvoch celých čísel priradiť nejakým spôsobom – a tým je sčítanie – celé číslo c, pričom $c = a + b$. Teda sčítanie je vlastne zobrazenie $\varphi : \mathbb{Z} \times \mathbb{Z}$ do $\mathbb{Z}$, kde $\varphi(a, b) = a + b$. Zobrazenia tohto typu budeme nazývať binárne operácie.

Definícia 2.1. Binárna operácia $\circ$ na neprázdnej množina M je zobrazenie množiny $M \times M$ do M, t. j. $\circ : M \times M \to M$.

Binárne operácie zvykneme označovať symbolmi $\circ, *, \diamond, \triangle, \heartsuit, \cdots$ a výsledok priradený binárnou operáciou usporiadanej dvojici (a, b) označujeme $a \circ b$, $a * b$, $a \diamond b$, $a \triangle b$, ...

Príklad 2.1. Nech je daná množina $\mathbb{N}$. Zobrazenia dané predpismi

$$a \circ b = a + b - 1, \qquad a * b = a^{b+1}$$

sú binárnymi operáciami na $\mathbb{N}$. Zobrazenie

$$a \triangle b = \frac{1}{2}(a + b)$$

nie je binárna operácia na $\mathbb{N}$, ale je binárnou operáciou na $\mathbb{Q}$. Zobrazenie

$$a \square b = a - b$$

nie je binárna operácia na $\mathbb{N}$, avšak na $\mathbb{Z}$ to binárna operácia je.

Definícia 2.2. Usporiadanú n-ticu $\mathcal{A} = (M, \circ_1, \circ_2, \ldots, \circ_{n-1})$, kde M je neprázdna množina a $\circ_1, \circ_2, \ldots, \circ_{n-1}$ sú binárne operácie na množine M, budeme nazývať **algebraická štruktúra**.

My sa budeme zaoberať najskôr algebraickými štruktúrami s jednou binárnou operáciou a následne algebraickými štruktúrami s dvomi binárnymi operáciami. Najjednoduchšou algebraickou štruktúrou s jednou binárnou operáciou je grupoid.

Definícia 2.3. Grupoid je algebraická štruktúra $(M, \circ)$, kde M je neprázdna množina a $\circ$ je na nej definovaná binárna operácia.

Definícia 2.4. Majme grupoid $(M, \circ)$. Hovoríme, že binárna operácia $\circ$ je

- **komutatívna**, ak $\forall a, b \in M$ platí $a \circ b = b \circ a$
- **asociatívna**, ak $\forall a, b, c \in M$ platí $a \circ (b \circ c) = (a \circ b) \circ c$

Nech $\oplus, \otimes$ sú dve binárne operácie na neprázdnej množine M. Hovoríme, že

- **operácia $\otimes$ je sprava distributívna vzhľadom na operáciu $\oplus$**, ak pre všetky $a, b, c \in M$ platí

$$(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c) \tag{2.1}$$

- **operácia $\otimes$ je zľava distributívna vzhľadom na operáciu** $\oplus$, ak pre všetky $a, b, c \in M$ platí

$$c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$$

- **operácia $\otimes$ je distributívna vzhľadom na operáciu** $\oplus$, ak $\otimes$ je súčasne distributívna vzhľadom na operáciu $\oplus$ sprava i zľava.

Príklad 2.2. Na množine celých čísel $\mathbb{Z}$ sú definované dve binárne operácie $\square$ a $\circ$ predpisom:

$$a \square b = a + b - 1, \quad a \circ b = a + b - ab$$

pre $\forall a, b \in Z$. Sú tieto binárne operácie komutatívne a asociatívne? Je binárna operácia $\circ$ distributívna vzhľadom na binárnu operáciu $\square$?

Riešenie:
Overíme komutatívnosť a asociatívnosť binárnej operácie $\square$. Operácia $\square$ je komutatívna, ak platí: $a \square b = b \square a$ pre $\forall a, b \in \mathbb{Z}$. Ľavá strana rovnosti je $a \square b = a + b - 1$, pravá strana $b \square a = b + a - 1$. Komutatívnosť operácie $\square$ vyplýva z komutatívnosti sčítania celých čísel.
Aby bola binárna operácia asociatívna, musí platiť: $a \square (b \square c) = (a \square b) \square c$. Počítajme:

$$a \square (b \square c) = a \square (b + c - 1) = a + b + c - 1 - 1 = a + b + c - 2,$$

$$(a \square b) \square c = (a + b - 1) \square c = a + b - 1 + c - 1 = a + b + c - 2.$$

Asociatívnosť binárnej operácie $\square$ je potvrdená. Komutatívnosť a asociatívnosť binárnej operácie $\circ$ čitateľ overí ľahko sám. Venujme sa overeniu distributívnosti operácie $\circ$ vzhľadom na $\square$.
Binárna operácia $\circ$ je komutatívna, stačí overiť len distributívnosť zľava, t. j. $a \circ (b \square c) = (a \circ b) \square (a \circ c)$. Dostávame:

$$a \circ (b \square c) = a \circ (b + c - 1) = a + b + c - 1 - a(b + c - 1) = 2a + b + c - ab - ac - 1$$

$$(a \circ b) \square (a \circ c) = (a + b - ab) \square (a + c - ac) = 2a + b + c - ab - ac - 1.$$

Porovnaním pravých strán vidíme, že binárna operácia $\circ$ je distributívna vzhľadom na operáciu $\square$.

Definícia 2.5. Nech $(M, \circ)$ je grupoid, $e \in M$. Hovoríme, že e je

- **ľavý neutrálny prvok**, ak pre $\forall a \in M$ platí $e \circ a = a$.
- **pravý neutrálny prvok**, ak pre $\forall a \in M$ platí $a \circ e = a$.
- **neutrálny prvok**, ak pre $\forall a \in M$ platí $e \circ a = a \circ e = a$.

Definícia 2.6. Nech $\circ$ je binárna operácia na neprázdnej množine M. Nech existuje neutrálny prvok $e \in M$, nech $a, b \in M$. Hovoríme, že a je

- **ľavý symetrizačný prvok k prvku** b**,** ak $a \circ b = e$.
- **pravý symetrizačný prvok k prvku** b**,** ak $b \circ a = e$.
- **symetrizačný prvok k prvku** b**,** ak $a \circ b = b \circ a = e$

Veta 2.1. *Nech $(M, \circ)$ je grupoid. Ak $e_l \in M$ je ľavý neutrálny prvok a $e_p \in M$ je pravý neutrálny prvok binárnej operácie $\circ$, potom $e_l = e_p$, a teda v M existuje neutrálny prvok $e = e_l = e_p$.*

Dôkaz:
Z predpokladov vety platí

$$e_l \circ e_p = e_p, \tag{2.2}$$

pretože e_l je ľavý neutrálny prvok. Súčasne platí

$$e_l \circ e_p = e_l, \tag{2.3}$$

pretože e_p je pravý neutrálny prvok. Z rovnosti ľavých strán vzťahov (2.2) a (2.3) vyplýva $e_l = e_p$. ■

Dôsledkom vety 2.1 je skutočnosť, že binárna operácia $\circ$ môže mať na neprázdnej množine nanajvýš jeden neutrálny prvok.

Príklad 2.3. Nech $\mathbb{Z}$ je množina celých čísel, $\triangle$ je binárna operácia definovaná $a \triangle b = a - b + 1$ pre $\forall a, b \in Z$. Hľadajme neutrálny prvok binárnej operácie $\triangle$.
Riešenie:
Z definície $e \in \mathbb{Z}$ je neutrálnym prvkom binárnej operácie $\triangle$, ak je splnená rovnosť: $e \circ a = a \circ e = a$ pre $\forall a \in \mathbb{Z}$. Pre pravý neutrálny prvok platí:

$$a \triangle e = a - e + 1 = a\ . \tag{2.4}$$

Riešením (2.4) dostaneme, že pravý neutrálny prvok $e_p = 1$. Obdobne pre ľavý neutrálny prvok riešime rovnicu:

$$e \triangle a = e - a + 1 = a \ . \tag{2.5}$$

Z (2.5) vidíme, že ľavý neutrálny prvok $e_l = 2a - 1$. Pretože $e_l \neq e_p$, binárna operácia $\triangle$ nemá neutrálny prvok na množine $\mathbb{Z}$.

Definícia 2.7. Nech $(M, \circ)$ je grupoid.

- **Pologrupa** je grupoid, ktorého operácia $\circ$ je asociatívna.
- **Monoid** je pologrupa, v ktorej existuje neutrálny prvok.
- **Grupa** je monoid, v ktorom ku každému prvku $a \in M$ existuje symetrizačný prvok $\overline{a}$.

***Poznámka* 2.1.** *Ak operácia $\circ$ je komutatívna, hovoríme o komutatívnom grupoide, pologrupe, monoide, grupe. Pre komutatívnu grupu sa v literatúre používa tiež termín abelovská grupa.*

Príklad 2.4. Na množine celých čísel $\mathbb{Z}$ je definovaná binárna operácia $\circ$ predpisom $a \circ b = a + b - 1$. Ukážme, že $(\mathbb{Z}, \circ)$ je abelovská grupa.

Riešenie:
S ľubovoľnými dvomi celými číslami aj výsledok operácie $\circ$ patrí do množiny celých čísel a v množine celých čísel platí komutatívnosť čítania, teda $\circ$ je komutatívna binárna operácia definovaná na $\mathbb{Z}$. Z toho vyplýva, že $(\mathbb{Z}, \circ)$ je komutatívny grupoid. Asociatívnosť binárnej operácie $\circ$ sme overili v príklade 2.2, teda $(\mathbb{Z}, \circ)$ je komutatívna pologrupa. Nájdime neutrálny prvok. Vzhľadom na komutatívnosť $\circ$ stačí nájsť pravý (resp. ľavý) neutrálny prvok. Z definície neutrálneho prvku platí $a \circ e = a$. Riešením tejto rovnice dostávame $a + e - 1 = a$. Neutrálnym prvkom je $e = 1$, $(\mathbb{Z}, \circ)$ je komutatívny monoid. Ešte nám treba ukázať, že k ľubovoľnému celému číslu existuje symetrizačný prvok. Riešením rovnice $a \circ \overline{a} = e$ dostávame $a + \overline{a} - 1 = 1$. Symetrizačným prvkom je $\overline{a} = 2 - a$. Tým sme ukázali, že $(\mathbb{Z}, \circ)$ je komutatívna (abelovská) grupa.

Príklad 2.5. Uvedieme niekoľko príkladov na algebraické štruktúry. Čitateľ ľahko sám overí vyslovené tvrdenia.

a) Nech $\mathbb{N}$ je množina prirodzených čísel. $(\mathbb{N}, +)$ je komutatívna pologrupa, $(\mathbb{N}, \cdot)$ je komutatívny monoid s neutrálnym prvkom 1.

b) Nech $\mathbb{N}_0 = \{0, 1, 2, 3, 4, \dots\}$. $(\mathbb{N}_0, +)$ je komutatívny monoid s neutrálnym prvkom 0.

c) Nech $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sú množiny celých, racionálnych a reálnych čísel. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sú komutatívne grupy s neutrálnym prvkom 0 a symetrizačným prvkom $-a$ ku každému prvku a. $(\mathbb{Q} - \{0\}, \cdot)$ a $(\mathbb{R} - \{0\}, \cdot)$ sú komutatívne grupy s neutrálnym prvkom 1 a symetrizačným prvkom $\frac{1}{a}$ ku každému prvku a. $(\mathbb{Z} - \{0\}, \cdot)$ je len komutatívny monoid.

d) Binárna operácia nemusí byť definovaná len pomocou operácií sčítania alebo násobenia. Nech X je ľubovoľná neprázdna množina a nech je definovaná množina $S = \{A \subseteq X\}$. Pre $A, B \in S$ operácia $\cap$ je definovaná ako prienik množín A, B. $(S, \cap)$ je komutatívny monoid s neutrálnym prvkom X .

Veta 2.2. *Nech $(M, \circ)$ je monoid, nech $a \in M$. Nech a_p je pravý a a_l je ľavý symetrizačný prvok k prvku $a \in M$. Potom $a_p = a_l$, a teda existuje symetrizačný prvok k prvku a.*

Dôkaz:
$(M, \circ)$ je monoid, teda existuje neutrálny prvok $e \in M$. Existencia symetrizačných prvkov znamená platnosť vzťahov

$$a \circ a_p = e \qquad \text{a súčasne} \qquad a_l \circ a = e.$$

$(M, \circ)$ je pologrupa, teda $\circ$ je asociatívna binárna operácia. Využitím asociatívnosti dostaneme

$$a_l = a_l \circ e = a_l \circ (a \circ a_p) = (a_l \circ a) \circ a_p = e \circ a_p = a_p.$$

■

Veta 2.3. *Nech* $(G, \circ)$ *je grupa,* $a, b, q \in G$.

$$\text{Ak platí} \quad q \circ a = q \circ b, \qquad \text{potom platí } a = b. \tag{2.6}$$

$$\text{Ak platí} \quad a \circ q = b \circ q, \qquad \text{potom platí } a = b. \tag{2.7}$$

Dôkaz:
Dokážeme (2.6). Stačí rovnicu $q \circ a = q \circ b$ vynásobiť zľava symetrizačným prvkom $\overline{q}$, ktorý v grupe existuje ku každému jej prvku. Dostaneme

$$\begin{aligned} \overline{q} \circ (q \circ a) &= \overline{q} \circ (q \circ b) \\ (\overline{q} \circ q) \circ a &= (\overline{q} \circ q) \circ b \\ e \circ a &= e \circ b \\ a &= b \end{aligned}$$

Implikácia (2.7) sa dokáže analogicky. ■

Veta 2.4. *V grupe* $(G, \circ)$ *majú každá z rovníc* $a \circ x = b$, $y \circ a = b$ *práve jedno riešenie* a *to* $x = \overline{a} \circ b$, $y = b \circ \overline{a}$.

Dôkaz:
O tom, že $x = \overline{a} \circ b$ a $y = b \circ \overline{a}$ sú riešenia rovníc $a \circ x = b$, $y \circ a = b$ sa presvedčíme priamym dosadením

$$a \circ x = a \circ (\overline{a} \circ b) = (a \circ \overline{a}) \circ b = e \circ b = b,$$

$$y \circ a = (b \circ \overline{a}) \circ a = b \circ (\overline{a} \circ a) = b \circ e = b$$

Nepriamo ešte dokážeme jednoznačnosť riešenia rovnice $a \circ x = b$. Nech $x_1 \neq x_2$ sú dve jej riešenia. Potom platí

$$a \circ x_1 = b, \qquad a \circ x_2 = b.$$

Porovnajme obe rovnice a vynásobme symetrizačným prvkom $\overline{a}$ zľava. Dostaneme

$$\begin{aligned} a \circ x_1 &= a \circ x_2, \\ \overline{a} \circ (a \circ x_1) &= \overline{a} \circ (a \circ x_2), \\ (\overline{a} \circ a) \circ x_1 &= (\overline{a} \circ a) \circ x_2, \\ e \circ x_1 &= e \circ x_2, \\ x_1 &= x_2, \end{aligned}$$

čo je spor s predpokladom. Analogicky sa dá dokázať jednoznačnosť riešenia rovnice $y \circ a = b$. ■

Veta 2.5. *Nech $(G, \circ)$ je grupa, $a \in G$. Symetrizačný prvok k prvku a je určený jednoznačne.*

DÔKAZ:
Nech $\overline{a}$, $\hat{a}$ sú dva symetrizačné prvky k prvku a. Potom platí $\overline{a} \circ a = e$ a tiež $\hat{a} \circ a = e$, čiže

$$\overline{a} \circ a = \hat{a} \circ a,$$

z čoho podľa vety 2.3 vyplýva $\overline{a} = \hat{a}$. ■

Veta 2.6. *Nech $\overline{a}$ je symetrizačný prvok k prvku a, $\overline{b}$ symetrizačný prvok k prvku b v grupe $(G, \circ)$. Potom symetrizačný prvok prvku $a \circ b$ je $\overline{b} \circ \overline{a}$.*

DÔKAZ:
Stačí dokázať, že $(a \circ b) \circ (\overline{b} \circ \overline{a}) = e$ a $(\overline{b} \circ \overline{a}) \circ (a \circ b) = e$.

$$(a \circ b) \circ (\overline{b} \circ \overline{a}) = a \circ [b \circ (\overline{b} \circ \overline{a})] = a \circ [(b \circ \overline{b}) \circ \overline{a}] = a \circ [e \circ \overline{a}] = a \circ \overline{a} = e.$$

$$(\overline{b} \circ \overline{a}) \circ (a \circ b) = [(\overline{b} \circ \overline{a}) \circ a] \circ b = [b \circ (a \circ \overline{a})] \circ \overline{b} = [b \circ e] \circ \overline{b} = b \circ \overline{b} = e.$$

■

Definícia 2.8. Nech $\mathcal{G} = (G, \circ)$, $\mathcal{H} = (H, \diamond)$ sú dve grupy. Ak $H \subseteq G$ a pre každé dva prvky $x,\ y \in H$ platí

$$x \diamond y = x \circ y, \tag{2.8}$$

hovoríme, že grupa $\mathcal{H}$ je podgrupou grupy $\mathcal{G}$. Ak navyše $H \neq G$, hovoríme, že $\mathcal{H}$ je vlastná podgrupa grupy $\mathcal{G}$.

Veta 2.7. *Nech grupa $(B, \diamond)$ je podgrupou grupy $(A, \circ)$, nech e_A, e_B sú po rade neutrálne prvky grúp $(A, \circ)$, $(B, \diamond)$. Potom $e_A = e_B$.*

DÔKAZ:
Z definície neutrálneho prvku grupy $(B, \diamond)$ platí $e_B = e_B \diamond e_B$. Pretože $(B, \diamond)$ je podgrupou grupy $(A, \circ)$, z inklúzie $B \subseteq A$ vyplýva, že e_B je tiež neutrálnym prvkom grupy $(A, \circ)$, a teda platí

$$e_B = e_B \circ e_B.$$

Pretože e_A je neutrálny prvok v grupe $(A, \circ)$, je

$$e_B = e_B \circ e_A.$$

Z posledných dvoch rovností máme

$$e_B \circ e_B = e_B \circ e_A,$$

z čoho podľa vety 2.3 máme $e_B = e_A$. ■

Veta 2.8. *Nech $(G, \circ)$ je grupa s neutrálnym prvkom e, nech $H \subset G$, $H \neq \emptyset$. Potom $(H, \circ)$ je podgrupou grupy $(G, \circ)$ vtedy a len vtedy, ak*

a) pre každé dva prvky $x, y \in H$ je aj $x \circ y \in H$,

b) pre každý prvok $a \in H$ je aj $\overline{a} \in H$, kde $\overline{a}$ je symetrizačný prvok k prvku a.

Dôkaz:
Ak $(H, \circ)$ je podgrupou grupy $(G, \circ)$, tak je sama grupou a vlastnosti a), b) sú splnené.

Naopak: Ak pre neprázdnu množinu H, ktorá je podmnožinou množiny G, platia vlastnosti a), b), treba ukázať, že $(H, \circ)$ je grupa. Keďže platí a) a H je neprázdna podmnožina množiny G, bude platiť aj asociatívnosť binárnej operácie $\circ$. Podľa b) ak $a \in H$, je aj symetrizačný prvok $\overline{a} \in H$, teda aj $a \circ \overline{a} = e \in H$. Dôkaz je ukončený, $(H, \circ)$ je grupa. ■

Príklad 2.6. Nech $\mathbb{Z}$ je množina celých, $\mathbb{Q}$ množina racionálnych a $\mathbb{R}$ množina reálnych čísel. Potom $(\mathbb{Z}, +)$ je podgrupou grupy $(\mathbb{Q}, +)$, $(\mathbb{Q}, +)$ je zas podgrupou grupy $(\mathbb{R}, +)$.

Príklad 2.7. Množina prirodzených čísel $\mathbb{N}$ spolu s operáciou sčítania $+$ nie je podgrupou grupy celých čísel $\mathbb{Z}$, pretože štruktúra $(\mathbb{N}, +)$ nie je grupou.

Príklad 2.8. Označme $\mathbb{B} = \{0, 1\}$ definujme $0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1$, $1 \oplus 1 = 0$. Štruktúra $(\mathbb{B}, \oplus)$ je komutatívna grupa, $\mathbb{B} \subset \mathbb{Z}$, ale $\mathbb{B}$ nie je podgrupou $\mathbb{Z}$ pretože $1 \oplus 1 \neq 1 + 1$ – neplatí vzťah (2.8) definície 2.8

2.2 Okruhy a telesá

V ďalšom sa budeme zaoberať algebraickými štruktúrami s dvomi binárnymi operáciami.

Definícia 2.9. Nech M je neprázdna množina, nech $\oplus$, $\otimes$ sú dve binárne operácie na množine M. Algebraická štruktúra $\mathcal{O} = (M, \oplus, \otimes)$ sa nazýva **okruh**, ak

- $(M, \oplus)$ je komutatívna grupa
- $(M, \otimes)$ je pologrupa
- Operácia $\otimes$ je distributívna vzhľadom na operáciu $\oplus$, t. j. platia distributívne zákony:

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) \qquad (a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c) \quad (2.9)$$

Grupu $(M, \oplus)$ budeme nazývať **aditívna grupa okruhu** $\mathcal{O}$, binárnu operáciu $\oplus$ **aditívna operácia**. Neutrálny prvok aditívnej operácie budeme nazývať **nulový prvok,** resp. **nula okruhu** $\mathcal{O}$ a označovať symbolom 0. Symetrizačný prvok k prvku a aditívnej operácie nazveme **opačný prvok** a budeme ho označovať $\ominus a$.

***Poznámka* 2.2.** *Nula okruhu $\mathcal{O}$ nemusí byť totožná s reálnym číslom $0 \in \mathbb{R}$. Pozor, "0" je symbol pre neutrálny prvok okruhu $\mathcal{O}$!*

Pologrupu $(M, \otimes)$ budeme nazývať **multiplikatívna pologrupa** okruhu $\mathcal{O}$ a binárnu operáciu $\otimes$ **multiplikatívna operácia**.

Poznámka* 2.3.** *Ak v okruhu $\mathcal{O} = (M, \oplus, \otimes)$ existuje neutrálny prvok multiplikatívnej operácie na množine M, tak ho nazývame **jednotkový prvok okruhu** $\mathcal{O}$, resp. **jednotka okruhu** a budeme ho označovať symbolom 1. Takýto okruh budeme nazývať **okruh s jednotkou.

Symetrizačný prvok k prvku a multiplikatívnej operácie budeme nazývať **inverzný prvok** a budeme ho označovať a^{-1}.

Poznámka* 2.4.** *Okruh $\mathcal{O} = (M, \oplus, \otimes)$, v ktorom je binárna operácia $\otimes$ komutatívna, sa nazýva **komutatívny okruh.

Príklad 2.9. Nech $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sú číselné množiny po rade celých, racionálnych, reálnych a komplexných čísel. Potom $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sú komutatívne okruhy s jednotkou.

Príklad 2.10. Na množine celých čísel $\mathbb{Z}$ sú definované dve binárne operácie $\oplus$ a $\otimes$ vzťahmi

$$a \oplus b = a + b - 1, \qquad a \otimes b = a + b - ab. \tag{2.10}$$

Ukážeme, že $(\mathbb{Z}, \oplus, \otimes)$ je komutatívny okruh s jednotkou.
Riešenie:
V príklade 2.4 sme ukázali, že $(\mathbb{Z}, \oplus)$ je abelovská grupa s nulovým prvkom 1 a ku každému prvku $a \in \mathbb{Z}$ je opačným prvkom prvok $2 - a$. Ľahko sa dá ukázať, že $(\mathbb{Z}, \otimes)$ je komutatívna pologrupa a že existuje vzhľadom na operáciu $\otimes$ jednotkový prvok a tým je 0. Z toho vyplýva, že $(\mathbb{Z}, \otimes)$ je komutatívny monoid. Distributívnosť operácie $\otimes$ vzhľadom na operáciu $\oplus$ sme ukázali v príklade 2.2. Teda $(\mathbb{Z}, \oplus, \otimes)$ je komutatívny okruh s jednotkou.

Veta 2.9. *Nech $\mathcal{O} = (M, \oplus, \otimes)$ je okruh. Potom pre všetky $a \in M$ platí*

$$a \otimes 0 = 0 \otimes a = 0 \tag{2.11}$$

Dôkaz:
Nech 0 je nulový prvok grupy $(M, \oplus)$. Pre ľubovoľné $b \in M$ platí

$$b \oplus 0 = b \tag{2.12}$$

Na rovnicu (2.12) aplikujme sprava operáciou $\otimes$ prvok a, čím po použití distributívneho zákona dostaneme:

$$\begin{aligned} (b \oplus 0) \otimes a &= b \otimes a, \\ (b \otimes a) \oplus (0 \otimes a) &= b \otimes a, \\ (0 \otimes a) &= 0. \end{aligned}$$

Obdobne ukážeme druhú časť tvrdenia $a \otimes 0 = 0$ ■

Definícia 2.10. Nech $\mathcal{T} = (M, \oplus, \otimes)$ je okruh. Hovoríme, že $\mathcal{T} = (M, \oplus, \otimes)$ je **teleso,** ak algebraická štruktúra $(M - \{0\}, \otimes)$ je grupou. Ak navyše operácia $\otimes$ je komutatívna na množine M, hovoríme, že $\mathcal{T}$ je komutatívne teleso, alebo tiež **pole**.

Poznámka* 2.5.** *Neutrálny prvok grupy* $(M - \{0\}, \otimes)$ *budeme nazývať* ***jednotkovým prvkom telesa $\mathcal{T}$ *a budeme ho označovať symbolom* 1. *Opäť poznamenávame, že symbol "*1*" teraz označuje jednotkový prvok telesa* $\mathcal{T}$ *a nemusí byť totožný s číslom* $1 \in \mathbb{R}$ *!*

Príklad 2.11. V príklade 2.10 sme ukázali, že $(\mathbb{Z}, \oplus, \otimes)$ s operáciami $\oplus$, $\otimes$ definovanými vzťahmi (2.10) je komutatívny okruh s jednotkovým prvkom, ktorým je $e = 0$. Môžeme o ňom tvrdiť, že je aj telesom?

Riešenie:
Aby sme ukázali, že $(\mathbb{Z}, \oplus, \otimes)$ je teleso, musíme ukázať, že $(\mathbb{Z} - \{1\}, \otimes)$ je grupa. Stačí ukázať, že ku každému prvku a z množiny $\{\mathbb{Z} - \{1\}\}$ existuje inverzný prvok a_s.

$$\begin{aligned} a \otimes a_s &= e = 0 \\ \text{Podľa definície operácie } \oplus \text{ je} \quad & a \oplus a_s = a + a_S - a a_S, \text{ a preto} \\ a + a_S - a a_S &= 0 \\ a_S(1 - a) &= -a \\ a_s &= -\frac{a}{1-a} \notin \mathbb{Z} \end{aligned}$$

Z posledného vzťahu vidíme, že $(\mathbb{Z} - \{1\}, \otimes)$ nie je grupa, a teda $(\mathbb{Z}, \oplus, \otimes)$ nie je teleso.

Veta 2.10. *Nech* a, b *sú ľubovoľné prvky telesa* $\mathcal{T}$*. Potom*

$$(\ominus a) \otimes b = a \otimes (\ominus b) = \ominus(a \otimes b) \tag{2.13}$$

$$(\ominus a) \otimes (\ominus b) = a \otimes b \tag{2.14}$$

Dôkaz:
Nech 0 je nulový prvok aditívnej operácie $\oplus$. Potom z rovnosti $a \oplus (\ominus a) = 0$, na ktorú aplikujeme sprava multiplikatívnou operáciou $\otimes$ prvok b, postupne dostaneme:

$$\begin{aligned} [a \oplus (\ominus a)] \otimes b &= 0 \otimes b \\ (a \otimes b) \oplus [(\ominus a) \otimes b] &= 0 \\ [(\ominus a) \otimes b] &= \ominus(a \otimes b) \end{aligned}$$

Analogicky sa dá dokázať platnosť rovnice $a \otimes (\ominus b) = \ominus(a \otimes b)$. Čím sme dokázali vzťah (2.13).

Aby sme dokázali vzťah (2.14), použijeme východiskovú rovnicu

$$0 \otimes b = [a \oplus (\ominus a)] \otimes b = 0$$

Úpravou a využitím práve dokázaného vzťahu (2.13) dostávame

$$\begin{aligned} (a \otimes b) \oplus [(\ominus a) \otimes b] &= 0 \\ (a \otimes b) &= \ominus[(\ominus a) \otimes b] \\ (a \otimes b) &= (\ominus a) \otimes (\ominus b) \end{aligned}$$

■

Definícia 2.11. Nech $(M, \oplus, \otimes)$ je okruh. Prvky $a, b \in M$, $a \neq 0$, $b \neq 0$, pre ktoré platí $a \otimes b = 0$, sa nazývajú **delitele nuly** okruhu $(M, \oplus, \otimes)$. Komutatívny okruh, ktorý nemá delitele nuly, sa nazýva **obor integrity** .

Príklad 2.12. Nech $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sú množiny po rade celých, racionálnych, reálnych a komplexných čísel. Potom $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sú obory integrity.

Veta 2.11. *V poli (t. j. v komutatívnom telese)* $\mathcal{P} = (M, \oplus, \otimes)$ *pre každé* $a,\ b \in M$ *platí:*

$$ak\ a \otimes b = 0 \quad potom \quad a = 0\ alebo\ b = 0. \tag{2.15}$$

Dôkaz:
Nech $\mathcal{P} = (M, \oplus, \otimes)$ je pole a platí $a \otimes b = 0$ pre ľubovoľné dva prvky $a, b \in M$. Nech $a \neq 0$, potom existuje inverzný prvok a^{-1} a platí

$$\begin{aligned} a^{-1} \otimes (a \otimes b) &= a^{-1} \otimes 0 \\ (a^{-1} \otimes a) \otimes b &= 0 \\ 1 \otimes b &= 0 \\ b &= 0 \end{aligned}$$

kde 1 je jednotka poľa $\mathcal{P}$. Obdobným spôsobom za predpokladu, že $b \neq 0$, môžeme dokázať rovnosť $a = 0$. ■

***Poznámka* 2.6.** *Práve dokázaná veta hovorí, že každé pole je oborom integrity.*

Príklad 2.13. Algebraické štruktúry $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ z príkladu 2.12 sú polia.

Príklad 2.14. Na množine reálnych čísel $\mathbb{R}$ definujeme už známe binárne operácie $\oplus$ a $\otimes$: $a \oplus b = a + b - 1$, $a \otimes b = a + b - ab$. Algebraická štruktúra $(\mathbb{R}, \oplus, \otimes)$ je pole. Ukážme to!

Riešenie:
$(\mathbb{R}, \oplus)$ je grupa s nulovým prvkom 1 a opačným prvkom ku každému prvku $a \in \mathbb{R}$ $\ominus a = 2 - a$. $(\mathbb{R}, \otimes)$ je dokonca monoid s jednotkovým prvkom 0. Distributívne zákony platia (ukázali sme v predchádzajúcich príkladoch). Aby sme ukázali, že $(\mathbb{R}-\{1\}, \otimes)$ je grupa, stačí ukázať, že ku každému (!) prvku $a \in (\mathbb{R}-\{1\})$ existuje inverzný prvok. Inverzný prvok $a^{-1} = -\frac{a}{1-a} \in \mathbb{R}$ pre ľubovoľné $a \in (\mathbb{R} - \{1\})$. Z toho vyplýva, že $(\mathbb{R}, \oplus, \otimes)$ je pole.

Definícia 2.12. Nech $(A, \oplus, \otimes)$, $(B, \boxplus, \boxtimes)$ sú dve telesá. Hovoríme, že $(B, \boxplus, \boxtimes)$ je **podtelesom** telesa $(A, \oplus, \otimes)$, ak platí

$$B \subseteq A, \tag{2.16}$$

$$\text{pre každé } a,\ b \in B \qquad \text{platí} \qquad a \boxplus b = a \oplus b \qquad a \boxtimes b = a \otimes b. \tag{2.17}$$

Ak navyše $A \neq B$, potom hovoríme, že $(B, \boxplus, \boxtimes)$ je **vlastným podtelesom** telesa $(A, \oplus, \otimes)$.
Analogicky sa definuje pojem **podokruh**.

Veta 2.12. *Nech $(A, \oplus, \otimes)$ je teleso, nech $B \subset A$. Potom $(B, \oplus, \otimes)$ je podtelesom telesa $(A, \oplus, \otimes)$ práve vtedy, keď platí*

a) Pre každé dva prvky $a,\ b \in B$ je aj $a \oplus b \in B$ a tiež $a \otimes b \in B$,

b) Pre každý prvok $a \in B$ je aj $\ominus a \in B$

c) Pre každý prvok $a \in B$ taký, že $a \neq 0$, je aj $a^{-1} \in B$.

Dôkaz:
Ak je $(B, \oplus, \otimes)$ podtelesom telesa $(A, \oplus, \otimes)$, je ono samo telesom, a preto a), b), c) platia.

Nech je $B \subset A$ a nech platia a), b), c). Vlastnosť (2.16) je splnená – podľa predpokladu $B \subset A$. Vlastnosť (2.17) takisto platí. Treba ukázať, že $(B, \oplus, \otimes)$ je teleso, t. j. že $(B, \oplus)$ je komutatívna grupa, $(B - \{0\}, \otimes)$ je grupa a platia distributívne zákony. Podľa vety 2.8 je $(B, \oplus)$ podgrupou grupy $(A, \oplus)$, rovnako $(B - \{0\}, \otimes)$ je podgrupou grupy $(A - \{0\}, \otimes)$ a distributívnosť sa zachová. ■

2.3 Poznámka k zvyškovým triedam

V teórii konečných algebraických štruktúr zohráva dôležitú úlohu množina

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\},$$

ktorú nazývame **množina zvyškových tried modulo n**. Zvyškové triedy modulo n tvoria rozklad množiny $\mathbb{Z}$ celých čísel v zmysle, ako sme o tom hovorili v časti 1.1 (str. 10). **Modul** je pevne stanovené číslo $n \in \mathbb{Z}$, pričom praktický význam má $n > 1$.
Každé celé číslo sa dá napísať v tvare $a = kn + x$, kde $0 \leq x < n$. Pretože zvyšok môže nadobúdať práve n rôznych hodnôt $0, 1, 2, \ldots, n-1$, každé celé číslo môžeme zaradiť práve do jednej z n zvyškových tried podľa toho, aký má zvyšok po delení modulom n. Trieda obsahujúca $x \in \{0, 1, 2, \ldots, n-1\}$ obsahuje aj všetky celé čísla, pre ktoré platí

$$\overline{x} = \{x + kn \mid k \in \mathbb{Z}\}$$

Celé čísla patriace do jednej triedy sa od seba líšia o n alebo o jeho celočíselný násobok. Ekvivalencia, ktorá rozložila množinu celých čísel na množinu zvyškových tried modulo n, sa nazýva **kongruencia**.

Definícia 2.13. Nech $n > 1$ je dané celé číslo a nech čísla $a, b \in \mathbb{Z}$. Hovoríme, že **a je kongruentné s b modulo n** , ak $a - b$ je celočíselným násobkom modula n. Označujeme $a \equiv b \pmod{n}$.

Príklad 2.15. Uvažujme $n = 3$. Množina zvyškových tried modulo 3 potom je $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, pričom

$$\overline{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$
$$\overline{1} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$
$$\overline{2} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

Na množine zvyškových tried $\mathbb{Z}_n$ je možné zaviesť sčítanie a násobenie používané v množine celých čísel $\mathbb{Z}$. Označme $\oplus_n$ sčítanie modulo n, $\otimes_n$ násobenie neodul n.

Definícia 2.14. Pre ľubovoľné $\overline{x}, \overline{y} \in \mathbb{Z}_n$ platí

$$\overline{x} \oplus_n \overline{y} = \overline{x + y} \tag{2.18}$$

$$\overline{x} \otimes_n \overline{y} = \overline{x \cdot y} \tag{2.19}$$

***Poznámka* 2.7.** *V definícii je inými slovami povedané:*

$$\overline{x} \oplus_n \overline{y} = \textit{zvyšok po delení} \quad (x+y) : n$$

$$\overline{x} \otimes_n \overline{y} = \textit{zvyšok po delení} \quad (xy) : n$$

Príklad 2.16. Na množine zvyškových tried $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ operácie sčítania a násobenia modulo 3 vyjadríme tabuľkami:

$\oplus_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\otimes_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Z tabuliek v príklade 2.16 ľahko overíme, že $(\mathbb{Z}_3, \oplus_3)$ je komutatívna grupa s neutrálnym prvkom $\overline{0}$ a symetrizačnými prvkami $\overline{0}$ k prvku $\overline{0}$, $\overline{2}$ k prvku $\overline{1}$ a $\overline{1}$ k prvku $\overline{2}$. $(\mathbb{Z}_3, \otimes_3)$ je komutatívny monoid s neutrálnym prvkom $\overline{1}$. Symetrizačné prvky existujú len k $\overline{1}$ a $\overline{2}$ (k prvku $\overline{1}$ je to $\overline{1}$, k prvku $\overline{2}$ je to $\overline{2}$). Ak uvažujeme algebraickú štruktúru $(\mathbb{Z}_3, \oplus_3, \otimes_3)$ ľahko overíme, že je to minimálne okruh s jednotkou (dokonca viac!). Operácie $\oplus_n$, $\otimes_n$ sú komutatívne a asociatívne a operácia $\otimes_n$ je distributívna vzhľadom na operáciu $\oplus_n$, nakoľko vznikli z operácií $+$ a $\cdot$ a zachovávajú si všetky ich "dobré" vlastnosti. Neutrálnym prvkom operácie $\oplus_n$ je $\overline{0}$, pre ľubovoľný prvok $\overline{x} \in \{\mathbb{Z}_n - \{\overline{0}\}\}$ je opačným prvkom $\ominus\overline{x} = n - \overline{x}$, pre $\overline{x} = \overline{0}$ je $\ominus\overline{0} = \overline{0}$.

Neutrálnym prvkom násobenia $\otimes_n$ je $\overline{1}$. Z povedaného by sa zdalo, že zvyškové triedy si zachovávajú tie isté aritmetické vlastnosti, ako množina celých čísel. Je to klamný dojem. Bezpečne vieme vo zvyškových triedach len sčítať a násobiť pre akékoľvek modulo n. Keď si uvedomíme, že na množine celých čísel aritmetická operácia "odčítanie" je pričítanie čísla opačného, vieme vo zvyškových triedach (bez ohľadu na modulo n) aj odčítať. Problematické je delenie. Kým algebraická štruktúra $(Z, +, \cdot)$ je oborom integrity, o algebraickej štruktúre $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ sa to už tvrdiť nedá. Ako príklad uveďme $(\mathbb{Z}_4, \oplus_4, \otimes_4)$, kde $\overline{2} \otimes_4 \overline{2} = \overline{0}$, pričom $\overline{2} \neq \overline{0}$. Iná situácia nastáva, ak n je prvočíslo. Vtedy algebraická štruktúra $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ je nielen obor integrity, ale dokonca pole.

Veta 2.13. *$(\mathbb{Z}_n, \oplus_n, \otimes_n)$ je pole práve vtedy, keď n je prvočíslo.*

DÔKAZ:
To, že algebraická štruktúra $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ je komutatívny okruh s jednotkou (pre akékoľvek $n > 1$), je zrejmé. Aby bola aj poľom, musí byť $(\mathbb{Z}_n - \{\overline{0}\}, \otimes_n)$ grupa. K tomu treba ukázať, že pre ľubovoľné $\overline{a} \in \mathbb{Z}_n - \{\overline{0}\}$ existuje inverzný prvok.
Nech n je prvočíslo, nech a je ľubovoľné celé číslo také, že $0 < a < n$. Potom najväčší spoločný deliteľ čísel a, n $NSD(a, n) = 1$. Z vlastností celých čísel vyplýva, že musia existovať také celé čísla c, d, že $ac + nd = 1$. Po úprave vzťahu dostávame $1 - ac = nd$, čo podľa definície znamená, že $a \equiv 1 \pmod{n}$. Čiže $\overline{a} \otimes_n \overline{c} = \overline{1}$ a teda $\overline{c}$ je inverzným prvkom k prvku $\overline{a}$, $\overline{a} \in \mathbb{Z}_n - \{\overline{0}\}$. Keďže $\overline{a}$ bolo ľubovoľné, inverzný prvok existuje ku každému $\overline{a}$.
Nech n nie je prvočíslo. Potom $n = k_1 \cdot k_2$, kde $1 < k_1$ a $k_2 < n$, k_1, $k_2 \in Z$, $\overline{k}_1$, $\overline{k}_2 \in \mathbb{Z}_n$. To ale znamená, že $\overline{k}_1 \otimes_n \overline{k}_2 = \overline{0}$, pričom $\overline{k}_1 \neq \overline{0}$ aj $\overline{k}_2 \neq \overline{0}$. Čiže $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ nie je ani obor integrity.

2.4 Aplikácie

Cézarovská šifra

Gaius Július Cézar (100 – 44 pred Kr.) občas v korešpondencii používal jednoduchú šifru, keď každé písmeno nahradil písmenom, ktoré v abecednom poradí leží tri písmená za ním a písmená V, X, Y, Z po rade písmenami A, B, C, D.

Telegrafná abeceda bez medzery má 26 znakov. Ak znaky takejto telegrafnej abecedy stotožníme s číslami od 0 po 25 podľa nasledujúcej tabuľky,

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

môžeme ich považovať za prvky okruhu $\mathbb{Z}_{26}$. Potom má význam písať napr. F $\oplus_{26}$ K = P, pretože znak F zodpovedá číslu 5, znak K zodpovedá číslu 10, znak P zodpovedá číslu 15 a $5 \oplus_{26} 10 = 15$ v okruhu $\mathbb{Z}_{26}$. Analogicky F$\otimes_{26}$K = Y, pretože $5 \otimes_{26} 10 = 24$ v okruhu $\mathbb{Z}_{26}$ a Y sme stotožnili s číslom 24.

Šifru, ktorú používal Cézar, môžeme potom zapísať ako zobrazenie

$$f : \mathbb{Z}_{26} \to \mathbb{Z}_{26} \quad \text{určené vzťahom} \quad y = x \oplus_{26} \text{D}, \text{ resp. y} = \text{x} \oplus_{26} 4.$$

Dešifrovací predpis je $x = g(y) = y \ominus_{26} 4$.

Zovšeobecnenie tejto šifry pre ľubovoľný posun k sa nazýva **cézarovská šifra**. Posun k tu plní úlohu kľúča. Šifrovacie zobrazenie je $e_k(x) = x \oplus_{26} k$, dešifrovacie zobrazenie je $d_k(y) = y \ominus_{26} k$. Ako kľúč možno použiť ktorýkoľvek prvok okruhu $\mathbb{Z}_{26}$ okrem prípadu $k = \mathrm{A} = 0$, pretože vtedy by $e_0(x)$ bolo identické zobrazenie.

Ak dostaneme text zašifrovaný cézarovskou šifrou, stačí na jeho dešifrovanie vyskúšať 25 možností dešifrovacieho zobrazenia $d_k(y) = y \ominus_{26} -k$ (pre k=1,2,...,25), čo je ľahká úloha. Myšlienka sťažiť dešifrovanie tak, že text najprv zašifrujeme kľúčom k_1 a potom výsledok kľúčom k_2, nie je dobrá, pretože

$$\text{ak} \quad e_{k_1}(x) = x \oplus_{26} k_1, \quad e_{k_2}(x) = x \oplus_{26} k_2, \text{ potom}$$

$e_{k_2} \circ e_{k_1}(x) = e_{k_2}(e_{k_1}(x)) = e_{k_2}(x \oplus_{26} k_1) = (x \oplus_{26} k_1) \oplus_{26} k_2 = x \oplus_{26} (k_1 \oplus_{26} k_2)$, čo znamená, že výsledok je totožný s výsledkom zašifrovania jedným kľúčom $k_3 = (k_1 \oplus_{26} k_2)$.

Afinná šifra

Použitím operácií okruhu $\mathbb{Z}_{26}$ môžeme skonštruovať i zložitejšiu šifru ako je cézarovská šifra. Takou je tzv. **afinná šifra**, ktorej šifrovacie a dešifrovacie zobrazenia sú dané vzťahmi

$$e_{(k_1,k_2)}(x) = (k_1 \otimes_{26} x) \oplus_{26} k_2, \qquad d_{(k_1,k_2)}(y) = k_1^{-1} \otimes_{26} (y \ominus_{26} k_2).$$

Kľúčom môže byť každá usporiadaná dvojica (k_1, k_2) prvkov $\mathbb{Z}_{26}$ taká, že ku prvku k_1 existuje inverzný prvok k_1^{-1} – t. j. k_1 môže byť z množiny $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ (okrem dvojice $(1, 0)$, pre ktorú je $e_{(1,0)}$ identické zobrazenie). Poznamenajme, že aj tento systém, ktorý má $(12.26 - 1)$ použiteľných kľúčov, je ľahko rozlúštiteľný.

Je množina šifrovacích zobrazení grupiodom?

Blokové symetrické kryptografické šifry pracujú tak, že priamy text (uložený v binárnom tvare) určený na zakryptovanie rozdelia na rovnako dlhé časti – bloky (najčastejšie po 64 alebo 128 bitov) a potom postupne šifrujú blok po bloku. Šifrovanie bloku je vlastne jeho zobrazenie, ktoré má za definičný obor i obor hodnôt množinu všetkých možných (najčastejšie 64- alebo 128-bitových) binárnych slov. Šifrovacie zobrazenie možno formálne zapísať v tvare $y = E_K(x)$,

kde x je šifrovaný blok priameho textu, y je príslušný zašifrovaný blok, K je šifrovací kľúč a $E_K(\cdot)$ je šifrovacie zobrazenie príslušné ku kľúču K. Aby bolo možné dešifrovať, musí byť zobrazenie $E_K(\cdot)$ bijekciou, a preto musí k nemu existovať inverzné zobrazenie, ktoré sa často označuje symbolom $D_K(\cdot)$.

Veľmi častou otázkou, od ktorej závisí bezpečnosť šifry je, či množina všetkých zobrazení

$$\mathcal{E} = \{E_K(\cdot)|\ K \text{ prebieha množinu všetkých kľúčov}\}$$

uzavretá na operáciu skladania zobrazení $\circ$, t. j. či pre ľubovoľné kľúče K_1, K_2 existuje kľúč K_3 taký, že $E_{K_2} \circ E_{K_1} = E_{K_3}$, t. j. či $(\mathcal{E}, \circ)$ je grupoid. Na príklade cézarovskej šifry sme videli, že ak je množina šifrovacích zobrazení grupoidom, viacnásobné zašifrovanie rôznymi kľúčmi neprináša zvýšenie bezpečnosti danej šifry.

Práve spomenuté úvahy sa viedli i o veľmi rozšírenom šifrovacom algoritme DES (Data Encryption Standard), ktorý používa 56-bitový kľúč, v súvislosti s úspešným pokusom nájsť šifrovací kľúč paralelným výpočtom na obrovskom počte počítačov na sieti Internet. Silné náznaky toho, že šifrovacie zobrazenia netvoria grupoid viedli k algoritmu 3-DES používajúcemu trojnásobné šifrovanie.

Dekadický číselník odolný proti chybám

Pri vstupe údajov z klávesnice do počítača dochádza najčastejšie k dvom typom chýb a to preklep a zámena poradia dvoch susedných znakov. Preto sa rôzne číselníky (číselník tovarov, kníh, čísla účtov, osobné čísla zamestnancov) často navrhujú tak, aby bolo možné zistiť, či bolo vložené správne číslo alebo nie, za predpokladu, že nastala najviac jedna chyba typu preklep alebo susedná zámena. Množine čísel číselníka v dekadickom tvare sa často hovorí **dekadický kód**, ak sú čísla v binárnom tvare, hovoríme o **binárnom kóde**.

Zabezpečenie dekadického kódu proti jednému preklepu je jednoduché. Ku každému $(n-1)$-miestnemu číslu sa pridá n-tý znak – tzv. **kontrolná číslica** tak, aby bola splnená nasledujúca kontrolná rovnica:

$$a_1 \oplus a_2 \oplus \cdots \oplus a_n = 0 \qquad (\text{v } \mathbb{Z}_{10}) \tag{2.20}$$

Kód s kontrolnou rovnicou 2.20 však neobjaví žiadnu susednú zámenu, pretože operácia $\oplus$ je komutatívna na $\mathbb{Z}_{10}$.

Preto bol urobený ďalší pokus skonštruovať kontrolnú rovnicu v tvare

$$\delta_1(a_1) \oplus \delta_2(a_2) \oplus \cdots \oplus \delta_n(a_n) = 0 \qquad (\text{v } \mathbb{Z}_{10}), \tag{2.21}$$

kde $\delta_1, \delta_2 \ldots, \delta_n$ sú vhodné permutácie prvkov množiny $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Teória konečných grúp však dokázala, že žiadna kontrolná rovnica typu 2.21 nedokáže odhaliť všetky susedné zámeny dekadického kódu. Dokonca neexistuje komutatívna grupa s desiatimi prvkami, kde by sa dala kontrolná rovnica typu 2.21 použiť na odhalenie susedných zámen.

Teória nekomutatívnych grúp však dáva riešenie s využitím nasledujúceho pojmu:

Definícia 2.15. Diederova grupa $\mathbb{D}_n$ je konečná grupa rádu $2.n$ s grupovou operáciou $*$ tvaru

$$\left\{1, a, a^2, \ldots, a^{n-1},\ b, a*b, a^2*b, \ldots, a^{n-1}*b\right\}, \tag{2.22}$$

kde platí

$$a^n = 1 \quad (a^i \neq 1 \text{ pre } i = 1, 2, \ldots, n-1 \tag{2.23}$$

$$b^2 = 1 \quad (b \neq 1) \tag{2.24}$$

$$b * a = a^{n-1} * b \tag{2.25}$$

Diederovu grupu $\mathbb{D}_n$ budeme označovať

$$\mathbb{D}_n = \left\langle a, b \mid a^n = 1 = b^2,\ b * a = a^{n-1} * b \right\rangle \tag{2.26}$$

Pre nás bude dôležitá Diederova grupa $\mathbb{D}_5 = \left\langle a, b \mid a^5 = 1 = b^2,\ b * a = a^4 * b \right\rangle$. Prvky grupy $\mathbb{D}_5$ možno priradiť dekadickým znakom podľa nasledujúcej tabuľky:

1	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
0	1	2	3	4	5	6	7	8	9

Pre grupovú operáciu $*$ v grupe D_5 bude platiť nasledujúca schéma

$i * j$	$0 \leq j \leq 4$	$5 \leq j \leq 9$
$0 \leq i \leq 4$	$(i + j) \mod 5$	$5 + [(i + j) \mod 5]$
$5 \leq i \leq 9$	$5 + [(i - j) \mod 5]$	$(i - j) \mod 5$

z ktorej dostaneme tabuľku pre operáciu $*$

		j									
	$*$	0	1	2	3	4	5	6	7	8	9
i	0	0	1	2	3	4	5	6	7	8	9
	1	1	2	3	4	0	6	7	8	9	5
	2	2	3	4	0	1	7	8	9	5	6
	3	3	4	0	1	2	8	9	5	6	7
	4	4	0	1	2	3	9	5	6	7	8
	5	5	9	8	7	6	0	4	3	2	1
	6	6	5	9	8	7	1	0	4	3	2
	7	7	6	5	9	8	2	1	0	4	3
	8	8	7	6	5	9	3	2	1	0	4
	9	9	8	7	6	5	4	3	2	1	0

Ak definujeme permutáciu množiny $\{0,1,2,3,4,5,6,7,8,9\}$ predpisom

$$\delta(a^i) = a^{4-i} \quad \text{a} \quad \delta(a^i * b) = a^i * b \quad \text{pre } \forall\ i = 0,1,2,3,4 \tag{2.27}$$

a permutácie δ_i predpisom

$$\delta_i = \underbrace{\delta \circ \delta \circ \cdots \circ \delta}_{i-\text{krát}} = \delta^i \tag{2.28}$$

potom n-miestny dekadický kód s kontrolnou rovnicou

$$\delta_1(a_1) * \delta_2(a_2) * \cdots * \delta_n(a_n) = 1 \qquad \text{v } \mathbb{D}_5 \tag{2.29}$$

umožní objaviť všetky chyby, ktoré vznikli jedným preklepom alebo jednou susednou zámenou.

Cvičenia

1. Zistite či definované binárne operácie sú komutatívne a asociatívne:

   a) $a \blacktriangle b = b$ pre $\forall a, b \in \mathbb{Z}$

   b) $a \nabla b = |a + b - 2|$ pre $\forall a, b \in \mathbb{Z}$

   c) $a \diamond b = \frac{1}{2}(a+b)(b+1) - 1$ pre $\forall a, b \in \mathbb{Q}$

2. Nájdite binárnu operáciu na množine M, ktorá

   a) je asociatívna a komutatívna,

   b) je asociatívna, a nie je komutatívna,

   c) nie je asociatívna a je komutatívna,

   b) nie je ani komutatívna, ani asociatívna.

3. Dokážte, že množina všetkých prostých zobrazení množiny M na množinu M s operáciou skladania zobrazení je grupa.

4. Nech je daná neprázdna množina X a $M = \{A \mid A \subset X\}$ je množina všetkých jej podmnožín. Pre ľubovoľné množiny $A, B \in M$ definujeme operáciu $\triangle$ vzťahom $A \triangle B = (A - B) \cup (B - A)$. Akú algebraickú štruktúru predstavuje $(M, \triangle)$?

