OBSAH

Kapitola 1

ZÁKLADNÉ ALGEBRAICKÉ ŠTRUKTÚRY

Zo strednej školy čitateľ pozná základné aritmetické operácie: sčítanie, odčítanie, násobenie a delenie reálnych čísel. Cieľom tejto úvodnej kapitoly je zovšeobecniť uvedené pojmy na pojem binárnej algebraickej operácie a uviesť základné vlastnosti binárnych operácií a algebraických štruktúr s jednou a dvoma binárnymi operáciami. Z nich najdôležitejšie budú *grupa* a *pole*, ktoré sú nevyhnutné pri definícii *vektorového priestoru* ako základného pojmu lineárnej algebry. Budeme predpokladať, že čitateľ pozná základné poznatky o množinách (rôzne spôsoby zadania množiny, spôsob dokazovania rovnosti množín, operácie s množinami ako sú prienik, zjednotenie, rozdiel, karteziánsky súčin, niektoré množinové identity atď.), o výrokoch a výrokových formách (operácie s výrokmi, tabuľky pravdivosti, niektoré dôležité tautológie, pojem oboru definície a oboru pravdivosti výrokovej formy, kvantifikátory a ich negovanie atď.), o binárnych reláciách a zobrazeniach (skladanie relácií a zobrazení, vzťah medzi reláciou ekvivalencie a rozkladom množiny na disjunktné triedy atď.). Pre úspešné štúdium tejto kapitoly, a celého skripta, bude veľmi užitočné čo najskôr si odstrániť prípadné nedostatky vo vedomostiach o práve vymenovanej problematike. Všetko to možno nájsť napr. v [11], [13] alebo [15].

§ 1. Grupoidy, pologrupy, monoidy

Uvažujme o sčítaní reálnych čísel. Ak vezmeme dve reálne čísla a, b (dva prvky množiny R), vieme určiť tretie reálne číslo c, ktoré nazveme súčet čísel a, b. Zapisujeme $c = a + b$. Reálne číslo c určíme tak, že reálne čísla a, b známym spôsobom sčítame. Je jasné, že takto môžeme sčítať ľubovoľné dve reálne čísla. Takže platí:

Ku každým dvom reálnym číslam $a, b \in R$
existuje reálne číslo $c \in R$ také, že $c = a + b$.

Alebo inými slovami:

Ku každej dvojici reálnych čísel $[a, b] \in R \times R$, kde $R \times R$ je karteziánsky štvorec množiny R, existuje reálne číslo $c \in R$ také, že $c = a + b$.

Nasledujúca definícia obsahuje zovšeobecnenie pojmu „aritmetická operácia v množine reálnych čísel" na pojem „binárna algebraická operácia v ľubovoľnej neprázdnej množine".

Definícia 1.1. Nech A je neprázdna množina. Zobrazenie

$$* : A \times A \to A$$

nazývame *binárna algebraická operácia* na množine A. Ak zobrazenie $*$ dvojici $[x, y] \in A \times A$ priraďuje prvok $z \in A$, tak miesto zápisu $*([x, y]) = z$ píšeme $x * y = z$. Prvok z nazývame *kompozíciou* prvkov x, y (v danom poradí). Niekedy ho nazývame aj výsledkom operácie $*$. Prvok x je prvý, prvok y druhý komponent danej operácie.

Príklad 1.1. Operácia sčítania „+“ je binárnou operáciou na množine prirodzených čísel N, zatiaľ čo operácia odčítania „−“ nie je binárnou operáciou na množine N. Je to preto, že nie každej dvojici $[x, y] \in N \times N$ možno priradiť kompozíciu $x - y \in N$. Napr. ak $x = 5$, $y = 7$, tak $5 - 7 \notin N$.

Príklad 1.2. Nech $\mathcal{P}(A)$ je systém všetkých podmnožín množiny A, kde $A \neq \emptyset$. Na množine $\mathcal{P}(A)$ uvažujme operáciu „$\cap$“ (prienik). Potom „$\cap$“ je binárnou operáciou na množine $\mathcal{P}(A)$. Naozaj platí: Ku každým dvom množinám $M, N \in \mathcal{P}(A)$ existuje prienik $M \cap N \in \mathcal{P}(A)$. Odôvodnite to.

Ako vidieť, na označenie binárnych operácií sa používajú rôzne znaky: $+$, $\cdot$, $-$, $:$, $\times$, $\cup$, $\cap$, $\ldots$, ktorých význam je v matematike (väčšinou) ustálený, ale aj iné znaky ako $*$, $\odot$, $\oplus$, $\triangle$, $\square$, a pod. Keďže znaky „+“ a „·“ sa používajú najčastejšie, pri použití znaku „+“ budeme hovoriť, že operácia je zapísaná *aditívne*, pri použití znaku „·“ povieme, že operácia je zapísaná *multiplikatívne*. Pri aditívnom zápise kompozíciu nazývame *súčet* a komponenty *sčítance*. Pri multiplikatívnom zápise kompozíciu nazývame *súčin* a komponenty *činitele*.

Teda

$$\underbrace{a+b}_{\text{sčítance}} \ - \text{súčet} \qquad\qquad \underbrace{a \cdot b}_{\text{činitele}} \ - \text{súčin}$$

Pri multiplikatívnom zápise, a len vtedy, môžeme znak operácie „·“ vynechať. Miesto $a \cdot b$ píšeme jednoducho ab.

Príklad 1.3. Na množine prirodzených čísel definujme nasledujúce operácie:

a) $a \triangle b = a + b + a \cdot b$, b) $a \square b = a + b - 1$,
c) $a \bigtriangledown b = a$, d) $a \circ b = a^b$,

kde na pravej strane rovností sú operácie obyčajné sčítanie, násobenie a umocňovanie prirodzených čísel. Napr.: $2 \triangle 3 = 11$, $2 \bigtriangledown 3 = 2$, $2 \circ 3 = 8$, atď.

Keď A je konečná množina s malým počtom prvkov, potom binárnu operáciu $*$ na tejto množine možno udať pomocou tzv. Cayleyho*) tabuľky. Tabuľku zostrojíme tak, že do záhlavia (zvisle i vodorovne) dáme prvky množiny A a na priesečníky riadkov a stĺpcov píšeme kompozície príslušných prvkov. Teda ak $A = \{a_1, a_2, \ldots, a_n\}$, Cayleyho tabuľka bude mať tvar

$$\begin{array}{c|cccccc}
* & a_1 & a_2 & \ldots & a_j & \ldots & a_n \\
\hline
a_1 & & & & & & \\
a_2 & & & & & & \\
\vdots & & & & \vdots & & \\
a_i & & & \ldots & a_k & & \\
\vdots & & & & & & \\
a_n & & & & & &
\end{array}$$

kde $a_k = a_i * a_j$. Príklady Cayleyho tabuliek sú v nasledujúcom texte.

*) Arthur Cayley (1821–1896), anglický matematik.

Príklad 1.4. Nech $A = \{a, b, c\}$. Operáciu $\square$ ako aj $\triangle$ na množine A „zadáme“ Cayleyho tabuľkou:

$\square$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\triangle$	a	b	c
a	a	a	a
b	c	b	c
c	b	b	a

Napíšte všetky možné kompozície prvkov množiny A v operácii $\square$ ako aj v operácii $\triangle$.

Definícia 1.2. Nech $*$ je operácia na množine A, ktorá má nasledujúcu vlastnosť:

(AZ) Pre každé $a, b, c \in A$ platí $(a * b) * c = a * (b * c)$.

Potom hovoríme, že $*$ je *asociatívna* operácia. Vlastnosť (AZ) nazývame asociatívny zákon.

Definícia 1.3. Nech $*$ je operácia na množine A, ktorá má nasledujúcu vlastnosť:

(KZ) Pre každé $a, b \in A$ platí $a * b = b * a$.

Potom hovoríme, že $*$ je *komutatívna* operácia. Vlastnosť (KZ) nazývame komutatívny zákon.

Poznámka 1.1. Z Cayleyho tabuľky ľahko zistíme, že daná operácia je komutatívna. Naozaj, tabuľka komutatívnej operácia je symetrická podľa osi, ktorá ide z ľavého horného rohu do pravého dolného (prečo?). Vidíme, že operácia $\square$ v príklade 1.4 je, zatiaľ čo operácia $\triangle$ nie je komutatívna.

Príklad 1.5. Na množine $K_4 = \{1, -1, i, -i\}$ je definovaná operácia „obyčajné násobenie komplexných čísel“. Máme tak nasledujúcu Cayleyho tabuľku:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Vidieť, že operácia je komutatívna. Je aj asociatívna, lebo ako vieme zo strednej školy, násobenie komplexných čísel je asociatívna operácia.

Príklad 1.6. Na množine racionálnych čísel Q definujeme operáciu $\bullet$ tak, že pre každé $a, b \in Q$ platí

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

kde na pravej strane rovnosti je aritmetický priemer čísel a, b. Napr. $2 \bullet 3 = \frac{5}{2}$, $\frac{2}{3} \bullet 7 = \frac{1}{2}(\frac{2}{3} + 7) = \frac{23}{6}$. Je jasné, že $\bullet$ je komutatívna operácia. Ukážeme, že nie je asociatívna. Počítame:

$$(a \bullet b) \bullet c = [\tfrac{1}{2}(a+b)] \bullet c = \tfrac{1}{2}(\tfrac{1}{2}(a+b)+c)) = \tfrac{1}{4}a + \tfrac{1}{4}b + \tfrac{1}{2}c,$$

zatiaľ čo

$$a \bullet (b \bullet c) = a \bullet (\tfrac{1}{2}(b+c)) = \tfrac{1}{2}(a + \tfrac{1}{2}(b+c)) = \tfrac{1}{2}a + \tfrac{1}{4}b + \tfrac{1}{4}c.$$

Vidieť, že rovnosť $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ neplatí pre ľubovoľné racionálne čísla a, b, c. Ak zvolíme napr. $a = b = 1,\ \ c = 3$, tak $(a \bullet b) \bullet c = \frac{1}{4} + \frac{1}{4} + \frac{3}{2} = 2$, ale $a \bullet (b \bullet c) = \frac{1}{2} + \frac{1}{4} + \frac{3}{4} = \frac{3}{2}$.

Príklad 1.7. Operácia z predchádzajúceho príkladu bola komutatívna a nebola asociatívna. Uvedieme príklad operácie, ktorá je asociatívna a nie je komutatívna. Štyri reálne čísla $a, b, c, d \in R$ zapísané do dvoch riadkov a dvoch stĺpcov takto

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

nazývame štvorcovou maticou druhého stupňa.*) Reálne čísla a, b, c, d sú prvky matice. Matice označujeme veľkými tučnými písmenami, napr.

$$\mathbf{A} = \begin{pmatrix} 2, & -\frac{5}{2} \\ 0, & \sqrt{3} \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} 1, & 0 \\ -1, & 5 \end{pmatrix}.$$

Množina

$$\mathcal{M} = \left\{ \begin{pmatrix} a, & b \\ c, & d \end{pmatrix};\quad a, b, c, d \in R \right\}$$

je množina všetkých matíc druhého stupňa s reálnymi prvkami. Na množine $\mathcal{M}$ definujeme násobenie „·“ takto:

Nech

$$\mathbf{A} = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} x, & y \\ z, & v \end{pmatrix}$$

sú ľubovoľné matice z množiny $\mathcal{M}$. Potom

$$\mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \cdot \begin{pmatrix} x, & y \\ z, & v \end{pmatrix} = \begin{pmatrix} ax + bz, & ay + bv \\ cx + dz, & cy + dv \end{pmatrix}.$$

Všimnime si, že pri násobení matíc násobíme každý riadok prvej matice s každým stĺpcom druhej matice. Prvý prvok riadku prvej matice násobíme s prvým prvkom stĺpca druhej matice, druhý prvok riadku prvej matice s druhým prvkom stĺpca druhej matice a vzniklé súčiny sčítame. Ak sme násobili i-tý riadok s j-tým stĺpcom $(i, j = 1, 2)$, výsledný súčin dáme do i-teho riadku a j-teho stĺpca výslednej matice. Napr.:

$$\begin{pmatrix} 1, & -3 \\ 2, & 1 \end{pmatrix} \cdot \begin{pmatrix} 2, & 2 \\ -1, & 3 \end{pmatrix} = \begin{pmatrix} 1 \cdot 2 + (-3) \cdot (-1), & 1 \cdot 2 + (-3) \cdot 3 \\ 2 \cdot 2 + 1 \cdot (-1), & 2 \cdot 2 + 1 \cdot 3 \end{pmatrix} = \begin{pmatrix} 5, & -7 \\ 3, & 7 \end{pmatrix}.$$

Aby sme ukázali, že násobenie matíc nie je komutatívne, vynásobíme dané matice v obrátenom poradí

$$\begin{pmatrix} 2, & 2 \\ -1, & 3 \end{pmatrix} \cdot \begin{pmatrix} 1, & -3 \\ 2, & 1 \end{pmatrix} = \begin{pmatrix} 6, & -4 \\ 5, & 6 \end{pmatrix}.$$

*) Druhého stupňa preto, lebo v nej máme 2 riadky a 2 stĺpce.

Vidíme, že sme dostali rôzne výsledky, t.j. komutatívny zákon pre násobenie matíc neplatí. Pre dôkaz neplatnosti komutatívneho zákona (akéhokoľvek tvrdenia v matematike) stačí nájsť príklad, v ktorom tento zákon (toto tvrdenie) neplatí. Takémuto príkladu hovoríme kontrapríklad. Na druhej strane, ak chceme dokázať, že nejaké tvrdenie (napr. asociatívny zákon pre matice druhého stupňa) platí, musíme to urobiť všeobecne.

Nech teda $\mathbf{A}, \mathbf{B}, \mathbf{C}$ sú ľubovoľné tri matice z množiny $\mathcal{M}$ také, že

$$\mathbf{A} = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} p, & r \\ s, & t \end{pmatrix}, \qquad \mathbf{C} = \begin{pmatrix} x, & y \\ u, & z \end{pmatrix}.$$

Najprv vypočítame

$$\begin{aligned}(\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{C} = \left[\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \cdot \begin{pmatrix} p, & r \\ s, & t \end{pmatrix}\right] \cdot \begin{pmatrix} x, & y \\ u, & z \end{pmatrix} &= \\ = \begin{pmatrix} ap + bs, & ar + bt \\ cp + ds, & cr + dt \end{pmatrix} \cdot \begin{pmatrix} x, & y \\ u, & z \end{pmatrix} &= \\ = \begin{pmatrix} apx + bsx + aru + btu, & apy + bsy + arz + btz \\ cpx + dsx + cru + dtu, & cpy + dsy + crz + dtz \end{pmatrix}&.\end{aligned}$$

Teraz vypočítame:

$$\begin{aligned}\mathbf{A} \cdot (\mathbf{B} \cdot \mathbf{C}) = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \cdot \left[\begin{pmatrix} p, & r \\ s, & t \end{pmatrix} \cdot \begin{pmatrix} x, & y \\ u, & z \end{pmatrix}\right] &= \\ = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \cdot \begin{pmatrix} px + ru, & py + rz \\ sx + tu, & sy + tz \end{pmatrix} &= \\ = \begin{pmatrix} apx + aru + bsx + btu, & apy + arz + bsy + btz \\ cpx + cru + dsx + dtu, & cpy + crz + dsy + dtz \end{pmatrix}&.\end{aligned}$$

Dostali sme rovnaké výsledky, teda asociatívny zákon platí.

Príklad 1.8. Niekedy treba zistiť komutatívnosť alebo asociatívnosť operácie zadanej Cayleyho tabuľkou. Ako sme povedali v poznámke 1.1, komutatívne operácie majú symetrické tabuľky podľa osi idúcej z ľavého horného do pravého dolného rohu tabuľky. Teda komutatívnosť operácie overíme ľahko. Zložitejšie je to s dokazovaním asociatívneho zákona. Musíme ho totiž overiť pre všetky trojice prvkov danej množiny. Ak má množina n prvkov, všetkých trojíc je n^3 (prečo?). Už pre $n = 3$ je to 27 trojíc. Ak to chceme zvládnuť aspoň pre malé tabuľky, musíme si postup „zracionalizovať“. Nech je daná operácia „$\cdot$“ tabuľkou na n-prvkovej množine A. Hovoríme, že prvok $x \in A$ asociuje, ak platí $(a \cdot x) \cdot b = a \cdot (x \cdot b)$ pre všetky dvojice prvkov $a, b \in A$. Čitateľ nech si premyslí, že dokázať asociatívny zákon pre operáciu „$\cdot$“ je to isté ako dokázať, že všetky prvky množiny A asociujú. To možno relatívne ľahko urobiť pomocou n dvojíc tabuliek. Ukážeme si to na operácii „$\cdot$“

definovanej na trojprvkovej množine $A = \{a, b, c\}$ nasledujúcou tabuľkou

$\cdot$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

Hneď vidno, že operácia je komutatívna. Dokážeme, že je asociatívna. Najprv overíme, že prvok $a \in A$ asociuje. Zostrojíme nasledujúcu dvojicu tabuliek:

$\cdot$	a	b	c
$a \cdot a = b$	c	a	b
$b \cdot a = c$	a	b	c
$c \cdot a = a$	b	c	a

$\cdot$	$a \cdot a = b$	$a \cdot b = c$	$a \cdot c = a$
a	c	a	b
b	a	b	c
c	b	c	a

Všimnime si, že napr. na treťom mieste druhého riadku prvej tabuľky je vypočítaný prvok $(b \cdot a) \cdot c$, zatiaľ čo na tom istom mieste v druhej tabuľke prvok $b \cdot (a \cdot c)$. Keďže oba tieto prvky sú rovné prvku c, platí $(b \cdot a) \cdot c = b \cdot (a \cdot c)$. Podobne to platí pre ostatné miesta oboch tabuliek. Polia tabuliek sú rovnaké, z čoho vyplýva, že prvok a asociuje. Nasledujúca dvojica tabuliek dokazuje, že prvok b tiež asociuje.

$\cdot$	a	b	c
$a \cdot b = c$	a	b	c
$b \cdot b = a$	b	c	a
$c \cdot b = b$	c	a	b

$\cdot$	$b \cdot a = c$	$b \cdot b = a$	$b \cdot c = b$
a	a	b	c
b	b	c	a
c	c	a	b

Ostatnú dvojicu tabuliek, ktorá dokáže, že prvok c asociuje tiež, si čitateľ zostrojí sám.

Príklad 1.9. Uvedieme príklady binárnych operácií na číselných množinách:

(1) Sčítanie na množine všetkých prirodzených čísel N.
(2) Sčítanie na množine celých čísel Z (na množine racionálnych čísel Q, na množine reálnych čísel R, na množine komplexných čísel C).
(3) Násobenie na množinách uvedených v bode 1 a 2.
(4) Odčítanie na množine Z (Q, R, C).
(5) Delenie na množine kladných racionálnych čísel Q^+ (na množine kladných reálnych čísel R^+).
(6) Umocňovanie na množine prirodzených čísel N; kompozíciou prirodzených čísel x, y je číslo $x^y \in N$.
(7) Výpočet geometrického priemeru na množine R^+. Kompozíciou dvoch kladných reálnych čísel x, y je $\sqrt{x \cdot y} \in R^+$.
(8) Určenie minima (maxima) dvoch reálnych čísel. Kompozíciou $x, y \in R$ je $\min(x, y)$, resp. $\max(x, y)$.
(9) Určenie najväčšieho spoločného deliteľa dvoch prirodzených čísel. Kompozíciou dvoch čísel $x, y \in N$ je ich najväčší spoločný deliteľ (x, y).

Operácie (1), (2) a (3) sú komutatívne aj asociatívne, operácie (4), (5), (6) nie sú ani komutatívne ani asociatívne, operácia (7) je komutatívna ale nie asociatívna, operácie (8), (9) sú aj komutatívne aj asociatívne.

Príklad 1.10. Na množine $\mathcal{M}$ matíc 2. stupňa s reálnymi prvkami z príkladu 1.7 možno definovať sčítanie takto:

$$\mathbf{A}+\mathbf{B}=\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}+\begin{pmatrix} x, & y \\ z, & v \end{pmatrix}=\begin{pmatrix} a+x, & b+y \\ c+z, & d+v \end{pmatrix}.$$

Ľahko sa možno presvedčiť, že táto operácia je asociatívna i komutatívna.

Teraz si definujeme ďalšie vlastnosti operácií.

Definícia 1.4. Nech $*$ je operácia na množine A. Prvok $e_1 \in A$ nazývame *ľavým neutrálnym prvkom* operácie $*$, ak pre každé $a \in A$ platí $e_1 * a = a$.

Podobne prvok e_2 nazývame *pravým neutrálnym prvkom* operácie $*$, ak pre každé $a \in A$ platí $a * e_2 = a$.

Prvok $e \in A$, ktorý je zároveň ľavým i pravým neutrálnym prvkom operácie $*$ nazývame *neutrálnym prvkom* operácie $*$. Pre takýto prvok platí: Pre každé $a \in A$ $e * a = a * e = a$.

Príklad 1.11. Všimnime si dve operácie definované nasledujúcimi Cayleyho tabuľkami:

$*$	a	b	c
a	a	b	c
b	c	a	b
c	a	b	c

$\star$	a	b	c
a	a	a	a
b	c	b	b
c	a	c	c

Prvá z nich má dva ľavé neutrálne prvky a žiadny pravý. Druhá dva pravé a žiadny ľavý. Z nasledujúcej vety bude jasné, čo sa stane, keď operácia má zároveň ľavé i pravé neutrálne prvky.

Veta 1.1. *Nech $e_1 \in A$ je ľubovoľný ľavý a prvok $e_2 \in A$ ľubovoľný pravý neutrálny prvok operácie $*$. Potom $e_1 = e_2$.*

Dôkaz. Keďže e_1 je ľavý neutrálny prvok, platí $e_1 * e_2 = e_2$. Podobne, keďže e_2 je pravý neutrálny prvok, platí $e_1 * e_2 = e_1$. Vidíme, že $e_1 = e_2$. □

Poznámka 1.2. Z tvrdenia vety vyplýva, že keď operácia má popri ľavých neutrálnych prvkoch aspoň jeden pravý, všetky tieto prvky splynú do jedného (obojstranného) neutrálneho prvku, t.j. *operácia nemá žiadny alebo práve jeden neutrálny prvok.* Toto tvrdenie je známe ako *veta o unicite neutrálneho prvku.*

Príklad 1.12. Neutrálnym prvkom operácií (2) z príkladu 1.9 je číslo 0. Neutrálnym prvkom operácií (3) je číslo 1. Ostatné operácie príkladu 1.9 neutrálny prvok nemajú. Prosíme čitateľa, aby sa presvedčil, že neutrálnym prvkom operácie z príkladu 1.7 je tzv. jednotková matica; podobne neutrálnym prvkom operácie z príkladu 1.10 je tzv. nulová matica

$$\mathbf{J}_2=\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, \qquad \mathbf{0}_2=\begin{pmatrix} 0, & 0 \\ 0, & 0 \end{pmatrix}.$$

Poznámka 1.3. Ak je operácia zapísaná aditívne (pomocou znaku „+“), neutrálnemu prvku hovoríme aj *nulový prvok,* podobne pri multiplikatívnom zápise (pomocou znaku „·“), neutrálnemu prvku hovoríme *jednotkový prvok.*

Definícia 1.5. Nech $*$ je operácia s neutrálnym prvkom e. Nech $x \in A$. Ak existuje prvok $x^{-1} \in A$ taký, že platí

$$x * x^{-1} = x^{-1} * x = e,$$

tak prvok x^{-1} nazývame *inverzný* k prvku x.

Príklad 1.13. Uvažujme o operácii násobenia matíc 2. stupňa definovanej v príklade 1.7. Vypočítajte inverzný prvok $\mathbf{A}^{-1}$ k matici

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

Máme nájsť maticu $\mathbf{A}^{-1}$ takú, že platí $\mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{A} \cdot \mathbf{A}^{-1} = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$.
Nech

$$\mathbf{A}^{-1} = \begin{pmatrix} x, & y \\ z, & v \end{pmatrix}.$$

Počítame

$$\mathbf{A}^{-1} \cdot \mathbf{A} = \begin{pmatrix} x, & y \\ z, & v \end{pmatrix} \cdot \begin{pmatrix} 3, & 4 \\ 1, & 2 \end{pmatrix} = \begin{pmatrix} 3x + y, & 4x + 2y \\ 3z + v, & 4z + 2v \end{pmatrix}.$$

Keďže $\mathbf{A}^{-1} \cdot \mathbf{A} = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$, máme

$$\begin{aligned} 3x + y = 1, \quad & 3z + v = 0, \\ 4x + 2y = 0, \quad & 4z + 2v = 1, \end{aligned}$$

odkiaľ ľahko vypočítame $x = 1, \quad y = -2, \quad z = -\frac{1}{2}, \quad v = \frac{3}{2}$, t.j. hľadaná matica je

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

Urobíme skúšku:

$$\mathbf{A}^{-1} \cdot \mathbf{A} = \begin{pmatrix} 1, & -2 \\ -\frac{1}{2}, & \frac{3}{2} \end{pmatrix} \cdot \begin{pmatrix} 3, & 4 \\ 1, & 2 \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}.$$

Podobne

$$\mathbf{A} \cdot \mathbf{A}^{-1} = \begin{pmatrix} 3, & 4 \\ 1, & 2 \end{pmatrix} \cdot \begin{pmatrix} 1, & -2 \\ -\frac{1}{2}, & \frac{3}{2} \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}.$$

Teda inverzný prvok k matici $\mathbf{A}$ je matica $\mathbf{A}^{-1}$. Voláme ju jednoducho inverzná matica.

Pokúsme sa nájsť inverznú maticu k matici

$$\mathbf{B} = \begin{pmatrix} 3, & 2 \\ 6, & 4 \end{pmatrix}.$$

Podobne ako vyššie

$$\mathbf{B}^{-1}\cdot\mathbf{B}=\begin{pmatrix}a, & b\\ c, & d\end{pmatrix}\cdot\begin{pmatrix}3, & 2\\ 6, & 4\end{pmatrix}=\begin{pmatrix}3a+6b, & 2a+4b\\ 3c+6d, & 2c+4d\end{pmatrix}=\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix},$$

odkiaľ

$$\begin{aligned}3a+6b&=1, & 3c+6d&=0,\\ 2a+4b&=0, & 2c+4d&=1.\end{aligned}$$

Skúsme vyriešiť prvú sústavu rovníc o 2 neznámych: Z druhej rovnice máme $a=-2b$. Dosadením do prvej rovnice je $3(-2b)+6b=1$ čiže $0=1$. Posledný výrok je nepravdivý, sústava riešenie nemá. K matici $\mathbf{B}$ teda inverzná matica neexistuje. Pokúste sa vyšetriť, kedy matica 2. stupňa má a kedy nemá inverznú maticu (pozri cvičenie 1.12).

Poznámka 1.4. Ak je operácia zapísaná aditívne (pomocou znaku „+"), inverzný prvok k prvku a označíme $-a$ a nazývame ho *opačný prvok.* Ak je operácia zapísaná multiplikatívne, inverzný prvok k prvku a označujeme ako vyššie a^{-1} (niekedy ho nazývame aj *prevrátený prvok*). Pri konkrétne zadaných množinách miesto slova prvok môžeme používať názov prvku danej množiny, napr. opačné číslo, prevrátené číslo, inverzná matica, inverzné zobrazenie, atď.

Definícia 1.6. Nech $\oplus,\odot$ sú operácie definované na množine A. Operácia $\odot$ je *zľava distributívna* vzhľadom na operáciu $\oplus$, ak pre každé $x,y,z\in A$ platí

$$\text{(ĽDZ)}\qquad x\odot(y\oplus z)=(x\odot y)\oplus(x\odot z).$$

Podobne operácia $\odot$ je *sprava distributívna* vzhľadom na $\oplus$, ak pre každé $x,y,z\in A$ platí

$$\text{(PDZ)}\qquad (y\oplus z)\odot x=(y\odot x)\oplus(z\odot x).$$

Ak je operácia $\odot$ zľava i sprava distributívna vzhľadom na $\oplus$, hovoríme, že je *distributívna* vzhľadom na operáciu $\oplus$. Vlastnosti (ĽDZ) resp. (PDZ) nazývame ľavý resp. pravý distributívny zákon.

Poznámka 1.5. Čitateľ zo strednej školy vie, že zátvorkami označujeme poradie operácií, pritom operácia v zátvorke sa robí najskôr. Platí však takýto dohovor: Ak sa v jednom výraze nachádzajú dve operácie zapísané aditívne a multiplikatívne a zátvorkou nie je vyznačené ich poradie, multiplikatívne zapísanú operáciu robíme najprv. Napr. na množine celých čísel (PDZ) píšeme $(y+z)\cdot x=y\cdot x+z\cdot x$, teda bez zátvoriek na pravej strane. Keďže znak násobenia možno vynechať, zápis možno ďalej zjednodušiť: $(y+z)x=yx+zx$.

Príklad 1.14 Dokážeme, že operácia „·" definovaná v príklade 1.7 je distributívna vzhľadom na operáciu + definovanú v príklade 1.10. Nech $\mathbf{A},\mathbf{B},\mathbf{C}\in\mathcal{M}$ sú ľubovoľné tri matice 2. stupňa, ktorých prvky sú reálne čísla. Pre určitosť nech

$$\mathbf{A}=\begin{pmatrix}x, & y\\ z, & v\end{pmatrix},\qquad \mathbf{B}=\begin{pmatrix}a, & b\\ c, & d\end{pmatrix},\qquad \mathbf{C}=\begin{pmatrix}k, & l\\ m, & n\end{pmatrix}.$$

Počítajme

$$\mathbf{A}\cdot(\mathbf{B}+\mathbf{C}) = \begin{pmatrix} x, & y \\ z, & v \end{pmatrix} \cdot \left[\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} + \begin{pmatrix} k, & l \\ m, & n \end{pmatrix}\right] =$$

$$= \begin{pmatrix} x, & y \\ z, & v \end{pmatrix} \cdot \begin{pmatrix} a+k, & b+l \\ c+m, & d+n \end{pmatrix} = \begin{pmatrix} xa+xk+yc+ym, & xb+xl+yd+yn \\ za+zk+vc+vm, & zb+zl+vd+vn \end{pmatrix} =$$

$$= \begin{pmatrix} xa+yc, & xb+yd \\ za+vc, & zb+vd \end{pmatrix} + \begin{pmatrix} xk+ym, & xl+yn \\ zk+vm, & zl+vn \end{pmatrix} = \begin{pmatrix} x, & y \\ z, & v \end{pmatrix} \cdot \begin{pmatrix} a, & b \\ c, & d \end{pmatrix} +$$

$$+ \begin{pmatrix} x, & y \\ z, & v \end{pmatrix} \cdot \begin{pmatrix} k, & l \\ m, & n \end{pmatrix} = \mathbf{A}\cdot\mathbf{B} + \mathbf{A}\cdot\mathbf{C}$$

Dokázali sme, že (ĽDZ) platí. Podobne sa dokáže i (PDZ). (Urobte to!)

Príklad 1.15 Nech operácia $+$ je obyčajné sčítanie definované na množine reálnych čísel. Na množine R definujme aj nasledovnú operáciu:
Pre každé $x, y \in R: \ x \star y = y$. Ukážeme, že operácia $\star$ je zľava distributívna k operácii $+$, ale nie je sprava distributívna k tej istej operácii. Naozaj $x \star (y+z) = y+z$ ako aj $(x \star y) + (x \star z) = y + z$. Teda $x \star (y+z) = (x \star y) + (x \star z)$. Ale ak vypočítame $(y+z) \star x = x$ ako aj $(y \star x) + (z \star x) = x + x = 2x$, vidíme, že stačí voliť $x \neq 0$, aby $(y+z) \star x \neq (y \star x) + (z \star x)$.

Veta 1.2. *Nech $*$ je asociatívna operácia definovaná na množine A. Nech e je neutrálny prvok danej operácie. Nech, ďalej, a_1^{-1} i a_2^{-1} sú inverzné prvky k prvku $a \in A$. Potom $a_1^{-1} = a_2^{-1}$.*

Dôkaz. Nech a_1^{-1} a a_2^{-1} sú inverzné prvky k prvku $a \in A$. Potom
$a_1^{-1} = a_1^{-1} * e = a_1^{-1} * (a * a_2^{-1}) = (a_1^{-1} * a) * a_2^{-1} = e * a_2^{-1} = a_2^{-1}$.

Poznámka 1.6. Vo vetách 1.1 a 1.2 sme dokázali tzv. unicitu (jedinečnosť) neutrálneho i inverzného prvku. Všimnime si, že na dôkaz unicity inverzného prvku sme potrebovali predpoklad, že operácia je asociatívna. Ak operácia nie je asociatívna, inverzný prvok nemusí byť iba jeden, ako uvidíme v nasledujúcom príklade.

Príklad 1.16. Nech je daná množina $A = \{e, a, b, c\}$ a na nej operácia $*$ daná tabuľkou:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	e	e
b	b	e	c	a
c	c	e	a	a

Vidieť, že e je neutrálny prvok, b, c sú dva rôzne inverzné prvky k prvku a. Je to možné preto, lebo (AZ) neplatí. Skutočne napr. $a * (b * c) = a * a = b$, ale $(a * b) * c = e * c = c$.

Príklad 1.17. Nech je daná množina $A = \{a, b\}$. Systém všetkých podmnožín množiny A je $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Zostrojíme Cayleyho tabuľky pre operácie zjednotenie a prienik na množine $\mathcal{P}(A)$.

Dané tabuľky sú:

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	A
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	A
$\{a\}$	$\{a\}$	$\{a\}$	A	A
$\{b\}$	$\{b\}$	A	$\{b\}$	A
A	A	A	A	A

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	A
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
A	$\emptyset$	$\{a\}$	$\{b\}$	A

Obe operácie sú asociatívne i komutatívne. $\emptyset$ je neutrálnym prvkom operácie zjednotenia. A je neutrálnym prvkom prieniku. Prienik je distributívny vzhľadom na zjednotenie. Aj naopak: Zjednotenie je distributívna operácia vzhľadom na prienik. (Skontrolujte to!) Teda prienik a zjednotenie sú navzájom distributívne. To vždy neplatí. Napríklad v množine reálnych čísel: násobenie je distributívne vzhľadom na sčítanie, zatiaľ čo sčítanie nie je distributívne vzhľadom na násobenie.

Poznámka 1.7. V oboch operáciách príkladu 1.17 sú zvláštne prvky, ktoré sa chovajú „agresívne“. Je to prvok A v operácii $\cup$ a prvok $\emptyset$ v operácii $\cap$. Presnejšie:

Prvok $a \in G$ operácie $*$ definovanej na množine G nazývame *agresívnym prvkom,* ak pre každé $x \in G$ platí: $a * x = x * a = a$.

Z predchádzajúcich príkladov binárnych operácií sme videli, že binárna operácia je vždy definovaná na nejakej neprázdnej množine. A práve množina a operácia na nej definovaná, spolu s vlastnosťami tejto operácie, tvoria algebraickú štruktúru s jednou operáciou. Postupne si budeme definovať tieto algebraické štruktúry: *grupoid, pologrupa, monoid, grupa.* Poslednej z nich, *grupe*, bude venovaný celý nasledujúci paragraf.

Definícia 1.7. Nech je daná neprázdna množina G a na nej definovaná binárna operácia $*$. Potom dvojicu $(G, *)$ nazývame *grupoid.*

Grupoid môže byť konečný, ak množina G je konečná, alebo nekonečný, ak množina G je nekonečná.

Grupoid môže byť komutatívny ak operácia $*$ je komutatívna, alebo nekomutatívny, ak operácia $*$ je nekomutatívna.

Ak nie je žiadna pochybnosť o tom aká operácia je definovaná na množine G, grupoid $(G, *)$ často označujeme skrátene: len znakom G.

Príklad 1.18. Uvedieme príklady grupoidov.

a) Operácie z bodov (1), (2) a (3) príkladu 1.9 spolu s množinami na ktorých sú definované dávajú tieto grupoidy: $(N,+)$, $(N,\cdot)$, $(Z,+)$, $(Z,\cdot)$, $(Q,+)$, $(Q,\cdot)$, $(R,+)$, $(R,\cdot)$, $(C,+)$, $(C,\cdot)$. Sú to všetko nekonečné komutatívne grupoidy.
b) Grupoidy s operáciami z bodu (4) a (5) príkladu 1.9 $(Z,-)$, $(Q,-)$, $(R,-)$, $(C,-)$, $(Q^+,:)$, $(R^+,:)$ sú nekonečné nekomutatívne grupoidy.
c) Ak operáciu umocňovanie na množine N z bodu (6) príkladu 1.9 označíme hoci znakom $\uparrow$, t.j. $a \uparrow b = a^b$, dostávame grupoid $(N, \uparrow)$, ktorý je tiež nekonečný a nekomutatívny.
d) Grupoidy $(\mathcal{M}, \cdot)$ z príkladu 1.7 a $(\mathcal{M}, +)$ z príkladu 1.10 sú nekonečné grupoidy. Prvý je nekomutatívny, druhý komutatívny.

e) Grupoidy s operáciami zadanými pomocou Cayleyho tabuľky v príkladoch 1.4, 1.5, 1.8, 1.11, 1.16 a 1.17 sú konečné. Grupoid z príkladu 1.5 označíme $(K_4, \cdot)$, grupoidy z príkladu 1.16 $(\mathcal{P}(A), \cup)$, $(\mathcal{P}(A), \cap)$ a podobne aj v ďalších príkladoch.

Definícia 1.8. Grupoid $(G, *)$, v ktorom operácia „$*$" je asociatívna sa nazýva *pologrupa.*

Množina G v danej pologrupe môže, ale nemusí obsahovať neutrálny prvok operácie. Ak ho obsahuje, hovoríme, že pologrupa je s neutrálnym prvkom. Takejto pologrupe hovoríme aj *monoid.*

Príklad 1.19. Čitateľ nech si skontroluje nasledovné tvrdenia:

a) Všetky grupoidy z príkladu 1.18 a) sú pologrupami. Všetky tieto pologrupy okrem pologrupy $(N, +)$ sú pologrupy s neutrálnym prvkom t.j. monoidami.
b) Grupoidy z príkladu 1.18 b) a c) pologrupami nie sú.
c) Grupoidy $(\mathcal{M}, +)$, $(\mathcal{M}, \cdot)$, $(K_4, \cdot)$, $(\mathcal{P}(A), \cup)$, $(\mathcal{P}(A), \cap)$ z príkladu 1.18 d) a e) sú tiež monoidy.
d) Grupoid $(Q, \bullet)$ z príkladu 1.6 ako aj $(A, *)$ z príkladu 1.16 pologrupou nie je.

Príklad 1.20. Uvedieme dôležitý príklad monoidu. Nech A je neprázdna množina a nech $\mathcal{Z} = \{f;\ f : A \to A\}$, t.j. $\mathcal{Z}$ je množina všetkých zobrazení množiny A do seba. Ak znakom $\circ$ označíme operáciu skladania zobrazení na množine A, tak štruktúra $(\mathcal{Z}, \circ)$ je monoid. Aby sme to dokázali, predpokladajme, že $f, g, h \in \mathcal{Z}$ sú ľubovoľné zobrazenia množiny A do seba a $x \in A$ je ľubovoľný prvok množiny A. Počítajme:

$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$,

znova:

$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$.

Vidíme, že $(f \circ g) \circ h = f \circ (g \circ h)$, t.j. skladanie zobrazení je asociatívne.

Neutrálnym prvkom operácie $\circ$ je identické zobrazenie $i : A \to A$ definované takto: *Pre všetky* $x \in A$ *je* $i(x) = x$. Dokážeme, že pre všetky $f \in \mathcal{Z}$ je $i \circ f = f \circ i = f$. Naozaj, ak $x \in A$ je ľubovoľný prvok množiny A, tak platí:

$$(i \circ f)(x) = i(f(x)) = f(x),$$

ako aj

$$(f \circ i)(x) = f(i(x)) = f(x),$$

čo znamená, že zobrazenie $i \circ f$ resp. $f \circ i$ zobrazuje tak, ako zobrazenie f.

Veta 1.3 (všeobecný asociatívny zákon)**.** *Nech $(P, \cdot)$ je pologrupa. Potom súčin viacerých činiteľov (prvkov množiny P) nezávisí od spôsobu uzátvorkovania.*

Veta 1.4 (všeobecný komutatívny zákon)**.** *Nech $(P, \cdot)$ je komutatívna pologrupa. Potom súčin viacerých činiteľov (prvkov množiny P) nezávisí od poradia činiteľov.*

Dôkazy oboch viet ponecháme na čitateľa (cvičenie 1.25 a 1.26).

Príklad 1.21. Na množine $A = \{a, b, c, d\}$ definujme binárnu operáciu „$\cdot$“ nasledovnou Cayleyho tabuľkou.

$\cdot$	a	b	c	d
a	b	d	a	c
b	c	a	d	b
c	a	c	b	d
d	d	b	c	a

Čitateľ si ľahko overí, že grupoid $(A, \cdot)$ nie je asociatívny. Ukážeme, že v takejto štruktúre nie je možné definovať tretiu mocninu. Naozaj: $(a \cdot a) \cdot a = b \cdot a = c$, ale $a \cdot (a \cdot a) = a \cdot b = d$, čiže súčin troch rovnakých činiteľov je raz rovný c raz d. Nevieme jednoznačne určiť hodnotu a^3. Teda v neasociatívnej štruktúre sa tretia, a tým ani vyššie mocniny, definovať nedajú. Inak je to v pologrupe, kde platí asociatívny zákon. Tam pre každý prvok pologrupy x platí $(x \cdot x) \cdot x = x \cdot (x \cdot x)$ a tak jednoznačne určený súčin troch prvkov môžeme označiť x^3.

Definícia 1.9. Nech $(P, \cdot)$ pologrupa. Nech $a \in P$ je ľubovoľný prvok pologrupy P a n je prirodzené číslo. Potom mocnina a^n prvku a je prvok pologrupy P majúci nasledovné vlastnosti:

(i) $$a^1 = a,$$

(ii) $$a^{n+1} = a^n \cdot a,$$

Ak pologrupa $(P, \cdot)$ je monoid s neutrálnym prvkom e, tak položíme:

(iii) $$a^0 = e.$$

Poznámka 1.8. V pologrupe bez neutrálneho prvku sú teda definované mocniny s prirodzeným exponentom, v monoide môže exponent nadobúdať nezáporné celočíselné hodnoty. Čitateľa upozorňujeme, že pojem mocnina bol v predchádzajúcej definícii definovaný pomocou matematickej indukcie. Mocniny v pologrupe (v monoide) majú známe vlastnosti (cvičenie 1.23 a 1.24).

Poznámka 1.9. Ak pologrupa má operáciu zapísanú aditívne t.j. $(P, +)$, tak miesto mocniny s prirodzeným exponentom

$$a^k = \underbrace{a \cdot a \cdot \ldots \cdot a}_{\text{k razy}} \quad \text{máme prirodzený násobok} \quad k \times a = \underbrace{a + a + \cdots + a}_{\text{k razy}}$$

a vzťahy (i), (ii) a (iii) budú mať tvar

(i') $$1 \times a = a,$$

(ii') $$(n + 1) \times a = n \times a + a,$$

(iii') $$0 \times a = 0,$$

kde znak 0 na ľavej strane rovnosti (iii') znamená celé číslo nula, na pravej neutrálny prvok pologrupy $(P, +)$.

Definícia 1.10. Nech H je neprázdna podmnožina množiny G. Nech $(G,*)$ je grupoid. Ak $(H,*)$ je tiež grupoid, tak ho nazývame *podgrupoid* grupoidu $(G,*)$. Fakt, že H je podgrupoidom G, označujeme $H \subseteq\subseteq G$.

Analogickým spôsobom sa definujú pojmy *podpologrupa a podmonoid* .

Poznámka 1.10. Keď sme operáciu v podgrupoide $(H,*)$ označili tým istým znakom ako v grupoide $(G,*)$, dopustili sme sa istej nepresnosti. Skutočne, operácia v grupoide G je zobrazenie $* : G \times G \to G$ a v grupoide H ide o iné zobrazenie $*_1 : H \times H \to H$, ktoré má (ak H je vlastnou podmnožinou G) iný definičný obor a iný obor hodnôt. Hovoríme, že operácia $*_1$ v podmnožine H je indukovaná operáciou $*$ v množine G, keď pre všetky prvky $a, b \in H$ platí $a *_1 b = a * b$. Ide o tzv. zúženie operácie $*$. A práve v takomto zmysle chápeme operáciu $*_1$ v podgrupoide H. Budeme ju preto v ďalšom označovať rovnako ako operáciu v grupoide G. Poznamenajme ešte, že v podmonoide sa nachádza aj neutrálny prvok monoidu. Môžeme mať aj podpologrupu monoidu, ktorá neutrálny prvok monoidu neobsahuje. Dokonca môžeme mať takú podpologrupu monoidu, ktorá je tiež monoidom ale nie je podmonoidom daného monoidu, lebo má iný neutrálny prvok. (Zostrojte taký príklad!)