5. Nech $M = \{1, -1, i, -i\}$, kde $i = \sqrt{-1}$. Akú algebraickú štruktúru predstavuje $(M, \circ)$, keď $\circ$ je obvyklé násobenie komplexných čísel?

6. Akú algebraickú štruktúru tvorí $(\mathbb{N} \times \mathbb{N}_0, \circ)$, keď $(a, b) \circ (c, d) = (ac, ad + b)$, pre ľubovoľné $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}_0$?

7. Nech $M = \{A \mid A \subseteq X$ je množina všetkých podmnožín neprázdnej konečnej množiny X. Akú algebraickú štruktúru predstavujú $(M, \cup)$, $(M, \cap)$, $(M, \cup, \cap)$, kde $\cup$ je zjednotenie a $\cap$ prienik dvoch množín?

8. Nech $A = \{a_1 + a_2\sqrt{5} \mid a_1, a_2 \in \mathbb{Z}\}$. Akú algebraickú štruktúru tvorí $(A, \oplus, \otimes)$, kde $\oplus$ je sčítanie dvojčlenov a $\otimes$ je násobenie dvojčlenov.

9. Dokážte, že kongruencia modulo n je na množine celých čísel reláciou ekvivalencie.

10. Zostrojte tabuľky pre operácie $\oplus_n$ a $\otimes_n$ a pre $n = 3, 4, 5, 6$ zistite, aké algebraické štruktúry tvoria $(\mathbb{Z}_n, \oplus_n)$, $(\mathbb{Z}_n, \otimes_n)$, $(\mathbb{Z}_n, \oplus_n, \otimes_n)$.

Kapitola 3

Polynómy

3.1 Definícia polynómu a operácie s polynómami

Definícia 3.1. Nech $\mathcal{P} = (P, \oplus, \otimes)$ je pole, $x \in P$, n prirodzené číslo. Označme

$$x^n = \underbrace{x \otimes x \otimes \cdots \otimes x}_{n\text{–krát}} \tag{3.1}$$

Nech $a_0, a_1, \ldots, a_n$ sú pevne zvolené prvky poľa $\mathcal{P}$, x premenná. Potom výraz

$$p_n(x) = a_0 \oplus (a_1 \otimes x) \oplus (a_2 \otimes x^2) \oplus \cdots \oplus (a_n \otimes x^n) \tag{3.2}$$

nazveme **polynómom** nad poľom $\mathcal{P}$. Hovoríme, že polynóm $p_n(x)$ má **stupeň** n, ak $a_n \neq 0$. Prvky $a_0, a_1, \ldots, a_n$ nazývame **koeficienty** polynómu $p_n(x)$.

***Poznámka* 3.1.** *Pre zjednodušenie budeme namiesto zápisu* (3.2) *používať štandardný zápis*

$$p_n(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{3.3}$$

avšak vždy budeme mať na mysli, že polynóm (3.3) *je nad všeobecným poľom a nie nevyhnutne nad poľom reálnych alebo komplexných čísel.*

***Poznámka* 3.2.** *Podľa definície je*

- $p_1(x) = a_0 + a_1x$, *kde* $a_1 \neq 0$ – *polynóm 1. stupňa*
- $p_0(x) = a_0$, *kde* $a_0 \neq 0$ – *polynóm nultého stupňa*

Ukázalo sa výhodné považovať polynóm $p_0(x) = 0$ *za polynóm stupňa* -1.

Definícia 3.2. Hovoríme, že dva polynómy nad poľom $\mathcal{P}$

$$p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \tag{3.4}$$
$$q_m(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \tag{3.5}$$

sa **rovnajú**, a píšeme $p_n(x) = q_m(x)$, ak $n = m$ a pre všetky $i = 0, 1, \ldots, n$ platí $a_i = b_i$.

***Poznámka* 3.3.** *Každý polynóm definuje zobrazenie z množiny* P *do množiny* P. *Budeme však rozlišovať medzi polynómom a zobrazením, ktoré on definuje. Ak* $P = \mathbb{Z}_2$ *a* $p(x) = x^3+x^2+x+1$, $q(x) = x+1$, *potom* $p(x)$ *je polynómom tretieho stupňa a* $q(x)$ *je polynómom prvého stupňa, a teda podľa definície 3.2 ide o rôzne polynómy, pričom* $p(1) = 0 = q(1)$ *a* $p(0) = 1 = q(0)$ – *ako funkcie sú tieto polynómy rovnaké. Polynóm teda chápeme ako výraz určujúci výpočtovú schému a nie ako funkciu.*

Odteraz predpokladajme, že $m \leq n$.

Súčet polynómov $p_n(x),\ q_m(x)$ je polynóm $r_n(x)$

$$r_n(x) = p_n(x) + q_m(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + \\ + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n. \tag{3.6}$$

Súčin polynómov $p_n(x),\ q_m(x)$ je polynóm $s_{n+m}(x)$

$$s_{n+m}(x) = p_n(x).q_m(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n+m}x^{n+m}, \tag{3.7}$$

kde

$$c_k = \sum_{i+j=k} a_i.b_j \qquad \text{pre } k = 0, 1, \ldots, n+m. \tag{3.8}$$

Násobok polynómu $p_n(x)$ **prvkom** $\alpha \in P$ je polynóm $t_n(x)$

$$t_n(x) = \alpha.p_n(x) = (\alpha.a_0) + (\alpha.a_1)x + (\alpha.a_2)x^2 + \cdots + (\alpha.a_n)x^n. \tag{3.9}$$

3.2 Korene polynómov

Už stredovekí matematici sa zaoberali myšlienkou nájsť riešenie rovnice tvaru

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = b, \tag{3.10}$$

kde $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = p(x)$ je polynóm nad poľom $\mathcal{P} = (P, +, .)$ a $b \in P$. Riešiť rovnicu 3.10 znamená nájsť také číslo c patriace danému poľu, aby $p(c) = b$. Rovnica 3.10 sa dá upraviť na tvar

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + (a_0 - b) = 0,$$

čo v konečnom dôsledku znamená nájsť riešenie rovnice 3.10 v prípade, že $b = 0$. V ďalšom sa budeme zaoberať otázkou ako nájsť všetky riešenia takejto rovnice. Podotýkame, že táto úloha nepatrí medzi triviálne. Hoci sa matematici venovali problematike viac ako tisíc rokov, nepodarilo sa im túto úlohu uspokojivo vyriešiť. Našou ambíciou v nasledujúcich riadkoch bude povedať si niečo o koreňoch rovníc s komplexnými, reálnymi i racionálnymi koeficientmi. Najskôr uveďme definíciu koreňa polynómu.

Definícia 3.3. Nech $p_n(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ je polynóm nad poľom $\mathcal{P} = (P, +, .)$, $c \in P$. Hovoríme, že c je **koreňom polynómu** $p_n(x)$ alebo tiež nulovým bodom polynómu $p_n(x)$, ak platí $p_n(c) = 0$.

Pojem koreň polynómu je úzko spojený s pojmom pole. Ten istý polynóm nad jedným poľom koreň nemá, v inom poli však áno. Napr. $p_2(x) = x^2 + 2$ v poli $\mathbb{R}$ reálnych čísel nemá koreň, v poli $\mathbb{C}$ komplexných čísel korene má. Ak uvažujeme pole komplexných čísel, platí nasledujúca veta, ktorú uvádzame bez dôkazu:

Veta 3.1 (**Základná veta algebry**). *Nech* $(\mathbb{C}, +, .)$ *je pole komplexných čísel. Každý polynóm* $p_n(x)$ *stupňa aspoň prvého má v poli komplexných čísel aspoň jeden koreň.*

Veta 3.2. *Nech* $p_n(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ *je polynóm n-tého stupňa (t. j.* $a_n \neq 0$*) nad telesom komplexných čísel* $\mathbb{C}$ *a nech* $c \in \mathbb{C}$ *je ľubovoľné číslo. Potom*

$$p_n(x) = p_n(c) + (x - c).q_{n-1}(x), \tag{3.11}$$

kde $q_{n-1}(x)$ *je polynóm stupňa* $n - 1$.

DÔKAZ:

$$\begin{aligned} p_n(x) - p_n(c) = \\ = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n - (a_0 + a_1c + a_2c^2 + \cdots + a_nc^n) = \\ = (a_0 - a_0) + a_1(x - c) + a_2(x^2 - c^2) + \cdots + a_n(x^n - c^n) = \\ = (x - c).\underbrace{\left[a_1 + a_2(x + c) + \cdots + a_n(x^{n-1} + x^{n-2}c + \cdots + c^{n-1})\right]}_{q_{n-1}(x)} \end{aligned}$$

Jednoduchou úpravou posledného vzťahu dostaneme tvrdenie vety. ■

Polynóm $q_{n-1}(x)$ vo vzťahu 3.11 je polynóm $(n-1)$-ho stupňa, ktorý má vo všeobecnosti tvar $q_{n-1}(x)=b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}$, $b_{n-1} \neq 0$. Pri riešení praktických úloh (spojených napr. s hľadaním koreňov polynómu $p(x)$) nás zaujímajú koeficienty $b_0, b_1, \ldots, b_{n-1}$. Odvodíme postup, ako tieto koeficienty získať.

Nech $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm n-tého stupňa nad telesom komplexných čísel. Podľa (3.11) platí

$$p_n(x) = p_n(c) + (x - c).q_{n-1}(x), \tag{3.12}$$

kde $q_{n-1}(x)$ je polynóm stupňa $n-1$ a $q_{n-1}(x) = b_0+b_1x+b_2x^2+\cdots+b_{n-1}x^{n-1}$. Dosaďme do 3.12 a upravme:

$$a_0 + a_1x + \cdots + a_nx^n = p_n(c) + (x - c).(b_0 + b_1x + \cdots + b_{n-1}x^{n-1}).$$

Po úprave dostaneme:

$$\begin{aligned} (a_0 - p_n(c) + cb_0) + (a_1 - b_0 + cb_1)x + (a_2 - b_1 + cb_2)x^2 + \cdots + \\ + (a_{n-1} - b_{n-2} + cb_{n-1})x^{n-1} + (a_n - b_{n-1})x^n = 0. \end{aligned}$$

Ak uvážime, že $0 = 0x^0+0x^1+0x^2+\cdots+0x^n$, z rovnosti polynómov dostávame:

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= a_{n-1} + cb_{n-1} \\ b_{n-3} &= a_{n-2} + cb_{n-2} \\ &\cdots \\ b_{n-j} &= a_{n-j+1} + cb_{n-j+1} \\ &\cdots \end{aligned}$$

$$\begin{aligned} b_0 &= a_1 + cb_1 \\ p_n(c) &= a_0 + cb_0. \end{aligned}$$

Ide o rekurentné vzťahy, ktoré pri označení $b_{-1} = p_n(c)$ môžeme zapísať vzťahmi

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-j} &= a_{n-j+1} + cb_{n-j+1} \qquad j = 2, 3, \ldots, n+1. \end{aligned}$$

Získané rovnosti sa zapisujú do **Hornerovej schémy**:

	a_n	a_{n-1}	$\ldots$	a_1	a_0
c		cb_{n-1}	$\ldots$	cb_1	cb_0
	b_{n-1}	b_{n-2}	$\ldots$	b_0	$p_n(c)$

***Poznámka* 3.4.** *Hornerova schéma sa dá využiť na elegantné delenie polynómu normovaným lineárnym polynómom a rovnako aj na výpočet hodnoty polynómu v ľubovoľnom bode. Predstavuje užitočnú pomôcku v technickej praxi, kde sa často vyskytujú polynómy s racionálnymi koeficientmi. Poznamenávame, že do Hornerovej schémy sa zapisujú všetky koeficienty polynómu $p(x)$ (aj nuly!).*

Pre ozrejmenie postupu výpočtov v Hornerovej schéme, uvedieme príklad.

Príklad 3.1. Polynóm $p(x) = 2x^5 + 3x^3 + x^2 - 2x + 1$ vydeľme lineárnym polynómom $x - 2$.

Riešenie:

	2	0	3	1	-2	1
2		4	8	22	46	88
	2	4	11	23	44	89

Na základe výpočtu v Hornerovej schéme môžeme polynóm $p(x)$ napísať v tvare danom vzťahom 3.11

$$p(x) = (x-2)(2x^4 + 4x^3 + 11x^2 + 23x + 44) + 89.$$

Podiel je $2x^4 + 4x^3 + 11x^2 + 23x + 44$ a zvyšok 89. 89 je súčasne aj hodnota polynómu $p(x)$ v bode $c = 2$.

V predchádzajúcich úvahách sme pracovali s ľubovoľným číslom $c \in \mathbb{C}$. Ak nejaké c je koreň polynómu $p_n(x)$, tak platia nasledujúce tvrdenia.

Veta 3.3. *Nech c je koreňom polynómu $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ n-tého stupňa nad poľom komplexných čísel. Potom existuje polynóm $q_{n-1}(x)$ stupňa $n-1$ taký, že*

$$p_n(x) = (x - c).q_{n-1}(x). \tag{3.13}$$

DÔKAZ:
Podľa predpokladu c je koreňom polynómu $p_n(x)$, čo podľa definície 3.3 znamená, že $p_n(c) = 0$. Tvrdenie vety vyplýva priamo z tvrdenia vety 3.2. ■

Veta 3.4. *Nech $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm n-tého stupňa nad poľom komplexných čísel. Potom*

$$p_n(x) = a_n.(x - c_1).(x - c_2).\ldots.(x - c_n), \tag{3.14}$$

kde $c_1, c_2, \ldots, c_n$ sú korene polynómu $p_n(x)$.

DÔKAZ:
Tvrdenie vety vyplýva z n-násobného použitia vety 3.3. ■

Definícia 3.4. Vzťah 3.14 nazývame **rozklad polynómu** $p_n(x)$ **na súčin koreňových činiteľov**. Každý polynóm $(x-c_i)$ prvého stupňa zo vzťahu (3.14) nazývame **koreňovým činiteľom** .

Medzi koreňmi $c_1, c_2, \ldots, c_n$ polynómu $p_n(x)$ môžu byť niektoré korene rovnaké. Vtedy hovoríme o viacnásobných koreňoch. Uvedieme definíciu a vetu.

Definícia 3.5. Ak

$$p_n(x) = (x - c)^k.q_{n-k}(x), \tag{3.15}$$

kde $q_{n-k}(c) \neq 0$, hovoríme, že c je k-**násobným koreňom** polynómu $p_n(x)$.

Veta 3.5. *Nech $c_1, c_2, \ldots, c_r$ sú rôzne korene polynómu $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ n-tého stupňa nad poľom komplexných čísel. Nech c_i je k_i-násobný koreň $(i = 1, 2, \ldots, r)$. Potom $k_1 + k_2 + \cdots + k_r = n$ a platí:*

$$p_n(x) = a_n.(x - c_1)^{k_1}.(x - c_2)^{k_2}.\ldots.(x - c_r)^{k_r}. \tag{3.16}$$

Vyslovené vety naznačujú, že úloha hľadať korene daného polynómu je ekvivalentná s úlohou nájsť rozklad polynómu na súčin koreňových činiteľov nad daným poľom. O tom, koľko koreňov má polynóm stupňa n nad poľom komplexných čísel, hovorí nasledujúca veta, ktorá je priamym dôsledkom základnej vety algebry – veta 3.1, str. 39.

Veta 3.6. *Polynóm stupňa n nad poľom komplexných čísel má v poli komplexných čísel práve n koreňov, ak tieto počítame aj s ich násobnosťami.*

Veta 3.7. *Rovnosť polynómov*

$$\begin{aligned} p_n(x) &= a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \\ q_m(x) &= b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \end{aligned}$$

nad poľom komplexných čísel $\mathbb{C}$ nastáva práve vtedy, keď pre každé $x \in \mathbb{C}$ je $p_n(x) = q_m(x)$.

Dôkaz:
Ak $p_n = q_m$ v zmysle rovnosti polynómov (pozri definíciu 3.2 na str. 38), potom $m = n$ a $a_i = b_i$ pre všetky $i = 0, 1, \ldots, n$, a preto aj $p_n(x) = q_m(x)$ pre všetky $x \in \mathbb{C}$.
Nech pre každé $x \in \mathbb{C}$ $p_n(x) = q_m(x)$. Predpokladajme $m \leq n$. Položme $r(x) = p_n(x) - q_m(x)$

$$r(x) = (a_0-b_0)+(a_1-b_1)x+\cdots+(a_m-b_m)x^m+a_{m+1}x^{m+1}+\cdots+a_nx^n. \quad (3.17)$$

Polynóm $r(x) = 0$ pre všetky $x \in \mathbb{C}$, čo je možné len tak, že všetky jeho koeficienty sú nulové. Ak by totiž niektorý z koeficientov bol nenulový, $r(x)$ by mal nananajvýš n koreňov. Musí teda byť $m = n$ a $a_i = b_i$ pre $i = 0, 1, \ldots, n$. ■

Ako sme už uviedli, nájsť korene polynómu n-tého stupňa nie je jednoduchá záležitosť. Uspokojivo vieme nájsť korene polynómov $2., 3.$ *a* $4.$ stupňa. Hľadať a nájsť korene polynómov vyššieho stupňa pri riešení praktických úloh je skôr predmetom numerickej matematiky než algebry. Pokiaľ predpokladáme, že skúmaný polynóm má racionálne korene, často ich umožní nájsť nasledujúca veta.

Veta 3.8. *Nech $p_n(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$ je polynóm s celočíselnými koeficientmi. Ak racionálne číslo $r = \frac{p}{q}$, kde p, q sú nesúdeliteľné čísla, je jeho koreňom, potom p delí a_0 a q delí a_n.*

Dôkaz:
Ak $r = \frac{p}{q}$ je koreňom polynómu $p_n(x)$, potom $p_n(r) = 0$, a teda

$$0 = a_0 + a_1\frac{p}{q} + a_2\frac{p^2}{q^2} + \cdots + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + a_n\frac{p^n}{q^n}$$

$$\begin{aligned} 0 &= a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_{n-1}p^{n-1}q + a_np^n \\ a_0q^n &= -\big(a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_{n-1}p^{n-1}q + a_np^n\big) \\ &= -p\big(a_1q^{n-1} + a_2pq^{n-2} + \cdots + a_{n-1}p^{n-2}q + a_np^{n-1}\big) \qquad (3.18) \\ a_np^n &= -\big(a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_{n-1}p^{n-1}q\big) \\ &= -q\big(a_0q^{n-1} + a_1pq^{n-2} + a_2p^2q^{n-3} + \cdots + a_{n-1}p^{n-1}\big) \qquad (3.19) \end{aligned}$$

Pravá strana v 3.18 je deliteľná p, musí byť p deliteľná aj ľavá strana vzťahu 3.18. Keďže $p,\ q$ sú nesúdeliteľné čísla, potom p delí a_0. Obdobnou úvahou zo vzťahu 3.19 dostaneme, že q delí a_n. ■

Postup pri zisťovaní, ktoré racionálne číslo je koreňom daného polynómu môžeme zhrnúť do nasledujúcich troch bodov:

1. Vyhľadáme všetkých deliteľov $q_1, q_2, \ldots, q_s$ koeficienta a_n.
2. Vyhľadáme všetkých deliteľov $p_1, p_2, \ldots, p_r$ koeficienta a_0.
3. Každé racionálne číslo, ktoré je koreňom polynómu, musí mať tvar $\frac{p_i}{q_j}$. Urobíme podiely $\frac{p_i}{q_j}$ pre všetky i, j, pre ktoré sú p_i, q_j nesúdeliteľné. Skúškou sa presvedčíme, ktoré z týchto čísel je koreňom.

Príklad 3.2. Daný je polynóm štvrtého stupňa $p(x) = x^4 + 3x^3 - x^2 - 5x + 2$. Nájdime všetky jeho racionálne korene.

Riešenie:
$a_n = a_4 = 1$, $a_0 = 2$, podľa tvrdenia vety 3.8 p musí deliť 2 a q musí deliť 1. Z toho vyplýva, že $p \in \{\pm1, \pm2\}$ a $q \in \{\pm1\}$. Ak označíme racionálny koreň písmenom t, tak $t \in \{\pm1, \pm2\}$. Stačí overiť, pre ktoré t, platí $p(t) = 0$. Využijeme pri tom Hornerovu schému.

	1	3	-1	-5	2
1		1	4	3	-2
	1	4	3	-2	0

	1	3	-1	-5	2
-1		-1	-2	3	2
	1	2	-3	-2	$4 \neq 0$

Z výpočtov vidíme, že 1 je koreňom polynómu a -1 koreňom nie je. Na základe vety 3.3 napíšeme polynóm $p(x)$ v tvare $p(x) = (x-1)(x^3 + 4x^2 + 3x - 2)$ a v ďalšom sa sústredíme len na polynóm $q(x) = (x^3 + 4x^2 + 3x - 2)$. Ak je

t koreňom polynómu $p(x)$, tak je aj koreňom polynómu $q(x)$ (presvedčte sa o tom!).

	1	4	3	-2
2		2	12	30
	1	6	15	$28 \neq 0$

	1	4	3	-2
-2		-2	-4	2
	1	2	-1	0

Našli sme ďalší koreň, a ak využijeme zápis $p(x) = (x-1)(x+2)(x^2+2x-1)$, riešením kvadratickej rovnice $x^2 + 2x - 1$ sa presvedčíme, že polynóm $p(x)$ už nemá žiadne racionálne korene.

***Poznámka* 3.5.** *Vo vete 3.8 sme predpokladali, že polynóm $p(x)$ má celočíselné koeficienty. Veta však platí aj pre polynómy s racionálnymi koeficientmi. Stačí dať koeficienty polynómu na spoločného menovateľa.*

V predchádzajúcich riadkoch sme sa zaoberali polynómami s racionálnymi aj celočíselnými koeficientmi a ich koreňmi. Teraz sa budeme zaoberať špeciálnymi vlastnosťami polynómov s reálnymi koeficientmi.

Veta 3.9. *Nech $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm n-tého stupňa nad telesom komplexných čísel. Nech všetky koeficienty polynómu $p_n(x)$ sú reálne čísla. Ak komplexné číslo $c = \alpha + i\beta$ je koreňom polynómu $p_n(x)$, potom aj komplexne združené číslo $\overline{c} = \alpha - i\beta$ je koreňom polynómu $p_n(x)$.*

Dôkaz:
Ak číslo $c = \alpha + i\beta$ je koreňom polynómu, tak

$$a_0 + a_1c + a_2c^2 + \cdots + a_nc^n \quad = \quad 0.$$

Z rovnosti dvoch komplexných čísel vyplýva rovnosť ich komplexne združených čísel

$$\overline{a_0 + a_1c + a_2c^2 + \cdots + a_nc^n} \quad = \quad \overline{0},$$

z čoho po úpravách dostaneme

$$\overline{a_0} + \overline{a_1c} + \overline{a_2c^2} + \cdots + \overline{a_nc^n} \quad = \quad \overline{0}.$$

Koeficienty polynómu sú podľa predpokladu vety reálne čísla, čiže platí $\overline{a}_i = a_i$, pre $i = 0, 1, 2, \ldots, n$, teda

$$a_0 + a_1\overline{c} + a_2(\overline{c})^2 + \cdots + a_n(\overline{c})^n \quad = \quad 0.$$

To ale znamená, že $\overline{c}$ je koreňom polynómu $p_n(x)$. ■

Ak budú čísla $c = \alpha + i\beta$ a $\overline{c} = \alpha - i\beta$, pričom $\beta \neq 0$ koreňmi polynómu, potom príslušný súčin koreňových činiteľov bude mať tvar

$$(x-c)(x-\overline{c}) = x^2 - x.(c+\overline{c}) + c.\overline{c} = x^2 - 2\alpha.x + (\alpha^2+\beta^2),$$

čo je kvadratický trojčlen s reálnymi koeficientmi. Ak zohľadníme tento fakt spolu s výsledkami vety 3.5 dostaneme nasledujúce tvrdenie.

Veta 3.10. *Nech $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm n-tého stupňa s reálnymi koeficientmi. Nech $c_1, c_2, \ldots, c_r$ sú všetky navzájom rôzne reálne korene s násobnosťami $n_1, n_2, \ldots, n_r$ a čísla $(\alpha_1 + i\beta_1), (\alpha_2 + i\beta_2), \ldots, (\alpha_s + i\beta_s)$ všetky rôzne komplexné korene také, že $\beta_k > 0$ pre $k = 1, 2, \ldots, s$ s násobnosťami $m_1, m_2, \ldots, m_s$. Potom aj čísla $(\alpha_1 - i\beta_1), (\alpha_2 - i\beta_2), \ldots, (\alpha_s - i\beta_s)$ sú po rade $m_1, m_2, \ldots, m_s$ - násobné korene polynómu $p_n(x)$ a platí*

$$\begin{aligned} p_n(x) = a_n.(x-c_1)^{n_1}.(x-c_2)^{n_2}.\ldots.(x-c_r)^{n_r}. \\ .(x^2+p_1x+q_1)^{m_1}.(x^2+p_2x+q_2)^{m_2}.\ldots.(x^2+p_sx+q_s)^{m_s}, \end{aligned} \quad (3.20)$$

kde $p_j = -2\alpha_j$ pre $j = 1, 2, \ldots, r$ a $q_k = \alpha_k^2 + \beta_k^2$ pre $k = 1, 2, \ldots, s$, pričom platí

$$n = n_1 + n_2 + \cdots + n_r + 2(m_1 + m_2 + \cdots + m_s).$$

Vzťah (3.20) *môžeme skrátene zapísať takto:*

$$p_n(x) = a_n. \prod_{j=1}^{r} (x-c_j)^{n_j}. \prod_{k=1}^{s} (x^2+p_kx+q_k)^{m_k}. \quad (3.21)$$

Dôkaz:
Dôkaz priamo vyplýva z vety 3.5 a 3.9.

3.3 Opakovaná Hornerova schéma a Taylorov rozvoj polynómu

V podkapitole 3.2 sme sa už stretli s pojmom Hornerova schéma a jej jednorazovým použitím, či už pri hľadaní hodnoty polynómu v danom bode alebo overovaní či číslo c je koreňom polynómu. Hornerova schéma sa dá použiť aj opakovane. Nech $p(x)$ je polynóm n-tého stupňa a $c \in \mathbb{C}$ je ľubovoľný prvok. Použitím Hornerovej schémy dostaneme

$$p(x) = p(c) + (x - c)q_1(x), \tag{3.22}$$

kde $q_1(x)$ je nejaký polynóm stupňa $n - 1$. Ak použijeme Hornerovu schému opakovane na polynóm $q_1(x)$, dostaneme

$$q_1(x) = q_1(c) + (x - c)q_2(x),$$

kde $q_2(x)$ je nejaký polynóm stupňa $n - 2$. Po dosadení do 3.22 dostaneme

$$\begin{aligned} p(x) &= p(c) + (x - c)\left[q_1(c) + (x - c)q_2(x)\right] \\ &= p(c) + (x - c)q_1(x) + (x - c)^2 q_2(x). \end{aligned}$$

Naznačený postup na daný polynóm n-tého stupňa môžeme uplatniť celkove n-krát. Označme $p(x) = q_0(x)$ získame vzťahy môžeme zapísať

$$q_{k-1}(x) = q_{k-1}(c) + (x - c)q_k(x), \qquad k = 1, 2, \ldots, n, \tag{3.23}$$

kde $q_k(x)$ je polynóm stupňa $n-k$. Spätným dosadzovaním do vzťahov určených 3.23 dostaneme

$$p(x) = p(c) + q_1(c)(x - c) + q_2(c)(x - c)^2 + \cdots + q_n(c)(x - c)^n \tag{3.24}$$

Ak uvážime, že $(x-c)^0 = 1$, vzťahom 3.24 sme polynóm $p(x)$ vyjadrili pomocou mocnín $(x - c)^k$ pre $k = 0, 1, \ldots, n$.

Príklad 3.3. Polynóm $p(x) = x^4-5x^3+2x^2+x-2$ vyjadríme pomocou mocnín $(x - 1)^k$, $k = 0, 1, \ldots, 4$.
Riešenie:
Použijeme opakovanú Hornerovu schému pre $c = 1$:

	1	-5	2	1	-2
1		1	-4	-2	-1
	1	-4	-2	-1	$\boxed{-3} = p(1)$
1		1	-3	-5	
	1	-3	-5	$\boxed{-6} = q_1(1)$	
1		1	-2		
	1	-2	$\boxed{-7} = q_2(1)$		
1		1			
	1	$\boxed{-1} = q_3(1)$			
1					
	$\boxed{1} = q_4(1)$				

Potom podľa 3.24

$$p(x) = -3 - 6(x-1) - 7(x-1)^2 - (x-1)^3 - (x-1)^4$$

Opakovaná Hornerova schéma je užitočným nástrojom aj na určovanie násobnosti koreňov polynómu. Ukážme si to na príklade.

Príklad 3.4. Daný je polynóm $p(x) = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16$ a číslo $c = -2$. Presvedčme sa, že je koreňom daného polynómu a určme jeho násobnosť.

Riešenie:
Použijeme opäť opakovanú Hornerovu schému pre $c = -2$

	1	7	16	8	-16	-16
-2		-2	-10	-12	8	16
	1	5	6	-4	-8	$\boxed{0}$
-2		-2	-6	0	8	
	1	3	0	-4	$\boxed{0}$	
-2		-2	-2	4		
	1	1	-2	$\boxed{0}$		
-2		-2	2			
	1	-1	$\boxed{0}$			
-2		-2				
	1	$\boxed{-3} \neq 0$				

Z výpočtu vyplýva, že prípad, keď $p(-2) = 0$, nastal celkom 4-krát. Teda $c = -2$ je štvornásobným koreňom polynómu. Z Hornerovej schémy zistíme aj rozklad

polynómu $p(x)$ na súčin koreňových činiteľov, čiže $p(x) = (x+2)^4(x-1)$. Piaty koreň polynómu je zrejmý priamo z rozkladu - je ním číslo 1. Teda $x_{1,2,3,4} = -2$ a $x_5 = 1$.

Úvahy okolo opakovanej Hornerovej schémy vyústili do vzťahu 3.24. Pozorný čitateľ objavil analógiu medzi spomínaným vzťahom a Taylorovým rozvojom funkcie, s ktorým sa často stretávame v diferenciálnom počte. V diferenciálnom počte na uskutočnenie Taylorovho rozvoja potrebujeme poznať derivácie danej funkcie, čo dostaneme len cez limity. Algebra takýmito prostriedkami vo všeobecnosti nedisponuje. Ak sa však sústredíme len na polynómy, zaobídeme sa aj bez limity. Zavedieme deriváciu polynómu a vyslovíme vetu o Taylorovom rozvoji polynómu.

Definícia 3.6. Nech $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm n-tého stupňa nad poľom komplexných čísel. **Deriváciou polynómu** $p_n(x)$ nazveme polynóm $Dp_n(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$.

***Poznámka* 3.6.** *V ďalšom budeme používať označenie $D^kp(x)$ pre k-tu deriváciu polynómu $p(x)$, pričom $D^kp(x) = D(D^{k-1}p(x))$ pre $k = 1, 2, \ldots$ a pre $k = 0$ položíme $D^0p(x) = p(x)$. Poznamenávame, že pre derivovanie súčtu a súčinu polynómov platia tie isté pravidlá ako pre derivovanie ľubovoľných funkcií, s ktorými sa stretávame v diferenciálnom počte.*

Dá sa dokázať veta o Taylorovom rozvoji polynómu (pozri v [11]) :

Veta 3.11. *Nech $p_n(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$ je polynóm n-tého stupňa nad poľom komplexných čísel a nech $c \in \mathbb{C}$ je ľubovoľné číslo. Potom pre prvky $q_k(c) \quad k = 0, 1, 2, \ldots, n$ vo vzťahu 3.24 platí*

$$q_k(c) = \frac{D^kp(c)}{k!} \qquad k = 0, 1, \ldots, n,$$

teda vzťah 3.24 *môžeme prepísať na tvar*

$$p(x) = p(c) + \frac{Dp(c)}{1!}(x-c) + \frac{D^2p(c)}{2!}(x-c)^2 + \cdots + \frac{D^np(c)}{n!}(x-c)^n \ .$$

3.4 Deliteľnosť polynómov

V predchádzajúcich častiach sme naznačili, že polynómy sa v okruhu polynómov nad daným poľom často správajú ako celé čísla v okruhu $(\mathbb{Z}, +, \cdot)$. Ukázali sme, že polynómy sa dajú sčítať, násobiť, deliť lineárnym polynómom $x - c$ so zvyškom alebo bez neho. Vzťah 3.20 vo vete 3.10 zas pripomína analógiu s rozkladom celého čísla na súčin prvočíselných základov, napr. $360 = 2^3 \cdot 3^2 \cdot 5$. V tejto sekcii budeme pokračovať v hľadaní analógie medzi týmito dvomi okruhmi. Zavedieme pojmy najväčší spoločný deliteľ polynómov, najmenší spoločný násobok, ako aj pojem ireducibilný polynóm nad daným poľom.

Definícia 3.7. Nech $p(x)$ a $q(x)$ sú dva polynómy z nejakého okruhu polynómov. Hovoríme, že polynóm $q(x)$ **delí** polynóm $p(x)$, ak existuje taký polynóm $r(x)$ z daného okruhu polynómov, že platí

$$p(x) = q(x).r(x) \tag{3.25}$$

a značíme to $q(x) \mid p(x)$. Polynóm $q(x)$ nazveme **triviálnym deliteľom** polynómu $p(x)$, ak stupeň polynómu $q(x)$ je nulový, alebo $q(x) \mid p(x)$ a súčasne $p(x) \mid q(x)$ (t. j. ak je polynóm $p(x)$ konštantným násobkom polynómu $q(x)$).

Definícia 3.8. Ak polynóm $r(x)$ delí oba polynómy $p(x)$ aj $q(x)$ hovoríme, že $r(x)$ je **spoločným deliteľom polynómov** $p(x)$ **a** $q(x)$.

Hovoríme, že $r(x)$ je **najväčší spoločný deliteľ polynómov** $p(x)$, $q(x)$, ak je spoločným deliteľom polynómov $p(x)$, $q(x)$ a je deliteľný každým iným spoločným deliteľom týchto polynómov. Značíme $r(x) = NSD(p(x), q(x))$.

***Poznámka* 3.7.** *Najväčší spoločný deliteľ $r(x)$ polynómov $p(x)$, $q(x)$ nie je určený jednoznačne, pretože ak $r(x)|p(x)$, t. j. ak existuje $s(x)$ taký, že $p(x) = r(x).s(x)$, potom pre ľubovoľný nenulový prvok $a \in \mathcal{P}$ je $p(x) = [a.r(x)].[a^{-1}.s(x)]$, čo znamená, že aj $a.r(x)|p(x)$.*

Normovaný najväčší spoločný deliteľ polynómov $p(x)$**,** $q(x)$ je ten ich najväčší spoločný deliteľ, ktorého koeficient pri najvyššej mocnine premennej x je rovný 1.

Položme si otázku – ako deliť dva polynómy? Postup popíšeme v nasledujúcich riadkoch. Majme polynómy:

$$p_n(x) \quad = \quad a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

$$q_m(x) \quad = \quad b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m.$$

Budeme predpokladať, že $m \leq n$. Vychádzame z toho, že polynóm $p_n(x)$ vyjadríme nasledujúcim vzťahom:

$$p_n(x) = \underbrace{\left[p_n(x) - \frac{a_n}{b_m}.q_m(x).x^{n-m}\right]}_{p_{n-1}(x)} + q_m(x).\left(\frac{a_n}{b_m}.x^{n-m}\right) =$$

$$= p_{n-1}(x) + q_m(x).c_{n-m}.x^{n-m}$$

V poslednej rovnici je $p_{n-1}(x)$ polynóm stupňa nanajvýš $n-1$ a $c_{n-m} = \frac{a_n}{b_m}$. Ak je stupeň polynómu $p_{n-1}(x)$ väčší alebo rovný ako m môžeme pokračovať ďalej

$$\begin{aligned} p_{n-1}(x) &= p_{n-2}(x) + q_m(x).c_{n-m-1}.x^{n-m-1}, \\ p_{n-2}(x) &= p_{n-3}(x) + q_m(x).c_{n-m-2}.x^{n-m-2}, \\ &\cdots \\ p_{n-k+1}(x) &= p_{n-k}(x) + q_m(x).c_{n-m-k+1}.x^{n-m-k+1}, \end{aligned}$$

a skončíme vtedy, keď stupeň polynómu $p_{n-k}(x)$ bude prvýkrát menší než m. Platí:

$$p_n(x) = \underbrace{p_{n-1}(x)}_{p_{n-2}(x)+q_m(x).c_{n-m-1}.x^{n-m-1}} + q_m(x).c_{n-m}.x^{n-m} =$$

$$= \underbrace{p_{n-2}(x)}_{p_{n-3}(x)+q_m(x).c_{n-m-2}.x^{n-m-2}} + q_m(x).c_{n-m}.x^{n-m} + q_m(x).c_{n-m-1}.x^{n-m-1} =$$

$$\cdots$$

$$= \underbrace{p_{n-k}(x)}_{r(x)} + q_m(x).\underbrace{(c_{n-m}.x^{n-m} + c_{n-m-1}.x^{n-m-1} + \cdots + c_1.x + c_0)}_{s(x) - \text{ polynóm stupňa } n-m}$$

Práve popísaný postup vedie ku vzťahu

$$p_n(x) = q_m(x).s(x) + r(x), \tag{3.26}$$

kde $s(x)$ je polynóm stupňa $n-m$ a $r(x)$ je polynóm stupňa menšieho než m. Práve uvedený vzťah je tvrdením vety o delení polynómov so zvyškom.

Veta 3.12. *(O delení so zvyškom) Nech $p(x)$ je polynóm n-tého stupňa a $q(x)$ je polynóm m-tého stupňa nad poľom komplexných čísel, pričom $m \leq n$. Nech $q(x) \neq 0$. Potom existujú nad poľom komplexných čísel polynómy $s(x)$ a $r(x)$ s vlastnosťou*

$$p_n(x) = q_m(x).s(x) + r(x),$$

pričom $s(x)$ je polynóm stupňa $n-m$ a $r(x)$ je polynóm stupňa menšieho než m.

Všimnime si, že polynóm $q(x) \neq 0$ delí polynómom $p(x)$ práve vtedy, keď zvyšok $r(x)$ po delení sa rovná 0. V nasledujúcej vete uvedieme základné vlastnosti deliteľnosti polynómov.

Veta 3.13.

a) Ak polynóm $p(x)$ je deliteľný polynómom $q(x)$ a polynóm $q(x)$ je deliteľný polynómom $r(x)$, potom aj polynóm $p(x)$ je deliteľný polynómom $r(x)$.

b) Ak polynómy $p(x)$ a $q(x)$ sú deliteľné polynómom $r(x)$, potom aj polynómy $p(x) \pm q(x)$ sú deliteľné polynómom $r(x)$.

c) Ak je polynóm $p(x)$ deliteľný polynómom $q(x)$, potom aj polynóm $p(x) \cdot s(x)$ je deliteľný polynómom $q(x)$ pre ľubovoľný polynóm $s(x)$.

d) Každý polynóm je deliteľný polynómom nultého stupňa.

e) Ak je polynóm $p(x)$ deliteľný polynómom $q(x)$, potom je polynóm $p(x)$ deliteľný aj polynómom $k \cdot q(x)$ pre ľubovoľnú nenulovú konštantu $k \in \mathbb{C}$, $k \neq 0$.

f) Ak je polynóm $p(x)$ deliteľný polynómom $q(x)$ a oba polynómy majú rovnaký stupeň, potom existuje nenulová konštanta $k \in \mathbb{C}$ taká, že $p(x) = k \cdot q(x)$.

Dôkaz:
Triviálny, všetky tvrdenia sa dajú ľahko dokázať z definície deliteľnosti polynómov. (Urobte to!) Na ukážku urobíme dôkaz bodu b).

Podľa predpokladu sú polynómy $p(x)$ a $q(x)$ sú deliteľné polynómom $r(x)$. Potom existujú polynómy $s_1(x)$ a $s_2(x)$ také, že platí $p(x) = r(x) \cdot s_1(x)$ a $q(x) = r(x) \cdot s_2(x)$. Potom

$$p(x) \pm q(x) = r(x) \cdot s_1(x) \pm r(x) \cdot s_2(x) = r(x) \cdot [s_1(x) \pm s_2(x)].$$

Ak označíme $s(x) = s_1(x) \pm s_2(x)$, dostaneme tvrdenie bodu b). ■

Pri výpočte najväčšieho spoločného deliteľa, resp. najmenšieho spoločného násobku polynómov, potrebujeme poznať rozklady daných polynómov na súčin ireducibilných polynómov nad daným poľom.

Definícia 3.9. Hovoríme, že polynóm $p(x)$, $st\{p(x)\} \geq 1$ nad poľom $\mathcal{P}$ je **reducibilný**, ak existujú dva polynómy $q(x)$, $r(x)$ oba aspoň prvého stupňa také, že

$$p(x) = q(x).r(x). \tag{3.27}$$

V opačnom prípade hovoríme, že $p(x)$ je **ireducibilný** polynóm.

***Poznámka* 3.8.** *Pri určovaní ireducibility polynómu je vždy dôležité uviesť, nad ktorým poľom polynóm uvažujeme. Polynóm môže byť nad jedným poľom ireducibilný, nad druhým už reducibilný. Napr. polynóm $p(x) = x^2 + 2$ je nad poľom reálnych čísel ireducibilný. $p(x)$ je polynóm druhého stupňa. Ak by bol reducibilný nad poľom reálnych čísel, musel by sa dať napísať ako súčin polynómov prvého stupňa. Nemá však reálne korene, nedá sa vyjadriť ako súčin koreňových činiteľov, ktoré sú polynómami prvého stupňa. Nad poľom komplexných čísel je už reducibilný, lebo v poli komplexných čísel má korene a vieme ho vyjadriť ako súčin koreňových činiteľov $x^2 + 2 = (x - i\sqrt{2})(x + i\sqrt{2})$.*

Poznámka 3.8 nás (možno?) privedie k úvahe o súvislosti existencie koreňov polynómu a jeho ireducibilite nad daným poľom. Môžeme tvrdiť, že polynóm je ireducibilný nad daným poľom, ak nemá v tomto poli korene? Zaoberajme sa najskôr polynómami nad poľom reálnych čísel $\mathbb{R}$ a vyslovme tvrdenie.

Veta 3.14. *Polynóm $p(x)$ s reálnymi koeficientmi je ireducibilný nad poľom reálnych čísel $\mathbb{R}$ práve vtedy, keď $st\{p(x)\} = 1$ alebo $st\{p(x)\} = 2$ a $p(x)$ nemá reálne korene.*

Dôkaz:
Nech polynóm $p(x)$ je ireducibilný nad poľom reálnych čísel $\mathbb{R}$. Zrejme $st\{p(x)\} \geq 1$. Podľa vety 3.1 v poli komplexných čísel má $p(x)$ aspoň jeden koreň. Nech tým koreňom je $c \in \mathbb{C}$. Môžu nastať dva prípady: $c \in \mathbb{R}$ alebo $c \in (\mathbb{C} - \mathbb{R})$. Ak $c \in \mathbb{R}$, tak podľa vety 3.3 platí, že $p(x) = (x - c)q(x)$. Keďže $p(x)$ je ireducibilný nad poľom reálnych čísel, tak $q(x)$ musí byť stupňa 0, čiže konštanta. Potom z rovnosti polynómov vyplýva aj rovnosť ich stupňov. Teda $st\{p(x)\} = 1$. V druhom prípade ak $c \in (\mathbb{C} - \mathbb{R})$, tak podľa vety 3.2 je koreňom

polynómu $p(x)$ aj $\overline{c} \in (\mathbb{C} - \mathbb{R})$ a $p(x) = (x - c)(x - \overline{c})q(x)$. Z rovnakého dôvodu ako v predchádzajúcom prípade stupeň polynómu $q(x)$ je 0 a stupeň polynómu $p(x)$ je 2. Naopak, ak $st\{p(x)\} = 1$, tak polynóm $p(x)$ je nad poľom reálnych čísel ireducibilný. Ak $st\{p(x)\} = 2$ a má len komplexné korene, tak $p(x) = x^2 - 2\alpha x + (\alpha^2 + \beta^2)$ a to je možné len keď $p(x) = (x - c)(x - \overline{c})$. Čiže $p(x)$ je nad poľom reálnych čísel ireducibilný. ■

***Poznámka* 3.9.** *Dá sa dokázať, že každý polynóm $p(x)$ stupňa 2 alebo 3 je ireducibilný nad poľom $\mathcal{P}$ práve vtedy, keď nemá v poli $\mathcal{P}$ korene. Toto platí pre ľubovoľné pole, konečné či nekonečné.*

Ako rýchlo nahliadneme z nasledujúceho príkladu, tvrdenie sa nedá zovšeobecniť na prípady, keď $st\{p(x)\} \geq 4$. Nad poľom reálnych čísel $\mathcal{R} = (\mathbb{R}, +, .)$ uvažujme polynóm $p(x) = x^4 + 1$. Keďže pre ľubovoľné $c \in \mathbb{R}$ platí $c^4 \geq 1$, $p(x)$ nemá v poli reálnych čísel korene. Napriek tomu je tento polynóm nad poľom $\mathcal{R}$ reducibilný, lebo $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$.

Príklad 3.5. Nad poľom reálnych čísel $\mathbb{R}$ rozložme na súčin ireducibilných polynómov a nájdime najväčší spoločný deliteľ polynómov $p(x)$ a $q(x)$, keď $p(x) = x^3 - x^2 + x - 1$ a $q(x) = 4x^4 - 13x^2 + 9$.

Riešenie:
Polynóm $p(x)$ má jeden z koreňov $c = 1$. Presvedčme sa o tom Hornerovou schémou.

	1	-1	1	-1
1		1	0	1
	1	0	1	0

Polynóm môžeme napísať v tvare $p(x) = (x - 1)(x^2 + 1)$, kde $x^2 + 1$ je už ireducibilný polynóm nad $\mathbb{R}$. Substitúciou $x^2 = t$ znížime stupeň polynómu $q(x)$ a riešením kvadratickej rovnice získame riešenie $t_1 = \dfrac{9}{4}$ a $t_2 = 1$, odkiaľ korene polynómu sú $x_1 = \dfrac{3}{2}$, $x_2 = -\dfrac{3}{2}$, $x_3 = 1$, $x_4 = -1$. Rozklad polynómu na súčin koreňových činiteľov a zároveň aj na súčin ireducibilných polynómov nad $\mathbb{R}$ je $q(x) = (x - \frac{3}{2})(x + \frac{3}{2})(x - 1)(x + 1)$. Porovnaním oboch rozkladov zistíme, že jediným polynómom, ktorý delí súčasne polynóm $p(x)$ aj $q(x)$ je $x - 1$. Je to normovaný najväčší spoločný deliteľ.

Na ilustráciu pojmu najväčší spoločný deliteľ polynómov uvedieme ešte jeden príklad.

Príklad 3.6. Nájdime všetkých spoločných deliteľov polynómov
$p(x) = 2x^4 - 6x^3 - 6x^2 + 22x - 12 = 2(x-1)^2(x+2)(x-3)$,
$q(x) = x^4 + 8x^3 + 15x^2 - 4x - 20 = (x-1)(x+2)^2(x+5)$.

Riešenie:
Spoločným deliteľom polynómov $p(x)$ a $q(x)$ je každý polynóm, ktorý má tvar $k(x-1)^m(x+2)^n$, kde $k \neq 0$ je ľubovoľné číslo a $m, n \in \{0, 1\}$. Normovaný najväčší spoločný deliteľ je $(x-1)(x+2)$.

Z uvedených príkladov vidíme, že ak chceme určiť spoločných deliteľov polynómov, potrebujeme poznať ich rozklad na súčin koreňových činiteľov, resp. na súčin ireducibilných polynómov nad daným poľom. To v niektorých prípadoch nie je celkom triviálna záležitosť. Iný spôsob ako určiť najväčšieho spoločného deliteľa (a tým aj všetkých spoločných deliteľov) daných polynómov je použitie Euklidovho algoritmu.

3.5 Euklidov algoritmus

Nech sú dané dva nenulové polynómy $p(x)$ a $q(x)$, pričom $st\{p(x)\} \geq st\{q(x)\}$ a $q(x) \nmid p(x)$. Polynóm $p(x)$ vydelíme polynómom $q(x)$ a dostaneme

$$p(x) = q(x).s(x) + r_1(x), \tag{3.28}$$

kde $s(x)$ je čiastočný podiel a $r_1(x)$ je nenulový zvyšok. Ďalej vydelíme polynóm $q(x)$ polynómom $r_1(x)$ a dostaneme

$$q(x) = r_1(x).s_1(x) + r_2(x), \tag{3.29}$$

kde $s_1(x)$ je čiastočný podiel a $r_2(x)$ je nenulový zvyšok. Analogicky dostávame

$$\begin{aligned} r_1(x) &= r_2(x).s_2(x) + r_3(x) \\ r_2(x) &= r_3(x).s_3(x) + r_4(x) \end{aligned}$$

V k-tom kroku dostávame

$$r_{k-2}(x) = r_{k-1}(x).s_{k-1}(x) + r_k(x), \tag{3.30}$$

kde $st\{q(x)\} > st\{r_1(x)\} > st\{r_1(x)\} > \cdots > st\{r_{k-1}(x)\} > st\{r_k(x)\}$. Keďže $st\{q(x)\}$ je nezáporné celé číslo, celý proces po m krokoch skončí. Posledné dve rovnosti budú

$$r_{m-2}(x) = r_{m-1}(x).s_{m-1}(x) + r_m(x) \tag{3.31}$$

$$r_{m-1}(x) \quad = \quad r_m(x).s_m(x) + 0 \tag{3.32}$$

Posledný nenulový zvyšok, t. j. $r_m(x)$, je najväčší spoločný deliteľ polynómov $q(x)$, $p(x)$. Ukážme to!

Zo vzťahu (3.32) vyplýva, že $r_m(x)$ delí $r_{m-1}(x)$. Z tejto skutočnosti a zo vzťahu (3.31) vyplýva, že $r_m(x)$ delí aj $r_{m-2}(x)$ atď. až dospejeme k záveru, že $r_m(x)$ delí $q(x)$ aj $p(x)$. Teraz ešte ukážeme, že $r_m(x)$ je deliteľný každým iným spoločným deliteľom polynómov $q(x)$, $p(x)$. Nech $t(x)$ delí $q(x)$ aj $p(x)$. Podľa (3.28) $r_1(x) = p(x) - q(x).s(x)$, a preto $t(x)$ delí aj $r_1(x)$. Podľa (3.29) $r_2(x) = q(x) - r_1(x).s_1(x)$, a preto $t(x)$ delí aj $r_2(x)$. Takto postupne dokážeme, že $t(x)$ delí $r_m(x)$.

Príklad 3.7. Nájdime najväčšieho spoločného deliteľa polynómov $p(x) = x^9 - 1$ a $q(x) = x^5 - 1$.

Riešenie:
Postupovať budeme podľa Euklidovho algoritmu a postupným delením dostaneme

$$\begin{aligned} x^9 - 1 &= (x^5 - 1)x^4 + (x^4 - 1) \\ (x^5 - 1) &= (x^4 - 1)x + (x - 1) \\ (x^4 - 1) &= (x - 1)(x^3 + x^2 + x + 1) + 0. \end{aligned}$$

Posledný nenulový zvyšok je $r_2(x) = x - 1$, ktorý je normovaným najväčším spoločným deliteľom polynómov $p(x)$ a $q(x)$.

Príklad 3.8. Nájdime najväčšieho spoločného deliteľa polynómov $p(x) = x^4 + 1$ a $q(x) = x^2 - 1$.

Riešenie:
Postupným delením podľa Euklidovho algoritmu dostaneme rovnosti

$$\begin{aligned} x^4 + 1 &= (x^2 - 1)(x^2 + 1) + 2 \\ x^2 - 1 &= 2\Big(\frac{x^2}{2} - \frac{1}{2}\Big) + 0 \end{aligned}$$

Posledný nenulový zvyšok je $r_1(x) = 2$, čiže sme našli najväčšieho nenormovaného spoločného deliteľa daných polynómov. Normovaným najväčším spoločným deliteľom je polynóm 1. Polynómy $p(x)$ a $q(x)$ sú nesúdeliteľné.

Veta 3.15 (Bezoutova rovnosť)**.** *Nech $p(x)$ a $q(x)$ sú nenulové polynómy a nech $r(x)$ je ich najväčší spoločný deliteľ. Potom existujú také polynómy $u(x)$ a $v(x)$, že platí*

$$r(x) = p(x).u(x) + q(x).v(x). \tag{3.33}$$

Dôkaz:
V Euklidovom algoritme (3.32) je najväčší spoločný deliteľ $r(x) = r_m(x)$. Zo vzťahu (3.31) máme

$$r(x) = r_{m-2}(x) - r_{m-1}(x).\underbrace{s_{m-1}(x)}_{-v_1(x)} \tag{3.34}$$

Ak položíme $u_1(x) = 1$ a $v_1(x) = -s_{m-1}(x)$, prepíšeme (3.34) takto

$$r(x) = r_{m-2}(x).u_1(x) + r_{m-1}.v_1(x). \tag{3.35}$$

Zo vzťahu (3.30) pre $k = m-1$ máme $r_{m-1}(x) = r_{m-3}(x) - r_{m-2}(x)s_{m-2}(x)$, z čoho po dosadení za $r_{m-1}(x)$ do (3.35)

$$\begin{aligned} r(x) &= r_{m-2}(x).u_1(x) + \left[r_{m-3}(x) - r_{m-2}(x).s_{m-2}(x)\right].v_1(x) \\ r(x) &= r_{m-3}(x).\underbrace{v_1(x)}_{u_2(x)} + r_{m-2}(x)\underbrace{\left[u_1(x) - s_{m-2}(x).v_1(x)\right]}_{v_2(x)} \\ r(x) &= r_{m-3}(x).u_2(x) + r_{m-2}.v_2(x). \end{aligned}$$

Takto po $(m-1)$ krokoch dostaneme

$$r(x) = p(x).u_{m-1}(x) + q(x).v_{m-1}(x). \tag{3.36}$$

■

Dôkaz predchádzajúcej vety dáva návod, ako k ľubovoľnému polynómu $p(x)$ zostrojiť polynóm $u(x)$ tak, aby súčin polynómov $p(x).u(x)$ po vydelení polynómom $q(x)$ dal zvyšok $r(x)$, ktorý je najväčším spoločným deliteľom polynómov $p(x)$, $q(x)$. Vzťah (3.33) možno totiž prepísať

$$p(x).u(x) = -q(x).v(x) + r(x).$$

Príklad 3.9. Nájdime najväčšieho spoločného deliteľa $r(x)$ pre polynómy $p(x) = x^4 + 2x^3 - x^2 - 4x - 2$ a $q(x) = x^4 + x^3 - x^2 - 2x - 2$ a polynómy $u(x)$ a $v(x)$ tak, aby platila Bezoutova rovnosť.