Príklad 1.22. Všimnime si štruktúry príkladu 1.18. Ľahko sa presvedčíme, že $(Z,-)$ je podgrupoid grupoidu $(R,-)$, pologrupa $(Z,\cdot)$ je podpologrupou pologrupy $(Q,.)$, pologrupa $(Z,+)$ je podpologrupou grupy $(Q,+)$ a tá zase podpologrupou grupy $(R,+)$. Vzhľadom na predchádzajúcu poznámku uveďme ešte, že aditívna pologrupa $(N,+)$ je podpologrupou – nie podmonoidom – monoidu $(N \cup \{0\},+)$ nezáporných celých čísel.

Cvičenia

1.1 Zistite, či sčítanie celých čísel je operácia na množine

$$A = \{x;\ x = 5n,\ kde\ n \in Z\}.$$

1.2. Na množine reálnych čísel sú dané nasledujúce operácie:

a) $x * y = 0$, b) $x * y = 1$, c) $x * y = x + y - xy$,
d) $x * y = x + y + xy$, e) $x * y = \frac{1}{2}(x + y)$.

Zistite, ktorá z daných operácií je komutatívna, ktorá je asociatívna a ktorá má neutrálny prvok. Ak neutrálny prvok existuje, určte ho.

1.3. Na množine kladných reálnych čísel sú dané nasledujúce operácie:

a) $a * b = \frac{a \cdot b}{a+b}$, b) $a * b = a^2 + b^2$,

Zistite, ktorá z operácií je komutatívna, ktorá asociatívna a ktorá má agresívny prvok.

1.4. Rozhodnite, ktorá z uvedených podmnožín $\{-1,0,1\}$, $(0,\infty)$, $(-\infty,0)$, $\langle -1,1\rangle$, $(0,1)$ množiny všetkých reálnych čísel je uzavretá vzhľadom na operáciu obvyklého násobenia.

1.5. Zistite, aké vlastnosti majú tieto operácie definované na množine N:

a) $x * y = x^y$, b) $x * y = \max(x,y)$,

1.6 Nech $\triangle$ je operácia na množine M. Operáciu ∇ definovanú rovnosťou $a \nabla b = b \triangle a$ nazývame operáciou opačnou k operácii $\triangle$. Ak $\triangle$ je asociatívna (komutatívna), tak aj ∇ je asociatívna (komutatívna). Dokážte to.

1.7. V množine celých čísel Z sú definované dve operácie $\oplus$, $\odot$ takto: Ak a, b sú ľubovoľné celé čísla, tak

$$a \oplus b = a + b + 1, \qquad a \odot b = a + b + ab.$$

Dokážte, že operácia $\odot$ je distributívna vzhľadom na operáciu $\oplus$. Platí to aj naopak?

1.8. Na množine všetkých nepárnych prirodzených čísel ${}^1N$ sú definované operácie $\oplus$ a $\odot$ takto: Nech a, b sú ľubovoľné prvky množiny ${}^1N$. Potom

$$a \oplus b = a + b + 1, \qquad a \odot b = \frac{1}{2}(a+1)(b+1) - 1.$$

Dokážte, že operácia $\odot$ je distributívna vzhľadom na operáciu $\oplus$.

1.9. Na množine R sú operácie $\odot, \oplus$ definované takto: Nech x, y sú ľubovoľné reálne čísla. Potom

$$x \odot y = 2x + 2y, \qquad x \oplus y = \frac{1}{2}xy.$$

Zistite, či operácia $\oplus$ je distributívna vzhľadom na operáciu $\odot$.

1.10. Zistite, či operácia „$*$" definovaná na množine Z rovnosťou $x * y = x$ je distributívna vzhľadom na sčítanie celých čísel.

1.11. Určte inverzné matice k nasledujúcim maticiam druhého stupňa:

$$\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \qquad a \in R.$$

1.12. Matica

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad a, b, c, d \in R$$

má inverznú maticu A^{-1} práve vtedy, keď $ad - bc \neq 0$. Dokážte to.

1.13. Nájdite všetky grupoidy definované na množine $\{x, y\}$. Zostavte ich Cayleyho tabuľky. Koľko je grupoidov? Ktoré z nich sú pologrupy?

1.14. Koľko operácií možno definovať na n-prvkovej množine?

1.15. Zostavte Cayleyho tabuľku pre operáciu „$\blacktriangle$" definovanú na množine $A = \{1, 2, 3, 4, 5, 6\}$ týmto spôsobom: ak $a, b \in A$, tak $a \blacktriangle b$ je počet prvočiniteľov čísla $10a + b$.

1.16. Zistite, či operácie dané nasledujúcimi tabuľkami sú asociatívne.

·	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	b	a	d
d	d	b	b	d

·	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

1.17. Nech $(G, \cdot)$ je grupoid majúci neutrálny prvok $e \in G$. Potom $(G, \cdot)$ je Abelova pologrupa práve vtedy, keď pre každé $a, b, c, d \in G$ platí: $(a \cdot b)(c \cdot d) = (a \cdot c)(b \cdot d)$. Dokážte to.

1.18. Neprázdny prienik dvoch podpologrúp danej pologrupy je tiež podpologrupa danej pologrupy. Dokážte to.

1.19. Prienik dvoch podmonoidov daného monoidu je podmonoid daného monoidu. Dokážte to.

1.20. Tvrdenia cvičení 1.18 a 1.19 možno zovšeobecniť na ľubovoľný systém podpologrúp resp. podmonoidov. Urobte to.

1.21. Každé dve podpologrupy pologrupy $(Z^+, +)$ majú neprázdny prienik. Dokážte to. Možno to povedať o podpologrupách pologrupy $(Z, +)$?

1.22. Existuje nekonečne mnoho podpologrúp pologrupy $(Z^+, \cdot)$, ktoré sú po dvoch disjunktné. Dokážte to.

1.23. Nech $(P, \cdot)$ je pologrupa. Dokážte, že pre každé $m, n \in N$ a každé $a \in P$ platí $a^m \cdot a^n = a^{m+n}$.

1.24. Nech $(P, \cdot)$ je komutatívna pologrupa. Dokážte, že pre každé $n \in N$ a každé $a, b \in P$ platí $(a \cdot b)^n = a^n \cdot b^n$.

***1.25.** Dokážte vetu 1.3 (všeobecný asociatívny zákon). *Nech $(P, \cdot)$ je pologrupa. Potom súčin viacerých činiteľov (prvkov množiny P) nezávisí od spôsobu uzátvorkovania.*
Návod. Predpokladajme, že máme n prvkov pologrupy P. Prvky označíme $a_1, a_2, \dots, a_n$. Najprv definujeme „partikulárne súčiny" prvkov a_i takto: $s_1 = a_1$, $s_2 = a_1a_2$, $s_3 = (a_1a_2)a_3$, $s_4 = ((a_1a_2)a_3)a_4$, $s_5 = (((a_1a_2)a_3)a_4)a_5 \dots$, $s_n = (\dots((a_1a_2)a_3)a_4 \dots a_{n-1})a_n$. Potom dokážeme matematickou indukciou podľa n, že „ľubovoľne uzátvorkovaný" súčin prvkov $a_1, a_2, \dots, a_n$ (v danom poradí!) sa vždy rovná prvku s_n.

***1.26.** Dokážte vetu 1.4 (všeobecný komutatívny zákon). *Nech $(P, \cdot)$ je komutatívna pologrupa. Potom súčin viacerých činiteľov (prvkov množiny P) nezávisí od poradia činiteľov.*
Návod. Nech $b, a_1, a_2, \dots, a_n$ sú ľubovoľné prvky pologrupy P. Matematickou indukciou podľa n dokážeme, že $ba_1a_2 \dots a_n = a_1a_2 \dots a_nb$ a potom opäť matematickou indukciou podľa n, že $a_{i_1}a_{i_2} \dots a_{i_n} = a_1a_2 \dots a_n$, kde $i_1, i_2, \dots, i_n$ je iné poradie indexov $1, 2, \dots, n$.

§ 2. Grupy

Pojem *grupy* je jedným z najdôležitejších pojmov algebry a matematiky vôbec. Čitateľa prosíme, aby mu venoval zvýšenú pozornosť. Ak si dobre osvojí základné vlastnosti grupy, veľmi často to ocení v ďalšom štúdiu.

Definícia 2.1. Pologrupa $(G, *)$ s neutrálnym prvkom $e \in G$, v ktorej ku každému prvku z G existuje v G inverzný prvok, sa nazýva *grupa.*

Alebo inak: Monoid, v ktorom každý prvok má inverzný prvok sa nazýva grupa.

Komutatívna grupa sa nazýva aj *Abelova* alebo *abelovská* grupa.[1] Ak grupa $(G, *)$ je konečná, tak počet prvkov množiny G nazývame *rádom grupy* a označujeme ho $r(G)$. O nekonečnej grupe niekedy hovoríme, že má nekonečný rád.

Definíciu grupy vyslovíme ešte raz tak, že osobitne uvedieme každú vlastnosť „grupovej" operácie:

Dvojica $(G, *)$, kde G je neprázdna množina, sa nazýva grupa, ak:

(i) Pre každé $a, b \in G$ existuje $c \in G$, také, že $a * b = c$,
t.j. $*$ je operácia na množine G.

(ii) Pre každé $a, b, c \in G$ platí $(a * b) * c = a * (b * c)$,
t.j. operácia $*$ je asociatívna.

(iii) Existuje také $e \in G$, že pre všetky $a \in G$ platí $a * e = e * a = a$,
t.j. v G existuje neutrálny prvok.

(iv) Ku každému $a \in G$ existuje $a^{-1} \in G$ také, že $a * a^{-1} = a^{-1} * a = e$,
t.j. ku každému prvku z G existuje v G inverzný prvok.

Grupa je abelovská, ak okrem toho

(v) pre každé $a, b \in G$ platí $a * b = b * a$,
t.j. operácia $*$ je komutatívna.

Aby sme dokázali, že algebraická štruktúra s jednou operáciou je grupa, stačí preveriť vlastnosti (i) - (iv).

Príklad 2.1. Na základe vedomostí zo strednej školy, ktoré máme o aritmetických operáciách na množine celých čísel ľahko zistíme, že algebraická štruktúra $(Z, +)$ je grupa. Zrejme $+$ je binárna operácia na Z, t.j. (i) platí. Keďže $+$ je asociatívna operácia (platí $(a+b)+c = a+(b+c)$ pre všetky $a, b, c \in Z$), je splnená aj podmienka (ii). Celé číslo 0 je neutrálnym prvkom operácie $+$, teda (iii) platí. Ku každému celému číslu $a \in Z$ je inverzným prvkom opačné číslo $-a \in Z$, t.j. platí aj (iv). Keďže platí aj (v), $(Z, +)$ je Abelova grupa.

Podobným spôsobom overíme, že aj $(Q, +)$, $(R, +)$, $(C, +)$, sú komutatívne grupy. Použitím stredoškolských vedomostí sa čitateľ môže presvedčiť, že aj nasledovné štruktúry sú grupy: $(Q^+, \cdot)$, $(R^+, \cdot)$, $(Q - \{0\}, \cdot)$, $(R - \{0\}, \cdot)$, $(C - \{0\}, \cdot)$. Sú to všetko nekonečné komutatívne grupy.

Príklad 2.2. Ľahko zistíme, že štruktúra $(K_4, \cdot)$ z príkladu 1.5 je konečná abelovská grupa. Skutočne, ak preskúmame Cayleyho tabuľku v príklade 1.5 vidíme, že vlastnosti (i) - (v) sú splnené. Asociatívnosť operácie „$\cdot$" nemusíme overovať ako v príklade 1.8, lebo ide o násobenie komplexných čísel a to asociatívne je. Neutrálnym prvkom je 1. Inverzné prvky: $1^{-1} = 1$, $(-1)^{-1} = -1$, $i^{-1} = -i$, $(-i)^{-1} = i$. Čitateľ si podobným spôsobom rýchlo overí, že aj štruktúra $(A, \cdot)$ z príkladu 1.8 je grupa. Jej neutrálnym prvkom je prvok c. Rád grupy K_4 je 4, rád grupy A je 3, čo zapisujeme $r(K_4) = 4$ a $r(A) = 3$.

[1] Niels Henrik Abel (1802-1829), nórsky matematik.

Príklad 2.3. Uvedieme príklad konečnej nekomutatívnej grupy. Za tým účelom definujme najprv permutáciu množiny troch prvkov $A_3 = \{1, 2, 3\}$ ako bijekciu $\pi : A_3 \to A_3$. Bijekciu π zapisujeme takto:

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ k_1 & k_2 & k_3 \end{pmatrix},$$

kde pod každým prvkom v prvom riadku je jeho obraz v zobrazení π, t.j. $\pi(1) = k_1$, $\pi(2) = k_2$, $\pi(3) = k_3$. Keďže zobrazenie π je bijektívne, v druhom riadku permutácie sa vždy nachádzajú všetky tri prvky množiny A_3. Rôznych permutácií je teda toľko, koľko je rôznych poradí troch prvkov v druhom riadku. A tých je, ako čitateľ vie, $3! = 6$. Všetky permutácie troch prvkov sú teda tieto:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Ich množinu označíme $S_3 = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}$. V množine S_3 definujeme operáciu skladania zobrazení (t.j. skladania permutácií) $\circ$. Zrejme ide o asociatívnu operáciu, lebo skladanie zobrazení je asociatívna operácia (pozri príklad 1.20). Vypočítame napríklad $\pi_4 \circ \pi_5$. Máme: $\pi_4 \circ \pi_5(1) = \pi_4(3) = 2$, $\pi_4 \circ \pi_5(2) = \pi_4(2) = 3$, $\pi_4 \circ \pi_5(3) = \pi_4(1) = 1$, Vidíme, že $\pi_4 \circ \pi_5 = \pi_2$. Čitateľ podobne vypočíta $\pi_5 \circ \pi_4 = \pi_3$. Teda operácia nie je komutatívna. Ak použijeme vyššie uvedný zápis permutácií, výpočet zapíšeme takto:

$$\pi_4 \circ \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \pi_2,$$

$$\pi_5 \circ \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \pi_3.$$

Podobne vypočítame aj ostatné súčiny. Dostaneme nasledovnú Cayleyho tabuľku:

$\circ$	π_1	π_2	π_3	π_4	π_5	π_6
π_1	π_1	π_2	π_3	π_4	π_5	π_6
π_2	π_2	π_3	π_1	π_6	π_4	π_5
π_3	π_3	π_1	π_2	π_5	π_6	π_4
π_4	π_4	π_5	π_6	π_1	π_2	π_3
π_5	π_5	π_6	π_4	π_3	π_1	π_2
π_6	π_6	π_4	π_5	π_2	π_3	π_1

Ak tabuľku preskúmame, (vediac, že ide o asociatívnu operáciu) zistíme, že štruktúra $(S_3, \circ)$ je nekomutatívna grupa. Neutrálnym prvkom je π_1, prvky π_2, π_3 sú inverzné jeden druhému a ostatné sú sami sebe inverzné. Grupu S_3 nazývame *symetrická grupa stupňa tri*. Jej rád je $r(S_3) = 6$. Ako uvidíme neskoršie je to najmenšia nekomutatívna grupa. Dve dôležité vlastnosti grupy sú uvedené v nasledujúcich dvoch vetách:

Veta 2.1. *Nech* $(G, *)$ *je grupa. Nech* $a, b, c \in G$ *sú ľubovoľné prvky grupy. Potom platia nasledovné dve pravidlá:*

$$\text{(PK)} \qquad a * c = b * c \quad \textit{implikuje} \quad a = b,$$

$$\text{(ĽK)} \qquad c * a = c * b \quad \textit{implikuje} \quad a = b.$$

Inými slovami: *V grupe možno krátiť (sprava i zľava) ľubovoľným prvkom.*

Poznámka 2.1. Výrok (PK) je pravidlo o krátení sprava, výrok (ĽK) je pravidlo o krátení zľava.

Dôkaz vety 2.1. Dokážeme pravidlo o krátení sprava. Nech a, b, c sú ľubovoľné prvky grupy G, pre ktoré platí $a * c = b * c$. Po vynásobení tejto rovnosti sprava prvkom $c^{-1} \in G$, ktorý existuje podľa vlastnosti (iv) definície 2.1 a pre ktorý platí $c * c^{-1} = e$ dostaneme: $(a * c) * c^{-1} = (b * c) * c^{-1}$, odkiaľ po uplatnení asociatívneho zákona, ako aj vlastnosti inverzného a neutrálneho prvku máme $a = b$, čím je dokázané pravidlo o krátení sprava. Pravidlo o krátení zľava sa dokáže podobne. □

Poznámka 2.2. Ak je grupa zapísaná aditívne, miesto slova „krátiť“ používame slovo „rušiť“. Teda v grupe $(G, +)$ pravidlo „o rušení“ je: *Ak* $a, b, c \in G$ *sú ľubovoľné prvky grupy* $(G, +)$, *tak z rovnosti* $a + c = b + c$ *vyplýva* $a = b$. Keďže znak $+$ sa používa len pre komutatívne operácie, nemusíme hovoriť o „rušení sprava“ a „rušení zľava“.

Veta 2.2. *Nech* $(G, *)$ *je grupa,* $a, b \in G$. *Potom existujú jednoznačne dané prvky grupy* $x_0, y_0 \in G$ *také, že* x_0 *vyhovuje prvej,* y_0 *druhej z nasledujúcich rovníc*

$$a * x = b \tag{2.1}$$

$$y * a = b \tag{2.2}$$

Inými slovami:V každej grupe má každá z rovníc (2.1) a (2.2) *jednoznačne určené riešenie.*

Dôkaz. A. Dôkaz existencie riešenia. Dokážeme existenciu x_0. Na to stačí zvoliť $x_0 = a^{-1} * b$, kde $a^{-1} \in G$ je inverzný prvok k prvku a.

Skutočne, ak dosadíme x_0 do ľavej strany rovnice (2.1), máme: $a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$. Podobne sa dokáže, že $y_0 = b * a^{-1}$.

B. Dokážeme jednoznačnosť hoci x_0. Použijeme nepriamy dôkaz. Predpokladajme, že rovnici (2.1) vyhovuje okrem x_0 ešte aj $x_1 \in G$, kde $x_1 \neq x_0$. Potom

$$a * x_0 = b,$$
$$a * x_1 = b.$$

Porovnaním máme $a * x_0 = a * x_1$, odkiaľ, uplatniac pravidlo o krátení zľava, dostaneme $x_0 = x_1$, čo je spor s predpokladom $x_1 \neq x_0$. □

Veta 2.3. *Nech $(G, \cdot)$ je grupa a $a, b \in G$ sú ľubovoľné prvky grupy. Potom*

$$(a^{-1})^{-1} = a, \tag{2.3}$$

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}. \tag{2.4}$$

Dôkaz. Keďže dôkaz je triviálny, ponecháva sa čitateľovi. □

Poznámka 2.3. Keďže každá grupa je pologrupou, dajú sa v nej definovať mocniny, kde exponent je nezáporné celé číslo tak, ako v definícii 1.9. V grupe však možno definovať mocninu aj so záporným celočíselným mocniteľom takto: *Nech k je záporné celé číslo a prvok a je ľubovoľný prvok grupy G. Potom definujeme* $a^k = (a^{-1})^{-k}$.

Poznamenajme ďalej, že analogicky ako podgrupoid možno definovať podgrupu:

Definícia 2.2. Nech H je neprázdna podmnožina množiny G. Nech $(G, *)$ je grupa. Ak $(H, *)$ je tiež grupa, tak ju nazývame *podgrupou* grupy $(G, *)$. Fakt, že H je podgrupou grupy G, označujeme $H \subseteq\subseteq G$.

Príklad 2.4. Všimnime si štruktúry príkladu 2.1. Ľahko sa presvedčíme, že grupa $(Z, +)$ je podgrupou grupy $(Q, +)$, tá je podgrupou grupy $(R, +)$ a tá zase podgrupou grupy $(C, +)$.

Príklad 2.5 Uvažujme množinu ${}^3Z = \{3k; k \in Z\}$. Vidíme, že do ${}^3Z$ patria tie celé čísla, ktoré sú deliteľné troma. (Aj nula medzi ne patrí, lebo $0 = 3 \cdot 0$.) Ak na množine ${}^3Z$ uvažujeme obyčajné sčítanie celých čísel, vidíme, že $({}^3Z, +)$ je podgrupou grupy $(Z, +)$. Presvedčte sa o tom.

Príklad 2.6 Uvažujme o grupe $(K_4, \cdot)$ z príkladu 1.5. definovanej na množine $K_4 = \{1, -1, i, -i\}$. Zoberme podmnožinu $K_2 = \{1, -1\}$ množiny K_4. Vidieť, že štrukúra $(K_2, \cdot)$ je podgrupou grupy $(K_4, \cdot)$. (Pozri tabuľku v príklade 1.5.)

Poznámka 2.4. Na základe definície 2.2 môžeme povedať, že podgrupa je taká podmnožina danej grupy, ktorá je sama grupou vzhľadom na danú operáciu. Čitateľ sa ľahko presvedčí o tom, že každá grupa má dve *triviálne* (samozrejmé) podgrupy. Jednou z nich je podgrupa pozostávajúca len z neutrálneho prvku grupy G t.j. grupa $(\{e\}, \cdot)$ a druhá samotná grupa G. Okrem nich grupa môže mať aj iné podgrupy. Voláme ich *netriviálne* alebo *vlastné* podgrupy.

Teraz dokážeme niekoľko viet o podgrupách. Aby sme si uľahčili vyjadrovanie a zjednodušili označovanie, budeme používať multiplikatívny zápis grupovej operácie.

Veta 2.4. *Nech $(G, \cdot)$ je grupa a H neprázdna podmnožina grupy G. Potom $(H, \cdot)$ je podgrupou grupy G práve vtedy, keď sú splnené nasledovné podmienky:*

$$\textit{Ak} \quad a, b \in H, \quad \textit{tak} \quad a \cdot b \in H, \tag{i}$$

$$\textit{Ak} \quad a \in H, \quad \textit{tak} \quad a^{-1} \in H, \tag{ii}$$

kde a^{-1} je inverzný prvok k prvku a v grupe G.

Dôkaz. I. Predpokladajme, že $H \subseteq\subseteq G$. Keďže $(H, \cdot)$ je grupoid, podmienka (i) je splnená. Hneď vidieť, že podgrupa $(H, \cdot)$ má ten istý neutrálny prvok e ako grupa G (prečo?). Vzhľadom na jednoznačnosť riešenia rovnice $a \cdot x = e$ v grupe G, aj inverzný prvok k prvku a v grupe H je ten istý ako v grupe G. Preto platí aj (ii).

II. Prepokladajme teda, že pre nejakú neprázdnu podmnožinu H grupy G platia podmienky (i) aj (ii). Musíme dokázať, že štruktúra $(H, \cdot)$ je grupa. Podľa podmienky (i) je grupoidom. Je aj pologrupou, lebo ak by v grupoide H existovali tri prvky, pre ktoré by asociatívny zákon neplatil, neplatil by pre ne ani v grupe G, čo je nemožné. Nech $a \in H$ je ľubovoľný prvok množiny H. Potom podľa (ii) aj $a^{-1} \in H$. Odtiaľ podľa (i) máme $a \cdot a^{-1} = e \in H$, t.j. H obsahuje neutrálny prvok. Keďže podmienka (ii) je vlastne podmienkou (iv) z definície 2.1, sme s dôkazom hotoví. $\square$

Pri dôkaze, že nejaká podmnožina grupy je podgrupou, musíme podľa predchádzajúcej vety preveriť dve podmienky. Podľa nasledujúcej vety stačí preveriť len jednu (pravdaže inú) podmienku.

Veta 2.5. *Nech $(G, \cdot)$ je grupa a H neprázdna podmnožina grupy G. Potom $(H, \cdot)$ je podgrupou grupy G práve vtedy, keď je splnená nasledovná podmienka:*

(iii) $$\text{Ak} \quad a, b \in H, \quad \text{tak} \quad a \cdot b^{-1} \in H.$$

Dôkaz. I. Nech $H \subseteq\subseteq G$. Je jednoduché zistiť (pozri prvú časť dôkazu predchádzajúcej vety), že podmienka (iii) je splnená.

II. Predpokladajme teda, že pre nejakú neprázdnu podmnožinu H grupy G platí podmienka (iii). Nech $a \in H$ je ľubovoľný prvok množiny H. Potom podľa (iii) $a \cdot a^{-1} = e \in H$, t.j. H obsahuje neutrálny prvok. Keďže $e, a \in H$, podľa (iii) máme $e \cdot a^{-1} = a^{-1} \in H$, čiže je splnená podmienka (ii) vety 2.4. Nech $a, b \in H$ sú ľubovoľné prvky množiny H. Potom podľa vyššie uvedeného je aj $b^{-1} \in H$. Preto podľa (iii) $a \cdot (b^{-1})^{-1} = a \cdot b \in H$, t.j. je splnená aj prvá podmienka (i) vety 2.4. Preto $H \subseteq\subseteq G$. $\square$

Veta 2.6. *Nech $(G, \cdot)$ je grupa. Nech H_1 a H_2 sú jej podgrupy. Potom aj $H_1 \cap H_2$ je podgrupa grupy G.*

Inými slovami: Prienik dvoch podgrúp je podgrupa.

Dôkaz. Podľa vety 2.5 nám stačí dokázať, že pre všetky $a, b \in H_1 \cap H_2$ $a \cdot b^{-1} \in H_1 \cap H_2$. Nech teda $a, b \in H_1 \cap H_2$. Potom $a, b \in H_1$ a zároveň $a, b \in H_2$. Keďže H_1 i H_2 sú podgrupy platí $a \cdot b^{-1} \in H_1$ a zároveň $a \cdot b^{-1} \in H_2$. Preto $a \cdot b^{-1} \in H_1 \cap H_2$. $\square$

Poznámka 2.5. Vetu 2.6 možno zovšeobecniť takto: *Nech $\mathcal{S}$ je neprázdny systém podgrúp grupy G. Potom $\bigcap_{H \in \mathcal{S}} H$ je tiež podgrupa grupy G* (cvičenie 2.17).

Podľa vety 2.6 a poznámky za ňou môžeme vysloviť nasledujúcu definíciu.

Definícia 2.3. Nech je daná podmnožina M grupy G. Nech $\mathcal{S}$ je systém všetkých tých podgrúp grupy G, z ktorých každá obsahuje množinu M. (Zrejme $\mathcal{S} \neq \emptyset$, lebo $G \in \mathcal{S}$.) Teda

$$\mathcal{S} = \{H;\ H \subseteq\subseteq G \quad \text{a zároveň} \quad H \supseteq M\}.$$

Podgrupu, ktorá je prienikom všetkých podgrúp systému $\mathcal{S}$ označíme $[M]$ a nazveme ju podgrupou *generovanou (vytvorenou)* množinou M.

Prvky množiny M sa nazývajú *generátory* podgrupy $[M]$.

Veta 2.7. *Podgrupa $[M]$ grupy G generovaná množinou M má tieto dve vlastnosti:*

(i) $[M] \supseteq M$,

(ii) *Ak* $H \subseteq\subseteq G$ *taká, že* $H \supseteq M$, *tak* $H \supseteq [M]$.

Podgrupa $[M]$ je vlastnosťami (i) a (ii) jednoznačne určená.

Dôkaz. Dôkaz oboch vlastností vykonáme triviálnou aplikáciou definície 2.3. Aby sme dokázali druhú časť vety, predpokladajme, že existujú dve podgrupy $[M]_1 \neq [M]_2$ majúce vlastnosti (i) a (ii). Potom z (ii) vyplýva ako $[M]_1 \supseteq [M]_2$, tak aj $[M]_1 \subseteq [M]_2$, čiže $[M]_1 = [M]_2$. Daný spor ukončuje dôkaz. □

Poznámka 2.6. Veta 2.7 nám hovorí, že $[M]$ je v istom zmysle najmenšia podgrupa grupy G obsahujúca množinu M. Keďže každá podgrupa obsahuje neutrálny prvok danej grupy, podľa vlastnosti (ii) vety 2.7 obsahuje aj triviálnu podgrupu $\{e\}$. Na druhej strane prázdna množina $\emptyset$ je podmnožinou každej množiny, teda aj každej podgrupy H. Preto podgrupa $[\emptyset]$ generovaná prázdnou množinou je prienikom všetkých podgrúp danej grupy. To znamená $[\emptyset] = \{e\}$. Nasledujúca veta je o tom, z čoho pozostáva podgrupa generovaná neprázdnou množinou.

Veta 2.8. *Nech $(G, \cdot)$ je grupa a $M \subseteq G$ jej neprázdna podmnožina. Potom*

$$[M] = \{a_1^{e_1} \cdot a_2^{e_2} \cdot \ldots \cdot a_k^{e_k};\ k \in N,\ a_i \in M,\ e_i \in \{1, -1\}\}. \tag{2.5}$$

Inými slovami: Podgrupa generovaná neprázdnou množinou pozostáva zo všetkých možných konečných súčinov prvkov množiny M a prvkov k nim inverzných.

Dôkaz. Pre lepšie vyjadrovanie množinu na pravej strane rovnosti (2.5) označíme $X = \{a_1^{e_1} \cdot a_2^{e_2} \cdot \ldots \cdot a_k^{e_k};\ k \in N,\ a_i \in M,\ e_i \in \{1, -1\}\}$. Dokážeme najskôr, že X je podgrupa grupy G. Naozaj, ak $x, y \in X$ sú dva ľubovoľné prvky množiny X, napríklad $x = a_1^{e_1} \cdot a_2^{e_2} \cdot \ldots \cdot a_k^{e_k}$, $y = b_1^{f_1} \cdot b_2^{f_2} \cdot \ldots \cdot b_h^{f_h}$, tak prvok $x \cdot y^{-1} = a_1^{e_1} \cdot a_2^{e_2} \cdot \ldots \cdot a_k^{e_k} \cdot b_h^{-f_h} \cdot \ldots \cdot b_2^{-f_2} \cdot b_1^{-f_1}$ je tiež prvkom množiny X. (Pozri vetu 2.3 a cvičenie 2.4.) Nech a je ľubovoľný prvok množiny M. Stačí položiť $k = 1$, $a_1 = a$, $e_1 = 1$, aby sme videli, že $a \in X$. Preto $M \subseteq X$, čiže množina X má vlastnosť (i) vety 2.7. Na druhej strane, každá podgrupa obsahujúca množinu M obsahuje aj všetky možné konečné súčiny prvkov množiny M a prvkov k nim inverzných. Preto X má aj vlastnosť (ii) vety 2.7. Môžeme uzavrieť $X = [M]$. □

Príklad 2.7. Uvažujme o podgrupe grupy $(Z, +)$ generovanej množinou $M = \{3, 5\}$. Podľa vety 2.8 podgrupa $[M]$ pozostáva zo všetkých konečných súčtov prvkov množiny M a prvkov k nim opačných. Keďže $1 = 3 + 3 - 5$ a tiež $-1 = 5 - 3 - 3$, je vidieť, že uvedenými súčtami možno „nagenerovať“ ľubovoľné celé číslo. Preto $[M] = Z$, t.j. množina M generuje celú grupu $(Z, +)$.

Príklad 2.8. Zistíme, akú podgrupu grupy $(S_3, \circ)$ generuje jednoprvková podmnožina $M = \{\pi_2\}$ množiny $S_3 = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}$. Podľa Cayleyho tabuľky z príkladu 2.3. máme: $\pi_2^2 = \pi_3$, $\pi_2^3 = \pi_1$, $\pi_2^4 = \pi_2, \cdots$. Vidíme, že $[M] = H$, kde $H = \{\pi_1, \pi_2, \pi_3\}$. Podgrupa $(H, \circ)$ je v ľavom hornom rohu tabuľky. Poznamenajme ešte, že rád podgrupy generovanej jediným prvkom nazývame rádom daného prvku. Keďže rád podgrupy H je $r(H) = 3$, píšeme tiež $r(\pi_2) = 3$.

Cvičenia

2.1. Zistite, či niektorý z nasledujúcich grupoidov je grupa.

·	a	b	c
a	b	a	c
b	b	c	a
c	c	a	b

·	a	b	c
a	a	b	c
b	b	a	c
c	c	c	a

·	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

2.2. Dokážte, že v Cayleyho tabuľke sa v každom riadku (stĺpci) nachádza každý prvok grupy práve raz.

2.3. Nech a, b, c sú pevne zvolené prvky grupy $(G, \cdot)$. Dokážte, že rovnica $xaxba = xbc$ má práve jedno riešenie.

2.4. Dokážte vetu 2.3 a toto zovšeobecnenie jej tvrdenia (2.4): *Nech* $a_1, a_2, \dots, a_n$ sú ľubovoľné prvky grupy G. Potom

(2.4') $$(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}.$$

2.5.. Je daná množina $A = \{a, b, c, d\}$ a na nej operácie $*, \circledast$ definované Cayleyho tabuľkami. Dokážte, že štruktúry $(A, *)$ a $(A, \circledast)$ sú komutatívne grupy.

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$\circledast$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

2.6. V grupách z príkladov 2.1, 2.2 a 2.3 a z predchádzajúceho cvičenia 2.5 určte niektoré podmnožiny, ktoré sú podgrupami daných grúp. Skúste nájsť všetky podgrupy grupy $(A, \circledast)$ z predchádzajúceho cvičenia.

2.7. Je daná množina $M = \{x, y\}$. Určte operáciu $*$ tak, aby $(M, *)$ bola grupa. Úlohu opakujte pre množinu $M_1 = \{x, y, z\}$.

2.8. Daná je množina $G = R - \{0\}$ a množina

$$M = \{x \in R;\, x = a + b\sqrt{2}, [a, b] \in Q \times Q, (a \neq 0 \vee b \neq 0)\}.$$

Zistite, či štruktúra $(M, \cdot)$ je podgrupou štruktúry $(G, \cdot)$, kde „·" je obyčajné násobenie reálnych čísel.

2.9. Nech $p, q, r \in R$ sú ľubovoľné, ale pevne zvolené reálne čísla. Na množine všetkých reálnych čísel definujte operáciu „$\star$" takto: Ak $a, b \in R$, tak $a \star b = pa + qb + r$. Ako treba voliť čísla p, q, r, aby $(R, \star)$ bola

a) pologrupou? b) komutatívnou pologrupou? c) monoidom?
d) komutatívnym monoidom? e) grupou?

2.10. Dokážte, že komplexné jednotky (komplexné čísla tvaru $\cos\alpha + i\sin\alpha$) tvoria grupu vzhľadom na násobenie komplexných čísel.

2.11. Nech $(G_1, \cdot)$ a $(G_2, \odot)$ sú grupy. Dokážte, že štruktúra $(G_1 \times G_2, \otimes)$ je grupa, ak operácia $\otimes$ je definovaná takto: $[a_1, a_2] \otimes [b_1, b_2] = [a_1 \cdot b_1,\ a_2 \odot b_2]$.

2.12. Nech $a \in G$ je ľubovoľný pevne zvolený prvok grupy G. Dokážte, že podmnožina $\{a^n; n \in Z\}$ je podgrupou grupy G.

2.13. Nájdite podgrupu aditívnej grupy celých čísel generovanú množinou $\{2,\ 3,\ 5\}$.

2.14. V každej abelovskej grupe tie prvky, ktoré sú sami sebe inverzné tvoria podgrupu. Dokážte to.

2.15. Nech $a \in G$ je ľubovoľný prvok grupy G. Ako sme poznamenali v príklade 2.8, rád pogrupy [{a}] generovanej prvkom a nazývame rádom prvku a. Dokážte, že ak všetky prvky danej grupy okrem neutrálneho majú rád dva, grupa je komutatívna.

2.16. Nech H je neprázdna podmnožina konečnej grupy G. Potom H je podgrupou grupy G práve vtedy, keď množina H je uzavretá vzhľadom na operáciu grupy G. Dokážte to.
(*Poznámka.* Vidíme, že pre konečný prípad nemusíme predpokladať, že množina H je uzavretá aj na inverzné prvky.)

2.17. Dokážte, že vetu 2.6 možno zovšeobecniť takto: *Nech $\mathcal{S}$ je neprázdny systém podgrúp grupy G. Potom* $\bigcap\limits_{H \in \mathcal{S}} H$ *je tiež podgrupa grupy G.*

§ 3. Okruhy, obory integrity, polia

Ak na neprázdnej množine definujeme dve binárne operácie majúce určité vlastnosti a určíme vzťah medzi týmito operáciami (napríklad tak, ako sme to urobili v definícii 1.6), dostaneme algebraickú štruktúru s dvoma operáciami. Z viacerých takýchto štruktúr známych z algebry uvedieme v tomto paragrafe *okruh* a jeho špeciálne prípady: *obor integrity, teleso* a *pole.*

Definícia 3.1. Nech A je neprázdna množina, na ktorej sú definované dve operácie „+“ a „·“. Potom štruktúra $(A, +, \cdot)$ je *okruh*, ak sú splnené nasledujúce podmienky:

(i) $(A, +)$ je komutatívna grupa,
(ii) $(A, \cdot)$ je pologrupa,
(iii) Operácia „·“ je distributívna vzhľadom na operáciu „+“, t.j. platí (ĽDZ) a (PDZ) z definície 1.6.

Ak $(A, \cdot)$ je komutatívna pologrupa, okruh $(A, +, \cdot)$ nazývame *komutatívnym okruhom.*

Ak $(A, \cdot)$ je pologrupa s neutrálnym prvkom, okruh $(A, +, \cdot)$ nazývame *okruhom s jednotkovým prvkom.*

Grupu $(A, +)$ nazývame *aditívna grupa okruhu.* Neutrálny prvok grupy $(A, +)$ voláme *nulový prvok okruhu.* Označujeme ho 0.

Pologrupu $(A, \cdot)$ nazývame *multiplikatívna pologrupa okruhu.* Neutrálny prvok pologrupy $(A, \cdot)$ (ak existuje) nazývame *jednotkovým prvkom okruhu.* Označujeme ho 1.

Okruh, ktorý obsahuje len nulový prvok, t.j. okruh $(\{0\}, +, \cdot)$ nazývame *triviálnym okruhom.* Okruh, ktorý obsahuje aspoň dva prvky je *netriviálny.*

Príklad 3.1. Prosíme čitateľa, aby sa presvedčil o tom, že štruktúry $(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$ sú okruhy. Všetky tieto tzv. *číselné okruhy* sú komutatívne.

Príklad 3.2. Uvedieme príklad nekomutatívneho okruhu. Všetko potrebné máme už pripravené. Vezmeme množinu $\mathcal{M}$ všetkých štvorcových matíc 2. stupňa s reálnymi prvkami definovanú v príklade 1.7 spolu s operáciou „+“ definovanou v príklade 1.10 a operáciou „·“ definovanou v príklade 1.7. Ľahko skontrolujeme, že $(\mathcal{M}, +)$ je abelovská grupa. To že $(\mathcal{M}, \cdot)$ je pologrupa, sme dokázali v príklade 1.7. Tam sme tiež ukázali, že operácia „·“ nie je komutatívna. V príklade 1.14 sme dokázali, že operácia „·“ je distributívna vzhľadom na operáciu „+“. Teda $(\mathcal{M}, +, \cdot)$ je nekomutatívny okruh. Ide o nekomutatívny okruh s jednotkovým prvkom (pozri príklad 1.12).

Príklad 3.3. Ak vezmeme množinu ^2Z všetkých párnych čísel a operácie sčítania a násobenia celých čísel, dostaneme okruh $(^2Z, +, \cdot)$ bez jednotkového prvku.

Veta 3.1. *Nech* 0 *je nulový prvok okruhu* $(A, +, \cdot)$. *Potom pre každý prvok* $a \in A$ *platí*

$$0 \cdot a = a \cdot 0 = 0.$$

Dôkaz. Zvolíme ľubovoľný prvok $a \in A$.
Platí

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0, \tag{3.1}$$

$$a \cdot 0 = a \cdot 0 + 0. \tag{3.2}$$

Ľavé strany rovností (3.1) a (3.2) sú rovnaké. Preto sa musia rovnať aj pravé strany: $a \cdot 0 + a \cdot 0 = a \cdot 0 + 0$. Podľa pravidla „o rušení“, ktoré platí v grupe $(A, +)$ (pozri vetu 2.1 a poznámku 2.2), platí $a \cdot 0 = 0$. Podobne sa dokáže, že $0 \cdot a = 0$ (urobte to!). □

Veta 3.2. *Nech* a, b *sú ľubovoľné prvky okruhu* A. *Potom platí*

$$(-a) \cdot b = a \cdot (-b) = -(ab), \tag{3.3}$$

$$(-a) \cdot (-b) = ab. \tag{3.4}$$

Dôkaz. Dokážeme (3.3). Je jasné, že prvok $-(ab)$ je opačný prvok k prvku ab. Dokážeme, že aj $(-a) \cdot b$ je opačný prvok k prvku ab. Skutočne: $a \cdot b + (-a) \cdot b =$

$= (a + (-a)) \cdot b = 0 \cdot b = 0$, kde sme použili najprv distributívny zákon a potom vetu 3.1. Podobne sa dokáže aj $(-a)\cdot b + a\cdot b = 0$. Keďže „+" je asociatívna operácia, podľa vety 1.2 opačný prvok je len jeden. Preto $(-a)\cdot b = -(ab)$. Podobne sa dokáže $a \cdot (-b) = -(ab)$.

Dokážeme (3.4). Počítame: $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = ab$. Dvakrát sme použili vzťah (3.3), potom fakt, že opačný prvok prvku opačného k danému prvku je daný prvok. □

Poznámka 3.1. Vzťahy (3.3), (3.4) z vety 3.2 sú tzv. znamienkové pravidlá: *„mínus krát plus je mínus"* a *„mínus krát mínus je plus."*

Veta 3.3. *Nech $(A, +, \cdot)$ je netriviálny okruh s jednotkovým prvkom. Potom* $0 \neq 1$.

Dôkaz. Ak by $0 = 1$, tak pre nejaké $a \neq 0$ by platilo $0 \cdot a = 1 \cdot a = a$ a zároveň $0 \cdot a = 0$. Odtiaľ máme $a = 0$, čo je spor s predpokladom. □

Podľa poznámky 1.9 možno v aditívnej grupe okruhu $(A, +, \cdot)$ definovať tzv. celočíselné násobky prvkov okruhu, t.j. ak $a \in A$ a $k \in Z$ je kladné celé číslo, tak $k \times a = \underbrace{a + a + \cdots + a}_{\text{k razy}}$ a tiež $-k \times a = \underbrace{(-a) + (-a) + \cdots + (-a)}_{\text{k razy}}$. V okruhoch, kde nemôže prísť k omylu (napríklad v číselných okruhoch alebo v okruhu matíc v príklade 3.2) zápis zjednodušujeme a miesto $k \times a$ píšeme len ka. Tiež máme $0 \times a = 0$, kde na ľavej strane rovnosti znakom 0 sme označili celé číslo nula, zatiaľ čo na pravej strane znak 0 je nulový prvok okruhu.

Veta 3.4. *Nech $(A, +, \cdot)$ je okruh. Potom pre každé $a, b \in A$ a pre každé $h, k \in Z$ platí*

$$(h + k) \times a = h \times a + k \times a$$
$$k \times (a \cdot b) = (k \times a) \cdot b = a \cdot (k \times b)$$

Dôkaz. Je triviálny. □

Príklad 3.4. Dokážeme tvrdenie: *Okruh $(A, +, \cdot)$ je komutatívny vtedy a len vtedy, keď v ňom pre ľubovoľné prvky $a, b \in A$ platí*

$$(a + b)^2 = a^2 + 2ab + b^2, \tag{3.5}$$

kde miesto zápisu $2 \times (ab)$ sme písali len $2ab$.

Dôkaz tvrdenia. I. Nech $(A, +, \cdot)$ je komutatívny okruh. Potom $(a + b)^2 = (a + b) \cdot (a + b) = (a + b) \cdot a + (a + b) \cdot b = a^2 + ba + ab + b^2 = a^2 + ab + ab + b^2 = a^2 + 2ab + b^2$. Použili sme dva razy distributívny zákon a potom okolnosť, že $(A, +, \cdot)$ je komutatívny okruh.

II. Nech $(A, +, \cdot)$ je okruh, v ktorom platí (3.5). Nech a, b sú ľubovoľné prvky okruhu. Počítajme $(a+b)^2 = (a+b)\cdot(a+b) = (a+b)\cdot a+(a+b)\cdot b = a^2+ba+ab+b^2$. Keďže (3.5) platí, máme:

$$a^2 + 2ab + b^2 = a^2 + ba + ab + b^2,$$

alebo

$$a^2 + ab + ab + b^2 = a^2 + ba + ab + b^2.$$

Po „vyrušení“ rovnakých členov dostaneme $ab = ba$, t.j. okruh $(A, +, \cdot)$ je komutatívny. $\square$

Definícia 3.2. Nech B je neprázdna podmnožina okruhu $(A, +, \cdot)$. Ak štruktúra $(B, +, \cdot)$ je tiež okruh, tak ho nazývame *podokruhom* okruhu A. Fakt, že okruh B je podokruhom okruhu A zapisujeme $B \subseteq\subseteq A$.

Príklad 3.5. Každý netriviálny okruh $(A, +, \cdot)$ má dva *triviálne podokruhy*: okruh $(\{0\}, +, \cdot)$ a okruh $(A, +, \cdot)$. Pravda okruh môže mať aj netriviálne podokruhy. Napríklad okruhy $(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$, sú *netriviálne* (nazývame ich aj *vlastné*) podokruhy okruhu $(C, +, \cdot)$.