Riešenie:
Najväčšieho spoločného deliteľa polynómov $p(x)$ a $q(x)$ nájdeme pomocou Euklidovho algoritmu ako posledný nenulový zvyšok v postupnosti rovností

$$x^4 + 2x^3 - x^2 - 4x - 2 \quad = \quad (x^4 + x^3 - x^2 - 2x - 2) \cdot 1 + (x^3 - 2x)$$

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

Najväčší spoločný deliteľ je $r(x) = x^2 - 2$. Polynómy $u(x)$ a $v(x)$ do Bezoutovej rovnosti dostaneme spätným dosadzovaním do rovností získaných Euklidovým algoritmom. Z druhej rovnosti dostaneme vzťah pre $r(x)$:

$$x^2 - 2 = \underbrace{(x^4 + x^3 - x^2 - 2x - 2)}_{q(x)} - (x^3 - 2x)(x+1) \tag{3.37}$$

Z prvej rovnosti vyjadríme

$$x^3 - 2x = \underbrace{(x^4 + 2x^3 - x^2 - 4x - 2)}_{p(x)} - \underbrace{(x^4 + x^3 - x^2 - 2x - 2)}_{q(x)} \cdot 1$$

a dosadíme do vzťahu 3.37. Dostaneme

$$\begin{aligned} x^2 - 2 &= q(x) - (p(x) - q(x)) \cdot (x+1) \\ &= q(x) - p(x) \cdot (x+1) + q(x) \cdot (x+1) \\ &= p(x) \underbrace{(-x-1)}_{u(x)} + q(x) \underbrace{(x+2)}_{v(x)} \end{aligned}$$

Podobne ako na množine celých čísel, aj na množine polynómov môžeme zviesť reláciu kongruencie modulo $q(x)$ nasledujúcim spôsobom:

Definícia 3.10. Polynómy $r(x)$ a $s(x)$ sú **kongruentné** modulo $q(x)$, píšeme $r(x) \equiv s(x) \mod q(x)$, ak polynóm $r(x) - s(x)$ je deliteľný polynómom $q(x)$.

Vieme teda riešiť rovnicu

$$p(x).y(x) \equiv r(x) \mod q(x). \tag{3.38}$$

Ak najväčším spoločným deliteľom polynómov $p(x)$, $q(x)$ je polynóm $r(x) = 1$, rovnica (3.38) má tvar

$$p(x).y(x) \equiv 1 \mod q(x). \tag{3.39}$$

Príklad 3.10. Postup výpočtu najväčšieho spoločného deliteľa $\mathrm{NSD}(a, b)$ celých čísel a, b spolu s výpočtom riešenia rovnice

$$b.y \equiv \mathrm{NSD}(a, b)$$

dáva nasledujúci rozšírený Euklidov algoritmus, ktorý sa dá ľahko upraviť aj pre polynómy. Algoritmus je zapísaný v jazyku C.

```
#include <stdio.h>
#include <string.h>

int main()
{
int a,b,i, nsd,inv;
int r[100],t[100],q[100];

printf("Zadaj a:\n");
scanf("%d", &a);
printf("Zadaj b:\n");
scanf("%d", &b);

for(i=0;i<100;i++) r[i]=0,t[i]=0,q[i]=0;

i=0; r[0]=a, r[1]=b, t[0]=0, t[1]=1;

while (r[i+1]!=0)
{q[i+1]=r[i]/r[i+1];
 r[i+2]=r[i]%r[i+1];
 t[i+2]=(t[i]-q[i+1]*t[i+1])%a;
 if(t[i+2]<0)t[i+2]=t[i+2]+a;
 i++;}

 nsd=r[i], inv=t[i];

printf("nsd(%d,%d) = %d\n", a, b, nsd);
printf("(%d)^-1 mod %d = %d\n", b, a, inv);

return 0;
}
```

3.6 Racionálna funkcia a jej rozklad na elementárne zlomky*

V matematickej analýze sa pri integrovaní reálnych racionálnych funkcií používa rozklad racionálnej funkcie na elementárne zlomky. V tejto kapitole vo veľmi zjednodušenej forme uvedieme základné pojmy a tvrdenia súvisiace s týmto postupom, ako aj samotný postup.

Definícia 3.11. Nech $p(x)$, $q(x)$ sú dva polynómy. Funkciu

$$f(x) = \frac{p(x)}{q(x)} \tag{3.40}$$

definovanú pre každé x, pre ktoré je $q(x) \neq 0$, nazveme **racionálnou funkciou**. Nech $\mathrm{st}\{p(x)\} = m$, $\mathrm{st}\{q(x)\} = n$. Ak $m < n$, hovoríme, že (3.40) je **rýdzo racionálna funkcia**.

***Poznámka* 3.10.** *Každá racionálna funkcia* (3.40) *sa dá vyjadriť ako súčet*

$$f(x) = r(x) + \frac{z(x)}{q(x)}, \tag{3.41}$$

kde $\frac{z(x)}{q(x)}$ *je rýdzo racionálna funkcia,* $r(x)$ *je polynóm – podiel a* $z(x)$ *zvyšok pri delení polynómu* $p(x)$ *polynómom* $q(x)$.

Príklad 3.11. Racionálnu funkciu $f(x) = \dfrac{2x^4 - 5x^2 + x - 1}{x + 2}$ vyjadrime ako súčet polynómu a rýdzo racionálnej funkcie.
Riešenie:
Výraz v menovateli racionálnej funkcie je lineárny polynóm. Na získanie podielu využijeme Hornerovu schému:

	2	0	-5	1	-1
-2		-4	8	-6	10
	2	-4	3	-5	9

Z Hornerovej schémy vidíme, že podiel $r(x) = 2x^3 - 4x^2 + 3x - 5$ a zvyšok $z(x) = 9$. Konečný tvar funkcie $f(x)$ v zmysle vzťahu (3.41) je

$$f(x) = 2x^3 - 4x^2 + 3x - 5 + \frac{9}{x + 2}.$$

A teraz prejdeme k definícii elementárnych zlomkov a zároveň uvedieme tvrdenia "legalizujúce" postup používaný pri rozklade.

Definícia 3.12. Funkcie tvaru

$$\frac{A}{(x-a)^k} \qquad \text{alebo} \qquad \frac{Mx+N}{(x^2+bx+c)^k}, \tag{3.42}$$

kde $A,\ M,\ N,\ a,\ b,\ c$ sú reálne čísla, k prirodzené číslo a (x^2+bx+c) nemá reálne korene, (t. j. $(b^2-4ac)<0$), nazývame **elementárnymi zlomkami**.

Veta 3.16. *Nech* $\frac{p(x)}{t(x)s(x)}$ *je rýdzo racionálna funkcia, pričom* $NSD(t(x),s(x)) = 1$. *Potom existujú jednoznačne určené rýdzo racionálne funkcie* $\frac{z_1}{t(x)}$, $\frac{z_2}{s(x)}$ *také, že*

$$\frac{p(x)}{t(x)s(x)} = \frac{z_1(x)}{t(x)} + \frac{z_2(x)}{s(x)}. \tag{3.43}$$

Dôkaz:
Najskôr ukážeme, že existujú také rýdzo racionálne funkcie, ktoré dajú rozklad uvedený vo vzťahu 3.43. Podľa predpokladu sú polynómy $t(x)$ a $s(x)$ nesúdeliteľné, teda ich najväčší normovaný spoločný deliteľ je 1. Potom ale na základe vety 3.15 pre vhodne zvolené polynómy $u(x)$ a $v(x)$ platí

$$t(x)\cdot u(x) + s(x)\cdot v(x) = 1 \tag{3.44}$$

Ak využijeme vzťah 3.44, dostávame

$$\frac{p(x)}{t(x)s(x)} = \frac{p(x)(t(x)u(x)+s(x)v(x))}{t(x)s(x)} = \\ = \frac{p(x)u(x)}{s(x)} + \frac{p(x)v(x)}{t(x)} = r_1(x) + \frac{z_1(x)}{s(x)} + r_2(x) + \frac{z_2(x)}{t(x)},$$

kde $r_i(x)$, $z_i(x)$ pre $i=1,2$ sú určené jednoznačne.
Ak odstránime zlomok vynásobením oboch strán súčinom polynómov $s(x)\cdot t(x)$, dostaneme

$$p(x) = (r_1(x)+r_2(x))t(x)s(x) + \underbrace{z_1(x)t(x)+z_2(x)s(x)}_{1}$$

Zistíme stupne polynómov na oboch stranách rovnosti a vidíme, že

$$st\{p(x)\} = st\{\big(r_1(x) + r_2(x)\big)t(x)s(x)\} \ .$$

Porovnaním stupňov na oboch stranách dostávame, že $r_1(x) + r_2(x) = 0$.
Ešte treba ukázať jednoznačnosť rozkladu. Nech okrem rozkladu daného vzťahom 3.43 existuje aj rozklad

$$\frac{p(x)}{t(x)s(x)} = \frac{\overline{z}_1(x)}{t(x)} + \frac{\overline{z}_2(x)}{s(x)} \ .$$

Potom

$$\frac{z_1(x) - \overline{z}_1(x)}{t(x)} = \frac{\overline{z}_2(x) - z_2(x)}{s(x)}$$

a $(z_1(x) - \overline{z}_2(x))s(x) = (\overline{z}_2(x) - z_2(x))t(x)$. Keďže podľa predpokladu vety $NSD(s(x), t(x)) = 1$, tak $s(x) \mid (\overline{z}_2(x) - z_2(x))$, čo ale znamená, že $\overline{z}_2(x) - z_2(x) = 0$, pretože $st\{\overline{z}_2(x) - z_2(x)\} < st\{s(x)\}$. A odtiaľ vyplýva, že $\overline{z}_2(x) = z_2(x)$. Obdobnou úvahou dokážeme, že $z_1(x) = \overline{z}_1(x)$. ■

Pre naše potreby budeme predpokladať, že polynómy $s(x)$, $t(x)$ v menovateli rýdzo racionálnej funkcie $\dfrac{p(x)}{t(x)s(x)}$ vo vzťahu 3.43 sú ireducibilné nad poľom reálnych čísel.

Bez dôkazu uvedieme nasledujúce dve tvrdenia, ktoré priamo dávajú návod na rozklad rýdzo racionálnej funkcie na elementárne zlomky.

Veta 3.17. *Nech funkcia* $f(x) = \dfrac{p(x)}{q(x)}$ *je rýdzo racionálna. Nech* c *je* k*-násobným koreňom polynómu* $q(x)$*. Potom existuje také číslo* A *a taký polynóm* $p_1(x)$ *stupňa nižšieho než stupeň polynómu* $(x-c)^{k-1}.q_1(x)$*, že platí*

$$\frac{p(x)}{q(x)} = \frac{A}{(x-c)^k} + \frac{p_1(x)}{(x-c)^{k-1}.q_1(x)} \ .$$

Veta 3.18. *Nech* $f(x) = \dfrac{p(x)}{q(x)}$ *je rýdzo racionálna funkcia. Nech koeficienty polynómu* $q(x)$ *sú reálne čísla. Nech komplexné číslo* $\alpha + i\beta$*,* $(\alpha \in \mathbb{R},\ \beta \in \mathbb{R},\ \beta \neq 0)$ *je* k*-násobným koreňom polynómu* $q(x)$*. Označme* $a = -2\alpha$*,* $b = \alpha^2 + \beta^2$*. Potom existujú čísla* M*,* N *a taký polynóm* $p_1(x)$ *stupňa nižšieho než stupeň polynómu* $(x^2 + ax + b)^{k-1}.q_1(x)$*, že platí*

$$\frac{p(x)}{q(x)} = \frac{Mx + N}{(x^2 + ax + b)^k} + \frac{p_1(x)}{(x^2 + ax + b)^{k-1}.q_1(x)} \ . \tag{3.45}$$

Nech $q(x) = (x-c)^k.q_1(x)$. Postupnou aplikáciou vety 3.17 dostaneme:

$$\begin{aligned}
\frac{p(x)}{q(x)} &= \frac{A_k}{(x-c)^k} + \frac{p_1(x)}{(x-c)^{k-1}.q_1(x)} = \\
&= \frac{A_k}{(x-c)^k} + \frac{A_{k-1}}{(x-c)^{k-1}} + \frac{p_2(x)}{(x-c)^{k-2}.q_1(x)} = \dots \\
\dots &= \frac{A_k}{(x-c)^k} + \frac{A_{k-1}}{(x-c)^{k-1}} + \dots + \frac{A_1}{(x-c)^1} + \frac{p_k(x)}{(x-c)^{k-k}.q_1(x)} = \\
&= \frac{A_k}{(x-c)^k} + \frac{A_{k-1}}{(x-c)^{k-1}} + \dots + \frac{A_1}{(x-c)^1} + \frac{p_k(x)}{q_1(x)} \,. \qquad (3.46)
\end{aligned}$$

Uvedením (3.46) na spoločného menovateľa, ktorým je $q(x) = (x-c)^k.q_1(x)$ dostaneme vyjadrenie čitateľa zlomku $f(x) = \dfrac{p(x)}{q(x)}$ pomocou čísel $A_1, A_2, \dots, A_k$. Porovnaním koeficientov pri rovnakých mocninách oboch vyjadrení dostaneme sústavu lineárnych rovníc pre $A_1, A_2, \dots, A_k$.

Analogicky, ak $q(x) = (x^2+ax+b)^k.q_1(x)$, tak postupnou aplikáciou vety 3.18 dostaneme:

$$\begin{aligned}
\frac{p(x)}{q(x)} &= \frac{M_kx+N_k}{(x^2+ax+b)^k} + \frac{p_1(x)}{(x^2+ax+b)^{k-1}.q_1(x)} = \\
&= \frac{M_kx+N_k}{(x^2+ax+b)^k} + \frac{M_{k-1}x+N_{k-1}}{(x^2+ax+b)^{k-1}} + \frac{p_2(x)}{(x^2+ax+b)^{k-2}.q_1(x)} = \dots = \\
&= \frac{M_kx+N_k}{(x^2+ax+b)^k} + \frac{M_{k-1}x+N_{k-1}}{(x^2+ax+b)^{k-1}} + \dots \\
&\quad \dots + \frac{M_1x+N_1}{(x^2+ax+b)^1} + \frac{p_k(x)}{(x^2+ax+b)^{k-k}.q_1(x)} = \\
&= \frac{M_kx+N_k}{(x^2+ax+b)^k} + \frac{M_{k-1}x+N_{k-1}}{(x^2+ax+b)^{k-1}} + \dots + \frac{M_1x+N_1}{(x^2+ax+b)^1} + \frac{p_k(x)}{q_1(x)} \,.
\end{aligned}$$

Uvedením posledného výrazu na spoločného menovateľa, ktorým je

$$q(x) = (x^2+ax+b)^k.q_1(x),$$

dostaneme vyjadrenie čitateľa zlomku $f(x) = \dfrac{p(x)}{q(x)}$ pomocou čísel $M_1, N_1, M_2, N_2 \dots, M_k, N_k$. Porovnaním koeficientov pri rovnakých mocninách oboch vyjadrení dostaneme sústavu lineárnych rovníc pre $M_1, N_1, M_2, N_2 \dots, M_k, N_k$.

***Poznámka* 3.11.** *Poznamenávame, že výrazy* $\frac{p_k(x)}{q_1(x)}$ *v predchádzajúcich riadkoch sú rýdzo racionálne funkcie, na ktoré opäť aplikujeme tvrdenia viet 3.17, resp. 3.18.*

Príklad 3.12. Nájdime rozklad funkcie $f(x) = \dfrac{x^2 - x + 1}{x^3 + 2x^2 + 2x + 1}$ na elementárne zlomky nad poľom reálnych čísel.
Riešenie:
Funkcia $f(x)$ je rýdzo racionálna, stupeň polynómu v čitateli je dva, stupeň polynómu v menovateli je tri. Polynóm $q(x) = x^3 + 2x^2 + 2x + 1$ má jeden koreň -1. Pomocou Hornerovej schémy vydelíme $q(x)$ lineárnym polynómom $(x+1)$:

	1	2	2	1
-1		-1	-1	-1
	1	1	1	0

Z Hornerovej schémy vyplýva, že $q(x) = (x+1)(x^2+x+1)$. Polynóm x^2+x+1 má len komplexné korene, čiže $q(x)$ je rozložený na súčin ireducibilných polynómov nad poľom reálnych čísel. Rozklad racionálnej funkcie $f(x)$ na elementárne zlomky potom vyzerá takto:

$$\begin{aligned} f(x) = \frac{x^2 - x + 1}{x^3 + 2x^2 + 2x + 1} &= \frac{A}{x+1} + \frac{Bx + C}{x^2 + x + 1} \\ &= \frac{A(x^2 + x + 1) + (Bx + C)(x + 1)}{(x + 1)(x^2 + x + 1)} \\ &= \frac{x^2(A + B) + x(A + B + C) + A + C}{(x + 1)(x^2 + x + 1)} \end{aligned}$$

Porovnaním koeficientov pri rovnakých mocninách premennej x polynómov v čitateli racionálnych funkcií dostaneme systém lineárnych rovníc:

$$\begin{aligned} A + B &= 1 \\ A + B + C &= -1 \\ A + C &= 1 \end{aligned}$$

Vyriešením sústavy dostaneme $A = 3$, $B = -2$, $C = -2$. Konečný tvar funkcie $f(x)$ rozloženej na elementárne zlomky je $f(x) = \dfrac{3}{x+1} - \dfrac{2x+2}{x^2+x+1}$.

3.7 Konečné polia

Pre človeka zvyknutého narábať s reálnymi a komplexnými číslami pripadajú nekonečné polia reálnych, resp. komplexných čísel najprirodzenejšie. V kapitole 2 v časti 2.3 (str. 29) sme videli, že existujú aj konečné polia typu $\mathbb{Z}_p$. Na prvý pohľad pôsobia takéto konečné polia len ako prakticky nepoužiteľná matematická hračka, avšak dnes je opak pravdou. Moderná teória kódovania či kryptografia sa bez konečných polí nezaobídu. Aplikácie môže čitateľ nájsť napríklad v [1], [2] a iných.

V tejto časti zhrnieme základné definície a vety (bez dôkazov) o konečných poliach v najmenšom možnom rozsahu nutnom pre porozumenie ich aplikácií. Podrobnú teóriu konečných polí nájde čitateľ v [5], [3], [4].

V časti 2.3 na str. 29 bol definovaný pojem množiny zvyškových tried modulo p, ktorá je označovaná symbolom $\mathbb{Z}_p$. Na $\mathbb{Z}_p$ bola zavedená aditívna operácia $\oplus$ a multiplikatívna operácia $\otimes$ predpismi:

$$r \oplus s = r + s \mod p \tag{3.47}$$

$$r \otimes s = r.s \mod p \tag{3.48}$$

Ukázali sme, že $\mathbb{Z}_p$ je pole práve vtedy, keď p je prvočíslo (pozri vetu 2.13 na str. 31).

V literatúre sa pre okruh zvyškových tried modulo p používa tiež termín **faktorový okruh modulo** p.

Definícia 3.13. Nech $\mathcal{P} = (P, +, .)$ je pole, $q(x)$ polynóm stupňa $n \geq 0$ nad poľom $\mathcal{P}$. Definujme **okruh polynómov modulo** $q(x)$ $\mathcal{P}/q(x)$ s operáciami $\boxplus$, $\boxtimes$ takto:

- Prvkami okruhu $\mathcal{P}/q(x)$ sú všetky polynómy $q(z)$ nad poľom $\mathcal{P}$ stupňa nanajvýš $n - 1$.
- Pre $a(z),\ b(z) \in \mathcal{P}/q(x)$ definujeme

  $$a(z) \boxplus b(z) = a(z) + b(z), \tag{3.49}$$

  t. j. ako obvyklý súčet polynómov.
- Pre $a(z),\ b(z) \in \mathcal{P}/q(x)$ definujeme

  $$a(z) \boxtimes b(z) = a(z).b(z) \mod q(z), \tag{3.50}$$

  t. j. ako zvyšok po delení polynómu $a(z).b(z)$ polynómom $q(z)$.

Ako sme už spomenuli $\mathbb{Z}_p$ je pole práve vtedy, keď p je prvočíslo. Analógiou tohoto tvrdenia je nasledujúca veta, ktorú uvádzame bez dôkazu.

Veta 3.19. *Pre každý ireducibilný polynóm $q(x)$ nad poľom $\mathcal{P}$ je okruh polynómov $\mathcal{P}/q(x)$ poľom.*

Definícia 3.14. Pole (komutatívne teleso) $\mathbb{Z}_p/q(x)$, kde p je prvočíslo a $q(x)$ ireducibilný polynóm stupňa n nad poľom $\mathbb{Z}_p$, sa nazýva **Galoisovo pole** (alebo Galoisovo teleso) a označuje sa $GF(p^n)$.

Ireducibilné polynómy nad $\mathbb{Z}_p$, kde p je prvočíslo, majú podstatný význam pre teóriu i praktické využitie konečných polí. Zistiť či polynóm $q(x)$ nad poľom $\mathbb{Z}_p$ je ireducibilný je podobná úloha ako úloha zistiť či dané číslo m je prvočíslo. Jednou z metód, ako vyriešiť otázku prvočíselnosti čísla m, je zistiť či sa dá napísať ako súčin dvoch prirodzených čísel väčších než 1, čomu sa tiež hovorí **faktorizovať** číslo m. Najjednoduchšou (ale nie najefektívnejšou) metódou je postupne vydeliť číslo m všetkými prirodzenými číslami $k = 2, 3, \ldots, [\sqrt{m}]$ (kde $[\sqrt{m}]$ znamená najväčšie prirodzené číslo menšie alebo rovnajúce sa $\sqrt{m}$). Ak pre niektoré k je delenie bez zvyšku, m nie je prvočíslo, inak m je prvočíslo.

Podobne zisťujeme ireducibilitu polynómu $a(x)$ stupňa m nad konečným poľom $\mathbb{Z}_p$. Stačí ho vydeliť postupne všetkými polynómami nenulového stupňa menšieho než $\left[\frac{m+1}{2}\right]$ (hranatá zátvorka tu znamená celú časť hodnoty výrazu v nej).

Príklad 3.13. Všetky ireducibilné polynómy stupňa 2 nad $\mathbb{Z}_3$ sú $x^2 + x + 2$, $x^2 + 2x + 2$, všetky ireducibilné polynómy tretieho stupňa sú $x^3 + 2x + 1$, $x^3 + x^2 + 2x + 1$, $x^3 + 2x^2 + 1$, $x^3 + 2x^2 + x + 1$.

Ďalšie ireducibilné polynómy nad $\mathbb{Z}_p$ pre $p = 2, 3, \ldots, 7$ a mnoho ďalších informácií o špeciálnych polynómoch možno nájsť na internetovej adrese [15].

Príklad 3.14. Pre informatiku sú mimoriadne dôležité Galoisove polia nad poľom $\mathbb{Z}_2$, pre ktorých konštrukciu sú potrebné ireducibilné polynómy nad $\mathbb{Z}_2$.

Nad poľom $\mathbb{Z}_2$ existuje jediný ireducibilný polynóm druhého stupňa a to $x^2 + x + 1$. Ďalšie ireducibilné polynómy nad $\mathbb{Z}_2$ možno nájsť v tabuľke 3.1 .

Počet ireducibilných polynómov stupňa n nad poľom $\mathbb{Z}_2$ pre $n = 2, 2, ..., 15$ je v nasledujúcej tabuľke:

2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	6	9	18	30	56	99	186	335	630	1161	2182

n	všetky ireducibilné polynómy stupňa n
2	x^2+x+1
3	x^3+x+1 x^3+x^2+1
4	x^4+x+1 x^4+x^3+1 $x^4+x^3+x^2+x+1$
5	x^5+x^2+1 x^5+x^3+1 $x^5+x^3+x^2+x+1$ $x^5+x^4+x^3+x^2+1$ $x^5+x^4+x^2+x+1$ $x^5+x^4+x^3+x+1$
6	x^6+x+1 x^6+x^5+1 x^6+x^3+1 $x^6+x^4+x^2+x+1$ $x^6+x^5+x^4+x^2+1$ $x^6+x^4+x^3+x+1$ $x^6+x^5+x^3+x^2+1$ $x^6+x^5+x^2+x+1$ $x^6+x^5+x^4+x+1$

Tabuľka 3.1: Tabuľka ireducibilných polynómov nad $\mathbb{Z}_2$.

Ukazuje sa, že jediné konečné polia sú len Galoisove polia typu $GF(p^n)$, kde p je prvočíslo a n prirodzené číslo $n > 0$ (pre $n = 1$ je $GF(p^1)$ rovné okruhu $\mathbb{Z}_p$ zvyškových tried modulo p), ako ukazuje nasledujúca veta, ktorú taktiež uvádzame bez dôkazu.

Veta 3.20. *Každé konečné pole je izomorfné s niektorým Galoisovým poľom. Dve konečné polia s rovnakým počtom prvkom sú izomorfné.*

Počet prvkov konečného poľa musí teda byť prvočíslo, alebo mocnina prvočísla. Existujú konečné polia, ktoré majú 2, 3, $4 = 2^2$, 5, 7, $8 = 2^3$, $9 = 3^2$, 11, 13, $16 = 2^4$, 17, 19, 23, $27 = 3^3, \ldots$ prvkov, neexistuje žiadne konečné pole, ktoré by malo 6, 10, 12, 14, ... prvkov.

Exponenciálna Reprezentácia	Polynomiálna Reprezentácia	Binárna Reprezentácia	Hexadecimálna Reprezentácia
0	0	0000	"0"
α^0	1	0001	"1"
α^1	x	0010	"2"
α^2	x^2	0100	"4"
α^3	x^3	1000	"8"
α^4	$x+1$	0011	"3"
α^5	x^2+x	0110	"6"
α^6	x^3+x^2	1100	"C"
α^7	x^3+x+1	1011	"B"
α^8	x^2+1	0101	"9"
α^9	x^3+x	1010	"A"
α^{10}	x^2+x+1	0111	"7"
α^{11}	x^3+x^2+x	1110	"E"
α^{12}	x^3+x^2+x+1	1111	"F"
α^{13}	x^3+x^2+1	1101	"D"
α^{14}	x^3+1	1010	"9"
$\alpha^{15}=\alpha^0=1$			

Tabuľka 3.2: Tabuľka prvkov poľa $GF(2^4)$ v rôznych reprezentáciách

Príklad 3.15. Galoisovo pole $GF(2^4)$.
Podľa definície 3.14 ide o pole $\mathbb{Z}_2/q(x)$, kde na mieste $q(x)$ použijeme ireducibilný polynóm

$$q(x) = x^4 + x + 1. \tag{3.51}$$

Ide teda o pole, ktorého prvkami sú všetky polynómy nad poľom $\mathbb{Z}_2$ nanajvýš tretieho stupňa (t. j. s koeficientmi 0 alebo 1), s operáciou sčítania polynómov 3.49 a s operáciou násobenia definovanou vzťahom 3.50.

Nenulové prvky $GF(2^4)$ je vhodné interpretovať v tzv. **exponenciálnej reprezentácii** ako mocniny niektorého polynómu $\alpha(x)$. Vezmime $\alpha(x) = x$. Potom $\alpha^0 = 1$, $\alpha^2 = x^2$, $\alpha^3 = x^3$. Polynomickú reprezentáciu prvku α^4 určíme ako zvyšok po delení $(x^4) : (x^4 + x + 1)$, čo je $-(x + 1)$. Pretože pracujeme s polynómami nad $\mathbb{Z}_2$, posledný výraz sa rovná polynómu $x+1$, a teda $\alpha^4 = x+1$. Polynóm prislúchajúci k α^5 získame ako zvyšok po delení $(x^5) : (x^4 + x + 1)$,

alebo ako súčin $\alpha\alpha^4 = x(x+1) = x^2 + x$. Takto vyplníme celú tabuľku. Platí: $\alpha^{15} = 1$, pretože $\alpha^{15} = \alpha\alpha^{14}$ = zvyšok po delení $(x^4 + x) : (x^4 + x + 1)$, čo je 1.

Binárnu reprezentáciu prvku poľa – polynómu – tvorí postupnosť jeho koeficientov. Keďže koeficienty sú prvkami poľa $\mathbb{Z}_2$, sú všetky polynómy nanajvýš tretieho stupňa nad $\mathbb{Z}_2$ reprezentovateľné ako bity štvorbitového slova. Hexadecimálna reprezentácia je obvyklá reprezentácia štvormiestnych čísel v dvojkovej sústave symbolmi "0"–"9", "A – "F".

Pravidlo sčítania prvkov z $GF(2^4)$ je jednoduché – príslušné štvorbitové slová binárnej reprezentácie sčítame ako prvky $\mathbb{Z}_2$ po bitoch. Vo väčšine programovacích jazykoch existuje na to binárna operácia XOR po bitoch.

Pre násobenie je veľmi vhodná exponenciálna reprezentácia podľa nasledujúceho príkladu

$$\text{"A"}.\text{"B"} = \alpha^9.\alpha^7 = \alpha^{(9+7)} = \alpha^{16} = \alpha^{15}\alpha^1 = 1.\alpha = \text{"2"}.$$

Samozrejme môžeme použiť aj polynomickú reprezentáciu a súčin dvoch prvkov – polynómov $p(x)$ a $s(x)$ počítať podľa definície ako zvyšok po delení polynómu $p(x).s(x)$ polynómom $q(x) = x^4 + x + 1$.

Výpočet inverzného prvku je použitím exponenciálnej reprezentácie jednoduchý. Použijeme vzťah

$$\alpha^i.\alpha^{15-i} = \alpha^{15} = 1 \qquad \text{pre } i = 1, 2, \ldots, 14, \tag{3.52}$$

z ktorého vyplýva, že inverzný prvok k prvku α^i je prvok α^{15-i}.

***Poznámka* 3.12.** *Vo všeobecnosti nie každý polynóm $\alpha(x)$ má tú vlastnosť, že postupnosť $\alpha(x), \alpha^2(x), \alpha^3(x), \ldots$ obsahuje všetky nenulové prvky príslušného konečného poľa. Ak by sme vzali polynóm $\beta(x) = x^2 + x$ (vlastne $\beta(x) = \alpha^5(x)$), potom postupnosť $\beta(x),\ \beta^2(x),\ \beta^3(x),\ \ldots$ je cyklická postupnosť*

$$\beta(x) = x^2 + x,\ \beta^2(x) = x^2 + x + 1,\ \beta^3(x) = 1,\ \beta^4(x) = \beta(x) = x^2 + x,\ \ldots$$

Definícia 3.15. Ak každý prvok poľa $\mathcal{P}$ možno napísať ako mocninu α^i prvku α, hovoríme, že α je **primitívny prvok poľa** $\mathcal{P}$.

Existenciu primitívneho prvku v konečnom telese zaručuje nasledujúca veta.

Veta 3.21. *Každé Galoisovo pole má primitívny prvok.*

Ak by sa ukázalo, že $\alpha(x) = x$ nie je primitívny prvok reprezentovaného poľa, treba pre exponenciálnu notáciu zvoliť za polynóm α iný polynóm.

Pre veľké hodnoty mocniny 2^n je výpočet inverzného polynómu pomocou jeho exponenciálneho tvaru nepraktický (pozri nasledujúcu poznámku), preto využijeme poznatky vety o Bezoutovej rovnosti 3.15 na str. 56, ktorej dôkaz dáva postup ako riešiť rovnicu pre známe polynómy $p(x)$, $q(x)$

$$p(x).y(x) \equiv r(x) \mod q(x).$$

pre ľubovoľné dané polynómy $p(x)$, $q(x)$, ktorých najväčší spoločný deliteľ je polynóm $r(x)$. Ak najväčším spoločným deliteľom polynómov $p(x)$, $q(x)$ je polynóm $r(x) = 1$, je posledná rovnica tvaru

$$p(x).y(x) \equiv 1 \mod q(x). \tag{3.53}$$

Ak teda polynóm $p(x)$ je prvkom okruhu Galoisovho poľa $\mathbb{Z}_2/q(x)$, kde $q(x)$ je ireducibilný polynóm (v našom konkrétnom prípade $q(x) = x^4 + x + 1$), potom stupeň polynómu $p(x)$ je menší než stupeň ireverzibilného polynómu $q(x)$ a najväčší spoločný deliteľ $p(x)$ a $q(x)$ je polynóm $r(x) = 1$. V tomto prípade riešenie $y(x)$ rovnice (3.53) je inverzným prvkom k prvku $p(x)$ v Galoisovom poli $\mathbb{Z}_2/q(x)$. Galoisove polia patria k základným matematickým aparátom pre kryptografiu a teóriu kódovania. Tu vidíme veľký praktický význam vety 3.15 o Bezoutovej rovnosti.

***Poznámka* 3.13.** *Exponenciálna reprezentácia prvkov Galoisovho poľa (a jej použitie na výpočet inverzných prvkov, resp. súčinu prvkov) je praktická len pre menšie Galoisove polia. Pre $GF(2^{64})$ by už takáto tabuľka musela obsahovať obrovské množstvo riadkov a bola by aj z časového hľadiska prakticky nevypočítateľná. Preto sa pre výpočet inverzného prvku v takýchto poliach používa postup z dôkazu vety 3.15 ilustrovaný v príklade 3.9 na str. 57, resp rozšírený Euklidov algoritmus.*

Rovnica $a^x = b$ má v obore reálnych čísel riešenie $x = \log_a(b)$. V konečnom poli je však hľadanie riešenia tej istej rovnice $\alpha^x = \beta$ veľmi ťažké – je porovnateľné s vyskúšaním všetkých prvkov konečného poľa či danej rovnici vyhovujú. Pri poliach s 2^{64} a viac prvkami je to súčasnou výpočtovou technikou pravdepodobne neriešiteľná úloha.

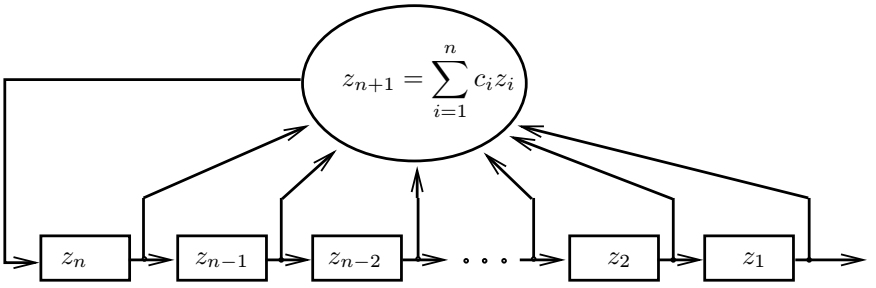
Problém nájsť taký prvok x konečného poľa $\mathcal{P}$, ktorý vyhovuje rovnici $\alpha^x = \beta$, sa nazýva **problém diskrétneho logaritmu**. *Na výpočtovej zložitosti problému diskrétneho logaritmu sú založené viaceré metódy súčasnej kryptografie.*

3.8 Aplikácie

Lineárny posuvný register

Lineárny posuvný register sa skladá z n buniek, každá z nich môže obsahovať hodnotu 0 alebo 1 – pozri obr. 3.1. Prepokladajme, že bunky sú očíslované číslami od 1 do n sprava doľava. Keď posuvný register dostane hodinový impulz, hodnota z prvej bunky sprava vystúpi z registra, do bunky i sa presunie obsah bunky $i+1$ postupne pre $i = 1, 2, \ldots, n-1$ a n-tá bunka sa naplní hodnotou $z_{n+1} = \sum_{i=1}^{n} c_i z_i$ počítanou podľa pravidiel poľa $\mathbb{Z}_2$.

Posuvné registre majú veľa výhod. Sú vhodné pre hardvérovú implementáciu, môžu produkovať postupnosti bitov s veľkou periódou, výstupná postupnosť bitov má veľmi dobré štatistické vlastnosti a štruktúru posuvných registrov možno dobre študovať pomocou algebraických techník. Výstup sa môže použiť ako pseudonáhodná postupnosť. Pretože hardvérová realizácia posuvného registra je jednoduchá, jeho činnosť veľmi rýchla, nachádzajú posuvné registre široké uplatnenie v kryptografii v tzv. prúdových šifrách, slúžiacich na šifrovanie napr. hlasu v telefónoch GSM, prevádzky WiFi zariadení atď.



Obr. 3.1: Lineárny posuvný register

Vlastnosti posuvného registra závisia od vlastností tzv. **väzbového polynómu**, ktorý má tvar:

$$c_1 x^n + c_2 x^{n-1} + \cdots + c_i x^{n+1-i} + \cdots + c_n x^1 + 1. \tag{3.54}$$

Primitívny polynóm stupňa n, je taký polynóm, ktorý je je ireducibilný, delí polynóm $x^{2^{n-1}} + 1$, ale nedelí žiaden polynóm $x^d + 1$ taký, že d delí $2^n - 1$.

Platí nasledujúce tvrdenie: Ak je väzbový polynóm primitívnym polynómom stupňa n, potom príslušný posuvný register má periódu $2^n - 1$.

Dôkaz posledného tvrdenia nie je triviálny a ani hľadanie hľadanie primitívnych polynómov nie je jednoduché. V kryptografickej literatúre možno nájsť obsiahle zoznamy vhodných primitívnych polynómov rôznych stupňov pre všetky možné aplikácie.

Pre nás je však najzaujímavejšia prekvapujúca skutočnosť, ako môžu súvisieť na prvý pohľad také vzdialené pojmy ako lineárne posuvné registre a teória polynómov nad poľom $\mathbb{Z}_2$.

CRC – Cyklický redundantný kód

CRC je skratka anglického termínu Cyclic Redundancy Check alebo Cyclic Redundancy Code. Používa sa na zabezpečenie správ (alebo ich častí) pridaním dodatočného a z hľadiska teórie informácie nadbytočného – redundantného údaja, ktorý však umožňuje s nezanedbateľnou pravdepodobnosťou určiť či prijatá správa bola alebo nebola počas prenosu zmenená.

Správa $\mathcal{M}$ dĺžky N bitov sa berie ako polynóm $P(x)$ nad $\mathbb{Z}_2$, ktorého koeficienty sú práve bity tejto správy – prvý prijatý bit je koeficient pri najvyššej mocnine premennej x. Polynóm $P(x)$ sa vydelí tzv. generujúcim polynómom $G(x)$. **Generujúci polynóm** je vopred dohodnutý polynóm známy vysielajúcej i prijímajúcej strane. Zvyšok po delení je polynóm $R(x)$. Koeficienty polynómu $R(x)$ sú výsledným CRC-kódom, ktorý sa pripojí za správou a takto rozšírená správa sa vyšle.

Prijímajúca strana prijme správu $\mathcal{M}$ rozšírenú o CRC-kód. K správe $\mathcal{M}$ zostrojí príslušný polynóm, ktorý vydelí generujúcim polynómom $G(x)$ a porovná zvyšok po delení $R(x)$ s prijatým CRC-kódom. Ak oba sú oba totožné, s veľkou pravdepodobnosťou nenastala pri prenose chyba.

Navrhnúť nový generujúci polynóm nie je triviálna úloha, všeobecne sa odporúča použiť ireducibilný polynóm. Najčastejšie používané polynómy sú 9-, 17-, 33- a 65-bitové, čo zodpovedá po rade označeniu CRC-8, CRC-16, CRC-32 a CRC-64. V literatúre i na internete možno nájsť dostatok preverených a odporúčaných generujúcich polynómov pre väčšinu bežných aplikácií.

Príklad generujúceho polynómu CRC-32-IEEE 802.3:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Upozornenie. CRC-kód zabezpečí správu proti náhodnej zmene pri prenose či ukladaní – t. j. proti prírode. Nezabezpečí ju však proti úmyselnej zlomyseľnej zmene, pretože falšovateľ spolu so správou môže zmeniť aj jej CRC, prípadne dokáže zmeniť správu tak, že sa jej CRC nezmení. Na ochranu proti zlomyseľnému útoku slúžia tzv. hashovacie funkcie a digitálny podpis.

Použitie Galoisových polí $GF(2^n)$ v kryptografii a teórii kódovania

Konečné algebraické štruktúry (konečné grupy, konečné okruhy, konečné polia, polynómy nad konečnými poľami) majú široké použitie v informatike pri navrhovaní kódov objavujúcich, či dokonca opravujúcich niekoľko chýb a tiež v kryptografii pri konštrukcii šifrovacích algoritmov. Princípom použitia týchto štruktúr je stotožnenie znakov používanej abecedy s prvkami použitej konečnej štruktúry, čím definujeme na danej abecede aditívnu a niekedy aj multiplikatívnu operáciu. Aby vzájomne jednoznačné priradenie znakov abecedy prvkom príslušnej konečnej štruktúry bolo možné, je nevyhnutné, aby sa počet prvkov tejto štruktúry rovnal počtu znakov používanej abecedy.

Najčastejšie sa na spomínané účely používajú okruhy zvyškových tried $\mathbb{Z}_q$. Taký okruh existuje pre ľubovoľné prirodzené číslo $q \geq 2$. Ak však chceme využívať aj multiplikatívnu operáciu okruhu $\mathbb{Z}_q$, môžu nastať problémy s tým, že nie ku každému $k \in \mathbb{Z}_q$ existuje inverzný prvok k^{-1}. Tento problém odpadá, ak je $\mathbb{Z}_q$ poľom, čo nastáva práve vtedy, keď číslo q je prvočíslom.

V informatike však veľmi často pracujeme s abecedou, ktorú tvoria všetky 8-bitové byty (a veľmi často aj 16- až 128-bitové a dokonca aj dlhšie údajové jednotky). V tomto prípade $\mathbb{Z}_{256}$ nie je poľom, žiadne párne číslo nemá v $\mathbb{Z}_{256}$ inverzný prvok. Situáciu v tomto prípade zachránime Galoisovým poľom $GF(2^8) = \mathbb{Z}_2/q(x)$, kde $q(x)$ je ireducibilný polynóm nad poľom $\mathbb{Z}_2$ stupňa 8. Na množine 8-bitových bytov tak zavedieme operáciu sčítania a násobenia a môžeme tak s nimi pracovať ako s prvkami konečného poľa.

Na použití Galoisových polí sú založené napríklad cyklické binárne kódy, BCH-kódy, šifrovací algoritmus Al-Gamal, najnovší šifrovací štandard AES a jeho rozšírená verzia Rijndael a mnoho ďalších.

Diffie–Hellmanova výmena kľúčov

Bob odcestoval do Austrálie, ale Alica ostala v Európe. Pred odchodom si zabudli dohodnúť tajný kľúč na šifrovanie správ. Ako si majú dohodnúť a poslať tento kľúč po verejných – a teda odpočúvateľných – linkách? Tento kryptografický problém rieši tzv. Diffie–Hellmanova výmena kľúčov.

- Alica a Bob si verejne vyberú veľké prvočíslo p a tiež prvok $a \in \mathbb{Z}_p$ (t. j. $0 < a \leq p-1$).
- Alica si zvolí tajné prirodzené číslo x a Bob zvolí tajné prirodzené číslo y.
- Alica vypočíta $\alpha = a^x$ v $\mathbb{Z}_p$ a zašle α verejnou poštou Bobovi.
- Bob vypočíta $\beta = a^y$ v $\mathbb{Z}_p$ a zašle β verejnou poštou Alici.
- Alica vypočíta kľúč $K_A = \beta^x$ v $\mathbb{Z}_p$.
- Bob vypočíta kľúč $K_B = \alpha^x$ v $\mathbb{Z}_p$.

Pretože $K_A = \beta^x = (a^y)^x = a^{(xy)} = (a^x)^y = \alpha^y = K_B$, Alica aj Bob majú rovnaký kľúč. Narušiteľ nedokáže zo znalosti čísel p, a, α, β určiť K_A, resp. K_B. Na to by mu stačilo vyriešiť rovnice $\alpha = a^x$, $\beta = a^y$, čo je však ťažký problém diskrétneho logaritmu. Na záver ešte poznamenajme, že namiesto $\mathbb{Z}_p$ možno pri práve popísanej procedúre použiť tiež veľké Galoisovo teleso $GF(p^n)$.

Cvičenia

1. Nech $\mathcal{P}(x)$ je množina všetkých polynómov nad poľom reálnych čísel a nech $\oplus_p$ je sčítanie a $\otimes_p$ je násobenie polynómov. Dokážte, že $(\mathcal{P}(x), \oplus_p, \otimes_p)$ nie je pole.
2. Nájdite normovaný polynóm s reálnymi koeficientmi najnižšieho možného stupňa, ktorý spĺňa podmienky:
   a) $x = 3$ je jeho jednoduchý a $y = -1$ dvojnásobný koreň a absolútny člen sa rovná 12.
   b) $x = -i$ je jeho jednoduchý a $y = 1 - i$ dvojnásobný koreň
   c) $x = 1 + i$ je jeho dvojnásobný koreň a absolútny člen sa rovná 1.

3. Pre akú hodnotu parametra a polynómu $p(x) = x^5 - ax^2 - ax + 1$ je $c = -1$ jeho:

   a) jednoduchým koreňom,

   b) dvojnásobným koreňom,

   c) trojnásobným koreňom?

4. Pomocou Hornerovej schémy vydeľte:

   a) polynóm $p(x) = -4x^6 - 20x^5 - 17x^4 + 2x - 3$ polynómom $x + 1$,

   b) polynóm $p(x) = 3x^4 + (1 - 3i)x^3 - 2ix^2 + ix + 1 - i$ polynómom $x - i$.

5. Nájdite všetky korene polynómu nad poľom komplexných čísel, keď poznáte jeden jeho koreň:

   a) $p(x) = x^4 - 4x^3 + 15x^2 - 22x + 10$, $x_1 = 1$,

   b) $q(x) = x^4 - 6x^3 + 14x^2 - 8x - 16$, $x_1 = 2 - 2i$.

6. Nad poľom reálnych čísel je daný polynóm $p(x)$. Určte násobnosť koreňa $c = -2$, ak $p(x) = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16$.

7. Určte koeficienty b, c polynómu $p(x) = x^3 + 3x^2 + bx + c$, keď viete, že súčet druhých mocnín jeho koreňov sa rovná 1 a jeden jeho koreň je $x_1 = -1$.

8. Nech x_1, x_2, x_3 sú nenulové korene polynómu $p(x) = x^3 + ax^2 + bx + c$, pre ktoré platí $x_1 : x_2 : x_3 = 3 : (-2) : 1$. Vypočítajte tieto korene, keď viete, že $12b - c = 0$.

9. Nájdite všetky racionálne korene polynómu $p(x)$ a určte ich násobnosť, keď $p(x) = 2x^5 + 9x^4 + 13x^3 + 7x^2 - 4$.

10. Nájdite rozklad polynómu $p(x) = x^6 - 2x^5 + x^4 + x^2 - 2x + 1$ na súčin ireducibilných polynómov nad poľom $\mathbb{R}$ a $\mathbb{C}$.

11. Nájdite rozklad polynómu $p(x) = x^4 - 5x^2 + 6$ nad poľom $\mathbb{Q}$ a $\mathbb{R}$.

12. Nájdite Taylorov rozvoj polynómov:

   a) $p(x) = x^4 - 8x^3 + 24x^2 - 50x + 90$ v bode $c = -2$,

   b) $p(x) = x^4 + 2ix^3 - (1 + i)x^2 - 3x + 7 + i$ v bode $c = -i$.

13. Aké podmienky musia spĺňať koeficienty p, q, m, aby polynóm $p(x) = x^4 + px^2 + q$ bol deliteľný polynómom $q(x) = x^2 + mx + 1$?

14. Nájdite Euklidovým algoritmom najväčšieho spoločného deliteľa polynómov:

    a) $p(x) = 2x^5 + 3x^3 - 2x^2 + x + 1$ a $q(x) = x^6 - x^4 - x^3 - 2x^2 + 2x$,

    b) $p(x) = x^4 - 4x^3 + 1$ a $q(x) = x^3 - 3x^2 + 1$.

15. Použitím Euklidovho algoritmu nájdite polynómy $u(x)$ a $v(x)$ tak, aby platila Bezoutova rovnosť, keď

    a) $p(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$, $q(x) = 3x^4 - 4x^3 - x^2 - x - 2$,

    b) $p(x) = 3x^3 - 2x^2 + x + 2$, $q(x) = x^2 - x + 1$.

16. Rozložte na elementárne zlomky nad poľom $\mathbb{R}$ racionálne funkcie:

$$f(x) = \frac{6x^2 + 7x + 4}{2x^3 + 3x^2 - 1} \qquad h(x) = \frac{2x^3 - 2x^2 + 4x - 4}{x^4 - 4}$$

Kapitola 4

Vektorové priestory

4.1 Základné pojmy

V tejto kapitole sa budeme zaoberať ďalšou algebraickou štruktúrou - vektorovým priestorom. Vektorový priestor je založený na dvoch algebraických štruktúrach, ktoré poznáme z predchádzajúcich kapitol, a to komutatívnej grupe a poli. K zavedeniu novej algebraickej štruktúry nás vedú dva aspekty:

a) aby zavedený pojem bol dostatočne všeobecný a aby obsiahol vlastnosti mnohých matematických objektov,

b) aby sa vypracovaná teória dala aplikovať pri riešení tak matematických ako aj nematematických problémov.

Pojem vektorového priestoru si priblížime cez predstavu vektora známeho už zo strednej školy. V geometrii alebo aj vo fyzike sme znázorňovali vektory ako orientované úsečky, ktorých jeden krajný bod bol prehlásený za počiatočný a druhý za koncový. Orientácia vektora bola naznačená šípkou. Naučili sme sa, že vektory je možné sčítať a násobiť ľubovoľným reálnym číslom ako aj to, že dva vektory sa považujú za rovnaké, keď môžeme jeden do druhého premiestniť rovnobežným posunutím. Pokiaľ vektory umiestnime v rovine do zvoleného súradnicového systému s počiatkom O a tento prehlásime za počiatočný bod vektora, tak koncový bod uvažovaného vektora je jednoznačne určený usporiadanou dvojicou súradníc (a_1, a_2), pričom a_1, a_2 sú ľubovoľné reálne čísla. Mno-

žinu všetkých vektorov v rovine si môžeme predstavovať ako množinu

$$V_2(\mathbb{R}) = \{\mathbf{a} = (a_1, a_2); a_1, a_2 \in \mathbb{R}\},$$

na ktorej definujeme dve operácie

a) sčítanie vektorov:

$$\mathbf{a} + \mathbf{b} = (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2), \text{ pre } \forall\ \mathbf{a}, \mathbf{b} \in V_2(\mathbb{R})$$

b) násobenie vektora reálnym číslom:

$$c \cdot \mathbf{a} = c \cdot (a_1, a_2) = (ca_1, ca_2), \text{ pre } \forall\ \mathbf{a} \in V_2(\mathbb{R}) \text{ a pre } \forall c \in \mathbb{R}\ .$$

Z vlastností reálnych čísel vyplýva, že definované sčítanie dvojíc reálnych čísel je komutatívne i asociatívne. Usporiadaná dvojica $(0, 0)$ plní úlohu neutrálneho prvku a ku každej usporiadanej dvojici $(a_1, a_2) \in V_2(\mathbb{R})$ existuje vzhľadom na sčítanie inverzný prvok $(-a_1, -a_2) \in V_2(\mathbb{R})$. $V_2(\mathbb{R})$ tvorí vzhľadom na sčítanie usporiadaných dvojíc komutatívnu grupu. Kým násobenie reálnych čísel je na množine $\mathbb{R}$ binárnou operáciou, násobenie usporiadanej dvojice reálnym číslom binárnou operáciou na množine $V_2(\mathbb{R})$ nie je. Je ale vonkajšou binárnou operáciou, t. j. zobrazením $\mathbb{R} \times V_2(\mathbb{R}) \to V_2(\mathbb{R})$. Pre toto zobrazenie je možné na základe vlastností reálnych čísel ukázať nasledujúce identity:

$$\begin{aligned} c \cdot (\mathbf{a} + \mathbf{b}) &= c \cdot \mathbf{a} + c \cdot \mathbf{b} \\ (c + c') \cdot \mathbf{a} &= c \cdot \mathbf{a} + c' \cdot \mathbf{a} \\ (c \cdot c') \cdot \mathbf{a} &= c \cdot (c' \cdot \mathbf{a}) \\ 1 \cdot \mathbf{a} &= \mathbf{a}, \end{aligned}$$

kde $c, c' \in \mathbb{R}$, $\mathbf{a}, \mathbf{b} \in V_2(\mathbb{R})$.