Veta 3.5. *Neprázdna podmnožina B okruhu $(A, +, \cdot)$ je podokruhom okruhu A práve vtedy, keď platia tieto podmienky:*

(i) *Pre každé* $a, b \in B$ *platí:* $a - b \in B$,

(ii) *Pre každé* $a, b \in B$ *platí:* $a \cdot b \in B$.

Dôkaz. I. Ak B je podokruhom okruhu A, tak podmienky (i) a (ii) zrejme platia.

II. Nech pre neprázdnu podmnožinu B okruhu A platia podmienky (i) a (ii). Prvá podmienka je vlastne podmienkou vety 2.5 o podgrupe. Preto grupa $(B, +)$ je podgrupou grupy $(A, +)$. Podmienka (ii) implikuje, že $(B, \cdot)$ je podpologrupou pologrupy $(A, \cdot)$ (odôvodnite to!). Podobne ľahké je dokázať, že aj v $(B, +, \cdot)$ platí ľavý i pravý distributívny zákon. $\square$

Veta 3.6. *Nech $\mathcal{S}$ je systém (nie nutne všetkých) podokruhov okruhu $(A, +, \cdot)$. Potom aj $\bigcap_{B \in \mathcal{S}} B$ je podokruhom okruhu A.*

Dôkaz, ktorý je podobný dôkazu vety 2.6 (pozri aj poznámku 2.5) sa vykoná aplikáciou vety 3.5 a ponecháva sa na čitateľa. $\square$

Definícia 3.3. Nech je daná podmnožina M okruhu A. Nech $\mathcal{S}$ je systém všetkých tých podokruhov okruhu A, z ktorých každý obsahuje množinu M. (Zrejme $\mathcal{S} \neq \emptyset$, lebo $A \in \mathcal{S}$.) Teda

$$\mathcal{S} = \{B;\ B \subseteq\subseteq A \text{ a zároveň } B \supseteq M\}$$

Podokruh, ktorý je prienikom všetkých podokruhov systému $\mathcal{S}$ označíme $[[M]]$ a nazveme ho *podokruhom generovaným (vytvoreným)* množinou M.

Prvky množiny M sa nazývajú generátory podokruhu $[[M]]$.

Veta 3.7. *Podokruh $[[M]]$ generovaný množinou M má tieto dve vlastnosti:*

(i) $[[M]] \supseteq M$,

(ii) *Ak* $B \subseteq\subseteq A$ *taký, že* $B \supseteq M$, *tak* $B \supseteq [[M]]$.

Podokruh $[[M]]$ je vlastnosťami (i) a (ii) jednoznačne určený.

Dôkaz je analogický dôkazu vety 2.7 a tak si ho čitateľ vykoná sám. $\square$

Poznámka 3.2. Poznamenajme podobne ako v poznámke 2.6, že $[[M]]$ je v istom zmysle najmenší podokruh obsahujúci množinu M. Keďže každý podokruh obsahuje aj triviálny podokruh $\{0\}$ a prázdna množina $\emptyset$ je podmnožinou každého podokruhu, podokruh $[[\emptyset]] = \{0\}$. Nasledujúca veta hovorí o tom, z čoho pozostáva podokruh generovaný neprázdnou množinou.

Veta 3.8. *Nech $(A, +, \cdot)$ je okruh a $M \subseteq A$ jeho neprázdna podmnožina. Potom podokruh generovaný neprázdnou množinou M pozostáva zo všetkých možných konečných súčtov všetkých možných konečných súčinov prvkov množiny M a prvkov k nim opačných.*

Dôkaz. Ak množinu týchto súčtov označíme B, tak aplikáciou vety 3.5 ľahko zistíme, že B je podokruh okruhu A. Zrejme $B \supseteq M$, lebo B obsahuje „jednočlenné“ súčty, z ktorých každý je len „jednočlenný“ súčin rovný nejakému prvku množiny M (premyslite to!). Na druhej strane, každý podokruh obsahujúci množinu M obsahuje aj všetky možné konečné súčty všetkých možných konečných súčinov prvkov množiny M a prvkov k nim opačných. Preto B spĺňa obe podmienky vety 3.7. Môžeme uzavrieť $B = [[M]]$. $\square$

Dôsledok. *Nech $(A, +, \cdot)$ je komutatívny okruh s jednotkovým prvkom 1. Nech $(B, +, \cdot)$ je jeho vlastný podokruh tiež obsahujúci jednotkový prvok 1. Ďalej nech $u \in A$ je taký prvok, že $u \notin B$. Potom*

$$[[B \cup \{u\}]] = \{a_0 + a_1 u + \cdots + a_n u^n;\ a_i \in B,\ n \in N\}.$$

Dôkaz. Stačí si uvedomiť, že každý prvok podokruhu $[[B \cup \{u\}]]$ je súčtom prvkov tvaru $\pm b_1 b_2 \ldots b_r$, kde $b_i \in B \cup \{u\}$. Ak s týchto prvkov je z podokruhu B, máme $\pm b_1 b_2 \ldots b_s \cdot u^{r-s}$. Vidieť, že každý člen súčtu má tvar $a \cdot u^k$, kde $a \in B$ a $k \in N$. $\square$

Poznámka 3.3. Práve dokázaný dôsledok využijeme neskoršie pri algebraickej definícii polynómov.

Príklad 3.6. Uvažujme o podokruhu okruhu $(Z, +, \cdot)$ generovanom množinou $M = \{3, 5\}$. Podobne ako v príklade 2.7 pomocou vety 2.7, teraz pomocou vety 3.8 ľahko zistíme, že podokruh $[[M]] = Z$.

Príklad 3.7. Uvažujme o okruhu matíc 2. stupňa s reálnymi prvkami $(\mathcal{M}, +, \cdot)$ z príkladu 3.2. Tento okruh má tú zvláštnosť, že v ňom existujú nenulové prvky, ktorých súčin je nulový prvok. Napríklad nasledujúci súčin nenulových matíc „dáva“ nulovú maticu.

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

Definícia 3.4. Nech $(A, +, \cdot)$ je okruh. Prvok $a \in A$ nazývame *ľavým (pravým) deliteľom nuly*, ak k nemu existuje taký prvok $b \in A$, že $b \neq 0$ a platí $a \cdot b = 0$ $(b \cdot a = 0)$. Ak prvok $a \in A$ je pravým alebo ľavým deliteľom nuly, nazývame ho *deliteľ nuly*.

Príklad 3.8. Ak $b \neq 0$ je ľubovoľný nenulový prvok okruhu A, tak podľa vety 3.1 platí $0 \cdot b = b \cdot 0 = 0$. Vidíme, že nulový prvok okruhu je deliteľom nuly.

Nazývame ho *triviálnym deliteľom nuly.* Triviálny deliteľ nuly teda obsahuje každý okruh. Z príkladu 3.7 vidieť, že existujú okruhy obsahujúce *netriviálne delitele nuly*, t.j. také delitele nuly, ktoré sú nenulovými prvkami okruhu.

Definícia 3.5. Okruh $(A, +, \cdot)$, ktorý neobsahuje netriviálne delitele nuly nazývame *obor integrity.* Teda v obore integrity platí:

(3.6) Ak $a, b \neq 0$ sú (nenulové) prvky oboru integrity, tak $a \cdot b \neq 0$.

Inými slovami: Okruh A je obor integrity, ak jeho nenulové prvky tvoria podpologrupu jeho multiplikatívnej pologrupy.

Poznámka 3.4. V niektorej literatúre sa požaduje, aby obor integrity (okrem toho, že nemá netriviálne delitele nuly) bol komutatívny okruh s jednotkovým prvkom.

Veta 3.9. *Netriviálny okruh $(A, +, \cdot)$ je oborom integrity práve vtedy, keď pre všetky $a, b, c \in A$, také, že $c \neq 0$ platí:*

(ĽKNP) *Rovnosť* $ca = cb$ *implikuje* $a = b$,

(PKNP) *rovnosť* $ac = bc$ *implikuje* $a = b$.

Inými slovami: *Okruh je oborom integrity práve vtedy, keď sa v ňom dá krátiť zľava i sprava nenulovým prvkom.*

Poznámka 3.5. Výroky (ĽKNP) a (PKNP) sú ľavé a pravé pravidlo o krátení nenulovým prvkom.

Dôkaz vety 3.9. I. Nech A je obor integrity. Dokážeme, že v ňom platí hoci ľavé pravidlo o krátení nenulovým prvkom. Nech teda $a, b, c \in A$ sú také prvky, že $c \neq 0$ a zároveň $ca = cb$. Odtiaľ máme $ca - cb = 0$ a odtiaľ $c(a - b) = 0$. Keďže $c \neq 0$ a okruh A neobsahuje netriviálne delitele nuly, musí byť $a - b = 0$, čiže $a = b$. Pravidlo (PKNP) sa dokáže podobne.

II. Nech v okruhu $(A, +, \cdot)$ platí ľavé i pravé pravidlo o krátení nenulovým prvkom. Dokážeme, že okruh je oborom integrity, t.j. neobsahuje netriviálne delitele nuly. Aby sme to dokázali, predpokladajme, že $a, x \in A$ sú také prvky, že $a \neq 0$ a zároveň $ax = 0$. Poslednú rovnosť možno napísať takto: $a \cdot x = a \cdot 0$, odkiaľ po krátení zľava nenulovým prvkom a dostaneme $x = 0$. To znamená, že A neobsahuje netriviálne delitele nuly, čiže je obor integrity. □

Definícia 3.6. Nech $(T, +, \cdot)$ je okruh s jednotkovým prvkom. Okruh $(T, +, \cdot)$ nazývame *telesom*, ak v jeho multiplikatívnej pologrupe $(T, \cdot)$ má každý nenulový prvok inverzný prvok.

Inými slovami: Okruh $(T, +, \cdot)$ je teleso, ak štruktúra $(T - \{0\}, \cdot)$ je grupa. Nazývame ju *multiplikatívna grupa telesa.*

Ak teleso $(F, +, \cdot)$ je komutatívny okruh, nazývame ho *pole.*

Príklad 3.9. Pomocou vedomostí zo strednej školy ľahko overíme, že okruhy $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$ sú komutatívne telesá, teda polia.

Príklad 3.10. Nech F je množina určená takto:

$$F = \{a + b\sqrt{2};\ a, b \in Q\}.$$

Na množine F definujeme obyčajné sčítanie „$+$" a násobenie „$\cdot$" reálnych čísel. Dokážeme, že štruktúra $(F, +, \cdot)$ je pole.

Čitateľ môže ľahko zistiť, že štruktúra $(F, +)$ je abelovská grupa.

Podobne ľahko zistíme, že $(F, \cdot)$ je komutatívna pologrupa s jednotkovým prvkom $1 + 0 \cdot \sqrt{2}$. Je to zrejmé, keďže násobenie reálnych čísel je asociatívne a súčin $(a + b\sqrt{2})(a_1 + b_1\sqrt{2}) = (aa_1 + 2bb_1) + (ab_1 + ba_1)\sqrt{2}$ je opäť z poľa F.

Zostáva zistiť, že ak $x = a + b\sqrt{2} \neq 0 + 0.\sqrt{2}$, tak existuje inverzný prvok k tomuto prvku. Presvedčíme sa o tom, že inverzný prvok je

$$x^{-1} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

Skutočne:

$$(a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}\right) =$$

$$= \frac{a^2}{a^2 - 2b^2} + \frac{-ab}{a^2 - 2b^2}\sqrt{2} + \frac{ab}{a^2 - 2b^2}\sqrt{2} - \frac{2b^2}{a^2 - 2b^2} = \frac{a^2 - 2b^2}{a^2 - 2b^2} = 1 + 0.\sqrt{2}.$$

Samozrejme, treba ešte dokázať, že ak $a + b\sqrt{2} \neq 0$, tak aj $a^2 - 2b^2 \neq 0$. Ponecháme to na čitateľa.

Keďže distributívny zákon (násobenie je distributívne vzhľadom na sčítanie) platí v celom obore reálnych čísel, platí zrejme aj v množine F.

Poznámka 3.6. Vnímavejší čitateľ iste postrehol, že na tomto mieste by bolo treba uviesť príklad telesa, čo nie je pole, t.j. má nekomutatívne násobenie. Takéto telesá skutočne existujú. S príkladom nekomutatívneho telesa sa stretneme v priebehu ďalšieho štúdia algebry.

Veta 3.10. *Každé teleso $(T, +, \cdot)$ je obor integrity.*

Dôkaz. Podľa vety 3.9 stačí dokázať, že v telese možno krátiť (zľava i sprava) nenulovým prvkom. Dokážeme napr. pravé krátenie (ľavé sa dokáže podobne). Nech $a, b, c \in T$ sú ľubovoľné prvky telesa T, také že $c \neq 0$ a zároveň $ac = bc$. Potom podľa definície 3.6 k prvku $c \neq 0$ existuje inverzný prvok c^{-1}. Ak ním vynásobíme rovnosť $ac = bc$ sprava, dostaneme $(ac) \cdot c^{-1} = (bc) \cdot c^{-1}$, odkiaľ po uplatnení asociatívneho zákona a vlastnosti jednotkového prvku okruhu máme $a = b$, čím je krátenie nenulovým prvkom sprava dokázané. □

Veta 3.11. *Okruh celých čísel $(Z, +, \cdot)$ je obor integrity.*

Dôkaz. Okruh celých čísel je podokruhom okruhu racionálnych čísel. Ale okruh racionálnych čísel je telesom, teda aj oborom integrity, čiže neobsahuje netriviálne delitele nuly. Nemôže ich teda obsahovať ani okruh celých čísel. □

Iný dôkaz tejto vety uvedieme neskoršie. Čitateľ ho môže nájsť napríklad v skripte [15, kap. VIII, veta 1.12].

Poznámka 3.7. Podľa viet 3.10 a 3.11 číselné polia $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$, ako aj okruh celých čísel $(Z, +, \cdot)$ sú obormi integrity. Keďže neobsahujú netriviálne delitele nuly, platí v nich tvrdenie známe zo strednej školy: *Ak súčin dvoch čísel sa rovná nule, tak jeden alebo druhý činiteľ sa rovná nule.* Čitateľ nech si uvedomí, že toto tvrdenie nemá „všeobecnú" platnosť. Neplatí v okruhoch, čo nie sú obormi integrity.

Definícia 3.7. Nech $(T,+,\cdot)$ je teleso. Ak S je taká podmnožina telesa T, že $(S,+,\cdot)$ je tiež teleso, tak S nazývame *podtelesom* telesa T. Označujeme: $S \subseteq\subseteq T$. V prípade komutatívneho telesa (poľa) používame názov *podpole*.

Príklad 3.11. Polia $(Q,+,\cdot)$, $(R,+,\cdot)$ sú podpoliami poľa $(C,+,\cdot)$.

Veta 3.12. *Neprázdna podmnožina S telesa $(T,+,\cdot)$ je podtelesom telesa T práve vtedy, keď platia tieto podmienky:*

(i) *Pre každé* $a,b \in S$ *platí:* $a-b \in S$,

(ii) *Pre každé* $a,b \in S$ *platí:* $a \cdot b \in S$,

(iii) *Pre každé* $a \in S$ *také, že* $a \neq 0$, *platí:* $a^{-1} \in S$.

Dôkaz ponecháme na čitateľa. □

Cvičenia

3.1. Zistite, či nasledujúce číselné množiny s operáciami obyčajného sčítania a násobenia sú okruhom, oborom integrity, alebo poľom.

a) $H = \{a + b\sqrt{3};\ a,b \in Z\}$,
b) $K = \{a + b\sqrt{3};\ a,b \in Q\}$,
c) $L = \{a + b\sqrt{2} + c\sqrt{3};\ a,b,c \in Q\}$,
d) $M = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6};\ a,b,c,d \in Q\}$.

3.2. Zistite, či množina $M = \{a,b,c,d\}$ s operáciami „+“ a „·“ definovanými nasledujúcimi Cayleyho tabuľkami

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	a	c
d	a	d	c	b

tvorí okruh. Je to obor integrity? Je to teleso?

3.3. Dokážte, že množina $M = \{a,b,c\}$ s operáciami $\square, \triangle$ je teleso (teda systém $(M,\square,\triangle)$ je teleso).

$\square$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\triangle$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

3.4. Zistite, či množina všetkých celých čísel je okruhom (oborom integrity) vzhľadom na operácie $\oplus, \odot$, ktoré sú dané vzťahmi

$$x \oplus y = x + y - 1, \qquad x \odot y = x + y - xy,$$

kde x, y sú ľubovoľné celé čísla.

3.5. Zistite, či štruktúra $(Z, \oplus, \odot)$, kde

$$a \oplus b = a + b + 2 \qquad a \odot b = ab + 2a + 2b + 2,$$

a a, b sú ľubovoľné celé čísla je okruhom. Je to obor integrity?

3.6. Dokážte, že ak v okruhu $(A, +, \cdot)$ pre každé $a \in A$ platí $a^2 = a$, tak A je komutatívny okruh.
(*Návod.* Najprv dokážte, že pre každé $a \in A$ platí $a + a = 0$.)

3.7. Dokážte, že $(Z, \oplus, \odot)$ je obor integrity, keď

$$a \oplus b = a + b + 1, \qquad a \odot b = a + b + ab,$$

kde a, b sú ľubovoľné celé čísla.

3.8. Nech $(A, +, \cdot)$, $(B, +, \cdot)$ sú okruhy. Nech v množine $(A \times B, +, \cdot)$ sú dané operácie „+" a „·" takto: Pre každé $(x, y), (u, v) \in A \times B$ platí

$$(x, y) + (u, v) = (x + u,\ y + v) \quad \text{a} \quad (x, y) \cdot (u, v) = (x \cdot u,\ y \cdot v).$$

Potom štruktúra $(A \times B, +, \cdot)$ je tiež okruhom. Dokážte to.
Poznámka Zrejme nevadí, že operácie vo všetkých troch okruhoch označujeme rovnako. Okruh $(A \times B, +, \cdot)$ nazývame direktným súčtom okruhov $(A, +, \cdot)$, $(B, +, \cdot)$.

3.9. Dokážte, že direktný súčet dvoch oborov integrity nie je oborom integrity.

3.10. Nech R je množina reálnych čísel. Nech ďalej „$\oplus$" a „$\odot$" sú binárne operácie definované na množine $R \times R$ dané takto:

a) $(a, b) \oplus (c, d) = (ac, bc + d)$, $\qquad (a, b) \odot (c, d) = (ac, bd)$,
b) $(a, b) \oplus (c, d) = (a + c, b + d)$, $\qquad (a, b) \odot (c, d) = (ac + bc, ad + bd)$,
c) $(a, b) \oplus (c, d) = (ad + bc, bd)$, $\qquad (a, b) \odot (c, d) = (ac, bd)$,

kde a, b, c, d sú ľubovoľné reálne čísla. Rozhodnite, či štruktúra $(R \times R, \oplus, \odot)$ je okruh, komutatívny okruh prípadne okruh s jednotkovým prvkom.

3.11. Nech

$$\mathcal{M} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a, b \in R \right\}.$$

Dokážte, že štruktúra $(\mathcal{M}, +, \cdot)$ je pole.

3.12. Rozhodnite, či platia výroky

a) Každý podokruh poľa je pole.
b) Každý nadokruh poľa je pole.

Ak áno, dokážte príslušný výrok, ak nie, nájdite kontrapríklad.

§ 4. Okruhy zvyškových tried

Na začiatku tohto paragrafu si uvedieme niektoré vlastnosti celých čísel založené na binárnej relácii „delí“. Najprv dokážeme nasledujúcu vetu.

Veta 4.1 (veta o delení so zvyškom). *Nech $a, b \in Z$ sú ľubovoľné celé čísla také, že $b \neq 0$. Potom existujú jednoznačne určené celé čísla $q, r \in Z$ také, že platí rovnosť*

$$a = b \cdot q + r, \qquad kde \qquad 0 \leq r < |b|. \tag{4.1}$$

Dôkaz. Najprv dokážeme, že stačí uvažovať o prípade, keď celé číslo b je kladné. Naozaj: Ak by existovali jednoznačne určené celé čísla q, r pre ľubovoľné celé číslo a a kladné celé číslo b také, aby platilo $a = bq + r$, kde $0 \leq r < b = |b|$, potom by platilo aj $a = (-b)(-q) + r$, kde $0 \leq r < b = |b| = |-b|$. Čitateľ nech si uvedomí, že z jednoznačnosti q podľa vety 1.2 vyplýva aj jednoznačnosť $-q$.

A. Existencia. Nech sú teda dané ľubovoľné celé čísla a, b také, že $b > 0$. Najprv definujme množinu

$$M = \{b \cdot k;\ k \in Z\}.$$

Máme dve možnosti:

1) $a \in M$. Potom existuje celé číslo $s \in Z$ také, že $a = b \cdot s$, čiže $a = bs + 0$. Vidíme, že $q = s$ a súčasne $r = 0$, čiže existencia čísel q, r je pre tento prípad dokázaná. (Zrejme $0 \leq r < b$, lebo $r = 0$ a $b > 0$.)

2) $a \notin M$ (čitateľ si premyslí, že v tomto prípade $b \neq 1$). Potom zrejme*) existuje celé číslo q také, že $bq < a < b(q+1)$, čiže $bq < a < bq + b$. Odtiaľ máme $0 < a - bq < b$. Teraz položme $a - bq = r$. Vidíme, že

$$a = bq + r, \qquad \text{kde} \qquad 0 < r < b.$$

Ak vezmeme do úvahy aj výsledok 1), máme

$$a = bq + r, \qquad \text{kde} \qquad 0 \leq r < b,$$

alebo vzhľadom na to, že $b > 0$

$$a = bq + r, \qquad \text{kde} \qquad 0 \leq r < |b|.$$

Tým je existencia čísel $q, r \in Z$ takých, že platí (4.1) dokázaná.

B. Jednoznačnosť. Nepriamo. Budeme predpokladať, že existujú dve rôzne dvojice q_1, r_1 a q_2, r_2 tak, že

$$a = bq_1 + r_1, \text{ kde } 0 \leq r_1 < b,$$

$$a = bq_2 + r_2, \text{ kde } 0 \leq r_2 < b.$$

*) Táto „zrejmosť“ je založená na tom, že čitateľ má dobrú predstavu o rozložení čísel množiny M na číselnej osi. Presný dôkaz využívajúci pojem „dobré usporiadanie množiny prirodzených čísel“ bude vykonaný v predmete teória čísel.

Ak by $q_1 = q_2$ mali by sme
$$bq_1 + r_1 = bq_1 + r_2,$$
odkiaľ $r_1 = r_2$ a dvojice by boli rovnaké, čo je v spore s predpokladom. Nech preto $q_1 \neq q_2$ napr. $q_1 < q_2$. Potom $q_1 + 1 \leq q_2$. Z toho vyplýva $bq_1 + b \leq bq_2$. Preto máme $a = bq_1 + r_1 < bq_1 + b \leq bq_2 \leq a$, t.j. $a < a$, čo je spor. □

Príklad 4.1. Ak si zvolíme celé číslo n väčšie ako jeden a budeme ním deliť celé čísla, pri delení môžeme dostať n rôznych nezáporných zvyškov. Sú to zvyšky $0, 1, 2, \dots, n-1$. Napr. ak $n = 6$ máme zvyšky $0, 1, 2, 3, 4, 5$. Pri delení čísla 20 máme zvyšok 2, lebo $20 = 6 \cdot 3 + 2$, pri delení 13 zvyšok 1, lebo $13 = 6 \cdot 2 + 1$. Aký zvyšok bude, ak číslom 6 vydelíme -13? Píšeme $-13 = 6 \cdot (-2) + (-1)$. Dostali sme „zvyšok“ -1. Nie sme spokojní, lebo to nie je nezáporné celé číslo. Počítajme: $-13 = 6(-2) + (-1) + 6 - 6 = 6(-2-1) + (-1) + 6 = 6 \cdot (-3) + 5$. Zvyšok je 5.

Definícia 4.1. Nech $a, b \in Z$ sú celé čísla. Hovoríme, že číslo a *delí* číslo b, čo zapisujeme $a \mid b$, ak existuje číslo $c \in Z$ také, že $b = a \cdot c$. Ak také celé číslo c neexistuje, tak hovoríme, že a *nedelí* b, čo zapisujeme $a \nmid b$.

Príklad 4.2. Vidíme, že $3 \mid 12$, $-3 \mid 12$, $3 \mid 0$, $1 \mid 7$, $7 \nmid 2$ a pod.

Veta 4.2. *Relácia „$\mid$“ definovaná na množine Z v definícii 4.1 má nasledovné vlastnosti. Pre všetky $a, b, c, x, y \in Z$ platí:*

(1) $a \mid 0$,
(2) $0 \mid a$ *práve vtedy, keď* $a = 0$,
(3) *ak* $a \mid b$, *tak* $(-a) \mid b$, $a \mid (-b)$, $(-a) \mid (-b)$,
(4) $a \mid a$,
(5) *ak* $a \mid b$ *a zároveň* $b \mid c$, *tak* $a \mid c$,
(6) *ak* $a \mid b$, *tak* $a \mid bc$,
(7) *ak* $a \mid b$, *tak* $ac \mid bc$,
(8) *ak* $ac \mid bc$ *a zároveň* $c \neq 0$, *tak* $a \mid b$,
(9) *ak* $a \mid b + c$ *a zároveň* $a \mid b$, *tak* $a \mid c$,
(10) *ak* $a \mid b$ *a zároveň* $a \mid c$, *tak* $a \mid (bx + cy)$. *)

Dôkaz uvedených tvrdení je jednoduchý. Ponecháme ho čitateľovi (cvičenie 4.1). □

Poznámka 4.1. Z vlastnosti (4) a (5) vyplýva, že relácia „ $\mid$ “ je reflexívna a tranzitívna.

Definícia 4.2. Nech a, b sú ľubovoľné celé čísla. Nech celé číslo d má tieto vlastnosti:

(i) $d \mid a$ a zároveň $d \mid b$,

(ii) ak d^* je také celé číslo, že $d^* \mid a$ a zároveň $d^* \mid b$, tak $d^* \mid d$.

Potom číslo d nazývame *najväčším spoločným deliteľom* (v skratke NSD) celých čísel a, b. Ďalej označíme $|d| = (a, b)$.

Inými slovami: Najväčší spoločný deliteľ je taký spoločný deliteľ, ktorý delia všetky spoločné delitele.

*) Môžeme písať aj $a \mid bx + cy$, teda bez zátvorky (prečo?).

Poznámka 4.2. Čitateľ ľahko skontroluje, že ak d je NSD čísel a, b, tak aj $-d$ je ich najväčším spoločným deliteľom. Ak napríklad $a = 12$, $b = 18$, tak ich spoločné delitele sú: $-6, -3, -2, -1, 1, 2, 3, 6$ a ich NSD je číslo 6 ako aj -6. Vidieť, že NSD vôbec nemusí byť „najväčší" v zmysle usporiadania celých čísel. Nezáporný NSD sme označili (a, b). Preto $(12, 18) = 6$.

Okrem toho hneď vidieť, že $(a, b) = (b, a)$, $(a, 0) = |a|$, $(0, b) = |b|$, $(0, 0) = 0$ pre všetky $a, b \in Z$.

Veta 4.3. *Nech a, b sú ľubovoľné celé čísla. Potom existuje ich najväčší spoločný deliteľ.*

Dôkaz. Vzhľadom na poznámku 4.2 stačí nájsť najväčší spoločný deliteľ pre nenulové celé čísla. Nech teda $a \neq 0$, $b \neq 0$. Vzhľadom na tú istú poznámku stačí nájsť taký NSD, ktorý je kladný. To urobíme takto:

Najprv definujeme množinu $M = \{ax + by;\ x, y \in Z\}$. Hovoríme, že takáto množina je množinou všetkých lineárnych kombinácií čísel a, b. Ľahko zistíme, že M obsahuje aj kladné celé čísla. Naozaj, ak a je kladné, stačí voliť $x = 1$, $y = 0$, ak a je záporné, stačí voliť $x = -1$, $y = 0$. Nech $d = ax_0 + by_0$ je najmenšie kladné celé číslo z množiny M. Dokážeme, že $d = (a, b)$. Podľa vety 4.1 existujú celé čísla q, r také, že platí

$$a = dq + r, \text{ kde } 0 \leq r < d.$$

Počítajme

$$a = dq + r = (ax_0 + by_0)q + r,$$

odkiaľ máme

$$r = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0)q.$$

Vidíme, že $r \in M$. Keďže $0 \leq r < d$ a d je najmenšie kladné číslo z množiny M, musí byť $r = 0$. Preto $a = dq$, čiže $d \mid a$. Analogicky dokážeme, že $d \mid b$. Teda d má prvú vlastnosť najväčšieho spoločného deliteľa. Dokážeme, že má aj druhú vlastnosť. Nech d^* je také celé číslo, že $d^* \mid a$ a zároveň $d^* \mid b$. Potom podľa (10) vety 4.2 $d^* \mid (ax_0 + by_0) = d$. Tým sme dokázali, že $d = (a, b)$. □

Dôsledok. *Nech d je najväčší spoločný deliteľ celých čísel a, b. Potom existujú celé čísla x_0, y_0, také, že $d = ax_0 + by_0$.*

Dôkaz. a) Predpokladajme najskôr, že $d \geq 0$. Ak niektoré z čísel napr. b je rovné nule a druhé ľubovoľné, máme $d = |a| = (a, 0)$. Potom ak $a \geq 0$, príslušné vyjadrenie je $d = a \cdot 1 + 0 \cdot c$ (číslo c je ľubovoľné celé číslo), ak $a < 0$, tak $d = -a = a \cdot (-1) + 0 \cdot c$ je príslušné vyjadrenie. Ak sú obe nenulové, vyjadrenie $d = ax_0 + by_0$ sme našli v dôkaze vety 4.3.

b) Teraz predpokladajme $d < 0$. Podľa bodu a) nájdeme vyjadrenie $|d| = ax_0 + by_0$, odkiaľ máme $d = a(-x_0) + b(-y_0)$. □

Definícia 4.3. Kladné celé číslo $p \neq 1$ sa nazýva *prvočíslo*, ak ho delia len tieto čísla: $1, -1, p, -p$. Teda prvočísla sú $2, 3, 5, 7, \cdots$.

Definícia 4.4. Celé čísla a, b nazývame *nesúdeliteľné*, ak $(a, b) = 1$.

Poznámka 4.3. Prvočíslo p je nesúdeliteľné s každým nenulovým celým číslom rôznym od $\pm p$.

Veta 4.4. *Nech a, b, c sú celé čísla také, že $a \mid bc$ a tiež $(a, b) = 1$. Potom $a \mid c$.*

Dôkaz. Ak $c = 0$, veta platí. Nech $c \neq 0$. Podľa dôsledku vety 4.3 existujú celé čísla x_0, y_0, také, že $ax_0 + by_0 = 1$. Odtiaľ, po vynásobení rovnosti číslom c, máme $acx_0 + bcy_0 = c$. Vidieť, že číslo a delí ľavú stranu rovnosti. Preto $a \mid c$, čo sme chceli dokázať. $\square$

Definícia 4.5. Nech je dané pevne zvolené celé číslo $n \geq 2$. Na množine Z definujme binárnu reláciu „$\equiv \pmod{n}$" takto:

$$\text{Pre všetky} \quad a, b \in Z \quad a \equiv b \pmod{n} \quad \text{vtedy a len vtedy, keď} \quad n \mid a - b.$$

Potom binárnu reláciu „$\equiv \pmod{n}$" nazývame *kongruenciou* podľa modulu n.

Vzťah $a \equiv b \pmod{n}$ čítame: „a kongruentné b modulo n".

Príklad 4.3. Nech $n = 6$. Potom $-14 \equiv 10 \pmod 6$, lebo $-14 - 10 = -24$ a $6 \mid (-24)$. Podobne $7 \equiv 19 \pmod 6$, lebo $6 \mid (-12) = 7 - 19$.

Veta 4.5. *Relácia „$\equiv \pmod{n}$" z definície 4.5 je reláciou ekvivalencie na množine Z.*

Dôkaz. Dokážeme, že relácia kongruencie je reflexívna, symetrická a tranzitívna. Nech a, b, c sú ľubovoľné celé čísla.

1) Platí $a \mid 0$, teda aj $a \mid a - a$, čiže $a \equiv a \pmod{n}$, t.j. relácia je reflexívna.

2) Ak $a \equiv b \pmod{n}$, tak $n \mid a - b$. Preto aj $n \mid b - a$, čiže $b \equiv a \pmod{n}$. Vidieť, že relácia je symetrická.

3) Ak $a \equiv b \pmod{n}$ a zároveň $b \equiv c \pmod{n}$, tak $n \mid a - b$ a zároveň $n \mid b - c$. Preto $n \mid (a - b) + (b - c) = a - c$, čiže $a \equiv c \pmod{n}$, t.j. relácia je tranzitívna. $\square$

Čitateľ už vie, každá relácia ekvivalencie „rozdelí" množinu na ktorej pôsobí na disjunktné triedy. Preto ak je na množine Z definovaná relácie kongruencie, je tým tiež daný jej rozklad na disjunktné triedy. Nech a je ľubovoľné celé číslo. Trieda, ktorú definuje je daná takto:

$$\overline{a} = \{x \in Z;\, x \equiv a \pmod{n}\}. \tag{2}$$

Triedy (2) nazývame zvyškové triedy podľa modulu n, alebo kratšie zvyškové triedy modulo n. Dokážeme o nich niekoľko pomocných viet. Najprv poznamenajme, že každé celé číslo $a \in Z$ patrí do triedy, ktorú definuje, t.j. $a \in \overline{a}$. Ďalej, dve rôzne zvyškové triedy sú aj disjunktné, t.j. $\overline{a} \neq \overline{b} \Rightarrow \overline{a} \cap \overline{b} = \emptyset$ (cvičenie 4.6).

Lema 4.1. *Nech $a_1 \in \overline{a}$. Potom $\overline{a} = \overline{a}_1$.* Inými slovami: *Zvyšková trieda je určená ľubovoľným svojím prvkom.*

Dôkaz. Najprv poznamenajme, že ak $a_1 \in \overline{a}$, tak $a_1 \equiv a \pmod{n}$. Máme dokázať rovnosť množín $\overline{a}$ a $\overline{a}_1$.

1) Nech $x \in \overline{a}$, čo znamená $x \equiv a \pmod{n}$. Ale je aj $a \equiv a_1 \pmod{n}$, a tak máme (tranzitívnosť) $x \equiv a_1 \pmod{n}$, t.j. $x \in \overline{a}_1$. Keďže x je ľubovoľný prvok triedy $\overline{a}$, platí $\overline{a} \subseteq \overline{a}_1$.

2) Inklúzia $\overline{a}_1 \subseteq \overline{a}$ sa dokáže podobne. Máme tak $\overline{a} = \overline{a}_1$. $\square$

Lema 4.2. *Dve celé čísla $x, y \in Z$ patria do tej istej zvyškovej triedy práve vtedy, keď $x \equiv y \pmod{n}$.*

Dôkaz. I. Nech $x \in \overline{a}$ a zároveň $x \equiv y \pmod{n}$. Potom $a \equiv x \pmod{n}$ a zároveň $x \equiv y \pmod{n}$, z čoho vyplýva $a \equiv y \pmod{n}$, čo znamená $y \in \overline{a}$.

II. Nech $x \in \overline{a}$ a zároveň $y \in \overline{a}$. Odtiaľ máme $x \equiv a \pmod{n}$ a zároveň $a \equiv y \pmod{n}$, čiže $x \equiv y \pmod{n}$. □

Lema 4.3. *Dve celé čísla $x, y \in Z$ patria do tej istej zvyškovej triedy práve vtedy, keď po delení číslom n dávajú ten istý zvyšok.*

Dôkaz. I. Nech dávajú ten istý zvyšok r, t.j.

$$\begin{aligned} x &= nq_1 + r, \\ y &= nq_2 + r. \end{aligned}$$

Po odčítaní máme

$$x - y = n(q_1 - q_2),$$

odkiaľ vyplýva $n \mid x - y$ alebo $x \equiv y \pmod{n}$. Potom podľa lemy 4.2 patria do tej istej zvyškovej triedy.

II. Nech celé čísla x, y patria do tej istej zvyškovej triedy. Potom podľa lemy 4.2 platí $x \equiv y \pmod{n}$, čiže $n \mid x - y$. To znamená, že existuje celé číslo k, také, že $x - y = kn$. Nech

$$\begin{aligned} x &= nq_1 + r_1, \quad \text{pričom} \quad 0 \le r_1 < n, \\ y &= nq_2 + r_2, \quad \text{pričom} \quad 0 \le r_2 < n. \end{aligned}$$

Odčítaním a ďalšou úpravou máme

$$\begin{aligned} x - y &= n(q_1 - q_2) + r_1 - r_2, \\ kn &= n(q_1 - q_2) + r_1 - r_2, \\ n(k - q_1 + q_2) &= r_1 - r_2. \end{aligned}$$

Vidieť, že číslo $r_1 - r_2$ je násobkom čísla n, pričom $0 \le |r_1 - r_2| < n$. To môže nastať len vtedy, keď $r_1 - r_2 = 0$, čiže keď $r_1 = r_2$. □

Lema 4.4. *Nech a, b, a_1, b_1 sú také celé čísla, že platí:*

$$a_1 \equiv a \pmod{n} \qquad b_1 \equiv b \pmod{n}$$

Potom platí tiež:

$$a_1 + b_1 \equiv a + b \pmod{n} \qquad a_1 \cdot b_1 \equiv a \cdot b \pmod{n}.$$

Inými slovami: *Kongruencia modulo n „zachováva“ operáciu sčítania i násobenia celých čísel.*

Dôkaz. 1) Dokážeme, že zachováva sčítanie. Nech $a_1 \equiv a \pmod{n}$ a zároveň $b_1 \equiv b \pmod{n}$. Potom $n \mid a_1 - a$ a zároveň $n \mid b_1 - b$, odkiaľ $n \mid a_1 - a + b_1 - b$ alebo $n \mid a_1 + b_1 - (a + b)$, čiže $a_1 + b_1 \equiv a + b \pmod{n}$.

2) Dokážeme, že zachováva násobenie. Nech $a_1 \equiv a \pmod n$ a zároveň $b_1 \equiv b \pmod n$. Potom $n \mid a_1 - a$ a zároveň $n \mid b_1 - b$, odkiaľ $n \mid a_1b_1 - ab_1$ a zároveň $n \mid ab_1 - ab$. Potom $n \mid a_1b_1 - ab_1 + ab_1 - ab$, čiže $n \mid a_1b_1 - ab$ alebo $a_1b_1 \equiv ab \pmod n$.

□

Cieľom ďalších úvah je uviesť definíciu a najjednoduchšie vlastnosti okruhu zvyškových tried.

Uvažujme o množine celých čísel $Z = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$. Dokázali sme (veta 4.1), že ak máme dve celé čísla a, n, kde $n > 1$, tak existujú jednoznačne dané celé čísla q, r také, že $a = nq + r$, kde $r \in \{0, 1, 2, \dots, n-1\}$. Ku každému celému číslu a je teda jednoznačne určený zvyšok r, ktorý dostaneme po delení čísla a číslom n. To znamená, že všetky celé čísla sa dajú roztriediť do n tried podľa toho, aký zvyšok „dávajú" po delení číslom n. Tieto tzv. zvyškové triedy podľa lemy 4.2 a 4.3 sú vlastne triedy kongruencie podľa modulu n. Zvyškové triedy v súhlase s vyššie uvedeným označíme $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}$. Do triedy $\overline{0}$ dáme všetky celé čísla ktoré dávajú zvyšok 0, do $\overline{1}$ tie celé čísla, ktoré dávajú zvyšok 1, atď. Zrejme platí $Z = \overline{0} \cup \overline{1} \cup \overline{2} \cup \dots \cup \overline{(n-1)}$. Okrem toho: Ak $\overline{a} \neq \overline{b}$, tak $\overline{a} \cap \overline{b} = \emptyset$. Systém zvyškových tried budeme označovať znakom Z_n. Teda

$$Z_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}.$$

Príklad 4.4. Ak $n = 6$, ide o tieto zvyškové triedy:

$$\begin{aligned}
\overline{0} &= \{\dots, -18, -12, -6, 0, \ \ 6, 12, 18, \dots\},\\
\overline{1} &= \{\dots, -17, -11, -5, 1, \ \ 7, 13, 19, \dots\},\\
\overline{2} &= \{\dots, -16, -10, -4, 2, \ \ 8, 14, 20, \dots\},\\
\overline{3} &= \{\dots, -15, \ -9, -3, 3, \ \ 9, 15, 21, \dots\},\\
\overline{4} &= \{\dots, -14, \ -8, -2, 4, 10, 16, 22, \dots\},\\
\overline{5} &= \{\dots, -13, \ -7, -1, 5, 11, 17, 23, \dots\}.
\end{aligned}$$

Systém $Z_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ je teda množinou zvyškových tried podľa modulu 6. Čitateľovi odporúčame, aby si podobne určil množiny Z_2, Z_3, Z_4, Z_5 a Z_7.

Príklad 4.5. Podľa toho čo sme povedali, platí: Ak celé číslo a patrí do triedy $\overline{x} \in Z_n$, tak ho možno písať v tvare $a = n \cdot q + x$. Napríklad ak $a \in \overline{2}, \overline{2} \in Z_6$, tak $a = 6q + 2$; ak $\overline{2} \in Z_3$, tak $a = 3q + 2$, atď. Preto zvyškové triedy množiny Z_n môžeme ľahko zapísať aj takto:

$$\begin{aligned}
\overline{0} &= \{x \in Z; \quad x = nq, \quad q \in Z\},\\
\overline{1} &= \{x \in Z; \quad x = nq + 1, \quad q \in Z\},\\
\overline{2} &= \{x \in Z; \quad x = nq + 2, \quad q \in Z\},\\
&\vdots\\
\overline{n-1} &= \{x \in Z; \quad x = nq + n - 1, \quad q \in Z\}.
\end{aligned}$$

Čitateľ nech si analogickým spôsobom napíše triedy systémov Z_2, Z_3, Z_4, Z_5 a Z_7. Tiež je dobré uvedomiť si, že $0 \in \overline{0}$, $1 \in \overline{1}, \dots, n-1 \in \overline{n-1}$.

Teraz na množine Z_n definujeme operácie sčítania a násobenia.

Definícia 4.6. Na množine zvyškových tried Z_n definujeme operácie „+“ a „·“ takto: Nech $\overline{a}$, $\overline{b}$ sú ľubovoľné prvky množiny Z_n. Potom

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Sčítanie a násobenie tried v definícii 4.6 sme definovali pomocou tzv. „reprezentantov tried“. Naozaj $a \in \overline{a}$ a $b \in \overline{b}$. Triedy $\overline{a}$, $\overline{b}$ sme sčítali tak, že sme vykonali súčet ich reprezentantov $a + b$ a súčtom bola trieda $\overline{a+b}$, ktorú tento súčet definoval t.j. trieda, do ktorej patrí súčet $a + b$. Podobne sme definovali aj súčin. Aby sme naše úvahy položili na seriózny základ, musíme dokázať, že súčet tried, ani ich súčin, nezávisí od výberu reprezentantov, t.j. výsledok bude taký istý nech už vyberieme reprezentantov akokoľvek. To dokážeme v nasledujúcej vete.

Veta 4.6. *Nech $\overline{a}$, $\overline{b}$ sú ľubovoľné triedy systému zvyškových tried Z_n. Nech $a_1 \in \overline{a}$, $b_1 \in \overline{b}$. Potom*

$$\overline{a_1 + b_1} = \overline{a+b} \qquad \overline{a_1 \cdot b_1} = \overline{a \cdot b}$$

Inými slovami: *Súčet ani súčin tried nezávisí od reprezentantov tried, pomocou ktorých definujeme výsledné triedy.*

Dôkaz. 1) Pre súčet: Nech $a_1 \in \overline{a}$, $b_1 \in \overline{b}$. Potom $a_1 \equiv a \pmod{n}$ a tiež $b_1 \equiv b \pmod{n}$. Podľa lemy 4.4 máme $a_1 + b_1 \equiv a + b \pmod{n}$, ale potom podľa lemy 4.2 $\overline{a_1 + b_1} = \overline{a+b}$.

2) Dôkaz pre súčin sa vykoná podobne. □

Príklad 4.6. Sčítajme napr. triedy $\overline{3}$ a $\overline{5} \in Z_6$. V triede $\overline{3}$ zvoľme napr. -9, v triede $\overline{5}$ zvoľme hoci 23. Pozrime sa kde padne súčet $-9 + 23 = 14$. Vidíme, že $14 \in \overline{2}$. Teda $\overline{3} + \overline{5} = \overline{2}$. Ak zvolíme iných reprezentantov napr. $9 \in \overline{3}$, $11 \in \overline{5}$, vidíme, že znova $9 + 11 = 20 \in \overline{2}$. Samozrejme, za reprezentantov tried $\overline{r}$ a $\overline{s}$ môžeme zvoliť aj r, s, lebo $r \in \overline{r}$, $s \in \overline{s}$ a zjednodušiť si tak počítanie. Podobne pre súčin. Vynásobme tie isté triedy $\overline{3}$ a $\overline{5} \in Z_6$. V triede $\overline{3}$ zvoľme ako vyššie -9, v triede $\overline{5}$ zvoľme 23. Pozrime sa kde padne súčin $-9 \cdot 23 = -207$. Vidíme, že $-207 \in \overline{3}$. Teda $\overline{3} \cdot \overline{5} = \overline{3}$. Ak zvolíme $9 \in \overline{3}$, $11 \in \overline{5}$, vidíme, že aj $9 \cdot 11 = 99 \in \overline{3}$.