Tak ako je možné zovšeobecniť sčítanie vektorov a násobenie vektora reálnym číslom na usporiadanú n-ticu reálnych čísel, "zovšeobecníme" aj spomínané binárne operácie a zavedieme abstraktný pojem vektorového priestoru nad ľubovoľným daným poľom. Uvedený príklad nám bude aj v ďalšom slúžiť ako pomôcka pre lepšiu predstavu vektorových priestorov.

Skôr ako pristúpime k samotnej definícii, urobíme nasledujúcu dohodu. V tejto kapitole budeme pracovať s pojmom vektorového priestoru, ktorý (ako sme už povedali) je založený na dvoch algebraických štruktúrach, a to na poli

$\mathcal{P} = (P, \boxplus, \boxdot)$ a komutatívnej grupe $\mathcal{V} = (V, \oplus)$. Prvky množiny V nazveme vektormi, grupu $\mathcal{V}$ grupou vektorov. Prvky poľa $\mathcal{P}$ budeme značiť italikou – napríklad $t \in P$, $s \in P$ a nazývať **skaláre**. Vektory – prvky grupy $\mathcal{V}$ – budeme označovať tučnými malými písmenami, napríklad $\mathbf{u} \in V$, $\mathbf{v} \in V$. Operáciu $\oplus$ nazveme **sčítaním vektorov**, vektor $\mathbf{w} = \mathbf{u} \oplus \mathbf{w}$ je **súčet vektorov u** a **w**.

Definícia 4.1. Nech $\mathcal{P} = (P, +, .)$ je pole s jednotkovým prvkom 1_P a nech $\mathcal{V} = (V, +)$ je komutatívna grupa. Nech $\otimes$ je tzv. vonkajšia operácia

$$\otimes : P \times V \to V, \tag{4.1}$$

ktorá každej usporiadanej dvojici $(t, \mathbf{v})$, $t \in P$, $\mathbf{v} \in V$ priradí prvok $t \otimes \mathbf{v} \in V$.

Hovoríme, že množina V s operáciou $+$ a vonkajšou operáciou $\otimes$ je **vektorový priestor** nad poľom $\mathcal{P}$, ak platí

$$\forall\, t, s \in P, \quad \forall\, \mathbf{v} \in V \qquad t \otimes (s \otimes \mathbf{v}) = (t \boxdot s) \otimes \mathbf{v} \tag{4.2}$$

$$\forall\, t, s \in P, \quad \forall\, \mathbf{v} \in V \qquad (t \boxplus s) \otimes \mathbf{v} = (t \otimes \mathbf{v}) \oplus (s \otimes \mathbf{v}) \tag{4.3}$$

$$\forall\, t \in P, \quad \forall\, \mathbf{u}, \mathbf{v}, \in V \qquad t \otimes (\mathbf{u} \oplus \mathbf{v}) = (t \otimes \mathbf{u}) \oplus (t \otimes \mathbf{v}) \tag{4.4}$$

$$\forall\, \mathbf{v}, \in V \qquad 1_P \otimes \mathbf{v} = \mathbf{v} \tag{4.5}$$

Pri tomto značení budeme pre jednoduchosť písať pre $t,\ s \in P$, $\mathbf{u} \in \mathcal{V}$, $\mathbf{v} \in \mathcal{V}$ $t + s$ namiesto $t \boxplus s$, ts resp. $t.s$ namiesto $t \boxdot s$, $t.\mathbf{v}$ alebo len $t\mathbf{v}$ namiesto $t \otimes \mathbf{v}$ a 1 namiesto 1_P. Toto si môžeme dovoliť bez ujmy na presnosti, pretože podľa príslušnosti operandov k množine P, resp. k množine V, bude jasné, o ktorú operáciu pôjde. Vždy však majme na pamäti, že operácia $+$ je iná v zápise $t + s$ ako v zápise $\mathbf{u} + \mathbf{v}$!

Vlastnosti (4.2) až (4.5) vektorového priestoru potom budú mať tvar

$$\forall\, t, s \in P, \quad \forall\, \mathbf{v} \in V \qquad t.(s.\mathbf{v}) = (ts).\mathbf{v} \tag{4.6}$$

$$\forall\, t, s \in P, \quad \forall\, \mathbf{v} \in V \qquad (t + s).\mathbf{v} = (t.\mathbf{v}) + (s.\mathbf{v}) \tag{4.7}$$

$$\forall\, t \in P, \quad \forall\, \mathbf{u}, \mathbf{v}, \in V \qquad t.(\mathbf{u} + \mathbf{v}) = (t.\mathbf{u}) + (t.\mathbf{v}) \tag{4.8}$$

$$\forall\, \mathbf{v}, \in V \qquad 1.\mathbf{v} = \mathbf{v} \tag{4.9}$$

Neutrálny prvok v grupe $\mathcal{V} = (V, +)$ označíme symbolom $\mathbf{o}$ a nazveme **nulový vektor**. Nulový prvok poľa $\mathcal{P}$ označíme symbolom 0. Symetrizačný prvok k vektoru $\mathbf{v} \in V$ označíme $-\mathbf{v}$ a nazveme **opačný vektor** k vektoru $\mathbf{v}$. Často budeme písať skrátene $\mathbf{u} - \mathbf{v}$ namiesto $\mathbf{u} + (-\mathbf{v})$. Vektorový priestor nad

poľom $\mathcal{P}$ budeme označovať symbolom $V(\mathcal{P})$, resp. $(V, \oplus, \otimes)$, ak budeme chcieť zdôrazniť, že ide o vektorový priestor s vnútornou operáciou $\oplus$ a vonkajšou operáciou $\otimes$.

V motivačnom príklade úlohu poľa $\mathcal{P}$ hralo pole reálnych čísel $\mathbb{R}$. Teraz uvedieme niekoľko príkladov, ktoré budú demonštrovať šírku zavedeného pojmu.

Príklad 4.1. Nech $\mathcal{P} = (P, +, \cdot)$ je ľubovoľné pole. Označme

$$V_n(\mathcal{P}) = \big\{(a_1, a_2, \ldots, a_n); a_i \in P,\ i = 1, 2, \ldots, n\big\}$$

množinu všetkých usporiadaných n-tíc prvkov z poľa $\mathcal{P}$. Na tejto množine definujeme súčet dvoch n-tíc vzťahom

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \tag{4.10}$$

a násobenie n-tice prvkom poľa $\mathcal{P}$ vzťahom

$$c \cdot (a_1, a_2, \ldots, a_n) = (ca_1, ca_2, \ldots, ca_n)\ . \tag{4.11}$$

Podobne ako v motivačnom príklade vzhľadom na definované operácie je $V_n(\mathcal{P})$ vektorovým priestorom nad poľom $\mathcal{P}$. Keďže $\mathcal{P}$ je pole, tak operácia $+$ je v poli asociatívna i komutatívna, teda túto vlastnosť má aj sčítanie usporiadaných n-tíc. Neutrálnym prvkom je n-tica $(0, 0, \ldots, 0)$ a inverzným prvkom k prvku $(a_1, a_2, \ldots, a_n)$ je n-tica $(-a_1, -a_2, \ldots, -a_n)$. Teda $V_n(\mathcal{P})$ je komutatívna grupa vzhľadom na sčítanie usporiadaných n-tíc. Vzťahy 4.2 - 4.5 je možné overiť vychádzajúc z vlastností poľa $\mathcal{P}$. V poli $\mathcal{P}$ platia distributívne zákony - vzťahy 4.3, 4.4; násobenie v poli $\mathcal{P}$ je asociatívne - vzťah 4.2 a nakoniec $1 \in P$ je jednotkou poľa $\mathcal{P}$. Zrejme $V_2(\mathbb{R})$ je špeciálnym prípadom vektorového priestoru $V_n(\mathcal{P})$.

Poznámka* 4.1.** *Vektorový priestor $V_n(\mathcal{P})$ z príkladu 4.1 s operáciami sčítania n -tíc a násobenia n-tice skalárom definovanými vzťahmi 4.10 a 4.11 nazývame* ***aritmetický priestor nad poľom $\mathcal{P}$.

Príklad 4.2. Skúmajme teraz množinu všetkých reálnych funkcií definovaných na intervale $(0, 1)$. Súčtom dvoch funkcií f a g je funkcia $f + g$, kde

$$(f + g)(x) = f(x) + g(x) \quad \text{pre každé } x \in (0, 1).$$

Súčinom funkcie f a reálneho čísla c je funkcia $c \cdot f$, kde

$$(c \cdot f)(x) = c \cdot f(x) \quad \text{pre každé } x \in (0, 1).$$

Ľahko možno overiť platnosť všetkých axióm vektorového priestoru. Urobte tak!

Príklad 4.3. Ak označíme $P_n = \{p(x); st\{p(x)\} \leq n\}$ množinu všetkých polynómov s reálnymi koeficientmi stupňa najviac n, kde n je dané prirodzené číslo, tak množina $(P_n, +, \cdot)$ s obvyklým sčítaním polynómov a obvyklým násobením polynómu reálnym číslom tvorí vektorový priestor nad poľom $\mathbb{R}$. Presvedčte sa o tom dôsledným preverením platnosti všetkých axióm vektorového priestoru!

Príklad 4.4. Množina všetkých polynómov práve n-tého stupňa, kde n je dané prirodzené číslo, netvorí vektorový priestor nad poľom reálnych čísel! Napr. $p(x) = x^3 + x - 1$ a $q(x) = -x^3 - 3x + 5$ sú polynómy práve tretieho stupňa. Ich súčet je polynóm $r(x) = 4x - 6$ stupňa prvého. Teda sčítanie polynómov nepredstavuje ani binárnu operáciu na množine polynómov práve tretieho stupňa.

Príklad 4.5. Ak v príklade 4.1 položíme $P = \mathbb{Q}$, resp. $P = \mathbb{R}$, $P = \mathbb{C}$, tak množiny $V_n(\mathbb{Q})$, $V_n(\mathbb{R})$, $V_n(\mathbb{C})$ sú vektorové priestory nad poľom racionálnych, resp. reálnych alebo komplexných čísel.

Príklad 4.6. Položme v príklade 4.1 $P = \mathbb{Z}_p$, kde p prvočíslo. Potom $\mathbb{Z}_p$ je konečné pole. Potom $V_n(\mathcal{P}) = V_n(\mathbb{Z}_p)$ je vektorový priestor nad konečným poľom $\mathbb{Z}_p$. Keďže prvkami $V_n(\mathbb{Z}_p)$ sú všetky usporiadané n-tice prvkov z poľa $\mathbb{Z}_p$ je počet prvkov $V_n(\mathbb{Z}_p)$ konečný a rovná sa číslu p^n.

***Poznámka* 4.2.** *Aj z uvedených príkladov vidíme, že pojem vektorový priestor je abstraktným pojmom (rovnako ako pojem vektor). Konkrétnu formu nadobúdajú až po zadefinovaní množiny objektov. Tak môžeme pojmom vektor označovať usporiadanú n-ticu prvkov číselného poľa, polynóm ľubovoľného stupňa, či – ako uvidíme neskôr – aj maticu.*

V nasledujúcej vete uvedieme jednoduché vlastnosti, ktoré platia v každom vektorovom priestore.

Veta 4.1. *Majme vektorový priestor $V(\mathcal{P}) = (V, +, \cdot)$ nad poľom $\mathcal{P}$. Potom platí*

$$0.\mathbf{v} = \mathbf{o} \quad \text{pre ľubovoľný vektor } \mathbf{v} \in V(\mathcal{P}) \tag{4.12}$$

$$(-1).\mathbf{v} = -\mathbf{v} \quad \text{pre ľubovoľný vektor } \mathbf{v} \in V(\mathcal{P}) \text{ a skalár } c \in P \tag{4.13}$$

$$c \cdot \mathbf{o} = \mathbf{o} \quad \text{pre ľubovoľný skalár } c \in P \tag{4.14}$$

$$c \cdot \mathbf{v} = \mathbf{o} \quad \text{práve vtedy, keď } c = 0 \text{ alebo } \mathbf{v} = 0 \tag{4.15}$$

DÔKAZ:
Dokážeme (4.12). Pre ľubovoľný vektor $\mathbf{v} \in V$ využijúc vlastností 4.5 a 4.3 platí:

$$\mathbf{v} = \mathbf{v} + 0.\mathbf{v} = 1.\mathbf{v} + 0.\mathbf{v} = (1 + 0).\mathbf{v}$$

Pretože rovnica $\mathbf{v} + \mathbf{x} = \mathbf{v}$ má v grupe $\mathcal{V}$ jediné riešenie, a to $\mathbf{x} = \mathbf{o}$, je $0.\mathbf{v} = \mathbf{o}$.

Teraz dokážeme (4.13). Pretože $\mathcal{V}$ je grupa a platia axiómy z definície vektorového priestoru, môžeme písať rovnosti

$$\mathbf{v} + (-1.)\mathbf{v} = 1.\mathbf{v} + (-1).\mathbf{v} = (1 - 1).\mathbf{v} = 0.\mathbf{v} = \mathbf{o}.$$

Pretože rovnica $\mathbf{v} + \mathbf{x} = \mathbf{o}$ má v grupe $\mathcal{V}$ jediné riešenie, a to $\mathbf{x} = -\mathbf{v}$, je $(-1).\mathbf{v} = -\mathbf{v}$.

Vzťah 4.14 dokážeme využijúc axiómu 4.2 a už dokázaný vzťah 4.12.

$$c.\mathbf{o} = c.(0.\mathbf{v}) = (c.0).\mathbf{v} = 0.\mathbf{v} = \mathbf{o}.$$

Posledný vzťah dokážeme využijúc vlastnosti poľa $\mathcal{P}$ a axióm 4.5 a 4.2 uvedených v definícii vektorového priestoru. Nech $c.\mathbf{v} = \mathbf{o}$ a $c \neq 0$, $\mathbf{v} \neq 0$. Ku skaláru c existuje v poli $\mathcal{P}$ inverzný prvok $c^{-1} \in P$. Môžeme písať rovnosti

$$\mathbf{v} = 1.\mathbf{v} = (c^{-1}.c).\mathbf{v} = c^{-1}(c.\mathbf{v}) = c^{-1}.\mathbf{0} = \mathbf{o},$$

čo je spor s predpokladom. Naopak, ak $c = 0$ alebo $\mathbf{v} = \mathbf{o}$, tak $c.\mathbf{v} = \mathbf{o}$ podľa už dokázaných tvrdení 4.12 a 4.14 vyslovenej vety. ■

4.2 Vektorový podpriestor

V predchádzajúcej kapitole sme ukázali, že množina $V_2(\mathbb{R})$ je vektorovým priestorom. Je ľahké presvedčiť sa, že množina $M = \{(a, 0); a \in \mathbb{R}\}$ (t. j. množina usporiadaných dvojíc reálnych čísel s nulovou druhou zložkou) je vektorový priestor nad poľom reálnych čísel $\mathbb{R}$. Navyše M je podmnožinou množiny $V_2(\mathbb{R})$. Tak sa dostávame k pojmu podpriestor vektorového priestoru.

Definícia 4.2. Vektorový priestor $(U, \boxplus, \boxtimes)$ nad poľom $\mathcal{P}$ nazveme **vektorový podpriestor** priestoru $(V, \oplus, \otimes)$ nad poľom $\mathcal{P}$, ak $U \subseteq V$ a pre všetky $\mathbf{u},\ \mathbf{v} \in U$ a všetky $t \in P$ platí:

a) $\mathbf{u} \boxplus \mathbf{v} = \mathbf{u} \oplus \mathbf{v}$,

b) $t \boxtimes \mathbf{v} = t \otimes \mathbf{v}$.

Nasledujúce tvrdenie je bezprostredným dôsledkom práve vyslovenej definície.

Veta 4.2. *Nech $\mathcal{L} = (V, +, \cdot)$ je vektorový priestor nad poľom $\mathcal{P}$, $\emptyset \neq U \subseteq V$. Potom $(U, +, \cdot)$ je vektorovým podpriestorom priestoru $\mathcal{L}$ práve vtedy, keď pre všetky $\mathbf{u},\ \mathbf{v} \in U$ a $t \in P$ platí*

$$a)\ \mathbf{u} + \mathbf{v} \in U,$$

$$b)\ t.\mathbf{u} \in U.$$

Dôkaz:
Ak $(U, +, .)$ je vektorovým podpriestorom priestoru $(V, +, .)$, tak na základe definície 4.2 a), b) platia. Naopak, ak platia a), b), potom $0\mathbf{u} = \mathbf{o} \in U$ a pre každé $\mathbf{v} \in U$ je aj $-1.\mathbf{v} = -\mathbf{v} \in U$, čo spolu s asociatívnosťou a komutatívnosťou operácie $+$ hovorí, že $(V, +)$ je komutatívna grupa. Keďže vlastnosti lineárneho priestoru 4.6 až 4.9 (pozri str. 79) platia pre všetky $t \in P$ a pre všetky $\mathbf{u},\ \mathbf{v} \in V$, musia platiť aj pre všetky $\mathbf{u},\ \mathbf{v} \in U$. ■

Príklad 4.7. Nech $M = \{(a, b, c);\ 2a - b = 0,\ a, b, c \in \mathbb{R}\}$. Ukážme, že M je podpriestorom vektorového priestoru $V_3(\mathbb{R})$.

Riešenie:
Využijeme vetu 4.2. Množina $M \neq \emptyset$, napr. $(1, 2, 0) \in M$ a $M \subset V_3(\mathbb{R})$. Ak $\mathbf{a} = (a, b, c) \in M$, tak $2a - b = 0$, čiže $b = 2a$. Rovnako, ak $\mathbf{a}' = (a', b', c') \in M$, tak $b' = 2a'$. Pre súčet vektorov $\mathbf{a}$ a $\mathbf{a}'$ platí

$$\mathbf{a} + \mathbf{a}' = (a, 2a, c) + (a', 2a', c') = (a + a', 2(a + a'), c + c').$$

Druhá súradnica súčtu vektorov je dvojnásobkom prvej, teda $\mathbf{a} + \mathbf{a}' \in M$. Podobne pre k-násobok $\mathbf{a}$ platí

$$k.\mathbf{a} = k.(a, 2a, c) = (ka, 2ka, kc), \quad k \in \mathbb{R},$$

čiže $k.\mathbf{a} \in M$. Tým sme ukázali, že M je podpriestorom vektorového priestoru $V_3(\mathbb{R})$.

Poznámka* 4.3.** *Každý neprázdny vektorový priestor $V(\mathcal{P})$ má aspoň dva podpriestory, a to množinu $V(\mathcal{P})$ a prázdnu množinu $\{\ \}$. Tieto podpriestory nazývame* ***nevlastné podpriestory *vektorového priestoru $V(\mathcal{P})$.*

Príklad 4.8. Lineárny priestor $V_8(\mathbb{Z}_2)$ je priestor všetkých 8-členných postupností núl a jednotiek – môžeme ho stotožniť s množinou všetkých 8-bitových bytov. Množina bytov s párnym počtom jednotiek je lineárnym podpriestorom priestoru $V_8(\mathbb{Z}_2)$. Overte.

Nech $V(\mathcal{P})$ je vektorový priestor. Množinu všetkých násobkov pevne zvoleného vektora $\mathbf{v}$ označme $[\mathbf{v}]$. Potom $[\mathbf{v}] = \{c.\mathbf{v};\ c \in P\}$ je podpriestorom $V(\mathcal{P})$. (Presvedčte sa o tom!) Toto tvrdenie môžeme dokonca zovšeobecniť, čo urobíme v nasledujúcej vete. K tomu ale potrebujeme nasledujúcu definíciu lineárnej kombinácie vektorov.

Definícia 4.3. Hovoríme, že vektor $\mathbf{x}$ je **lineárnou kombináciou vektorov** $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$, ak existujú také prvky $t_1, t_2, \ldots, t_n$ poľa $\mathcal{P}$, že

$$\mathbf{x} = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_n\mathbf{v}_n = \sum_{i=1}^{n} t_i\mathbf{v}_i. \tag{4.16}$$

Množinu všetkých lineárnych kombinácií vektorov $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ budeme označovať $\big[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\big]$, čo znamená, že

$$\big[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\big] = \big\{t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_n\mathbf{v}_n;\ t_i \in P,\ i = 1, \ldots, n\big\}. \tag{4.17}$$

Veta 4.3. *Nech $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú vektory vektorového priestoru $V(\mathcal{P})$. Potom $\big[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\big]$ je podpriestorom vektorového priestoru $V(\mathcal{P})$.*

Dôkaz:
Triviálny, čitateľ si vetu dokáže ľahko sám využijúc vetu 4.2. ■

***Poznámka* 4.4.** *Hovoríme, že podpriestor $\big[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\big]$ je generovaný (vytvorený) vektormi $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$, alebo, že $\big[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\big]$ je **lineárnym obalom vektorov** $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.*

Príklad 4.9. Nájdime podpriestor vektorového priestoru $V_3(\mathbb{R})$ generovaný vektormi $\mathbf{u} = (0, 2, 1)$ a $\mathbf{v} = (1, 1, 1)$.

Riešenie:
Podpriestor $[\mathbf{u}, \mathbf{v}]$ tvoria všetky vektory tvaru

$$x_1.(0, 2, 1) + x_2.(1, 1, 1) = (x_2, 2x_1 + x_2, x_1 + x_2),$$

kde x_1, x_2 sú ľubovoľné reálne čísla.

4.3 Báza vektorového priestoru

V predchádzajúcej podkapitole sme množinu všetkých lineárnych kombinácií vektorov $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ nazvali priestorom generovaným týmito vektormi. K daným vektorom sme teda hľadali vektorový priestor, ktorý generujú. Teraz úlohu zmeníme. K zadanému vektorovému priestoru $V(\mathcal{P})$ budeme hľadať vektory, ktoré ho generujú. To znamená, že budeme hľadať vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ tak, aby sa každý vektor z vektorového priestoru $V(\mathcal{P})$ dal napísať ako ich lineárna kombinácia.

Uvažujme vektorový priestor $V_2(\mathbb{R})$ a vektory $(1,0)$ a $(0,1)$. Tieto vektory generujú $V_2(\mathbb{R})$, pretože pre ľubovoľný vektor $(x,y) \in V_2(\mathbb{R})$ platí

$$(x,y) = x.(1,0) + y.(0,1).$$

Ale aj vektory $(1,5)$, $(0,5)$ a $(1,4)$ generujú vektorový priestor $V_2(\mathbb{R})$. Ľubovoľný vektor $(x,y) \in V_2(\mathbb{R})$ sa dá napísať ako lineárna kombinácia

$$(x,y) = (x+y).(1,5) - x.(0,5) - y.(1,4).$$

Prvá množina vektorov generujúcich $V_2(\mathbb{R})$ bola dvojprvková, druhá množina bola trojprvková. Dostali sme sa k otázke – aký najmenší počet vektorov generuje daný vektorový priestor? Odpoveď na túto otázku nájdeme v tejto podkapitole. Najskôr sa ale budeme zaoberať pojmom lineárnej nezávislosti vektorov, ktorý zohráva kľúčovú úlohu v teórii vektorových priestorov.

Definícia 4.4. Hovoríme, že vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú **lineárne nezávislé**, ak z rovnosti

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{o}$$

vyplýva

$$a_1 = 0, \quad a_2 = 0, \quad \ldots, \quad a_n = 0.$$

Vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú **lineárne závislé**, ak

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{o}$$

a existuje aspoň jeden koeficient $a_i \neq 0$.

Príklad 4.10. Uvažujme trojicu vektorov $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ vektorového priestoru $V_3(\mathbb{R})$, kde $\mathbf{v}_1 = (1,0,1)$, $\mathbf{v}_2 = (0,-1,1)$, $\mathbf{v}_3 = (1,0,-1)$. Ukážme, že táto trojica vektorov je lineárne nezávislá.

Riešenie:
Podľa definície 4.4 vektory $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ sú lineárne nezávislé, keď ich lineárna kombinácia sa rovná nulovému vektoru len pre jedinú možnú trojicu koeficientov lineárnej kombinácie – a to nulovú. Teda

$$c_1.\mathbf{v}_1 + c_2.\mathbf{v}_2 + c_3.\mathbf{v}_3 = \mathbf{o}$$

a po dosadení dostávame sústavu troch rovníc o troch neznámych

$$c_1 \cdot (1,0,1) + c_2 \cdot (0,-1,1) + c_3 \cdot (1,0,-1) = (0,0,0).$$

Po rozpísaní po zložkách

$$\begin{array}{rrrr} c_1 & & + c_3 & = 0 \\ & - c_2 & & = 0 \\ c_1 & + c_2 & - c_3 & = 0 \end{array}$$

Jednoduchým výpočtom dostávame riešenie $c_1 = 0,\ c_2 = 0,\ c_3 = 0$, teda vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne nezávislé.

Príklad 4.11. Uvažujme inú trojicu vektorov $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$, keď $\mathbf{v}_1 = (1,0,1)$, $\mathbf{v}_2 = (0,-1,1)$, $\mathbf{v}_3 = (1,1,0)$. Ukážeme, že táto trojica vektorov je lineárne závislá.

Riešenie:
Tak ako v predchádzajúcom príklade budeme vychádzať z definície lineárnej závislosti vektorov. Podľa definície sú vektory závislé, ak v rovnosti $c_1.\mathbf{v}_1 + c_2.\mathbf{v}_2 + c_3.\mathbf{v}_3 = \mathbf{o}$ existuje aspoň jeden koeficient lineárnej kombinácie rôzny od nuly. Ľahko overíme, že $1.\mathbf{v}_1 - 1.\mathbf{v}_2 - 1.\mathbf{v}_3 = \mathbf{o}$. Našli sme koeficienty lineárnej kombinácie, z ktorých je aspoň jeden nenulový (v našom prípade dokonca všetky tri), teda vektory $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ sú lineárne závislé.

Pozorný čitateľ si všimol, že v predchádzajúcom príklade je vektor $\mathbf{v}_3$ lineárnou kombináciou predchádzajúcich dvoch vektorov ($\mathbf{v}_3 = \mathbf{v}_1 - \mathbf{v}_2$) a ukázali sme, že takáto trojica vektorov je lineárne závislá. Že to nie je náhoda, presvedčíme sa v nasledujúcom tvrdení.

Veta 4.4. *Vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$, $n > 1$ vektorového priestoru $V(\mathcal{P})$ sú lineárne závislé práve vtedy, keď jeden z nich je lineárnou kombináciou ostatných.*

Dôkaz:
Nech vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne závislé. Potom existujú konštanty

$t_1, t_2, \ldots, t_n \in P$ také, že

$$\mathbf{o} = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_n\mathbf{v}_n \tag{4.18}$$

a existuje také k, pre ktoré platí $t_k \neq 0$. V poli $\mathcal{P}$ existuje k takémuto t_k inverzný prvok t_k^{-1}. Úpravou vzťahu 4.18 dostaneme

$$\mathbf{o} = t_k^{-1}(t_1\mathbf{v}_1) + t_k^{-1}(t_2\mathbf{v}_2) + \cdots + t_k^{-1}(t_n\mathbf{v}_n)$$

Pre dané k zo vzťahu 4.18 dostaneme

$$\mathbf{v}_k = (-t_k^{-1}t_1)\mathbf{v}_1 + \cdots + (-t_k^{-1}t_{k-1})\mathbf{v}_{k-1} + (-t_k^{-1}t_{k+1})\mathbf{v}_{k+1} + \cdots + (-t_k^{-1}t_n)\mathbf{v}_n,$$

čiže $\mathbf{v}_k$ je lineárnou kombináciou ostatných vektorov.

Naopak, nech je niektorý z vektorov $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ lineárnou kombináciou ostatných, t. j. nech

$$\mathbf{v}_k = t_1\mathbf{v}_1 + \cdots + t_{k-1}\mathbf{v}_{k-1} + t_{k+1}\mathbf{v}_{k+1} + \cdots + t_n\mathbf{v}_n.$$

Potom

$$\mathbf{o} = t_1\mathbf{v}_1 + \cdots + t_{k-1}\mathbf{v}_{k-1} + (-1)\mathbf{v}_k + t_{k+1}\mathbf{v}_{k+1} + \cdots + t_n\mathbf{v}_n,$$

kde $t_k = -1$. Vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne závislé. ■

***Poznámka* 4.5.** *Jednoduchými a ľahko dokázateľnými dôsledkami vety 4.4 sú nasledujúce tvrdenia*

a) Dva vektory sú závislé práve vtedy, keď jeden z nich je násobkom druhého.

b) Ak jeden z vektorov $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$, $n \geq 1$ je nulový, potom sú tieto vektory lineárne závislé.

c) Ak sú dva z vektorov $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$, $n \geq 2$ rovnaké, alebo niektorý z nich je násobkom iného, potom sú tieto vektory lineárne závislé.

Veta 4.5. *Nech vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ vektorového priestoru $V(\mathcal{P})$ sú lineárne nezávislé a nech $t, t_2, t_3, \ldots, t_n$, $t \neq 0$, sú prvky poľa $\mathcal{P}$. Potom aj vektory*

$$t.\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \tag{4.19}$$

a

$$\mathbf{v}_1 + t_2.\mathbf{v}_2 + t_3.\mathbf{v}_3 + \cdots + t_n.\mathbf{v}_n, \mathbf{v}_2, \ldots, \mathbf{v}_n \tag{4.20}$$

sú lineárne nezávislé.

DÔKAZ:
Dokážeme najskôr vzťah 4.19. Nech

$$a_1.(t.\mathbf{v}_1) + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{o}.$$

Využijeme vlastnosť 4.2 definície vektorového priestoru a môžeme písať

$$(a_1.t).\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{o}.$$

Pretože vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne nezávislé, je

$$a_1.t = 0, \quad a_2 = 0, \quad \ldots, \quad a_n = 0,$$

a teda, (keďže $t \neq 0$), aj

$$a_1 = 0, \quad a_2 = 0, \quad \ldots, \quad a_n = 0,$$

z čoho vyplýva nezávislosť vektorov (4.19). Podobne dokážeme aj druhú časť tvrdenia. Nech

$$a_1.\big(\mathbf{v}_1 + t_2.\mathbf{v}_2 + t_3.\mathbf{v}_3 + \cdots + t_n.\mathbf{v}_n\big) + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{o},$$

čo sa dá upraviť na tvar

$$a_1.\mathbf{v}_1 + (a_2 + a_1t_2)\mathbf{v}_2 + (a_3 + a_1t_3)\mathbf{v}_3 + \cdots + (a_n + a_1t_n)\mathbf{v}_n = \mathbf{o}.$$

Pretože vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne nezávislé, je

$$\begin{aligned} a_1 &= 0 \\ a_i + a_1t_i &= 0 \quad \text{pre } i = 2, 3, \ldots, n, \end{aligned}$$

z čoho vyplýva, že $a_i = 0$ pre $i = 1, 2, \ldots, n$. Tým sme lineárnu nezávislosť vektorov (4.20) dokázali. ■

***Poznámka* 4.6.** *Vo vete 4.5 sme dokázali, že ak množinu lineárne nezávislých vektorov upravíme tak, že jeden z vektorov nahradíme jeho ľubovoľným nenulovým násobkom, alebo k jednému vektoru pripočítame lineárnu kombináciu ostatných vektorov, zostane sústava lineárne nezávislou. Na túto skutočnosť si častokrát spomenieme pri riešení sústav lineárnych rovníc.*

Následne uvedieme vetu, ktorá hovorí o súvislosti medzi lineárnym obalom a lineárnou závislosťou vektorov.

Veta 4.6. *Nech* $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ *sú lineárne nezávislé vektory vektorového priestoru* $V(\mathcal{P})$. *Nech pre* $\mathbf{u} \in V(\mathcal{P})$ *platí, že* $\mathbf{u} \in \left[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\right]$ *Potom*

a) vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n, \mathbf{u}$ *sú lineárne závislé;*

b) $\left[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n, \mathbf{u}\right] = \left[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\right]$.

DÔKAZ:
Triviálny. a) Ak $\mathbf{u} \in \left[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\right]$, tak podľa tvrdenia vety 4.4 sú lineárne závislé. b) Označme $T = \left[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\right]$ a $U = \left[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n, \mathbf{u}\right]$. Zrejme platí $T \subseteq U$. Naopak každý vektor z množiny U sa dá vyjadriť ako lineárna kombinácia vektorov $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$. Teda $U \subseteq T$, čo znamená, že $U = T$. ■

***Poznámka* 4.7.** *Nech* $\left[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\right] = V(\mathcal{P})$ *a vektory* $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ *sú lineárne závislé. Z tvrdenia b) vety 4.6 vieme, že* $V(\mathcal{P})$ *generuje aj* $m-1$ *vektorov z množiny* $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$. *Ak aj týchto* $m-1$ *vektorov je lineárne závislých, tvrdenie vety použijeme znova a "vyškrtnene" ďalší vektor. Potupne dostaneme takú sústavu vektorov, ktorá je lineárne nezávislá a generuje vektorový priestor* $V(\mathcal{P})$. *Dostávame sa k pojmu báza vektorového priestoru.*

Definícia 4.5. Množinu $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ vektorov vektorového priestoru $V(\mathcal{P})$ nazveme **bázou vektorového priestoru**, ak platí:

a) vektory $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ sú lineárne nezávislé,

b) každý vektor $\mathbf{a} \in V(\mathcal{P})$ možno napísať ako lineárnu kombináciu vektorov $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$.

***Poznámka* 4.8.** *Nie v každom vektorovom priestore existuje báza. (V ktorom nie?)*

Definícia 4.6. Hovoríme, že vektorový priestor $V(\mathcal{P})$ má **konečnú dimenziu** n, kde $n \in \mathbb{N}_0$, ak existuje báza $\mathcal{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ s počtom prvkov n.

***Poznámka* 4.9.** *Budeme sa zaoberať len vektorovými priestormi s konečnou dimenziou.*

Veta 4.7. *Nech $\mathcal{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ je báza vektorového priestoru $V(\mathcal{P})$, nech $\mathbf{w} \in V(\mathcal{P})$ a $\mathbf{w} \neq \mathbf{o}$. Potom existuje aspoň jeden vektor $\mathbf{b}_k$ bázy $\mathcal{B}$ taký, že*

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{w}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n \tag{4.21}$$

je tiež bázou vektorového priestoru $V(\mathcal{P})$.

Dôkaz:
Nech

$$\mathbf{w} = a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_k\mathbf{b}_k + \cdots + a_n\mathbf{b}_n. \tag{4.22}$$

Pretože $\mathbf{w} \neq \mathbf{o}$, je aspoň jeden koeficient lineárnej kombinácie (4.22) nenulový. Nech je to koeficient a_k. V ďalšom postupe budeme vychádzať z definície bázy vektorového priestoru. Najskôr ukážeme, že vektory

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{w}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$$

sú lineárne nezávislé.

Nech

$$\mathbf{o} = \sum_{\substack{i=1\\i\neq k}}^{n} c_i\mathbf{b}_i + c_k\mathbf{w} = \sum_{\substack{i=1\\i\neq k}}^{n} c_i\mathbf{b}_i + \sum_{i=1}^{n} c_k a_i\mathbf{b}_i = \sum_{\substack{i=1\\i\neq k}}^{n}(c_i + c_k a_i)\mathbf{b}_i + c_k a_k\mathbf{b}_k \tag{4.23}$$

Vyjadrili sme nulový vektor $\mathbf{o}$ ako lineárnu kombináciu vektorov bázy $\mathcal{B}$, preto všetky koeficienty tejto lineárnej kombinácie musia byť nulové – teda aj koeficient $c_k a_k = 0$, čo je možné len vtedy, keď $c_k = 0$, pretože $a_k \neq 0$. Pre $c_k = 0$ rovnosť (4.23) bude v tvare

$$\mathbf{o} = \sum_{\substack{i=1\\i\neq k}}^{n} c_i\mathbf{b}_i, \tag{4.24}$$

odkiaľ z lineárnej nezávislosti vektorov $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$ vyplýva $c_i = 0$ pre $i = 1, 2, \ldots, k-1, k+1, \ldots, n$. Tým sme dokázali lineárnu nezávislosť vektorov (4.21).

Potrebujeme dokázať, že ľubovoľný vektor $\mathbf{x} \in V(\mathcal{P})$ sa dá vyjadriť ako lineárna kombinácia vektorov $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{w}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$. Keďže $\mathbf{x} \in V(\mathcal{P})$, potom

$$\mathbf{x} = x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \cdots + x_k\mathbf{b}_k + \cdots + x_n\mathbf{b}_n. \tag{4.25}$$

Pre $\mathbf{w}$ platí (4.22), z ktorého môžeme vyjadriť vektor $\mathbf{b}_k$ nasledujúcim postupom:

$$a_k\mathbf{b}_k = \mathbf{w} - \sum_{\substack{i=1\\ i\neq k}}^{n} a_i\mathbf{b}_i,$$

$$\mathbf{b}_k = a_k^{-1}\mathbf{w} - \sum_{\substack{i=1\\ i\neq k}}^{n} a_k^{-1}a_i\mathbf{b}_i.$$

Poznamenajme, že k bolo zvolené tak, že $a_k \neq 0$ a teda existuje a_k^{-1}.

Po dosadení do (4.25) dostaneme

$$\begin{aligned}
\mathbf{x} &= \sum_{\substack{i=1\\ i\neq k}}^{n} x_i\mathbf{b}_i + x_k\mathbf{b}_k \\
\mathbf{x} &= \sum_{\substack{i=1\\ i\neq k}}^{n} x_i\mathbf{b}_i + x_k\left[a_k^{-1}\mathbf{w} - \sum_{\substack{i=1\\ i\neq k}}^{n} a_k^{-1}a_i\mathbf{b}_i\right] \\
\mathbf{x} &= \sum_{\substack{i=1\\ i\neq k}}^{n} (x_i - a_k^{-1}a_ix_k)\mathbf{b}_i + a_k^{-1}x_k\mathbf{w}.
\end{aligned}$$

Podľa posledného vzťahu je možné každý vektor $\mathbf{x}$ vyjadriť ako lineárnu kombináciu vektorov

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{w}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n.$$

Vektory $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{w}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$ tvoria bázu vektorového priestoru $V(\mathcal{P})$. ■

***Poznámka* 4.10.** *Z dôkazu vety 4.7 vyplýva praktický záver, že vektorom* $\mathbf{w}$ *je možné nahradiť ktorýkoľvek z vektorov* $\mathbf{b}_k$*, ktorý sa v lineárnej kombinácii* (4.22) *vyskytuje s nenulovým koeficientom* a_k*.*

Z toho, čo sme si povedali doteraz vyplýva, že bázu vektorového priestoru tvoria ľubovoľné vektory, ktoré sú lineárne nezávislé a ktoré generujú vektorový priestor. To ale znamená, že ten istý vektorový priestor môžu generovať rôzne množiny vektorov. Vzniká prirodzená otázka, ako je to s počtom vektorov tvoriacich rôzne bázy toho istého vektorového priestoru. Odpoveď dáva nasledujúca veta.

Veta 4.8. *Nech $\mathcal{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$, $\mathcal{C} = (\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m)$ sú dve rôzne bázy vektorového priestoru $V(\mathcal{P})$. Potom $m = n$, t. j. obe bázy majú rovnaký počet prvkov.*

Dôkaz:
Predpokladajme $m \leq n$. Podla vety 4.7 existuje k, $1 \leq k \leq n$ také, že vektory $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{c}_1, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$ tvoria tiež bázu lineárneho priestoru $V(\mathcal{P})$, ktorú označíme symbolom $\mathcal{B}_1$. Nech má báza $\mathcal{B}_j = (\mathbf{b}_1^j, \mathbf{b}_2^j, \ldots, \mathbf{b}_n^j)$, kde $(n-j)$ prvkov je z bázy $\mathcal{B}$ a j prvkov je z bázy $\mathcal{C}$ – sú to práve vektory $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_j$. Nech

$$\mathbf{c}_{j+1} = \sum_{i=1}^{n} t_i \mathbf{b}_i^j \tag{4.26}$$

Medzi sčítancami 4.26 musí byť aspoň jeden vektor $\mathbf{b}_{k_1}$ pôvodnej bázy $\mathcal{B}$ s nenulovým koeficientom, inak by bol vektor $\mathbf{c}_{j+1}$ lineárnou kombináciou prvkov bázy $\mathcal{C}$, čo by bolo v spore s lineárnou nezávislosťou prvkov bázy $\mathcal{C}$. Podla vety 4.7 a podľa poznámky za touto vetou možno vytvoriť bázu $\mathcal{B}_{j+1}$ nahradením vektora $\mathbf{b}_{k_1}$ vektorom $\mathbf{c}_{j+1}$. Táto báza bude obsahovať vektory $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_j, \mathbf{c}_{j+1}$ a $(n-j-1)$ vektorov z bázy $\mathcal{B}$.
Báza $\mathcal{B}_n$ bude obsahovať vektory $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$. Keby bolo $n < m$, vektor $\mathbf{c}_{n+1}$ by sa dal vyjadriť ako lineárna kombinácia ostatných vektorov z $\mathcal{C}$, čo by bolo v spore s lineárnou nezávislosťou vektorov bázy $\mathcal{C}$. ■

Definícia 4.7. Nech $V(\mathcal{P})$ je vektorový priestor s konečnou dimenziou n. Nech $\mathcal{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ je báza vektorového priestoru $V(\mathcal{P})$ a $\mathbf{x} \in V(\mathcal{P})$. Nech

$$\mathbf{x} = t_1\mathbf{b}_1 + t_2\mathbf{b}_2 + \cdots + t_n\mathbf{b}_n = \sum_{i=1}^{n} t_i\mathbf{b}_i. \tag{4.27}$$

Prvky $t_1, t_2, \ldots, t_n$ nazývame **súradnice vektora $\mathbf{x}$** v báze $\mathcal{B}$.

Vektorový priestor s konečnou dimenziou umožňuje veľmi efektívne charakterizovať pomocou jeho bázy nasledujúca veta.

Veta 4.9. *Nech $V(\mathcal{P})$ je vektorový priestor s konečnou dimenziou n. Nech $\mathcal{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ je jeho báza. Potom ľubovoľný vektor $\mathbf{x} \in V(\mathcal{P})$ sa dá jednoznačne vyjadriť v tvare*

$$\mathbf{x} = t_1\mathbf{b}_1 + t_2\mathbf{b}_2 + \cdots + t_n\mathbf{b}_n = \sum_{i=1}^{n} t_i\mathbf{b}_i. \tag{4.28}$$

Dôkaz:
Predpokladajme, že vektor $\mathbf{x}$ sa dá vyjadriť v tvare lineárnej kombinácie vektorov bázy dvomi spôsobmi:

$$\begin{aligned}\mathbf{x} &= t_1\mathbf{b}_1 + t_2\mathbf{b}_2 + \cdots + t_n\mathbf{b}_n \\ \mathbf{x} &= s_1\mathbf{b}_1 + s_2\mathbf{b}_2 + \cdots + s_n\mathbf{b}_n\end{aligned}$$

Potom

$$\mathbf{o} = (t_1 - s_1)\mathbf{b}_1 + (t_2 - s_2)\mathbf{b}_2 + \cdots + (t_n - s_n)\mathbf{b}_n.$$

Z lineárnej nezávislosti vektorov bázy $\mathcal{B}$ vyplýva $(t_i - s_i) = 0$, a teda $t_i = s_i$ pre $i = 1, 2, \ldots, n$. ■

Význam dokázanej vety spočíva v tom, že v n rozmernom vektorovom priestore sa ľubovoľný jeho vektor dá charakterizovať pomocou bázy, ktorá je n-prvková, teda pomocou jeho n súradníc. V tom istom vektorovom priestore môže mať ten istý vektor $\mathbf{u}$ pri rôznych bázach rôzne súradnice.

Príklad 4.12. Uvažujme vektorový priestor $V_3(\mathbb{R})$. Jeho prvkami sú usporiadané trojice reálnych čísel (a_1, a_2, a_3). Každá trojica sa dá vyjadriť v tvare lineárnej kombinácie

$$(a_1, a_2, a_3) = a_1(1, 0, 0) + a_2(0, 1, 0) + a_3(0, 0, 1).$$

Vektory $\mathbf{e}_1 = (1, 0, 0)$, $\mathbf{e}_2 = (0, 1, 0)$, $\mathbf{e}_3 = (0, 0, 1)$ sú lineárne nezávislé a keďže a_1, a_2, a_3 boli ľubovoľné reálne čísla, generujú vektorový priestor $V_3(\mathbb{R})$ – našli sme bázu vektorového priestoru. Označme ju $\mathcal{B}_0$.

***Poznámka* 4.11.** *Príklad 4.12 môžeme zovšeobecniť. Bázu $\mathcal{B}_0$ n -rozmerného priestoru $V_n(\mathbb{R})$ tvoria vektory*

$$\mathbf{e}_1 = (1, 0, \ldots, 0),\ \mathbf{e}_2 = (0, 1, \ldots, 0), \ldots,\ \mathbf{e}_n = (0, 0, \ldots, 1)$$

Príklad 4.13. Uvažujme vektory $\mathbf{b}_1 = (1, 0, 1)$, $\mathbf{b}_2 = (0, 1, 0)$ a $\mathbf{b}_3 = (0, 1, -1)$. Presvedčme sa, že tvoria bázu vektorového priestoru $V_3(\mathbb{R})$ a nájdime súradnice vektora $\mathbf{a} = (2, 1, 3)$ v tejto báze.

Riešenie:
Zistíme najskôr či dané tri vektory sú lineárne nezávislé. Riešme rovnicu

$$c_1 \cdot \mathbf{b}_1 + c_2 \cdot \mathbf{b}_2 + c_3 \cdot \mathbf{b}_3 = \mathbf{o}.$$

Po rozpísaní dostaneme sústavu troch rovníc o troch neznámych

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

Sústava má jediné riešenie $c_1 = 0,\ c_2 = 0,\ c_3 = 0$. Vektory $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ tvoria bázu, označme ju $\mathcal{B}_1$.
Teraz nájdime súradnice vektora $\mathbf{a}$ v báze $\mathcal{B}_1$. Vektor $\mathbf{a}$ vyjadríme ako lineárnu kombináciu vektorov bázy $\mathcal{B}_1$:

$$s_1 \cdot \mathbf{b}_1 + s_2 \cdot \mathbf{b}_2 + s_3 \cdot \mathbf{b}_3 = \mathbf{a}$$

a následne riešme sústavu rovníc

$$\begin{aligned} s_1 &= 2 \\ + s_2 + s_3 &= 1 \\ s_1 - s_3 &= 3 \end{aligned}$$

Vyriešením sústavy dostaneme súradnice $s_1 = 2,\ s_2 = 2,\ s_3 = -1$, teda môžeme písať $\mathbf{a} = (2, 2, -1)_{\mathcal{B}_1}$.

Príklad 4.14. Na začiatku kapitoly sme uviedli, že polynómy stupňa najviac n tvoria nad poľom reálnych čísel vektorový priestor, označme ho $P_n(\mathbb{R})$. V našom príklade zvoľme $n = 2$ a zaoberajme sa reálnymi polynómami najviac druhého stupňa. Všeobecné vyjadrenie takého polynómu je

$$p_2(x) = a_0 + a_1 x + a_2 x^2, \text{ kde } a_0, a_1, a_2 \in \mathbb{R}.$$

Ľahko overíme, že báza tohoto vektorového priestoru je

$$\mathcal{B}_0 = (\mathbf{b}_0(x) = 1, \mathbf{b}_1(x) = x, \mathbf{b}_2(x) = x^2).$$

Inou bázou vektorového priestoru $P_2(\mathbb{R})$ je $\mathcal{B}_2 = \big(\mathbf{r}_1(x), \mathbf{r}_2(x), \mathbf{r}_3(x)\big)$, kde $\mathbf{r}_1(x) = x$, $\mathbf{r}_2(x) = 1$, $\mathbf{r}_3(x) = 1 + x^2$. Presvedčme sa o tom. Stačí overiť, že vektory $\mathbf{r}_1(x),\ \mathbf{r}_2(x),\ \mathbf{r}_3(x)$ sú lineárne nezávislé.

$$c_1 \cdot \mathbf{r}_1(x) + c_2 \cdot \mathbf{r}_2(x) + c_3 \cdot \mathbf{r}_3(x) = \mathbf{o}$$

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

Jediným riešením sústavy rovníc je $c_1 = 0,\ c_2 = 0,\ c_3 = 0$, vektory $\mathbf{r}_1(x), \mathbf{r}_2(x), \mathbf{r}_3(x)$ tvoria bázu vektorového priestoru $P_2(\mathbb{R})$.

Príklad 4.15. Daný je polynóm $p_4(x) = x^4 - 5x^3 + 2x^2 + x - 2,\ p_4(x) \in P_4(\mathbb{R})$. V báze $\mathcal{B}_0 = (\mathbf{b}_0(x) = 1, \mathbf{b}_1(x) = x, \mathbf{b}_2(x) = x^2, \mathbf{b}_3(x) = x^3, \mathbf{b}_4(x) = x^4)$ má súradnice $p_4(x) = (-2, 1, 2, -5, 1)_{\mathcal{B}_0}$. Aké súradnice bude mať $p_4(x)$ v báze $\mathcal{B}_1$, keď

$$\mathcal{B}_1 = \big(1, (x-1), (x-1)^2, (x-1)^3, (x-1)^4\big)?$$

Riešenie:
Vyjadríme polynóm $p_4(x)$ ako lineárnu kombináciu polynómov – vektorov bázy $\mathcal{B}_1$.

$$p_4(x) = s_1 \cdot 1 + s_2 \cdot (x-1) + s_3 \cdot (x-1)^2 + s_4 \cdot (x-1)^3 + s_5 \cdot (x-1)^4.$$

Zápis predstavuje Taylorov rozvoj polynómu v bode $c = 1$. Z riešenia príkladu 3.3 získame nasledujúci výsledok: $p_4(x) = (-3. - 6, -7, -1, -1)_{\mathcal{B}_1}$.

4.4 Izomorfizmus vektorových priestorov

Doteraz sme sa zakaždým zaoberali štruktúrou len jedného vektorového priestoru a bokom zostal prípadný vzťah medzi dvomi, resp. viacerými vektorovými priestormi definovanými nad tým istým poľom. Aspoň v základných črtách tak urobíme v tejto podkapitole.

Skúmajme dva vektorové priestory – $V_3(\mathbb{R})$ a $P_2(\mathbb{R})$. Vieme, že $V_3(\mathbb{R})$ je množinou všetkých usporiadaných trojíc reálnych čísel, na ktorej sme definovali operácie sčítania dvoch usporiadaných trojíc po zložkách a násobenie usporiadanej trojice reálnou konštantou. $P_2(\mathbb{R})$ je vektorový priestor polynómov nanajvýš druhého stupňa nad poľom reálnych čísel. Pri dôkladnejšom štúdiu zistíme podobnosť medzi týmito dvomi priestormi. Definujme zobrazenie $\varphi : P_2(\mathbb{R}) \to V_3(\mathbb{R})$ takto: Pre ľubovoľný vektor $\boldsymbol{\alpha} = a_0 + a_1 x + a_2 x^2 \in P_2(\mathbb{R})$

$$\varphi(\boldsymbol{\alpha}) = (a_0, a_1, a_2).$$

Obraz vektora $\varphi(\boldsymbol{\alpha})$ je usporiadaná trojica reálnych čísel a ľahko sa presvedčíme, že φ je vzájomne jednoznačným zobrazením $V_3(\mathbb{R})$ na $P_2(\mathbb{R})$.
Navyše ak $\boldsymbol{\beta} = b_0 + b_1 x + b_2 x^2$, tak

$$\begin{aligned} \varphi(\boldsymbol{\alpha} + \boldsymbol{\beta}) &= \varphi\big((a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2\big) \\ &= (a_0 + b_0, a_1 + b_1, a_2 + b_2) \\ &= (a_0, a_1, a_2) + (b_0, b_1, b_2) \end{aligned}$$

$$= \quad \varphi(\boldsymbol{\alpha}) + \varphi(\boldsymbol{\beta}).$$

Podobne ak c je ľubovoľné reálne číslo, tak

$$\begin{aligned} \varphi(c \cdot \boldsymbol{\alpha}) &= \varphi(c \cdot a_0 + c \cdot a_1 x + c \cdot a_2 x^2) \\ &= (c \cdot a_0, c \cdot a_1, c \cdot a_2) \\ &= c \cdot (a_0, a_1, a_2) \\ &= c \cdot \varphi(\boldsymbol{\alpha}). \end{aligned}$$

Vidíme, že zobrazenie φ zachováva operácie vektorového priestoru – súčtu vektorov priraďuje súčet ich obrazov a súčinu skalára s vektorom priraďuje súčin skalára s jeho obrazom. Takéto zobrazenie vektorových priestorov nazývame izomorfizmus.

Definícia 4.8. Nech $(U, +, \cdot)$, $(V, +, \cdot)$ sú dva vektorové priestory nad tým istým poľom $(P, +, \cdot)$. Zobrazenie $\varphi : U \to V$ nazveme **izmorfizmom**, ak platí

a) φ je vzájomne jednoznačné zobrazenie U na V,

b) pre každé $\mathbf{x},\ \mathbf{y} \in U \quad \varphi(\mathbf{x} + \mathbf{y}) = \varphi(\mathbf{x}) + \varphi(\mathbf{y})$,

c) pre každé $\mathbf{x} \in U$ a pre každé $t \in P \quad \varphi(t\mathbf{x}) = t\varphi(\mathbf{x})$.

Ak medzi dvoma vektorovými priestormi existuje izomorfizmus, hovoríme, že tieto vektorové priestory sú **izomorfné**.