Veta 4.7. *Ak v množine zvyškových tried modulo n definujeme operácie „+“ a „·“ ako v definícii 4.6, tak štruktúra $(Z_n, +, \cdot)$ je komutatívny okruh s jednotkovým prvkom.*

Dôkaz. I. Dokážeme, že štruktúra $(Z, +)$ je abelovská grupa.

a) Z definície 4.6 a vety 4.6 vyplýva, že $(Z_n, +)$ je grupoid.

b) Dokážeme, že operácia „+“ je asociatívna. Nech $\overline{r}, \overline{s}, \overline{t} \in Z_n$ sú ľubovoľné prvky množiny Z_n. Počítajme

$$(\overline{r} + \overline{s}) + \overline{t} = \overline{r+s} + \overline{t} = \overline{(r+s)+t} = \overline{r+(s+t)} = \overline{r} + \overline{s+t} = \overline{r} + (\overline{s} + \overline{t}).$$

Teda $(Z_n, +)$ je pologrupa.

c) Neutrálnym prvkom pologrupy $(Z_n, +)$ je trieda $\overline{0}$. Dôkaz tohto faktu ponecháme na čitateľa.

d) Nech $\overline{r} \in Z_n$ je ľubovoľná trieda množiny Z_n. Potom $-\overline{r} = \overline{n-r}$. Skutočne

$$\overline{r} + \overline{n-r} = \overline{r+n-r} = \overline{n} = \overline{0},$$

podobne

$$\overline{n-r} + \overline{r} = \overline{n-r+r} = \overline{n} = \overline{0}.$$

e) Čitateľ ľahko dokáže, že operácia „+“ je komutatívna.

II. Dokážeme, že štruktúra $(Z_n, \cdot)$ je komutatívna pologrupa s neutrálnym prvkom (komutatívny monoid).

a) Podobne, ako vyššie, z definície 4.6 a vety 4.6 vyplýva, že štruktúra $(Z_n, \cdot)$ je grupoid.

b) Dôkaz asociatívnosti je podobný ako pri sčítaní. Nech $\overline{r}, \overline{s}, \overline{t} \in Z_n$ sú ľubovoľné prvky množiny Z_n. Počítajme

$$(\overline{r} \cdot \overline{s}) \cdot \overline{t} = \overline{r \cdot s} \cdot \overline{t} = \overline{(r \cdot s) \cdot t} = \overline{r \cdot (s \cdot t)} = \overline{r} \cdot \overline{s \cdot t} = \overline{r} \cdot (\overline{s} \cdot \overline{t}).$$

Teda $(Z_n, \cdot)$ je pologrupa.

Komutatívnosť operácie „$\cdot$“ je zrejmá. Tiež vidieť, že $\overline{1} \in Z_n$ je neutrálnym prvkom operácie „$\cdot$“ (overte to!).

III. Dokážeme, že operácia „$\cdot$“ je distributívna vzhľadom na operáciu „+“. Keďže operácia „$\cdot$“ je komutatívna, stačí dokázať len jeden, napr. pravý, distributívny zákon. Nech $\overline{r}, \overline{s}, \overline{t} \in Z_n$ sú ľubovoľné prvky množiny Z_n.
Počítajme

$$(\overline{r} + \overline{s}) \cdot \overline{t} = \overline{r+s} \cdot \overline{t} = \overline{(r+s) \cdot t} = \overline{r \cdot t + s \cdot t} = \overline{r \cdot t} + \overline{s \cdot t} = \overline{r} \cdot \overline{t} + \overline{s} \cdot \overline{t}.$$

Vidíme, že distributívny zákon platí. Tým je veta dokázaná. □

Príklad 4.7. Nasledujúce Cayleyho tabuľky sú tabuľky okruhu $(Z_6, +, \cdot)$. Čitateľ si môže skontrolovať, že prvá tabuľka je naozaj tabuľkou grupy $(Z_6, +)$ a druhá tabuľkou monoidu $(Z_6, \cdot)$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Všimnime si, že pre nenulové prvky tohto okruhu $\overline{2}, \overline{3} \in Z_6$ platí $\overline{2} \cdot \overline{3} = \overline{0}$. Teda máme ďalší príklad okruhu, čo nie je oborom integrity. Avšak existujú také okruhy zvyškových tried, ktoré obormi integrity sú. Hovorí o tom nasledujúca veta.

Veta 4.8. *Okruh $(Z_n, +, \cdot)$ je pole (teda aj obor integrity) práve vtedy, keď n je prvočíslo.*

Dôkaz. I. Nech $(Z_n, +, \cdot)$ je pole. Ak by n nebolo prvočíslo, potom by existovali také čísla $r, s \in Z$, že $n = r \cdot s$ (kde $1 < r,\ s < n$) a mali by sme $\overline{r} \cdot \overline{s} = \overline{0}$ t.j. Z_n by nebol obor integrity a teda ani pole – spor!

II. Nech n je prvočíslo. Nech $\overline{r} \in Z_n$ je ľubovoľná trieda okruhu Z_n taká, že $\overline{r} \neq \overline{0}$. Potom čísla r a n sú nesúdeliteľné. Odtiaľ vyplýva existencia celých čísel x, y takých, že platí $rx + ny = 1$ (pozri dôsledok vety 4.3). Preto $\overline{rx+ny} = \overline{1}$, čiže $\overline{rx} + \overline{ny} = \overline{1}$, a teda $\overline{rx} + \overline{ny} = \overline{1}$. Keďže $\overline{n} = \overline{0}$, máme $\overline{rx} + \overline{0}\overline{y} = \overline{1}$ a tak $\overline{rx} = \overline{1}$, čo znamená, že $\overline{x} = (\overline{r})^{-1}$. Vidíme, že ľubovoľný nenulový prvok okruhu $(Z_n, +, \cdot)$

má inverzný prvok, čím sme dokázali, že $(Z_n, +, \cdot)$ je pole a teda aj obor integrity.
□

Príklad 4.8. Uvedieme tabuľky poľa $(Z_5, +, \cdot)$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Čitateľa prosíme, aby si skontroloval, že štruktúra $(Z_5, +, \cdot)$ má všetky vlastnosti poľa. Napr. prvky $\overline{1}$ a $\overline{4}$ sú vzhľadom na násobenie sami sebe inverzné, zatiaľ čo prvok $\overline{3}$ je inverzný prvku $\overline{2}$ a naopak.

Poznámka 4.4. Doteraz sme sa zoznámili s poľom racionálnych, reálnych a komplexných čísel: $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$. Tieto tzv. číselné polia vlastne poznáme zo strednej školy (i keď sa tam pojem pole nepoužíval). Sú to všetko nekonečné polia. Ako sme videli v tomto paragrafe, môžu existovať aj konečné polia, ako sú polia zvyškových tried podľa prvočíselného modulu, t.j. polia $(Z_2, +, \cdot)$, $(Z_3, +, \cdot)$, $(Z_5, +, \cdot)$, atď. Neskoršie sa zoznámime aj s ďalšími konečnými poliami. V číselných poliach bežne používame zlomky. Napríklad: ak a je nenulové reálne číslo, tak v poli reálnych čísel k nemu existuje inverzný prvok a^{-1}, ktorý zapíšeme bežným spôsobom v tvare zlomku $a^{-1} = \frac{1}{a}$. Tento zápis (t.j. v tvare zlomku) sa v konečných poliach nepoužíva. Napriek tomu v ďalšom texte sa vyskytnú úvahy, v ktorých máme na mysli pole v úplnej všeobecnosti (t.j. konečné alebo nekonečné) a zlomky pre jednoduchosť používame. V tomto prípade čitateľ vždy môže miesto výrazu $\frac{a}{b}$ použiť výraz $a \cdot b^{-1}$, ktorý je prípustný aj v konečných poliach.

Príklad 4.9. V poli zvyškových tried $(Z_5, +, \cdot)$ riešte rovnicu $(\overline{3} \cdot x) + \overline{4} = \overline{3}$.

Riešenie. Pri počítaní budeme využívať Cayleyho tabuľky operácií $+, \cdot$, ktoré sme zostrojili v príklade 4.8. K obom stranám rovnice pripočítame prvok $\overline{1}$, ktorý je opačný k prvku $\overline{4}$. Dostaneme $\overline{3} \cdot x = \overline{4}$.

V obyčajnej algebre by sme teraz delili prvok $\overline{4}$ prvkom $\overline{3}$. Ako to urobíme tu? Z tabuľky pre násobenie vidíme, že inverzným prvkom prvku $\overline{3}$ je prvok $\overline{2}$. Preto poslednú rovnicu násobíme zľava $\overline{2}$. Máme

$$\overline{2} \cdot (\overline{3} \cdot x) = \overline{2} \cdot \overline{4}.$$

Uplatnením asociatívneho zákona a vlastnosti neutrálneho prvku dostávame $x = \overline{3}$.

Skúška: Dosadením do ľavej strany rovnice máme: $(\overline{3} \cdot x) + \overline{4} = (\overline{3} \cdot \overline{3}) + \overline{4} = \overline{4} + \overline{4} = \overline{3}$. Vidíme, že pravá strana rovnice sa rovná ľavej.

Cvičenia

4.1. Dokážte vetu 4.2. Formulujte zovšeobecnenie tvrdenia (10) a dokážte ho.

4.2. Nech $a, b \in Z$ sú ľubovoľné celé čísla a k ľubovoľné prirodzené číslo. Potom platí: Ak $a \equiv b \pmod{n}$, tak aj $ka \equiv kb \pmod{kn}$. Dokážte to.

4.3. Určte všetky celé čísla x, také, že $0 \leq x < 15$ a zároveň $3x \equiv 6 \pmod{15}$.

4.4. Dokážte, že platí $6^k \equiv 6 \pmod{10}$, kde k je ľubovoľné prirodzené číslo.

4.5. Zostavte Cayleyho tabuľky pre operácie $\oplus, \odot$ v okruhoch Z_2, Z_3, Z_4, Z_7.

4.6. Nech $Z_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ je systém tried podľa modulu n. Nech $\overline{a}, \overline{b} \in Z_n$. Potom platí:

$$Z = \overline{0} \cup \overline{1} \cup \overline{2} \cup \cdots \cup \overline{(n-1)}.$$

Okrem toho:

$$\text{Ak} \quad \overline{a} \neq \overline{b}, \quad \text{tak} \quad \overline{a} \cap \overline{b} = \emptyset.$$

Dokážte to.

4.7. Dokážte bod c) a e) z prvej časti dôkazu vety 4.7.

4.8. Nech $(Z_n, +, \cdot)$ je okruh zvyškových tried podľa modulu n. Potom prvok $\overline{b} \in Z_n$ má v monoide $(Z_n, \cdot)$ inverzný prvok práve vtedy, keď čísla b a n sú nesúdeliteľné, t.j. $(b, n) = 1$. Dokážte to.

4.9. V poli $(Z_5, \oplus, \odot)$ riešte rovnice: $\overline{4} \oplus x = \overline{2}$, $\overline{3} \oplus x = \overline{1}$, $\overline{2} \oplus x = \overline{4}$, $(\overline{2} \odot x) \oplus \overline{3} = \overline{1}$, $(\overline{4} \odot x) \oplus \overline{4} = \overline{2}$ s neznámou x.

4.10. V okruhu $(Z_4, \oplus, \odot)$ riešte rovnicu $(\overline{2} \odot x) \oplus \overline{3} = \overline{2}$ s neznámou x.

4.11. Zistite, ktorá z nasledujúcich množín

$$\{1, 3, 4, 5, 9\}, \{1, 3, 5, 7, 8\}, \{1, 8\}, \{1, 10\}$$

je grupa vzhľadom na operáciu násobenia zvyškových tried podľa modulu 11.

Kapitola 2

VEKTOROVÉ PRIESTORY

§ 1. Vektorový priestor nad poľom

Pojem vektorového priestoru je základným pojmom tejto kapitoly. Preto venujme jeho definícii náležitú pozornosť. Začneme príkladom.

Príklad 1.1. Na strednej škole sa definuje vektor ako „posunutie" v rovine, prípadne v priestore. Znázorňujeme ho orientovanou úsečkou. Dve orientované úsečky predstavujú ten istý vektor, keď sú súhlasne orientované a majú rovnakú dĺžku. Označme množinu všetkých vektorov, ktoré ležia v nejakej rovine znakom $\boldsymbol{V}$. V zhode s tým čo sme povedali, tieto vektory si môžeme predstaviť ako všetky možné orientované úsečky vychádzajúce z nejakého pevne zvoleného bodu danej roviny. Nech $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}} \in \boldsymbol{V}$ sú dva ľubovoľné vektory. Tieto vektory vieme sčítať pomocou tzv. rovnobežníkového pravidla. Môžeme teda predpokladať, že

1. ak $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}} \in \boldsymbol{V}$, tak existuje vektor $\vec{\boldsymbol{a}}+\vec{\boldsymbol{b}} \in \boldsymbol{V}$, ktorý nazývame súčtom vektorov $\vec{\boldsymbol{a}}$ a $\vec{\boldsymbol{b}}$.

Zo známych vlastností rovnobežníka (čitateľ urobí dobre, keď si nakreslí obrázky) vyplývajú nasledujúce dve pravidlá:

2. Ak $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}} \in \boldsymbol{V}$, tak $\vec{\boldsymbol{a}} + \vec{\boldsymbol{b}} = \vec{\boldsymbol{b}} + \vec{\boldsymbol{a}}$, t.j. sčítanie vektorov je komutatívne.

3. Ak $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}}, \vec{\boldsymbol{c}} \in \boldsymbol{V}$, tak $(\vec{\boldsymbol{a}}+\vec{\boldsymbol{b}})+\vec{\boldsymbol{c}} = \vec{\boldsymbol{a}}+(\vec{\boldsymbol{b}}+\vec{\boldsymbol{c}})$, t.j. sčítanie vektorov je asociatívne.

Na strednej škole sa tiež definuje nulový vektor $\vec{\mathbf{0}}$ (posunutie, ktoré má nulovú veľkosť), o ktorom platí pravidlo:

4. Nech $\vec{\boldsymbol{a}}$ je ľubovoľný vektor množiny $\boldsymbol{V}$. Potom $\vec{\boldsymbol{a}} + \vec{\mathbf{0}} = \vec{\mathbf{0}} + \vec{\boldsymbol{a}} = \vec{\boldsymbol{a}}$.

Poznáme aj pojem vektora $-\vec{\boldsymbol{a}}$ (inverzné posunutie k posunutiu $\vec{\boldsymbol{a}}$). Platí pravidlo:

5. Ku každému vektoru $\vec{\boldsymbol{a}} \in \boldsymbol{V}$ existuje vektor $-\vec{\boldsymbol{a}}$ (zvaný opačný), o ktorom platí $-\vec{\boldsymbol{a}} + \vec{\boldsymbol{a}} = \vec{\boldsymbol{a}} + (-\vec{\boldsymbol{a}}) = \vec{\mathbf{0}}$.

Keď si pozorne všimneme pravidlá 1. až 5., zistíme, že tieto sú nič iné ako axiómy komutatívnej grupy, teda množina $\boldsymbol{V}$ je vzhľadom na operáciu „+" komutatívna grupa.

Čitateľovi je iste známe, že vektor $\vec{\boldsymbol{a}} \in \boldsymbol{V}$ je možné násobiť reálnym číslom k. Súčin $k \cdot \vec{\boldsymbol{a}}$ je vektor, ktorý leží na tej istej priamke ako vektor $\vec{\boldsymbol{a}}$, ale jeho veľkosť (t.j. veľkosť orientovanej úsečky, ktorá ho predstavuje) je $|k|$-násobok veľkosti vektora $\vec{\boldsymbol{a}}$, pričom orientácia vektora $k \cdot \vec{\boldsymbol{a}}$ je súhlasná s orientáciou vektora $\vec{\boldsymbol{a}}$ ak $k > 0$, ale opačná ak $k < 0$. Okrem toho $0 \cdot \vec{\boldsymbol{a}} = \vec{\mathbf{0}}$. Ľahko sa presvedčíme, že ak

$\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}}$ sú vektory, s, t reálne čísla, platia pravidlá:

6. $s \cdot (\vec{\boldsymbol{a}} + \vec{\boldsymbol{b}}) = s \cdot \vec{\boldsymbol{a}} + s \cdot \vec{\boldsymbol{b}}$,
7. $(s + t) \cdot \vec{\boldsymbol{a}} = s \cdot \vec{\boldsymbol{a}} + t \cdot \vec{\boldsymbol{a}}$,
8. $(s \cdot t) \cdot \vec{\boldsymbol{a}} = s \cdot (t \cdot \vec{\boldsymbol{a}})$,
9. $1 \cdot \vec{\boldsymbol{a}} = \vec{\boldsymbol{a}}$.

Mnohé ďalšie príklady v matematike nás vedú k definícii algebraickej štruktúry $\boldsymbol{V}$ majúcej také vlastnosti, ako množina vektorov v rovine z príkladu 1.1. Presnejšie: $\boldsymbol{V}$ je množina objektov, ktoré vzhľadom na sčítanie tvoria komutatívnu grupu (platia pravidlá 1. - 5.) a kde je definované násobenie prvkov množiny $\boldsymbol{V}$ prvkami nejakého poľa F (v príklade 1.1 to bolo pole reálnych čísel) tak, že platia pravidlá 6. - 9. Ďalším príkladom takejto štruktúry je napr. množina komplexných čísel C. Štruktúra $(C, +)$ je komutatívna grupa (operácia „+" je obyčajné sčítanie komplexných čísel). Ďalej pre každé komplexné číslo $\boldsymbol{\alpha} \in C$ a každé reálne číslo $s \in R$ je definovaný súčin $s \cdot \boldsymbol{\alpha} \in C$, pričom zrejme platia pravidlá 6. – 9. Štruktúru takýchto vlastností nazývame „vektorový priestor". Vyslovíme presnú definíciu vektorového priestoru.

Definícia 1.1. Nech F je pole*) a $(\boldsymbol{V}, +)$ komutatívna grupa. Definujme operáciu „·" takto: $\cdot : F \times \boldsymbol{V} \to \boldsymbol{V}$. To znamená, že „·" je zobrazenie, ktoré každej dvojici $(s, \boldsymbol{\alpha}) \in F \times \boldsymbol{V}$ priraďuje prvok $\boldsymbol{\beta} \in \boldsymbol{V}$ t.j. $(s, \boldsymbol{\alpha}) \mapsto \boldsymbol{\beta}$, čo zapisujeme $s \cdot \boldsymbol{\alpha} = \boldsymbol{\beta}$.

Množinu $\boldsymbol{V}$ nazývame *vektorovým priestorom nad poľom* F, ak sú splnené nasledujúce podmienky (axiómy):

$$(V_1) \qquad s \cdot (\boldsymbol{\alpha} + \boldsymbol{\beta}) = s \cdot \boldsymbol{\alpha} + s \cdot \boldsymbol{\beta},$$

$$(V_2) \qquad (s + t) \cdot \boldsymbol{\alpha} = s \cdot \boldsymbol{\alpha} + t \cdot \boldsymbol{\alpha},$$

$$(V_3) \qquad (s \cdot t) \cdot \boldsymbol{\alpha} = s \cdot (t \cdot \boldsymbol{\alpha}),$$

$$(V_4) \qquad 1 \cdot \boldsymbol{\alpha} = \boldsymbol{\alpha},$$

kde $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}, s, t \in F$.**)

Ak chceme zdôrazniť, že vektorový priestor $\boldsymbol{V}$ je nad poľom F, miesto $\boldsymbol{V}$ často píšeme $\boldsymbol{V}(F)$. Prvky množiny $\boldsymbol{V}$ nazývame *vektory*. Budeme ich označovať $\boldsymbol{\alpha}, \boldsymbol{\beta}, \cdots$, alebo $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}}, \cdots$. Nulový prvok grupy $\boldsymbol{V}$ (nulový vektor) označíme $\vec{\boldsymbol{0}}$. (Rozlišujte medzi nulovým vektorom $\vec{\boldsymbol{0}}$ a nulovým prvkom poľa F, ktorý označíme 0.) Prvky poľa F nazývame *skaláry*. Operáciu „+" grupy $(\boldsymbol{V}, +)$ nazývame *vnútornou operáciou* a operáciu „·" (násobenie vektora skalárom) *vonkajšou operáciou* vektorového priestoru V. Súčin $s \cdot \boldsymbol{\alpha}$ nazývame *skalárny násobok vektora* $\boldsymbol{\alpha}$ (bodku spravidla vynecháme: $s\boldsymbol{\alpha}$). Ak F je pole reálnych čísel R, vektorový priestor $\boldsymbol{V}$ nazývame

---

*) Nulový prvok poľa F budeme v tejto kapitole volať nula, označovať 0, jednotkový prvok poľa F budeme označovať 1.

**) Nespôsobí nedorozumenie, že dve rôzne operácie sčítania definované v grupe $(\boldsymbol{V}, +)$ a v poli F označujeme tým istým znakom „+". Analogicky označujeme rovnakým znakom „·" operáciu násobenia v poli F i násobenie vektora prvkami poľa F.

reálny vektorový priestor. Dva doposiaľ uvedené vektorové priestory (množina posunutí v rovine a množina komplexných čísel) sú reálne vektorové priestory. Uvedieme ďalšie príklady vektorových priestorov.

Príklad 1.2. Každé pole $(F, +, \cdot)$ je vektorovým priestorom nad F. Prvky poľa F sú vektory i skaláry. Operácia „+" je sčítanie vektorov, operácia „·" je násobenie vektora skalárom.

Príklad 1.3. Podobne ako v príklade 1.1 môžeme uvažovať množinu $\boldsymbol{V}$ všetkých posunutí v trojrozmernom priestore, resp. množinu všetkých orientovaných úsečiek vychádzajúcich z pevne zvoleného bodu*) tohoto priestoru, pričom operácie sčítania vektorov a násobenie reálnym číslom sú definované ako v príklade 1.1. Množina $\boldsymbol{V}$ je tiež reálny vektorový priestor.

Príklad 1.4 (dôležitý). Nech F je pole. Množina všetkých n-tíc prvkov poľa F označíme $\boldsymbol{V}_n(F)$. Nech $\boldsymbol{\alpha} = (x_1, x_2, \ldots, x_n)$, $\boldsymbol{\beta} = (y_1, y_2, \ldots, y_n)$ sú ľubovoľné n-tice z $\boldsymbol{V}_n(F)$. Ich súčet definujeme takto:

$$\boldsymbol{\alpha} + \boldsymbol{\beta} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

Nech $s \in F$. Skalárny násobok $s \cdot \boldsymbol{\alpha}$ definujeme nasledovne:

$$s\boldsymbol{\alpha} = (sx_1, sx_2, \ldots, sx_n).$$

Je možné ľahko skontrolovať (cvičenie 1.1 c), že $\boldsymbol{V}_n(F)$ je vektorový priestor. Nulovým vektorom je zrejme $\vec{\mathbf{0}} = (0, 0 \ldots, 0)$. Poznamenajme ešte, že prvky $x_1, x_2, \ldots, x_n$ nazývame zložky vektora $\boldsymbol{\alpha}$, ako aj to, že $\boldsymbol{\alpha} = \boldsymbol{\beta}$ práve vtedy, keď $x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$. Pozanamenajme ďalej, že priestor $\boldsymbol{V}_n(F)$ nazývame *aritmetickým priestorom nad F*.

Príklad 1.5. Uvažujme o vektorovom priestore $\boldsymbol{V}_3(Z_2)$ (špeciálny prípad $\boldsymbol{V}_n(F)$). Čitateľovi pripomenieme, že Z_2 je pole zvyškových tried modulo 2, t.j. $Z_2 = \{\overline{0}, \overline{1}\}$. Vidíme, že vektorový priestor $\boldsymbol{V}_3(Z_2)$ má 8 prvkov:
$\boldsymbol{V}_3(Z_2) = \{(\overline{0}, \overline{0}, \overline{0}), (\overline{0}, \overline{0}, \overline{1}), (\overline{0}, \overline{1}, \overline{0}), (\overline{0}, \overline{1}, \overline{1}), (\overline{1}, \overline{0}, \overline{0}), (\overline{1}, \overline{0}, \overline{1}), (\overline{1}, \overline{1}, 0), (\overline{1}, \overline{1}, \overline{1})\}$.
Keďže pole Z_2 má len 2 prvky, pre skalárny násobok vektora napr. $\boldsymbol{\alpha} = (\overline{1}, \overline{0}, \overline{1})$ máme len 2 možnosti: $\overline{0} \cdot (\overline{1}, \overline{0}, \overline{1}) = (\overline{0}, \overline{0}, \overline{0})$ a $\overline{1} \cdot (\overline{1}, \overline{0}, \overline{1}) = (\overline{1}, \overline{0}, \overline{1})$.

Príklad 1.6. Nech $\boldsymbol{W}$ je množina všetkých reálnych spojitých funkcií definovaných na intervale $\langle 0, 1\rangle$. Ak $f, g \in \boldsymbol{W}$, súčet $f + g$ je funkcia h (píšeme $h = f + g$), pre ktorú platí $h(x) = f(x) + g(x)$ pre všetky $x \in \langle 0, 1\rangle$. Zrejme aj $f + g \in \boldsymbol{W}$ a $(\boldsymbol{W}, +)$ je komutatívna grupa. Analogicky definujeme skalárny násobok $s \cdot f$, kde $s \in R$. Vidieť, že $\boldsymbol{W}$ je reálny vektorový priestor.

Príklad 1.7. Nech F je pole. Zobrazenie $f : \boldsymbol{V}_n(F) \to F$ sa nazýva lineárnou formou nad $\boldsymbol{V}_n(F)$, ak je dané vzťahom

$$f(\boldsymbol{\alpha}) = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n, \tag{1.1}$$

*) Tento bod obyčajne volíme za počiatok súradnicového systému.

kde $\boldsymbol{\alpha} = (x_1, x_2, \ldots, x_n) \in \boldsymbol{V}_n(F)$ a $a_1, a_2, \ldots, a_n \in F$. Množinu všetkých lineárnych foriem nad $V_n(F)$ budeme označovať $\boldsymbol{L}_n(F)$. Nech $f, g \in \boldsymbol{L}_n(F)$, kde forma f je daná vzťahom (1.1) a forma g vzťahom $g(\boldsymbol{\alpha}) = b_1x_1 + b_2x_2 + \cdots + b_nx_n$, pričom $b_1, b_2, \ldots, b_n \in F$. Súčet foriem f, g je forma h definovaná takto:

$$h(\boldsymbol{\alpha}) = f(\boldsymbol{\alpha}) + g(\boldsymbol{\alpha}) = (a_1 + b_1)x_1 + (a_2 + b_2)x_2 + \cdots + (a_n + b_n)x_n.$$

Skalárny násobok $s \cdot f$, kde $s \in F$ definujeme $sf(\boldsymbol{\alpha}) = sa_1x_1 + sa_2x_2 + \cdots + sa_nx_n$. Ľahko sa ukáže (cvičenie 1.1.e), že $\boldsymbol{L}_n(F)$ je vektorový priestor nad F (nulový vektor priestoru je $0(\boldsymbol{\alpha}) = 0x_1 + 0x_2 + \cdots + 0x_n$, opačný vektor k vektoru (1.1) je $-f(\boldsymbol{\alpha}) = -a_1x_1 + (-a_2)x_2 + \cdots + (-a_n)x_n$).

Nasledujúci príklad bude pre nás obzvlášť dôležitý.

Príklad 1.8. Nech $f \in \boldsymbol{L}_n(F)$ je lineárna forma nad $\boldsymbol{V}_n(F)$ daná vzťahom (1.1). Výrokovú funkciu φ definovanú vzťahom

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = a, \tag{1.2}$$

kde a je pevne zvolený prvok poľa F, nazývame lineárna rovnica s n neznámymi nad F. Výroková funkcia φ teda každému vektoru $\boldsymbol{\alpha} = (x_1, x_2, \ldots, x_n) \in \boldsymbol{V}_n(F)$ priraďuje výrok: „hodnota formy f pre vektor $\boldsymbol{\alpha}$ je a“. Množinu všetkých lineárnych rovníc s n neznámymi nad F budeme označovať $\boldsymbol{R}_n(F)$. Nech φ je rovnica definovaná vzťahom (1.2) a ψ nasledovná rovnica:

$$b_1x_1 + b_2x_2 + \cdots + b_nx_n = b.$$

Súčet rovníc $\varphi + \psi$ je rovnica definovaná takto:

$$(a_1 + b_1)x_1 + (a_2 + b_2)x_2 + \cdots + (a_n + b_n)x_n = a + b.$$

Skalárny násobok rovnice (1.2) $s \cdot \varphi$ je

$$sa_1x_1 + sa_2x_2 + \cdots + sa_nx_n = sa,$$

kde $s \in F$. Podobne ako v predchádzajúcom príklade ľahko skontrolujeme (cvičenie 1.1 f), že $\boldsymbol{R}_n(F)$ je vektorový priestor nad F (nulový vektor je rovnica $0 \cdot x_1 + 0 \cdot x_2 + \cdots + 0 \cdot x_n = 0$).

Veta 1.1. *Nech $\boldsymbol{\alpha}$ je ľubovoľný vektor priestoru $\boldsymbol{V}(F)$ a s ľubovoľný skalár (prvok poľa F). Potom platí*

$$0 \cdot \boldsymbol{\alpha} = \vec{\mathbf{0}}; \qquad s \cdot \vec{\mathbf{0}} = \vec{\mathbf{0}}. \tag{1.3}$$

Dôkaz. a) $0 \cdot \boldsymbol{\alpha} = (0 + 0) \cdot \boldsymbol{\alpha} = 0 \cdot \boldsymbol{\alpha} + 0 \cdot \boldsymbol{\alpha}$. Ďalej $0 \cdot \boldsymbol{\alpha} = 0 \cdot \boldsymbol{\alpha} + \vec{\mathbf{0}}$. Porovnaním máme $0 \cdot \boldsymbol{\alpha} + 0 \cdot \boldsymbol{\alpha} = 0 \cdot \boldsymbol{\alpha} + \vec{\mathbf{0}}$, odkiaľ (známa vlastnosť grupy) vyplýva $0 \cdot \boldsymbol{\alpha} = \vec{\mathbf{0}}$.

b) Dôkaz vzťahu $s \cdot \vec{\mathbf{0}} = \vec{\mathbf{0}}$ ponecháme na čitateľa. □

Cvičenia

1.1. Dokážte podrobne, že nasledujúce množiny sú vektorové priestory:

a) množina komplexných čísel C nad poľom reálnych čísel R,
b) množina $\boldsymbol{V}$ všetkých posunutí v trojrozmernom priestore z príkladu 1.3,
c) množina $\boldsymbol{V}_n(F)$ z príkladu 1.4
d) množina $\boldsymbol{W}$ všetkých reálnych funkcií na $\langle 0,1\rangle$ z príkladu 1.6,
e) množinu $\boldsymbol{L}_n(F)$ všetkých lineárnych foriem nad $\boldsymbol{V}_n(F)$ (príklad 1.7),
f) množina $\boldsymbol{R}_n(F)$ všetkých lineárnych rovníc o n neznámych nad F (príklad 1.8).

1.2. Nech $f \in \boldsymbol{L}_n(F)$ je lineárna forma nad $\boldsymbol{V}_n(F)$ definovaná vzťahom (1.1). Nech ďalej $s \in F$ a $\boldsymbol{\alpha} = (x_1, x_2, \dots, x_n)$, $\boldsymbol{\beta} = (y_1, y_2, \dots, y_n)$ sú dva vektory z $\boldsymbol{V}_n(F)$. Dokážte, že platia tzv. podmienky linearity

$$f(\boldsymbol{\alpha}+\boldsymbol{\beta}) = f(\boldsymbol{\alpha}) + f(\boldsymbol{\beta}), \tag{1.4}$$

$$f(s\boldsymbol{\alpha}) = s \cdot f(\boldsymbol{\alpha}). \tag{1.5}$$

1.3. Napíšte všetky prvky vektorového priestoru $\boldsymbol{V}_3(Z_3)$.

1.4. Koľko prvkov má vektorový priestor $\boldsymbol{V}_n(Z_p)$, kde $n \geqq 1$ je prirodzené číslo a p je prvočíslo?

1.5. Dokážte:

a) $(-1)\boldsymbol{\alpha}$ je opačný prvok k vektoru $\boldsymbol{\alpha}$,
b) ak $s\boldsymbol{\alpha} = \vec{\mathbf{0}}$, tak $s = 0$ alebo $\boldsymbol{\alpha} = \vec{\mathbf{0}}$,
c) ak $s\boldsymbol{\alpha} = t\boldsymbol{\alpha}$, tak $s = t$ alebo $\boldsymbol{\alpha} = \vec{\mathbf{0}}$,
d) ak $s\boldsymbol{\alpha} = s\boldsymbol{\beta}$, tak $s = 0$ alebo $\boldsymbol{\alpha} = \boldsymbol{\beta}$.

1.6. Funkcia $f : F \to F$ definovaná vzťahom

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

kde $a_n, a_{n-1}, \dots, a_0 \in F$ a $n \geqq 0$ je celé číslo, sa nazýva polynóm jednej premennej n-tého stupňa s koeficientami z poľa F. Sčítanie polynómov a skalárny násobok polynómu sa definuje ako v príklade 1.6.

a) Zistite, či množina všetkých polynómov jednej premennej s racionálnymi koeficientami je vektorovým priestorom nad poľom racionálnych čísel Q?
b) Tvorí množina všetkých polynómov stupňa 4 s reálnymi koeficientami reálny vektorový priestor?
c) Tvorí vektorový priestor množina $\boldsymbol{P}_n(R)$ všetkých polynómov jednej premennej s reálnymi koeficientami stupňa najviac $n-1$?

1.7. Určte reálne čísla x, y, z tak, aby platilo $\boldsymbol{\alpha} = \boldsymbol{\beta}$, keď $\boldsymbol{\alpha} = (1,2,3)$ a $\boldsymbol{\beta} = (x+y+z, x-y-z, x+2x+3z)$, pričom $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}_3(R)$.

1.8. Určte lineárnu formu $\boldsymbol{L}_2(R)$, ktorá vo vektore $\boldsymbol{\alpha} = (-1,3)$ nadobúda hodnotu 7 a vo vektore $\boldsymbol{\beta} = (1,1)$ hodnotu 5.

§ 2. Lineárna závislosť a nezávislosť

Definícia 2.1. Nech $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n \in \boldsymbol{V}(F)$ sú vektory a $s_1, s_2, \dots, s_n \in F$ sú skaláry. Vektor

$$\boldsymbol{\alpha} = s_1\boldsymbol{\alpha}_1 + s_2\boldsymbol{\alpha}_2 + \cdots + s_n\boldsymbol{\alpha}_n$$

sa nazýva *lineárna kombinácia* vektorov $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$. Skaláry $s_1, s_2, \dots, s_n$ sú koeficienty lineárnej kombinácie.

Príklad 2.1. Pre vektory $\boldsymbol{\alpha} = (1, 2, 3)$, $\boldsymbol{\beta} = (-1, 4, -2)$, $\boldsymbol{\gamma} = (5, -8, 12)$ z $V_3(R)$ platí $\boldsymbol{\gamma} = 2\boldsymbol{\alpha} + (-3)\boldsymbol{\beta}$, t.j. $\boldsymbol{\gamma}$ je lineárnou kombináciou vektorov $\boldsymbol{\alpha}, \boldsymbol{\beta}$.

Definícia 2.2. Hovoríme, že vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$ vektorového priestoru $\boldsymbol{V}(F)$ sú *lineárne závislé*, ak existuje n-tica skalárov $c_1, c_2, \dots, c_n \in F$ takých, že aspoň pre jeden index i platí $c_i \neq 0$ a že je splnená nasledujúca rovnosť

$$c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \cdots + c_n\boldsymbol{\alpha}_n = \vec{\mathbf{0}}. \tag{2.1}$$

Vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$ sú *lineárne nezávislé,* ak z rovnosti (2.1) vyplýva $c_1 = c_2 = \cdots = c_n = 0$.

Príklad 2.2. Vektory $\boldsymbol{\alpha} = (3, -1)$, $\boldsymbol{\beta} = (-1, 1)$, $\boldsymbol{\gamma} = \left(-1, \frac{5}{3}\right)$ vektorového priestoru $\boldsymbol{V}_2(R)$ sú lineárne závislé, lebo $\frac{2}{3}\boldsymbol{\alpha} + 4\boldsymbol{\beta} - 2\boldsymbol{\gamma} = \vec{\mathbf{0}}$. Vektory $\mu = (1, 2)$, $\nu = (3, 1)$ sú lineárne nezávislé. Skutočne, z rovnice $c_1(1, 2) + c_2(3, 1) = (0, 0)$ vyplýva $c_1 = c_2 = 0$. (Odôvodnite podrobne.)

Veta 2.1. *Vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n \in \boldsymbol{V}(F)$ sú lineárne závislé práve vtedy, keď aspoň jeden z nich je lineárnou kombináciou ostatných.*

Dôkaz. I. Ak pre nejaké i platí

$$\boldsymbol{\alpha}_i = b_1\boldsymbol{\alpha}_1 + b_2\boldsymbol{\alpha}_2 + \cdots + b_{i-1}\boldsymbol{\alpha}_{i-1} + b_{i+1}\boldsymbol{\alpha}_{i+1} + \cdots + b_n\boldsymbol{\alpha}_n,$$

tak

$$b_1\boldsymbol{\alpha}_1 + b_2\boldsymbol{\alpha}_2 + \cdots + b_{i-1}\boldsymbol{\alpha}_{i-1} + (-1)\boldsymbol{\alpha}_i + b_{i+1}\boldsymbol{\alpha}_{i+1} + \cdots + b_n\boldsymbol{\alpha}_n = \vec{\mathbf{0}}.$$

Keďže $-1 \neq 0$, vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$ sú lineárne závislé.

II. Nech vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$ sú lineárne závislé, t.j. nech platí

$$c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \cdots + c_i\boldsymbol{\alpha}_i + \cdots + c_n\boldsymbol{\alpha}_n = \vec{\mathbf{0}},$$

pričom napr. $c_i \neq 0$. Potom je

$$\boldsymbol{\alpha}_i = -\frac{c_1}{c_i}\boldsymbol{\alpha}_1 - \frac{c_2}{c_i}\boldsymbol{\alpha}_2 - \cdots - \frac{c_{i-1}}{c_i}\boldsymbol{\alpha}_{i-1} - \frac{c_{i+1}}{c_i}\boldsymbol{\alpha}_{i+1} - \cdots - \frac{c_n}{c_i}\boldsymbol{\alpha}_n,$$

t.j. $\boldsymbol{\alpha}_i$ je lineárna kombinácia ostatných vektorov. □

Poznámka 2.1. Nad konečným poľom vektor $\boldsymbol{\alpha}_i$ uvedieme v tvare

$$\boldsymbol{\alpha}_i = -c_1c_i^{-1}\boldsymbol{\alpha}_1 - c_2c_i^{-1}\boldsymbol{\alpha}_2 - \cdots - c_{i-1}c_i^{-1}\boldsymbol{\alpha}_{i-1} - c_{i+1}c_i^{-1}\boldsymbol{\alpha}_{i+1} - \cdots - c_nc_i^{-1}\boldsymbol{\alpha}_n.$$

Pozri poznámku 4.4 v kapitole 1.

Veta 2.2. *Nenulové vektory* $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n \in \boldsymbol{V}(F)$ *sú lineárne závislé práve vtedy, keď jeden z nich je lineárnou kombináciou predchádzajúcich.*

Veta 2.3. *Nech* A, B *sú neprázdne konečné podmnožiny vektorového priestoru* $\boldsymbol{V}(F)$. *Potom*

a) Ak A *je taká množina vektorov, že* $\vec{\mathbf{0}} \in A$, *tak vektory množiny* A *sú lineárne závislé.*

b) Ak vektory nejakej podmnožiny B *množiny vektorov* A *sú lineárne závislé, tak aj vektory množiny* A *sú lineárne závislé.*

c) Ak vektory množiny A *sú lineárne nezávislé, tak vektory každej jej neprázdnej podmnožiny* B *sú lineárne nezávislé.*

Dôkazy viet 2.2 a 2.3 ponecháme na čitateľa (cvičenie 2.1).

Príklad 2.3. Zistíme, či vektory $\boldsymbol{\alpha} = (1,1)$, $\boldsymbol{\beta} = (-1,3)$, $\boldsymbol{\gamma} = (2,-3) \in V_2(R)$ sú lineárne závislé. Ak áno, vyjadríme jeden z nich ako lineárnu kombináciu ostatných.

Máme vlastne zistiť, či existuje nenulová trojica reálnych čísel c_1, c_2, c_3, taká, že platí $c_1\boldsymbol{\alpha} + c_2\boldsymbol{\beta} + c_3\boldsymbol{\gamma} = \vec{\mathbf{0}}$, t.j.

$$c_1(1,1) + c_2(-1,3) + c_3(2,-3) = (0,0)$$

alebo (po sčítaní vektorov na ľavej strane)

$$(c_1 - c_2 + 2c_3,\ c_1 + 3c_2 - 3c_3) = (0,0),$$

odkiaľ vyplýva

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

Sústava má zrejme aj nenulové riešenie. Ak zvolíme napr. $c_3 = 1$ dostaneme sústavu

$$\begin{aligned} c_1 - c_2 &= -2, \\ c_1 + 3c_2 &= 3, \end{aligned}$$

po vyriešení ktorej dostaneme $c_1 = -\frac{3}{4}$, $c_2 = \frac{5}{4}$. Skutočne $-\frac{3}{4}\boldsymbol{\alpha} + \frac{5}{4}\boldsymbol{\beta} + \boldsymbol{\gamma} = -\frac{3}{4}(1,\,1) + \frac{5}{4}(-1,\,3) + (2,\,-3) = \left(-\frac{3}{4},\,-\frac{3}{4}\right) + \left(-\frac{5}{4},\,\frac{15}{4}\right) + \left(\frac{8}{4},\,-\frac{12}{4}\right) = (0,0)$. Vidíme, že vektory α, β, γ sú lineárne závislé. Vyjadríme jeden z nich napr. γ ako lineárnu kombináciu zvyšných dvoch: $\boldsymbol{\gamma} = \frac{3}{4}\boldsymbol{\alpha} - \frac{5}{4}\boldsymbol{\beta}$.

Cvičenie

2.1. Dokážte vety 2.2 a 2.3.

2.2. Dokážte:

a) Jednoprvková množina $\{\boldsymbol{\alpha}\}$, kde $\boldsymbol{\alpha} \in \boldsymbol{V}(F)$ pričom $\boldsymbol{\alpha} \neq \vec{\mathbf{0}}$ tvorí lineárne nezávislý systém vektorov.

b) Dva vektory $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}(F)$ sú lineárne závislé práve vtedy, keď jeden je skalárnym násobkom druhého (takéto vektory sa niekedy nazývajú kolineárne).

2.3. Zistite, či nasledujúce systémy vektorov sú lineárne závislé:

a) $(2,3),(4,5) \in \boldsymbol{V}_2(R)$
b) $(1,2,3),(3,-1,2),(4,-6,2) \in \boldsymbol{V}_3(R)$
c) $(1,2,3),(3,-1,2),(5,3,8) \in \boldsymbol{V}_3(R)$

2.4. Ľubovoľné tri vektory $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma} \in \boldsymbol{V}_2(R)$ sú lineárne závislé. Dokážte to.

2.5. Zistite, či nasledujúce systémy vektorov vektorového priestoru všetkých polynómov s reálnymi koeficientami stupňa menšieho ako 5 (cvičenie 1.6c) sú lineárne nezávislé.

a) $1, x^2, x^4$,
b) $1, (x-1)^2, (x-1)^2$,
c) $1, (x-1)^2, 3x^2-6x$.

2.6. Nech $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}$ sú tri lineárne nezávislé vektory vektorového priestoru $\boldsymbol{V}$. Zistite, či nasledujúce systémy vektorov sú lineárne nezávislé.

a) $\boldsymbol{\alpha},\ \boldsymbol{\alpha}+\boldsymbol{\beta},\ \boldsymbol{\alpha}+\boldsymbol{\gamma}$
b) $\boldsymbol{\alpha}+\boldsymbol{\beta},\ \boldsymbol{\alpha}+\boldsymbol{\beta},\ \boldsymbol{\alpha}+\boldsymbol{\gamma},\ \boldsymbol{\alpha}-\boldsymbol{\gamma}$
c) $\boldsymbol{\alpha}+\boldsymbol{\beta},\ \boldsymbol{\alpha}+\boldsymbol{\gamma},\ \boldsymbol{\beta}+\boldsymbol{\gamma}$
d) $3\boldsymbol{\alpha},\ 2\boldsymbol{\beta},\ \boldsymbol{\gamma}$
e) $\boldsymbol{\alpha}+\boldsymbol{\beta}+\boldsymbol{\gamma},\ \boldsymbol{\alpha}+\boldsymbol{\beta}-\boldsymbol{\gamma},\ \boldsymbol{\alpha}-\boldsymbol{\beta}+\boldsymbol{\gamma}$
f) $\boldsymbol{\alpha}+2\boldsymbol{\beta}-\boldsymbol{\gamma},\ 2\boldsymbol{\alpha}-4\boldsymbol{\beta}+5\boldsymbol{\gamma},\ \boldsymbol{\alpha}-\boldsymbol{\beta}+4\boldsymbol{\gamma}$.