Izomorfné priestory sú z nášho hľadiska úplne totožné. To znamená, že ak preštudujeme nejaký vektorový priestor, tak výsledky môžeme aplikovať na všetky izomorfné vektorové priestory. Tento fakt značne uľahčuje štúdium vektorových priestorov, lebo sa môžeme sústrediť na štúdium vektorových priestorov $V_n(\mathcal{P})$, ktoré majú pomerne jednoduchú štruktúru.

Veta 4.10. *Každý vektorový priestor $V(\mathcal{P})$ s konečnou dimenziou n je izomorfný s vektorovým priestorom $V_n(\mathcal{P})$.*

Dôkaz:
Nech $\mathcal{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ je báza vektorového priestoru $V(\mathcal{P})$. Podľa vety 4.9 ľubovoľný vektor $\mathbf{v} \in V(\mathcal{P})$ sa dá jednoznačne vyjadriť v tvare

$$\mathbf{v} = v_1\mathbf{b}_1 + v_2\mathbf{b}_2 + \cdots + v_n\mathbf{b}_n = \sum_{i=1}^{n} v_i\mathbf{b}_i.$$

Definujme zobrazenie $\varphi : V(\mathcal{P}) \to V_n(\mathcal{P})$ predpisom

$$\varphi(\mathbf{v}) = (v_1, v_2, \ldots, v_n),$$

kde $(v_1, v_2, \ldots, v_n)$ sú súradnice vektora $\mathbf{v}$ v báze $\mathcal{B}$. Overiť platnosť podmienok a), b), c) z definície 4.8 pre takto definované zobrazenie φ je triviálna úloha. ■

***Poznámka* 4.12.** *Ak sú dva priestory izomorfné, môže existovať viac izomorfných zobrazení medzi nimi. Každá báza vektorového priestoru $V(\mathcal{P})$ predstavuje iné zobrazenie, pretože súradnice vektora sú vzhľadom na rôzne bázy vždy iné n-tice.*

4.5 Aplikácie

Lineárny kód

Vektorové priestory a podpriestory nad konečnými poľami majú dôležité aplikácie v teórii samoopravných a chyby objavujúcich kódov.

Majme abecedu $A = \{a_1, a_2, \ldots, a_q\}$, ktorej n-znakové slová chceme použiť na prenos alebo uloženie údajov, pričom požadujeme, aby sme boli schopní zistiť, či pri prenose alebo uložení nastala chyba.

Všetky n-znakové slová môžeme považovať za prvky karteziánskeho súčinu A^n. Zabezpečiť sa proti chybám možno len tak, že pre naše údaje nepoužijeme všetky slová z A^n, ale len ich podmnožinu $\mathcal{K} \subseteq A^n$. Podmnožinu $\mathcal{K}$ nazveme **kódom**, slová z množiny $\mathcal{K}$ nazveme kódovými slovami, slová z $A^n - \mathcal{K}$ nazveme nekódovými slovami. Ak prijmeme kódové slovo, predpokladáme, že nenastala chyba, ak prijmeme nekódové slovo, vieme s určitosťou, že chyba pri prenose nastala.

Veľmi známym príkladom práve spomenutého prístupu je 8-bitový kód s kontrolou parity, ktorý používa len 8-bitové slová s párnym počtom jednotkových bitov. Pri prijatí slova s nepárnym počtom jednotkových bitov je detekovaná chyba.

Majme abecedu $A = \{a_1, a_2, \ldots, a_q\}$, kde q je prvočíslo alebo $q = p^m$, kde p je prvočíslo. Potom možno na množine A zaviesť operácie sčítania a násobenia tak, aby A s týmito operáciami bolo konečné pole. Na množinu všetkých n-znakových slov A^n sa možno dívať ako na aritmetický vektorový priestor $V_n(A)$ nad konečným poľom A (pozri poznámku 4.1 na str. 80).

Veľmi široké uplatnenie našiel tzv. **lineárny** (n, k) **kód**, ktorý je definovaný ako k-dimenzionálny podpriestor $\mathcal{K}$ aritmetického priestoru $V_n(A)$.

Lineárny (n, k)-kód ako k-dimenzionálny podpriestor priestoru A^n musí mať k-prvkovú bázu $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\}$. Potom každé kódové slovo $\mathbf{a} \in A^n$ má jednoznačné vyjadrenie

$$\mathbf{a} = a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_k\mathbf{b}_k, \tag{4.29}$$

kde $a_1, a_2, \ldots, a_n$ sú súradnice vektora $\mathbf{a}$ v báze $\mathcal{B}$. Ak $|A| = q$, potom na mieste každého a_i môže stáť q rôznych čísel, z čoho vyplýva, že existuje q^k rôznych k-tic $a_1, a_2, \ldots, a_k$, dosadením ktorých do (4.29) dostaneme q^k rôznych kódových slov kódu $\mathcal{K}$. Lineárny (n, k)-kód má teda q^k slov.

Lineárny (n, k) kód môžu charakterizovať dva matice. Prvou z nich je matica

$$\mathbf{G} = \begin{bmatrix} \mathbf{b}_1^T \\ \mathbf{b}_2^T \\ \ldots \\ \mathbf{b}_k^T \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{k1} & b_{k2} & \ldots & b_{kn} \end{bmatrix} \tag{4.30}$$

typu $(k \times n)$, ktorá sa nazýva **generujúca matica kódu $\mathcal{K}$.**

Druhou možnosťou charakterizácie lineárneho (n, k) kódu je tzv. **kontrolná matica H** typu $((n - k) \times n)$ s hodnosťou $n - k$, pre ktorú platí

$$\mathbf{x} \in \mathcal{K} \quad \text{práve vtedy, keď} \quad \mathbf{H}.\mathbf{x} = \mathbf{o}, \tag{4.31}$$

kde $\mathbf{o}$ je nulový vektor priestoru $V_n(A)$.

Dá sa ukázať, že matica $\mathbf{H}$ typu $((n - k) \times n)$ je kontrolnou maticou kódu $\mathcal{K}$ práve vtedy, keď

$$\dim(\mathbf{H}) = (n - k) \quad \text{a} \quad \mathbf{G}.\mathbf{H}^T = \mathbf{O}_{k\times(n-k)}, \tag{4.32}$$

kde $\mathbf{O}_{k\times(n-k)}$ je nulová matica typu $(k \times (n - k))$.

Pomocu algebraických vlastností matíc $\mathbf{G}$ a $\mathbf{H}$ možno študovať vlastnosti kódu $\mathcal{K}$ a možno tak definovať kódy, ktoré nielenže detekujú istý predom daný počet chýb, ale dokážu niekoľko chýb aj opraviť za predpokladu, že ich počet nepresiahol dovolené číslo. Takéto kódy sa volajú samoopravné kódy.

Cvičenia

1. Dokážte, že množina $\mathbb{C} = \{(a+ib, c+id) \mid a, b, c, d \in \mathbb{R}\}$ spolu s operáciami sčítania dvojíc a násobenia dvojice skalárom, tvorí vektorový priestor nad poľom reálnych čísel.

2. Zistite či množina $\mathbb{R}_+ = \{x \in \mathbb{R}; x > 0\}$ vzhľadom na operácie

$$\mathbf{x} \oplus \mathbf{y} = \mathbf{xy},\ c \odot \mathbf{x} = \mathbf{x}^c,\ \mathbf{x}, \mathbf{y} \in \mathbb{R}_+,\ c \in \mathbb{R}$$

   tvorí vektorový priestor nad poľom reálnych čísel.

3. Zistite či daná množina M tvorí vektorový podpriestor vektorového priestoru $V_2(\mathbb{R})$ vzhľadom na štandardné operácie sčítania usporiadaných dvojíc a násobenie usporiadanej dvojice skalárom:

   a) $M = \{(x, y) \in V_2(\mathbb{R}) \mid x \geq 0, y \geq 0\}$,
   b) $M = \{(x, y) \in V_2(\mathbb{R}) \mid x = y\}$,
   c) $M = \{(x, y) \in V_2(\mathbb{R}) \mid xy \geq 0\}$,
   d) $M = \{(x, y) \in V_2(\mathbb{R}) \mid xy = 0\}$.

3. Uveďte všetky vektory, ktoré generujú podpriestor $[(1, 2, 1), (2, 1, 2)]$ vektorového priestoru $V_3(\mathbb{Z}_3)$.

4. Nech $\mathcal{L} = [(4, 3, 2, 1), (1, 2, 3, 4), (1, 1, 1, 0)]$ je podpriestor vektorového priestoru $V_4(\mathbb{Z}_5)$. Patrí vektor $(4, 4, 4, 4)$ do $\mathcal{L}$?

5. Nech vektory $\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{u}$ vektorového priestoru $V(\mathcal{P})$ sú lineárne nezávislé. Zistite či sú lineárne závislé alebo lineárne nezávislé vektory:

   a) $\mathbf{x} + \mathbf{y},\ \mathbf{y} + \mathbf{z},\ \mathbf{z} + \mathbf{u},\ \mathbf{u} + \mathbf{x}$,
   b) $\mathbf{x} + \mathbf{y} + \mathbf{z},\ \mathbf{y} + \mathbf{z} + \mathbf{u},\ \mathbf{z} + \mathbf{u} + \mathbf{x},\ \mathbf{u} + \mathbf{x} + \mathbf{y}$,
   c) $\mathbf{x} + \mathbf{y} + \mathbf{z} + \mathbf{u},\ \mathbf{x} - \mathbf{y} + \mathbf{z} + \mathbf{u},\ \mathbf{x} + \mathbf{y} + \mathbf{z} - \mathbf{u},\ \mathbf{x} - \mathbf{y} + \mathbf{z} - \mathbf{u}$.

6. Pre aké reálne číslo a budú vektory $(2, -1, 3)$, $(4, a, -5)$, $(-3, 2, 4)$ lineárne nezávislé?

7. Určte lineárnu nezávislosť, resp. lineárnu závislosť pre:

   a) usporiadané trojice reálnych čísel $(1, 0, 2), (2, 0, 1), (1, 2, 0)$,

b) usporiadané štvorice reálnych čísel $(-1,-1,1,1)$, $(1,-1,1,-1)$, $(-1,1,1,-1)$, $(1,1,1,1)$,

c) funkcie $f(x) = cos2x, g(x) = sin^2x, h(x) = 13$,

d) polynómy 1, $1+x$, $1+x^2$, $1+x^3$.

8. Nájdite nejakú bázu a určte dimenziu podpriestoru $\mathcal{M}$ vektorového priestoru $V_n(\mathbb{R})$, keď $\mathcal{M} = \{(x_1, x_2, \ldots, x_n) \in V_n(\mathbb{R}) \mid x_1 + x_2 + \cdots + x_n = 0\}$.

9. Nájdite bázu a určte dimenziu lineárneho obalu množiny

   a) $M_1 = \{(1,2,3), (1,1,0), (0,1,1), (1,1,1), (1,0,0)\}$,

   b) $M_2 = \{1+x, 1-x, 1+x^2, 1-x^2, 1+x^3, 1-x^3\}$,

   c) $M_3 = \{(1,2,3,0), (3,4,1,2)\}$

   vo vektorovom priestore a) $V_3(\mathbb{R})$, b) polynómov nanajvýš tretieho stupňa, c) $V_4(\mathbb{Z}_5)$.

10. Vo vektorovom priestore polynómov nanajvýš tretieho stupňa nad poľom reálnych čísel nájdite súradnice polynómu $p(x) = 2x^3 - 3x^2 + 4$ v bázach $\mathcal{B}_1 = \{1, x+2, (x+2)^2, (x+2)^3\}$, $\mathcal{B}_2 = \{1, 1-x, (1-x)^2, (1-x)^3\}$.

11. Dokážte tvrdenia vyslovené v poznámke 4.5.

12. Dá sa z množiny $M = \{(3,3,8), (3,2,1), (2,4,6), (5,4,13), (1,3,3)\}$ vybrať taký vektor $\mathbf{x}$, aby vektor $\mathbf{v} = (3,1,2)$ mal v báze $\mathcal{B} = \{(1,2,3), \mathbf{x}, (2,1,5)\}$ súradnice $(-7,4,3)_{\mathcal{B}}$?

13. Nájdite súradnice vektora $\mathbf{v}$ v báze $\mathcal{B}$ vektorového priestoru $V_3(\mathbb{R})$:

   a) $\mathbf{v} = (2,1,1), \mathcal{B} = \{(2,7,3), (3,9,4), (1,5,3)\}$

   b) $\mathbf{v} = (2,1,1), \mathcal{B} = \{(1,0,1), (1,0,0), (1,1,1)\}$

14. Nech $Q = \{a + b\sqrt{2} \mid a, b \in Q\}$ vzhľadom na operácie štandardné sčítanie a násobenie skalárom tvorí vektorový priestor nad poľom racionálnych čísel, ktorý označíme $Q(\sqrt{2})$. Dokážte, že vektorové priestory $Q(\sqrt{2})$ a $V_2(Q)$ sú izomorfné.

Kapitola 5

Matice a determinanty

5.1 Matice

V lineárnej algebre zohráva významnú úlohu teória matíc. Výsledky, ktoré v tejto kapitole odvodíme, môžeme aplikovať pri riešení sústav lineárnych rovníc a následne aj pri ďalšom štúdiu vektorových priestorov. V úvode kapitoly je nutné uviesť základné pojmy.

Definícia 5.1. Nech $\mathcal{P} = (P, +, \cdot)$ je pole. Obdĺžnikovú schému $m \cdot n$ prvkov poľa $\mathcal{P}$ usporiadanú do $m \geq 1$ riadkov a $n \geq 1$ stĺpcov nazývame **maticou** typu $m \times n$ nad poľom $\mathcal{P}$.

Matice budeme označovať veľkými tučnými latinskými písmenami $\mathbf{A}, \mathbf{B}, \mathbf{C}, \ldots$ Symbolmi tvaru $a_{ij}, b_{ij}, \ldots$ budeme označovať tie prvky matice, ktoré sa nachádzajú v i-tom riadku a j-tom stĺpci matice. Maticu $\mathbf{A}$ typu $m \times n$ s prvkami a_{ij} budeme zapisovať

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} . \tag{5.1}$$

Používajú sa tiež skrátené zápisy matice:

$$\mathbf{A} = \Big(a_{ij}\Big)_{i=1,2,\ldots,m}^{j=1,2,\ldots,n} = \big(a_{ij}\big)_{m,n} = \big(a_{ij}\big)_{m\times n} = \big(a_{ij}\big)_{mn} = \big(a_{ij}\big) .$$

Prvky matice **A** podľa definície sú prvkami poľa $\mathcal{P}$. Vo všeobecnosti môžu byť prvkami ľubovoľnej algebraickej štruktúry. My sa obmedzíme na prípady, keď matice budú definované nad poliami. Najčastejšie budú prvky matíc z poľa reálnych čísel, vtedy hovoríme o **reálnych maticiach**. V prípade, že matica bude definovaná nad poľom komplexných čísel, hovoríme o **komplexných maticiach**. V informatike sa často používajú matice nad konečnými poľami typu $\mathbb{Z}_p$ alebo $GF(p^k)$.

Množinu všetkých matíc typu $m \times n$ nad poľom $\mathcal{P}$ budeme označovať $\mathcal{M}_{m\times n}(P)$, prípadne len $\mathcal{M}_{m\times n}$, keď bude z kontextu jasné, o aké pole ide.

Príklad 5.1.

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

je matica typu 2×4, ktorej prvky sú z poľa reálnych čísel.

Na maticu typu $m \times n$ nad poľom $\mathcal{P}$ sa môžeme pozerať z rôznych uhlov. Ak $m = n = 1$, tak dostávame maticu typu 1×1 – maticu tvorí jediný prvok poľa $\mathcal{P}$. V prípade, že $m = 1$, dostaneme maticu typu $1 \times n$, ktorú tvorí usporiadaná n-tica prvkov poľa $\mathcal{P}$, ináč nazývaná aj **riadkový vektor** . Rovnako maticu typu $m \times 1$ nazývame aj **stĺpcový vektor** . Takéto matice sú prvkami vektorového priestoru $V_n(\mathcal{P})$, resp. $V_m(\mathcal{P})$. Niektoré ďalšie špeciálne typy matíc uvedieme v nasledujúcej definícii.

Definícia 5.2. Nech **A** je matica definovaná v (5.1).

a) Ak $m = n$, hovoríme, že **A** je **štvorcová matica** stupňa n (resp. rádu n).

b) Ak $a_{ij} = 0$ pre všetky $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, hovoríme, že **A** je **nulová matica** a značíme ju $\mathbf{O}_{m\times n}$, $\mathbf{O}_{m,n}$, $\mathbf{O}_{mn}$, alebo len **O**.

c) Ak v štvorcovej matici **A** rádu n je $a_{ij} = 0$ pre všetky $i \neq j$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$, hovoríme, že **A** je **diagonálna matica**.

d) Ak v štvorcovej matici **A** rádu n je $a_{ii} = 1$ a $a_{ij} = 0$ pre všetky $i \neq j$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$, hovoríme, že **A** je **jednotková matica** a značíme ju $\mathbf{E}_n$ alebo len **E**.

e) Ak v štvorcovej matici **A** rádu n je $a_{ij} = 0$ pre všetky $i > j$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$, hovoríme, že **A** je **horná trojuholníková matica**. Ak $a_{ij} = 0$ pre všetky $i < j$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$, hovoríme, že **A** je **dolná trojuholníková matica**.

f) Ak v štvorcovej matici $\mathbf{A}$ rádu n je $a_{ij} = a_{ji}$ pre všetky $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$, hovoríme, že $\mathbf{A}$ je **symetrická matica**.
Ak $a_{ij} = -a_{ji}$ pre všetky $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$, hovoríme, že $\mathbf{A}$ je **antisymetrická matica**. (V antisymetrickej matici musí byť $a_{ii} = 0$ pre všetky $i = 1, 2, \ldots, n$.)

g) Ak z danej matice $\mathbf{A}$ vytvoríme inú maticu $\mathbf{B}$ tak, že z matice $\mathbf{A}$ vylúčime niektoré riadky a niektoré stĺpce, hovoríme, že matica $\mathbf{B}$ je podmatica matice $\mathbf{A}$.

h) Ak rozdelíme maticu $\mathbf{A}$ na niekoľko podmatíc tak, že spolu tvoria celú maticu, hovoríme o **blokovej matici** a jednotlivé podmatice nazývame bloky.

Napr. majme maticu

$$\mathbf{A} = \left(\begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{32} & a_{43} & a_{44} \end{array}\right) \tag{5.2}$$

Zvislými a vodorovnými čiarami sme maticu $\mathbf{A}$ rozdelili na bloky

$$\mathbf{A} = \begin{pmatrix} \mathbf{A_{11}} & \mathbf{A_{12}} \\ \mathbf{A_{21}} & \mathbf{A_{22}} \end{pmatrix}, \tag{5.3}$$

pričom jednotlivé bloky sú

$$\mathbf{A_{11}} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \mathbf{A_{12}} = \begin{pmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{pmatrix}$$

$$\mathbf{A_{21}} = \begin{pmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{pmatrix} \quad \mathbf{A_{22}} = \begin{pmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{pmatrix}$$

Príklad 5.2. Pre názornosť uvedieme príklady niektorých špeciálnych typov matíc uvedených v definícii 5.2:

$$\mathbf{A} = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

Matice $\mathbf{A}$ aj $\mathbf{B}$ sú diagonálne matice stupňa 3.

$$\mathbf{C} = \begin{pmatrix} 6 & 1 & 3 & 2 \\ 0 & -1 & 0 & 4 \\ 0 & 0 & 5 & 3 \end{pmatrix} \qquad \mathbf{D} = \begin{pmatrix} -2 & 0 & 0 \\ 8 & 7 & 0 \\ 2 & 2 & 5 \end{pmatrix}$$

Matica $\mathbf{C}$ je horná trojuholníková matica typu 3×4 a matica $\mathbf{D}$ je dolná trojuholníková matica typu 3×3.

$$\mathbf{F} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \\ 3 & 1 & 4 \end{pmatrix} \qquad \mathbf{H} = \begin{pmatrix} 0 & 2 & 3 \\ -2 & 0 & -1 \\ -3 & 1 & 0 \end{pmatrix}$$

Matica $\mathbf{F}$ je symetrická a matica $\mathbf{H}$ antisymetrická matica stupňa 3.

Definícia 5.3. Budeme hovoriť, že **matica** $\mathbf{A} = \left(a_{ij}\right)_{m\times n}$ **sa rovná matici** $\mathbf{B} = \left(b_{ij}\right)_{p\times q}$, ak sú rovnakého typu, t. j. $m = p$ a $n = q$, a pre všetky $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$ je $a_{ij} = b_{ij}$. Píšeme $\mathbf{A} = \mathbf{B}$.

Zavedieme operácie na maticiach, ktoré už poznáme z kapitoly vektorové priestory – sčítanie matíc a násobenie matice skalárom.

Definícia 5.4. Nech $\mathbf{A} = \left(a_{ij}\right)$, $\mathbf{B} = \left(b_{ij}\right)$ sú matice rovnakého typu $m \times n$. **Súčet matíc A a matice B** je matica $\mathbf{C} = \left(c_{ij}\right)$ typu $m \times n$ s prvkami

$$c_{ij} = a_{ij} + c_{ij}. \tag{5.4}$$

Označujeme $\mathbf{C} = \mathbf{A} + \mathbf{B}$.

Skalárny c-násobok matice $\mathbf{A} = \left(a_{ij}\right)$ typu $m \times n$ je matica $\mathbf{C} = \left(c_{ij}\right)$ typu $m \times n$ s prvkami

$$c_{ij} = c \cdot a_{ij}, \tag{5.5}$$

pričom $c \in P$. Označujeme $\mathbf{C} = c \cdot \mathbf{A}$

Poznámka* 5.1.** *V prípade, že $c = -1$, píšeme $\mathbf{B} = -\mathbf{A}$ a maticu $-\mathbf{A}$ nazývame* ***opačnou maticou *k matici $\mathbf{A}$.*

Príklad 5.3. Vypočítajme čomu sa rovná $2\mathbf{A} - \mathbf{B}$, keď

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & 1 \end{pmatrix}$$

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

Príklad 5.4. Rýchlo nahliadneme, že množina všetkých matíc typu $m \times n$ nad poľom $\mathbb{R}$ spolu s práve definovanými operáciami sčítania matíc a násobenia matice skalárom tvorí vektorový priestor.
$\big(\mathcal{M}_{m\times n}(\mathbb{R}), +\big)$ je komutatívna grupa. Zrejme

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

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

keďže sčítanie reálnych čísel je komutatívne i asociatívne. Neutrálnym prvkom je nulová matica $\mathbf{O}_{m\times n}$ a opačným prvkom k prvku $\mathbf{A}$ je $-\mathbf{A}$.
Potrebné je ešte overiť platnosť vzťahov 4.2 – 4.5 z definície vektorového priestoru, ktoré pre ľubovoľné $r, s \in \mathbb{R}$ a pre ľubovoľné matice $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m\times n}$ vyzerajú

$$t \cdot (s \cdot \mathbf{A}) = (t \cdot s) \cdot \mathbf{A}$$

$$(t + s) \cdot \mathbf{A} = t \cdot \mathbf{A} + s \cdot \mathbf{A}$$

$$t \cdot (\mathbf{A} + \mathbf{B}) = t \cdot \mathbf{A} + t \cdot \mathbf{B}$$

$$1 \cdot \mathbf{A} = \mathbf{A}$$

Rozpísaním a porovnaním ľavých a pravých strán rovností sa o tom presvedčí čitateľ sám.

***Poznámka* 5.2.** *V príklade 5.4 sme ukázali, že všetky matice typu $m \times n$ tvoria vektorový priestor nad poľom reálnych čísel. Dimenzia vektorového priestoru je $m \cdot n$ a bázou $\mathcal{B}_0$ je množina matíc $\mathbf{E}_{pq} = \big(e_{ij}^{pq}\big)$, ktorá je definovaná pre $p = 1, \ldots, m,\ q = 1, \ldots, n$ takto*

$$e_{ij}^{pq} = \begin{cases} 1, & \text{pre } i = p \text{ a } j = q \\ 0 & \text{inak} \end{cases} \tag{5.6}$$

Napr. pre $m = 2$ a $n = 3$

$$\mathbf{E}_{13} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Definícia 5.5. Nech $\mathbf{A} = \left(a_{ij}\right)$ je matica typu $m \times n$, $\mathbf{B} = \left(b_{ij}\right)$ je matica typu $n \times p$. **Súčinom matíc A a B** rozumieme maticu $\mathbf{C} = \left(c_{ij}\right)$ typu $m \times p$ s prvkami

$$c_{ij} = \sum_{k=1}^{n} a_{ik}.b_{kj} \tag{5.7}$$

pre všetky $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, p$. Značíme $\mathbf{C} = \mathbf{A} \cdot \mathbf{B}$.

Príklad 5.5. Nech

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 2 & 1 \end{pmatrix}$$

$$\mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 4 & 4 \end{pmatrix}$$

***Poznámka* 5.3.** *Násobenie matíc* $\mathbf{A}, \mathbf{B}$ *(v prípade, že súčin vôbec existuje) nie je vo všeobecnosti komutatívne! Napr.*

$$\mathbf{A} = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$$

$$\mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 0 \\ 2 & 3 \end{pmatrix}$$

$$\mathbf{B} \cdot \mathbf{A} = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & -1 \end{pmatrix}$$

V nasledujúcej vete uvedieme v ucelenom tvare vlastnosti operácií, ktoré sme na maticiach definovali.

Veta 5.1. *Nech* $\mathbf{A}_{m\times n}$, $\mathbf{B}_{n\times p}$, $\mathbf{C}_{n\times p}$, $\mathbf{D}_{p\times r}$ *sú matice nad poľom* $\mathcal{P}$, $t, s, \in P$. *Potom platí:*

a) $\mathbf{A}(\mathbf{BD}) = (\mathbf{AB})\mathbf{D}$ *(asociatívnosť násobenia)*

b) $(\mathbf{B}+\mathbf{C})\mathbf{D} = \mathbf{BD}+\mathbf{CD}$ *(distributívnosť násobenia sprava)*

c) $\mathbf{A}(\mathbf{B}+\mathbf{C}) = \mathbf{AB}+\mathbf{AC}$ *(distributívnosť násobenia zľava)*

d) $t(s\mathbf{A}) = (ts)\mathbf{A}$

e) $\mathbf{E}_m\mathbf{A}_{m\times n} = \mathbf{A}_{m\times n} = \mathbf{A}_{m\times n}\mathbf{E}_n$

f) $\mathbf{O}_{m\times n} + \mathbf{A}_{m\times n} = \mathbf{A}_{m\times n}$

g) $\mathbf{O}_{m\times n}\mathbf{B}_{n\times p} = \mathbf{O}_{m\times n}$

h) $\mathbf{B}_{n\times p}\mathbf{O}_{p\times r} = \mathbf{O}_{n\times r}$

DÔKAZ:
Platnosť každej z uvedených rovností sa overí rozpísaním pravej a ľavej strany využijúc definícií operácií matíc a rovnosti matíc. Dokážeme asociatívnosť násobenia matíc. Najskôr ukážeme, že matice na oboch stranách sú rovnakého typu. Označme $\mathbf{F} = \mathbf{AB}$ – je to matica typu $m \times p$. $\mathbf{FD} = \mathbf{G}$ je matica typu $m \times r$. Na druhej strane označme $\mathbf{P} = \mathbf{BD}$, čo je matica typu $n \times r$ a nakoniec $\mathbf{Q} = \mathbf{AP}$, ktorá je typu $m\times r$. Matice $\mathbf{G}$ a $\mathbf{Q}$ sú rovnakého typu. Nech $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, $\mathbf{D} = (d_{ij})$, $\mathbf{F} = (f_{it})$, $\mathbf{G} = (g_{iv})$, $\mathbf{P} = (p_{sv})$, $\mathbf{Q} = (q_{iv})$. Potom

$$q_{iv} = \sum_{\beta=1}^{n} a_{i\beta}p_{\beta v} = \sum_{\beta=1}^{n} a_{i\beta}\Big(\sum_{\alpha=1}^{p} b_{\beta\alpha}d_{\alpha v}\Big) = \sum_{\beta=1}^{n}\sum_{\alpha=1}^{p} a_{i\beta}b_{\beta\alpha}d_{\alpha v}$$

$$g_{iv} = \sum_{\lambda=1}^{p} f_{i\lambda}d_{\lambda v} = \sum_{\lambda=1}^{p} \Big(\sum_{\delta=1}^{n} a_{i\delta}b_{\delta\lambda}\Big)d_{\lambda v} = \sum_{\delta=1}^{n}\sum_{\lambda=1}^{p} a_{i\delta}b_{\delta\lambda}d_{\lambda v}$$

Porovnaním dostaneme $q_{iv} = g_{iv}$ pre $i = 1, 2, \ldots, m$ a $v = 1, 2, \ldots, r$. ■

***Poznámka* 5.4.** *Vo vete 5.1 sme neuviedli komutatívnosť a asociatívnosť sčítania matíc. Tieto vlastnosti sú evidentné.*

Definícia 5.6. Nech $\mathbf{A}$ je štvorcová matica stupňa n. Potom **k-tou mocninou matice $\mathbf{A}$** rozumieme štvorcovú maticu stupňa k, ktorú označujeme $\mathbf{A}^k$ a definujeme

$$\mathbf{A}^k = \begin{cases} \mathbf{E}_n, & k = 0 \\ \mathbf{A}^{k-1}\mathbf{A} & k = 1, 2, \ldots \end{cases}$$

Príklad 5.6. Vypočítajme štvrtú mocninu matice $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$.

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

$$\mathbf{A}^3 = \mathbf{A^2} \cdot \mathbf{A} = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{A}^4 = \mathbf{A^3} \cdot \mathbf{A} = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix}$$

Definícia 5.7. Nech matica $\mathbf{A} = (a_{ij})$ je typu $m \times n$. **Transponovanou maticou** k matici $\mathbf{A}$ nazývame maticu $\mathbf{A}^T = (a_{ij}^T)$ typu $n \times m$, pre prvky ktorej platí

$$a_{ij}^T = a_{ji}. \tag{5.8}$$

Veta 5.2. *Pre ľubovoľné matice* $\mathbf{A}_{m\times n}$, $\mathbf{B}_{m\times n}$, $\mathbf{C}_{n\times p}$ *a pre ľubovoľné* $c \in P$ *platí*

a) $(\mathbf{A}^T)^T = \mathbf{A}$,

b) $(\mathbf{A} + \mathbf{B})^T = \mathbf{A}^T + \mathbf{B}^T$,

c) $(c \cdot \mathbf{A})^T = c \cdot \mathbf{A}^T$,

d) $(\mathbf{BC})^T = \mathbf{C}^T\mathbf{B}^T$.

Dôkaz:
Prvé tri tvrdenia sú zrejmé. Dokážeme štvrté. Označme $\mathbf{F} = \mathbf{B}\cdot\mathbf{C}$, $\mathbf{H} = \mathbf{C}^T\cdot\mathbf{B}^T$, $\mathbf{G} = \mathbf{F}^T$. Najskôr porovnajme typy matíc $\mathbf{F}$ a $\mathbf{H}$.
$\mathbf{F}$ je typu $m \times p$, potom $\mathbf{G}$ je typu $p \times m$. Matica $\mathbf{H} = \mathbf{C}^T \cdot \mathbf{B}^T$ je tiež typu $p \times m$. Pre ľubovoľné $i = 1, 2, \ldots, p$ a $j = 1, 2, \ldots, m$

$$g_{ij} = f_{ij}^T = f_{ji} = \sum_{k=1}^{n} b_{jk}c_{ki} = \sum_{k=1}^{n} b_{kj}^T c_{ik}^T = \sum_{k=1}^{n} c_{ik}^T b_{kj}^T = h_{ij}$$

■

Definícia 5.8. Nech $\mathcal{P}$ je podpoľom poľa reálnych čísel. Nech $V_n(\mathcal{P})$ je vektorový priestor nad poľom $\mathcal{P}$ a nech sú dané vektory $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in V_n(\mathcal{P})$, $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in V_n(\mathcal{P})$. **Skalárny súčin** $\mathbf{u}.\mathbf{v}$ vektorov $\mathbf{u}$, $\mathbf{v}$ definujeme predpisom

$$\mathbf{u}.\mathbf{v} = (u_1v_1 + u_2v_2 + \cdots + u_nv_n) = \sum_{i=1}^{n} u_iv_i. \tag{5.9}$$

Pomocou skalárneho súčinu riadkových vektorov matice $\mathbf{A}$ a stĺpcových vektorov matice $\mathbf{B}$ možno výhodne vyjadriť prvky ich maticového súčinu. Uvažujme najprv jednoduchý prípad, kedy je matica $\mathbf{A}$ typu $n \times 1$ a matica $\mathbf{B}$ typu $1 \times n$. V úvode kapitoly sme nazvali maticou typu $n \times 1$ stĺpcový vektor, ktorý má tvar

$$\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix}$$

Potom vektor $\mathbf{v}^T$ je maticou typu $1 \times n$

$$\mathbf{v}^T = \big(v_1, v_2, \ldots, v_n\big).$$

Nech $\mathbf{u}, \mathbf{v}$ sú dva vektory aritmetického vektorového priestoru $V_n(\mathcal{P})$, $\mathbf{u}^T = (u_1, u_2, \ldots, u_n)$, $\mathbf{v}^T = (v_1, v_2, \ldots, v_n)$ oba uvažované ako jednostĺpcové matice. Potom pre ich maticový súčin platí

$$\mathbf{u}^T.\mathbf{v} = \big(u_1, \quad u_2, \quad \ldots, \quad u_n\big)_{1\times n} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}_{n\times 1} = \left(\sum_{i=1}^{n} u_i v_i\right)_{1\times 1} \tag{5.10}$$

Výsledkom je matica typu 1×1 s jediným prvkom, ktorého hodnota je rovná skalárnemu súčinu vektorov $\mathbf{u}$, $\mathbf{v}$.

V definícii 5.2 pod písmenom i) sme hovorili o rozdelení matice $\mathbf{A}$ na bloky. Často sa ukazuje vhodným nasledujúce rozdelenie:

$$\mathbf{A} = \left(\begin{array}{c|c|c|c|c} a_{11} & a_{12} & \ldots & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & \ldots & a_{mn} \end{array}\right) = \big(\mathbf{s_1} \quad \mathbf{s_2} \quad \ldots \quad \ldots \quad \mathbf{s_n},\big)$$

kde $\mathbf{s_j} = (a_{1j}, a_{2j}, \ldots, a_{mj})^T$ je j-ty stĺpec matice $\mathbf{A}$.

$$\mathbf{A} = \left(\begin{array}{ccccc} a_{11} & a_{12} & \ldots & \ldots & a_{1n} \\ \hline a_{21} & a_{22} & \ldots & \ldots & a_{2n} \\ \hline \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \hline a_{m1} & a_{m2} & \ldots & \ldots & a_{mn} \end{array}\right) = \begin{pmatrix} \mathbf{r_1^T} \\ \mathbf{r_2^T} \\ \ldots \\ \ldots \\ \mathbf{r_m^T} \end{pmatrix},$$

kde $\mathbf{r_i^T} = \big(a_{i1}, a_{i2}, \ldots, a_{in}\big)$ je i-ty riadok matice $\mathbf{A}$

Nech $\mathbf{A} = \big(a_{ij}\big)_{m\times n}$ je matica typu $m \times n$, $\mathbf{B} = \big(b_{ij}\big)_{n\times p}$ matica typu $n \times p$, $\mathbf{r_i^T}$ pre $i = 1, 2, \ldots, m$ riadkové vektory matice $\mathbf{A}$, $\mathbf{s_i}$ pre $j = 1, 2, \ldots, p$ stĺpcové vektory matice $\mathbf{B}$. Potom súčin matíc $\mathbf{A} \cdot \mathbf{B}$ schematicky vyjadríme

$$\mathbf{A}.\mathbf{B} = \begin{pmatrix} \mathbf{r_1^T} \\ \mathbf{r_2^T} \\ \ldots \\ \mathbf{r_m^T} \end{pmatrix} . \begin{pmatrix} \mathbf{s_1} & \mathbf{s_2} & \ldots & \mathbf{s_p} \end{pmatrix} = \begin{pmatrix} \mathbf{r_1^T s_1} & \mathbf{r_1^T s_2} & \ldots & \mathbf{r_1^T s_p} \\ \mathbf{r_2^T s_1} & \mathbf{r_2^T s_2} & \ldots & \mathbf{r_2^T s_p} \\ \ldots & \ldots & \ldots & \ldots \\ \mathbf{r_m^T s_1} & \mathbf{r_m^T s_2} & \ldots & \mathbf{r_m^T s_p} \end{pmatrix}$$

5.2 Determinant matice

Skôr ako pristúpime k definícii determinantu matice, pripomenieme si pojem permutácie a zavedieme nevyhnutné pojmy súvisiace s permutáciou. Pre naše potreby sa budeme zaoberať permutáciou n-prvkovej množiny $\{1, 2, \ldots, n\}$.

Definícia 5.9. Nech $n \in \mathbb{N}$ je prirodzené číslo. Permutácia množiny $\langle n\rangle = \{1, 2, \ldots, n\}$ je bijektívne zobrazenie π množiny $\langle n\rangle$ na seba.

Permutácia je teda zobrazenie

$$\pi : \langle n\rangle \to \langle n\rangle.$$

Obraz prvku $i \in \{1, 2, \ldots, n\}$ v permutácii π budeme značiť $\pi(i)$. Permutáciu π zapisujeme

$$\pi = \big\{(i, \pi(i)) \mid i \in \langle n\rangle\big\} = \big\{(i, \pi(i)) \mid i \in \{1, 2, \ldots, n\}\big\}.$$

Častejšie

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}$$

alebo len

$$\pi = \big(\pi(1) \quad \pi(2) \quad \pi(3) \quad \ldots \quad \pi(n)\big)$$

Množinu všetkých permutácií množiny $\langle n\rangle$ budeme označovať Π.

Definícia 5.10. Ak pre $i < j,\ \ i, j \in \{1, 2, \ldots, n\}$ je $\pi(i) > \pi(j)$, hovoríme, že dvojica (i, j) predstavuje **inverziu v permutácii** π.

Znamienko permutácie π je číslo

$$\text{zn } \pi = (-1)^k,$$

kde k je počet inverzií v permutácii π. Ak má permutácia π párny počet inverzií, hovoríme, že π je **párna permutácia**. V opačnom prípade hovoríme, že π je **nepárna permutácia**.

Permutácia π je zobrazenie, takže dve permutácie je možné skladať a výsledné zobrazenie je zas permutácia. Ak na množine Π zadefinujeme binárnu operáciu skladanie permutácií $\circ$:

$$\forall\ \pi_1, \pi_2 \in \Pi \quad \forall\ i \in \langle n \rangle \qquad (\pi_1 \circ \pi_2)(i) = \pi_1(\pi_2(i)), \tag{5.11}$$

tak sa dá ukázať (urobte to!), že $(\Pi, \circ)$ je nekomutatívna grupa, Neutrálnym prvkom je **identická permutácia**

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

a symetrizačným prvkom pre danú permutáciu π je taká permutácia $\overline{\pi}$, pre ktorú platí

$$\pi \circ \overline{\pi} = \overline{\pi} \circ \pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}.$$

Permutáciu $\overline{\pi}$ nazývame tiež **inverzná permutácia** .

Zrejmé sú aj nasledujúce tvrdenia známe z kombinatoriky – a síce:

a) Počet všetkých permutácií je $n!$

b) Počet párnych permutácií je rovnaký ako počet nepárnych permutácií.

b) Vzájomne inverzné permutácie majú rovnaké znamienko.

Príklad 5.7. Uvažujme množinu $A = \{1, 2, 3\}$. Nájdime všetky permutácie tejto množiny, nájdime počty inverzií pre príslušné permutácie a zároveň aj ich znamienka.

Riešenie:
Množina A je trojprvková, počet všetkých permutácií bude $3! = 6$. Riešenie úlohy zo zadania uvedieme prehľadne v tabuľke:

Permutácia	*Počet inverzií*	*Znamienko permutácie*
(1 2 3)	0	$(-1)^0 = +1$
(2 1 3)	1	$(-1)^1 = -1$
(2 3 1)	2	$(-1)^2 = +1$
(3 1 2)	2	$(-1)^2 = +1$
(3 2 1)	3	$(-1)^3 = -1$
(1 3 2)	1	$(-1)^1 = -1$

Venujme sa podrobnejšie permutácii, ktorá sa nachádza v piatom riadku tabuľky:

$$\pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Inverziu tvoria dvojice $(1,2)$, $(1,3)$ a $(2,3)$, lebo $\pi_5(1) > \pi_5(2)$, $\pi_5(1) > \pi_5(3)$ a $\pi_5(2) > \pi_5(3)$. V tabuľke si tiež všimneme, že počet nepárnych a počet párnych permutácií je rovnaký a rovný 3 .

A teraz už vyslovíme definíciu determinantu matice.

Definícia 5.11. Determinantom danej štvorcovej matice $\mathbf{A} = (a_{ij})$ stupňa n nad číselným poľom nazývame číslo (prvok tohto poľa)

$$\det\mathbf{A} = \sum_{\pi\in\Pi} \text{zn } \pi . a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}, \tag{5.12}$$

kde Π je množina všetkých permutácií množiny $\{1, 2, \dots, n\}$.

Determinant matice $\mathbf{A}$ označujeme:

$$\det\mathbf{A} = |A| = |a_{ij}| = |a_{ij}|_{n,n} = |a_{ij}|_{n\times n} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

***Poznámka* 5.5.** *Definícia determinantu môže naoko pôsobiť nezrozumiteľne. Hovorí o tom, že determinant matice* $\mathbf{A}$ *je číslo, ktoré dostaneme ako súčet* $n!$ *sčítancov. Sčítance sú vybrané* n*-tice prvkov matice* $\mathbf{A}$ *také, že prvé indexy prvkov tvoria identickú permutáciu (vyberieme tak z každého riadku jeden prvok) a druhé indexy predstavujú nejakú permutáciu* π *množiny* $\{1, 2, \dots, n\}$ *(vyberieme tak z každého stĺpca jeden prvok). Ak je permutácia* π *párna, sčítancu priradíme znamienko* $+$*. V prípade, že permutácia* π *je nepárna, sčítancu priradíme znamienko* $-$*.*

Príklad 5.8. Daná je matica

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Vypočítajme det$\mathbf{A}$. Využijeme definíciu 5.11 a výpočty z príkladu 5.7. Pretože matica $\mathbf{A}$ je stupňa 3, výraz det$\mathbf{A}$ bude mať 6 sčítancov. Permutácie (2 1 3), (3 2 1), (1 3 2) sú nepárne, budú sa v súčte vyskytovať so znamienkom $-$.

$$\det\mathbf{A} = a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}$$

Determinanty matíc tretieho stupňa môžeme počítať podľa schémy

$$\left|\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ & \searrow & \times \quad \times & & \swarrow \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ & \swarrow & \times \quad \times & & \searrow \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}\right|$$

Tento spôsob nazývame Sarusovo pravidlo : K matici pripíšeme vpravo ešte raz prvý a druhý stĺpec. Vynásobíme všetky trojice prvkov ležiacich na priamkach "juhovýchodného smeru" a pridáme k nim kladné znamienko. Potom vynásobíme všetky trojice prvkov ležiacich na priamkach "juhozápadného smeru" a priradíme im záporné znamienko. Nakoniec všetky trojice sčítame a dostaneme hodnotu determinantu matice.

Upozornenie: Sarusovým pravidlom je možné počítať iba determinanty matíc tretieho stupňa!

Príklad 5.9. Vypočítajme determinant matice

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

Matica $\mathbf{A}$ je tretieho stupňa, det$\mathbf{A}$ vypočítame Sarusovým pravidlom podľa schémy:

$$\left|\begin{array}{ccc|cc} 2 & 1 & 0 & 2 & 1 \\ 1 & 2 & 1 & 1 & 2 \\ 3 & 2 & 2 & 3 & 2 \end{array}\right| = 2\cdot 2\cdot 2 + 1\cdot 1\cdot 3 + 0\cdot 1\cdot 2 - 0\cdot 2\cdot 3 - 2\cdot 1\cdot 2 - 1\cdot 1\cdot 2 = 5$$

Ako sme uviedli, počítať determinanty matíc štvrtého a vyššieho stupňa pomocou Sarusovho pravidla nie je možné. Použiť na výpočet takýchto determinantov definíciu je zas nepraktické. V nasledujúcej časti ukážeme, ako sa vysporiadať s touto úlohou. Najskôr uvedieme vety, ktoré sú z praktického pohľadu pre výpočet determinantov užitočné.

Veta 5.3. *Nech* $\mathbf{A}$ *je štvorcová matica a* $\mathbf{A}^T$ *k nej transponovaná matica. Potom*

$$\det\mathbf{A} = \det\mathbf{A}^T$$

Dôkaz:
Z definície transponovanej matice platí $\mathbf{A}^T = \left(a_{ij}^T\right) = (a_{ji})$. Determinant je súčet $n!$ sčítancov súčinov n-tíc prvkov matice, pričom z každého riadku a každého stĺpca vyberieme práve po jednom prvku. Pri výpočte determinantu matice $\mathbf{A}^T$ pomocou definície zmeníme akurát "filozofiu" výberu prvkov matice. Stĺpcové indexy budú predstavovať identickú permutáciu množiny $\{1, 2, \ldots, n\}$ a riadkové indexy budú ich obrazmi v permutácii π. ■

Veta 5.4. *Nech matica* $\mathbf{B}$ *vznikla zo štvorcovej matice* $\mathbf{A}$ *vzájomnou výmenou* i*-teho a* j*-teho riadku. Potom*

$$\det\mathbf{B} = -\det\mathbf{A}$$

Dôkaz:
Aby sme dokázali tvrdenie vety, stačí si uvedomiť, že matica $\mathbf{A}$ i matica $\mathbf{B}$ sú rovnakého stupňa, čiže pri výpočte determinantov matíc vystupuje rovnaký počet sčítancov. Nech stĺpcové indexy prvkov pri výpočte $\det\mathbf{A}$ zodpovedajú permutácii π a stĺpcové indexy prvkov pri výpočte $\det\mathbf{B}$ zodpovedajú permutácii $\tilde{\pi}$.

Predpokladajme, že matica $\mathbf{B}$ vznikne z matice $\mathbf{A}$ vzájomnou výmenou i-teho a j-teho riadku, pre určitosť predpokladajme, že $i < j$. Pre prvky množiny $\{1, 2, \ldots, n\}$ platí $\tilde{\pi}(i) = \pi(j)$ a $\tilde{\pi}(j) = \pi(i)$, ostatné prvky zostanú nezmenené. Presun prvku $\pi(i)$ na miesto j znamená $j - i$ výmien susedných prvkov. Na presun prvku $\pi(j)$ na pozíciu i potrebujeme $j - i - 1$ výmien susedných prvkov. Aby vznikla z permutácie π permutácia $\tilde{\pi}$, potrebujeme celkove $2(j - i) - 1$ výmien, každá výmena znamená zmenu počtu inverzií o 1. Keďže $2(j - i) - 1$ je nepárne číslo, zn $\tilde{\pi} = -\text{zn}\ \pi$, čo znamená, že $\det\mathbf{B} = -\det\mathbf{A}$. ■

Veta 5.5. *Nech matica* $\mathbf{B}$ *vznikla zo štvorcovej matice* $\mathbf{A}$ *vynásobením jej* i*-teho riadku prvkom* $k \in P$*. Potom*

$$\det\mathbf{B} = k.\det\mathbf{A}. \tag{5.13}$$

Dôkaz:
V matici $\mathbf{B}$ má i-ty riadok tvar $k \cdot \mathbf{a}_i = (ka_{i1}, ka_{i2}, \ldots, ka_{in})$. Pri výpočte $\det\mathbf{B}$ v každom sčítanci sa vyskytuje konštanta k, teda platí tvrdenie vety. ■

Veta 5.6. *Ak má štvorcová matica* $\mathbf{A}$ *dva riadky rovnaké, potom*

$$\det\mathbf{A} = 0. \tag{5.14}$$

Dôkaz:
Nech v matici $\mathbf{A}$ sú rovnaké i-ty a j-ty riadok a nech matica $\mathbf{B}$ vznikne z matice $\mathbf{A}$ výmenou týchto dvoch riadkov. Podľa vety 5.4 platí $\det\mathbf{B} = -\det\mathbf{A}$ a zároveň platí $\det\mathbf{B} = \det\mathbf{A}$. Čo znamená, že $\det\mathbf{A} = 0$. ■

Veta 5.7. *Ak má štvorcová matica* $\mathbf{A}$ *jeden riadok nulový, potom*

$$\det\mathbf{A} = 0. \tag{5.15}$$

Dôkaz:
Nech nulovým riadkom matice $\mathbf{A}$ je i-ty riadok, ktorý môžeme napísať ako $\mathbf{a}_i = (0 \cdot a_{i1}, k \cdot a_{i2}, \ldots, k \cdot a_{in})$. Podľa tvrdenia už dokázanej vety 5.5 platí $\det\mathbf{A} = 0.\det\mathbf{A} = 0$. ■

Veta 5.8. *Ak sa matice* $\mathbf{A}$ *a* $\mathbf{B}$ *líšia iba v* i*-tom riadku, potom*

$$\begin{vmatrix} \mathbf{a}_1^T \\ \vdots \\ \mathbf{a}_{i-1}^T \\ \mathbf{a}_i^T \\ \mathbf{a}_{i+1}^T \\ \vdots \\ \mathbf{a}_1^T \end{vmatrix} + \begin{vmatrix} \mathbf{a}_1^T \\ \vdots \\ \mathbf{a}_{i-1}^T \\ \mathbf{b}_i^T \\ \mathbf{a}_{i+1}^T \\ \vdots \\ \mathbf{a}_1^T \end{vmatrix} = \begin{vmatrix} \mathbf{a}_1^T \\ \vdots \\ \mathbf{a}_{i-1}^T \\ \mathbf{a}_i^T + \mathbf{b}_i^T \\ \mathbf{a}_{i+1}^T \\ \vdots \\ \mathbf{a}_1^T \end{vmatrix},$$

kde $\mathbf{a}_i^T$, $\mathbf{b}_i^T$ *sú riadkové vektory matice* $\mathbf{A}$, *resp.* $\mathbf{B}$.

DÔKAZ:
Stačí si uvedomiť, že každý zo sčítancov pri výpočte determinantu na pravej strane rovnosti obsahuje súčin $a_{1\pi(1)} \cdot a_{2\pi(2)} \cdot \cdots \cdot (a_{i\pi(i)} + b_{i\pi(i)}) \cdots \cdot a_{n\pi(n)} =$ $a_{1\pi(1)} \cdot a_{2\pi(2)} \cdot \cdots \cdot a_{i\pi(i)} \cdots \cdot a_{n\pi(n)} + a_{1\pi(1)} \cdot a_{2\pi(2)} \cdot \cdots \cdot b_{i\pi(i)} \cdots \cdot a_{n\pi(n)}$. ■

Veta 5.9. *Ak matica* $\mathbf{B}$ *vznikla zo štvorcovej matice* $\mathbf{A}$ *pripočítaním* k*-násobku* i*-teho riadku* k *ľubovoľnému inému riadku, potom*

$$\det\mathbf{B} = \det\mathbf{A} \tag{5.16}$$

DÔKAZ:
Triviálny. Matica $\mathbf{B}$ sa od matice $\mathbf{A}$ líši len j-tym riadkom, $j \neq i$, ktorý má tvar $a_{j1} + ka_{i1},\ a_{j2} + ka_{i2},\ \ldots,\ a_{jn} + ka_{in}$. Vzhľadom na už dokázané tvrdenia môžeme písať $\det\mathbf{B} = \det\mathbf{A} + k \cdot \det\tilde{\mathbf{A}}$, kde matica $\tilde{\mathbf{A}}$ má dva riadky rovnaké. To ale znamená, že $\det\mathbf{B} = \det\mathbf{A}$. ■

Veta 5.10. *Ak matica* $\mathbf{B}$ *vznikla zo štvorcovej matice* $\mathbf{A}$ *tak, že k* i*-temu riadku bola pripočítaná lineárna kombinácia iných riadkov, potom*

$$\det\mathbf{B} = \det\mathbf{A} \tag{5.17}$$

DÔKAZ:
Tvrdenie vety vyplýva z tvrdení viet 5.8 a 5.9. ■

***Poznámka* 5.6.** *Tvrdenia 5.4 - 5.10 platia aj pre stĺpce. Platnosť tvrdení vyplýva z vety 5.3.*

Vety 5.4 až 5.10 nám dávajú užitočný nástroj na zjednodušenie výpočtov determinantov všetkých stupňov. Na základe dokázaných tvrdení upravíme maticu tak, že nezmeníme hodnotu jej determinantu. Pre praktický výpočet determinantu má význam nasledujúca veta.

Veta 5.11. *Nech* $\mathbf{A}$ *je štvorcová horná alebo dolná trojuholníková matica. Potom*

$$\det\mathbf{A} = a_{11}.a_{22}.\ldots.a_{nn} \tag{5.18}$$

Dôkaz:
Nech $\mathbf{A}$ je horná trojuholníková matica

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{mn} \end{pmatrix}$$

Z definície determinantu vieme, že v každom sčítanci je každý riadok a stĺpec zastúpený práve raz. Ak nepočítame nulové sčítance, z prvého stĺpca musíme vybrať prvok a_{11}. Z druhého stĺpca je použiteľný len prvok a_{22} (prvky prvého riadku už nemôžeme vyberať), z tretieho stĺpca má zmysel vybrať len prvok a_{33}. Opakovaním naznačeného postupu vyberieme prvky z hlavnej diagonály a dostaneme tak tvrdenie vety. ■

Na ilustráciu uvedieme príklad, v ktorom využijeme vlastnosti vyslovené v predchádzajúcich vetách.

Príklad 5.10. Vypočítajme determinant matice

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

úpravou na hornú trojuholníkovú maticu.

Riešenie:

$$\det\mathbf{A} = \begin{vmatrix} 2 & 1 & -1 & 2 \\ 1 & 2 & 1 & 1 \\ 0 & 3 & 1 & -1 \\ 1 & -1 & -1 & 0 \end{vmatrix}$$

Urobíme vzájomnú výmenu prvého a druhého riadku, hodnota determinantu sa zmení (-1)-krát.

$$\det\mathbf{A} = - \begin{vmatrix} 1 & 2 & 1 & 1 \\ 2 & 1 & -1 & 2 \\ 0 & 3 & 1 & -1 \\ 1 & -1 & -1 & 0 \end{vmatrix}$$

Prvý riadok vynásobíme číslom -2 a pripočítame k druhému riadku. Súčasne vynásobíme prvý riadok číslom -1 a pripočítame k štvrtému riadku. Hodnota determinantu sa nezmení.

$$\det\mathbf{A} = -\begin{vmatrix} 1 & 2 & 1 & 1 \\ 0 & -3 & -3 & 0 \\ 0 & 3 & 1 & -1 \\ 0 & -3 & -2 & -1 \end{vmatrix}$$

K tretiemu riadku pripočítame druhý riadok a k štvrtému riadku pripočítame (-1)-násobok druhého riadku. Hodnota determinantu zostane bez zmeny.

$$\det\mathbf{A} = -\begin{vmatrix} 1 & 2 & 1 & 1 \\ 0 & -3 & -3 & 0 \\ 0 & 0 & -2 & -1 \\ 0 & 0 & 1 & -1 \end{vmatrix}$$

Urobíme vzájomnú výmenu tretieho a štvrtého riadku, hodnota determinantu sa vynásobí číslom (-1).

$$\det\mathbf{A} = \begin{vmatrix} 1 & 2 & 1 & 1 \\ 0 & -3 & -3 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -2 & -1 \end{vmatrix}$$

Dvojnásobok tretieho riadku pripočítame k štvrtému, hodnota determinantu sa nezmení.

$$\det\mathbf{A} = \begin{vmatrix} 1 & 2 & 1 & 1 \\ 0 & -3 & -3 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -3 \end{vmatrix}$$

Vykonanými úpravami sme upravili maticu na trojuholníkový tvar. Podľa vety 5.11 platí

$$\det\mathbf{A} = 1 \cdot (-3) \cdot 1 \cdot (-3) = 9.$$

Uviedli sme jednoduchý spôsob výpočtu determinantov tretieho stupňa Sarusovým pravidlom aj jeden zo spôsobov výpočtu determinantov n-tého stupňa, pričom $n \geq 4$ – úpravou na trojuholníkový tvar. Teraz uvedieme spôsob, pri ktorom vyjadríme determinant n-tého stupňa pomocou determinantov nižších stupňov.

Definícia 5.12. Nech $\mathbf{A} = (a_{ij})$ je štvorcová matica n-tého stupňa a nech $\mathbf{A_{ij}}$ je štvorcová matica stupňa $(n-1)$, ktorá vznikne z matice $\mathbf{A}$ vynechaním i-teho riadku a j-teho stĺpca. Číslo

$$A_{ij} = (-1)^{i+j} \det \mathbf{A_{ij}} \tag{5.19}$$

pre $i,\ j \in \{1, 2, \ldots, n\}$ sa nazýva **algebraický doplnok** prvku a_{ij}.

Veta 5.12. *Nech* $\mathbf{A} = (a_{ij})$ *je štvorcová matica stupňa* n. *Potom*

$$\sum_{k=1}^{n} a_{ik} A_{jk} = a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = \begin{cases} \det\mathbf{A} & ak\ i = j \\ 0 & ak\ i \neq j \end{cases}, \tag{5.20}$$

$$\sum_{k=1}^{n} a_{ki} A_{kj} = a_{1i}A_{1j} + a_{2i}A_{2j} + \cdots + a_{ni}A_{nj} = \begin{cases} \det\mathbf{A} & ak\ i = j \\ 0 & ak\ i \neq j \end{cases}. \tag{5.21}$$

Dôkaz:
Dôkazy oboch rovností majú rovnakú myšlienku. Naznačíme dôkaz prvej rovnosti. Sčítance z definície determinantu

$$\det\mathbf{A} = \sum_{\pi \in \Pi} \text{zn}\ \pi . a_{1\pi(1)} a_{2\pi(2)} \ldots a_{n\pi(n)}$$

rozdelíme do n skupín tak, aby každý sčítanec v prvej skupine obsahoval prvok a_{i1}, v druhej $a_{i2,}$, ... atď. Všetky sčítance k-tej skupiny pre $k = 1, 2, \ldots, n$ vytvoríme takto:

Postupnou výmenou susedných riadkov a stĺpcov dostaneme i-ty riadok na miesto prvého riadku a k-ty stĺpec na miesto prvého stĺpca. Týmito výmenami dostaneme prvok a_{ik} na pozíciu $(1, 1)$ a hodnotu determinantu zmeníme vynásobením číslom $(-1)^{i+k}$. Pretože po vynechaní prvého riadku a prvého stĺpca dostaneme z takto upravenej matice subdeterminant $\det\mathbf{A_{ij}}$, dávajú sčítance k-tej skupiny súčet $(-1)^{i+k} a_{ik} \det\mathbf{A_{ij}} = a_{ik}A_{ik}$. Ak naznačený postup zopakujeme pre všetky skupiny a urobíme súčet, dostaneme tvrdenie vety pre prípad, že $i = j$.

V prípade, že $i \neq j$ budeme vychádzať z toho, čo sme doposiaľ dokázali. K i-temu riadku matice pripočítame j-ty riadok . Tak z matice $\det\mathbf{A}$ dostaneme $\det\mathbf{B}$ a platí $\det\mathbf{A} = \det\mathbf{B} = (a_{i1} + a_{j1})A_{i1} + \cdots + (a_{in} + a_{jn})A_{in} = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in} + a_{j1}A_{i1} + a_{j2}A_{j2} + \cdots + a_{jn}A_{in} = \det\mathbf{A} + a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}$. Z toho vyplýva, že $a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in} = 0$. ■

Definícia 5.13. Pre $i, j = 1, 2, \ldots, n$ vzťahy

$$\begin{aligned} a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in} &= \det\mathbf{A} \\ a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{nj}A_{nj} &= \det\mathbf{A} \end{aligned}$$

nazývame **Laplaceovým rozvojom** determinantu det**A** podľa prvkov i-teho riadku, resp. podľa prvkov j-teho stĺpca.

***Poznámka* 5.7.** *Laplaceov rozvoj determinantu, či už podľa prvkov ľubovoľného riadku alebo stĺpca, umožňuje výpočet determinantu n-tého stupňa pomocou determinantov $(n-1)$-vého stupňa. Determinanty $(n-1)$-vého stupňa opakovaným použitím Laplaceovho rozvoja počítame pomocou determinantov $(n-2)$-hého stupňa atď. Laplaceov rozvoj aplikujeme dovtedy, kým nedosiahneme determinanty aspoň tretieho stupňa, ktoré spočítame Sarusovým pravidlom.*

Takýto postup môže byť zdĺhavý, hlavne ak vybratý riadok, resp. stĺpec, podľa ktorého robíme Laplaceov rozvoj, obsahuje veľa nenulových prvkov. Odporúčame pre rozvoj zvoliť riadky, resp. stĺpce, v ktorých je veľa nulových prvkov. Pokiaľ také v matici nie sú, použitím úprav, ktoré nemenia hodnotu determinantu, je vhodné upraviť maticu tak, aby v riadku, resp. stĺpci, bol jeden prvok nenulový a ostatné nulové. Laplaceov rozvoj robíme podľa takéhoto riadku, resp. stĺpca, čo značne urýchli výpočet.

Pre lepšie pochopenie predchádzajúcich riadkov uvedieme príklad.

Príklad 5.11. Počítajme determinant

$$\det\mathbf{A} = \begin{vmatrix} 1 & 4 & 0 & 3 \\ 2 & -1 & 1 & 5 \\ 0 & 4 & 1 & 4 \\ 3 & 5 & 9 & 2 \end{vmatrix}$$

Riešenie:
Najskôr zvolíme postup bez úprav matice. Urobíme Laplaceov rozvoj podľa prvkov prvého stĺpca.

$$\det\mathbf{A} = 1\cdot(-1)^{1+1}\begin{vmatrix} -1 & 1 & 5 \\ 4 & 1 & 4 \\ 5 & 9 & 2 \end{vmatrix} + 2\cdot(-1)^{2+1}\begin{vmatrix} 4 & 0 & 3 \\ 4 & 1 & 4 \\ 5 & 9 & 2 \end{vmatrix} +$$

$$+ 0\cdot(-1)^{3+1}\begin{vmatrix} 4 & 0 & 3 \\ -1 & 1 & 5 \\ 5 & 9 & 2 \end{vmatrix} + 3\cdot(-1)^{4+1}\begin{vmatrix} 4 & 0 & 3 \\ -1 & 1 & 5 \\ 4 & 1 & 4 \end{vmatrix}$$

Determinanty matíc tretieho stupňa vypočítame podľa Sarusovho pravidla a dostaneme

$$\det\mathbf{A} = 1\cdot 201 - 2\cdot(-43) + 0\cdot(-214) - 3\cdot(-19) = 344.$$

A teraz zvolíme postup, pri ktorom sa vyhneme počítaniu štyroch determinantov. Namiesto toho stačí vypočítať determinant jeden. Maticu $\mathbf{A}$ upravíme tak, aby sme mali v prvom stĺpci v druhom, treťom a štvrtom riadku nuly. Dosiahneme to tak, že (-2)-násobok prvého riadku pripočítame k druhému riadku a (-3)-násobok prvého riadku pripočítame k štvrtému riadku. Hodnota determinantu sa týmito operáciami nezmení(viď veta 5.9).

$$\det\mathbf{A} = \begin{vmatrix} 1 & 4 & 0 & 3 \\ 2 & -1 & 1 & 5 \\ 0 & 4 & 1 & 4 \\ 3 & 5 & 9 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 4 & 0 & 3 \\ 0 & -9 & 1 & -1 \\ 0 & 4 & 1 & 4 \\ 0 & -7 & 9 & -7 \end{vmatrix} = 1(-1)^2\begin{vmatrix} -9 & 1 & -1 \\ 4 & 1 & 4 \\ -7 & 9 & -7 \end{vmatrix} = 344$$

***Poznámka* 5.8.** *V príklade sme naznačili postup vedúci k zjednodušeniu počítania determinantov. Vo všeobecnosti v determinante volíme taký prvok a_{ij}, ktorý sa nachádza v riadku (resp. stĺpci) s najväčším počtom nulových prvkov a podľa možnosti sa rovná jednej, alebo je deliteľom ostatných prvkov stĺpca (resp. riadku). Nedržíme sa však vždy prísne tohto postupu, ale využívame všetky možnosti, ktoré vedú k zjednodušeniu výpočtu.*

Príklad 5.12. Vandermondov determinant

je determinant tvaru

$$\det\begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \dots & \dots & \dots & \dots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{pmatrix} \tag{5.22}$$

kde $a_1, a_2 \ldots, a_n$ sú prvky ľubovoľného poľa.
V ľubovoľnom poli platí

$$\det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ a_1^{n-1} & a_2^{n-1} & \ldots & a_n^{n-1} \end{pmatrix} = \prod_{1 \le j < i \le n} (a_i - a_j) \tag{5.23}$$

Dôkaz:
Pre $n = 2$

$$\det \begin{pmatrix} 1 & 1 \\ a_1 & a_2 \end{pmatrix} = (a_2 - a_1) \tag{5.24}$$

Indukčný krok ukážeme pre $n = 3$.

$$\det \begin{pmatrix} 1 & 1 & 1 \\ a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \end{pmatrix} = \det \begin{pmatrix} 1 & 1 & 1 \\ 0 & a_2 - a_1 & a_3 - a_1 \\ 0 & a_2^2 - a_1 a_2 & a_3^2 - a_1 a_3 \end{pmatrix} =$$

$$= 1 . \det \begin{pmatrix} a_2 - a_1 & a_3 - a_1 \\ a_2^2 - a_1 a_2 & a_3^2 - a_1 a_3 \end{pmatrix} = \det \begin{pmatrix} (a_2 - a_1) & (a_3 - a_1) \\ (a_2 - a_1) a_2 & (a_3 - a_1) a_3 \end{pmatrix} =$$

$$(a_2 - a_1)(a_3 - a_1) . \det \begin{pmatrix} 1 & 1 \\ a_2 & a_3 \end{pmatrix} = (a_2 - a_1)(a_3 - a_1)(a_3 - a_2), \tag{5.25}$$

kde prvá úprava spočívala v odčítaní a_1 násobku $(i-1)$-ho riadku od i-teho riadku (v poradí od posledného k prvému riadku), druhá úprava je rozvojom determinantu podľa prvého stĺpca a kde posledná rovnosť vyplýva z indukčného predpokladu. ■

Zo vzťahu 5.23 vyplýva, že Vandermondov determinant sa rovná nule práve vtedy, keď existuje aspoň jedna dvojica čísel a_i, a_j, $i \neq j$ takých, že $a_i = a_j$. Vandermondov determinant je rôzny od nuly práve vtedy, keď sú čísla $a_1, a_2, \ldots, a_n$ všetky rôzne.

V informatike sa Vandermondov determinant často vyskytuje pri riešení rôznych problémov kódovania (napríklad pri tzv. BCH-kódoch – pozri literatúru napr. [1], [2]). Má tiež množstvo aplikácií v teórii pravdepodobnosti a iných častiach aplikovanej matematiky.

Veta 5.13. *Nech* $\mathbf{A} = \big(a_{ij}\big)$, $\mathbf{B} = \big(b_{ij}\big)$ *sú štvorcové matice rádu* n. *Potom*

$$\det(\mathbf{A} \cdot \mathbf{B}) = \det\mathbf{A} \cdot \det\mathbf{B} \tag{5.26}$$

Dôkaz:
Nech $\mathbf{AB} = \mathbf{C}= (c_{ij})$. Pre $i, k = 1, 2, \ldots, n$ je potom

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

Nech $\pi = (k_1, k_2, \ldots, k_n)$ je ľubovoľná permutácia množiny $\{1, 2, \ldots, n\}$ a $z = zn\ \pi$. Determinant $\det(\mathbf{A} \cdot \mathbf{B})$ určíme z definície. Uvažujme najskôr súčin

$$\begin{aligned} c_{1k_1}c_{2k_2}\ldots c_{nk_n} &= (a_{11}b_{1k_1} + a_{12}b_{2k_1} + \cdots + a_{1n}b_{nk_1}) \cdot (a_{21}b_{1k_2} + \ldots \\ &\cdots + a_{22}b_{2k_2} + \cdots + a_{2n}b_{nk_2}) \cdot \cdots \cdot (a_{n1}b_{1k_n} + a_{n2}b_{2k_n} + \cdots + a_{nn}b_{nk_n}) = \\ &= \sum_{j_1, j_2, \ldots j_n} a_{1j_1}a_{2j_2}\cdots a_{nj_n}b_{j_1k_1}b_{j_2k_2}\cdots b_{j_nk_n}. \end{aligned}$$

$$\begin{aligned} \det(\mathbf{A} \cdot \mathbf{B}) &= \sum_{\pi=(k_1,k_2,\ldots,k_n)} zn\ \pi\ c_{1k_1}c_{2k_2}\ldots c_{nk_n} = \\ &= \sum_{\pi=(k_1,k_2,\ldots,k_n)} zn\ \pi \sum_{j_1,j_2,\ldots j_n} a_{1j_1}a_{2j_2}\cdots a_{nj_n}b_{j_1k_1}b_{j_2k_2}\cdots b_{j_nk_n} = \\ &= \sum_{j_1,j_2,\ldots j_n} a_{1j_1}a_{2j_2}\cdots a_{nj_n} \sum_{\pi=(k_1,k_2,\ldots,k_n)} zn\ \pi b_{j_1k_1}b_{j_2k_2}\cdots b_{j_nk_n} = \\ &= \sum_{\pi'=(j_1,j_2,\ldots j_n)} z'\ a_{1j_1}a_{2j_2}\cdots a_{nj_n} \sum_{\pi=(k_1,k_2,\ldots,k_n)} z\ b_{j_1k_1}b_{j_2k_2}\cdots b_{j_nk_n} = \\ &= \det\mathbf{A} \cdot \det\mathbf{B} \quad \text{pre} \quad j_1, j_2, \ldots j_n \in \{1, 2, \ldots, n\}, \end{aligned}$$

kde pre zjednodušenie zápisu je použité značenie $z = zn\ \pi$, $z' = zn\ \pi'$. Využili sme tiež skutočnosť, že ak $j_1, j_2, \ldots j_n$ nie je permutácia, potom

$$\sum_{\pi=(k_1,k_2,\ldots,k_n)} zn\ \pi\ b_{j_1k_1}b_{j_2k_2}\cdots b_{j_nk_n} = 0,$$

keďže ide o Laplaceov rozvoj $\det\mathbf{B}$ s aspoň dvomi rovnakými riadkami a bola použitá rovnosť $z' \cdot z' = zn\ \pi' \cdot zn\ \pi' = 1$. ■

5.2.1 Hodnosť matice a riadková ekvivalencia matíc

Po krátkom odbočení sa znova vrátime k štúdiu vektorových priestorov $V_n(\mathcal{P})$. Pri riešení úloh efektne využijeme matice.

Majme danú množinu vektorov $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$ vektorového priestoru $V_n(\mathcal{P})$. Nech

$$\begin{aligned} \mathbf{a}_1 &= (a_{11}, a_{12}, \ldots, a_{1n}), \\ \mathbf{a}_2 &= (a_{21}, a_{22}, \ldots, a_{2n}), \\ &\vdots \\ \mathbf{a}_m &= (a_{m1}, a_{m2}, \ldots, a_{mn}). \end{aligned}$$

Takémuto systému vektorov možno priradiť maticu, ktorej riadky budú práve vektory $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$, teda

$$\mathbf{A} = \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \ldots \\ \mathbf{a}_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

Postup je možno aj obrátiť. Každej matici $\mathbf{A}$ typu $m \times n$ priradíme podpriestor vektorového priestoru $V_n(\mathcal{P})$.

Definícia 5.14. Podpriestorom prislúchajúcim k matici A typu $m \times n$ nad poľom $\mathcal{P}$ nazývame vektorový podpriestor priestoru $V_n(\mathcal{P})$ generovaný riadkami matice chápanými ako vektory z $V_n(\mathcal{P})$. Značíme V_A.

Príklad 5.13. Nech je daná matica

$$\mathbf{A} = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 9 \\ 3 & 2 & 2 & 0 \end{pmatrix}$$

Riadky matice $\mathbf{A}$ chápeme ako vektory vektorového priestoru $V_4(\mathbb{R})$, teda podpriestor prislúchajúci matici má tvar $V_A = [(2,1,0,1), (1,2,1,9), (3,2,2,0)]$

Jeden a ten istý vektorový podpriestor môžu generovať rôzne množiny vektorov. Vzniká otázka, ktorým maticiam typu $m \times n$ nad poľom $\mathcal{P}$ prislúcha ten

istý podpriestor vektorového priestoru $V_n(\mathcal{P})$. Odpoveď na túto otázku, ako aj na otázky ohľadne bázy takéhoto podpriestoru a jeho dimenzie, budeme hľadať v tejto podkapitole.

Definícia 5.15. Elementárnymi riadkovými operáciami na ľubovoľnej matici $\mathbf{A}$ rozumieme každú z nasledujúcich úprav:

a) vzájomná výmena dvoch riadkov,

b) vynásobenie niektorého riadku nenulovým skalárom,

c) pripočítanie k-násobku niektorého riadku k inému riadku matice.

Poznámka* 5.9.** *Elementárne operácie uvedené v definícii 5.15 sú definované aj pre stĺpce matice a nazývajú sa* ***elementárne stĺpcové operácie*.*

Definícia 5.16. Hovoríme, že matica $\mathbf{A}$ typu $m \times n$ **je riadkovo ekvivalentná s maticou $\mathbf{B}$** typu $m \times n$, ak maticu $\mathbf{B}$ možno dostať z matice $\mathbf{A}$ pomocou konečnej postupnosti elementárnych riadkových operácií. Označujeme $\mathbf{A} \sim \mathbf{B}$.

Veta 5.14. *Riadkovo ekvivalentným maticiam prislúcha ten istý vektorový podpriestor.*

Dôkaz:
Nech $\mathbf{A}$ je matica typu $m \times n$ a $V_A = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m]$ k nej prislúchajúci podpriestor. Aby sme dokázali tvrdenie vety, stačí dokázať, že V_A sa nezmení, keď na matici $\mathbf{A}$ vykonáme ktorúkoľvek elementárnu riadkovú operáciu. Postupne preberme všetky tri prípady.

a) Vzájomná výmena ľubovoľných dvoch riadkov nezmení podpriestor V_A. Zrejme platí $[\mathbf{a}_1, \ldots, \mathbf{a}_i, \mathbf{a}_j, \ldots, \mathbf{a}_m] = [\mathbf{a}_1, \ldots, \mathbf{a}_j, \mathbf{a}_i, \ldots, \mathbf{a}_m]$. V lineárnej kombinácii vektorov $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$ na poradí sčítancov nezáleží, lebo pre sčítanie vektorov platí komutatívny zákon.

b) Ak ľubovoľný riadok matice $\mathbf{A}$ vynásobíme skalárom $k \neq 0$, tak V_A sa opäť nezmení. Je zrejmá rovnosť $[\mathbf{a}_1, \ldots, \mathbf{a}_i, \ldots, \mathbf{a}_m] = [\mathbf{a}_1, \ldots, k\mathbf{a}_i, \ldots, \mathbf{a}_m]$

c) Potrebujeme ešte dokázať, že ak k-násobok jedného riadku pripočítame k inému riadku, V_A sa nezmení. Na všeobecnosti dôkazu sa nič nezmení, keď pre určitosť budeme predpokladať, že k-násobok prvého riadku matice $\mathbf{A}$ pripočítame k druhému jej riadku.

Označme $S = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m]$, $T = [\mathbf{a}_1, k\mathbf{a}_1 + \mathbf{a}_2, \ldots, \mathbf{a}_m]$. Teraz musíme dokázať, že $S = T$. Keďže každý vektor generujúci T patrí do S, platí aj $T \subseteq S$. Aby platilo $S \subseteq T$, stačí ukázať, že každý vektor $\boldsymbol{\beta} \in S$ sa dá napísať ako lineárna kombinácia vektorov generujúcich podpriestor T.

Pre ľubovoľný vektor $\boldsymbol{\beta} \in S$ platí $\boldsymbol{\beta} = c_1\mathbf{a}_1 + \cdots + c_m\mathbf{a}_m$. Ale ten istý vektor $\boldsymbol{\beta}$ môžeme vyjadriť aj ako lineárnu kombináciu

$$\boldsymbol{\beta} = (c_1 - kc_2)\mathbf{a}_1 + c_2(k\mathbf{a}_1 + \mathbf{a}_2) + \cdots + c_m\mathbf{a}_m.$$

To znamená, že $\boldsymbol{\beta} \in T$ a platí $S = T$. ■

Teraz už vieme, že riadkovo ekvivalentné matice generujú ten istý podpriestor vektorového priestoru $V_n(\mathcal{P})$. Aby sme vedeli určiť jeho bázu a dimenziu, uvedieme nasledujúce vety, ktoré nám budú nápomocné pri riešení zadanej úlohy.

Veta 5.15 (Gaussova eliminačná metóda)**.** *Každú nenulovú maticu* $\mathbf{A}$ *typu* $m \times n$ *je možné pomocou elementárnych operácií upraviť na maticu* $\mathbf{G}$ $m \times n$*, ktorá má tvar*

$$\mathbf{G} = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1k} & \cdots & g_{1n} \\ 0 & g_{22} & \cdots & g_{2k} & \cdots & g_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & g_{kk} & \cdots & g_{kn} \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{5.27}$$

kde $g_{ii} \neq 0$ *pre* $i = 1, 2, \ldots, k$, $k \leq m$, $k \leq n$.

Dôkaz:
Podľa predpokladu je $\mathbf{A} \neq \mathbf{O}$. To znamená, že v matici $\mathbf{A}$ je aspoň jeden prvok nenulový. Nech je ním a_{ij}. Výmenou i-teho riadku s prvým riadkom a j-teho stĺpca s prvým stĺpcom dostaneme maticu $\mathbf{B} \sim \mathbf{A}$, ktorá má na pozícii $(1, 1)$ nenulový prvok. Vynásobením prvého riadku matice $\mathbf{B} = (b_{uv})$ číslom $-b_{u1}/b_{11} = -b_{u1}/a_{ij}$ a postupným pripočítavaním k u-temu riadku pre $u = 2, 3, \ldots, m$, dostaneme v prvom stĺpci pod hlavnou diagonálou nuly. Ak v matici $\mathbf{C}$, ktorá vznikne z matice $\mathbf{B}$ vynechaním prvého riadku a prvého stĺpca, sú len nulové prvky, potom matica $\mathbf{A}$ je upravená na požadovaný tvar. V opačnom prípade popísaný postup opakujeme. Po konečnom počte krokov z matice $\mathbf{A}$ dostaneme maticu $\mathbf{G}$. ■

***Poznámka* 5.10.** *Dôkaz vety 5.15 je konštruktívny. Dáva priamo návod, ako upraviť maticu* $\mathbf{A}$ *na hornú trojuholníkovú maticu Gaussovou eliminačnou metódou.*

Príklad 5.14. Maticu

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 4 & 1 & 3 \\ 3 & 6 & 12 & 0 & 2 \\ -1 & 2 & 1 & 1 & -1 \end{pmatrix}$$

upravme na trojuholníkový tvar Gaussovou eliminačnou metódou.

Prvý riadok matice vynásobíme číslom (-3) a pripočítame k druhému riadku. Súčasne pripočítame prvý riadok k tretiemu. Dostaneme maticu $\mathbf{B} \sim \mathbf{A}$

$$\mathbf{B} = \begin{pmatrix} 1 & 2 & 4 & 1 & 3 \\ 0 & 0 & 0 & -3 & -7 \\ 0 & 4 & 5 & 2 & 2 \end{pmatrix}$$

V matici $\mathbf{B}$ urobíme vzájomnú výmenu tretieho a druhého riadku. Dostaneme maticu $\mathbf{C} \sim \mathbf{B}$

$$\mathbf{C} = \begin{pmatrix} 1 & 2 & 4 & 1 & 3 \\ 0 & 4 & 5 & 2 & 2 \\ 0 & 0 & 0 & -3 & -7 \end{pmatrix}$$

V poslednom kroku vzájomne vymeníme tretí stĺpec so štvrtým a dostaneme maticu $\mathbf{G} \sim \mathbf{C}$

$$\mathbf{G} = \begin{pmatrix} 1 & 2 & 1 & 4 & 3 \\ 0 & 4 & 2 & 5 & 2 \\ 0 & 0 & -3 & 0 & -7 \end{pmatrix}$$

Veta 5.16 (Jordanova eliminačná metóda)**.** *Každú nenulovú maticu* $\mathbf{A}$ *typu* $m \times n$ *je možné pomocou elementárnych operácií upraviť na maticu* $\mathbf{J}$ *typu* $m \times n$*, ktorá má tvar*

$$\mathbf{J} = \begin{pmatrix} j_{11} & 0 & \dots & 0 & j_{1,k+1} & \dots & j_{1n} \\ 0 & j_{22} & \dots & 0 & j_{2,k+} & \dots & j_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & j_{kk} & j_{k,k+1} & \dots & j_{kn} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}, \tag{5.28}$$

kde $j_{ii} \neq 0$ *pre* $i = 1, 2, \dots, k$, $k \leq m$, $k \leq n$.

DÔKAZ:
Danú maticu **A** upravíme Gaussovou eliminačnou metódou na maticu **G**. Pomocou nenulových prvkov na hlavnej diagonále vyrobíme elementárnymi riadkovými úpravami nulové prvky v stĺpcoch nad nimi. Postupujeme pritom zdola nahor a sprava doľava. ■

Príklad 5.15. Maticu

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 4 & 1 & 3 \\ 3 & 6 & 12 & 0 & 2 \\ -1 & 2 & 1 & 1 & -1 \end{pmatrix}$$

upravme Jordanovou eliminačnou metódou.

V príklade 5.14 sme upravili maticu **A** Gaussovou eliminačnou metódou na hornú trojuholníkovú maticu. Využijeme to a budeme pokračovať úpravami matice

$$\mathbf{G} = \begin{pmatrix} 1 & 2 & 1 & 4 & 3 \\ 0 & 4 & 2 & 5 & 2 \\ 0 & 0 & -3 & 0 & -7 \end{pmatrix}$$

Tretí riadok matice **G** vynásobíme číslom $\frac{2}{3}$ a pripočítame k druhému riadku a súčasne vynásobíme $\frac{1}{3}$ a pripočítame k prvému riadku. Dostaneme maticu $\mathbf{H} \sim \mathbf{G}$

$$\mathbf{H} = \begin{pmatrix} 1 & 2 & 0 & 4 & 2/3 \\ 0 & 4 & 0 & 5 & -8/3 \\ 0 & 0 & -3 & 0 & -7 \end{pmatrix}$$

V matici **H** vynásobíme druhý riadok $\frac{-1}{2}$ a pripočítame k prvému riadku. Dostaneme tak maticu $\mathbf{J} \sim \mathbf{H}$

$$\mathbf{J} = \begin{pmatrix} 1 & 0 & 0 & 3/2 & 2 \\ 0 & 4 & 0 & 5 & -8/3 \\ 0 & 0 & -3 & 0 & -7 \end{pmatrix}$$

***Poznámka* 5.11.** *Výsledný tvar matice upravenej Gaussovou alebo Jordanovou eliminačnou metódou nie je určený jednoznačne. Záleží na tom, akú postupnosť elementárnych operácií zvolíme.*

Riadkové elementárne operácie je možné na matici $\mathbf{A}$ typu $m \times n$ vykonať aj pomocou násobenia tejto matice zľava vhodnou maticou:

a) Vzájomnú výmenu i-teho a j-teho riadku matice $\mathbf{A}$ dosiahneme, ak maticu $\mathbf{A}$ vynásobíme zľava maticou $\mathbf{E}_{ij}$, ktorá vznikla z jednotkovej matice $\mathbf{E}_m$ výmenou i-teho a j-teho riadku.

b) Vynásobenie i-teho riadku nenulovým skalárom k dosiahneme tak, že maticu $\mathbf{A}$ vynásobíme zľava maticou $\mathbf{E}_i(k)$, ktorú dostaneme z jednotkovej matice $\mathbf{E}_m$ nahradením prvku $e_{ii} = 1$ prvkom $e'_{ii} = k$.

c) Pripočítanie k-násobku j-teho riadku k i-temu dosiahneme vynásobením matice $\mathbf{A}$ zľava maticou $\mathbf{E}_{ij}(k)$, ktorá vznikne z matice $\mathbf{E}_m$ nahradením prvku $e_{ij} = 0$ prvkom $e'_{ij} = k$.

Uvedomme si, že matica $\mathbf{E}_{ij}$ a matice $\mathbf{E}_i(k)$, $\mathbf{E}_{ij}(k)$ (pre $k \neq 0$) sú štvorcové regulárne matice stupňa m.

Uvedené tvrdenia ozrejmíme ukážkou popísaných úkonov:

a) Výmena prvého a druhého riadku matice $\mathbf{A}$

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} a_{21} & a_{22} & \dots & a_{2n} \\ a_{11} & a_{12} & \dots & a_{1n} \\ a_{31} & a_{32} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

b) Vynásobenie prvého riadku matice $\mathbf{A}$ skalárom k:

$$\begin{pmatrix} k & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} ka_{11} & ka_{12} & \dots & ka_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

c) Pripočítanie k-násobku j-teho riadku k prvému:

$$\begin{pmatrix} 1 & 0 & \dots & k & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} =$$

$$\begin{pmatrix} a_{11} + ka_{j1} & a_{12} + ka_{j2} & \dots & a_{1n} + ka_{jn} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Poznámka* 5.12.** *Matice* $\mathbf{E}_{ij}$, $\mathbf{E}_i(k)$ *a* $\mathbf{E}_{ij}(k)$ *nazývame* ***elementárne matice*. Ak by sme maticu* $\mathbf{A}$ *násobili elementárnymi maticami sprava, vykonali by sme na matici* $\mathbf{A}$ *stĺpcové elementárne operácie. Elementárne operácie by boli v tomto prípade stupňa* n*.*

Veta 5.17. *Nenulové riadky matice upravenej Jordanovou eliminačnou metódou sú lineárne nezávislé vektory.*

Dôkaz:
Nech $\mathbf{j}_1 = (j_{11}, j_{12}, \dots, j_{1n}), \dots, \mathbf{j}_p = (j_{p1}, j_{p2}, \dots, j_{pn})$ sú nenulové riadky matice $\mathbf{J}$ upravenej Jordanovou eliminačnou metódou. Aby sme dokázali ich lineárnu nezávislosť, stačí ukázať, že žiaden z vektorov $\mathbf{j}_1, \mathbf{j}_2, \dots, \mathbf{j}_p$ nie je lineárnou kombináciou predchádzajúcich vektorov. Budeme postupovať nepriamo.
Nech $\mathbf{j}_k = c_1\mathbf{j}_1 + c_2\mathbf{j}_2 + \dots + c_{k-1}\mathbf{j}_{k-1}$, nech prvý nenulový prvok vektora (riadku) $\mathbf{j}_k$ je j_{kl}. Ostatné vektory vystupujúce v lineárnej kombinácii majú l-tú súradnicu nulovú, teda aj l-tá súradnica ich súčtu je nulová. To je ale spor s predpokladom. ■

***Poznámka* 5.13.** *Dôsledkom vety 5.17 je tvrdenie: Nech* $\mathbf{A}$ *je matica,* V_A *je podpriestor prislúchajúci k matici* $\mathbf{A}$ *a nech* $\mathbf{B}$ *je matica upravená Jordanovou eliminačnou metódou riadkovo ekvivalentná s* $\mathbf{A}$*. Potom bázu priestoru* V_A *tvoria nenulové riadky matice* $\mathbf{B}$*.*

Teraz zadefinujeme jeden z najdôležitejších pojmov teórie matíc – hodnosť matice.

Definícia 5.17. Hodnosť matice A je dimenzia podpriestoru V_A prislúchajúceho matici. Označujeme $h(\mathbf{A})$.

***Poznámka* 5.14.** *Hodnosť matice upravenej Jordanovou eliminačnou metódou sa rovná počtu jej nenulových riadkov. Riadkovo ekvivalentné matice majú rovnakú hodnosť.*

***Poznámka* 5.15.** *Ak máme nájsť hodnosť matice, nemusíme maticu vždy upravovať Jordanovou eliminačnou metódou. Stačí, ak maticu upravíme na hornú trojuholníkovú maticu Gaussovou eliminačnou metódou. Čitateľ si iste sám dokáže, že nenulové riadky takejto matice sú lineárne nezávislé vektory.*

Príklad 5.16. Daná je matica

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ -2 & -3 & -4 & -5 \\ 3 & 4 & 5 & 6 \\ -4 & -5 & -6 & -7 \\ 5 & 6 & 7 & 8 \end{pmatrix}.$$

Nájdime bázu vektorového priestoru prislúchajúceho matici **A** a určme jeho dimenziu.

Riešenie:
Najskôr nájdeme vektorový priestor prislúchajúci matici **A**. Je to $V_A = [(1,2,3,4),(-2,-3,-4,-5),(3,4,5,6),(-4,-5,-6,-7),(5,6,7,8)]$. Je to podpriestor vektorového priestoru $V_4(\mathbb{R})$. Aby sme našli jeho bázu, podľa poznámky 5.13, je potrebné upraviť maticu **A** Jordanovou eliminačnou metódou. Ak v matici **A** vynásobíme prvý riadok postupne skalármi 2, -3, 4, -5 a následne pripočítame k druhému, tretiemu, štvrtému a piatemu riadku, dostaneme maticu $\mathbf{B} \sim \mathbf{A}$, konkrétne

$$\mathbf{B} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & -2 & -4 & -6 \\ 0 & 3 & 6 & 9 \\ 0 & -4 & -8 & -12 \end{pmatrix}.$$

V matici **B** pripočítame (-2)-násobok druhého riadku k prvému a následne pripočítame druhý riadok vynásobený postupne skalármi 2, -3 a 4 k tretiemu,

štvrtému a piatemu riadku. Dostaneme maticu $\mathbf{C} \sim \mathbf{B}$, ktorá je už upravená v zmysle Jordanovej eliminačnej metódy.

$$\mathbf{C} = \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Nenulové riadky matice $\mathbf{C}$ určujú bázické vektory priestoru V_A a ich počet jeho dimenziu. $\mathcal{B}_{V_A} = \{(1, 0, -1, -2), (0, 1, 2, 3)\}$ a $dim(V_A) = 2$.

Definícia 5.18. Nech $\mathbf{A}$ je štvorcová matica stupňa n. **Nulita matice** je číslo $d = n - h(\mathbf{A})$.

Príklad 5.17. Nájdime nulitu matice

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

Riešenie:
Elementárnymi riadkovými operáciami postupne dostaneme matice

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

Maticu $\mathbf{A}$ sme upravili Gaussovou eliminačnou metódou, počet nenulových riadkov je 2, čo znamená, že $h(\mathbf{A}) = 2$. Nulita matice je $d = 3 - 2 = 1$.

Veta 5.18. *Elementárne riadkové operácie nemenia hodnosť matice* $\mathbf{A}$.

Dôkaz:
To, že prvé dve elementárne riadkové operácie (vzájomná výmena dvoch riadkov a vynásobenie riadku nenulovým skalárom) nemenia jej hodnosť je zrejmé. Dokážeme, že ak k-násobok i-teho riadku pripočítame k j-temu riadku, hodnosť matice zostane nezmenená.

Nech hodnosť matice $h(\mathbf{A}) = r$. To znamená, že v matici $h(\mathbf{A})$ existuje r lineárne nezávislých riadkov. Pripočítajme k j-temu riadku k-násobok i-teho riadku. Dostaneme tak maticu $\mathbf{B} \sim \mathbf{A}$, ktorá sa od matice $\mathbf{A}$ líši iba j-tym riadkom. Platí $\mathbf{b}_i = \mathbf{a}_i$ pre $i \neq j$, $i = 1, 2, \ldots, r$ a $\mathbf{b}_j = k\mathbf{a}_i + \mathbf{a}_j$. Ďalej budeme postupovať podľa definície lineárnej nezávislosti vektorov. Uvažujme rovnosť

$$c_1\mathbf{a}_1 + \cdots + c_i\mathbf{a}_i + c_j(k\mathbf{a}_i + \mathbf{a}_j) + \cdots + c_r\mathbf{a}_r = \mathbf{o}.$$

Po úprave dostávame

$$c_1\mathbf{a}_1 + \cdots + (c_i + kc_j)\mathbf{a}_i + c_j\mathbf{a}_j + \cdots + c_r\mathbf{a}_r = \mathbf{o}.$$

Vzhľadom na lineárnu nezávislosť vektorov $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_r$ platí, že všetky koeficienty lineárnej kombinácie na ľavej strane rovnosti sú nulové, t. j.

$$c_1 = c_2 = \ldots c_i = c_i + kc_j = \cdots = c_r = 0,$$

nakoľko $c_i = 0$, $c_j = 0$, potom aj $c_i + kc_j = 0$. To znamená, že aj vektory $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_i, \ldots, k\mathbf{a}_i + \mathbf{a}_j, \ldots, \mathbf{a}_r$ sú lineárne nezávislé, hodnosť matice $\mathbf{A}$ sa nezmenila. ■

Veta 5.19. *Pre každú maticu* $\mathbf{A}$ *platí*

$$h(\mathbf{A}) = h(\mathbf{A}^T). \tag{5.29}$$

Dôkaz:
Triviálny. Nech horná trojuholníková matica $\mathbf{B}$ vznikne z matice $\mathbf{A}$ postupnosťou elementárnych riadkových operácií. Potom $h(\mathbf{B}) = h(\mathbf{A})$. Transponovaná matica $\mathbf{B}^T$ vznikne z matice $\mathbf{A}^T$ tou istou postupnosťou elementárnych stĺpcových operácií. Preto platí $h(\mathbf{B}^T) = h(\mathbf{A}^T)$. $\mathbf{B}^T$ je dolná trojuholníková matica. Matice $\mathbf{B}^T$ i $\mathbf{B}$ majú rovnaký počet nenulových diagonálnych prvkov, preto platí $h(\mathbf{B}) = h(\mathbf{B}^T)$. V konečnom dôsledku platí $h(\mathbf{A}) = h(\mathbf{B}) = h(\mathbf{B}^T) = h(\mathbf{A}^T)$. ■

Teraz dokázaná veta hovorí, že v každej matici $\mathbf{A}$ sa maximálny počet lineárne nezávislých riadkových vektorov rovná maximálnemu počtu lineárne nezávislých stĺpcových vektorov. Ak je matica $\mathbf{A}$ typu $m \times n$, potom $h(\mathbf{A}) \leq \min\{m, n\}$.

Definícia 5.19. Nech $\mathbf{A}$ je štvorcová matica stupňa n. Hovoríme, že matica $\mathbf{A}$ je **regulárna**, ak $h(\mathbf{A}) = n$. Ak $h(\mathbf{A}) < n$ hovoríme, že matica $\mathbf{A}$ je **singulárna**.

Príklad 5.18. Daná je matica

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

Zistime, či je matica $\mathbf{A}$ regulárna.

Riešenie:
Vypočítajme hodnosť matice $\mathbf{A}$ úpravou na trojuholníkový tvar Gaussovou eliminačnou metódou. Dostaneme

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

Hodnosť $h(\mathbf{A}) = 2 \leq 3 = n$, matica $\mathbf{A}$ nie je regulárna, je singulárna.

Veta 5.20. *Nech* $\mathbf{A}$ *je štvorcová matica stupňa* n*. Riadkové vektory matice* $\mathbf{A}$ *sú lineárne závislé práve vtedy, keď*

$$\det\mathbf{A} = 0.$$

Dôkaz:
a) Nech riadkové vektory $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ sú lineárne závislé. Potom jeden z vektorov je lineárnou kombináciou ostatných. Predpokladajme, že je to vektor $\mathbf{a}_1$. Platí $\mathbf{a}_1 = c_2\mathbf{a}_2 + c_3\mathbf{a}_3 + \cdots + c_n\mathbf{a}_n$. Potom

$$\det\mathbf{A} = \begin{vmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \vdots \\ \mathbf{a}_n \end{vmatrix} = \begin{vmatrix} c_2\mathbf{a}_2 & + & c_3\mathbf{a}_3 & + & \ldots & + & c_n\mathbf{a}_n \\ & & & \mathbf{a}_2 & & & \\ & & & \mathbf{a}_3 & & & \\ & & & \vdots & & & \\ & & & \mathbf{a}_n & & & \end{vmatrix} =$$

$$= c_2 \begin{vmatrix} \mathbf{a}_2 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \vdots \\ \mathbf{a}_n \end{vmatrix} + c_3 \begin{vmatrix} \mathbf{a}_3 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \vdots \\ \mathbf{a}_n \end{vmatrix} + \cdots + c_n \begin{vmatrix} \mathbf{a}_n \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \vdots \\ \mathbf{a}_n \end{vmatrix} = c_2 \cdot 0 + c_3 \cdot 0 + \cdots + c_n \cdot 0 = 0.$$

b) Nech $\det\mathbf{A} = 0$. Potrebujeme dokázať, že vektory $\mathbf{a}_1, \mathbf{a}, \ldots, \mathbf{a}_n$ sú lineárne závislé. Počítajme determinant matice $\mathbf{A}$ pomocou úpravy matice na trojuholníkový tvar. Nech $\mathbf{B}$ je trojuholníková matica, ktorá vznikla z matice $\mathbf{A}$ Gaussovou eliminačnou metódou. Potom $\det\mathbf{B} = \pm\det\mathbf{A} = 0$. To znamená, že niektorý prvok na hlavnej diagonále matice $\mathbf{B}$ bol nulový, teda $h(\mathbf{B}) < n$, maximálny počet lineárne nezávislých riadkových vektorov je menší ako n, riadkové vektory matice $\mathbf{A}$ sú lineárne závislé. ■

***Poznámka* 5.16.** *Dôsledkom vety 5.20 je nasledujúce tvrdenie. Matica* $\mathbf{A}$ *je regulárna práve vtedy, keď* $\det\mathbf{A} \neq 0$.

Veta 5.21. *Každú regulárnu maticu je možné upraviť na diagonálnu maticu Jordanovou eliminačnou metódou použitím iba riadkových elementárnych operácií (resp. použitím iba stĺpcových elementárnych operácií).*

Dôkaz:
Matica uvažovaná vo vete je regulárna, teda determinant matice je nenulový. To ale znamená, že po úprave Jordanovou eliminačnou metódou musia byť diagonálne prvky nenulové.

Tvrdenie vety dokážeme pre elementárne riadkové operácie. Stačí ukázať, že v i-tom stĺpci je vždy možné nájsť prvok, pomocou ktorého vytvoríme nulové nediagonálne prvky a nepotrebujeme meniť stĺpce. Nech v i-tom kroku Jordanovej eliminačnej metódy (prvých $i-1$ stĺpcov je už upravených) budú v i-tom stĺpci všetky prvky na pozíciách (k, i) pre $k = i, i+1, \ldots, n$ nulové. To ale znamená, že i-ty stĺpec je lineárnou kombináciou prvých $(i-1)$ stĺpcov, čo je spor s predpokladom, že matica j regulárna. ■

Príklad 5.19. Nájdime také $a \in \mathbb{R}$, aby bola matica $\mathbf{A}$ regulárna.

$$\mathbf{A} = \begin{pmatrix} a & 1 & 0 \\ 2 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}.$$

Úlohu vyriešime na základe tvrdenia z poznámky 5.16. Vypočítame determinant matice $\mathbf{A}$:

$$\det\mathbf{A} = \begin{vmatrix} a & 1 & 0 \\ 2 & 1 & 1 \\ -1 & 0 & 1 \end{vmatrix} = a - 3 \neq 0.$$

Matica $\mathbf{A}$ bude regulárna, ak $a \neq 3$.

5.2.2 Inverzná matica

Definícia 5.20. Nech $\mathbf{A}$ je štvorcová matica stupňa n. Nech existuje štvorcová matica $\mathbf{B}$ stupňa n taká, že

$$\mathbf{A}.\mathbf{B} = \mathbf{B}.\mathbf{A} = \mathbf{E_n}, \tag{5.30}$$

kde $\mathbf{E_n}$ je jednotková matica stupňa n. Potom hovoríme, že $\mathbf{B}$ je **inverzná matica** k matici $\mathbf{A}$. Značíme ju $\mathbf{A^{-1}}$.

Z definície ešte nevyplýva, že inverzná matica k danej štvorcovej matici musí existovať. Ak však existuje, tak je tiež štvorcová a rovnakého stupňa ako daná matica. Z praktického hľadiska nás bude zaujímať, k akým maticiam inverzná matica existuje a ako ju vypočítame.

Veta 5.22. *Nech* $\mathbf{A}$ *je ľubovoľná matica. Ak existujú matice* $\mathbf{B}$, $\mathbf{C}$ *tak, že* $\mathbf{AB} = \mathbf{CA} = \mathbf{E}$, *potom platí*

$$\mathbf{B} = \mathbf{C} = \mathbf{A}^{-1}.$$

Dôkaz:
Najskôr si všimnime, že ak také matice $\mathbf{B}$, $\mathbf{C}$ existujú, tak všetky tri matice $\mathbf{A}, \mathbf{B}, \mathbf{C}$ sú štvorcové a rovnakého stupňa. Potrebujeme ešte dokázať, že $\mathbf{B} = \mathbf{C}$. Keďže

$$\mathbf{B} = \mathbf{EB} = (\mathbf{CA})\,\mathbf{B} = \mathbf{C}\,(\mathbf{AB}) = \mathbf{CE} = \mathbf{C}.$$

■

Veta 5.23. *Ak pre štvorcovú maticu* $\mathbf{A}$ *existuje inverzná matica* $\mathbf{A}^{-1}$, *potom* $\det\mathbf{A} \neq 0$ *a platí*

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

Dôkaz:
Nech existuje inverzná matica $\mathbf{A^{-1}}$. Zo vzťahu $\mathbf{E} = \mathbf{A}.\mathbf{A^{-1}}$ a z tvrdenia vety 5.13 vyplýva

$$1 = \det\mathbf{E} = \det\mathbf{A}\det\mathbf{A^{-1}}.$$

Z posledného vzťahu vyplýva, že $\det\mathbf{A} \neq 0$ (aj $\det\mathbf{A^{-1}} \neq 0$) a tiež tvrdenie vety. ■

Teraz už môžeme uviesť nutnú a postačujúcu podmienku existencie inverznej matice.

Veta 5.24. *Pre štvorcovú maticu* $\mathbf{A}$ *existuje inverzná matica* $\mathbf{A^{-1}}$ *práve vtedy, keď* $\mathbf{A}$ *je regulárna.*

Dôkaz:
a) Ak matica $\mathbf{A}$ má inverznú maticu $\mathbf{A^{-1}}$, tak podľa vety 5.23 je $\det\mathbf{A} \neq 0$, čo znamená, že matica $\mathbf{A}$ je regulárna.

b) Nech matica $\mathbf{A}$ je regulárna. Potom podľa tvrdenia vety 5.21 môžeme každú regulárnu maticu upraviť na jednotkovú maticu použitím len elementárnych riadkových operácií. Každá z týchto úprav sa dá realizovať vynásobením matice $\mathbf{A}$ zľava vhodnou elementárnou maticou. To ale znamená, že existujú regulárne matice (elementárne matice sú regulárne!) $\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_i$ také, že

$$\mathbf{B}_i\mathbf{B}_{i-1} \cdot \cdots \cdot \mathbf{B}_1\mathbf{A} = \mathbf{E}.$$

Ak označíme $\mathbf{B} = \mathbf{B}_i\mathbf{B}_{i-1} \cdot \cdots \cdot \mathbf{B}_1$, dostaneme $\mathbf{BA} = \mathbf{E}$. Podľa vety 5.22 je $\mathbf{B} = \mathbf{A}^{-1}$. Dokázali sme existenciu inverznej matice. ■

***Poznámka* 5.17.** *Dôkaz vety bol konštruktívny. Dáva návod, ako inverznú maticu skonštruovať:*
Praktický výpočet inverznej matice k štvorcovej matici $\mathbf{A}$ *stupňa n začneme z blokovej matice* $(\mathbf{A}|\mathbf{E_n})$. *Túto postupne upravujeme Jordanovou eliminačnou metódou – riadkovými elementárnymi operáciami na tvar* $(\mathbf{E_n}|\mathbf{B})$. *Jednotlivé elementárne úpravy možno zapísať ako postupné násobenie matice* $(\mathbf{A}|\mathbf{E_n})$ *štvorcovými maticami* $\mathbf{B_1}, \mathbf{B_2}, \ldots \mathbf{B_k}$, *t. j.*

$$\begin{aligned}(\mathbf{A}|\mathbf{E_n}) \sim \mathbf{B_1}\,(\mathbf{A}|\mathbf{E_n}) \sim \mathbf{B_2B_1}\,(\mathbf{A}|\mathbf{E_n}) \sim \cdots \sim \\ \sim \mathbf{B_kB_{k-1}}\ldots\mathbf{B_2B_1}\,(\mathbf{A}|\mathbf{E_n}) = \\ = (\mathbf{B_kB_{k-1}}\ldots\mathbf{B_2B_1A}|\mathbf{B_kB_{k-1}}\ldots\mathbf{B_2B_1E_n}) = (\mathbf{BA}|\mathbf{BE_n}) = (\mathbf{E_n}|\mathbf{B})\end{aligned}$$

Odtiaľ

$$\begin{aligned}\mathbf{BA} &= \mathbf{E_n} \\ \mathbf{B} &= \mathbf{A^{-1}}.\end{aligned}$$

Pri tomto spôsobe výpočtu inverznej matice nemusíme vopred zisťovať či je matica $\mathbf{A}$ *regulárna. Ak by bola matica* $\mathbf{A}$ *singulárna, v procese výpočtu to odhalíme – ďalšími úpravami sa nedá dosiahnuť jednotková matica. Ak je regulárna, k nej inverznú maticu nájdeme.*

Príklad 5.20. Nájdime inverznú maticu k matici

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

Riešenie:
Napíšeme blokovú maticu $(\mathbf{A}|\mathbf{E_n})$ a tú upravujeme, kým nedostaneme blokovú maticu tvaru $(\mathbf{E_n}|\mathbf{A^{-1}})$.

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ -1 & 2 & 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 3 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 2 & 3 & 1 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & -2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & -1 & 2 \\ 0 & 1 & 0 & -1 & -1 & 3 \\ 0 & 0 & 1 & 1 & 1 & -2 \end{array}\right) \Longrightarrow \mathbf{A}^{-1} = \begin{pmatrix} 0 & -1 & 2 \\ -1 & -1 & 3 \\ 1 & 1 & -2 \end{pmatrix}$$

Uvedieme iný spôsob výpočtu inverznej matice, ktorý je založený na výpočte algebraických doplnkov (pozri definíciu 5.12 na str.119). Je však nepraktický už pre výpočet determinantov štvrtého stupňa.