2.7. Nech vektory $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}$ sú lineárne závislé a $\boldsymbol{\alpha}$ nie je lineárnou kombináciou vektorov $\boldsymbol{\beta}$ a $\boldsymbol{\gamma}$. Potom jeden z vektorov $\boldsymbol{\beta},\boldsymbol{\gamma}$ je skalárnym násobkom druhého. Dokážte to.

2.8. Nech $(x,y),(u,v)$ sú dva vektory z $\boldsymbol{V}_2(F)$. Dokážte, že tieto vektory sú lineárne závislé vtedy a len vtedy, keď $xv = yu$.

2.9. Dokážte, že platí nasledovný „silnejší“ variant vety 2.2:
Vektory $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\ldots,\boldsymbol{\alpha}_n$, kde $\boldsymbol{\alpha}_1 \neq \vec{\mathbf{0}}$ sú lineárne závislé práve vtedy, keď jeden z nich je lineárnou kombináciou predchádzajúcich.

§ 3. Podpriestory

Definícia 3.1. Nech $\boldsymbol{V}(F)$ je vektorový priestor nad poľom F. Nech $\boldsymbol{P} \subseteq \boldsymbol{V}$ je taká neprázdna podmnožina priestoru $\boldsymbol{V}$, že $\boldsymbol{P}$ tvorí vektorový priestor nad F vzhľadom na operácie sčítanie vektorov a násobenie vektora skalárom definované vo $\boldsymbol{V}(F)$. Potom $\boldsymbol{P}$ nazývame *podpriestorom* priestoru $\boldsymbol{V}$. Označujeme $\boldsymbol{P} \subseteq\subseteq \boldsymbol{V}$.

Zrejme $\{\vec{\mathbf{0}}\}$, $\boldsymbol{V}(F)$ sú podpriestory priestoru $\boldsymbol{V}(F)$. Nazývame ich *triviálne*. Podpriestory, ktoré nie sú triviálne voláme *vlastné*.

Veta 3.1. *Neprázdna podmnožina $\boldsymbol{P}$ vektorového priestoru $\boldsymbol{V}(F)$ je podpriestorom priestoru $\boldsymbol{V}(F)$ práve vtedy, keď sú splnené nasledujúce podmienky:*
1. Pre ľubovoľné dva vektory $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{P}$ platí $\boldsymbol{\alpha} + \boldsymbol{\beta} \in \boldsymbol{P}$.
2. Pre ľubovoľný vektor $\boldsymbol{\alpha} \in \boldsymbol{P}$ a ľubovoľný skalár $s \in F$ platí $s\boldsymbol{\alpha} \in \boldsymbol{P}$.

Dôkaz. I. Ak $\boldsymbol{P}$ je podpriestor priestoru $\boldsymbol{V}$, podmienky 1. a 2. sú zrejme splnené.

II. Nech $\boldsymbol{P}$ je neprázdna podmnožina priestoru $\boldsymbol{V}$, pre ktorú platia podmienky 1. a 2. Dokážeme, že $(\boldsymbol{P}, +)$ je podgrupa komutatívnej grupy $(\boldsymbol{V}, +)$. Z podmienky 1. vyplýva, že operácia „+" je v množine $\boldsymbol{P}$ uzavretá. Asociovanosť a komutatívnosť sčítania vyplýva z týchto vlastností v grupe $(\boldsymbol{V}, +)$. Zostáva dokázať, že $\vec{\mathbf{0}} \in \boldsymbol{P}$ a že každému prvku $\boldsymbol{\alpha} \in \boldsymbol{P}$ existuje v množine $\boldsymbol{P}$ opačný prvok. To však dostaneme okamžite takto: Z podmienky 2. : $(-1)\boldsymbol{\alpha} \in \boldsymbol{P}$, z podmienky 1.: $1 \cdot \boldsymbol{\alpha} + (-1)\boldsymbol{\alpha} = (1 + (-1))\boldsymbol{\alpha} = 0 \cdot \boldsymbol{\alpha} = \vec{\mathbf{0}} \in \boldsymbol{P}$. Vidíme, že $-\boldsymbol{\alpha} = (-1)\boldsymbol{\alpha}$.

Nakoniec z podmienky 2. vyplýva, že na $\boldsymbol{P}$ je definovaný aj skalárny násobok vektora. Ľahko sa presvedčíme, že v množine $\boldsymbol{P}$ platia aj vlastnosti (V_1) – (V_4). □

Príklad 3.1. Nech $\boldsymbol{P} = \{(x_1, x_2, x_3);\ (x_1, x_2, x_3) \in \boldsymbol{V}_3(R), x_3 = 0\}$. Dokážeme, že $\boldsymbol{P}$ je podpriestor priestoru $\boldsymbol{V}_3(R)$.

Skutočne $(x_1, x_2, 0) + (y_1, y_2, 0) = (x_1 + y_1, x_2 + y_2, 0) \in \boldsymbol{P}$, podobne $c(x_1, x_2, 0) = (cx_1, cx_2, 0) \in \boldsymbol{P}$, kde $c \in R$ t.j. podmienky 1. a 2. z vety 3.1 sú splnené.

Príklad 3.2. Množina $\boldsymbol{P}$ všetkých polynómov s reálnymi koeficientami definovaných na intervale $\langle 0, 1\rangle$ (pozri cvičenie 1.6) je podmnožina vektorového priestoru $\boldsymbol{W}$ všetkých reálnych spojitých funkcií definovaných na intervale $\langle 0, 1\rangle$ (pozri príklad 1.6). Čitateľ sa ľahko presvedčí o tom, že $\boldsymbol{P}$ je podpriestor priestoru $\boldsymbol{W}$.

Veta 3.2. *Nech $\boldsymbol{P}, \boldsymbol{S}$ sú podpriestory vektorového priestoru $\boldsymbol{V}(F)$. Potom aj $\boldsymbol{P} \cap \boldsymbol{S}$ je podpriestor priestoru $\boldsymbol{V}(F)$.*

Dôkaz. Dokážeme, že v $\boldsymbol{P} \cap \boldsymbol{S}$ platia obe podmienky vety 3.1. Skutočne ak $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{P} \cap \boldsymbol{S}$, tak $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{P}$ a zároveň $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{S}$. Keďže $\boldsymbol{P}, \boldsymbol{S}$ sú podpriestory, tak $\boldsymbol{\alpha} + \boldsymbol{\beta} \in \boldsymbol{P}$ a zároveň $\boldsymbol{\alpha} + \boldsymbol{\beta} \in \boldsymbol{S}$, odkiaľ vyplýva $\boldsymbol{\alpha} + \boldsymbol{\beta} \in \boldsymbol{P} \cap \boldsymbol{S}$. Druhá podmienka sa dokáže podobne. □

Poznámka 3.1. Vetu 3.2 možno zovšeobecniť takto: *Nech $\mathcal{P}$ je ľubovoľný systém podpriestorov priestoru $\boldsymbol{V}(F)$. Potom aj $\bigcap_{\boldsymbol{P} \in \mathcal{P}} \boldsymbol{P}$ je podpriestor priestoru $\boldsymbol{V}(F)$.* (Dokážte to v cvičení 3.4).

Podľa vety 3.2 a poznámky 3.1 môžeme vysloviť nasledujúcu definíciu.

Definícia 3.2. Nech je daná podmnožina M priestoru $\boldsymbol{V}(F)$ Nech $\mathcal{P}$ je systém všetkých tých podpriestorov priestoru $\boldsymbol{V}(F)$, z ktorých každý obsahuje množinu M. (Zrejme $\mathcal{P} \neq \emptyset$, lebo $\boldsymbol{V}(F) \in \mathcal{P}$.) Teda

$$\mathcal{P} = \{\boldsymbol{P};\ \boldsymbol{P} \subseteq\subseteq \boldsymbol{V}(F) \quad \text{a zároveň} \quad \boldsymbol{P} \supseteq M\}$$

Podpriestor, ktorý je prienikom všetkých podpriestorov systému $\mathcal{P}$ označíme $[M]$ a nazveme ho podpriestorom *generovaným (vytvoreným)* množinou M, niekedy tiež *lineárnym obalom* množiny M. Vektory množiny M sa nazývajú *generátory* podpriestoru $[M]$.

Poznámka 3.2. Ak M je konečná množina, t.j.

$$M = \{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k\}, \tag{3.1}$$

tak podpriestor $[M]$ označujeme aj $[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k]$.

Veta 3.3. *Podpriestor $[M]$ vektorového priestoru $\boldsymbol{V}(F)$ generovaný vektormi množiny M má tieto dve vlastnosti:*

(i) $[M] \supseteq M$,
(ii) *Ak* $\boldsymbol{P} \subseteq\subseteq \boldsymbol{V}(F)$ *pričom* $\boldsymbol{P} \supseteq M$, *tak* $\boldsymbol{P} \supseteq [M]$.

Podpriestor $[M]$ je vlastnosťami (i) a (ii) jednoznačne určený.

Dôkaz. Dôkaz oboch vlastností vykonáme triviálnou aplikáciou definície 3.2. Aby sme dokázali jednoznačnosť, predpokladajme, že existujú dva podpriestory $[M]_1 \neq [M]_2$ majúce vlastnosti (i) a (ii). Potom z (ii) vyplýva ako $[M]_1 \supseteq [M]_2$, tak aj $[M]_1 \subseteq [M]_2$, čiže $[M]_1 = [M]_2$. Daný spor ukončuje dôkaz. □

Veta 3.3 nám hovorí, že $[M]$ je v istom zmysle najmenší podpriestor obsahujúci množinu M.

Označme písmenom $\boldsymbol{K}$ množinu všetkých lineárnych kombinácií vektorov množiny M, kde $M \subseteq \boldsymbol{V}(F)$ je neprázdna množina. Teda

$$\boldsymbol{K} = \{c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \dots + c_k\boldsymbol{\alpha}_k;\ c_i \in F,\ \boldsymbol{\alpha}_i \in M,\ k \in N\}. \tag{3.2}$$

Pomocou vety 3.1 rýchlo overíme, že $\boldsymbol{K}$ je podpriestor priestoru $\boldsymbol{V}(F)$. Naozaj: súčet dvoch lineárnych kombinácií vektorov množiny M je zase lineárna kombinácia z množiny $\boldsymbol{K}$. Podobne aj skalárny násobok lineárnej kombinácie z množiny $\boldsymbol{K}$ je opäť prvok množiny $\boldsymbol{K}$. Dokážeme viac:

Veta 3.4. *Nech M je neprázdna podmnožina vektorového priestoru $\boldsymbol{V}(F)$. Potom $[M] = \boldsymbol{K}$.*

Dôkaz. Keďže podpriestor $\boldsymbol{K}$ obsahuje všetky vektory množiny M (to znamená $\boldsymbol{K} \supseteq M$), podľa tvrdenia (ii) vety 3.3 je $\boldsymbol{K} \supseteq [M]$. Na druhej strane podpriestor $[M]$ zrejme obsahuje aj všetky lineárne kombinácie vektorov množiny M. Preto $\boldsymbol{K} \subseteq [M]$. □

Poznámka 3.3. Čitateľ si rýchlo overí, že ak $M = \emptyset$, tak $[M] = [\emptyset] = \{\vec{\mathbf{0}}\}$. Naozaj: Prázdna množina je podmnožinou každého podpriestoru vektorového priestoru $\boldsymbol{V}(F)$, preto systém $\mathcal{P}$ z definície 3.2 obsahuje všetky podpriestory priestoru $\boldsymbol{V}(F)$. Ich prienik je zrejme triviálny podpriestor $\{\vec{\mathbf{0}}\}$.

Príklad 3.3. Nech $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}_3(R)$, $\boldsymbol{\alpha} = (0,1,1)$, $\boldsymbol{\beta} \in (1,1,0)$ a $x, y \in R$. Majme na mysli podpriestor generovaný vektormi $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}_3(R)$. Počítame $x\boldsymbol{\alpha} + y\boldsymbol{\beta} = x(0,1,1) + y(1,1,0) = (y, x+y, x)$. Vidíme, že podpriestor $[\boldsymbol{\alpha}, \boldsymbol{\beta}]$ priestoru $\boldsymbol{V}_3(R)$ generovaný vektormi množiny $M = \{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ pozostáva z takých vektorov, ktorých druhá zložka sa rovná súčtu prvej a tretej.

Príklad 3.4. Nech $\boldsymbol{\varepsilon}_1 = (1,0,0)$, $\boldsymbol{\varepsilon}_2 = (0,1,0)$, $\boldsymbol{\varepsilon}_3 = (0,0,1)$ sú vektory priestoru $\boldsymbol{V}_3(R)$. Ukážeme, že $[\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_3] = \boldsymbol{V}_3(R)$.

Skutočne. Nech $\boldsymbol{\alpha} = (x_1, x_2, x_3)$ je ľubovoľný vektor priestoru $\boldsymbol{V}_3(R)$. Zrejme je $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + x_3\boldsymbol{\varepsilon}_3$ a tak vektory $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_3$ generujú celý priestor $\boldsymbol{V}_3(R)$.

Aby sme sa mohli lepšie vyjadrovať, zavedieme pojem *sústava vektorov.* Pod týmto pojmom budeme rozumieť vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots \boldsymbol{\alpha}_k \in \boldsymbol{V}(F)$, z ktorých niektoré sa môžu aj opakovať. Danú sústavu označíme takto: $\mathcal{S} = [\![\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k]\!]$. Tak napríklad z množiny vektorov $S = \{\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}\}$ môžeme vytvoriť sústavu $\mathcal{S} = [\![\boldsymbol{\alpha}, \boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\gamma}]\!]$ alebo sústavu $\mathcal{T} = [\![\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\beta}, \boldsymbol{\gamma}]\!]$. Naopak, z danej sústavy môžeme vytvoriť množinu tak, že do nej zahrnieme každý prvok sústavy len raz. Je jasné, že každá množina vektorov je aj sústavou vektorov, ale nie každá sústava je aj množinou. Nech S je množina vektorov a $\mathcal{S}$ je sústava vektorov z nej vytvorená. Podobne ako vyššie označíme množinu všetkých lineárnych kombinácií vektorov množiny S znakom $\boldsymbol{K}$. Ak teraz vytvoríme množinu všetkých lineárnych kombinácií vektorov sústavy $\mathcal{S}$, dostaneme tú istú množinu $\boldsymbol{K}$ (overte to!). Preto môžeme hovoriť o podpriestore $[\mathcal{S}]$ generovanom sústavou $\mathcal{S}$.

Definícia 3.3. Nech $\mathcal{S}, \mathcal{T}$ sú dve sústavy vektorov vektorového priestoru $\boldsymbol{V}(F)$. Sústavy $\mathcal{S}, \mathcal{T}$ nazveme *lineárne ekvivalentné*, keď obe generujú ten istý podpriestor priestoru $V(F)$, t.j. keď $[\mathcal{S}] = [\mathcal{T}]$.

Veľmi často budeme používať nasledujúcu vetu.

Veta 3.5. *Nech je daná nasledujúca sústava $\mathcal{S}$ vektorov vektorového priestoru $\boldsymbol{V}(F)$:*

$$\mathcal{S} = [\![\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_i, \dots, \boldsymbol{\alpha}_j, \dots, \boldsymbol{\alpha}_k]\!].$$

Nech sústava $\mathcal{T}$ vznikne zo sústavy $\mathcal{S}$ jednou z týchto operácií:

(a) *Zámenou poradia vektorov sústavy $\mathcal{S}$.*

(b) *Zámenou vektora $\boldsymbol{\alpha}_i$ za vektor $s\boldsymbol{\alpha}_i$, kde $0 \neq s \in F$.*

(c) *Zámenou vektora $\boldsymbol{\alpha}_i$ za vektor $\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_j$.*

Potom platí $[\mathcal{S}] = [\mathcal{T}]$, t.j. sústavy $\mathcal{S}$ a $\mathcal{T}$ sú lineárne ekvivalentné.

Poznámka 3.4. Operácie (a), (b), (c) nazývame *elementárne operácie.*

Dôkaz vety 3.5. Dokážeme, $[\mathcal{S}] \subseteq [\mathcal{T}]$. Nech $\boldsymbol{\alpha}$ je ľubovoľný vektor z $[\mathcal{S}]$. Potom $\boldsymbol{\alpha}$ možno vyjadriť ako lineárnu kombináciu vektorov sústavy $\mathcal{S}$, t.j.

$$\boldsymbol{\alpha} = c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \dots + c_i\boldsymbol{\alpha}_i + \dots + c_j\boldsymbol{\alpha}_j + \dots + c_n\boldsymbol{\alpha}_n.$$

Dokážeme, že $\boldsymbol{\alpha}$ možno vyjadriť ako lineárnu kombináciu vektorov sústavy $\mathcal{T}$. V prípade (a) je to zrejmé. V prípade (b) máme:

$$\begin{aligned}\boldsymbol{\alpha} &= c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \dots + c_i\boldsymbol{\alpha}_i + \dots + c_j\boldsymbol{\alpha}_j + \dots + c_n\boldsymbol{\alpha}_n = \\ &= c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \dots + \tfrac{c_i}{s}(s\boldsymbol{\alpha}_i) + \dots + c_j\boldsymbol{\alpha}_j + \dots + c_n\boldsymbol{\alpha}_n.\end{aligned}$$

V prípade (c):

$$\begin{aligned}\boldsymbol{\alpha} &= c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \dots + c_i\boldsymbol{\alpha}_i + \dots + c_j\boldsymbol{\alpha}_j + \dots + c_n\boldsymbol{\alpha}_n = \\ &= c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \dots + c_i(\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_j) + \dots + (c_j - c_i)\boldsymbol{\alpha}_j + \dots + c_n\boldsymbol{\alpha}_n.\end{aligned}$$

Dôkaz inklúzie $[\mathcal{T}] \subseteq [\mathcal{S}]$ ponecháme na čitateľa. □

Veta 3.6(Steinitzova veta o výmene). *Nech vektory*

$$\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n \tag{3.3}$$

generujú priestor $\boldsymbol{V}(F)$, *t.j.* $\boldsymbol{V}(F) = [\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n]$. *Nech ďalej*

$$\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_k \tag{3.4}$$

je k *lineárne nezávislých vektorov tohto priestoru. Potom* $k \leqq n$ *a pri vhodnom prečíslovaní vektorov (3.3) platí*

$$[\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_k, \boldsymbol{\alpha}_{k+1}, \dots, \boldsymbol{\alpha}_n] = \boldsymbol{V}(F).$$

Dôkaz. Vetu dokážeme matematickou indukciou podľa k.

I. Nech $k = 1$. Potom

$$\boldsymbol{\beta}_1 = c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \dots + c_n\boldsymbol{\alpha}_n. \tag{a}$$

Vektor $\boldsymbol{\beta}_1 \neq \vec{\mathbf{0}}$ (inak by množina vektorov (3.4) bola lineárne závislá), tak aspoň jeden z koeficientov c_i v (a) je rôzny od nuly. Prečíslovaním vektorov (3.3) je možné dosiahnuť, aby $c_1 \neq 0$. Potom z (a) vypočítame

$$\boldsymbol{\alpha}_1 = d_1\boldsymbol{\beta}_1 + d_2\boldsymbol{\alpha}_2 + d_3\boldsymbol{\alpha}_3 + \dots + d_n\boldsymbol{\alpha}_n, \tag{b}$$

odkiaľ vyplýva

$$[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] \subseteq [\boldsymbol{\beta}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3, \dots, \boldsymbol{\alpha}_n].$$

Skutočne, ak nejaký vektor je možné vyjadriť ako lineárnu kombináciu vektorov $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$, tak (vzhľadom na (b)) je možné vyjadriť ho aj ako lineárnu kombináciu vektorov $\boldsymbol{\beta}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$. Podobne z (a) vyplýva $[\boldsymbol{\beta}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] \subseteq$ $\subseteq [\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots \boldsymbol{\alpha}_n]$. Máme tak $[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] = [\boldsymbol{\beta}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] = \boldsymbol{V}$ a veta pre $k = 1$ platí. (Zrejme $1 = k \leqq n$.)

II. Predpokladajme, že veta je správna pre $k-1$, t.j. platí $k - 1 \leqq n$ a

$$[\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_{k-1}, \boldsymbol{\alpha}_k, \boldsymbol{\alpha}_{k+1}, \dots, \boldsymbol{\alpha}_n] = [\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] = \boldsymbol{V}(F). \tag{c}$$

Potom máme

$$\boldsymbol{\beta}_k = c'_1\boldsymbol{\beta}_1 + c'_2\boldsymbol{\beta}_2 + \dots + c'_{k-1}\boldsymbol{\beta}_{k-1} + c'_k\boldsymbol{\alpha}_k + \dots + c'_n\boldsymbol{\alpha}_n. \tag{d}$$

Ak by sa v (d) všetky skaláry $c'_k, c'_{k+1}, \dots, c'_n$ rovnali nule, vektor $\boldsymbol{\beta}_k$ by bol lineárnou kombináciou vektorov $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_{k-1}$ čo nie je, lebo vektory (3.4) sú lineárne nezávislé. Vhodným prečíslovaním vektorov $\boldsymbol{\alpha}_k, \dots, \boldsymbol{\alpha}_n$ možno dosiahnuť, že $c'_k \neq 0$. Potom z (d) vypočítame $\boldsymbol{\alpha}_k$, t.j.

$$\boldsymbol{\alpha}_k = d'_1\boldsymbol{\beta}_1 + d'_2\boldsymbol{\beta}_2 + \dots + d'_k\boldsymbol{\beta}_k + d'_{k+1}\boldsymbol{\alpha}_{k+1} + \dots + d'_n\boldsymbol{\alpha}_n. \tag{e}$$

Z (d) vyplýva $[\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_k, \boldsymbol{\alpha}_{k+1}, \dots, \boldsymbol{\alpha}_n] \subseteq [\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_{k-1}, \boldsymbol{\alpha}_k, \dots, \boldsymbol{\alpha}_n]$, z (e) máme $[\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_{k-1}, \boldsymbol{\alpha}_k, \dots, \boldsymbol{\alpha}_n] \subseteq [\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_k, \boldsymbol{\alpha}_{k+1}, \dots, \boldsymbol{\alpha}_n]$ a tak vzhľadom na (c) je $[\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_k, \boldsymbol{\alpha}_{k+1}, \dots, \boldsymbol{\alpha}_n] = [\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_{k-1}, \boldsymbol{\alpha}_k, \dots, \boldsymbol{\alpha}_n] = [\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] = \boldsymbol{V}(F)$.

Zostáva dokázať $k \leqq n$. To dokážeme takto: Podľa indukčného predpokladu je $k-1 \leqq n$. Ak by $k-1 = n$, mali by sme $[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] = [\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_{k-1}] = \boldsymbol{V}$. To by znamenalo $\boldsymbol{\beta}_k = d_1\boldsymbol{\beta}_1 + d_2\boldsymbol{\beta}_2 + \cdots + d_{k-1}\boldsymbol{\beta}_{k-1}$, čo nemôže byť, lebo vektory (3.4) sú lineárne nezávislé. Teda $k-1 < n$, odkiaľ $k \leqq n$. □

Cvičenia

3.1. Ktoré z nasledujúcich množín vektorov priestoru $\boldsymbol{V}_3(R)$ sú podpriestormi:

$$\begin{aligned}
A &= \{(x_1, x_2, x_3);\quad x_1 = 0\},\\
B &= \{(x_1, x_2, x_3);\quad x_2 = 3\},\\
C &= \{(x_1, x_2, x_3);\quad 4x_1 - x_2 = 0\},\\
D &= \{(x_1, x_2, x_3);\quad ax_1 + bx_2 + cx_3 = 0,\quad a, b, c \in R\},\\
E &= \{(x_1, x_2, x_3);\quad ax_1 + bx_2 + cx_3 = d,\quad a, b, c, d \in R\},
\end{aligned}$$

Aký je geometrický význam množín A, B, C, D, E?

3.2. Nájdite všetky podpriestory priestoru $\boldsymbol{V}_3(Z_2)$.

3.3. Dokážte, že nasledujúce dve podmnožiny vektorového priestoru $\boldsymbol{P}$ všetkých polynómov jednej premennej s racionálnymi koeficientami sú podpriestormi priestoru $\boldsymbol{P}$.

$$\begin{aligned}
\boldsymbol{P}_3 &= \{ax^3 + bx^2 + cx + d;\quad a, b, c, d \in Q\},\\
\boldsymbol{P}_3' &= \{ax^3 + bx^2 + cx;\quad a, b, c \in Q\}.
\end{aligned}$$

V akom vzťahu sú podpriestory $\boldsymbol{P}_3$ a $\boldsymbol{P}_3'$?

3.4. Nech $\mathcal{P}$ je ľubovoľný systém podpriestorov priestoru $\boldsymbol{V}(F)$. Potom aj $\bigcap_{\boldsymbol{P} \in \mathcal{P}} \boldsymbol{P}$ je podpriestor priestoru $\boldsymbol{V}(F)$. Dokážte to.

3.5. Nájdite kontrapríklad, ktorý dokazuje, že nasledujúce tvrdenie je nepravdivé: Nech $\boldsymbol{P}_1, \boldsymbol{P}_2, \dots, \boldsymbol{P}_k$ sú podpriestory priestoru $\boldsymbol{V}$. Potom aj $\boldsymbol{P}_1 \cup \boldsymbol{P}_2 \cup \cdots \cup \boldsymbol{P}_k$ je podpriestor priestoru $\boldsymbol{V}$.

3.6. Dokážte , že ľubovoľné štyri vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3, \boldsymbol{\alpha}_4 \in \boldsymbol{V}_3(R)$ sú lineárne závislé. (Použite Steinitzovu vetu.)

3.7. Nájdite podpriestor priestoru $\boldsymbol{V}_3(R)$, ktorý generujú vektory $\boldsymbol{\alpha}_1 = (1, 2, 3)$, $\boldsymbol{\alpha}_2 = (-1, 0, 4)$. Dokážte, že množina všetkých vektorov tohto podpriestoru je $\{(x, y, z) \in \boldsymbol{V}_3(R);\ 8x - 7y + 2z = 0\}$.

3.8. Aké podpriestory priestoru $\boldsymbol{P}_3$ (pozri cv. 3.3) generujú nasledujúce množiny vektorov ($\boldsymbol{P}_3$ je vektorový priestor polynómov nad poľom Q).

$A = \{3x, 7\}$ $\quad E = \{x^3 + x^2, 3x^2, x, 7\}$,
$B = \{3x^2, 7\}$, $\quad F = \{(x-1)^3, (x-1)^2, x-1, 1\}$,
$C = \{x^3, 2x^2\}$, $\quad G = \{2x^2\}$,
$D = \{x^3 + x^2, x\}$, $\quad H = \{x^2, 1\}$.

Ktoré z uvedených množín generujú ten istý podpriestor? Ktoré generujú celý priestor $\boldsymbol{P}_3$?

3.9. Dokážte, že nasledujúce dvojice A_i, B_i množín vektorov priestoru $\boldsymbol{V}_3(R)$ sú lineárne ekvivalentné.

$A_1 = \{(1,0,0)\}$, $\quad B_1 = \{(3,0,0),\ (5,0,0)\}$
$A_2 = \{(1,0,0),(0,1,0)\}$, $\quad B_2 = \{(1,2,0),(2,3,0)\}$
$A_3 = \{(1,-2,3),(4,-3,2),(5,1,0)\}$, $\quad B_3 = \{(8,-6,4),(5,1,0),(6,-1,3)\}$.

3.10. Nech $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\delta}$ sú vektory vektorového priestoru $\boldsymbol{V}(F)$. Ak je sústava vektorov $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}$ lineárne nezávislá, tak $\boldsymbol{\delta} \in [\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}]$ práve vtedy, keď sústava $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\delta}$ je lineárne závislá. Dokážte to.

3.11. Nech $\boldsymbol{S}$ je podpriestor priestoru $\boldsymbol{V}$ a $M, N \subseteq \boldsymbol{V}$. Potom

a) Ak $M \subseteq N$, tak $[M] \subseteq [N]$
b) $[\boldsymbol{S}] = \boldsymbol{S}$
c) Ak $M \subseteq N$ a $N \subseteq [M]$, tak $[M] = [N]$.

Dokážte to.

§ 4. Dimenzia a báza

Definícia 4.1. Hovoríme, že vektorový priestor $\boldsymbol{V}$ má *konečnú dimenziu* n, ak v ňom existuje n lineárne nezávislých vektorov a neexistuje v ňom väčší počet (t.j. väčší ako n) lineárne nezávislých vektorov. Označujeme $d(\boldsymbol{V}) = n$. Priestor dimenzie n nazývame *n-rozmerný vektorový priestor*.

Definícia 4.2. Ľubovoľnú množinu $B = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n\}$ n lineárne nezávislých vektorov n-rozmerného priestoru $\boldsymbol{V}$ nazývame *bázou* priestoru $\boldsymbol{V}$.

Príklad 4.1. Ukážeme, že aritmetický priestor $\boldsymbol{V}_n(F)$ má dimenziu n. Predovšetkým existuje v ňom n lineárne nezávislých vektorov. Sú to vektory

$$\begin{aligned}
\boldsymbol{\varepsilon}_1 &= (1,0,0,\ldots,0),\\
\boldsymbol{\varepsilon}_2 &= (0,1,0,\ldots,0),\\
\boldsymbol{\varepsilon}_3 &= (0,0,1,\ldots,0),\\
&\vdots\\
\boldsymbol{\varepsilon}_n &= (0,0,0,\ldots,1).
\end{aligned}$$

Skutočne: Žiadny vektor $\boldsymbol{\varepsilon}_i$ nemôže byť lineárnou kombináciou ostatných, lebo jednotkový prvok (poľa F), ktorý je na i-tom mieste nemožno dostať žiadnou lineárnou kombináciou nulových prvkov. Dokážeme, že

$$\boldsymbol{V}_n(F) = [\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n].$$

Skutočne, ak $\boldsymbol{\alpha} = (x_1, x_2, \dots, x_n)$ je ľubovoľný vektor priestoru $\boldsymbol{V}_n(F)$, tak ho môžeme vyjadriť v tvare $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n$.

Nech $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_m$ je ľubovoľná m-tica lineárne nezávislých vektorov priestoru $\boldsymbol{V}_n(F)$. Podľa Steinitzovej vety (veta 3.6) je $m \leqq n$, t.j. v priestore $\boldsymbol{V}_n(F)$ neexistuje väčší počet lineárne nezávislých vektorov ako n. Vektory $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n$ teda tvoria bázu priestoru $\boldsymbol{V}_n(F)$.

Poznámka 4.1. Bázu $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ z príkladu 4.1 nazývame kanonická báza priestoru $\boldsymbol{V}_n(F)$.

Definícia 4.3. Hovoríme, že priestor $\boldsymbol{V}$ je *nekonečnej dimenzie*, ak v priestore $\boldsymbol{V}$ existuje ľubovoľný počet lineárne nezávislých vektorov.

Príklad 4.2. Vektorový priestor spojitých reálnych funkcií definovaných na intervale $\langle 0, 1\rangle$ má nekonečnú dimenziu, lebo

$$f_1(x) = x,\ f_2(x) = x^2,\ f_3(x) = x^3, \dots$$

tvorí nekonečnú množinu lineárne nezávislých vektorov tohoto priestoru.

Veta 4.1. *Nech $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ je báza priestoru $\boldsymbol{V}$. Každý vektor $\boldsymbol{\alpha} \in V$ je možné vyjadriť ako lineárnu kombináciu vektorov bázy. Toto vyjadrenie je jednoznačné.*

Dôkaz. V n-rozmernom priestore $\boldsymbol{V}$ vektory $\boldsymbol{\alpha}, \boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n$ sú lineárne závislé (lebo ich je $n+1$), t.j. platí

$$c_0\boldsymbol{\alpha} + c_1\boldsymbol{\varepsilon}_1 + c_2\boldsymbol{\varepsilon}_2 + \dots + c_n\boldsymbol{\varepsilon}_n = \vec{\mathbf{0}}, \tag{4.1}$$

pričom aspoň jedno $c_i (i = 0, 1, \dots, n)$ je rôzne od nuly. Ak by $c_0 = 0$, vektory bázy $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n$ by boli lineárne závislé. Preto $c_0 \neq 0$. Z (4,1) máme

$$\boldsymbol{\alpha} = -\frac{c_1}{c_0}\boldsymbol{\varepsilon}_1 - \frac{c_2}{c_0}\boldsymbol{\varepsilon}_2 - \dots - \frac{c_n}{c_0}\boldsymbol{\varepsilon}_n,$$

alebo (označiac $-\frac{c_i}{c_0} = x_i$)

$$\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n, \tag{4.2}$$

čo dokazuje prvé tvrdenie vety. Zostáva dokázať, že vyjadrenie (4.2) je jednoznačné. Nepriamo. Nech platí (4.2) a okrem toho $\boldsymbol{\alpha} = x_1'\boldsymbol{\varepsilon}_1 + x_2'\boldsymbol{\varepsilon}_2 + \dots + x_n'\boldsymbol{\varepsilon}_n$. Potom máme $x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n = x_1'\boldsymbol{\varepsilon}_1 + x_2'\boldsymbol{\varepsilon}_2 + \dots + x_n'\boldsymbol{\varepsilon}_n$, z čoho vyplýva $(x_1 - x_1')\boldsymbol{\varepsilon}_1 + (x_2 - x_2')\boldsymbol{\varepsilon}_2 + \dots + (x_n - x_n')\boldsymbol{\varepsilon}_n = \vec{\mathbf{0}}$. Keďže vektory $\boldsymbol{\varepsilon}_1\boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n$ sú lineárne nezávislé, platí $x_1 - x_1' = 0$, $x_2 - x_2' = 0, \dots, x_n - x_n' = 0$, to znamená $x_1 = x_1', x_2 = x_2', \dots, x_n = x_2'$, čo dokazuje druhé tvrdenie vety. □

Definícia 4.4. Nech $B = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n\}$ je báza vektorového priestoru $\boldsymbol{V}(F)$ a $\boldsymbol{\alpha} \in \boldsymbol{V}$ je ľubovoľný vektor tohto priestoru. Potom skaláry $x_1, x_2, \ldots, x_n \in F$ z jednoznačného vyjadrenia (4.2) nazývame súradnice vektora $\boldsymbol{\alpha}$ vzhľadom na bázu B. Niekedy hovoríme aj o vektore súradníc $(x_1, x_2, \ldots, x_n)$.

Poznámka 4.2. Z vety 4.1 vyplýva, že vektor je jednoznačne určený svojimi súradnicami. Z viet 3.6 a 4.1 dostávame nasledujúce dôsledky.

Dôsledok 1. *Vektory bázy* $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n$ *generujú celý vektorový priestor* $\boldsymbol{V}$, *t.j.* $[\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n] = \boldsymbol{V}$.

Dôkaz prenecháme čitateľovi.

Dôsledok 2. *Nech lineárne nezávislé vektory* $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k$ *generujú podpriestor* $\boldsymbol{P}$ *priestoru* $\boldsymbol{V}$. *Potom* $d(\boldsymbol{P}) = k$.

Dôkaz. Podľa predpokladu $\boldsymbol{P}$ obsahuje k lineárne nezávislých vektorov $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k$. Nech $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_m$ sú ľubovoľné lineárne nezávislé vektory podpriestoru $\boldsymbol{P}$. Nakoľko $[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k] = \boldsymbol{P}$, zo Steinitzovej vety máme $m \leqq k$. To znamená $d(\boldsymbol{P}) = k$. $\square$

Dôsledok 3. *Nech lineárne nezávislé vektory* $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k$ *n-rozmerného vektorového priestoru generujú celý priestor* $\boldsymbol{V}$. *Potom* $k = n$, *t.j. vektory* $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k$ *tvoria bázu priestoru* $\boldsymbol{V}$.

Dôkaz vyplýva z dôsledku 2.

Poznámka 4.3. Dôsledok 3 nám umožňuje definovať bázu ako množinu lineárne nezávislých vektorov, ktorá generuje celý vektorový priestor.

Dôsledok 4. *Nech* n *vektorov* $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_n$ *n-rozmerného vektorového priestoru generuje celý priestor* $\boldsymbol{V}$. *Potom vektory* $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_n$ *sú lineárne nezávislé, t.j. tvoria bázu priestoru* $\boldsymbol{V}$.

Dôkaz. Ak by vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_n$ boli lineárne závislé, tak by sa jeden z nich, napríklad $\boldsymbol{\alpha}_n$ dal vyjadriť ako lineárna kombinácia ostatných. Potom by ale $[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_{n-1}] = \boldsymbol{V}$. Ak $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n$ je báza priestoru $\boldsymbol{V}$, tak (nakoľko $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n$ sú lineárne nezávislé vektory) podľa Steinitzovej vety je $n - 1 \geqq n$, čo je nemožné. $\square$

Príklad 4.3. V priestore $\boldsymbol{V}_2(R)$ vektory $\boldsymbol{\varepsilon}_1 = (1, 0)$, $\boldsymbol{\varepsilon}_2 = (1, 1)$ tvoria bázu. Skutočne z príkladu 4.1 vyplýva, že $d(V_2(R)) = 2$ a vektory $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2$ sú lineárne nezávislé, lebo z rovnice $c_1(1, 0) + c_2(1, 1) = (0, 0)$ vyplýva $c_1 = c_2 = 0$. Nech $\boldsymbol{\alpha} = (a, b)$ je ľubovoľný vektor priestoru $\boldsymbol{V}(R)$. Vypočítajme jeho súradnice x_1, x_2 vzhľadom na bázu $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2\}$. Podľa vety 4.1 máme $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2$, t.j. $(a, b) = x_1(1, 0) + x_2(1, 1)$, čiže $(a, b) = (x_1 + x_2, x_2)$, odkiaľ $x_1 = a - b$, $x_2 = b$.

Príklad 4.4. Uvažujme vektorový priestor $\boldsymbol{P}_n(R)$ všetkých polynómov s reálnymi koeficientami stupňa najviac $n - 1$. Tento priestor je n-rozmerný. Naozaj polynómy

$$f_1(x) = 1,\ f_2(x) = x,\ f_3(x) = x^2, \ldots, f_n(x) = x^{n-1} \tag{4.3}$$

sú lineárne nezávislé a ľubovoľný polynóm možno vyjadriť ako ich lineárnu kombináciu. Podľa poznámky 4.3 polynómy (4.3) tvoria bázu priestoru $\boldsymbol{P}_n(R)$ a koeficienty ľubovoľného polynómu z priestoru $\boldsymbol{P}_n(R)$ sú súradnice tohoto polynómu vzhľadom na bázu (4.3). Napr. polynóm $f(x) = 3 - 2x + 4x^2$ má v priestore $\boldsymbol{P}_5(R)$ súradnice $x_1 = 3,\ \ x_2 = -2,\ \ x_3 = 4,\ \ x_4 = x_5 = 0.$

Ak v priestore $\boldsymbol{P}_n(R)$ zvolíme inú bázu

$$B = \{1, x-1, (x-1)^2, \dots, (x-1)^{n-1}\}$$

z Taylorovho vzorca*) vyplýva, že súradnice polynómu $f(x) \in \boldsymbol{P}_n(R)$ sú

$$x_1 = f(1),\ x_2 = \frac{f'(1)}{1!},\ x_3 = \frac{f''(1)}{2!}, \dots, x_n = \frac{f^{(n-1)}(1)}{(n-1)!}.$$

Príklad 4.5. Vypočítajme súradnice vektora $\boldsymbol{\alpha} = (x_1, x_2, \dots, x_n) \in \boldsymbol{V}_n(F)$ vzhľadom na bázu $B = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$, kde vektory $\boldsymbol{\varepsilon}_i$ boli definované v príklade 4.1.

Vidieť, že platí

$$(x_1, x_2, \dots, x_n) = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_n\boldsymbol{\varepsilon}_n,$$

čo znamená, že súradnice vektora $\boldsymbol{\alpha}$ vzhľadom na bázu B sa rovnajú jeho zložkám. Napr. vo $\boldsymbol{V}_3(R)$ príslušné vyjadrenie vektora $\boldsymbol{\alpha} = (3, -7, 2)$ je $\boldsymbol{\alpha} = 3\boldsymbol{\varepsilon}_1 - 7\boldsymbol{\varepsilon}_2 + 2\boldsymbol{\varepsilon}_3$.

Príklad 4.6. Vypočítajme súradnice x_1, x_2, x_3 vektora $\boldsymbol{\alpha} = (3, -7, 2) \in \boldsymbol{V}_3(R)$ vzhľadom na bázu $\{\eta_1, \eta_2, \eta_3\}$, kde $\eta_1 = (1, 0, 0)$, $\eta_2 = (1, 1, 0)$, $\eta_3 = (1, 1, 1)$. Píšeme $(3, -7, 2) = x_1(1, 0, 0) + x_2(1, 1, 0) + x_3(1, 1, 1)$ odkiaľ

$$\begin{aligned} x_1 + x_2 + x_3 &= 3 \\ x_2 + x_3 &= -7 \\ x_3 &= 2. \end{aligned}$$

Riešením sústavy dostaneme $x_1 = 10$, $x_2 = -9$, $x_3 = 2$.

Príklad 4.7. Vo vektorovom priestore $\boldsymbol{L}_3(R)$ lineárnych foriem nad $\boldsymbol{V}_3(R)$ (príklad 1.6) formu $f(\boldsymbol{\alpha}) = 3x_1 - 7x_2 + 2x_3$, kde $\boldsymbol{\alpha} = (x_1, x_2, x_3)$ vyjadríme ako lineárnu kombináciu foriem $f_1(\boldsymbol{\alpha}) = x_1,\ f_2(x) = x_1 + x_2,\ f_3(\boldsymbol{\alpha}) = x_1 + x_2 + x_3$. Čitateľ rýchlo overí, že množina $\{f_1(\boldsymbol{\alpha}),\ f_2(\boldsymbol{\alpha}),\ f_3(\boldsymbol{\alpha})\}$ je báza priestoru $\boldsymbol{L}_3(R)$. Postupom ako v príklade 4.6 nájdeme, že $f(\boldsymbol{\alpha}) = 10f_1(\boldsymbol{\alpha}) - 9f_2(\boldsymbol{\alpha}) + 2f_3(\boldsymbol{\alpha})$.

Príklad 4.8. Vypočítame dimenziu podpriestoru $\boldsymbol{P}$ vektorového priestoru $\boldsymbol{V}_3(R)$ definovaného takto:

$$\boldsymbol{P} = \{(x_1, x_2, x_3); 2x_1 + 3x_2 - 4x_3 = 0;\ \text{kde } x_1, x_2, x_3 \in R\}.$$

Hneď vidieť, že vektory $(3, -2, 0)$, $(1, 2, 2) \in \boldsymbol{P}$ sú lineárne nezávislé. Ale ľubovoľný vektor $(x_1, x_2, x_3) \in \boldsymbol{P}$ môžeme vyjadriť ako ich lineárnu kombináciu. Skutočne $(x_1 + x_2 - \frac{3}{2}x_3)(3, -2, 0) + \frac{1}{2}x_3(1, 2, 2) = (3x_1 + 3x_2 - 4x_3, -2x_1 - 2x_2 + {}$ ${}+4x_3, x_3) = (x_1 + (2x_1 + 3x_2 - 4x_3), x_2 - (2x_1 + 3x_2 - 4x_3), x_3) = (x_1, x_2, x_3)$. To znamená $\boldsymbol{P} = [(3, -2, 0), (1, 2, 2)]$ a teda $d(\boldsymbol{P}) = 2$.

Čitateľovi odporúčame, aby si rozmyslel, akým spôsobom možno vypočítať koeficienty $x_1 + x_2 - \frac{3}{2}x_3$ resp. $\frac{1}{2}x_3$.

*) Ak čitateľ Taylorov vzorec ešte nepozná, môže túto časť príkladu vynechať.

Veta 4.2. *Nech $\boldsymbol{V}$ je n-rozmerný vektorový priestor a $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k$ sú lineárne nezávislé vektory tohto priestoru. Potom $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k\} \subseteq B$, kde B je nejaká báza priestoru $\boldsymbol{V}$.*

Poznámka 4.4. Inými slovami veta 4.2 hovorí, že ľubovoľnú množinu lineárne nezávislých vektorov n-rozmerného vektorového priestoru možno doplniť na bázu tohoto priestoru.

Dôkaz vety 4.2. Nech $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n\}$ je nejaká báza priestoru $\boldsymbol{V}$. Keďže (dôsledok 1 za vetou 4.1) $[\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n] = \boldsymbol{V}$ a vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k$ sú lineárne nezávislé, podľa Steinitzovej vety je $k \leqq n$ a pri vhodnom prečíslovaní vektorov $\boldsymbol{\varepsilon}_i$ je $[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k, \boldsymbol{\varepsilon}_{k+1}, \ldots, \boldsymbol{\varepsilon}_n] = \boldsymbol{V}$. Podľa dôsledku 4 za vetou 4.1 vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k, \boldsymbol{\varepsilon}_{k+1}, \ldots, \boldsymbol{\varepsilon}_n$ tvoria bázu priestoru $\boldsymbol{V}$. □

Z cvičenia 3.5 vieme, že ak $\boldsymbol{P}$ a $\boldsymbol{S}$ sú podpriestory priestoru $\boldsymbol{V}$, tak $\boldsymbol{P} \cup \boldsymbol{S}$ nemusí byť podpriestor priestoru $\boldsymbol{V}$. Môžeme však vytvoriť podpriestor $[\boldsymbol{P} \cup \boldsymbol{S}]$.

Definícia 4.5. Nech $\boldsymbol{P}$ a $\boldsymbol{S}$ sú podpriestory priestoru $\boldsymbol{V}(F)$. Podpriestor $[\boldsymbol{P} \cup \boldsymbol{S}]$ nazývame spojením podpriestorov $\boldsymbol{P}$ a $\boldsymbol{S}$. Označíme $[\boldsymbol{P} \cup \boldsymbol{S}] = \boldsymbol{P} \vee \boldsymbol{S}$.

Veta 4.3. *Nech $\boldsymbol{P}, \boldsymbol{S}$ sú podpriestory priestoru $\boldsymbol{V}$. Potom*

$$\boldsymbol{P} \vee \boldsymbol{S} = \{\boldsymbol{\alpha} + \boldsymbol{\beta};\ \boldsymbol{\alpha} \in \boldsymbol{P},\ \boldsymbol{\beta} \in \boldsymbol{S}\}.$$

Dôkaz. Podľa vety 3.4 (vzhľadom na definíciu 4.5) je

$$\boldsymbol{P} \vee \boldsymbol{S} = \{c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \cdots + c_n\boldsymbol{\alpha}_n;\ n \in N,\ \boldsymbol{\alpha}_i \in \boldsymbol{P} \cup \boldsymbol{S},\ c_i \in F\}.$$

Bez ujmy na všeobecnosti môžeme predpokladať, že $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k \in \boldsymbol{P}$ a $\boldsymbol{\alpha}_{k+1}, \ldots, \boldsymbol{\alpha}_n \in \boldsymbol{S}$. Vidíme, že každý vektor $\boldsymbol{\gamma} \in \boldsymbol{P} \vee \boldsymbol{S}$ je možné písať vo forme $\boldsymbol{\gamma} = (c_1\boldsymbol{\alpha}_1 + \cdots + c_n\boldsymbol{\alpha}_k) + (c_{k+1}\boldsymbol{\alpha}_{k+1} + \cdots + c_n\boldsymbol{\alpha}_n) = \boldsymbol{\alpha} + \boldsymbol{\beta}$, kde $\boldsymbol{\alpha} \in \boldsymbol{P}$, $\boldsymbol{\beta} \in \boldsymbol{S}$. □

Poznámka 4.5. V niektorej literatúre sa spojenie podpriestorov $\boldsymbol{P} \vee \boldsymbol{S}$ nazýva lineárny súčet podpriestorov $\boldsymbol{P}$ a $\boldsymbol{S}$ a označuje sa $\boldsymbol{P} + \boldsymbol{S}$.

Veta 4.4. *Nech $\boldsymbol{P}, \boldsymbol{S}$ sú podpriestory vektorového priestoru $\boldsymbol{F}(F)$ konečnej dimenzie. Potom*

$$d(\boldsymbol{P} \cap \boldsymbol{S}) + d(\boldsymbol{P} \vee \boldsymbol{S}) = d(\boldsymbol{P}) + d(\boldsymbol{S}). \tag{4.4}$$

Dôkaz. Ak $\boldsymbol{P} \subseteq \boldsymbol{S}$, tak $\boldsymbol{P} \cap \boldsymbol{S} = \boldsymbol{P}$ a $\boldsymbol{P} \vee \boldsymbol{S} = \boldsymbol{S}$ a tvrdenie vety je zrejmé. Podobne aj v prípade $\boldsymbol{S} \subseteq \boldsymbol{P}$. Nech teda $\boldsymbol{P} \nsubseteq \boldsymbol{S}$ a tiež $\boldsymbol{S} \nsubseteq \boldsymbol{P}$. Budeme rozlišovať dva prípady:

a) Nech $\boldsymbol{P} \cap \boldsymbol{S} = \{\vec{\mathbf{0}}\}$. Nech $\{\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_r\}$ a $\{\boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2, \ldots, \boldsymbol{\gamma}_t\}$ sú bázy priestorov $\boldsymbol{P}$ a $\boldsymbol{S}$. Zrejme je $[\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_r, \boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2, \ldots, \boldsymbol{\gamma}_t] = \boldsymbol{P} \vee \boldsymbol{S}$ (prečo?). Dokážeme, že vektory $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_r, \boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2, \ldots, \boldsymbol{\gamma}_t$ sú lineárne nezávislé, t.j. tvoria bázu priestoru $\boldsymbol{P} \vee \boldsymbol{S}$. Ak by boli lineárne závislé, bol by niektorý vektor $\boldsymbol{\gamma}_i$ lineárnou kombináciou predchádzajúcich (prečo?) : $\boldsymbol{\gamma}_i = b_1\boldsymbol{\beta}_1 + b_2\boldsymbol{\beta}_2 + \cdots + b_r\boldsymbol{\beta}_r + c_1\boldsymbol{\gamma}_1 + \cdots + c_{i-1}\boldsymbol{\gamma}_{i-1}$. Uvažujme vektor $\boldsymbol{\delta} = \boldsymbol{\gamma}_i - c_1\boldsymbol{\gamma}_1 - c_2\boldsymbol{\gamma}_2 - c_{i-1}\boldsymbol{\gamma}_{i-1} = b_1\boldsymbol{\beta}_1 + b_2\boldsymbol{\beta}_2 + \cdots + b_r\boldsymbol{\beta}_r$.

Zrejme $\boldsymbol{\delta} \in \boldsymbol{P}$ a súčasne $\boldsymbol{\delta} \in \boldsymbol{S}$ a teda $\boldsymbol{\delta} \in \boldsymbol{P} \cap \boldsymbol{S} = \{\vec{\mathbf{0}}\}$, čiže $\boldsymbol{\delta} = \vec{\mathbf{0}}$. Potom ale vektory $\gamma_1, \gamma_1, \dots, \gamma_i$ sú lineárne závislé, a teda aj vektory $\gamma_1, \gamma_2, \dots, \gamma_t$, čo je v spore s tým, že sú bázou priestoru $\boldsymbol{S}$. Dokázali sme $d(\boldsymbol{P} \vee \boldsymbol{S}) = r + t$. Keďže $d(\boldsymbol{P} \cap \boldsymbol{S}) = 0$, tvrdenie (4.4) platí.

b) Nech $\boldsymbol{P} \cap \boldsymbol{S} \neq \{\vec{\mathbf{0}}\}$. Nech $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k\}$ je bázou priestoru $\boldsymbol{P} \cap \boldsymbol{S}$. Nakoľko $\boldsymbol{P} \cap \boldsymbol{S} \subseteq \boldsymbol{P}$ ako aj $\boldsymbol{P} \cap \boldsymbol{S} \subseteq \boldsymbol{S}$ možno túto bázu podľa vety 4.2 doplniť na bázu $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k, \boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_l\}$ priestoru $\boldsymbol{P}$ ako aj na bázu $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k, \gamma_1, \gamma_2, \dots, \gamma_m\}$ priestoru $\boldsymbol{S}$. Máme tak $d(\boldsymbol{P}) = k + l$, $d(\boldsymbol{S}) = k + m$. Na dokončenie dôkazu stačí dokázať, že $d(\boldsymbol{P} \vee \boldsymbol{S}) = k + l + m$. Skutočne vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k, \boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_l, \gamma_1, \gamma_2, \dots, \gamma_m$ generujú podpriestor $\boldsymbol{P} \vee \boldsymbol{S}$ (čitateľ si rozmyslí, prečo). Stačí dokázať, že sú lineárne nezávislé, t.j. tvoria bázu priestoru $\boldsymbol{P} \vee \boldsymbol{S}$. Aby sme to dokázali predpokladajme opak, t.j. že tieto vektory sú lineárne závislé. Keďže vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k, \boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \dots, \boldsymbol{\beta}_l$ sú lineárne nezávislé, (tvoria bázu podpriestoru $\boldsymbol{P}$), niektorý vektor γ_j je lineárnou kombináciou predchádzajúcich vektorov (prečo?):

$$\gamma_j = a_1\boldsymbol{\alpha}_1 + \dots + a_k\boldsymbol{\alpha}_k + b_1\boldsymbol{\beta}_1 + \dots + b_l\boldsymbol{\beta}_l + c_1\gamma_1 + \dots + c_{j-1}\gamma_{j-1}.$$

Odtiaľ vidieť, že vektor

$$\boldsymbol{\delta} = \gamma_j - c_1\gamma_1 - \dots - c_{j-1}\gamma_{j-1} = a_1\boldsymbol{\alpha}_1 + \dots + a_k\boldsymbol{\alpha}_k + b_1\boldsymbol{\beta}_1 + \dots + b_l\boldsymbol{\beta}_l \tag{4.5}$$

patrí do $\boldsymbol{P} \cap \boldsymbol{S}$. Naozaj, z ľavej strany (4.5) vyplýva $\boldsymbol{\delta} \in \boldsymbol{S}$, z pravej strany $\boldsymbol{\delta} \in \boldsymbol{P}$. Teda $\boldsymbol{\delta} \in \boldsymbol{P} \cap \boldsymbol{S}$. Keďže $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k$ tvoria bázu $\boldsymbol{P} \cap \boldsymbol{S}$, je $b_1 = b_2 = \dots = b_l = 0$ a $\boldsymbol{\delta} = \gamma_j - c_1\gamma_1 - \dots - c_{j-1}\gamma_{j-1} = a_1\boldsymbol{\alpha}_1 + a_2\boldsymbol{\alpha}_2 + \dots + a_k\boldsymbol{\alpha}_k$. Z poslednej rovnice vidieť, že vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k, \gamma_1, \dots, \gamma_j$ a teda aj vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k, \gamma_1, \gamma_2, \dots, \gamma_m$ sú lineárne závislé, čo je spor s tým, že vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k, \gamma_1, \gamma_2, \dots, \gamma_m$ tvoria bázu priestoru $\boldsymbol{S}$. □

Príklad 4.9. Vypočítajme dimenziu vektorového priestoru $\boldsymbol{P} \cap \boldsymbol{S}$, keď $\boldsymbol{P}, \boldsymbol{S} \subseteq\subseteq \boldsymbol{V}_4(R)$ a $\boldsymbol{P} = [(1,1,-2,3),(1,2,3,0)]$, $\boldsymbol{S} = [(2,1,-9,9)(1,0,1,0)]$.

Riešenie. Čitateľ na prvý pohľad vidí, že $d(\boldsymbol{P}) = d(\boldsymbol{S}) = 2$. Vypočítame $d(\boldsymbol{P} \vee \boldsymbol{S})$. Je zrejmé, že podpriestor $\boldsymbol{P} \vee \boldsymbol{S} = [\boldsymbol{P} \cup \boldsymbol{S}]$ je generovaný vektormi $\boldsymbol{\alpha} = (1,1,-2,3)$ $\boldsymbol{\beta} = (1,2,3,0)$, $\gamma = (2,1,-9,9)$, $\boldsymbol{\delta} = (1,0,1,0)$. Množinu týchto 4 vektorov zameníme za množinu s nimi lineárne ekvivalentnú (veta 3.5) takto: $\boldsymbol{\alpha}' = \boldsymbol{\alpha} - \boldsymbol{\delta} = (0,1,-3,3)$, $\boldsymbol{\beta}' = \boldsymbol{\beta} - \boldsymbol{\delta} = (0,2,2,0)$, $\gamma' = \gamma - 2\boldsymbol{\delta} = (0,1,-11,9)$, $\boldsymbol{\delta}' = \boldsymbol{\delta} = (1,0,1,0)$, túto zase za množinu $\boldsymbol{\alpha}'' = \boldsymbol{\alpha}'$, $\boldsymbol{\beta}'' = \boldsymbol{\beta}' - 2\boldsymbol{\alpha}' = (0,0,8,-6)$, $\gamma'' = \gamma' - \boldsymbol{\alpha}' = (0,0,-8,6)$, $\boldsymbol{\delta}'' = \boldsymbol{\delta}'$ a túto za množinu $\boldsymbol{\alpha}''' = \boldsymbol{\alpha}''$, $\boldsymbol{\beta}''' = \boldsymbol{\beta}'' + \gamma'' = (0,0,0,0)$, $\gamma''' = \gamma''$, $\boldsymbol{\delta}''' = \boldsymbol{\delta}''$. Podľa vety 3.5 nulový vektor $\boldsymbol{\beta}'''$ môžeme vynechať a dostaneme množinu vektorov $\boldsymbol{\alpha}'''\gamma''', \boldsymbol{\delta}'''$, ktoré tiež generujú priestor $\boldsymbol{P} \vee \boldsymbol{S}$, t.j. $\boldsymbol{P} \vee \boldsymbol{S} = [(0,1,-3,3),\ (0,0,-8,6),\ (1,0,1,0)]$. Vektory $\boldsymbol{\alpha}'''$, γ''', $\boldsymbol{\delta}'''$ sú lineárne nezávislé (čitateľ ľahko skontroluje, že žiadny z nich nie je možné vyjadriť ako lineárnu kombináciu predchádzajúcich), preto $d(\boldsymbol{P} \vee \boldsymbol{S}) = 3$. Podľa vety 4.4 $d(\boldsymbol{P} \cap \boldsymbol{S}) + 3 = 2 + 2$, čiže $d(\boldsymbol{P} \cap \boldsymbol{S}) = 1$.

Poznámka 4.6. Postup použitý v príklade podrobnejšie zdôvodníme pri vypočítavaní hodnosti matice v nasledujúcej kapitole.

Definícia 4.6. Nech $\boldsymbol{P}$ a $\boldsymbol{S}$ sú podpriestory vektorového priestoru $\boldsymbol{V}(F)$ také, že $\boldsymbol{P} \cap \boldsymbol{S} = \{\vec{\mathbf{0}}\}$. Potom spojenie $\boldsymbol{P} \vee \boldsymbol{S}$ nazývame direktný súčet podpriestorov $\boldsymbol{P}, \boldsymbol{S}$ a označíme $\boldsymbol{P} + \boldsymbol{S}$.

Veta 4.5. *Nech $\boldsymbol{P}$ a $\boldsymbol{S}$ sú podpriestory vektorového priestoru $\boldsymbol{V}(F)$ také, že $\boldsymbol{P} \cap \boldsymbol{S} = \{\vec{\mathbf{0}}\}$. Potom*

(i) každý vektor $\gamma \in \boldsymbol{P} + \boldsymbol{S}$ možno jednoznačne vyjadriť v tvare $\gamma = \boldsymbol{\alpha} + \boldsymbol{\beta}$, kde $\boldsymbol{\alpha} \in \boldsymbol{P}$ a $\boldsymbol{\beta} \in \boldsymbol{S}$,

(ii) $d(\boldsymbol{P} + \boldsymbol{S}) = d(\boldsymbol{P}) + d(\boldsymbol{S})$.

Dôkaz. (i). Keďže $\boldsymbol{P}+\boldsymbol{S} = \boldsymbol{P} \vee \boldsymbol{S}$, podľa vety 4.3 každý vektor $\boldsymbol{\gamma} \in \boldsymbol{P}+\boldsymbol{S}$ možno vyjadriť v tvare $\boldsymbol{\gamma} = \boldsymbol{\alpha}+\boldsymbol{\beta}$, kde $\boldsymbol{\alpha} \in \boldsymbol{P}$, $\boldsymbol{\beta} \in \boldsymbol{S}$. Zostáva dokázať jednoznačnosť tohto vyjadrenia. Ak by $\boldsymbol{\gamma} = \boldsymbol{\alpha} + \boldsymbol{\beta}$ a tiež $\boldsymbol{\gamma} = \boldsymbol{\alpha}' + \boldsymbol{\beta}'$, kde $\boldsymbol{\alpha}, \boldsymbol{\alpha}' \in \boldsymbol{P}, \boldsymbol{\beta}, \boldsymbol{\beta}' \in \boldsymbol{S}$ pričom napr. $\boldsymbol{\alpha} \neq \boldsymbol{\alpha}'$, mali by sme $\boldsymbol{\alpha} + \boldsymbol{\beta} = \boldsymbol{\alpha}' + \boldsymbol{\beta}'$. Odtiaľ ale vyplýva $\boldsymbol{\alpha} - \boldsymbol{\alpha}' = \boldsymbol{\beta}' - \boldsymbol{\beta}$. Nakoľko $\boldsymbol{\alpha} - \boldsymbol{\alpha}' \in \boldsymbol{P}$, $\boldsymbol{\beta}' - \boldsymbol{\beta} \in \boldsymbol{S}$ vidíme, že $\boldsymbol{\alpha} - \boldsymbol{\alpha}' \in \boldsymbol{P} \cap \boldsymbol{S} = \{\vec{\mathbf{0}}\}$, t.j. $\boldsymbol{\alpha} - \boldsymbol{\alpha}' = \vec{\mathbf{0}}$, čo je spor s $\boldsymbol{\alpha} \neq \boldsymbol{\alpha}'$.

(ii) Dôkaz vyplýva z vety 4.4 a z toho, že $d(\boldsymbol{P} \cap \boldsymbol{S}) = 0$. □

Cvičenia

4.1. V priestore $\boldsymbol{V}_3(R)$ sú dané vektory $\boldsymbol{\eta}_1 = (1,0,0)$, $\boldsymbol{\eta}_2 = (1,1,0)$, $\boldsymbol{\eta}_3 = (1,1,1)$. Dokážte, že $\{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \boldsymbol{\eta}_3\}$ je báza priestoru $\boldsymbol{V}_3(R)$ a vypočítajte súradnice vektora $\boldsymbol{\alpha} = (a,b,c) \in \boldsymbol{V}_3(R)$ vzhľadom na túto bázu.

4.2. Dokážte, že vektory $\eta_1 = (1,0,0,\ldots,0)$, $\eta_2 = (1,1,0,\ldots,0), \ldots$ $\ldots, \eta_n = (1,1,1,\ldots,1)$ tvoria bázu priestoru $\boldsymbol{V}_n(R)$ a vypočítajte súradnice vektora $\boldsymbol{\alpha} = (a_1, a_2, \ldots, a_n)$ vzhľadom na túto bázu.

4.3. Zistite dimenzie všetkých podpriestorov z cvičenia 3.1.
Návod. V každom z týchto podpriestorov zvoľte množinu lineárne nezávislých vektorov, ktorá ho generuje.

4.4. Zistite dimenzie všetkých podpriestorov priestoru $\boldsymbol{V}_3(Z_2)$ (pozri cvičenie 3.2).

4.5. Zistite dimenziu nasledujúcich podpriestorov priestoru $\boldsymbol{V}_3(R)$

$\boldsymbol{P}_1 = [(3,0,0),(5,0,0)]$,
$\boldsymbol{P}_2 = [(1,2,0),(2,3,0)]$,
$\boldsymbol{P}_3 = [(1,-2,3),(4,-3,2),(5,1,0)]$.

Návod. Podobne ako v príklade 4.9 nahraďte sústavy vektorov, ktoré generujú podpriestory $\boldsymbol{P}_1, \boldsymbol{P}_2, \boldsymbol{P}_3$ sústavami s nimi lineárne ekvivalentných ale lineárne nezávislých vektorov.

4.6. Nech $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3\}$ je báza 3-rozmerného priestoru $\boldsymbol{V}(R)$. Dokážte, že každá z množín

$B_1 = \{\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2,\ \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_3,\ \boldsymbol{\alpha}_2 + \boldsymbol{\alpha}_3\}$,
$B_2 = \{\boldsymbol{\alpha}_1 + 3\boldsymbol{\alpha}_2,\ \boldsymbol{\alpha}_2 + 3\boldsymbol{\alpha}_3,\ \boldsymbol{\alpha}_3 + 3\boldsymbol{\alpha}_1\}$
$B_3 = \{\boldsymbol{\alpha}_1,\ \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2,\ \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2,\ \boldsymbol{\alpha}_3\}$

je báza priestoru $\boldsymbol{V}(R)$ a vypočítajte súradnice vektorov $\boldsymbol{\alpha}_1$, $\boldsymbol{\alpha}_2$, $\boldsymbol{\alpha}_3$ vzhľadom na bázu B_1, B_2 a B_3.

4.7. Nech $\boldsymbol{P}_1 = [\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k]$ a $\boldsymbol{P}_2 = [\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k, \boldsymbol{\beta}]$, kde $\boldsymbol{\beta}$ je lineárnou kombináciou vektorov $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_k$. Potom $d(\boldsymbol{P}_1) = d(\boldsymbol{P}_2)$. Dokážte.

Návod. Dokážte, že $\boldsymbol{P}_1 = \boldsymbol{P}_2$.

4.8. Nech $\boldsymbol{P}$ a $\boldsymbol{S}$ sú také podpriestory vektorového priestoru $\boldsymbol{V}(F)$, že $\boldsymbol{P} \cap \boldsymbol{S} = \{\vec{\mathbf{0}}\}$ a $\boldsymbol{P} \vee \boldsymbol{S} = \boldsymbol{V}$, potom hovoríme, že priestory sú navzájom komplementárne (jeden je komplementom - doplnkom druhého). Dokážte nasledovné:

a) Ak $d(\boldsymbol{V}) = n$, tak $d(\boldsymbol{P}) + d(\boldsymbol{S}) = n$.
b) Ak $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_k, \boldsymbol{\varepsilon}_{k+1}, \dots, \boldsymbol{\varepsilon}_n\}$ je báza priestoru $\boldsymbol{V}$, tak priestory $[\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_k] = \boldsymbol{P}$ a $[\boldsymbol{\varepsilon}_{k+1}, \dots, \boldsymbol{\varepsilon}_n] = \boldsymbol{S}$ sú komplementárne.

4.9. Nech $\boldsymbol{P}$ a $\boldsymbol{S}$ sú podpriestory n-rozmerného priestoru $\boldsymbol{V}(F)$. Dokážte nasledovné:

a) Ak $d(\boldsymbol{P}) + d(\boldsymbol{S}) = n$, a zároveň $\boldsymbol{P} \cap \boldsymbol{S} = \{\vec{\mathbf{0}}\}$, tak $\boldsymbol{P}$ a $\boldsymbol{S}$ sú komplementárne.
b) Ak $d(\boldsymbol{P}) + d(\boldsymbol{S}) = n$, a zároveň $\boldsymbol{P} \vee \boldsymbol{S} = \boldsymbol{V}$, tak $\boldsymbol{P}$ a $\boldsymbol{S}$ sú komplementárne.

4.10. Nech $\boldsymbol{P}$ a $\boldsymbol{S}$ sú komplementárne podpriestory priestoru $\boldsymbol{V}$. Nech $\boldsymbol{W}$ je podpriestor priestoru $\boldsymbol{V}$. Musia byť aj $\boldsymbol{P} \cap \boldsymbol{W}$ a $\boldsymbol{S} \cap \boldsymbol{W}$ komplementárne podpriestory? Ak áno, dokážte to, ak nie, nájdite protipríklad.

§ 5. Skalárny súčin

V príklade 1.1 sme definovali vektorový priestor $\boldsymbol{V}$ ako množinu orientovaných úsečiek v rovine vychádzajúcich z jedného pevného bodu. V priestore $\boldsymbol{V}$ možno definovať pojmy: veľkosť vektora, uhol dvoch vektorov, skalárny súčin atď. Čitateľ pozná tieto pojmy zo strednej školy. Pri zovšeobecňovaní týchto pojmov na *reálne* vektorové priestory budeme vychádzať z pojmu skalárneho súčinu, ktorý si teraz definujeme.

Definícia 5.1. Nech ľubovoľnej dvojici vektorov $\boldsymbol{\alpha}, \boldsymbol{\beta}$ reálneho vektorového priestoru $\boldsymbol{E}(R)$ je priradený skalár $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in R$ tak, že sú splnené nasledujúce podmienky:

(E$_1$) $(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (\boldsymbol{\beta}, \boldsymbol{\alpha})$,

(E$_2$) $s(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (s\boldsymbol{\alpha}, \boldsymbol{\beta}), kde\ s \in R$,

(E$_3$) $(\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2, \boldsymbol{\beta}) = (\boldsymbol{\alpha}_1, \boldsymbol{\beta}) + (\boldsymbol{\alpha}_2, \boldsymbol{\beta})$,

(E$_4$) $(\boldsymbol{\alpha}, \boldsymbol{\alpha}) \geqq 0$, pričom $(\boldsymbol{\alpha}, \boldsymbol{\alpha}) = 0$ práve vtedy, keď $\boldsymbol{\alpha} = \vec{\mathbf{0}}$.

Skalár $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ nazývame *skalárny súčin* vektorov $\boldsymbol{\alpha}, \boldsymbol{\beta}$.

Poznámka 5.1. Podmienka E_1 (E_3) hovorí, že skalárny súčin je komutatívny (distributívny vzhľadom na sčítanie vektorov).

Definícia 5.2. Reálny vektorový priestor $\boldsymbol{E}(R)$, v ktorom je definovaný skalárny súčin nazývame *euklidovský vektorový priestor.*

Veta 5.1. *Pre každý vektor $\boldsymbol{\alpha}$ euklidovského vektorového priestoru $\boldsymbol{E}(R)$ platí* $(\boldsymbol{\alpha}, \vec{\mathbf{0}}) = 0$.

Dôkaz. $(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (\boldsymbol{\alpha}, \boldsymbol{\beta} + \vec{\mathbf{0}}) = (\boldsymbol{\alpha}, \boldsymbol{\beta}) + (\boldsymbol{\alpha}, \vec{\mathbf{0}})$. Na druhej strane máme $(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (\boldsymbol{\alpha}, \boldsymbol{\beta}) + 0$. Odtiaľ $(\boldsymbol{\alpha}, \boldsymbol{\beta}) + (\boldsymbol{\alpha}, \vec{\mathbf{0}}) = (\boldsymbol{\alpha}, \boldsymbol{\beta}) + 0$, čiže $(\boldsymbol{\alpha}, \vec{\mathbf{0}}) = 0$. $\square$

Príklad 5.1. Vo vektorovom priestore orientovaných úsečiek (príklad 1.3) sa definuje skalárny súčin $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}}$ takto: $(\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}}) = |\vec{\boldsymbol{a}}| \cdot |\vec{\boldsymbol{b}}| \cos\omega$, kde $|\vec{\boldsymbol{a}}|, |\vec{\boldsymbol{b}}|$ sú dĺžky vektorov $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}}$; $w = \measuredangle(\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}})$. Dokážeme, že podmienky $(E_1) - (E_4)$ v definícii 5.1 sú splnené. Platnosť podmienok (E_1) a (E_2) je zrejmá. Aby sme dokázali platnosť podmienky (E_3) stačí si uvedomiť, že $|\vec{\boldsymbol{a}}| \cdot |\vec{\boldsymbol{b}}| \cdot \cos\omega = |\vec{\boldsymbol{b}}| \cdot |\vec{\boldsymbol{a}}|_b$, kde $|\vec{\boldsymbol{a}}|_b$ je dĺžka kolmého priemetu orientovanej úsečky $\vec{\boldsymbol{a}}$ na priamku, na ktorej leží vektor $\vec{\boldsymbol{b}}$. Ďalej platí: „priemet súčtu dvoch vektorov je súčet priemetov týchto vektorov“. Máme tak $(\vec{\boldsymbol{a}}_1 + \vec{\boldsymbol{a}}_2, \vec{\boldsymbol{b}}) = |\vec{\boldsymbol{b}}| \cdot |\vec{\boldsymbol{a}}_1 + \vec{\boldsymbol{a}}_2|_b = |\vec{\boldsymbol{b}}|(|\vec{\boldsymbol{a}}_1|_b + |\vec{\boldsymbol{a}}_2|_b) = |\vec{\boldsymbol{b}}| \cdot |\vec{\boldsymbol{a}}_1|_b + |\vec{\boldsymbol{b}}| \cdot |\vec{\boldsymbol{a}}_2|_b = = (\vec{\boldsymbol{a}}_1, \vec{\boldsymbol{b}}) + (\vec{\boldsymbol{a}}_2, \vec{\boldsymbol{b}})$. Podmienka (E_4) je splnená tiež, lebo $(\vec{\boldsymbol{a}}, \vec{\boldsymbol{a}}) = |\vec{\boldsymbol{a}}| \cdot |\vec{\boldsymbol{a}}| \cos 0 = = |\vec{\boldsymbol{a}}|^2 \geqq 0$.

Príklad 5.2. V aritmetickom vektorovom priestore $\boldsymbol{V}_n(R)$ definujeme skalárny súčin vektorov $\boldsymbol{\alpha} = (x_1, x_2, \ldots, x_n)$, $\boldsymbol{\beta} = (y_1, y_2, \ldots, y_n)$ takto:

$$(\boldsymbol{\alpha}, \boldsymbol{\beta}) = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n. \tag{5.1}$$

Čitateľ ľahko dokáže, že podmienky $(E_1) - (E_4)$ sú splnené.

Príklad 5.3. Vo vektorovom priestore reálnych spojitých funkcií definovaných na intervale $\langle 0, 1\rangle$ (príklad 1.6), definujeme skalárny súčin takto:

$$(f, g) = \int_0^1 f(x) \cdot g(x) dx.$$

Podmienky $(E_1) - (E_4)$ sa dokážu použitím základných viet o určitom integráli. (Ak čitateľ tieto vety nepozná, môže sa k príkladu vrátiť neskoršie.)

Veta 5.2. *Nech $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{E}(R)$ sú ľubovoľné vektory euklidovského priestoru. Potom*

$$(\boldsymbol{\alpha}, \boldsymbol{\beta})^2 \leqq (\boldsymbol{\alpha}, \boldsymbol{\alpha}) \cdot (\boldsymbol{\beta}, \boldsymbol{\beta}). \tag{5.2}$$

Poznámka 5.2. Nerovnosť (5.2) sa nazýva Schwarzova nerovnosť.

Dôkaz vety 5.2. Ak $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{E}(R)$ $t \in R$, máme (podmienka (E_4))

$$(\boldsymbol{\alpha} - t\boldsymbol{\beta}, \boldsymbol{\alpha} - t\boldsymbol{\beta}) \geqq 0,$$

alebo

$$t^2(\boldsymbol{\beta}, \boldsymbol{\beta}) - 2t(\boldsymbol{\alpha}, \boldsymbol{\beta}) + (\boldsymbol{\alpha}, \boldsymbol{\alpha}) \geqq 0. \tag{5.3}$$

Ak je $\boldsymbol{\beta} = \vec{\mathbf{0}}$ nerovnosť (5.2) platí. Nech $\boldsymbol{\beta} \neq \vec{\mathbf{0}}$. Potom $(\boldsymbol{\beta}, \boldsymbol{\beta}) \neq 0$. Položíme $t = \frac{(\boldsymbol{\alpha}, \boldsymbol{\beta})}{(\boldsymbol{\beta}, \boldsymbol{\beta})}$ a dosadíme do (5.3):

$$\frac{(\boldsymbol{\alpha}, \boldsymbol{\beta})^2}{(\boldsymbol{\beta}, \boldsymbol{\beta})} - 2\frac{(\boldsymbol{\alpha}, \boldsymbol{\beta})^2}{(\boldsymbol{\beta}, \boldsymbol{\beta})} + (\boldsymbol{\alpha}, \boldsymbol{\alpha}) \geqq 0,$$

z čoho vyplýva (5.2). □

Definícia 5.3. Nech $\boldsymbol{\alpha}$ je vektor euklidovského vektorového priestoru. Skalár $\sqrt{(\boldsymbol{\alpha}, \boldsymbol{\alpha})}$ nazývame *veľkosťou* alebo *absolútnou hodnotou* vektora $\boldsymbol{\alpha}$, čo označujeme $|\boldsymbol{\alpha}| = \sqrt{(\boldsymbol{\alpha}, \boldsymbol{\alpha})}$.

Poznámka 5.3. Schwarzova nerovnosť sa často uvádza v tvare

$$(\boldsymbol{\alpha}, \boldsymbol{\beta}) \leqq |\boldsymbol{\alpha}| \cdot |\boldsymbol{\beta}|, \tag{5.4}$$

ktorý ľahko dostaneme z nerovnosti (5.2).

Poznámka 5.4. Vidíme, že definícia veľkosti vektora je v zhode s príkladom 5.1, lebo $|\vec{\boldsymbol{a}}| = \sqrt{|\vec{\boldsymbol{a}}| \cdot |\vec{\boldsymbol{a}}| \cos 0} = \sqrt{|\vec{\boldsymbol{a}}|^2}$.

Príklad 5.4. Vypočítajme veľkosť vektora $\boldsymbol{\alpha} = \sin x$ vektorového priestoru spojitých reálnych funkcií definovaných na intervale $\langle 0, 1 \rangle$:

$$|\boldsymbol{\alpha}| = \sqrt{\int_0^1 \sin^2 x dx} = \sqrt{\int_0^1 \frac{1 - \cos 2x}{2} dx} = \sqrt{\left[\frac{1}{2}x - \frac{1}{4}\sin 2x\right]_0^1} =$$

$$= \sqrt{\frac{1}{2} - \frac{1}{4}\sin 2} \doteq \sqrt{0,5 - 0,227} = 0,522.$$

Aby sme mohli definovať uhol dvoch vektorov, dokážeme nasledujúci dôsledok vety 5.2.

Dôsledok. *Pre ľubovoľné dva vektory* $\boldsymbol{\alpha}, \boldsymbol{\beta} \neq \vec{\mathbf{0}}$ *euklidovského priestoru platí*

$$-1 \leqq \frac{(\boldsymbol{\alpha}, \boldsymbol{\beta})}{|\boldsymbol{\alpha}| \cdot |\boldsymbol{\beta}|} \leqq 1. \tag{5.5}$$

Dôkaz. Podľa nerovnosti (5.2) máme

$$\frac{(\boldsymbol{\alpha}, \boldsymbol{\beta})^2}{(\boldsymbol{\alpha}, \boldsymbol{\alpha})(\boldsymbol{\beta}, \boldsymbol{\beta})} \leqq 1,$$

z čoho dostávame

$$-1 \leqq \frac{(\boldsymbol{\alpha}, \boldsymbol{\beta})}{\sqrt{(\boldsymbol{\alpha}, \boldsymbol{\alpha})}\sqrt{(\boldsymbol{\beta}, \boldsymbol{\beta})}} \leqq 1,$$

čo je vlastne nerovnosť (5.5). □

Definícia 5.4. Nech $\boldsymbol{\alpha}, \boldsymbol{\beta}$ sú dva nenulové vektory euklidovského vektorového priestoru. Uhlom $\omega = \measuredangle(\boldsymbol{\alpha}, \boldsymbol{\beta})$ vektorov $\boldsymbol{\alpha}, \boldsymbol{\beta}$ nazveme hodnotu

$$\omega = \arccos \frac{(\boldsymbol{\alpha}, \boldsymbol{\beta})}{|\boldsymbol{\alpha}| \cdot |\boldsymbol{\beta}|}, \text{ kde } \ 0 \leqq \omega \leqq \pi.$$

Poznámka 5.5. Nenulovosť vektorov $\boldsymbol{\alpha}, \boldsymbol{\beta}$ a nerovnosť (5.5) zaručuje existenciu hodnoty ω.

Definícia 5.5. Vektory $\boldsymbol{\alpha}, \boldsymbol{\beta}$ sa nazývajú *ortogonálne*, ak $(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 0$.

Poznámka 5.6. Podľa tejto definície nulový vektor a ľubovoľný vektor sú ortogonálne.

Príklad 5.5. Uhol vektorov $\boldsymbol{\alpha} = (3, 0)$ a $\boldsymbol{\beta} = (2, 2)$ priestoru $\boldsymbol{V}_2(R)$ je

$$\omega = \arccos \frac{(\boldsymbol{\alpha}, \boldsymbol{\beta})}{|\boldsymbol{\alpha}| \cdot |\boldsymbol{\beta}|} = \arccos \frac{6 + 0}{\sqrt{3^2}\sqrt{2^2 + 2^2}} = \arccos \frac{6}{3 \cdot 2\sqrt{2}} = \arccos \frac{1}{\sqrt{2}} = \frac{\pi}{4}.$$

Príklad 5.6. Nech vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_n$ sú po dvoch ortogonálne. Dokážeme, že

$$|\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2 + \cdots + \boldsymbol{\alpha}_n|^2 = |\boldsymbol{\alpha}_1|^2 + |\boldsymbol{\alpha}_2|^2 + \cdots + |\boldsymbol{\alpha}_n|^2.$$

Skutočne: $|\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2 + \cdots + \boldsymbol{\alpha}_n|^2 = (\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2 + \cdots + \boldsymbol{\alpha}_n,\ \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2 + \cdots + \boldsymbol{\alpha}_n) =$
$= (\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_1) + (\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2) + \cdots + (\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_n) + (\boldsymbol{\alpha}_2, \boldsymbol{\alpha}_1) + (\boldsymbol{\alpha}_2, \boldsymbol{\alpha}_2) + \cdots + (\boldsymbol{\alpha}_2, \boldsymbol{\alpha}_n) + \cdots$
$\cdots + (\boldsymbol{\alpha}_n, \boldsymbol{\alpha}_1) + (\boldsymbol{\alpha}_n, \boldsymbol{\alpha}_2) + \cdots + (\boldsymbol{\alpha}_n, \boldsymbol{\alpha}_n) = |\boldsymbol{\alpha}_1|^2 + |\boldsymbol{\alpha}_2|^2 + \cdots + |\boldsymbol{\alpha}_n|^2$.
Dva nenulové ortogonálne vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2$ z priestoru orientovaných úsečiek môžeme považovať za strany obdĺžnika s uhlopriečkou $\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2$ (príklad 1.1). Rovnosť $|\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2|^2 = |\boldsymbol{\alpha}_1|^2 + |\boldsymbol{\alpha}_2|^2$ je vlastne Pytagorova veta.

Príklad 5.7. Ukážeme, že v euklidovskom priestore pre dva ľubovoľné vektory platí nerovnosť.

$$|\boldsymbol{\alpha} + \boldsymbol{\beta}| \leqq |\boldsymbol{\alpha}| + |\boldsymbol{\beta}|. \tag{5.6}$$

Skutočne: $|\boldsymbol{\alpha}+\boldsymbol{\beta}|^2 = (\boldsymbol{\alpha}+\boldsymbol{\beta}, \boldsymbol{\alpha}+\boldsymbol{\beta}) = (\boldsymbol{\alpha}, \boldsymbol{\alpha}) + 2(\boldsymbol{\alpha}, \boldsymbol{\beta}) + (\boldsymbol{\beta}, \boldsymbol{\beta})$. Ale podľa (5.4) je $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \leqq |\boldsymbol{\alpha}||\boldsymbol{\beta}|$. Vidíme, že

$$|\boldsymbol{\alpha}+\boldsymbol{\beta}|^2 = (\boldsymbol{\alpha}, \boldsymbol{\alpha}) + 2(\boldsymbol{\alpha}, \boldsymbol{\beta}) + (\boldsymbol{\beta}, \boldsymbol{\beta}) \leqq |\boldsymbol{\alpha}|^2 + 2|\boldsymbol{\alpha}||\boldsymbol{\beta}| + |\boldsymbol{\beta}|^2 = (|\boldsymbol{\alpha}| + |\boldsymbol{\beta}|)^2,$$

odkiaľ dostaneme nerovnosť (5.6.).

Poznámka 5.7. Nerovnosť (5.6) nazývame trojuholníková nerovnosť.

V euklidovskom vektorovom priestore hrajú dôležitú úlohu bázy, ktoré tvoria vektory po dvoch ortogonálne.

Veta 5.3. *Nech*

$$\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n \tag{5.7}$$

je n-tica nenulových vektorov n-rozmerného vektorového priestoru $\boldsymbol{E}(R)$ a nech $(\boldsymbol{\varepsilon}_i, \boldsymbol{\varepsilon}_j) = 0$ pre $i \neq j$, t.j. vektory (5.7) sú po dvoch ortogonálne. Potom vektory (5.7) tvoria bázu priestoru $\boldsymbol{E}(R)$.

Dôkaz. Stačí dokázať, že vektory (5.7) sú lineárne nezávislé, t.j. že rovnosť

$$c_1\boldsymbol{\varepsilon}_1 + c_2\boldsymbol{\varepsilon}_2 + \cdots + c_n\boldsymbol{\varepsilon}_n = \vec{\mathbf{0}} \tag{5.8}$$

platí len pre $c_1 = c_2 = \cdots = c_n = 0 \in R$. Skutočne, ak (5.8) násobíme skalárne vektorom $\boldsymbol{\varepsilon}_i$ $(i = 1, 2, \ldots, n)$, dostaneme

$$c_1 \cdot 0 + c_2 \cdot 0 + \cdots + c_i(\boldsymbol{\varepsilon}_i, \boldsymbol{\varepsilon}_i) + \cdots + c_n \cdot 0 = 0$$

Odtiaľ vzhľadom na $(\boldsymbol{\varepsilon}_i, \boldsymbol{\varepsilon}_i) \neq 0$ máme $c_i = 0$ $(i = 1, 2, \ldots, n)$. □

Definícia 5.6. Báza (5.7) sa nazýva *ortogonálna báza* euklidovského priestoru. Ak okrem toho platí $|\boldsymbol{\varepsilon}_i| = 1$ pre $i = 1, 2, \ldots, n$ báza (5.7) sa nazýva *ortonormálnou.*

Poznámka 5.8. Ak báza $B = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n\}$ je ortogonálna, tak báza

$$B' = \left\{\frac{\boldsymbol{\varepsilon}_1}{|\boldsymbol{\varepsilon}_1|}, \frac{\boldsymbol{\varepsilon}_2}{|\boldsymbol{\varepsilon}_2|}, \ldots, \frac{\boldsymbol{\varepsilon}_n}{|\boldsymbol{\varepsilon}_n|}\right\}$$

je ortonormálna. Ortonormálna báza je napríklad kanonická báza priestoru $\boldsymbol{V}_n(R)$.

Veta 5.4. *V každom n-rozmernom euklidovskom priestore $\boldsymbol{E}(R)$ existuje ortogonálna báza.*

Dôkaz. Je jasné, že v priestore $\boldsymbol{E}(R)$ existuje nejaká báza $B = \{\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \ldots, \boldsymbol{\mu}_n\}$. Zostrojíme bázu $B' = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n\}$, ktorá je ortogonálna.