Veta 5.25. *Pre regulárnu maticu* $\mathbf{A}$ *rádu* n *platí*

$$\mathbf{A^{-1}} = \begin{pmatrix} \frac{A_{11}}{\det\mathbf{A}} & \frac{A_{21}}{\det\mathbf{A}} & \dots & \frac{A_{n1}}{\det\mathbf{A}} \\ \frac{A_{12}}{\det\mathbf{A}} & \frac{A_{22}}{\det\mathbf{A}} & \dots & \frac{A_{n2}}{\det\mathbf{A}} \\ \dots & \dots & \dots & \dots \\ \frac{A_{1n}}{\det\mathbf{A}} & \frac{A_{2n}}{\det\mathbf{A}} & \dots & \frac{A_{nn}}{\det\mathbf{A}} \end{pmatrix} = \frac{1}{\det\mathbf{A}} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}, \tag{5.31}$$

kde A_{ij} *je algebraický doplnok*[1] *prvku* a_{ij} *pre* $i, j = 1, 2, \dots, n$.

[1] Pozri definíciu 5.12 na str. 119.

Dôkaz:
Označme

$$\mathbf{B} = \frac{1}{\det\mathbf{A}} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}, \quad \mathbf{AB} = \mathbf{C} = (c_{ij}).$$

Vzhľadom na vetu 5.22 stačí ukázať, že $\mathbf{C} = \mathbf{E}$. Využijeme vetu 5.12, na základe ktorej pre výpočet prvkov c_{ij}, $i, j = 1, 2, \dots, n$, matice $\mathbf{C}$ platí

$$c_{ij} = \frac{1}{\det\mathbf{A}} \left(a_{i1}A_{j1} + a_{i2}A_{j2} + \dots + a_{in}A_{jn}\right) = \begin{cases} 1 & \text{ak } i = j \\ 0 & \text{ak } i \neq j \end{cases}$$

Teda $\mathbf{C}$ je jednotková matica a $\mathbf{B}$ je inverzná k matici $\mathbf{A}$. ■

Definícia 5.21. Maticu (A_{ji}) nazývame **adjungovanou maticou** k matici $\mathbf{A} = (a_{ij})$, kde A_{ij} sú algebraické doplnky k prvkom a_{ij}.
Označujeme ju adj$\mathbf{A} = (A_{ji})$.

Príklad 5.21. Vypočítajme inverznú maticu k matici

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

Riešenie:
Najskôr vypočítame determinant matice $\mathbf{A}$:

$$\mathbf{A} = \begin{vmatrix} 1 & 0 & -1 \\ 2 & 1 & 0 \\ 3 & 1 & 1 \end{vmatrix} = 1 - 2 + 3 = 2$$

Ďalej vypočítame algebraické doplnky:

$$A_{11} = + \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} = 1 \quad A_{21} = - \begin{vmatrix} 0 & -1 \\ 1 & 1 \end{vmatrix} = -1 \quad A_{31} = + \begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix} = 1$$

$$A_{12} = - \begin{vmatrix} 2 & 0 \\ 3 & 1 \end{vmatrix} = -2 \quad A_{22} = + \begin{vmatrix} 1 & -1 \\ 3 & 1 \end{vmatrix} = 4 \quad A_{32} = - \begin{vmatrix} 1 & -1 \\ 2 & 0 \end{vmatrix} = -2$$

$$A_{13} = + \begin{vmatrix} 2 & 1 \\ 3 & 1 \end{vmatrix} = -1 \quad A_{23} = - \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = -1 \quad A_{33} = + \begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix} = 1$$

Inverznú maticu $\mathbf{A}^{-1}$ zostrojíme využijúc tvrdenie vety 5.25:

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

5.3 Aplikácie

Matice v teórii grafov

Graf je štruktúra pozostávajúca z vrcholov a hrán. Každá **hrana** je určená neusporiadanou dvojicou vrcholov ktoré „spája“. Podľa presnej matematickej definície je graf G usporiadanou dvojicou (V, H) množín, kde V je konečná neprázdna množina a H je množina neusporiadaných dvojíc $\{u, v\}$ takých, že $u \in V$, $v \in V$, $u \neq v$. Množina V sa volá **množina vrcholov grafu** alebo **vrcholová množina grafu** G, množina H sa volá **množina hrán grafu** alebo hranová množina grafu G.

Majme graf $G = (V, H)$, kde $V = \{v_1, v_2, \ldots, v_n\}$. Hranovú množinu H grafu G plne popisuje tzv. **matica susednosti** $\mathbf{S} = \{s_{ij}\}$ typu $n \times n$, pre prvky ktorej platí

$$s_{ij} = \begin{cases} 1, & \text{ak } \{v_i, v_j\} \in H \\ 0, & \text{ak } \{v_i, v_j\} \notin H \end{cases} \tag{5.32}$$

Sled z vrchola u do vrchola v v grafe G je striedavá postupnosť vrcholov a hrán tvaru

$$u = u_1, \{u_1, u_2\}, u_2, \{u_2, u_3\}, u_3, \ldots, u_{k-1}, \{u_{k-1}, u_k\}, u_k = v \tag{5.33}$$

Dĺžkou sledu nazveme počet hrán postupnosti (5.33).

Označme $\mathbf{S^m} = \underbrace{\mathbf{S} \times \mathbf{S} \times \cdots \times \mathbf{S}}_{m-\text{krát}}$. Dá sa ukázať zaujímavý fakt, že v matici $\mathbf{S^m} = \{s_{ij}^{(m)}\}$ sa prvok $s_{ij}^{(m)}$ rovná počtu takých rôznych sledov z v_i do v_j, ktoré majú dĺžku práve m.

Hillovská šifra

Klasická všeobecná monoalfabetická šifra používa ako kľúč permutáciu π znakov abecedy A. Jej princípom je postupné nahrádzanie znaku x_i prameho textu znakom $\pi(x_i)$. Na prvý pohľad nerozlúštiteľná šifra (vzhľadom na obrovské množstvo kľúčov – pre telegrafnú abecedu 26!) sa ukázala slabou – sú proti nej možné efektívne útoky na základe frekvenčnej analýzy jazyka. Tieto útoky využívajú skutočnosť, že jednotlivé znaky, ich dvojice, trojice atď. sa v reálnom jazyku vyskytujú s rôznou relatívnou početnosťou.

Roku 1929 navrhol Lester S. Hill nasledujúcu šifru: Telegrafnú abecedu bez medzery s 26 znakmi stotožnil s okruhom $\mathbb{Z}_{26}$. Ako kľúč bude slúžiť štvorcová regulárna matica

$$\mathbf{K} = \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \dots & \dots & \dots & \dots \\ k_{n1} & b_{n2} & \dots & k_{nn} \end{pmatrix} \tag{5.34}$$

taká, že k nej existuje v $\mathbb{Z}_{26}$ inverzná matica $\mathbf{K}^{-1}$. Šifrovať sa bude naraz n znakov – n-prvkový vektor $\mathbf{x} = [x_1, x_2 \dots, x_n]$ predpisom

$$\mathbf{y} = \mathbf{K}.\mathbf{x} \qquad \text{čiže} \qquad \begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \dots & \dots & \dots & \dots \\ k_{n1} & b_{n2} & \dots & k_{nn} \end{pmatrix} . \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}. \tag{5.35}$$

Priamy text (text určený na zašifrovanie) sa rozdelí na reťazce o n znakoch. Označme tieto reťazce postupne $\mathbf{x_1}, \mathbf{x_2}, \mathbf{x_3}, \dots$. Zašifrovaný text potom bude $\mathbf{y_1} = \mathbf{K}.\mathbf{x_1},\ \mathbf{y_2} = \mathbf{K}.\mathbf{x_2},\ \mathbf{y_3} = \mathbf{K}.\mathbf{x_3},\ \dots$.

Výhodou hillovskej šifry je, že znemožňuje využitie frekvenčnej analýzy na kryptoanalýzu. Jej nevýhodou je, že šifrovacie zobrazenie je lineárne. Ak dostaneme informáciu, že n n-znakových reťazcov $\mathbf{x_1}, \mathbf{x_2}, \dots, \mathbf{x_n}$ prameho textu zodpovedá po rade reťazcom $\mathbf{y_1}, \mathbf{y_2}, \dots, \mathbf{y_n}$ zašifrovaného textu, potom možno písať:

$$(\mathbf{y_1}, \mathbf{y_2}, \dots, \mathbf{y_n}) = \mathbf{K}.(\mathbf{x_1}, \mathbf{x_2}, \dots, \mathbf{x_n}), \tag{5.36}$$

$$\begin{pmatrix} y_{11} & y_{12} & \dots & y_{1n} \\ y_{21} & y_{22} & \dots & y_{2n} \\ \dots & \dots & \dots & \dots \\ y_{n1} & b_{n2} & \dots & y_{nn} \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \dots & \dots & \dots & \dots \\ k_{n1} & b_{n2} & \dots & k_{nn} \end{pmatrix} . \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \dots & \dots & \dots & \dots \\ y_{n1} & b_{n2} & \dots & y_{nn} \end{pmatrix}$$

v maticovom tvare

$$\mathbf{Y} = \mathbf{KX}, \tag{5.37}$$

kde $\mathbf{X} = (\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n})$, $\mathbf{Y} = (\mathbf{y_1}, \mathbf{y_2}, \ldots, \mathbf{y_n})$. Ak k matici $\mathbf{X}$ existuje inverzná matica $\mathbf{X^{-1}}$, potom vynásobením maticovej rovnice (5.37) maticou $\mathbf{X^{-1}}$ sprava dostaneme

$$\mathbf{K} = \mathbf{Y}.\mathbf{X^{-1}}.$$

Práve popísaný útok patrí k útokom typu „known plaintext attack“, kedy kryptoanalytik pozná zodpovedajúce časti priameho a zašifrovaného textu. Pre možnosť takéhoto útoku sa hillovská šifra nepokladá za bezpečnú šifru. Násobenie vektora $\mathbf{x}$ znakov priameho textu regulárnou maticou $\mathbf{K}$ typu $\mathbf{y} = \mathbf{K}.\mathbf{x}$ sa však využíva v niektorých moderných systémoch ako ich súčasť na zabezpečenie rýchlej difúzie[2] informácie po celom šifrovanom bloku – je to tak napríklad pri najnovšom prijatom šifrovacom štandarde AES (Advanced Encryption Standard)[3].

Matice prechodov v markovovských reťazcoch

V teórii komunikačných sietí sa študuje nasledujúci model poruchy spojenia. Spojenie môže byť v dvoch stavoch: stav 1 – spojenie funguje, stav 2 – porucha. Stavy spojenia sa môžu meniť v diskrétnych časových okamihoch $1, 2, \ldots$. Predpokladajme, že podmienená pravdepodobnosť javu, že spojenie bude v čase $t + 1$ v stave j za predpokladu, že v čase t bolo v stave i je p_{ij} – t. j. závisí len od stavu i a nie od predchádzajúcej histórie. Tieto pravdepodobnosti môžeme usporiadať do štvorcovej matice

$$\mathbf{P} = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} \tag{5.38}$$

Zaujíma nás, aká je podmienená pravdepodobnosť $p_{ij}^{(m)}$ javu, že spojenie bude v čase $t + m$ v stave j za predpokladu, že v čase t bolo v stave i. Dá sa ukázať, že

$$\begin{pmatrix} p_{11}^{(m)} & p_{12}^{(m)} \\ p_{21}^{(m)} & p_{22}^{(m)} \end{pmatrix} = \underbrace{P.P.\ldots.P}_{\mathbf{m}\text{-krát}} = \mathbf{P^m} \tag{5.39}$$

[2]Difúziou sa voľne myslí skutočnosť, že každý bit zašifrovaného textu bude závisieť od každého bitu priameho textu.

[3]Moderný symetrický šifrovací algoritmus AES šifruje 128 bitový blok priameho textu na 128-bitový blok zašifrovaného textu.

Analogicky možno popísať i systémy o n stavoch štvorcovou maticou podmienených pravdepodobností a študovať ako sa bude systém v čas správať.

Často sa hľadá tzv. stacionárne rozdelenie pravdepodobností jednotlivých stavov $\mathbf{p} = (p_1, p_2, \ldots, p_n)^T$, do ktorého sa systém ustáli po dlhom čase. Pre vektor $\mathbf{p}$ musí platiť

$$\mathbf{p}^T.\mathbf{P} = \mathbf{p}^T \tag{5.40}$$

Cvičenia

1. Dokážte, že matice $\mathbf{E}_{pq}$ definované vzťahom (5.6) sú lineárne nezávislé.
2. Nech

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & -2 \\ 4 & 3 & 7 \\ 6 & 5 & 0 \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} 1 & -2 & 0 \\ 2 & 3 & 1 \\ -1 & 2 & 0 \end{pmatrix},$$

   a) vypočítajte $3\mathbf{A} - \mathbf{B}$,
   b) vypočítajte $(\mathbf{A} + \mathbf{B})^T$,
   c) vypočítajte $\mathbf{AB}$, $\mathbf{BA}$,
   d) každú z matíc $\mathbf{A}$, $\mathbf{B}$ vyjadrite ako súčet symetrickej a antisymetrickej matice,
   e) vyjadrite maticu $\mathbf{B}$ ako lineárnu kombináciu matíc $\mathbf{E}_{pq}$.

3. Akú algebraickú štruktúru tvoria tvoria všetky diagonálne matice n-tého stupňa nad poľom reálnych čísel vzhľadom na operácie sčítanie a násobenie matíc ?
4. Pre prirodzené číslo n vypočítajte $\mathbf{A^n}$, keď

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

5. Tvoria matice typu

$$\begin{pmatrix} a+b & 2b \\ 2a & a-b \end{pmatrix},$$

   kde a, b sú reálne čísla, vektorový priestor nad poľom reálnych čísel vzhľadom na operácie sčítania matíc a násobenia matice skalárom? Ak áno,

určte jeho dimenziu a nájdite nejakú jeho bázu. Aké súradnice bude mať matica

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

v tejto báze?

6. Napíšte všetky permutácie množiny $A = \{1, 2, 3\}$ a zostrojte multiplikatívnu tabuľku vzhľadom na operáciu skladania permutácií, ktorá bola definovaná vzťahom (5.11). Dokážte, že $(A, \circ)$ tvorí nekomutatívnu grupu.

7. Určte počet inverzií a paritu permutácie:

   a)
   $$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 4 & 1 & 5 \end{pmatrix},$$

   b)
   $$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & \dots & n-2 & n-1 & n \\ 3 & 4 & 5 & \dots & n & 1 & 2 \end{pmatrix},\ n \geq 3.$$

8. Nájdite všetky čísla $i, j, k \in \{1, 2, 3, 4, 5, 6, 7\}$ tak, aby súčin

   $$a_{21}a_{33}a_{7i}a_{5j}a_{6k}a_{16}a_{45}$$

   vystupoval v det$\mathbf{A}$ so znamienkom $+$.

9. Vypočítajte:

   $a)$ $\begin{vmatrix} 1 & 2 & -3 & 4 \\ 0 & -1 & -2 & 0 \\ 3 & 1 & -1 & 2 \\ 4 & 0 & 1 & 3 \end{vmatrix}$ $b)$ $\begin{vmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{vmatrix}$ $c)$ $\begin{vmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{vmatrix}$

10. Vypočítajte matice stupňa $n > 1$:

    $a)$ $\begin{vmatrix} 1^2 & 1 & 1 & \dots & 1 \\ 2 & 2^2 & 2 & \dots & 2 \\ \dots & \dots & \dots & \dots & \dots \\ n & n & n & \dots & n^n \end{vmatrix}$ $b)$ $\begin{vmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 4 & \dots & n+1 \\ \dots & \dots & \dots & \dots & \dots \\ n & n+1 & n+2 & \dots & 2n-1 \end{vmatrix}$

$$c)\ \begin{vmatrix} b & b & \dots & b & b \\ a & b & \dots & b & b \\ \dots & \dots & \dots & \dots & \dots \\ a & a & \dots & b & b \\ a & a & \dots & a & b \end{vmatrix} \qquad d)\ \begin{vmatrix} 1 & 2 & 3 & \dots & n-2 & n-1 & n \\ 2 & 3 & 4 & \dots & n-1 & n & n \\ 3 & 4 & 5 & \dots & n & n & n \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ n & n & n & \dots & n & n & n \end{vmatrix}$$

11. Laplaceovým rozvojom vypočítajte determinant matice nad poľom $(\mathbb{Z}_7, \oplus_7, \otimes_7)$:

$$a)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} \quad b)\ \begin{pmatrix} 5 & 1 & 3 & 2 & 4 \\ 3 & 3 & 2 & 1 & 3 \\ 4 & 2 & 3 & 5 & 6 \\ 2 & 1 & 3 & 2 & 2 \\ 4 & 3 & 1 & 5 & 1 \end{pmatrix} \quad c)\ \begin{pmatrix} 2 & 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 & 1 \\ 1 & 1 & 4 & 1 & 1 \\ 1 & 1 & 1 & 5 & 1 \\ 1 & 1 & 1 & 1 & 6 \end{pmatrix}$$

12. Nájdite hodnosť matice:

$$a)\ \begin{pmatrix} 1 & -4 & -2 & 2 \\ 2 & 1 & -1 & 1 \\ 2 & -2 & -2 & 2 \\ 4 & 1 & -3 & 3 \end{pmatrix} \quad b)\ \begin{pmatrix} 2 & 7 & 3 & 1 \\ 1 & 3 & 5 & -2 \\ 2 & 8 & -4 & 6 \\ 5 & 18 & 4 & 5 \end{pmatrix} \quad c)\ \begin{pmatrix} 3 & -1 & -2 & 1 \\ 9 & -3 & 4 & 8 \\ 3 & -1 & 2 & 3 \\ 3 & 1 & 4 & 4 \end{pmatrix}$$

13. Pre akú hodnotu parametra a sa hodnosť matice $\mathbf{A}$ rovná jej stupňu?

$$a)\quad \mathbf{A} = \begin{pmatrix} 1 & a & -1 & 1 \\ 0 & 2 & 1 & 1 \\ a & 3 & 1 & 0 \\ 1 & 1 & -1 & 0 \end{pmatrix} \qquad b)\quad \mathbf{A} = \begin{pmatrix} a & 1 & 0 & a \\ 1 & a & a & 0 \\ 0 & a & a & 1 \\ a & 0 & 1 & a \end{pmatrix}$$

14. Pomocou adjungovanej matice nájdite inverznú maticu k matici:

$$a)\quad \mathbf{A} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 1 & 3 & 4 \\ 2 & -1 & 2 & 3 \end{pmatrix} \qquad b)\quad \mathbf{A} = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 3 & 1 & 1 & 1 \\ 4 & 3 & 2 & 1 \\ 5 & 4 & 3 & 2 \end{pmatrix}$$

15. Využitím inverznej matice (ak existuje) riešte rovnicu $\mathbf{XA} + \mathbf{2B} = \mathbf{C}$, ak:

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \\ 2 & 1 & -2 \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} 2 & 1 & 0 \\ 3 & -4 & 7 \\ 4 & 2 & 3 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & -1 & 2 \\ 3 & 1 & 1 \\ 4 & 2 & 3 \end{pmatrix}$$

16. Nad poľom $(\mathbb{Z}_5, \oplus_5, \otimes_5)$ nájdite inverznú maticu k danej matici:

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

Kapitola 6

Systémy lineárnych rovníc

Jednou z klasických úloh matematiky, s ktorou sa stretávame už od základnej školy, je riešenie systému rovníc. Aj my sme sa už v predchádzajúcich častiach pri úlohách o riešení lineárnej nezávislosti vektorov, ale aj iných úlohách z kapitoly o vektorových priestoroch, stretli so systémami rovníc. Napr. sme riešili úlohu: Nájdime súradnice vektora $\mathbf{b} \in V_m(\mathcal{P})$ v báze $\mathcal{B} = \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$, keď $\mathbf{a}_i \in V_m(\mathcal{P})$ pre $i = 1, 2, \ldots, n$. Súradnice vektora $\mathbf{b}$ v báze $\mathcal{B}$ sú koeficienty lineárnej kombinácie

$$\mathbf{b} = x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \cdots + x_n\mathbf{a}_n. \tag{6.1}$$

Ak $\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{im})$ pre $i = 1, 2, \ldots, n$ a $\mathbf{b} = (b_1, b_2, \ldots, b_m)$, lineárnu kombináciu (6.1) môžeme písať v tvare

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{array} \tag{6.2}$$

Systém (6.2) nazývame **systémom** alebo **sústavou** m **lineárnych rovníc o** n **neznámych** $x_1, x_2, \ldots, x_n$. **Riešením systému rovníc** sa nazýva každá usporiadaná n-tica $(u_1, u_2, \ldots, u_n)$ prvkov z poľa $\mathcal{P}$ taká, že po dosadení u_i za x_i do systému (6.2) dostaneme m rovností, resp. identít. Riešiť systém rovníc (6.2) znamená nájsť všetky takéto n-tice.

Ku každému systému (6.2) lineárnych rovníc je možné priradiť dve matice:

a) Maticu skladajúcu sa z koeficientov pri neznámych

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \tag{6.3}$$

ktorú nazývame **maticou systému** (6.2).

b) Maticu, ktorú dostaneme z matice $\mathbf{A}$ tak, že k nej pridáme stĺpec pravých strán rovníc zo systému (6.2)

$$\widetilde{\mathbf{A}} = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right). \tag{6.4}$$

Maticu $\widetilde{\mathbf{A}}$ nazývame **rozšírenou maticou systému** (6.2).

Označme $\mathbf{A} = \left(a_{ij}\right)_{m\times n}$, $\mathbf{b} = (b_1, b_2, \dots, b_m)^T$, $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$. Systém (6.2) môžeme v maticovom tvare zapísať nasledujúco:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} . \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{pmatrix}$$

a skrátene

$$\mathbf{A}.\mathbf{x} = \mathbf{b} \tag{6.5}$$

V zmysle tohto zápisu nájsť riešenie systému rovníc (6.2), znamená nájsť všetky vektory $\mathbf{u} \in V_n(\mathcal{P})$, pre ktoré je $\mathbf{A}.\mathbf{u} = \mathbf{b}$.

Systém (6.2), resp. (6.5) nazveme **homogénny**, ak $\mathbf{b} = \mathbf{o}$. Inak je systém rovníc (6.2), resp. (6.5) **nehomogénny**.

Definícia 6.1. Dva systémy rovníc $\mathbf{Ax} = \mathbf{b}$, $\mathbf{Cx} = \mathbf{d}$ o rovnakom počte neznámych sa nazývajú **ekvivalentné**, ak majú rovnaké množiny riešení.

***Poznámka* 6.1.** *Ekvivalentné systémy nemusia mať rovnaký počet rovníc.*

Hlavnými problémami, ktorými sa budeme v tejto kapitole zaoberať, bude riešiteľnosť systémov a metódy hľadania riešení. Rozhodujúcu úlohu bude mať pri tom nasledujúca veta.

Veta 6.1. *Ak rozšírené matice dvoch systémov lineárnych rovníc sú riadkovo ekvivalentné, tak systémy majú rovnakú množinu riešení.*

Dôkaz:
Triviálny. Stačí ukázať, že ak na rozšírenej matici systému vykonáme niektorú z elementárnych riadkových operácií, nezmení sa množina riešení systému. ■

***Poznámka* 6.2.** *Podstata postupu riešenia systému lineárnych rovníc* $\mathbf{A}.\mathbf{x} = \mathbf{b}$ *spočíva v jeho úprave na systém* $\mathbf{C}.\mathbf{x} = \mathbf{d}$*, ktorý už riešiť vieme a jeho riešenie bude aj riešením pôvodného systému. Vo vete 6.1 hovoríme o elementárnych riadkových operáciách. Samozrejme je možné použiť aj výmenu stĺpcov matice systému, ale treba si zapamätať, že s touto úpravou súvisí aj zmena poradia premenných.*

Nutnú a postačujúcu podmienku riešiteľnosti systému lineárnych rovníc dáva nasledujúca veta.

Veta 6.2 (Frobeniova veta)**.** *Systém lineárnych rovníc o n neznámych*

$$\mathbf{A}\mathbf{x} = \mathbf{b}$$

má riešenie práve vtedy, keď hodnosť matice systému sa rovná hodnosti rozšírenej matice systému a platí

a) Ak $h(\mathbf{A}) = h(\widetilde{\mathbf{A}}) = n$*, potom má systém práve jedno riešenie.*

b) Ak $h(\mathbf{A}) = h(\widetilde{\mathbf{A}}) = k < n$*, potom má systém nekonečne veľa riešení, pričom* $n - k$ *neznámych je ľubovoľne voliteľných.*

Dôkaz:
Dôkaz vychádza z prevodu rozšírenej matice systému lineárnych rovníc $(\mathbf{A}|\mathbf{b})$ na tvar $(\mathbf{C}|\mathbf{d})$. Uvažujme najskôr systém lineárnych rovníc $(\mathbf{A}|\mathbf{b})$, ktorý má rozšírenú maticu

$$\widetilde{\mathbf{A}} = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right).$$

Pomocou elementárnych riadkových operácií (príp. výmenou stĺpcov) Jordanovou eliminačnou metódou upravíme maticu $\widetilde{\mathbf{A}}$ na maticu $\widetilde{\mathbf{C}}$, pričom hodnosť upravenej matice sa nezmení, t. j. $h(\widetilde{\mathbf{C}}) = h(\widetilde{\mathbf{A}})$.

$$\widetilde{\mathbf{C}} = \left(\begin{array}{ccccccc|c} c_{11} & 0 & \dots & 0 & c_{1,k+1} & \dots & c_{1n} & d_1 \\ 0 & c_{22} & 0\dots & 0 & c_{1,k+1} & \dots & c_{2n} & d_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0\dots & c_{kk} & c_{k,k+1} & \dots & c_{kn} & d_k \\ 0 & 0 & 0\dots & 0 & 0 & \dots & 0 & d_{k+1} \\ 0 & 0 & 0\dots & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0\dots & 0 & 0 & \dots & 0 & 0 \end{array}\right). \tag{6.6}$$

Predpokladajme, že sme pri Jordanovej eliminácii použili len riadkové operácie. Keďže $\widetilde{\mathbf{C}} \sim \widetilde{\mathbf{A}}$, systémy $(\mathbf{A}|\mathbf{b})$ a $(\mathbf{C}|\mathbf{d})$ majú rovnakú množinu riešení a riešenie systému nájdeme použijúc maticu $\widetilde{\mathbf{C}}$. Vzhľadom na prvok d_{k+1} môžu nastať dva prípady:
a) Nech $d_{k+1} \neq 0$. Potom $(k+1)$-vá rovnica má tvar

$$0x_1 + 0x_2 + \cdots + 0x_n = d_{k+1} \neq 0,$$

čo je spor. Platí $k = h(\mathbf{C}) < h(\widetilde{\mathbf{C}}) = k+1$, systém nemá riešenie.
b) Nech $d_{k+1} = 0$. Potom $k = h(\mathbf{C}) = h(\widetilde{\mathbf{C}})$. Budeme rozlišovať dva prípady: Ak $k = n$, potom výsledná matica $\widetilde{\mathbf{C}}$ má tvar

$$\widetilde{\mathbf{C}} = \left(\begin{array}{cccc|c} c_{11} & 0 & \dots & 0 & d_1 \\ 0 & c_{22} & 0\dots & 0 & d_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0\dots & c_{nn} & d_n \end{array}\right),$$

odkiaľ dostávame pre $i = 1, 2, \dots, n$ jednoznačne dané riešenie

$$x_i = \frac{d_i}{c_{ii}}.$$

Ak $k < n$, potom má matica $\widetilde{\mathbf{C}}$ po vynechaní posledných nulových riadkov tvar

$$\widetilde{\mathbf{C}} = \left(\begin{array}{ccccccc|c} c_{11} & 0 & \dots & 0 & c_{1,k+1} & \dots & c_{1n} & d_1 \\ 0 & c_{22} & 0\dots & 0 & c_{1,k+1} & \dots & c_{2n} & d_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0\dots & c_{kk} & c_{k,k+1} & \dots & c_{kn} & d_k \end{array}\right),$$

potom i-ta rovnica systému prislúchajúcemu k upravenej matici $\widetilde{\mathbf{C}}$ je

$$c_{ii}x_i + c_{i,k+1}x_{k+1} + \cdots + c_{in}x_n = d_i.$$

Každú premennú x_i pre $i = 1, 2, \ldots, k$ môžeme vyjadriť pomocou premenných $x_{k+1}, x_{k+2}, \ldots, x_n$ nasledujúco

$$x_i = \frac{d_i}{c_{ii}} - \frac{c_{i,k+1}}{c_{ii}} x_{k+1} - \frac{c_{i,k+2}}{c_{ii}} x_{k+2} - \cdots - \frac{c_{i,n}}{c_{ii}} x_n \tag{6.7}$$

Na určenie n neznámych zostalo po úprave k podmienok, pričom $k < n$. To znamená, že neznáme nemôžu byť určené jednoznačne. Vznikla určitá voľnosť tým, že chýba $(n - k)$ ďalších podmienok na jednoznačné určenie riešenia. Za neznáme $x_{k+1}, x_{k+2}, \ldots, x_n$ volíme ľubovoľné $t_1, t_2, \ldots, t_{n-k}$ a k nim potom jednoznačne dopočítame hodnoty premenných $x_1, x_2, \ldots, x_k$ podľa posledne uvedených vzťahov (6.7). Systém má nekonečne veľa riešení. ■

Na ozrejmenie vyslovenej teórie uvedieme príklady.

Príklad 6.1. Riešme systém lineárnych rovníc

$$\begin{aligned} x_1 + \ x_2 + 3x_3 &= 1 \\ 2x_1 + \ x_2 - 2x_3 &= 1 \\ x_1 + \ x_2 + \ x_3 &= 3 \\ x_1 + 2x_2 - 3x_3 &= 1 \end{aligned}$$

Riešenie:
K danému systému rovníc napíšeme rozšírenú maticu a tú budeme pomocou elementárnych riadkových operácií upravovať Gaussovou eliminačnou metódou na trojuholníkový tvar. V matici $\widetilde{\mathbf{A}}$ vynásobíme prvý riadok najskôr číslom (-2) a pripočítame k druhému riadku a potom (-1)-násobok prvého riadku postupne pripočítame k tretiemu a štvrtému riadku. V matici $\widetilde{\mathbf{A_1}}$ pripočítame druhý riadok k poslednému riadku a nakoniec v matici $\widetilde{\mathbf{A_2}}$ (-7)-násobok tretieho riadku pripočítame k poslednému riadku. Dostali sme tak postupnosť ekvivalentných matíc

$$\widetilde{\mathbf{A}} = \left(\begin{array}{rrr|r} 1 & 1 & 3 & 1 \\ 2 & 1 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ 1 & 2 & -3 & 1 \end{array}\right) \sim \widetilde{\mathbf{A_1}} = \left(\begin{array}{rrr|r} 1 & 1 & 3 & 1 \\ 0 & -1 & -8 & -1 \\ 0 & 0 & -2 & 2 \\ 0 & 1 & -6 & 0 \end{array}\right) \sim$$

$$\sim \widetilde{\mathbf{A_2}} = \left(\begin{array}{rrr|r} 1 & 1 & 3 & 1 \\ 0 & -1 & -8 & -1 \\ 0 & 0 & -2 & 2 \\ 0 & 0 & -14 & -1 \end{array}\right) \sim \widetilde{\mathbf{A_3}} = \left(\begin{array}{rrr|r} 1 & 1 & 3 & 1 \\ 0 & -1 & -8 & -1 \\ 0 & 0 & -2 & 2 \\ 0 & 0 & 0 & -15 \end{array}\right)$$

Matica $\widetilde{\mathbf{A_3}}$ je už upravená na trojuholníkový tvar a vidíme, že $h(\mathbf{A}) = 3$, $h(\widetilde{\mathbf{A}}) = 4$, to znamená, že systém nemá riešenie.

Príklad 6.2. Nájdime riešenie systému lineárnych rovníc Jordanovou eliminačnou metódou.

$$\begin{aligned} x_1 + x_2 - 3x_3 - 2x_4 &= 1 \\ 3x_1 - x_2 - x_3 - 10x_4 &= -9 \\ x_1 - 3x_2 + 5x_3 - 6x_4 &= -11 \\ -x_1 - 5x_2 + 11x_3 - 2x_4 &= -13 \end{aligned}$$

Riešenie:
Rozšírenú maticu sústavy najskôr upravíme na hornú trojuholníkovú maticu Gaussovou eliminačnou metódou a následne dokončíme na tvar požadovaný pri Jordanovej eliminačnej metóde. Dostávame postupnosť ekvivalentných matíc:

$$\widetilde{\mathbf{A}} = \left(\begin{array}{cccc|c} 1 & 1 & -3 & -2 & 1 \\ 3 & -1 & -1 & -10 & -9 \\ 1 & -3 & 5 & -6 & -11 \\ -1 & -5 & 11 & -2 & -13 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & -3 & -2 & 1 \\ 0 & -4 & 8 & -4 & -12 \\ 0 & -4 & 8 & -4 & -12 \\ 0 & -4 & 8 & -4 & -12 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 1 & 1 & -3 & -2 & 1 \\ 0 & -4 & 8 & -4 & -12 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & -3 & -2 & 1 \\ 0 & 1 & -2 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 1 & 0 & -1 & -3 & -2 \\ 0 & 1 & -2 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \Longrightarrow h(\mathbf{A}) = 2 = h(\widetilde{\mathbf{A}}) < 4 = n$$

Systém má nekonečne veľa riešení. Z poslednej matice napíšeme systém rovníc ekvivalentný s pôvodným systémom:

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

Zvolíme dva parametre: $x_3 = t_1$, $x_4 = t_2$ a premenné x_1 a x_2 vyčíslime v závislosti od zvolených parametrov: $x_1 = -2 + t_1 + 3t_2$, $x_2 = 3 + 2t_1 - t_2$. Ak označíme $\mathbf{x} = (x_1, x_2, x_3, x_4)^T$, výsledok môžeme zapísať v tvare:

$$\mathbf{x} = (-2 + t_1 + 3t_2,\ 3 + 2t_1 - t_2,\ t_1,\ t_2)^T = \\ = (-2, 3, 0, 0,)^T + t_1(1, 2, 1, 0)^T + t_2(3, -1, 0, 1)^T, \quad t_1, t_2 \in \mathbb{R}$$

Príklad 6.3. Gaussovou eliminačnou metódou riešme systém lineárnych rovníc

$$\begin{aligned} -x_1 \qquad + 3x_3 &= 17 \\ 2x_1 - x_2 + 2x_3 &= 4 \\ 3x_1 + x_2 + x_3 &= 1 \end{aligned}$$

Riešenie:
Uskutočnením elementárnych riadkových operácií dostávame postupnosť ekvivalentných matíc

$$\widetilde{\mathbf{A}} = \left(\begin{array}{rrr|r} -1 & 0 & 3 & 17 \\ 2 & -1 & 2 & 4 \\ 3 & 1 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{rrr|r} -1 & 0 & 3 & 17 \\ 0 & -1 & 8 & 38 \\ 0 & 1 & 10 & 52 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{rrr|r} -1 & 0 & 3 & 17 \\ 0 & -1 & 8 & 38 \\ 0 & 0 & 18 & 90 \end{array}\right) \Longrightarrow h(\mathbf{A}) = 3 = h(\widetilde{\mathbf{A}}) = n$$

Systém má jediné riešenie, ktoré dostaneme vyriešením ekvivalentného systému

$$\begin{aligned} -x_1 \qquad + 3x_3 &= 17 \\ - x_2 + 8x_3 &= 38 \\ 18x_3 &= 90 \end{aligned}$$

Z poslednej rovnice dostaneme $x_3 = 5$. Dosadením do druhej a prvej rovnice dostaneme $x_2 = 2$ a $x_1 = -2$, t. j. $\mathbf{x} = (-2, 2, 5)^T$.

6.0.1 Homogénny systém lineárnych rovníc

V ďalšom budeme študovať homogénne systémy lineárnych rovníc. Homogénny systém m lineárnych rovníc o n premenných nad poľom $\mathcal{P}$ má tvar:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= 0 \end{aligned} \tag{6.8}$$

Na rozdiel od nehomogénneho systému lineárnych rovníc, má systém (6.8) vždy riešenie. Nie je ťažké presvedčiť sa, že n-tica $(0, 0, \ldots, 0) \in V_n(\mathcal{P})$ je riešením každého homogénneho systému. Takéto riešenie sa nazýva **triviálne riešenie**. Každé iné riešenie sa nazýva **netriviálne riešenie**.

Veta 6.3. *Nech U je množina všetkých riešení systému* (6.8)*. Potom U je vektorový podpriestor priestoru $V_n(\mathcal{P})$.*

Dôkaz:
Podľa vety 4.2 stačí ukázať neprázdnosť množiny U a jej uzavretosť na operáciu sčítania jej prvkov a násobenie jej prvku skalárom. U je neprázdna množina, lebo systém (6.8) má aspoň triviálne riešenie. Treba dokázať, že ak $\mathbf{a}, \mathbf{b} \in U$, potom aj $(\mathbf{a} + \mathbf{b}) \in U$. Ak $\mathbf{a}, \mathbf{b} \in U$, tak $\mathbf{A} \cdot \mathbf{a} = \mathbf{o}$, $\mathbf{A} \cdot \mathbf{b} = \mathbf{o}$. Pre matice platí distributívny zákon, takže platí aj

$$\mathbf{A} \cdot (\mathbf{a} + \mathbf{b}) = \mathbf{A} \cdot \mathbf{a} + \mathbf{A} \cdot \mathbf{b} = \mathbf{o}.$$

To znamená, že $\mathbf{a} + \mathbf{b}$ je riešením systému (6.8). Podobne dokážeme, ak $\mathbf{a} \in U$ a $c \in P$, tak aj $c \cdot \mathbf{a} \in U$. Pre matice platí

$$\mathbf{A} \cdot (c \cdot \mathbf{a}) = c \cdot (\mathbf{A} \cdot \mathbf{a}) = \mathbf{o},$$

teda $c \cdot \mathbf{a}$ je riešením (6.8). ■

Riešením homogénneho systému lineárnych rovníc sa zaoberá nasledujúca veta.

Veta 6.4. *Homogénny systém m lineárnych rovníc o n neznámych*

$$\mathbf{A}\mathbf{x} = \mathbf{o} \tag{6.9}$$

má vždy aspoň jedno riešenie (tzv. triviálne riešenie) $\mathbf{x} = \mathbf{o} = (0, 0, \ldots, 0)^T$. Pritom platí:

a) Ak $h(\mathbf{A}) = n$, potom má tento systém iba triviálne riešenie.

b) Ak $h(\mathbf{A}) = k < n$, potom má tento systém nekonečne veľa riešení, ktoré tvoria $(n - k)$-dimenzionálny podpriestor vektorového priestoru $V_n(\mathcal{P})$.

Dôkaz:
Ľahko sa overí, že $\mathbf{x} = \mathbf{o}$ je riešením systému (6.9). Analogicky ako v dôkaze Frobeniovej vety rozšírenú maticu $(\mathbf{A}|\mathbf{o})$ systému (6.9) možno upraviť Jordanovou

eliminačnou metódou a následným vynechaním nulových riadkov na tvar

$$\widetilde{\mathbf{C}} = \left(\begin{array}{ccccccc|c} c_{11} & 0 & \dots & 0 & c_{1,k+1} & \dots & c_{1n} & 0 \\ 0 & c_{22} & 0\dots & 0 & c_{1,k+1} & \dots & c_{2n} & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & 0\dots & c_{kk} & c_{k,k+1} & \dots & c_{kn} & 0 \end{array}\right), \tag{6.10}$$

pričom $\mathbf{A} \sim \widetilde{\mathbf{C}}$, $h(\mathbf{A}) = h(\widetilde{\mathbf{C}}) = k$. Ak $k = n$, matica (6.10) má tvar

$$\widetilde{\mathbf{C}} = \left(\begin{array}{cccc|c} c_{11} & 0 & \dots & 0 & 0 \\ 0 & c_{22} & 0\dots & 0 & 0 \\ \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & 0\dots & c_{nn} & 0 \end{array}\right) \tag{6.11}$$

odkiaľ vyplýva, že jediným riešením systému (6.9) je $\mathbf{x} = \mathbf{o}$. Ak $k < n$, potom má matica $\widetilde{\mathbf{C}}$ tvar

$$\widetilde{\mathbf{C}} = \left(\begin{array}{ccccccc|c} c_{11} & 0 & \dots & 0 & c_{1,k+1} & \dots & c_{1n} & 0 \\ 0 & c_{22} & 0\dots & 0 & c_{1,k+1} & \dots & c_{2n} & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & 0\dots & c_{kk} & c_{k,k+1} & \dots & c_{kn} & 0 \end{array}\right) \tag{6.12}$$

Predpokladajme, že sme pri Jordanovej eliminácii používali len riadkové operácie. Potom z tvaru matice $\widetilde{\mathbf{C}}$ vyplýva, že i-ta rovnica má tvar

$$c_{ii}x_i + c_{i,k+1}x_{k+1} + c_{i,k+2}x_{k+2} + \dots + c_{in}x_n = 0$$

pre $i = 1, 2, \dots, k$, potom dostávame riešenie

$$x_i = -\frac{c_{i,k+1}}{c_{ii}}x_{k+1} - \frac{c_{i,k+2}}{c_{ii}}x_{k+2} - \dots - \frac{c_{i,n}}{c_{ii}}x_n \tag{6.13}$$

Položíme $x_{k+1} = t_1,\ x_{k+2} = t_2,\ \dots,\ x_n = t_{n-k}$, kde každé t_i je ľubovoľne voliteľné. Hodnoty premenných $x_1, x_2, \dots, x_k$ k nim potom jednoznačne dopočítame podľa vzťahov (6.13). ■

Poznámka 6.3. *Označme* $g_{ij} = -c_{ij}/c_{ii}$ *pre* $i = 1, 2, \ldots, k,\ j = k+1, k+2, \ldots, n$. *Potom riešenie systému* $\mathbf{Ax} = \mathbf{o}$ *má tvar:*

$$\begin{array}{rcccccccc} x_1 & = & g_{1,k+1}t_1 & + & g_{1,k+2}t_2 & + & \ldots & + & g_{1n}t_{n-k} \\ x_2 & = & g_{2,k+1}t_1 & + & g_{2,k+2}t_2 & + & \ldots & + & g_{2n}t_{n-k} \\ \multicolumn{9}{c}{\dotfill} \\ x_k & = & g_{k,k+1}t_1 & + & g_{k,k+2}t_2 & + & \ldots & + & g_{kn}t_{n-k} \\ x_{k+1} & = & t_1 & & & & & & \\ x_{k+2} & = & & & t_2 & & & & \\ \multicolumn{9}{c}{\dotfill} \\ x_n & = & & & & & \ldots & & t_{n-k} \end{array}$$

Ak položíme $t_1 = 1, t_2 = t_3 = \cdots = t_{n-k} = 0$, *dostaneme tak jedno riešenie systému* (6.8)

$$\mathbf{r_1} = (g_{1,k+1}, g_{2,k+1}, \ldots, g_{k,k+1}, 1, 0, \ldots, 0)^T.$$

Podobne, ak položíme $t_1 = 0, t_2 = 1, t_3 = \cdots = t_{n-k} = 0$, *dostaneme ďalšie riešenie*

$$\mathbf{r_2} = (g_{1,k+2}, g_{2,k+2}, \ldots, g_{k,k+2}, 0, 1, 0, \ldots, 0)^T,$$

atď. Nakoniec položíme $t_1 = t_2 = \cdots = t_{n-k+1} = 0, t_{n-k} = 1$ *a dostaneme*

$$\mathbf{r_{n-k}} = (g_{1,k+2}, g_{2,k+2}, \ldots, g_{k,k+2}, 0, 0, \ldots, 0, 1)^T.$$

Je zrejmé, že $\mathbf{r_1}, \mathbf{r_2}, \ldots, \mathbf{r_{n-k}}$ *sú lineárne nezávislé riešenia. Keďže každé riešenie* $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ *systému* (6.8) *sa dá vyjadriť v tvare*

$$\mathbf{x} = t_1\mathbf{r_1} + t_2\mathbf{r_2} + \cdots + t_{n-k}\mathbf{r}_{n-k},$$

$\mathbf{r_1}, \mathbf{r_2}, \ldots, \mathbf{r_{n-k}}$ *tvoria bázu vektorového priestoru všetkých riešení systému, ktorý má dimenziu* $(n-k)$.

Príklad 6.4. Jordanovou eliminačnou metódou riešme sústavu rovníc

$$\begin{aligned} 2x_1 + x_2 - 4x_3 &= 0 \\ 6x_1 + 5x_2 - 8x_3 &= 0 \\ 4x_1 - 5x_2 - 6x_3 &= 0 \end{aligned}$$

Riešenie:
Uvedieme len východiskovú a výslednú maticu, Výpočet ponecháme čitateľovi.

$$\mathbf{A} = \left(\begin{array}{rrr|r} 2 & 1 & -4 & 0 \\ 6 & 5 & -8 & 0 \\ 4 & -5 & -6 & 0 \end{array}\right) \sim \cdots \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

Nakoľko $h(\mathbf{A}) = 3 = n$, systém má len jediné riešenie $\mathbf{x} = (0, 0, \ldots, 0)^T$.

Príklad 6.5. Nájdime riešenie homogénneho systému lineárnych rovníc

$$\begin{aligned} x_1 + x_2 - 3x_3 - 2x_4 &= 0 \\ 3x_1 - x_2 - x_3 - 10x_4 &= 0 \\ x_1 - 3x_2 + 5x_3 - 6x_4 &= 0 \\ -x_1 - 5x_2 + 11x_3 - 2x_4 &= 0 \end{aligned}$$

Riešenie:
Opäť uvedieme len východiskovú a finálnu maticu.

$$\widetilde{\mathbf{A}} = \left(\begin{array}{cccc|c} 1 & 1 & -3 & -2 & 0 \\ 3 & -1 & -1 & -10 & 0 \\ 1 & -3 & 5 & -6 & 0 \\ -1 & -5 & 11 & -2 & 0 \end{array}\right) \sim \cdots \sim \left(\begin{array}{cccc|c} 1 & 0 & -1 & -3 & 0 \\ 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Dostali sme ekvivalentný systém lineárnych rovníc

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

Položíme $x_3 = t_1,\ x_4 = t_2$ a dostaneme riešenie $x_1 = t_1 + 3t_2,\ x_2 = 2t_1 - t_2$, ktoré zapíšeme

$$\mathbf{x} = (t_1 + 3t_2, 2t_1 - t_2, t_1, t_2)^T = t_1(1, 2, 1, 0)^T + t_2(3, -1, 0, 1)^T,\ t_1, t_2 \in \mathbb{R}$$

Pozorný čitateľ postrehol, že s "podobným" riešením sme sa už stretli. V príklade 6.2 sme riešili sústavu

$$\begin{aligned} x_1 + x_2 - 3x_3 - 2x_4 &= 1 \\ 3x_1 - x_2 - x_3 - 10x_4 &= -9 \\ x_1 - 3x_2 + 5x_3 - 6x_4 &= -11 \\ -x_1 - 5x_2 + 11x_3 - 2x_4 &= -13 \end{aligned}$$

Pri riešení sme postupovali Jordanovou eliminačnou metódou s nasledujúcimi výsledkami:

$$\widetilde{\mathbf{A}} = \left(\begin{array}{cccc|c} 1 & 1 & -3 & -2 & 1 \\ 3 & -1 & -1 & -10 & -9 \\ 1 & -3 & 5 & -6 & -11 \\ -1 & -5 & 11 & -2 & -13 \end{array}\right) \sim \cdots \sim \left(\begin{array}{cccc|c} 1 & 0 & -1 & -3 & -2 \\ 0 & 1 & -2 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$$\mathbf{x} = (-2 + t_1 + 3t_2,\ 3 + 2t_1 - t_2,\ t_1,\ t_2)^T = \\ = (-2, 3, 0, 0,)^T + t_1(1, 2, 1, 0)^T + t_2(3, -1, 0, 1)^T, \quad t_1, t_2 \in \mathbb{R} \quad (6.14)$$

Vidíme, že riešenie nehomogénneho systému sa dá vyjadriť ako súčet riešenia homogénneho systému a nejakého konkrétneho riešenia nehomogénneho systému. Je to spôsobené tým, že oba systémy majú rovnakú maticu systému, a teda pri ich úprave je možné použiť tie isté elementárne operácie. Keďže výsledné riešenie je zložené z dvoch riešení, hovoríme o **skladaní (resp. superpozícii) riešení**. Všeobecnú platnosť tohto princípu vyjadríme v nasledujúcej vete.

Veta 6.5. *Nech* $\mathbf{x_b}$ *je jedno pevné konkrétne riešenie nehomogénneho systému*

$$\mathbf{Ax} = \mathbf{b}. \quad (6.15)$$

Potom ľubovoľné riešenie tohto nehomogénneho systému možno napísať ako

$$\mathbf{x} = \mathbf{x_b} + \mathbf{x_o}, \quad (6.16)$$

kde $\mathbf{x_o}$ *je riešenie homogénneho systému* $\mathbf{Ax} = \mathbf{o}$.

Dôkaz:
Majme jedno pevne zvolené riešenie $\mathbf{x_b}$ systému (6.15). Nech $\mathbf{u}$ je ľubovoľné riešenie systému (6.15). Pretože $\mathbf{Au} = \mathbf{Ax_b} = \mathbf{b}$, je

$$\mathbf{o} = \mathbf{Au} - \mathbf{Ax_b} = \mathbf{A}(\mathbf{u} - \mathbf{x_b}),$$

čo znamená, že $\mathbf{u} - \mathbf{x_b}$ je riešením homogénneho systému $\mathbf{Ax} = \mathbf{o}$. Vyjadrenie $\mathbf{u} = \mathbf{x_b} + (\mathbf{u} - \mathbf{x_b})$ je už vyjadrenie riešenia $\mathbf{u}$ systému (6.15) v požadovanom tvare.
Každý vektor v tvare $\mathbf{u} = \mathbf{x_b} + \mathbf{x_o}$ je riešením nehomogénneho systému (6.15), pretože $\mathbf{Au} = \mathbf{A}.(\mathbf{x_b} + \mathbf{x_o}) = \mathbf{Ax_b} + \mathbf{Ax_o} = \mathbf{b} + \mathbf{o} = \mathbf{o}$. ■

6.0.2 Cramerovo pravidlo

V tejto časti sa sústredíme na špeciálne systémy lineárnych rovníc – a síce na také, v ktorých je matica sústavy regulárna. Majme n rovníc o n neznámych

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n \end{array}, \tag{6.17}$$

alebo skrátene $\mathbf{Ax} = \mathbf{b}$, kde $\mathbf{A}$ je štvorcová matica typu $n \times n$.

Veta 6.6. *Daný je systém lineárnych rovníc* $\mathbf{Ax} = \mathbf{b}$*, kde* $\mathbf{A}$ *je štvorcová matica typu* $n \times n$*. Ak* $\mathbf{A}$ *je regulárna, potom tento systém má jediné riešenie* $\mathbf{x}$*, pre ktoré platí*

$$\mathbf{x} = \mathbf{A^{-1}b} \tag{6.18}$$

Dôkaz:
Matica $\mathbf{A}$ je podľa predpokladu regulárna, inverzná matica k nej existuje. Potom pre riešenie $\mathbf{x}$ platí:

$$\mathbf{x} = \mathbf{E_n x} = (\mathbf{A^{-1}A})\mathbf{x} = \mathbf{A^{-1}}(\mathbf{Ax}) = \mathbf{A^{-1}b},$$

čo je tvrdenie vety. ■

Príklad 6.6. Nájdime riešenie sústavy lineárnych rovníc podľa vety 6.6.

$$\begin{array}{rrrrr} x_1 & + 2x_2 & - x_3 & = & -1 \\ & + 2x_2 & + x_3 & = & 2 \\ 3x_1 & + x_2 & + 2x_3 & = & 7 \end{array}$$

Riešenie:
Riešením sústavy je vektor $\mathbf{x} = (x_1, x_2, x_3)^T$, ktorý vypočítame podľa vzťahu $\mathbf{x} = \mathbf{A^{-1}b}$. Najskôr vypočítame inverznú maticu k matici sústavy.

$$\left(\begin{array}{ccc|ccc} 1 & 2 & -1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 \\ 3 & 1 & 2 & 0 & 0 & 1 \end{array}\right) \sim \cdots \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/5 & -1/3 & 4/15 \\ 0 & 1 & 0 & 1/5 & 1/3 & -1/15 \\ 0 & 0 & 1 & -2/5 & 1/3 & 2/15 \end{array}\right)$$

Inverznú maticu napíšeme v tvare

$$\mathbf{A^{-1}} = \begin{pmatrix} 1/5 & -1/3 & 4/15 \\ 1/5 & 1/3 & -1/15 \\ -2/5 & 1/3 & 2/15 \end{pmatrix} = \frac{1}{15} \cdot \begin{pmatrix} 3 & -5 & 4 \\ 3 & 5 & -1 \\ -6 & 5 & 2 \end{pmatrix}$$

a dosadíme do (6.18) :

$$\mathbf{x} = \frac{1}{15} \cdot \begin{pmatrix} 3 & -5 & 4 \\ 3 & 5 & -1 \\ -6 & 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 2 \\ 7 \end{pmatrix} = \frac{1}{15} \cdot (15, 0, 30) = (1, 0, 2)$$

Sústava má jediné riešenie $\mathbf{x} = (1, 0, 2)^T$.