Položíme

$$\boldsymbol{\varepsilon}_1 = \boldsymbol{\mu}_1.$$

Nech

$$\boldsymbol{\varepsilon}_2 = \boldsymbol{\mu}_2 + c_1\boldsymbol{\varepsilon}_1.$$

Reálne číslo c_1 určíme tak, aby platilo $(\boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_1) = 0$, t.j.

$$(\boldsymbol{\mu}_2 + c_1\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_1) = 0, \qquad \text{alebo} \qquad (\boldsymbol{\mu}_2, \boldsymbol{\varepsilon}_1) + c_1(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_1) = 0,$$

odkiaľ

$$c_1 = -\frac{(\boldsymbol{\varepsilon}_1, \boldsymbol{\mu}_2)}{(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_1)}.$$

Aby sme určili tretí vektor ortogonálnej bázy, položíme

$$\boldsymbol{\varepsilon}_3 = \boldsymbol{\mu}_3 + d_1\boldsymbol{\varepsilon}_1 + d_2\boldsymbol{\varepsilon}_2,$$

kde skaláry (reálne čísla) d_1, d_2 určíme tak, aby platilo $(\boldsymbol{\varepsilon}_3, \boldsymbol{\varepsilon}_1) = 0$, $(\boldsymbol{\varepsilon}_3, \boldsymbol{\varepsilon}_2) = 0$, alebo

$$(\boldsymbol{\mu}_3 + d_1\boldsymbol{\varepsilon}_1 + d_2\boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_1) = 0,$$
$$(\boldsymbol{\mu}_3 + d_1\boldsymbol{\varepsilon}_1 + d_2\boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_2) = 0,$$

odkiaľ vzhľadom na to, že $(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2) = 0$, máme

$$d_1 = -\frac{(\boldsymbol{\mu}_3, \boldsymbol{\varepsilon}_1)}{(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_1)}, \quad d_2 = -\frac{(\boldsymbol{\mu}_3, \boldsymbol{\varepsilon}_2)}{(\boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_2)}.$$

Takto postupujeme ďalej. Predpokladajme, že už máme vektory $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_{k-1}$. Aby sme určili $\boldsymbol{\varepsilon}_k$, položíme

$$\boldsymbol{\varepsilon}_k = \boldsymbol{\mu}_k + s_1\boldsymbol{\varepsilon}_1 + s_2\boldsymbol{\varepsilon}_2 + \cdots + s_{k-1}\boldsymbol{\varepsilon}_{k-1}, \tag{5.9}$$

kde skaláry $s_1, s_2, \dots, s_{k-1}$ určíme tak aby platilo

$$\begin{aligned}(\boldsymbol{\varepsilon}_k, \boldsymbol{\varepsilon}_1) &= 0,\\ (\boldsymbol{\varepsilon}_k, \boldsymbol{\varepsilon}_2) &= 0,\\ &\vdots\\ (\boldsymbol{\varepsilon}_k, \boldsymbol{\varepsilon}_{k-1}) &= 0.\end{aligned}$$

Ak do týchto vzťahov dosadíme (5.9) a využijeme fakt, že $(\boldsymbol{\varepsilon}_i, \boldsymbol{\varepsilon}_j) = 0$ pre $i \neq j$, $1 \leq i, j \leqq k-1$, vypočítame

$$\begin{aligned}s_1 &= -\frac{(\boldsymbol{\mu}_k, \boldsymbol{\varepsilon}_1)}{(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_1)},\\ s_2 &= -\frac{(\boldsymbol{\mu}_k, \boldsymbol{\varepsilon}_2)}{(\boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_2)},\\ &\vdots\\ s_{k-1} &= -\frac{(\boldsymbol{\mu}_k, \boldsymbol{\varepsilon}_{k-1})}{(\boldsymbol{\varepsilon}_{k-1}, \boldsymbol{\varepsilon}_{k-1})}.\end{aligned}$$

V postupe pokračujeme, kým nevyčerpáme všetky vektory bázy B. Dokážeme, že vektory $\boldsymbol{\varepsilon}_k$ sú nenulové, t.j. $\boldsymbol{\varepsilon}_k \neq \vec{\mathbf{0}}$ pre $k = 1, 2, \dots, n$. Aby sme to dokázali, všimnime si, že $\boldsymbol{\varepsilon}_k$ je lineárnou kombináciou vektorov $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \dots, \boldsymbol{\mu}_k$ (prečo?). Máme tak

$$\boldsymbol{\varepsilon}_k = t_1\boldsymbol{\mu}_1 + t_2\boldsymbol{\mu}_2 + \cdots + t_k\boldsymbol{\mu}_k,$$

kde zrejme $t_k = 1$. Ak by $\boldsymbol{\varepsilon}_k = \vec{\mathbf{0}}$, vektory $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \dots, \boldsymbol{\mu}_k$ by boli lineárne závislé, čo nie je, lebo sú to vektory bázy B. Keďže vektory $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n$ sú nenulové a (vzhľadom na konštrukciu) po dvoch ortogonálne, podľa vety 5.3 tvoria bázu priestoru $\boldsymbol{E}(R)$. $\square$

Poznámka 5.9. *Postup konštrukcie vektorov* $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n$ *sa nazýva ortogonalizačný proces.*

Príklad 5.8. Nech $\boldsymbol{\mu}_1 = (0,0,3)$, $\boldsymbol{\mu}_2 = (0,1,2)$, $\boldsymbol{\mu}_3 = (1,1,1)$ sú vektory priestoru $\boldsymbol{V}_3(R)$. Zrejme tvoria bázu. Uplatníme ortogonalizačný proces:

$$\boldsymbol{\varepsilon}_1 = (0,0,3), \qquad \boldsymbol{\varepsilon}_2 = \boldsymbol{\mu}_2 + c_1\boldsymbol{\varepsilon}_1,$$

kde c_1 určíme tak, aby $(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2) = 0$, t.j. $(\boldsymbol{\varepsilon}_1, \boldsymbol{\mu}_2) + c_1(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_1) = 0$, odkiaľ čitateľ vypočíta $c_1 = -\frac{2}{3}$. (Skalárny súčin počítame podľa (5.1).) Preto je

$$\boldsymbol{\varepsilon}_2 = \boldsymbol{\mu}_2 - \frac{2}{3}\boldsymbol{\varepsilon}_1 = (0,1,2) - \frac{2}{3}(0,0,3) = (0,1,0).$$

Ďalej položíme $\boldsymbol{\varepsilon}_3 = \boldsymbol{\mu}_3 + d_1\boldsymbol{\varepsilon}_1 + d_2\boldsymbol{\varepsilon}_2$, kde skaláry určíme tak, aby platilo $(\boldsymbol{\varepsilon}_3, \boldsymbol{\varepsilon}_1) = 0$, $(\boldsymbol{\varepsilon}_3, \boldsymbol{\varepsilon}_2) = 0$, čiže

$$(\boldsymbol{\mu}_3, \boldsymbol{\varepsilon}_1) + d_1(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_1) = 0, \quad (\boldsymbol{\mu}_3, \boldsymbol{\varepsilon}_2) + d_2(\boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_2) = 0,$$

odkiaľ dostaneme $d_1 = -\frac{1}{3}$ a $d_2 = -1$. Teda máme

$$\varepsilon_3 = \boldsymbol{\mu}_3 - \frac{1}{3}\boldsymbol{\varepsilon}_1 - \boldsymbol{\varepsilon}_2 = (1,0,0).$$

Ortogonálna báza je $\boldsymbol{\varepsilon}_1 = (0,0,3)$, $\boldsymbol{\varepsilon}_2 = (0,1,0)$, $\boldsymbol{\varepsilon}_3 = (1,0,0)$, ortonormálna báza je $\boldsymbol{\varepsilon}_1' = \frac{\boldsymbol{\varepsilon}_1}{|\boldsymbol{\varepsilon}_1|} = (0,0,1)$, $\boldsymbol{\varepsilon}_2' = \boldsymbol{\varepsilon}_2$, $\boldsymbol{\varepsilon}_3' = \boldsymbol{\varepsilon}_3$.

Veta 5.5. *Nech* $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n\}$ *je ortonormálna báza euklidovského priestoru. Potom súradnice ľubovoľného vektora* $\boldsymbol{\alpha}$ *v tejto báze sú skalárne súčiny vektora* $\boldsymbol{\alpha}$ *a príslušných vektorov bázy.*

Dôkaz. Nech

$$\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_n\boldsymbol{\varepsilon}_n.$$

je

$$(\boldsymbol{\alpha}, \boldsymbol{\varepsilon}_1) = x_1(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_1) + x_2(\boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_1) + \cdots + x_n(\boldsymbol{\varepsilon}_n, \boldsymbol{\varepsilon}_1).$$

Keďže $(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_1) = 1$ $(\boldsymbol{\varepsilon}_i, \boldsymbol{\varepsilon}_1) = 0$, kde $i \neq 1$, máme $x_1 = (\boldsymbol{\alpha}, \boldsymbol{\varepsilon}_1)$ a analogicky $x_2 = (\boldsymbol{\alpha}, \boldsymbol{\varepsilon}_2)$, $x_3 = (\boldsymbol{\alpha}, \boldsymbol{\varepsilon}_3), \ldots, x_n = (\boldsymbol{\alpha}, \boldsymbol{\varepsilon}_n)$. □

Cvičenia

5.1. Dokážte podrobne platnosť podmienok $(E_1) - (E_4)$ z definície 5.1 v príkladoch 5.2 a 5.3.

5.2. Použitím definície skalárneho súčinu v príklade 5.2 resp. 5.3 vypočítajte skalárny súčin a a uhol vektorov α, β.

a) $\alpha = (3, -3, \sqrt{3})$, $\beta = (-3, -3, \sqrt{3})$, kde $\alpha, \beta \in \boldsymbol{V}_3(R)$

b) $\alpha = x$, $\beta = \sin x$, kde α, β sú vektory vektorového priestoru reálnych funkcií definovaných na intervale $\langle 0, 1 \rangle$.

c) $\alpha = \sin x$, $\beta = \cos x$, kde α, β sú vektory priestoru ako za b)

5.3. Nech α, β, γ sú tri vektory euklidovského priestoru. Dokážte, že platí

$$|\alpha - \gamma| \le |\alpha - \beta| + |\beta - \gamma|.$$

Návod. Použite nerovnosť (5.6) v príklade 5.7.

5.4. Nech $\alpha = (x_1, x_2, x_3)$, $\beta = (y_1, y_2, y_3)$ sú vektory priestoru $\boldsymbol{V}_3(R)$. Zistite, či nasledujúce rovnosti definujú skalárny súčin v priestore $\boldsymbol{V}_3(R)$.

a) $(\alpha, \beta) = x_1y_1 + x_1y_2 + x_2y_1 + 2x_2y_2 + x_3y_3$,
b) $(\alpha, \beta) = 3x_1y_1 + x_1y_2 + x_1y_3 + x_2y_1 - 4x_2y_2 + \frac{3}{2}x_2y_3 + x_3y_1 + \frac{3}{2}x_3y_2$,
c) $(\alpha, \beta) = 2x_1y_1 - x_1y_2 - x_2y_1 + 4x_2y_2 + x_2y_3 + x_3y_2 + 3x_3y_3$.

5.5. Nech B je báza vektorového priestoru $\boldsymbol{V}$. Nájdite ortonormálnu bázu B' tohoto priestoru

a) $B = \{\alpha, \beta, \gamma\}$, kde $\alpha = (2, 2, 2)$, $\beta = (3, -1, 0)$, $\gamma = (7, 0, 0)$ sú vektory priestoru $\boldsymbol{V}_3(R)$.
b) $B = \{\alpha, \beta, \gamma\}$, kde $\alpha = 1$, $\beta = x$, $\gamma = x^2$ sú vektory priestoru všetkých polynómov stupňa najviac 2 s reálnymi koeficientami.

Skalárny súčin je definovaný v prípade a) ako v príklade 5.2, v prípade b) ako v príklade 5.3.

Kapitola 3

MATICE A SÚSTAVY LINEÁRNYCH ROVNÍC

Príklad 1.1. Uvažujme o sústave 3 rovníc so štyrmi neznámymi

$$\begin{aligned} 3x_1 - 4x_2 \; + \; x_3 - 2x_4 \; &= \; 5 \\ 2x_1 \qquad + \frac{1}{3}x_3 - \; x_4 \; &= -2 \\ 2x_1 + \sqrt{3}x_2 \qquad - 7x_4 \; &= \sqrt{5} \end{aligned} \tag{1.1}$$

vektorového priestoru $\boldsymbol{R}_4(R)$ (pozri príklad 1.8 v kapitole 2).
Sústavu (1.1) možno úspornejšie zapísať pomocou tabuľky:

$$\begin{pmatrix} 3, & -4, & 1, & -2, & 5 \\ 2, & 0, & \frac{1}{3}, & -1, & -2 \\ 2, & \sqrt{3}, & 0, & -7, & \sqrt{5} \end{pmatrix}$$

Túto tabuľku pätnástich reálnych čísel chápeme ako celok (ako jeden matematický objekt) a nazývame ju maticou nad poľom reálnych čísel.

Definícia 1.1. Nech je dané pole F a prirodzené čísla $m, n \geqq 1$. Tabuľku mn prvkov poľa F usporiadaných do m riadkov a n stĺpcov takto:

$$\begin{pmatrix} a_{11}, & a_{12}, & \cdots, & a_{1k}, & \cdots, & a_{1n} \\ a_{21}, & a_{22}, & \cdots, & a_{2k}, & \cdots, & a_{2n} \\ \vdots & & & & & \\ a_{i1}, & a_{i2}, & \cdots, & a_{ik}, & \cdots, & a_{in} \\ \vdots & & & & & \\ a_{m1}, & a_{m2}, & \cdots, & a_{mk}, & \cdots, & a_{mn} \end{pmatrix} \tag{1.2}$$

nazývame *matica* typu $m \times n$ nad poľom F.

Matice budeme označovať veľkými písmenami tzv. bezpätkového písma napríklad $\mathsf{A}, \mathsf{B}, \mathsf{C}$ a pod. Prvok a_{ik} poľa F je prvkom matice ležiacim v i-tom riadku a k-tom stĺpci matice. Prirodzené číslo i je *riadkový* a k *stĺpcový* index prvku a_{ik}. Ak maticu (1.2) označíme A, skrátene píšeme

$$\mathsf{A} = (a_{ik}) \qquad i = 1, 2, \dots, m, k = 1, 2, \dots, n,$$

alebo tiež $\mathsf{A}_{m,n}$ resp. $(a_{ik})_{m,n}$. Riadky matice A, označíme ich $\boldsymbol{\varrho}_1, \boldsymbol{\varrho}_2, \dots, \boldsymbol{\varrho}_i, \dots, \boldsymbol{\varrho}_m$, môžeme považovať za prvky priestoru $\boldsymbol{V}_n(F)$, stĺpce $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \dots, \boldsymbol{\sigma}_k, \dots, \boldsymbol{\sigma}_n$ za prvky priestoru $\boldsymbol{V}_m(F)$.

Matica, ktorej všetky prvky sa rovnajú nule (presnejšie nulovému prvku poľa F) sa nazýva *nulová* matica. Ak je typu $m \times n$ označíme ju $\mathbf{0}_{m,n}$.

Matica $\mathbf{A}$, v ktorej $m = n$, t.j. je typu $n \times n$ sa nazýva *štvorcová*. Označujeme ju $\mathbf{A}_n$. Prvky $a_{11}, a_{22}, \ldots, a_{nn}$ tvoria *hlavnú*, prvky $a_{1n}, a_{2,n-1}, \ldots, a_{n1}$, *vedľajšiu diagonálu* matice $\mathbf{A}_n$. Štvorcová matica sa nazýva *diagonálna*, ak všetky prvky neležiace na hlavnej diagonále sa rovnajú nule (nulovému prvku poľa F). Diagonálna matica, ktorej všetky prvky na hlavnej diagonále sa rovnajú jednej (t.j. jednotkovému prvku poľa F) sa nazýva *jednotková*. Označujeme ju $\mathbf{J}_n$.

Poznámka 1.1. Pri zapisovaní matíc nie je nutné dávať čiarky medzi prvkami matice. Budeme tak robiť len vtedy, keď sa tým zvýši čitateľnosť. Nič menej, pri matici typu $1 \times n$ čiarky dávame vždy.

Príklad 1.2. Všetky nasledujúce matice majú reálne prvky (sú nad poľom R).

$$\mathbf{A} = \begin{pmatrix} 1 & \sqrt{3} \\ -1 & 0 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} 1 & 2 & -\sqrt{3} & 4 \\ 5 & 2 & 1 & -2 \end{pmatrix},$$

$$\mathbf{C} = (1,\ 2,\ 3), \qquad \mathbf{E} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\mathbf{0}_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \mathbf{J}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Matica $\mathbf{A}$ je typu 2×2, matica $\mathbf{B}$ typu 2×4, $\mathbf{C}$ typu 1×3, $\mathbf{E}$ typu 3×3, $\mathbf{0}_{2,3}$ typu 2×3, $\mathbf{J}_4$ typu 4×4. $\mathbf{A}, \mathbf{E}, \mathbf{J}_4$ sú štvorcové, $\mathbf{E}, \mathbf{J}_4$ diagonálne, $\mathbf{0}_{2,3}$ nulová a $\mathbf{J}_4$ jednotková matica.

Definícia 1.2. Dve matice $\mathbf{A}_{m,n}$, $\mathbf{B}_{r,s}$ sa *rovnajú*, ak sú rovnakého typu a ak sa rovnajú sebe odpovedajúce prvky. T.j. $\mathbf{A} = \mathbf{B}$ práve keď $m = r$, $n = s$ a $a_{ik} = b_{ik}$ pre $i = 1, 2, \ldots, m$, $k = 1, 2, \ldots, n$.

Definícia 1.3. Ak riadky matice $\mathbf{A}$ píšeme ako stĺpce matice $\mathbf{B}$ (v tom istom poradí), hovoríme, že sme napísali maticu *transponovanú* k matici $\mathbf{A}$. Označujeme $\mathbf{B} = \mathbf{A}^T$. Teda ak $\mathbf{A} = (a_{ik})_{m,n}$, tak $\mathbf{A}^T = (a_{ki})_{n,m}$.

Príklad 1.3.

$$\mathbf{A} = \begin{pmatrix} 2 & -3 & 4 \\ 2 & 0 & -1 \end{pmatrix}, \qquad \mathbf{A}^T = \begin{pmatrix} 2 & 2 \\ -3 & 0 \\ 4 & -1 \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} 1 & 2 & -3 \\ 2 & 0 & 1 \\ -3 & 1 & 7 \end{pmatrix}, \qquad \mathbf{B}^T = \begin{pmatrix} 1 & 2 & -3 \\ 2 & 0 & 1 \\ -3 & 1 & 7 \end{pmatrix}.$$

Definícia 1.4. Matica $\mathbf{A}$ sa nazýva *symetrická* ak $\mathbf{A} = \mathbf{A}^T$.

Je zrejmé, že symetrická matica je štvorcovou maticou. Matica $\mathbf{B}$ v príklade 1.3 je symetrická. V symetrickej matici platí $a_{ki} = a_{ik}$.

Definícia 1.5. Súčet dvoch matíc typu $m \times n$ $\mathbf{A} = (a_{ik})$, $\mathbf{B} = (b_{ik})$ definujeme takto:

$$\mathbf{A} + \mathbf{B} = (a_{ik} + b_{ik}), i = 1, 2, \ldots, m, \; k = 1, 2, \ldots, n. \tag{1.3}$$

Poznámka 1.2. Sčítanie matíc je teda definované len pre matice rovnakého typu. Zrejme nemôže prísť k nedorozumeniu, keď znakom „+" označujeme v (1.3) dve rôzne operácie. Na ľavej strane (1.3) je to sčítanie matíc, kým na pravej strane sčítanie prvkov poľa F.

Príklad 1.4. Sčítajme matice

$$\mathbf{A} = \begin{pmatrix} 2 & 3 & -1 \\ 4 & -3 & 2 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} \sqrt{3}, & -3, & 2 \\ 1, & 1, & 0 \end{pmatrix}.$$

Máme

$$\mathbf{A} + \mathbf{B} = \begin{pmatrix} 2 + \sqrt{3} & 0 & 1 \\ 5 & -2 & 2 \end{pmatrix}.$$

Veta 1.1. *Nech $\boldsymbol{M}(F)$ je množina všetkých matíc typu $m \times n$ nad poľom F. Potom štruktúra $(\boldsymbol{M}(F), +)$ je abelovská grupa.*

Dôkaz. Čitateľ si ľahko dokáže, že sčítanie matíc je asociatívne, t.j. pre všetky $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \boldsymbol{M}(F)$ platí

$$\mathbf{A} + (\mathbf{B} + \mathbf{C}) = (\mathbf{A} + \mathbf{B}) + \mathbf{C}. \tag{1.4}$$

Aj zvyšok dôkazu ponechajme na čitateľa. Poznamenajme len, že neutrálnym prvkom operácie $+$ je nulová matica $\mathbf{0}_{m,n}$. □

Definícia 1.6. Nech $\mathbf{A} = (a_{ik})$ je matica nad poľom F a $s \in F$. Násobok $s \cdot \mathbf{A}$ matice $\mathbf{A}$ prvkom s definujeme takto:

$$s \cdot \mathbf{A} = (sa_{ik}) \quad i = 1, 2, \ldots, m, \quad k = 1, 2, \ldots, n. \tag{1.5}$$

Napríklad, ak $\mathbf{A} = \begin{pmatrix} 2 & -3 & 4 \\ \sqrt{2} & 6 & 7 \end{pmatrix}$, tak $\qquad \frac{1}{2}\mathbf{A} = \begin{pmatrix} 1 & -\frac{3}{2} & 2 \\ \frac{\sqrt{2}}{2} & 3 & \frac{7}{2} \end{pmatrix}.$

Veta 1.2. *Množina $\boldsymbol{M}(F)$ všetkých matíc typu $m \times n$ nad poľom F tvorí vektorový priestor nad F, v ktorom sčítanie vektorov (matíc) je definované vzťahom* (1.3) *a násobenie skalárom vzťahom* (1.5).

Dôkaz. Podľa vety 1.1 $(\boldsymbol{M}(F), +)$ je abelovská grupa. Čitateľ ľahko skontroluje, že sú splnené aj podmienky $(V_1) - (V_4)$ z definície 1.1 kapitoly 2. □

Príklad 1.5. Množina
$$\boldsymbol{M}(Q)=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix};\quad a,b,c,d\in Q\right\}$$
je vektorový priestor dimenzie 4 nad poľom racionálnych čísel. Je ľahké overiť, že množina
$$\left\{\begin{pmatrix} 1 & 0\\ 0 & 0\end{pmatrix},\begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix},\begin{pmatrix} 0 & 0\\ 1 & 0\end{pmatrix},\begin{pmatrix} 0 & 0\\ 0 & 1\end{pmatrix}\right\}$$
je báza priestoru $\boldsymbol{M}(Q)$.

Množina matíc rovnakého typu je teda ďalší príklad vektorového priestoru konečnej dimenzie. Je účelné zaviesť ďalšiu operáciu v množine matíc (nad daným poľom) totiž násobenie matíc. Násobenie zavedieme len pre také dvojice matíc, kde prvá má toľko stĺpcov koľko má druhá riadkov.

Definícia 1.7. Nech $\mathsf{A}=(a_{ij})$ je matica typu $m\times p$, $\mathsf{B}=(b_{jk})$ matica typu $p\times n$. Súčin matíc $\mathsf{A}\cdot\mathsf{B}$ (v tomto poradí) je matica $\mathsf{C}=(c_{ik})$ typu $m\times n$, kde $c_{ik}=\sum\limits_{j=1}^{p}a_{ij}b_{jk}$. T.j.

$$\mathsf{A}\cdot\mathsf{B}=\mathsf{C}=(c_{ik})=\Big(\sum_{j=1}^{p}a_{ij}b_{jk}\Big),\ i=1,2,\dots,m;\ k=1,2,\dots,n. \tag{1.6}$$

Inými slovami: Prvok c_{ik} ležiaci v i-tom riadku a k-tom stĺpci matice $\mathsf{A}\cdot\mathsf{B}$ je súčet súčinov prvkov i-teho riadku matice A a k-teho stĺpca matice B. Teda prvok c_{ik} vypočítame takto:
$$c_{ik}=a_{i1}\cdot b_{1k}+a_{i2}\cdot b_{2k}+\cdots+a_{i,p-1}\cdot b_{p-1,k}+a_{ip}\cdot b_{pk}.$$

Príklad 1.6. Násobme matice
$$\begin{pmatrix} 1, & 2, & 3\\ -1, & 0, & 2\end{pmatrix}\begin{pmatrix} 1, & 1, & 2, & 2\\ -1, & -1, & 3, & 3\\ 0, & 1, & 2, & -1\end{pmatrix}=\begin{pmatrix} -1, & 2, & 14, & 5\\ -1, & 1, & 2, & -4\end{pmatrix}.$$
Vidíme, že vynásobením matíc typu 2×3 a 3×4 sme dostali maticu typu 2×4. Prvok 5 tejto matice sme vypočítali takto: $5=1\cdot 2+2\cdot 3+3\cdot(-1)$. Ak príslušný riadok resp. stĺpec pokladáme za maticu typu 1×3 resp. 3×1, môžeme to zapísať takto:
$$(1,2,3)\begin{pmatrix} 2\\ 3\\ -1\end{pmatrix}=5.$$

Lema 1.1. *Nech matice* $\mathsf{A},\mathsf{B},\mathsf{C}$ *sú (po rade) typu* $m\times p$, $p\times r$, $r\times n$. *Potom platí*
$$\mathsf{A}\cdot(\mathsf{B}\cdot\mathsf{C})=(\mathsf{A}\cdot\mathsf{B})\cdot\mathsf{C}. \tag{1.7}$$

Dôkaz. Nech pre určitosť $\mathsf{A}=(a_{ij})_{m,p}$, $\mathsf{B}=(b_{jh})_{p,r}$, $\mathsf{C}=(c_{hk})_{r,n}$. Počítame:
$$(\mathsf{A}\cdot\mathsf{B})\cdot\mathsf{C}=\Big(\sum_{j=1}^{p}a_{ij}b_{jh}\Big)\cdot(c_{hk})=\Big(\sum_{h=1}^{r}\Big[\sum_{j=1}^{p}a_{ij}b_{jh}\Big]c_{hk}\Big)=\Big(\sum_{h=1}^{r}\sum_{j=1}^{p}[a_{ij}b_{jh}]c_{hk}\Big)=$$
$$=\Big(\sum_{h=1}^{r}\sum_{j=1}^{p}a_{ij}[b_{jh}\cdot c_{hk}]\Big)=\Big(\sum_{j=1}^{p}a_{ij}\sum_{h=1}^{r}b_{jh}c_{hk}\Big)=(a_{ij})\cdot\Big(\sum_{h=1}^{r}b_{jh}c_{hk}\Big)=\mathsf{A}\cdot(\mathsf{B}\cdot\mathsf{C}).\quad\square$$

Lema 1.2. *Nech matice* $\mathbf{A}, \mathbf{B}$ *sú typu* $m \times p$ *a matica* $\mathbf{C}$ *typu* $p \times n$. *Potom*

$$(\mathbf{A}+\mathbf{B}) \cdot \mathbf{C} = \mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}. \tag{1.8}$$

Nech naopak matica $\mathbf{C}$ *je typu* $m \times p$ *a matice* $\mathbf{A}, \mathbf{B}$ *typu* $p \times n$. *Potom*

$$\mathbf{C} \cdot (\mathbf{A}+\mathbf{B}) = \mathbf{C} \cdot \mathbf{A} + \mathbf{C} \cdot \mathbf{B}. \tag{1.9}$$

Dôkaz prenecháme čitateľovi. □

Poznámka 1.3. Z liem 1.1 resp. 1.2 vidieť, že násobenie matíc je asociatívne resp. násobenie matíc je distributívne vzhľadom na sčítanie matíc. Na nasledujúcom príklade sa presvedčíme, že násobenie matíc je nekomutatívne, t.j. $\mathbf{A} \cdot \mathbf{B}$ sa nemusí vždy rovnať $\mathbf{B} \cdot \mathbf{A}$ i keď sú oba súčiny definované.

$$\begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ -1 & 5 \end{pmatrix}.$$

Veta 1.3. *Nech* $\mathcal{M}_n(F)$ *je množina všetkých matíc typu* $n \times n$ *(kde* $n \geq 2$*) nad poľom* F. *Potom štruktúra* $(\mathcal{M}_n(F), +, \cdot)$ *je nekomutatívny okruh s jednotkovým prvkom obsahujúci netriviálne delitele nuly.*

Dôkaz. Z vety 1.1 vyplýva, že $(\mathcal{M}_n(F), +)$ je abelovská grupa. Z definície 1.5 a lemy 1.1 vyplýva, že $(\mathcal{M}_n(F), \cdot)$ je pologrupa. Podľa lemy 1.2 platia oba distributívne zákony. Ľahko sa presvedčíme, že $\mathbf{J}_n$ je neutrálny prvok vzhľadom na operáciu násobenia. Podobne ľahko overíme, že okruh má netriviálne delitele nuly (t.j. nie je obor integrity). Napr. v $(\mathcal{M}_2(R), +, \cdot)$ je

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

□

Cvičenia

1.1. Nech $\mathbf{A}, \mathbf{B}, \mathbf{C}$ sú matice nad poľom racionálnych čísel

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

Vypočítajte

a) maticu $3\mathbf{A} + \frac{2}{3}\mathbf{B} - \mathbf{C}$,
b) maticu $\mathbf{X}$, keď platí $3\mathbf{A} + 2\mathbf{X} = 4\mathbf{B} + 3\mathbf{C}$.

1.2. Vypočítajte $2\mathbf{A}-3\mathbf{B}$, $\mathbf{AB}-\mathbf{BA}$, $\mathbf{AB}-\mathbf{A}$, $\mathbf{A}^3-\mathbf{B}^2$ ak

$$\mathbf{A}=\begin{pmatrix}1 & -1\\ 0 & 3\end{pmatrix}, \qquad \mathbf{B}=\begin{pmatrix}2 & 2\\ 1 & 2\end{pmatrix}.$$

1.3. Nájdite všetky matice $\mathbf{A}$ typu 2×2 nad poľom reálnych čísel, pre ktoré platí

a) $\mathbf{A}\cdot\mathbf{A}=\mathbf{0}_{2,2}$,
b) $\mathbf{A}\cdot\mathbf{A}=\mathbf{A}$,
c) $\mathbf{A}\cdot\mathbf{A}=\mathbf{J}_2$.

1.4. Dokážte, že platí

a) $(\mathbf{A}+\mathbf{B})^T=\mathbf{A}^T+\mathbf{B}^T$,
b) $(\mathbf{AB})^T=\mathbf{B}^T\cdot\mathbf{A}^T$,
c) $(s\mathbf{A})^T=s\mathbf{A}^T$,

kde $\mathbf{A},\mathbf{B}$ sú matice (vhodného typu) nad poľom F a $s\in F$.

1.5. Vypočítajte

a) $\begin{pmatrix}2 & -3\\ 1 & 2\end{pmatrix}^3$ b) $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^n$, c) $\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}^k$,

1.6. Dokážte, že pre každú maticu

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

platí

$$\mathbf{A}^2-(a+d)\mathbf{A}+(ad-bc)\mathbf{J}_2=\mathbf{0}_{2,2}.$$

1.7. Nájdite všetky matice $\mathbf{X},\mathbf{Y}$, pre ktoré platí $\mathbf{XA}=\mathbf{AX}$, $\mathbf{YB}=\mathbf{BY}$, keď

$$\mathbf{A}=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \quad \mathbf{B}=\begin{pmatrix}1 & -1\\ 3 & 2\end{pmatrix}.$$

1.8. Nech $M_2(R)$ je vektorový priestor matíc typu (2×2) nad poľom reálnych čísel. Určte dimenziu tohto priestoru, zvoľte v ňom bázu a vypočítajte súradnice vektora

$$\mathbf{A}=\begin{pmatrix}1 & -3\\ 2 & 8\end{pmatrix}$$

v tejto báze.

§ 2. Sústavy lineárnych rovníc

V príklade 1.8 kapitoly 2 sme definovali lineárnu rovnicu s n neznámymi nad poľom F ako výrokovú formu φ definovanú vzťahom

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = a, \tag{2.1}$$

kde a je pevne zvolený prvok poľa F a ľavá strana výrokovej formy (2.1) je lineárna forma $f \in \boldsymbol{L}_n(F)$ (pozri príklad 1.7 kapitoly 2). Výroková forma φ teda každému vektoru $\boldsymbol{\alpha} = (x_1, x_2, \dots, x_n) \in \boldsymbol{V}_n(F)$ priraďuje výrok „hodnota formy f pre vektor $\boldsymbol{\alpha}$ je a“. V príklade 1.8 kapitoly 2 sme dokázali, že množina $\boldsymbol{R}_n(F)$ všetkých lineárnych rovníc o n neznámych tvorí vektorový priestor nad F.

Definícia 2.1. Vektor $\boldsymbol{\tau} = (t_1, t_2, \dots, t_n) \in \boldsymbol{V}_n(F)$ nazývame *riešením* rovnice (2.1) ak výrok $a_1t_1 + a_2t_2 + \dots a_nt_n = a$ je pravdivý.

Definícia 2.2. Rovnice

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + \ & a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + \ & a_{2n}x_n = b_2, \\ \vdots \qquad & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + \ & a_{mn}x_n = b_m, \end{aligned} \tag{2.2}$$

nazývame *sústavou* $\mathcal{S}$ *m rovníc s n neznámymi nad* F. Teda $\mathcal{S} \subseteq \boldsymbol{R}_n(F)$.

Vektor $\boldsymbol{\tau} = (t_1, t_2, \dots, t_n)$ nazývame *riešením sústavy* (2.2), ak je riešením každej rovnice danej sústavy. Nech S je množina všetkých riešení sústavy (2.2). Je jasné, že $S \subseteq \boldsymbol{V}_n(F)$. Ak S obsahuje aspoň jeden vektor, t.j. $S \neq \emptyset$, hovoríme, že sústava $\mathcal{S}$ je *riešiteľná.* V prípade $S = \emptyset$, hovoríme, že sústava (2.2) nemá riešenie.

Poznámka 2.1. Miesto „sústava m rovníc s n neznámymi“ hovoríme tiež „systém m rovníc s n neznámymi“.

Poznámka 2.2. Spolu so sústavou rovníc musí byť vždy udané pole nad akým sústavu uvažujeme. Napr. sústava

$$\begin{aligned} \bar{2}x + \bar{3}y &= \bar{1}, \\ \bar{4}x + \bar{1}y &= \bar{3}, \end{aligned} \tag{2.3}$$

nad poľom Z_5 je iná, ako sústava formálne napísaná rovnako, ale nad poľom Z_7. Ako uvidíme v príklade 2.1, táto sústava je nad Z_5 neriešiteľná, zatiaľ čo nad Z_7 má riešenie.

Definícia 2.3. Dve sústavy $\mathcal{S}$ a $\mathcal{S}'$ rovníc s n neznámymi sú ekvivalentné, ak majú tú istú množinu riešení, t.j. ak $S = S'$.

Veta 2.1. *Nech $\mathcal{S}$ je sústava rovníc* (2.2). *Nech sústava $\mathcal{S}'$ vznikne zo sústavy $\mathcal{S}$ konečnou postupnosťou operácií nasledovného typu:*

(i) *zmenou poradia rovníc sústavy,*
(ii) *násobením ľubovoľnej rovnice sústavy $\mathcal{S}$ nenulovým prvkom poľa F,*
(iii) *nahradením ľubovoľnej rovnice sústavy súčtom tejto rovnice a niektorej (inej) rovnice sústavy,*

potom sústavy $\mathcal{S}$ a $\mathcal{S}'$ sú ekvivalentné.

Dôkaz. Operáciou (i) sa zrejme nemôže zmeniť množina riešení sústavy $\mathcal{S}$. Keďže v poli F možno krátiť ľubovoľným nenulovým prvkom $c \in F$, majú rovnice $a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i$ a $c(a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n) = b_i c$ rovnakú množinu riešení. To znamená, ak vykonáme v $\mathcal{S}$ operáciu typu (ii) dostaneme sústavu $\mathcal{S}'$ takej vlastnosti, že každé riešenie sústavy $\mathcal{S}$ je aj riešením sústavy $\mathcal{S}'$ a naopak. Podobne v prípade (iii). Každé riešenie, ktoré vyhovuje rovnici

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i \tag{2.4}$$

ako aj rovnici

$$a_{j1}x_1 + a_{j2}x_2 + \cdots + a_{jn}x_n = b_j \tag{2.5}$$

vyhovuje zrejme aj ich súčtu

$$(a_{i1} + a_{j1})x_1 + (a_{i2} + a_{j2})x_2 + \cdots + (a_{in} + a_{jn})x_n = b_i + b_j. \tag{2.6}$$

Preto ak rovnicu (2.4) nahradíme súčtom rovníc (2.4) a (2.5) dostaneme sústavu $\mathcal{S}'$ takú, že každé riešenie sústavy $\mathcal{S}$ je aj riešením sústavy $\mathcal{S}'$. Pomocou operácie (ii) a (iii) ľahko prejdeme od sústavy $\mathcal{S}'$ k sústave $\mathcal{S}$. Menovite: rovnicu (2.5) násobíme číslom -1 (dostaneme ekvivalentnú sústavu $\mathcal{S}^*$) a potom ju sčítame s (2.6). Teda každé riešenie sústavy $\mathcal{S}'$ je aj riešením sústavy $\mathcal{S}$. Zvyšok dôkazu je zrejmý. □

Poznámka 2.3. Operácie (i), (ii), (iii) voláme elementárne operácie. Porovnaj operácie vo vete 3.5 kapitoly 2.

Príklad 2.1. Pomocou elementárnych operácií nájdeme riešenie sústavy (2.3) nad Z_5 i Z_7. Najprv nad poľom Z_5. Prvú rovnicu (2.3) násobme $\bar{3} \in Z_5$. Dostaneme

$$\begin{aligned} \bar{1}x + \bar{4}y &= \bar{3}, \\ \bar{4}x + \bar{1}y &= \bar{3}. \end{aligned}$$

Prvú rovnicu pripočítame k druhej rovnici. Dostaneme sústavu

$$\begin{aligned} \bar{1}x + \bar{4}y &= \bar{3}, \\ \bar{0}x + \bar{0}y &= \bar{1}. \end{aligned} \tag{2.7}$$

Druhej rovnici zrejme nevyhovuje žiadny vektor zo $\boldsymbol{V}_2(Z_5)$. Teda množina riešení sústavy (2.7) a teda aj (2.3) je prázdna.

Sústavu (2.3) teraz uvažujme nad Z_7. Prvú rovnicu (2.3) vynásobme $\bar{4} \in Z_7$. Dostaneme sústavu

$$\begin{aligned} \bar{1}x + \bar{5}y &= \bar{4}, \\ \bar{4}x + \bar{1}y &= \bar{3}. \end{aligned}$$

Pripočítaním $\bar{3}$-násobku prvej rovnice k druhej máme

$$\begin{aligned} \bar{x} + \bar{5}y &= \bar{4}, \\ \bar{0}x + \bar{2}y &= \bar{1}. \end{aligned}$$

Pripočítaním druhej rovnice k prvej máme

$$\begin{aligned} \bar{1}x + \bar{0}y &= \bar{5}, \\ \bar{0}x + \bar{2}y &= \bar{1}, \end{aligned}$$

odkiaľ hneď vidieť, že vektor $\boldsymbol{\tau} = (\bar{5}, \bar{4})$ je jediným riešením sústavy (2.3).

Cvičenia

2.1. Sústavu

$$\begin{aligned} \bar{1}x + \bar{2}y &= \bar{2}, \\ \bar{2}x + \bar{1}y &= \bar{1} \end{aligned}$$

riešte nad poľom Z_3 a potom nad poľom Z_7.

2.2 Postupom ako v príklade 2.1 riešte nad poľom Z_5 nasledovné sústavy rovníc.

$$a)\quad \begin{aligned} \bar{3}x + \bar{2}y + \bar{4}z &= \bar{1}, \\ \bar{1}x + \bar{2}y + \bar{3}z &= \bar{2}, \\ \bar{4}x + \bar{4}y + \bar{2}z &= \bar{4}, \end{aligned} \qquad b)\quad \begin{aligned} \bar{2}x + \bar{2}y + \bar{3}z &= \bar{4}, \\ \bar{1}x + \bar{3}y + \bar{4}z &= \bar{0}, \\ \bar{1}x + \bar{2}y + \bar{3}z &= \bar{4}. \end{aligned}$$

2.3. Nech sústava rovníc

$$\begin{aligned} a_1x + b_1y &= c_1, \\ a_2x + b_2y &= c_2, \end{aligned}$$

kde $a_1, b_1, c_1, a_2, b_2, c_2 \in R$ má dve rôzne riešenia. Potom má nekonečne veľa riešení. Dokážte.

§ 3. Hodnosť matice

Uvažujme o matici

$$\begin{pmatrix} a_{11}, & a_{12}, \cdots, & a_{1n} \\ a_{21}, & a_{22}, \cdots, & a_{2n} \\ \vdots & & \\ a_{i1}, & a_{i2}, \cdots, & a_{in} \\ \vdots & & \\ a_{j1}, & a_{j2}, \cdots, & a_{jn} \\ \vdots & & \\ a_{m1}, & a_{m2}, \cdots, & a_{mn} \end{pmatrix}$$

typu $m \times n$ nad poľom F. Ako sme už povedali v paragrafe 1, riadky $\boldsymbol{\varrho}_1, \boldsymbol{\varrho}_2, \ldots, \boldsymbol{\varrho}_m$ matice $\mathbf{A}$ môžeme považovať za prvky vektorového priestoru $\boldsymbol{V}_n(F)$ a stĺpce $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_n$, za prvky vektorového priestoru $\boldsymbol{V}_m(F)$. Riadky generujú podpriestor $\boldsymbol{R} = [\boldsymbol{\varrho}_1, \boldsymbol{\varrho}_2, \ldots, \boldsymbol{\varrho}_m]$ priestoru $\boldsymbol{V}_n(F)$, stĺpce generujú podpriestor $\boldsymbol{S} = [\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_n]$ priestoru $\boldsymbol{V}_m(F)$. Dokážeme, že $d(\boldsymbol{R}) = d(\boldsymbol{S})$. Aby sme to dokázali, pripomeňme si najskôr elementárne operácie z vety 3.5 kapitoly 2. Tam sme dokázali, že ak sústava $\mathcal{T}$ vznikne zo sústavy $\mathcal{S}$ vektorov $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_k\}$, kde $\boldsymbol{\alpha}_i \in \boldsymbol{V}(F)$ jednou z týchto operácií:

(3.1)
(a) zmenou poradia vektorov sústavy $\mathcal{S}$,
(b) zámenou vektora $\boldsymbol{\alpha}_i$ za vektor $s\boldsymbol{\alpha}_i$, kde $0 \neq s \in F$,
(c) zámenou vektora $\boldsymbol{\alpha}_i$ za vektor $\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_j$,

tak $[\mathcal{T}] = [\mathcal{S}]$.

Ak operácie (3.1) aplikujeme na riadky matice $\mathbf{A}$, hovoríme o elementárnych riadkových operáciách (ero), ak na stĺpce, tak o elementárnych stĺpcových operáciách (eso). Dokážeme nasledujúce dve lemy.

Lema 3.1. *Nech matica* $\mathbf{B}$ *vznikne z matice* $\mathbf{A}$ *tak, že na nej vykonáme riadkové alebo stĺpcové operácie* (ero *alebo* eso)*. Potom riadky (stĺpce) matice* $\mathbf{A}$ *generujú podpriestor priestoru* $\boldsymbol{V}_n(F)$ $(\boldsymbol{V}_m(F))$ *tej istej dimenzie ako riadky (stĺpce) matice* $\mathbf{B}$.

Dôkaz. Nech matica $\mathbf{A} = (a_{ik})$ je typu $m \times n$ s riadkami $\boldsymbol{\varrho}_1, \boldsymbol{\varrho}_2, \ldots, \boldsymbol{\varrho}_m$ a stĺpcami $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_n$. Po vykonaní ero alebo eso dostaneme maticu $\mathbf{B} = (b_{ik})$, ktorá zrejme je tiež typu $m \times n$ s riadkami $\boldsymbol{\varrho}'_1, \boldsymbol{\varrho}'_2, \ldots, \boldsymbol{\varrho}'_m$ a stĺpcami $\boldsymbol{\sigma}'_1, \boldsymbol{\sigma}'_2, \ldots, \boldsymbol{\sigma}'_n$. Nech $[\boldsymbol{\varrho}_1, \boldsymbol{\varrho}_2, \ldots, \boldsymbol{\varrho}_m] = \boldsymbol{R}$, $[\boldsymbol{\varrho}'_1, \boldsymbol{\varrho}'_2, \ldots, \boldsymbol{\varrho}'_m] = \boldsymbol{R}'$. Dokážeme, že oba podpriestory $\boldsymbol{R}$ i $\boldsymbol{R}'$ priestoru $\boldsymbol{V}_n(F)$ majú rovnakú dimenziu.

Ak matica $\mathbf{B}$ vznikla z matice $\mathbf{A}$ len riadkovými operáciami, tak podľa vety 3.5 kapitoly 2 je $\boldsymbol{R} = \boldsymbol{R}'$ a teda tiež $d(\boldsymbol{R}) = d(\boldsymbol{R}')$. Stačí teda uvažovať stĺpcové operácie (eso). Nech pre určitosť $d(\boldsymbol{R}) = h$ a nech $\boldsymbol{\varrho}_{j_1}, \boldsymbol{\varrho}_{j_2}, \ldots, \boldsymbol{\varrho}_{j_h}$ sú lineárne nezávislé riadky matice $\boldsymbol{A}$, ktoré generujú podpriestor $\boldsymbol{R}$. Ide teda o riadky

$$\begin{aligned} \boldsymbol{\varrho}_{j_1} &= (a_{j_1 1}, a_{j_1 2}, \ldots, a_{j_1 k}, \ldots, a_{j_1 l}, \ldots, a_{j_1 n}) \\ \boldsymbol{\varrho}_{j_2} &= (a_{j_2 1}, a_{j_2 2}, \ldots, a_{j_2 k}, \ldots, a_{j_2 l}, \ldots, a_{j_2 n}) \\ &\;\vdots \\ \boldsymbol{\varrho}_{j_h} &= (a_{j_h 1}, a_{j_h 2}, \ldots, a_{j_h k}, \ldots, a_{j_h l}, \ldots, a_{j_h n}) \end{aligned} \tag{3.2}$$

Podľa predpokladu sú riadky $\boldsymbol{\varrho}_{j_1}, \ldots, \boldsymbol{\varrho}_{j_h}$ lineárne nezávislé, teda rovnica

$$c_1\boldsymbol{\varrho}_{j_1} + c_2\boldsymbol{\varrho}_{j_2} + \cdots + c_h\boldsymbol{\varrho}_{j_h} = (0, 0, \ldots, 0) \tag{3.3}$$

je splnená, len ak $c_1 = c_2 = \cdots = c_h = 0$. Rovnicu (3.3) možno napísať ako sústavu rovníc (prečo?):

$$\begin{aligned} c_1 a_{j_1 1} + c_2 a_{j_2 1} + \cdots + c_h a_{j_h 1} &= 0, \\ c_1 a_{j_1 2} + c_2 a_{j_2 2} + \cdots + c_h a_{j_h 2} &= 0, \\ &\vdots \\ c_1 a_{j_1 k} + c_2 a_{j_2 k} + \cdots + c_h a_{j_h k} &= 0, \\ &\vdots \\ c_1 a_{j_1 l} + c_2 a_{j_2 l} + \cdots + c_h a_{j_h l} &= 0, \\ &\vdots \\ c_1 a_{j_1 n} + c_2 a_{j_2 n} + \cdots + c_h a_{j_h n} &= 0, \end{aligned} \tag{3.4}$$

ktorej vyhovuje len $c_1 = c_2 = \cdots = c_h = 0$ (t.j. má jediné riešenie $(0, 0, \ldots, 0)$. Všimnime si, že jednotlivé stĺpce v (3.2) sú koeficienty jednotlivých rovníc v (3.4). Ak vykonáme v matici $\mathbf{A}$ eso typu (a), (b) alebo (c), vykonáme tým v sústave (3.4) ekvivalentnú úpravu typu (a), (b) alebo (c). Dostaneme maticu $\mathbf{B}$ s riadkami $\boldsymbol{\varrho}'_{j_1}, \boldsymbol{\varrho}'_{j_2}, \ldots, \boldsymbol{\varrho}'_{j_h}$, ktorej zodpovedá sústava ekvivalentná so sústavou (3.4) a teda podľa vety 3.1 majúca jediné riešenie $c_1 = c_2 = \cdots = c_h = 0$. To znamená, že aj riadky $\boldsymbol{\varrho}'_{j_1}, \boldsymbol{\varrho}'_{j_2}, \ldots, \boldsymbol{\varrho}'_{j_h}$ matice $\mathbf{B}$ sú lineárne nezávislé. Odtiaľ máme $d(\boldsymbol{R}') \geqq h = d(\boldsymbol{R})$. Stačí si uvedomiť, že maticu $\mathbf{A}$ môžeme dostať z matice $\mathbf{B}$ tiež pomocou vhodne zvolených eso (čitateľ si rozmyslí, ako to urobíme). Preto aj $d(\boldsymbol{R}) = h \geqq d(\boldsymbol{R}')$. Teda $d(\boldsymbol{R}) = d(\boldsymbol{R}')$. Vidíme, že vykonaním operácií eso sa dimenzia podpriestoru generovaného riadkami matice nemení.