Veta 6.7. *(Cramerovo pravidlo) Nech je daný systém lineárnych rovníc* $\mathbf{Ax} = \mathbf{b}$ *s regulárnou maticou* $\mathbf{A}$ *stupňa* n*. Potom pre jediné riešenie* $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ *tohto systému platí*

$$x_i = \frac{\det \mathbf{B_i}}{\det \mathbf{A}}, \quad i = 1, 2, \ldots, n, \tag{6.19}$$

kde $\mathbf{B_i}$ *je matica, ktorá vznikne z matice* $\mathbf{A}$ *nahradením jej* i*-teho stĺpca stĺpcovým vektorom* $\mathbf{b}$*.*

Dôkaz:
Zo vzťahu (6.18) vyplýva, že $\mathbf{x} = \mathbf{A^{-1}b}$. Po dosadení za $\mathbf{A^{-1}}$ zo vzťahu (5.31) (veta 5.25 na str. 138) dostávame

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \mathbf{A^{-1}b} = \frac{1}{\det \mathbf{A}} \begin{pmatrix} A_{11} & A_{21} & \ldots & A_{n1} \\ A_{12} & A_{22} & \ldots & A_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{1n} & A_{2n} & \ldots & A_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}. \tag{6.20}$$

Z posledného vzťahu vyplýva pre každé x_i, $i = 1, 2, \ldots, n$

$$x_i = \frac{1}{\det \mathbf{A}}(b_1 A_{1i} + b_2 A_{2i} + \cdots + b_n A_{ni}). \tag{6.21}$$

Výraz na pravej strane posledného vzťahu predstavuje Laplaceov rozvoj podľa i-teho stĺpca matice $\mathbf{B_i}$, ktorá vznikla nahradením i-teho stĺpca matice $\mathbf{A}$ stĺpcovým vektorom $\mathbf{b}$. ■

Príklad 6.7. Cramerovým pravidlom vyriešme sústavu rovníc

$$\begin{aligned} x_1 - 2x_2 + x_3 &= 0 \\ 3x_1 - 5x_2 - 2x_3 &= -3 \\ 7x_1 - 3x_2 + x_3 &= 16 \end{aligned}$$

Riešenie:
Aby sme našli riešenie systému podľa vzťahov (6.19), je potrebné vypočítať štyri determinanty tretieho stupňa

$$\det\mathbf{A} = \begin{vmatrix} 1 & -2 & 1 \\ 3 & -5 & -2 \\ 7 & -3 & 1 \end{vmatrix} = 49 \qquad \det\mathbf{B_1} = \begin{vmatrix} 0 & -2 & 1 \\ -3 & -5 & -2 \\ 16 & -3 & 1 \end{vmatrix} = 147$$

$$\det\mathbf{B_2} = \begin{vmatrix} 1 & 0 & 1 \\ 3 & -3 & -2 \\ 7 & 16 & 1 \end{vmatrix} = 98 \qquad \det\mathbf{B_3} = \begin{vmatrix} 1 & -2 & 0 \\ 3 & -5 & -3 \\ 7 & -3 & 16 \end{vmatrix} = 49.$$

Potom $x_1 = 147/49 = 3,\ x_2 = 98/49 = 2,\ x_3 = 49/49 = 1,\ \mathbf{x} = (3,2,1)^T$.

6.1 Súradnice vektora vzhľadom na rôzne bázy

V predchádzajúcich kapitolách sme sa už stretli s pojmami báza a súradnice vektora v danej báze. Trochu si ich v krátkosti pripomenieme.
Nech $(U,+,\cdot)$ je ľubovoľný konečnorozmerný vektorový priestor nad daným poľom $\mathcal{P}$ a nech $\mathcal{B} = \{\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_n}\}$ je nejaká jeho báza. Potom ľubovoľný vektor $\mathbf{u} \in U$ sa dá jednoznačne vyjadriť v tvare lineárnej kombinácie

$$\mathbf{u} = s_1\mathbf{u_1} + s_2\mathbf{u_2} + \cdots + s_n\mathbf{u_n}.$$

Tým je každému vektoru $\mathbf{u} \in U$ jednoznačne priradená usporiadaná n-tica prvkov $s_i \in P$, ktorá predstavuje súradnice vektora v danej báze. Pri narábaní so súradnicami vektora je mimoriadne dôležité uvádzať, vzhľadom na akú bázu dané súradnice vektora uvažujeme. Presvedčí nás o tom aj nasledujúci krátky príklad.

Príklad 6.8. Štandardnou bázou vektorového priestoru usporiadaných trojíc reálnych čísel $V_3(\mathbb{R})$ je báza $\mathcal{B}_0 = \{(1,0,0),(0,1,0),(0,0,1)\}$. Nech je daný $\mathbf{u} = (1,-1,1) \in V_3(\mathbb{R})$. Vidíme, že každá zložka vektora $\mathbf{u}$ je zároveň aj jeho súradnicou v báze $\mathcal{B}_0$. Ak však zvolíme vo vektorovom priestore inú bázu, budú sa zložky vektora $\mathbf{u}$ vo všeobecnosti odlišovať od jeho súradníc v "novej" báze. Napr. $\mathcal{B}_1 = \{(0,1,-1),(1,1,1),(1,0,1)\}$ je tiež bázou priestoru $V_3(\mathbb{R})$. V tejto báze sú súradnice vektora $\mathbf{u} = (0,-1,2)$. (Presvedčte sa o tom!)

Zaoberajme sa všeobecnejším prípadom. Nech vo vektorovom priestore $V_n(\mathcal{P})$ sú dané dve bázy: $\boldsymbol{\alpha} = \{\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \ldots, \boldsymbol{\alpha_n}\}$ a $\boldsymbol{\beta} = \{\boldsymbol{\beta_1}, \boldsymbol{\beta_2}, \ldots, \boldsymbol{\beta_n}\}$. Ľubovoľný vektor

$\boldsymbol{\gamma} \in V_n(\mathcal{P})$ sa dá napísať

$$\boldsymbol{\gamma} = x_1\boldsymbol{\alpha_1} + x_2\boldsymbol{\alpha_2} + \cdots + x_n\boldsymbol{\alpha_n} \tag{6.22}$$

$$\boldsymbol{\gamma} = y_1\boldsymbol{\beta_1} + y_2\boldsymbol{\beta_2} + \cdots + y_n\boldsymbol{\beta_n} \tag{6.23}$$

Je zrejmé, že $\mathbf{x} = (x_1, x_2, \ldots, x_n)_{\boldsymbol{\alpha}}$ sú súradnice vektora $\boldsymbol{\gamma}$ v báze $\boldsymbol{\alpha}$ a že $\mathbf{y} = (y_1, y_2, \ldots, y_n)_{\boldsymbol{\beta}}$ sú súradnice vektora $\boldsymbol{\gamma}$ v báze $\boldsymbol{\beta}$.
Vzhľadom na to, že $\boldsymbol{\alpha} = \{\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \ldots, \boldsymbol{\alpha_n}\}$ je báza $V_n(\mathcal{P})$ a $\boldsymbol{\beta_i} \in V_n(\mathcal{P})$ pre $i = 1, 2, \ldots, n$ tak platí

$$\begin{aligned}
\boldsymbol{\beta_1} &= p_{11}\boldsymbol{\alpha_1} + p_{12}\boldsymbol{\alpha_2} + \cdots + p_{1n}\boldsymbol{\alpha_n} \\
\boldsymbol{\beta_2} &= p_{21}\boldsymbol{\alpha_1} + p_{22}\boldsymbol{\alpha_2} + \cdots + p_{2n}\boldsymbol{\alpha_n} \\
&\vdots \\
\boldsymbol{\beta_n} &= p_{n1}\boldsymbol{\alpha_1} + p_{n2}\boldsymbol{\alpha_2} + \cdots + p_{nn}\boldsymbol{\alpha_n},
\end{aligned} \tag{6.24}$$

čo môžeme skrátene napísať $\boldsymbol{\beta} = \mathbf{P} \cdot \boldsymbol{\alpha}$. Pritom $\boldsymbol{\alpha}, \boldsymbol{\beta}$ chápeme ako matice typu $n \times 1$ a $\mathbf{P} = (p_{ij})$ je matica stupňa n. Všimnime si, že súradnice "nového" bázického vektora $\boldsymbol{\beta_i}$ v "starej" báze tvoria i-ty riadok matice $\mathbf{P}$. Matica $\mathbf{P}$ sa nazýva **matica prechodu** od bázy $\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \ldots, \boldsymbol{\alpha_n}$ k báze $\boldsymbol{\beta_1}, \boldsymbol{\beta_2}, \ldots, \boldsymbol{\beta_n}$.

***Poznámka* 6.4.** *Matica prechodu* $\mathbf{P}$ *je vždy regulárna! Toto tvrdenie sa dá dokázať jednoduchým spôsobom:*
Predpokladajme, že tomu tak nie je. To ale znamená, že riadky matice sú lineárne závislé. Nech napr. i-ty riadok je lineárnou kombináciou predchádzajúcich riadkov. V tom prípade platí, že $\boldsymbol{\beta_i} = c_1\boldsymbol{\beta_1} + c_2\boldsymbol{\beta_2} + \cdots + c_{i-1}\boldsymbol{\beta_{i-1}}$, *čo je ale spor s predpokladom, že* $\boldsymbol{\beta_i}$, $i = 1, 2, \ldots, n$ *sú bázické vektory.*

Teraz vyslovíme vetu, v ktorej ukážeme, ako pomocou matice prechodu a starých súradníc daného vektora, vypočítame jeho súradnice v novej báze.

Veta 6.8. *Nech* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ *je n-tica súradníc vektora* $\boldsymbol{\gamma}$ *vzhľadom na bázu* $\boldsymbol{\alpha} = \{\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \ldots, \boldsymbol{\alpha_n}\}$. *Nech* $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ *je n-tica súradníc toho istého vektora vzhľadom na bázu* $\boldsymbol{\beta} = \{\boldsymbol{\beta_1}, \boldsymbol{\beta_2}, \ldots, \boldsymbol{\beta_n}\}$. *Potom*

$$\mathbf{y} = \mathbf{x} \cdot \mathbf{P}^{-1}, \tag{6.25}$$

pričom $\mathbf{P}$ *je matica prechodu od bázy* $\boldsymbol{\alpha}$ *k báze* $\boldsymbol{\beta}$.

Dôkaz:
Na základe vzťahov (6.22) a (6.23) môžeme písať

$$\boldsymbol{\gamma} = x_1\boldsymbol{\alpha_1} + x_2\boldsymbol{\alpha_2} + \cdots + x_n\boldsymbol{\alpha_n} = y_1\boldsymbol{\beta_1} + y_2\boldsymbol{\beta_2} + \cdots + y_n\boldsymbol{\beta_n} \tag{6.26}$$

Použijeme vyjadrenia vektorov $\boldsymbol{\beta_i}$ zo vzťahov (6.24) a dostaneme

$$\begin{aligned}
&\boldsymbol{\gamma} = y_1\boldsymbol{\beta_1} + y_2\boldsymbol{\beta_2} + \cdots + y_n\boldsymbol{\beta_n} = \\
&= y_1(p_{11}\boldsymbol{\alpha_1} + p_{12}\boldsymbol{\alpha_2} + \cdots + p_{1n}\boldsymbol{\alpha_n}) + y_2(p_{21}\boldsymbol{\alpha_1} + p_{22}\boldsymbol{\alpha_2} + \cdots + p_{2n}\boldsymbol{\alpha_n}) + \ldots \\
&\cdots + y_n(p_{n1}\boldsymbol{\alpha_1} + p_{n2}\boldsymbol{\alpha_2} + \cdots + p_{nn}\boldsymbol{\alpha_n}) = (y_1p_{11} + y_2p_{21} + \cdots + y_np_{n1}) \cdot \boldsymbol{\alpha_1} + \\
&+ (y_1p_{12} + y_2p_{22} + \cdots + y_np_{n2}) \cdot \boldsymbol{\alpha_2} + \cdots + (y_1p_{1n} + y_2p_{2n} + \cdots + y_np_{nn}) \cdot \boldsymbol{\alpha_n}
\end{aligned}$$

Porovnaním koeficientov pri vektoroch $\boldsymbol{\alpha_i}$ vo vzťahu (6.26) a v práve odvodených vzťahoch dostaneme

$$\begin{aligned}
x_1 &= y_1p_{11} + y_2p_{21} + \cdots + y_np_{n1} \\
x_2 &= y_1p_{12} + y_2p_{22} + \cdots + y_np_{n2} \\
&\vdots \\
x_n &= y_1p_{1n} + y_2p_{2n} + \cdots + y_np_{nn},
\end{aligned}$$

a v maticovom tvare $\mathbf{x} = \mathbf{y} \cdot \mathbf{P}$. Matica prechodu $\mathbf{P}$ je regulárna, potom k nej existuje inverzná matica $\mathbf{P}^{-1}$. Stačí len vynásobiť vzťah $\mathbf{x} = \mathbf{y} \cdot \mathbf{P}$ maticou $\mathbf{P}^{-1}$ sprava a dostaneme tvrdenie vety, že $\mathbf{y} = \mathbf{x} \cdot \mathbf{P^{-1}}$. ■

Príklad 6.9. Majme vektor $\boldsymbol{\gamma} \in V_3(\mathbb{R})$ a $\boldsymbol{\gamma} = (1,2,1)_{\boldsymbol{\alpha}}$ sú jeho súradnice v báze $\boldsymbol{\alpha} = \{\boldsymbol{\alpha_1} = (-1,1,0), \boldsymbol{\alpha_2} = (0,-1,1), \boldsymbol{\alpha_3} = (1,1,2)\}$. Uvažujme novú bázu $\boldsymbol{\beta} = \{\boldsymbol{\beta_1} = (-1,0,1), \boldsymbol{\beta_2} = (0,1,1), \boldsymbol{\beta_3} = (0,-1,0)\}$ vektorového priestoru $V_3(\mathbb{R})$. Nájdime súradnice vektora $\boldsymbol{\gamma}$ v báze $\boldsymbol{\beta}$.

Riešenie:
Zostrojíme maticu prechodu od bázy $\boldsymbol{\alpha}$ k báze $\boldsymbol{\beta}$. Jej riadky sú súradnice vektorov $\boldsymbol{\beta_1}$, $\boldsymbol{\beta_2}$, $\boldsymbol{\beta_3}$ v báze $\boldsymbol{\alpha}$. Riešime teda tri sústavy rovníc o troch neznámych:

$$\boldsymbol{\beta_1} = p_{11}\boldsymbol{\alpha_1} + p_{12}\boldsymbol{\alpha_2} + p_{13}\boldsymbol{\alpha_3} \tag{6.27}$$
$$\boldsymbol{\beta_2} = p_{21}\boldsymbol{\alpha_1} + p_{22}\boldsymbol{\alpha_2} + p_{23}\boldsymbol{\alpha_3} \tag{6.28}$$
$$\boldsymbol{\beta_3} = p_{31}\boldsymbol{\alpha_1} + p_{32}\boldsymbol{\alpha_2} + p_{33}\boldsymbol{\alpha_3} \tag{6.29}$$

Po dosadení do (6.27) dostávame

$$(-1,0,1)^T = p_{11}(-1,1,0)^T + p_{12}(0,-1,1)^T + p_{13}(1,1,2)^T \tag{6.30}$$

a vyriešením sústavy $p_{11} = 1,\ p_{12} = 1,\ p_{13} = 0$. Analogicky riešením systému daného vzťahmi (6.28) a (6.29) dostávame : $p_{21} = 1/2,\ p_{22} = 0,\ p_{23} = 1/2$

a $p_{31} = -/4,\ p_{32} = 1/2,\ p_{33} = -1/4.$
K matici prechodu od bázy $\boldsymbol{\alpha}$ k báze $\boldsymbol{\beta}$

$$\mathbf{P} = \begin{pmatrix} 1 & 1 & 0 \\ 1/2 & 0 & 1/2 \\ -1/4 & 1/2 & -1/4 \end{pmatrix}$$

nájdeme inverznú maticu

$$\mathbf{P}^{-1} = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & 2 \\ -1 & 3 & 2 \end{pmatrix}$$

a podľa vzťahu (6.25) vypočítame súradnice daného vektora v novej báze

$$\boldsymbol{\gamma}_{\boldsymbol{\beta}} = \begin{pmatrix} 1, & 2, & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -2 \\ 0 & 1 & 2 \\ -1 & 3 & 2 \end{pmatrix} = (0, 4, 4)_{\boldsymbol{\beta}}$$

6.2 Vlastné hodnoty a vlastné vektory matice

Definícia 6.2. Hovoríme, že zobrazenie $f : V_n(\mathcal{P}) \to V_m(\mathcal{P})$ je **lineárne zobrazenie**, ak platí:

$$f(\mathbf{x} + \mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y}) \qquad \text{a} \qquad f(t\mathbf{x}) = tf(\mathbf{x}), \tag{6.31}$$

pre ľubovoľné $\mathbf{x}, \mathbf{y} \in V_m(\mathcal{P})$ a $t \in P$.

Predpisom $\mathbf{y} = \mathbf{A}\mathbf{x}$ môžeme definovať zobrazenie vektorového priestoru $V_n(\mathcal{P})$ do vektorového priestoru $V_m(\mathcal{P})$, ktoré každej usporiadanej n-tici $\mathbf{x} \in V_n(\mathcal{P})$ priraďuje práve jednu usporiadanú m-ticu $\mathbf{y} \in V_m(\mathcal{P})$ a to vektor $\mathbf{A}\mathbf{x}$. Z vlastností operácií násobenia a sčítania matíc vyplýva, že zobrazenie $f : V_n(\mathcal{P}) \to V_m(\mathcal{P})$ definované vzťahom

$$f(\mathbf{x}) = \mathbf{A}\mathbf{x}, \quad \mathbf{x} \in V_n(\mathcal{P}) \tag{6.32}$$

kde $\mathbf{A}$ je matica typu $m \times n$, je linárne zobrazenie priestoru $V_n(\mathcal{P})$ do vektorového priestoru $V_m(\mathcal{P})$. Bez dôkazu uveďme, že všetky lineárne zobrazenia priestoru $V_n(\mathcal{P})$ do priestoru $V_m(\mathcal{P})$ sa dajú vyjadriť v tvare (6.32).

Pri riešení mnohých matematických problémov vzniká otázka, kedy takto definované lineárne zobrazenie vektor $\mathbf{x}$ len „natiahne", t. j. kedy

$$\mathbf{Ax} = \lambda\mathbf{x} = \lambda\mathbf{Ex}. \tag{6.33}$$

Vzťah (6.33) nastane práve vtedy, keď

$$(\mathbf{A} - \lambda\mathbf{E})\mathbf{x} = \mathbf{o}. \tag{6.34}$$

Z teórie lineárnych rovníc vieme, že jedno z riešení rovnice (6.34) je $\mathbf{x} = \mathbf{0}$. Nenulové riešenie má však len vtedy, keď je matica $(\mathbf{A} - \lambda\mathbf{E})$ singulárna, čo nastane práve vtedy, keď

$$\det(\mathbf{A} - \lambda\mathbf{E}) = 0. \tag{6.35}$$

Definícia 6.3. Nech $\mathbf{A}$ je štvorcová matica stupňa n nad poľom reálnych čísel. Determinant

$$\det(\mathbf{A} - \lambda\mathbf{E}) \tag{6.36}$$

nazývame **charakteristickým polynómom** matice $\mathbf{A}$.
Rovnicu

$$\det(\mathbf{A} - \lambda\mathbf{E}) = b_0\lambda^n + b_1\lambda^{n-1} + \cdots + b_{n-1}\lambda + b_0 = 0 \tag{6.37}$$

nazývame **charakteristickou rovnicou** matice $\mathbf{A}$.
Korene charakteristickej rovnice (6.37) matice $\mathbf{A}$ nazývame **vlastné hodnoty** (resp. **charakteristické čísla**) matice $\mathbf{A}$.

Definícia 6.4. Nech λ_0 je vlastná hodnota matice $\mathbf{A}$. Stĺpcový vektor $\mathbf{x} \neq \mathbf{o}$, pre ktorý platí

$$(\mathbf{A} - \lambda_0\mathbf{E})\,\mathbf{x} = \mathbf{o} \tag{6.38}$$

nazývame **vlastným vektorom** (resp. **charakteristickým vektorom**) prislúchajúcim vlastnej hodnote λ_0.

Z definície 6.4 vidíme, že pre danú vlastnú hodnotu λ_0 matice $\mathbf{A}$ je príslušný vlastný vektor $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ netriviálnym riešením systému (6.38), t. j. riešením systému

$$\begin{array}{rcrcl} (a_{11} - \lambda_0)x_1 + & a_{12}x_2 + \ldots + & a_{1n}x_n = 0 \\ a_{21}x_1 + & (a_{22} - \lambda_0)x_2 + \ldots + & a_{2n}x_n = 0 \\ \multicolumn{3}{c}{\dotfill} \\ a_{n1}x_1 + & a_{n2}x_2 + \ldots + & (a_{nn} - \lambda_0)x_n = 0 \end{array} \tag{6.39}$$

***Poznámka* 6.5.** *Pre vlastnú hodnotu λ_0 je matica $(\mathbf{A} - \lambda_0\mathbf{E})$ singulárna, čo znamená, že systém lineárnych rovníc $(\mathbf{A} - \lambda_0\mathbf{E})\,\mathbf{x} = \mathbf{o}$ má nekonečne veľa riešení, lebo $k = h(\mathbf{A} - \lambda_0\mathbf{E}) < n$. Číslo $d = n - k$ udáva maximálny počet lineárne nezávislých riešení tohto systému.*

Príklad 6.10. Nájdime vlastné hodnoty matice $\mathbf{A}$ a k nim prislúchajúce vlastné vektory, keď

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

Riešenie:
Najskôr nájdeme charakteristický polynóm

$$\det(\mathbf{A} - \lambda\mathbf{E}) = \begin{vmatrix} 1-\lambda & -1 & 1 \\ 1 & 1-\lambda & -1 \\ 2 & -1 & 0-\lambda \end{vmatrix} = -\lambda^3 + 2\lambda^2 + \lambda - 2.$$

Riešením charakteristickej rovnice $-\lambda^3 + 2\lambda^2 + \lambda - 2 = 0$ dostaneme vlastné hodnoty $\lambda_1 = -1,\ \lambda_2 = 1,\ \lambda_3 = 2$. Príslušný homogénny systém lineárnych rovníc má tvar:

$$\begin{aligned} (1-\lambda)x_1 - \quad x_2 + \quad x_3 &= 0 \\ x_1 + (1-\lambda)x_2 - \quad x_3 &= 0 \\ 2x_1 - \quad x_2 + (0-\lambda)x_3 &= 0. \end{aligned}$$

Ak $\lambda_1 = -1$, dostaneme systém:

$$\begin{aligned} (1-(-1))x_1 - \quad x_2 + \quad x_3 &= 0 \\ x_1 + (1-(-1))x_2 - \quad x_3 &= 0 \\ 2x_1 - \quad x_2 + (0-(-1))x_3 &= 0. \end{aligned}$$

ktorý má riešenie $\mathbf{x} = (-t/5, 3t/5, t)^T = t(-1/5, 3/5, 1)^T, t \in \mathbb{R}$. Potom vlastné vektory zodpovedajúce vlastnej hodnote $\lambda_1 = -1$ sú všetky vektory tvaru $\mathbf{x} = t(-1/5, 3/5, 1)^T$, pre $t \in \mathbb{R},\ t \neq 0$.
Pre $\lambda_2 = 1$ dostávame systém

$$\begin{aligned} -x_2 + x_3 &= 0 \\ x_1 \quad - x_3 &= 0 \\ 2x_1 - x_2 - x_3 &= 0, \end{aligned}$$

vyriešením ktorého dostaneme pre vlastnú hodnotu $\lambda_2 = 1$ vlastné vektory tvaru $\mathbf{x} = t(1,1,1)^T$, pre $t \in \mathbb{R},\ t \neq 0$.
A nakoniec $\lambda_3 = 2$ a zodpovedajúci systém

$$\begin{aligned} -x_1 - x_2 + x_3 &= 0 \\ x_1 + x_2 - x_3 &= 0 \\ 2x_1 - x_2 - 2x_3 &= 0. \end{aligned}$$

Riešením systému sú vlastné vektory zodpovedajúce vlastnej hodnote $\lambda_3 = 2$, ktoré majú tvar $\mathbf{x} = t(1,0,1)^T$, pre $t \in \mathbb{R},\ t \neq 0$.

Príklad 6.11. Nájdime vlastné hodnoty a im zodpovedajúce vlastné vektory matice

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

Riešenie:
Charakteristický polynóm je

$$\det(\mathbf{A} - \lambda\mathbf{E}) = \begin{vmatrix} 0-\lambda & 1 & 0 \\ -4 & 4-\lambda & 0 \\ -2 & 1 & 2-\lambda \end{vmatrix} = -\lambda^3 + 6\lambda^2 - 12\lambda + 8.$$

Charakteristický polynóm má jeden trojnásobný koreň $\lambda_1 = \lambda_2 = \lambda_3 = 2$, čo je zároveň aj vlastná hodnota matice $\mathbf{A}$. Zostáva nájsť k nej vlastný vektor. Zodpovedajúci homogénny systém rovníc

$$\begin{aligned} -2x_1 + x_2 &= 0 \\ -4x_1 + 2x_2 &= 0 \\ -2x_1 + 3x_2 &= 0, \end{aligned}$$

má riešenie $\mathbf{x} = (t_1/2, t_1, t_2)^T = t_1(1/2,1,0)^T + t_2(0,0,1)^T$, pre ľubovoľné $t_1, t_2 \in \mathbb{R}$ a $t_1, t_2 \neq 0$.

Veta 6.9. *Nech λ_0 je vlastná hodnota matice $\mathbf{A}$. Všetky vlastné vektory prislúchajúce tej istej vlastnej hodnote λ_0 spolu s nulovým vektorom $\mathbf{o}$ tvoria vektorový podpriestor s dimenziou $n - h(\mathbf{A} - \lambda_0\mathbf{E})$.*

Dôkaz:
Overíme podmienky z vety 4.2. Nech $\mathcal{X}_{\lambda_0}$ je množina všetkých vlastných vlastných vektorov prislúchajúcich vlastnej hodnote λ_0. Podľa predpokladu $\mathbf{o} \in \mathcal{X}_{\lambda_0}$,

takže stačí ukázať, že ľubovoľná lineárna kombinácia dvoch vlastných vektorov prislúchajúcich tej istej vlastnej hodnote λ_0 je tiež k nej prislúchajúci vlastný vektor. Nech tými vektormi sú $\mathbf{x}$ a $\mathbf{y}$ a nech $c_1, c_2 \in \mathbb{R},\ c_1, c_2 \neq 0$. Overíme či $c_1\mathbf{x} + c_2\mathbf{y}$ je vlastný vektor zodpovedajúci λ_0.

$$(\mathbf{A} - \lambda_0\mathbf{E}) \cdot (c_1\mathbf{x} + c_2\mathbf{y}) = c_1(\mathbf{A} - \lambda_0\mathbf{E})\mathbf{x} + c_2(\mathbf{A} - \lambda_0\mathbf{E})\mathbf{y} = c_1\mathbf{o} + c_2\mathbf{o} = \mathbf{o},$$

čo znamená, že $(c_1\mathbf{x} + c_2\mathbf{y}) \in \mathcal{X}_{\lambda_0}$. Dimenzia podpriestoru všetkých vlastných vektorov prislúchajúcich vlastnej hodnote λ_0 vyplýva z poznámky 6.5. ■

Veta 6.10. *Vlastné vektory* $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}$ *prislúchajúce rôznym vlastným hodnotám* $\lambda_1, \lambda_2, \ldots, \lambda_k$ *sú lineárne nezávislé.*

Dôkaz:
Matematickou indukciou podľa k. Pre $k = 1$ je tvrdenie vety zrejmé. Nech tvrdenie vety platí pre $(k-1)$ vektorov prislúchajúcim $(k-1)$ vlastným hodnotám. Majme teraz vektory $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}$ prislúchajúce rôznym vlastným hodnotám $\lambda_1, \lambda_2, \ldots, \lambda_k$. Nech

$$a_1\mathbf{x_1} + a_2\mathbf{x_2} + \cdots + a_k\mathbf{x_k} = \mathbf{o}. \tag{6.40}$$

Pre každú vlastnú hodnotu λ_i a každý vlastný vektor $\mathbf{x}_i$, ktorý jej zodpovedá platí $\mathbf{Ax_i} = \lambda_i\mathbf{x}_i$, $i = 1, 2, \ldots, k$. Potom platí:

$$\begin{aligned}\mathbf{0} = \mathbf{A0} = \mathbf{A}(a_1\mathbf{x_1} + a_2\mathbf{x_2} + \cdots + a_k\mathbf{x_k}) = \\ = a_1(\mathbf{Ax_1}) + a_2(\mathbf{Ax_2}) + \cdots + a_k(\mathbf{Ax_k}) = \\ = a_1\lambda_1\mathbf{x_1} + a_2\lambda_2\mathbf{x_2} + \cdots + a_k\lambda_k\mathbf{x_k}\end{aligned} \tag{6.41}$$

Vynásobme rovnicu (6.40) číslom λ_k a odčítajme od rovnice (6.41). Dostaneme

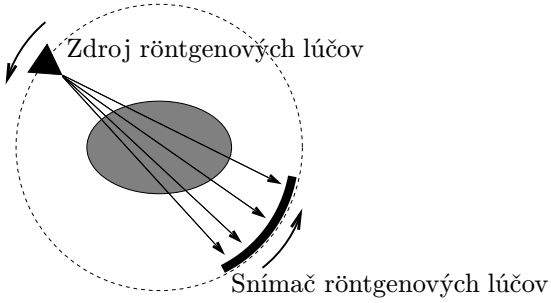
$$\begin{aligned}a_1(\lambda_1 - \lambda_k)\mathbf{x_1} + a_2(\lambda_2 - \lambda_k)\mathbf{x_2} + \ldots \\ \cdots + a_{k-1}(\lambda_{k-1} - \lambda_k)\mathbf{x_{k-1}} + a_k(\lambda_k - \lambda_k)\mathbf{x_k} = \\ = a_1(\lambda_1 - \lambda_k)\mathbf{x_1} + a_2(\lambda_2 - \lambda_k)\mathbf{x_2} + \cdots + a_{k-1}(\lambda_{k-1} - \lambda_k)\mathbf{x_{k-1}} = \mathbf{o}.\end{aligned} \tag{6.42}$$

Podľa indukčného predpokladu sú vektory $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_{k-1}}$ lineárne nezávislé, a preto $a_i(\lambda_i - \lambda_k) = 0$ pre $i = 1, 2, \ldots, k-1$, z čoho (keďže $\lambda_i \neq \lambda_k$) vyplýva $a_i = 0$ pre $i = 1, 2, \ldots, k-1$. Z posledného faktu a z (6.40) vyplýva $a_k\mathbf{x}_k = \mathbf{o}$, a teda aj $a_k = 0$. ■

6.3 Aplikácie

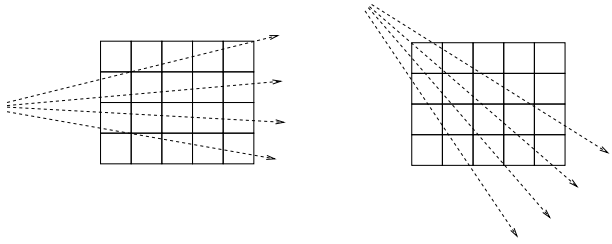
Počítačová tomografia

Počítačová tomografia je diagnostická technika, ktorá umožňuje zobraziť priečny rez ľudským telom. Pri snímaní obrazu zvoleného rezu rotuje v zvolenej rovine okolo snímaného objektu na jednej strane zdroj röntgenového žiarenia a na druhej strane snímač, ktorý zaznamenáva intenzitu jednotlivých röntgenových lúčov po prechode objektom.



Obr. 6.1: Princíp usporiadania tomografu

Objekt si modelujeme akoby bol poskladaný z malých kociek (rozmeru rádovo desatín milimetra) ktoré označíme $k_1, k_2, \ldots, k_m$. Označme symbolom m_i priepustnosť žiarenia kockou k_i. Priepustnosť bude číslo v intervale $\langle 0, 1 \rangle$ a bude definovaná ako pomer intenzity röntgenového lúča pred prechodom kockou k jeho intenzite po prechode kockou. Ak určíme priepustnosti všetkých kociek v žiadanom reze, dokážeme z nich vykresliť obraz tohoto rezu.



Obr. 6.2: Prechod lúčov objektom

Označme $\mathcal{M}_i$ množinu práve tých kociek, ktorými prejde röntgenový lúč i so začiatočnou intenzitou I. Po prechode týmito kockami sa jeho intenzita zmenší na hodnotu I_i. Potom

$$I_i = I \cdot \prod_{j \in \mathcal{M}_i} m_j \tag{6.43}$$

odkiaľ

$$\log \frac{I}{I_i} = \sum_{j \in \mathcal{M}_i} \log m_j \tag{6.44}$$

Majme zmerané intenzity m lúčov po prechode zobrazovaným objektom. Označme

$$a_{ij} = \begin{cases} 1 & \text{ak lúč } i \text{ prechádza kockou } j \\ 0 & \text{inak} \end{cases} \tag{6.45}$$

Ak označíme $x_i = \log m_i$ pre $i = 1, 2, \ldots, n$, možno rovnicu (6.44) prepísať v tvare

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = \log \frac{I}{I_i} \tag{6.46}$$

Pre všetky lúče tak dostávame nasledujúci systém lineárnych rovníc

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= \log \tfrac{I}{I_1} \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= \log \tfrac{I}{I_2} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= \log \tfrac{I}{I_m} \end{aligned} \tag{6.47}$$

Z riešenia sústavy (6.47) potom dostaneme $m_i = 10^{x_i}$ pre $i = 1, 2, \ldots, n$.

Úloha lineárneho programovania

Táto kapitola sa zaoberala sústavou lineárnych rovníc tvaru

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \ . \end{aligned} \tag{6.48}$$

Vieme, že rovnicu možno zapísať v maticovom tvare ako $\mathbf{A}.\mathbf{x} = \mathbf{b}$, kde $\mathbf{A} = (a_{ij})$ je matica ľavej strany systému (6.48), $\mathbf{b}$ je stĺpcový vektor pravých strán $\mathbf{b} = (b_1, b_2, \ldots, b_m)^T$ a $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ stĺpcový vektor neznámych, $\mathbf{x} \in \mathbb{R}^n$. Vieme, že tento systém má aspoň jedno riešenie práve vtedy, keď hodnosť matice systému $\mathbf{A}$ sa rovná hodnosti rozšírenej matice $(\mathbf{A}|\mathbf{b})$ systému (6.48) a vtedy každé riešenie (6.48) dostaneme ako súčet jedného pevne vzatého riešenia nehomogénneho systému a niektorého riešenia homogénneho systému.

V mnohých praktických úlohách premenné $x_1, x_2, \ldots, x_n$ predstavujú množstvá reálnych látok, substrátov alebo objektov a sústava rovníc (6.48) predstavuje ohraničenia pre tieto množstvá. Preto nás zaujímajú len také riešenia sústavy (6.48), pre ktoré je $x_1 \geq 0,\ x_2 \geq 0,\ \ldots,\ x_n \geq 0$, t. j. pre ktoré sú množstvá nezáporné. Každému nezápornému riešeniu je priradená hodnota lineárnej kriteriálnej funkcie

$$f(\mathbf{x}) = c_1x_1 + c_2x_2 + \cdots + c_nx_n = \mathbf{c}^T.\mathbf{x}$$

predstavujúca náklady na riešenie $\mathbf{x}$. Pochopiteľne zo všetkých nezáporných riešení nás zaujíma to, ktoré nám prináša čo najmenšie náklady. Tento problém rieši úloha lineárneho programovania.

Definícia 6.5. Úloha lineárneho programovania je nájsť také reálne čísla $x_1, x_2, \ldots, x_n$, pre ktoré je

$$f(\mathbf{x}) = \mathbf{c}^T.\mathbf{x} = c_1x_1 + c_2x_2 + \cdots + c_nx_n \quad \text{minimálne}$$

za predpokladov:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \\ \\ x_1, x_2, \ldots, x_n &\geq 0 \end{aligned}$$

Skrátene pomocou maticových zápisov možno úlohu lineárneho programovania formulovať takto: Minimalizujte $\mathbf{c}^T.\mathbf{x}$ za predpokladov $\mathbf{A}.\mathbf{x} = \mathbf{b}$, $\mathbf{x} \geq 0$. Na úlohu lineárneho programovania vedú riešenia praktických problémov ako napríklad problém optimalizácie výrobného plánu, problém optimalizácie zásobovania (dopravná úloha), problém optimalizácie kŕmnych dávok a stoviek (možno tisícov) ďalších.

Skúmanie práve formulovanej úlohy podstatne využíva všetky poznatky teórie systémov lineárnych rovníc, lineárnych priestorov a podpriestorov. Na ich základe bolo možné navrhnúť niekoľko efektívnych algoritmov riešenia úlohy lineárneho programovania. Priekopníkmi v tejto oblasti boli George Dantzig – tvorca slávnej simplexovej metódy, Leonid Kantorovič a Vasilij Leotief – nositelia Nobelovej ceny za ekonómiu a mnohí ďalší.

Na riešenie úlohy lineárneho programovania máme dnes napríklad tzv. revidovanú simplexovú metódu, ktorou (alebo jej modifikáciami) zvládneme s dnešnou výpočtovou technikou aj úlohy s tisíckami premenných.

Oceňovanie webovských stránok

Vyhľadávanie informácií na internete je založené na identifikácii webovských stránok obsahujúcich dané kľúčové slová alebo frázy. Keďže internet dnes obsahuje okolo 10 miliárd stránok, tých stránok, ktoré obsahujú hľadanú frázu, môže byť veľmi veľa. Používateľ by privítal, keby mu jeho vyhľadávač ponúkal jednotlivé stránky v poradí od najvýznamnejších k najmenej významným.

Vyhľadávanie informácií na internete uľahčujú rôzne vyhľadávače, ktorých je dnes aj niekoľko tisíc. Medzi nimi je bez pochybností najúspešnejší vyhľadávač Google, ktorého úspech spočíva (okrem iného) v jedinečnom a veľmi elegantnom spôsobe oceňovania webovských stránok.

Nech všetky stránky na internete sú $S_1, S_2, \ldots, S_n$, kde n je ich počet ($n \approx 10^{10}$). Označme $r_1, r_2, \ldots, r_n$ významy – relevancie stránok $S_1, S_2, \ldots, S_n$. Výpočet relevancií stránok vychádza z nasledujúcej tézy: Každý odkaz na danú stránku S_i zvyšuje je relevanciu. Príspevok k relevancii stránky S_i od stánky S_j je priamo úmerný relevancii stránky S_j a nepriamo úmerný počtu stránok, na ktoré sa stránka S_j odkazuje.

$$a_{ij} = \begin{cases} 1 & \text{ak stránka } S_j \text{ obsahuje odkaz na stránku } S_i \\ 0 & \text{inak} \end{cases} \tag{6.49}$$

Počet odkazov, na ktoré sa stránka S_j odkazuje, je $\sum_{k=1}^{n} a_{kj}$, jej príspevok k relevancii stránky S_i je $K \cdot \dfrac{a_{ij}}{\sum_{k=1}^{n} a_{kj}} r_j$, ak $\sum_{k=1}^{n} a_{kj} \neq 0$, kde K je nejaká nenulová konštanta, inak je príslušný príspevok nulový.

Ak označíme

$$A_{ij} = \begin{cases} \dfrac{a_{ij}}{\sum_{k=1}^{n} a_{kj}} & \text{ak } \sum_{k=1}^{n} a_{kj} \neq 0 \\ 0 & \text{ak } \sum_{k=1}^{n} a_{kj} = 0 \end{cases} \tag{6.50}$$

potom možno príspevok stránky S_j k relevancii stránky S_i napísať ako $K \cdot A_{ij} r_j$ a relevanciu stránky S_i vypočítať ako

$$r_i = K \cdot \sum_{j=1}^{n} A_{ij} r_j \quad \text{pre } i = 1, 2, \ldots n, \tag{6.51}$$

v maticovom zápise

$$\mathbf{A}.\mathbf{r} = \frac{1}{K} \cdot \mathbf{r} \text{ resp. } \mathbf{A}.\mathbf{r} = \lambda \cdot \mathbf{r} \tag{6.52}$$

Ak má rovnica (6.52) riešenie, možno z nej vypočítať vektor relevancií $\mathbf{r}$. Hodnoty čísla λ, pre ktoré má (6.52) riešenie, sú vlastné hodnoty matice $\mathbf{A}$. Vektory $\mathbf{r}$ vyhovujúce rovnici (6.52) sú vlastné vektory prislúchajúce vlastnej hodnote λ.

Malým pozmenením matice $\mathbf{A}$

$$A_{ij} = \begin{cases} \dfrac{a_{ij}}{\sum_{k=1}^{n} a_{kj}} & \text{ak } \sum_{k=1}^{n} a_{kj} \neq 0 \\ \dfrac{1}{n} & \text{ak } \sum_{k=1}^{n} a_{kj} = 0 \end{cases} \tag{6.53}$$

dostaneme maticu, pre ktorú sa všetky stĺpcové súčty rovnajú 1, je totiž

$$\sum_{i=1}^{n} A_{ij} = \sum_{i=1}^{n} \left(\frac{a_{ij}}{\sum_{k=1}^{n} a_{kj}} \right) = \frac{\sum_{i=1}^{n} a_{ij}}{\sum_{k=1}^{n} a_{kj}} = 1,$$

ak $\sum_{k=1}^{n} a_{kj} \neq 0$, resp.

$$\sum_{i=1}^{n} A_{ij} = \sum_{i=1}^{n} \frac{1}{n} = 1,$$

ak $\sum_{k=1}^{n} a_{kj} = 0$. Z teoretických rozborov vyplýva, že takáto matica $\mathbf{A}$ má vlastnú hodnotu $\lambda = 1$, a preto stačí riešiť rovnicu

$$\mathbf{A} \cdot \mathbf{r} = \mathbf{r} \; . \tag{6.54}$$

Pre malé n vyriešiť rovnicu (6.52) nie je problém. V skutočnosti $n \approx 10^8$, takže matica $\mathbf{A}$ má rádovo 10^{16} prvkov. Vzniká tak problém, ktorý sa dotýka nielen algebry, ale aj informatiky a spracovania údajov (napr. s uložením matice $\mathbf{A}$, jej aktualizáciou, rýchlym prístupom k jej prvkom), numerickej matematiky, teórie grafov, výpočtovej zložitosti a mnohých ďalších, bez podpory ktorých by bola činnosť vyhľadávača Google nemysliteľná.

Cvičenia

1. Riešte systém lineárnych rovníc Gaussovou eliminačnou metódou:

a)
$$\begin{aligned} x_1 + x_2 + 2x_3 + 3x_4 &= 1 \\ 3x_1 - x_2 - x_3 - 2x_4 &= -4 \\ 2x_1 + 3x_2 - x_3 - x_4 &= -6 \\ x_1 + 2x_2 + 3x_3 - x_4 &= -4 \end{aligned}$$

b)
$$\begin{aligned} x_1 + x_2 - 3x_3 &= -1 \\ 2x_1 + x_2 - 2x_3 &= 1 \\ x_1 + x_2 + x_3 &= 3 \\ x_1 + 2x_2 - 3x_3 &= 1 \end{aligned}$$

c)
$$\begin{aligned} x_1 - 2x_2 + 3x_3 - 4x_4 &= 4 \\ + x_2 - x_3 + x_4 &= -3 \\ x_1 + 3x_2 - 3x_4 &= 1 \\ - 7x_2 + 3x_3 + x_4 &= -3 \end{aligned}$$

2. Pre akú hodnotu parametra p má sústava nekonečne veľa riešení?

$$\begin{aligned} px_1 - x_2 + 3x_3 &= 2 \\ -x_1 + x_2 - x_3 &= 0 \\ x_1 + px_2 + x_3 &= 4 \end{aligned}$$

3. Jordanovou eliminačnou metódou nad poľom $(\mathbb{Z}_5, \oplus_5, \otimes_5)$ riešte systém lineárnych rovníc:

a)
$$\begin{aligned} 2x_1 + x_2 + 4x_3 + x_4 &= 1 \\ 3x_1 + 3x_2 + 2x_3 + 2x_4 &= 2 \\ x_2 + 4x_3 + 2x_4 &= 2 \\ 2x_1 + 4x_2 + x_3 + 2x_4 &= 2 \end{aligned}$$

b)
$$\begin{aligned} x_1 + x_2 + 3x_3 &= 4 \\ 2x_1 + x_2 + 3x_3 &= 1 \\ x_1 + x_2 + x_3 &= 3 \\ x_1 + 2x_2 + 2x_3 &= 1 \end{aligned}$$

4. Riešte homogénne systémy lineárnych rovníc:

a)
$$\begin{aligned} x_1 + x_2 + x_3 - x_4 &= 0 \\ 2x_1 - 3x_2 - 2x_3 + x_4 &= 0 \\ x_1 + 2x_2 - 3x_3 + x_4 &= 0 \end{aligned}$$

b)
$$\begin{aligned} x_1 + 4x_2 - 3x_3 &= 0 \\ x_1 - 3x_2 - x_3 &= 0 \\ 2x_1 + x_2 - 4x_3 &= 0 \end{aligned}$$

c)
$$\begin{aligned} x_1 - 3x_2 + 2x_3 \quad\quad - x_5 &= 0 \\ 4x_1 + 2x_2 - 2x_3 + x_4 - 2x_5 &= 0 \\ 6x_1 + x_2 - 4x_3 - 2x_4 + 2x_5 &= 0 \\ 5x_1 - x_2 \quad\quad + x_4 - 3x_5 &= 0 \end{aligned}$$

5. Nad poľom $(\mathbb{Z}_7, \oplus_7, \otimes_7)$ riešte homogénne systémy rovníc:

a)
$$\begin{aligned} x_1 + 3x_2 + x_3 + x_4 &= 0 \\ 3x_1 \quad\quad + 3x_3 \quad\quad &= 0 \\ x_1 + x_2 + 4x_3 + x_4 &= 0 \\ x_1 + x_2 + x_3 + 5x_4 &= 0 \end{aligned}$$

b)
$$\begin{aligned} x_1 + 4x_2 + 4x_3 &= 0 \\ x_1 + 4x_2 + 6x_3 &= 0 \\ 2x_1 + x_2 + 3x_3 &= 0 \end{aligned}$$

c)
$$\begin{aligned} 3x_1 + 5x_2 + x_3 + 2x_4 + 4x_5 &= 0 \\ 2x_1 + x_2 + 3x_3 + 5x_4 + 2x_5 &= 0 \\ x_1 + 4x_2 + x_3 \quad\quad + 3x_5 &= 0 \\ 2x_1 + 5x_2 + 6x_3 + x_4 + 3x_5 &= 0 \end{aligned}$$

7. Použitím Cramerovho pravidla riešte systémy lineárnych rovníc:

a)
$$\begin{aligned} 3x_1 - 2x_2 + 5x_3 - 6x_4 &= 21 \\ 7x_1 + x_2 - 3x_3 - 4x_4 &= 23 \\ 6x_1 + 5x_2 - 13x_3 + 3x_4 &= 1 \\ 2x_1 - 13x_2 + 40x_3 - 16x_4 &= 74 \end{aligned}$$

b)
$$\begin{aligned} 3x_1 + 2x_2 + x_3 &= 5 \\ 2x_1 + 3x_2 + x_3 &= 1 \\ 2x_1 + x_2 + 3x_3 &= 11 \end{aligned}$$

c)
$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 &= 0 \\ x_1 - x_2 + 2x_3 - 2x_4 + 3x_5 &= 0 \\ x_1 + x_2 + 4x_3 + 4x_4 + 9x_5 &= 0 \\ x_1 - x_2 + 8x_3 - 8x_4 + 27x_5 &= 0 \\ x_1 + x_2 + 16x_3 + 16x_4 + 81x_5 &= 0 \end{aligned}$$

8. Dokážte tvrdenie: Nech $\mathbf{P}$ je regulárna matica n-tého stupňa, nech $\boldsymbol{\alpha} = \{\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \ldots, \boldsymbol{\alpha_n}\}$ je báza $V_n(\mathcal{P})$ a nech

$$\begin{aligned} \boldsymbol{\beta_1} &= p_{11}\boldsymbol{\alpha_1} + p_{12}\boldsymbol{\alpha_2} + \cdots + p_{1n}\boldsymbol{\alpha_n} \\ \boldsymbol{\beta_2} &= p_{21}\boldsymbol{\alpha_1} + p_{22}\boldsymbol{\alpha_2} + \cdots + p_{2n}\boldsymbol{\alpha_n} \\ &\vdots \\ \boldsymbol{\beta_n} &= p_{n1}\boldsymbol{\alpha_1} + p_{n2}\boldsymbol{\alpha_2} + \cdots + p_{nn}\boldsymbol{\alpha_n}. \end{aligned}$$

Potom vektory $\boldsymbol{\beta_1}, \boldsymbol{\beta_2}, \ldots, \boldsymbol{\beta_n}$ tvoria bázu vektorového priestoru $V_n(\mathcal{P})$.

9. Vektor $\mathbf{a}$ má v báze $\boldsymbol{\beta_1} = \{(1,0,-1),(0,2,1),(1,-1,0)\}$ súradnice $(-1,0,2)_{\boldsymbol{\beta_1}}$. Vypočítajte súradnice vektora $\mathbf{a}$ vzhľadom na bázu $\boldsymbol{\beta_2} = \{(1,-1,0),(0,0,1),(1,0,1)\}$.

10. Daná je báza $\boldsymbol{\beta_2} = \{(1,0,1),(0,1,1),(2,0,1)\}$ vektorového priestoru $V_3(\mathbb{R})$ a matica prechodu $\mathbf{P}$ od bázy $\boldsymbol{\beta_1}$ k $\boldsymbol{\beta_2}$. Nájdite bázu $\boldsymbol{\beta_1}$, keď

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

11. Nájdite vlastné hodnoty a k nim zodpovedajúce vlastné vektory matíc:

$$\mathbf{A} = \begin{pmatrix} 5 & 6 & -3 \\ -1 & 0 & 1 \\ 1 & 2 & -1 \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} 3 & 1 & 0 \\ -4 & -1 & 0 \\ 4 & -8 & -2 \end{pmatrix}$$

$$\mathbf{C} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

12. Pre akú hodnotu parametra a má matica $\mathbf{A}$ trojnásobnú vlastnú hodnotu, keď

$$\mathbf{A} = \begin{pmatrix} 4 & 4 & 0 \\ -1 & a & 0 \\ -2 & -4 & 2 \end{pmatrix}?$$

Register

Literatúra

[1] Adámek, J.: *Kódování*, SNTL Praha 1989

[2] Berlehamp, R., R.: *Algebraic Coding Theory*, McGraw-Hill, New York 1968 (*Ruský preklad: Algebrajičeskaja teorija kodirovanija, Mir, Moskva 1971*)

[3] Birkhoff, G., Saunders Mac Lane: *Algebra*, Alfa – vydavateľstvo technickej a ekonomickej literatúry, Bratislava 1973

[4] Saunders Mac Lane, Birkhoff, G.: *Prehľad modernej algebry*, Alfa – vydavateľstvo technickej a ekonomickej literatúry, Bratislava 1979

[5] Birkhoff, G., Bartee, T., O.: *Aplikovaná algebra*, Alfa – vydavateľstvo technickej a ekonomickej literatúry, Bratislava 1981

[6] Demlová, M., Nagy, J.: *Algebra*, SNTL - Nakladatelství technické literatury, Praha 1985

[7] Brandts, J., Křížek, M.: *Lineární algebra ukrytá v internetovém vyhledávači Google*, Pokroky matematiky, fyziky a astronomie, roč. *52*, č. 3, 2007, str. 195–204

[8] Fadejev, A., K., Sominskij, J., S.: *Zbierka úloh z vyššej algebry*, Alfa Bratislava 1968

[9] Chvál, V., Mikola, M.: *Lineárna algebra*, Katolícka univerzita, Ružomberok 2000, ISBN 80-89039-00-6

[10] Kaprálik, P., Tvarožek, J. : *Zbierka riešených príkladov a úloh z lineárnej algebry a analytickej geometrie*, Alfa, Bratislava 1987

[11] Katriňák, T., Gavalec, M., Gedeonová, E., Smítal, J.: *Algebra a teoretická aritmetika*, Univerzita Komenského, Bratislava 2002, ISBN 80-223-1674-1

[12] Mikola, M: *Algebra*, Žilinská univerzita v Žiline, Žilina 1998, ISBN 80-7100-510-X

[13] Špániková, E., Wisztová, E.: *Zbierka úloh z algebry*, Žilinská univerzita v Žiline, Žilina 2003, ISBN 80-7080-110-5

[14] Zlatoš. P.: *Lineárna algebra a geometria*, Bratislava 2006

[15] http://fchabaud.free.fr/English/default.php?COUNT=1&FILE0=Poly

Autori:	Doc. RNDr. Stanislav Palúch, CSc. RNDr. Ida Stankovianska, CSc.
Názov:	**ALGEBRA a jej inžinierske aplikácie**
Vydala:	Žilinská univerzita v EDIS-vydavateľstve ŽU v roku 2008 ako svoju XXX. publikáciu
Vedecký redaktor:	prof. Ing. Petr Cenek, CSc.
Jazyková redaktorka	PhDr. Katarína Šimánková
Technický redaktor:	XXX XXXXXXXXXXX xxxx
Určené:	pre študentov Fakulty riadenia a informatiky
Vydanie:	prvé
Náklad:	XXX výtlačkov
AH/VH:	XX/XX
Druh tlače:	xxxxxxx
Typografický systém:	LaTeX pod o. s. Linux

ISBN 80-XXXX-XX-X