Analogickými úvahami sa tiež presvedčíme, že ak $[\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_n] = \boldsymbol{S}$ a $[\boldsymbol{\sigma}'_1, \boldsymbol{\sigma}'_2, \ldots, \boldsymbol{\sigma}'_n] = \boldsymbol{S}'$, tak $d(\boldsymbol{S}) = d(\boldsymbol{S}')$. □

Lema 3.2. *Nech $\boldsymbol{\varrho}_1, \boldsymbol{\varrho}_2, \ldots, \boldsymbol{\varrho}_m$ sú riadky a $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_n$ stĺpce matice $\mathbf{A}$ typu $m \times n$. Nech $\boldsymbol{R} = [\boldsymbol{\varrho}_1, \boldsymbol{\varrho}_2, \ldots, \boldsymbol{\varrho}_m]$ a $\boldsymbol{S} = [\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_n]$. Potom platí $d(\boldsymbol{R}) = d(\boldsymbol{S})$.*

Dôkaz. Ak matica $\mathbf{A}$ je nulová matica, zrejme platí $d(\boldsymbol{R}) = d(\boldsymbol{S}) = 0$, t.j. lema platí. Nech teda $\mathbf{A} \neq \mathbf{0}_{m,n}$.

Dôkaz vykonáme tak, že maticu $\mathbf{A}$ transformujeme postupne pomocou ero resp. eso a dostaneme postupnosť matíc

$$\mathbf{A} \to \mathbf{A}_1 \to \mathbf{A}_2 \to \cdots \to \mathbf{A}_l \to \cdots \to \mathbf{A}_d, \tag{3.5}$$

pričom matica $\mathbf{A}_d$ bude takého tvaru, že v nej ľahko určíme $d(\boldsymbol{R})$ i $d(\boldsymbol{S})$.

Najprv pomocou výmen riadkov a stĺpcov dosiahneme, že matica $\mathbf{A}_1$ je tvaru

$$\mathbf{A} = \begin{pmatrix} a_{11}, & a_{12}, & a_{13}, & \cdots, & a_{1n} \\ a_{21}, & a_{22}, & a_{23}, & \cdots, & a_{2n} \\ \vdots & & & & \\ a_{m1}, & a_{m2}, & a_{m3}, & \cdots, & a_{mn} \end{pmatrix},$$

kde $a_{11} \neq 0$. To je vždy možné, lebo $\mathbf{A} \neq \mathbf{0}_{m,n}$. Potom robíme nasledovné ero. Ak je $a_{21} \neq 0$, vynásobíme prvý riadok $-\frac{a_{21}}{a_{11}}$ a pripočítame ho k druhému riadku. Potom prvý riadok vynásobíme $-\frac{a_{11}}{a_{21}}$. Ak je $a_{21} = 0$, necháme prvý i druhý riadok bez zmeny. Ŕalej, ak je $a_{31} \neq 0$, vynásobíme prvý riadok $-\frac{a_{31}}{a_{11}}$ a pripočítame ho tretiemu riadku. Potom prvý riadok vynásobíme $-\frac{a_{11}}{a_{31}}$. Ak je $a_{31} = 0$, necháme prvý aj tretí riadok bez zmeny. Takto postupujeme ďalej, kým nedostaneme maticu tvaru

$$\begin{pmatrix} a_{11}, & a_{12}, & a_{13}, & \cdots, & a_{1n} \\ 0, & a'_{22}, & a'_{23}, & \cdots, & a'_{2n} \\ 0, & a'_{32}, & a'_{33}, & \cdots, & a'_{3n} \\ \vdots & & & & \\ 0, & a'_{m2}, & a'_{m3}, & \cdots, & a'_{mn} \end{pmatrix},$$

v ktorej sme výmenou riadkov a stĺpcov dosiahli (ak to bolo treba), že $a'_{22} \neq 0$. Ak $a'_{32} \neq 0$, tak druhý riadok vynásobíme $-\frac{a'_{32}}{a'_{22}}$ a pripočítame ho k tretiemu riadku. Potom druhý riadok vynásobíme $-\frac{a'_{22}}{a'_{32}}$. V postupe pokračujeme ďalej, kým nedostaneme maticu

$$\mathbf{A}_3 = \begin{pmatrix} a_{11}, & a_{12}, & a_{13}, & \cdots, & a_{1n} \\ 0, & a'_{22}, & a'_{23}, & \cdots, & a'_{2n} \\ 0, & 0, & a''_{33}, & \cdots, & a''_{3n} \\ \vdots & & & & \\ 0, & 0, & a''_{m3}, & \cdots, & a''_{mn} \end{pmatrix},$$

kde, ak to bolo treba, sme urobili výmenu riadkov a stĺpcov, aby $a''_{33} \neq 0$. V postupe pokračujeme pre tretí a ďalšie stĺpce dovtedy, kým nedostaneme maticu tvaru

$$\mathbf{A}_l = \begin{pmatrix} b_{11}, & b_{12}, & b_{13}, & \cdots, & b_{1h}, & b_{1,h+1}, & \cdots, & b_{1n} \\ 0, & b_{22}, & b_{23}, & \cdots, & b_{2h}, & b_{2,h+1}, & \cdots, & b_{2n} \\ 0, & 0, & b_{33}, & \cdots, & b_{3h}, & b_{3,h+1}, & \cdots, & b_{3n} \\ 0, & 0, & 0, & \cdots, & & & & \\ \vdots & & & & & & & \\ 0, & 0, & 0, & \cdots, & b_{hh}, & b_{h,h+1}, & \cdots, & b_{hn} \\ 0, & 0, & 0, & \cdots, & 0, & 0, & \cdots, & 0 \\ \vdots & & & & & & & \\ 0, & 0, & 0, & \cdots, & 0, & 0, & \cdots, & 0 \end{pmatrix},$$

kde $b_{ii} \neq 0$ pre $i = 1, 2, \ldots, h$. Zrejme $b_{11} = a_{11}$, $b_{22} = a'_{22}$, $b_{33} = a''_{33}$ atď. Maticu $\mathbf{A}_l$ ďalej transformujeme elementárnymi stĺpcovými operáciami (eso), tak, že ak $b_{12} \neq 0$ tak prvý stĺpec násobíme $-\frac{b_{12}}{b_{11}}$ a pripočítame ho k druhému stĺpcu, atď., čím dosiahneme v prvom riadku okrem b_{11} samé nulové prvky. V postupe pokračujeme, až dostaneme maticu tvaru

$$\mathbf{A}_d = \begin{pmatrix} b_{11}, & 0, & 0, & \cdots, & 0, & 0, & \cdots, & 0 \\ 0, & b_{22}, & 0, & \cdots, & 0, & 0, & \cdots, & 0 \\ 0, & 0, & b_{33}, & \cdots, & 0, & 0, & \cdots, & 0 \\ \vdots & & & & & & & \\ 0, & 0, & 0, & \cdots, & b_{hh}, & 0, & \cdots, & 0 \\ 0, & 0, & 0, & \cdots, & 0, & 0, & \cdots, & 0 \\ \vdots & & & & & & & \\ 0, & 0, & 0, & \cdots, & 0, & 0, & \cdots, & 0 \end{pmatrix},$$

kde $b_{ii} \neq 0$ pre $i = 1, 2, \dots, h$. Matica $\mathbf{A}_d$ zrejme obsahuje h lineárne nezávislých riadkov i stĺpcov, t.j. dimenzia vektorových podpriestorov generovaných riadkami i stĺpcami matice je rovná h. Keďže matica $\mathbf{A}_d$ vznikla z matice $\mathbf{A}$ len postupným vykonávaním ero a eso , podľa lemy 3.1 aj $d(\boldsymbol{R}) = d(\boldsymbol{S}) = h$, čo bolo treba dokázať. □

Lema 3.2 nám umožňuje vysloviť nasledujúcu definíciu.

Definícia 3.1. Nech $\mathbf{A}$ je matica typu $m \times n$ s riadkami $\boldsymbol{\varrho}_1, \boldsymbol{\varrho}_2, \dots, \boldsymbol{\varrho}_m$ a stĺpcami $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \dots, \boldsymbol{\sigma}_n$. Nech $\boldsymbol{R} = [\boldsymbol{\varrho}_1, \boldsymbol{\varrho}_2, \dots, \boldsymbol{\varrho}_m]$ a $\boldsymbol{S} = [\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \dots, \boldsymbol{\sigma}_n]$. Potom hodnotu $h = d(\boldsymbol{R}) = d(\boldsymbol{S})$ nazývame *hodnosťou* matice $\mathbf{A}$. Označujeme $h = h(\mathbf{A})$.

Poznámka 3.1. Niekedy sa definuje *riadková hodnosť* matice $h_r(\mathbf{A}) = d(\boldsymbol{R})$ a *stĺpcová hodnosť* $h_s(\mathbf{A}) = d(\boldsymbol{S})$ a dokáže sa, že $h_r(\mathbf{A}) = h_s(\mathbf{A})$.

Poznámka 3.2. Podľa definície 3.1 matica $\mathbf{A}$ má hodnosť h, ak v nej existuje h lineárne nezávislých riadkov (stĺpcov) a každý väčší počet riadkov (stĺpcov) matice je už lineárne závislý.

Poznámka 3.3. Dôkaz lemy 3.2 nám poskytuje postup na výpočet hodnosti matice. Matice (3.5) sú takej vlastnosti, že každú možno dostať z inej pomocou ero resp. eso. Takéto matice voláme ekvivalentné, čo často označujeme $\mathbf{A} \sim \mathbf{A}_1 \sim \mathbf{A}_2 \sim \cdots \sim \mathbf{A}_l \sim \cdots \sim \mathbf{A}_d$. Pre ne platí $h(\mathbf{A}) = h(\mathbf{A}_1) = h(\mathbf{A}_2) = \cdots = h(\mathbf{A}_l) = \cdots = h(\mathbf{A}_d)$. Pri výpočte hodnosti matice môžeme postup prerušiť pri matici $\mathbf{A}_l$. Hodnosť matice $\mathbf{A}$ sa rovná počtu nenulových riadkov matice $\mathbf{A}_l$. O matici $\mathbf{A}_l$ často hovoríme, že je upravená na lichobežníkový tvar. Je to preto, že nenulové prvky $b_{11}, b_{22}, \dots, b_{hh}$ a prvky, nachádzajúce sa vpravo od nich, vytvárajú akýsi „lichobežník“. Pravda môže sa stať, že „dolná základňa lichobežníka“ obsahuje len jeden prvok b_{hh}. Pri výpočte hodnosti nemusíme vypisovať nulové riadky matíc. Ukážeme si to na príklade.

Príklad 3.1. Nájdeme hodnosť matice $\mathbf{A}$ typu 4×5.

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 4 & 2 & 3 \\ 2 & 0 & \frac{1}{2} & 4 & 3 \\ 4 & 1 & 5 & 10 & 9 \\ 2 & 1 & \frac{9}{2} & 6 & 6 \end{pmatrix}.$$

Elementárnymi riadkovými resp. stĺpcovými operáciami upravujeme:

$$\begin{pmatrix} 0 & 1 & 4 & 2 & 3 \\ 2 & 0 & \frac{1}{2} & 4 & 3 \\ 4 & 1 & 5 & 10 & 9 \\ 2 & 1 & \frac{9}{2} & 6 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 4 & 2 & 3 \\ 0 & 2 & \frac{1}{2} & 4 & 3 \\ 1 & 4 & 5 & 10 & 9 \\ 1 & 2 & \frac{9}{2} & 6 & 6 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & 0 & 4 & 2 & 3 \\ 0 & 2 & \frac{1}{2} & 4 & 3 \\ 0 & 4 & 1 & 8 & 6 \\ 0 & 2 & \frac{1}{2} & 4 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 4 & 2 & 3 \\ 0 & 2 & \frac{1}{2} & 4 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Vidíme, že $h(\mathbf{A}) = 2$.

Príklad 3.2. Sú dané vektory $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\delta} \in \boldsymbol{V}_5(Q)$ takto:

$$\begin{aligned} \boldsymbol{\alpha} &= (0,\ 1,\ 4,\ 2,\ 3), \\ \boldsymbol{\beta} &= (2,\ 0,\ \frac{1}{2},\ 4,\ 3), \\ \boldsymbol{\gamma} &= (4,\ 1,\ 5,\ 10,\ 9), \\ \boldsymbol{\delta} &= (2,\ 1,\ \frac{9}{5},\ 6,\ 6). \end{aligned}$$

Vypočítame dimenziu podpriestoru, ktorý dané vektory generujú. Dané vektory možno pokladať za riadky matice. Dimenzia daného vektorového priestoru sa rovná hodnosti danej matice. V našom prípade je to matica $\mathbf{A}$ z predchádzajúceho príkladu. Dimenzia podpriestoru je preto 2.

Príklad 3.3. Nech $\boldsymbol{P} = [\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2]$, $\boldsymbol{S} = [\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \boldsymbol{\beta}_3]$ sú dva podpriestory vektorového priestoru $\boldsymbol{V}_5(R)$. Vypočítajme dimenziu priestorov $\boldsymbol{P} \cap \boldsymbol{S}$ a $\boldsymbol{P} \vee \boldsymbol{S}$, keď je dané

$$\begin{aligned} \boldsymbol{\alpha}_1 &= (1,\ -2,\ 3,\ 4,\ 2), \\ \boldsymbol{\alpha}_2 &= (2,\ 3,\ 3,\ 0,\ 1), \\ \boldsymbol{\beta}_1 &= (-1,\ -5,\ 0,\ 4,\ 1), \\ \boldsymbol{\beta}_2 &= (2,\ 2,\ 3,\ 1,\ 1), \\ \boldsymbol{\beta}_3 &= (2,\ 1,\ 1,\ 0,\ 0). \end{aligned}$$

Zrejme $\boldsymbol{P} \vee \boldsymbol{S} = [\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \boldsymbol{\beta}_3]$. Aby sme vypočítali $d(\boldsymbol{P} \vee \boldsymbol{S})$, stačí zistiť hodnosť matice

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

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

$$\rightarrow \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & -3 & -1 & -3 \\ 0 & 0 & -2 & -2 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & -3 & -1 & -3 \\ 0 & 0 & 0 & -\frac{4}{3} & 1 \end{pmatrix},$$

kde pri prvej úprave sme dvojnásobok prvého riadku odpočítali od druhého, štvrtého a piateho riadku a pripočítali prvý riadok k tretiemu; pri druhej úprave sme druhý riadok pripočítali k tretiemu a odpočítali od štvrtého a piateho riadku; pri tretej vynechali nulový riadok a vymenili poradie riadkov atď. Teda $d(\boldsymbol{P} \vee \boldsymbol{S}) = 4$. Keď si uvedomíme, že prvé dva riadky našej matice sú vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2$ už po prvej úprave matice $\mathbf{A}$ vidíme $d(\boldsymbol{P}) = 2$. Treba vypočítať dimenziu podpriestoru $\boldsymbol{S}$. Zistíme hodnosť matice:

$$\mathbf{B} = \begin{pmatrix} -1 & -5 & 0 & 4 & 1 \\ 2 & 2 & 3 & 1 & 1 \\ 2 & 1 & 1 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & -5 & 0 & 4 & 1 \\ 0 & -8 & 3 & 9 & 3 \\ 0 & -9 & 1 & 8 & 2 \end{pmatrix} \rightarrow$$

$$\rightarrow \begin{pmatrix} -1 & 0 & -5 & 4 & 1 \\ 0 & 1 & -9 & 8 & 2 \\ 0 & 3 & -8 & 9 & 3 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & 0 & -5 & 4 & 1 \\ 0 & 1 & -9 & 8 & 2 \\ 0 & 0 & 19 & -15 & -3 \end{pmatrix}.$$

Teda je $d(\boldsymbol{S}) = 3$. Podľa vety 4.4 kapitoly 2 je $d(\boldsymbol{P} \cap S) + d(\boldsymbol{P} \vee \boldsymbol{S}) = d(\boldsymbol{P}) + d(\boldsymbol{S})$, t.j. $d(\boldsymbol{P} \cap \boldsymbol{S}) + 4 = 2 + 3$, odkiaľ $d(\boldsymbol{P} \cap \boldsymbol{S}) = 1$.

Cvičenia

3.1. Vypočítajte hodnosť nasledujúcich matíc (nad poľom Q).

$$\begin{pmatrix} 1 & -3 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 2 & -7 \\ 6 & -21 \end{pmatrix}, \begin{pmatrix} \frac{2}{3} & \frac{11}{8} \\ \frac{10}{21}, & \frac{55}{56} \end{pmatrix},$$

$$\begin{pmatrix} 1 & -1 & 3 \\ 4 & 5 & 8 \\ -3 & -6 & -5 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 8 & 2 & 1 & 0 \\ 4 & 5 & 3 & 3 & 2 & 1 \\ 5 & 8 & 10 & 1 & 1 & -3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & -2 & 7 & 5 & 8 & 0 & 3 \\ 1 & 1 & -2 & 3 & 6 & 5 & 4 \\ 2 & -3 & 6 & 7 & -1 & 0 & 8 \\ 1 & -4 & 8 & 4 & -7 & -5 & 4 \\ 0 & 2 & -1 & 1 & 15 & 5 & -1 \end{pmatrix}.$$

3.2. Určte dimenziu vektorových priestorov generovaných nasledujúcimi skupinami vektorov:

a) $(1, -1, 3), (3, 0, 8), (4, 2, 0) \in \boldsymbol{V}_3(R)$,
b) $(2, 3, -5, 4), (1, 0, 3, 7), (1, 3, -8, -3), (4, 3, 1, 18) \in \boldsymbol{V}_4(R)$,
c) $(1, 1, -1, 3, 2), (4, 1, 1, -5, 7)$, $(2, 0, 0, -1, 5)$, $(8, 2, 0, 5, 1)$, $(-1, 0, -2, 7, 0) \in \boldsymbol{V}_5(R)$.

3.3. Vypočítajte dimenziu priestorov $\boldsymbol{P} \cap \boldsymbol{S}$ a $\boldsymbol{P} \vee \boldsymbol{S}$, keď je dané:

a) $\boldsymbol{P} = [(3, -1, 2), (2, 0, 1), (1, -1, 1)]$, $\boldsymbol{S} = [(1, 2, 3), (6, -4, 5), (4, -2, 3)]$,

b) $\boldsymbol{P} = \{(x_1, x_2, x_3);\ x_2 = 0\}$, $\boldsymbol{S} = \{(x_1, x_2, x_3);\ 4x_1 - x_2 = 0\}$,

kde $\boldsymbol{P}$ a $\boldsymbol{S}$ sú podpriestory priestoru $\boldsymbol{V}_3(R)$.

3.4. Prepočítajte si ešte raz cvičenie 4.5 v kapitole 2 s využitím pojmu hodnosť matice.

3.5. K vektorom $\boldsymbol{\alpha} = (1, -1, 3, 2)$, $\boldsymbol{\beta} = (2, 2, 1, 1)$ vektorového priestoru $\boldsymbol{V}_4(R)$ zvoľte dva vektory $\boldsymbol{\gamma}, \boldsymbol{\delta} \in \boldsymbol{V}_4(R)$ tak, aby množina $\{\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\delta}\}$ bola bázou priestoru $\boldsymbol{V}_4(R)$.

§ 4. Gaussova eliminačná metóda

Uvažujme o sústave lineárnych rovníc (nad poľom F)

$$
\begin{aligned}
a_{11}x_1 + \ a_{12}x_2 + \cdots + \ a_{1n}x_n &= b_1,\\
a_{21}x_1 + \ a_{22}x_2 + \cdots + \ a_{2n}x_n &= b_2,\\
&\ \vdots \\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m.
\end{aligned}
\tag{4.1}
$$

Sústavu (4.1) môžeme „maticovo“ zapísať takto (odôvodnite):

$$
\begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n}\\ a_{21}, & a_{22}, & \dots, & a_{2n}\\ \vdots & & & \\ a_{m1}, & a_{m2}, & \dots, & a_{mn} \end{pmatrix}
\begin{pmatrix} x_1\\ x_2\\ \vdots\\ x_n \end{pmatrix}
=
\begin{pmatrix} b_1\\ b_2\\ \vdots\\ b_m \end{pmatrix}.
\tag{4.2}
$$

Ak matice v rovnici (4.2) pomenujeme M, $\vec{\boldsymbol{x}}$ resp. $\vec{\boldsymbol{b}}$, môžeme sústavu (4.1) zapísať stručne

$$\mathsf{M} \cdot \vec{\boldsymbol{x}} = \vec{\boldsymbol{b}}. \tag{4.3}$$

Definícia 4.1. Maticu M z (4.3) nazývame *maticou sústavy* (4.3). Ak ju rozšírime o stĺpec $\vec{\boldsymbol{b}}$, dostaneme *rozšírenú maticu sústavy* M'. T.j.

$$
\mathsf{M} = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n}\\ a_{21}, & a_{22}, & \dots, & a_{2n}\\ \vdots & & & \\ a_{m1}, & a_{m2}, & \dots, & a_{mn} \end{pmatrix}, \quad
\mathsf{M}' = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n}, & b_1\\ a_{21}, & a_{22}, & \dots, & a_{2n}, & b_2\\ \vdots & & & & \\ a_{m1}, & a_{m2}, & \dots, & a_{mn}, & b_m \end{pmatrix}.
$$

Sústavu rovníc (4.1) niekedy zapisujeme aj v tvare

$$
\begin{pmatrix} a_{11}\\ a_{21}\\ \vdots\\ a_{m1} \end{pmatrix} x_1 +
\begin{pmatrix} a_{12}\\ a_{22}\\ \vdots\\ a_{m2} \end{pmatrix} x_2 + \cdots +
\begin{pmatrix} a_{1n}\\ a_{2n}\\ \vdots\\ a_{mn} \end{pmatrix} x_n =
\begin{pmatrix} b_1\\ b_2\\ \vdots\\ b_m \end{pmatrix}
\tag{4.4}
$$

alebo stručnejšie

$$\boldsymbol{\sigma}_1 x_1 + \boldsymbol{\sigma}_2 x_2 + \cdots + \boldsymbol{\sigma}_n x_n = \vec{\boldsymbol{b}}, \tag{4.5}$$

kde sme stĺpce matice $\mathbf{M}'$ označili $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_n, \vec{\boldsymbol{b}}$.

V paragrafe 2 sme vysvetlili, čo je riešením sústavy (4.1). Povedali sme, že sústava (4.1) je riešiteľná, ak množina S riešení sústavy je neprázdna. Naopak, ak $S = \emptyset$, hovoríme, že sústava nemá riešenie. O tom, kedy je sústava (4.1) riešiteľná, hovorí nasledujúca veta.

Veta 4.1 (Frobeniova). *Sústava lineárnych rovníc* (4.1) *má riešenie práve vtedy, keď* $h(\mathbf{M}) = h(\mathbf{M}')$ *(hodnosť matice sústavy sa rovná hodnosti rozšírenej matice sústavy).*

Dôkaz. I. Nech sústava (4.1) má riešenie $\boldsymbol{\tau} = (t_1, t_2, \ldots, t_n)$. Potom podľa (4.5) platí $\boldsymbol{\sigma}_1 t_1 + \boldsymbol{\sigma}_2 t_2 + \cdots + \boldsymbol{\sigma}_n t_n = \vec{\boldsymbol{b}}$, t.j. posledný stĺpec matice $\mathbf{M}'$ je lineárnou kombináciou ostatných stĺpcov matice a tak $h(\mathbf{M}) = h(\mathbf{M}')$ (pozri cvičenie 4.7 kapitoly 2).

II. Nech naopak v sústave (4.1) platí $h(\mathbf{M}) = h(\mathbf{M}') = h$. Nech $\boldsymbol{\sigma}_{i_1}, \boldsymbol{\sigma}_{i_2}, \ldots, \boldsymbol{\sigma}_{i_h}$ je h lineárne nezávislých stĺpcov matice $\mathbf{M}$. Keďže $h(\mathbf{M}') = h$, vidíme, že $h+1$ stĺpcov $\boldsymbol{\sigma}_{i_1}, \boldsymbol{\sigma}_{i_2}, \ldots, \boldsymbol{\sigma}_{i_h}, \vec{\boldsymbol{b}}$ matice $\mathbf{M}'$ je lineárne závislých, t.j. existujú prvky $c_1, c_2, \ldots, c_{h+1} \in F$ nie všetky rovné nule, že platí

$$c_1 \boldsymbol{\sigma}_{i_1} + c_2 \boldsymbol{\sigma}_{i_2} + \cdots + c_h \boldsymbol{\sigma}_{i_h} + c_{h+1} \vec{\boldsymbol{b}} = \vec{\mathbf{0}}. \tag{4.6}$$

Keby $c_{h+1} = 0$, stĺpce $\boldsymbol{\sigma}_{i_1}, \boldsymbol{\sigma}_{i_2}, \ldots, \boldsymbol{\sigma}_{i_h}$ by boli lineárne závislé. Teda $c_{h+1} \neq 0$. Z (4.6) máme

$$-\frac{c_1}{c_{h+1}} \boldsymbol{\sigma}_{i_1} - \frac{c_2}{c_{h+1}} \boldsymbol{\sigma}_{i_2} - \cdots - \frac{c_h}{c_{h+1}} \boldsymbol{\sigma}_{i_h} = \vec{\boldsymbol{b}}. \tag{4.7}$$

Z (4.7) vyplýva, že stĺpec $\vec{\boldsymbol{b}}$ je lineárnou kombináciou všetkých stĺpcov matice $\mathbf{M}$, t.j.

$$t_1 \boldsymbol{\sigma}_1 + t_2 \boldsymbol{\sigma}_2 + \cdots + t_n \boldsymbol{\sigma}_n = \vec{\boldsymbol{b}}, \tag{4.8}$$

kde $t_k = 0$ ak sa stĺpec $\boldsymbol{\sigma}_k$ nenachádza na ľavej strane (4.7) resp. $t_k = -\frac{c_j}{c_{h+1}}$, ak $\boldsymbol{\sigma}_k = \boldsymbol{\sigma}_{i_j}$ pre nejaké $j = 1, 2, \ldots, h$.

Z (4.8) však vidieť, že vektor $\boldsymbol{\tau} = (t_1, t_2, \ldots, t_n)$ je riešením sústavy (4.5) resp. (4.1). Tým je dôkaz vety skončený. □

Dôsledok 1. *Nech pre sústavu* (4.1) *platí* $h(\mathbf{M}) = h(\mathbf{M}') = h$. *Potom existuje sústava lineárnych rovníc ekvivalentná sústave* (4.1) *majúca práve* h *rovníc.*

Dôkaz. Keďže $h(\mathbf{M}') = h$, sústava (4.1) obsahuje práve h lineárne nezávislých rovníc. Tieto rovnice tvoria bázu podpriestoru $\boldsymbol{R}'_n(F)$ priestoru lineárnych rovníc $\boldsymbol{R}_n(F)$ (pozri príklad 1.8 kapitoly 2), ktorý generujú rovnice sústavy (4.1). Každá z ostatných rovníc sústavy (ak taká vôbec existuje) sa dá vyjadriť ako lineárna kombinácia rovníc, ktoré tvoria bázu. Pomocou elementárnych operácií z vety 2.1 ľahko prejdeme k ekvivalentnej sústave, ktorá obsahuje len rovnice bázy. (Rovnice, ktoré majú všetky koeficienty nulové, vynecháme). □

Dôsledok 2. *Nech pre sústavu* (4.1) *platí* $h(\mathbf{M}) = h(\mathbf{M}') = n$. *Potom sústava* (4.1) *má práve jedno riešenie.*

Dôkaz. Keďže platí $h(\mathbf{M}) = h(\mathbf{M'})$, sústava má aspoň jedno riešenie. Že má práve jedno dokážeme nepriamo. Nech platia predpoklady vety a nech napriek tomu sústava (4.1) má dve rôzne riešenia $\boldsymbol{\tau} = (t_1, t_2, \dots, t_n)$ a $\boldsymbol{\tau}' = (t'_1, t'_2, \dots, t'_n)$. Potom z (4.5) máme

$$\begin{aligned} \boldsymbol{\sigma}_1 t_1 + \boldsymbol{\sigma}_2 t_2 + \cdots + \boldsymbol{\sigma}_n t_n &= \vec{\boldsymbol{b}}, \\ \boldsymbol{\sigma}_1 t'_1 + \boldsymbol{\sigma}_2 t'_2 + \cdots + \boldsymbol{\sigma}_n t'_n &= \vec{\boldsymbol{b}}, \end{aligned}$$

odkiaľ dostaneme

$$\boldsymbol{\sigma}_1(t_1 - t'_1) + \boldsymbol{\sigma}_2(t_2 - t'_2) + \cdots + \boldsymbol{\sigma}_n(t_n - t'_n) = \vec{\mathbf{0}}.$$

Keďže $h(\mathbf{M}) = n$, stĺpce $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \dots, \boldsymbol{\sigma}_n$ sú lineárne nezávislé a tak $t_1 - t'_1 = 0$, $t_2 - t'_2 = 0, \dots, t_n - t'_n = 0$, t.j. $\boldsymbol{\tau} = \boldsymbol{\tau}'$. Máme spor. □

Dôsledok 3. *Nech pre sústavu* (4.1) *platí* $h(\mathbf{M}) = h(\mathbf{M}') = h < n$. *Potom* $n - h$ *neznámych možno ľubovoľne zvoliť a pre každú voľbu týchto* $n - h$ *neznámych existuje práve jedno riešenie sústavy* (4.1).

Dôkaz. Podľa dôsledku 1 existuje sústava h rovníc ekvivalentná so sústavou (4.1). Nech je to nasledujúci sústava:

$$\begin{aligned} &c_{11}x_1 + c_{12}x_2 + \cdots + c_{1h}x_h + c_{1h+1}x_{h+1} + \cdots + c_{1n}x_n = d_1, \\ &c_{21}x_1 + c_{22}x_2 + \cdots + c_{2h}x_h + c_{2h+1}x_{h+1} + \cdots + c_{2n}x_n = d_2, \\ &\;\vdots \\ &c_{h1}x_1 + c_{h2}x_2 + \cdots + c_{hh}x_h + c_{hh+1}x_{h+1} + \cdots + c_{hn}x_n = d_h. \end{aligned}$$

Matica tejto sústavy má hodnosť h. Preto obsahuje h lineárne nezávislých stĺpcov. Bez ujmy na všeobecnosti môžeme predpokladať, že je to prvých h stĺpcov matice (v opačnom prípade by sme stĺpce takto usporiadali). Teraz položme $x_{h+1} = p_1$, $x_{h+2} = p_2, \dots, x_n = p_{n-h}$, kde $p_1, p_2, \dots, p_{n-h}$ sú ľubovoľne vybrané prvky poľa F (parametre). Sústavu zapíšeme v tvare

$$\begin{aligned} &c_{11}x_1 + c_{12}x_2 + \cdots + c_{1h}x_h = d_1 - c_{1h+1}p_1 - \cdots - c_{1n}p_{n-h} \\ &c_{21}x_1 + c_{22}x_2 + \cdots + c_{2h}x_h = d_2 - c_{2h+1}p_1 - \cdots - c_{2n}p_{n-h} \\ &\;\vdots \\ &c_{h1}x_1 + c_{h2}x_2 + \cdots + c_{hh}x_h = d_h - c_{hh+1}p_1 - \cdots - c_{hn}p_{n-h} \end{aligned} \tag{4.9}$$

Podľa dôsledku 2 má sústava (4.9) a tým aj ekvivalentná sústava (4.1) *pre každú voľbu neznámych* $x_{h+1}, x_{h+2}, \dots, x_h$, čiže parametrov $p_1, p_2, \dots, p_{n-h}$, práve jedno riešenie. □

Poznámka 4.1. Keďže $h < n$, t.j. $n - h$ je aspoň jeden a každé pole má aspoň dva prvky, sústava (4.1) má pri splnení podmienok dôsledku 3 aspoň dve rôzne riešenia. Samozrejme, ak F je nekonečné pole (napr. pole reálnych čísel), sústava (4.1) má nekonečne veľa riešení.

Keď sústavu (4.9) skutočne vyriešime, neznáme $x_1, x_2, \dots, x_h$ vyjadríme pomocou parametrov $p_1, \dots, p_{n-h}$. Hovoríme, že sústava (4.9) a teda aj (4.1) má všeobecné $(n-h)$ - parametrické riešenie resp. riešenie s $n-h$ stupňami voľnosti. Ak za parametre dosadíme konkrétne prvky poľa F, dostaneme konkrétne (partikulárne) riešenie danej sústavy. Postup môžeme sledovať na nasledujúcom príklade.

Príklad 4.1. Nad poľom racionálnych čísel riešme sústavu rovníc, keď vieme, že $h(\mathbf{M}) = h(\mathbf{M}') = 2$.

$$\begin{aligned} 2x_1 + 3x_2 - x_3 + 2x_4 &= 13, \\ x_1 - 2x_2 + 4x_3 + x_4 &= -6, \\ 3x_1 + x_2 + 3x_3 + 3x_4 &= 7, \\ x_1 + 5x_2 - 5x_3 + x_4 &= 19. \end{aligned}$$

Riešenie. Ihneď vidieť, že ak od tretej rovnice odpočítame prvú i druhú rovnicu a ku štvrtej pripočítame druhú a odpočítame prvú, dostaneme rovnice s nulovými koeficientami, ktoré vynecháme. Zostane

$$\begin{aligned} 2x_1 + 3x_2 - x_3 + 2x_4 &= 13, \\ x_1 - 2x_2 + 4x_3 + x_4 &= -6. \end{aligned}$$

Ľahko skontrolujeme, že prvé dva stĺpce matice sústavy sú lineárne nezávislé. Položíme $x_3 = p_1$, $x_4 = p_2$, kde $p_1, p_2 \in Q$ sú parametre.

$$\begin{aligned} 2x_1 + 3x_2 &= 13 + p_1 - 2p_2 \\ x_1 - 2x_2 &= -6 - 4p_1 - p_2 \end{aligned}$$

Danú sústavu (pri pevnej voľbe x_3 a x_4 je to sústava dvoch rovníc o dvoch neznámych) vyriešime:

$$x_1 = \frac{8}{7} - \frac{10}{7}p_1 - p_2, \quad x_2 = \frac{25}{7} + \frac{9}{7}p_1.$$

Keďže $x_3 = p_1$, $x_4 = p_2$, máme všeobecné riešenie sústavy s dvoma stupňami voľnosti (2-parametrické riešenie):

$$\boldsymbol{\tau} = \Big(\frac{8}{7} - \frac{10}{7}p_1 - p_2,\ \frac{25}{7} + \frac{9}{7}p_1,\ p_1,\ p_2\Big).$$

Pomocou neho zapíšeme množinu všetkých riešení sústavy

$$S = \left\{\Big(\frac{8}{7} - \frac{10}{7}p_1 - p_2,\ \frac{25}{7} + \frac{9}{7}p_1,\ p_1,\ p_2\Big);\ p_1, p_2 \in Q\right\}.$$

Vidieť, že S je nekonečná množina. Pre napr. $p_1 = 1$, $p_2 = 0$ dostávame partikulárne riešenie $(-\frac{2}{7}, \frac{34}{7}, 1, 0) \in S$.

Teraz popíšeme všeobecný postup na riešenie sústavy lineárnych rovníc známy pod názvom *Gaussova eliminačná metóda.* Pri tomto postupe nemusíme vopred poznať hodnosti $h(\mathbf{M})$ resp. $h(\mathbf{M}')$. Zistíme ich počas postupu na konci ktorého, v prípade $h(\mathbf{M}) = h(\mathbf{M}')$, dostaneme riešenie sústavy. Pri Gaussovej eliminačnej metóde môžeme pracovať priamo s rovnicami alebo, čo je pohodlnejšie, s rozšírenou maticou danej sústavy.

Princíp Gaussovej eliminačnej metódy spočíva v postupnom vykonávaní riadkových elementárnych operácií tak dlho, kým nedostaneme sústavu (s pôvodnou ekvivalentnú), ktorá evidentne nemá riešenie, alebo ktorej riešenie vieme ľahko určiť. Menovite, napíšeme rozšírenú maticu sústavy (4.1):

$$\begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n}, & b_1 \\ a_{21}, & a_{22}, & \dots, & a_{2n}, & b_2 \\ \vdots \\ a_{m1}, & a_{m2}, & \dots, & a_{mn}, & b_m \end{pmatrix} \tag{4.10}$$

Ak na maticu (4.10) uplatníme niektorú ero, dostaneme podľa vety 2.1 rozšírenú maticu sústavy, ktorá je so sústavou (4.1) ekvivalentná. Okrem ero môžeme meniť aj poradie stĺpcov matice sústavy (stĺpec $\vec{\boldsymbol{b}}$ teda ponecháme na mieste), ale v tomto prípade si poznamenáme, ktorý stĺpec patrí ktorej neznámej. Operácie vykonávame postupom ako v leme 3.2, kým nenastane jeden z týchto dvoch prípadov:

(i) Pri postupe sa vyskytne riadok typu $(0, 0, \dots, 0, c)$, kde $c \neq 0$. V tomto prípade je $h(\mathbf{M}) \neq h(\mathbf{M}')$ (čitateľ si rozmyslí, prečo). Výpočet prerušíme, lebo sústava nemá riešenie.

(ii) Dostaneme maticu tvaru

$$\begin{pmatrix} c_{11}, & c_{12}, & c_{13}, & \dots, & c_{1h}, & c_{1,h+1}, & \dots, & c_{1n}, & d_1 \\ 0, & c_{22}, & c_{23}, & \dots, & c_{2h}, & c_{2,h+1}, & \dots, & c_{2n}, & d_2 \\ 0, & 0, & c_{33}, & \dots, & c_{3h}, & c_{3,h+1}, & \dots, & c_{3n}, & d_3 \\ \vdots \\ 0, & 0, & 0, & \dots, & c_{hh}, & c_{h,h+1}, & \dots, & c_{hn}, & d_h \end{pmatrix}, \tag{4.11}$$

kde sme vynechali všetky nulové riadky a kde $c_{11}, c_{22}, \dots, c_{hh} \neq 0$. Z matice (4.11) zrekonštruujeme nasledujúcu sústavu ekvivalentnú so sústavou (4.1). (Predpokladáme, že sme nevymieňali stĺpcec matice.)

$$\begin{aligned} c_{11}x_1 + c_{12}x_2 + c_{13}x_3 + \dots + c_{1h}x_n + c_{1,h+1}x_{h+1} + \dots + c_{1n}x_n &= d_1, \\ c_{22}x_2 + c_{23}x_3 + \dots + c_{2h}x_h + c_{2,h+1}x_{h+1} + \dots + c_{2n}x_n &= d_2, \\ c_{33}x_3 + \dots + c_{3h}x_h + c_{3,h+1}x_{h+1} + \dots + c_{2n}x_n &= d_3, \\ &\vdots \\ c_{hh}x_h + c_{h,h+1}x_{h+1} + \dots + c_{hn}x_n &= d_h. \end{aligned} \tag{4.12}$$

Teraz máme dve možnosti. 1) $h = h(\mathbf{M}) = h(\mathbf{M}') = n$. V tomto prípade máme n rovníc. Posledná obsahuje jedinú neznámu x_n, ktorú z nej vypočítame. Predposledná rovnica obsahuje 2 neznáme x_{n-1}, x_n, z ktorých x_n poznáme a x_{n-1}

vypočítame, atď. až z prvej rovnice vypočítame neznámu x_1. Dostaneme riešenie sústavy, ktoré je podľa dôsledku 2 vety 4.1 jediné.

2) $h = h(\mathbf{M}) = h(\mathbf{M}') < n$. Ako v dôkaze dôsledku 3 vety 4.1 položíme $x_{h+1} = p_1$, $x_{h+2} = p_2, \dots, x_n = p_{n-h}$. Sústava (4.12) prejde do tvaru

$$\begin{aligned} c_{11}x_2 + c_{12}x_2 + c_{13}x_3 + \cdots + c_{1h}x_h &= d_1 - c_{1,h+1}p_1 - \cdots - c_{1n}p_{n-h},\\ c_{22}x_2 + c_{23}x_3 + \cdots + c_{2h}x_h &= d_2 - c_{2,h+1}p_1 - \cdots - c_{2n}p_{n-h},\\ c_{33}x_3 + \cdots + c_{3h}x_h &= d_3 - c_{3,h+1}p_1 - \cdots - c_{3n}p_{n-h},\\ &\vdots\\ c_{hh}x_h &= d_n - c_{h,h+1}p_1 - \cdots - c_{hn}p_{n-h}. \end{aligned}$$

Z poslednej rovnice vypočítame x_h, ďalej (postupne dosadzujúc) z predposlednej x_{h-1}, atď. až z prvej x_1. Všetky neznáme $x_1, \dots, x_h$ máme vyjadrené pomocou parametrov $p_1, \dots, p_{n-h}$.

Postup sa dobre objasní na nasledujúcich príkladoch.

Príklad 4.2. Nad poľom racionálnych čísel riešte nasledujúci sústavu.

$$\begin{aligned} x_1 + 2x_2 + x_3 - x_4 &= 1,\\ 2x_1 + 3x_2 - x_3 + 2x_4 &= 3,\\ 4x_1 + 7x_2 + x_3 &= 5,\\ 5x_1 + 7x_2 - 4x_3 + 7x_4 &= 10. \end{aligned}$$

Riešenie. Napíšeme rozšírenú maticu sústavy a postupne uplatňujeme ero.

$$\begin{pmatrix} 1 & 2 & 1 & -1 & 1\\ 2 & 3 & -1 & 2 & 3\\ 4 & 7 & 1 & 0 & 5\\ 5 & 7 & -4 & 7 & 10 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & -1 & 1\\ 0 & -1 & -3 & 4 & 1\\ 0 & -1 & -3 & 4 & 1\\ 0 & -3 & -9 & 12 & 5 \end{pmatrix} \to$$

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

Vidieť, že $h(\mathbf{M}) = 2$, zatiaľ čo $h(\mathbf{M}') = 3$. Sústava nemá riešenie.

Príklad 4.3. Nad telesom racionálnych čísel riešte sústavu rovníc

$$\begin{aligned} x_1 - 2x_2 + 4x_3 + x_4 &= -6,\\ 2x_1 + 3x_2 - x_3 + 2x_4 &= 13,\\ 2x_1 + 5x_2 + x_3 + x_4 &= 8,\\ 3x_1 + x_2 + 3x_3 + x_4 &= 1. \end{aligned}$$

Riešenie. Napíšeme rozšírenú maticu sústavy a postupne uplatníme ero.

$$\begin{pmatrix} 1 & -2 & 4 & 1 & -6\\ 2 & 3 & -1 & 2 & 13\\ 2 & 5 & 1 & 1 & 8\\ 3 & 1 & 3 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -2 & 4 & 1 & -6\\ 0 & 7 & -9 & 0 & 25\\ 0 & 9 & -7 & -1 & 20\\ 0 & 7 & -9 & -2 & 19 \end{pmatrix}$$

V matici najprv vymeníme druhý a tretí riadok, potom (označiac stĺpce pre neznáme) druhý a štvrtý stĺpec.

$$
\begin{array}{ccccc} x_1 & x_4 & x_3 & x_2 & \end{array}
$$
$$
\begin{pmatrix} 1 & 1 & 4 & -2 & -6 \\ 0 & -1 & -7 & 9 & 20 \\ 0 & 0 & -9 & 7 & 25 \\ 0 & -2 & -9 & 7 & 19 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 4 & -2 & -6 \\ 0 & -1 & -7 & 9 & 20 \\ 0 & 0 & -9 & 7 & 25 \\ 0 & 0 & 5 & -11 & -21 \end{pmatrix} \to
$$

$$
\begin{array}{ccccc} x_1 & x_4 & x_3 & x_2 & \end{array}
$$
$$
\to \begin{pmatrix} 1 & 1 & 4 & -2 & -6 \\ 0 & -1 & -7 & 9 & 20 \\ 0 & 0 & -9 & 7 & 25 \\ 0 & 0 & 0 & -\frac{64}{9} & -\frac{64}{9} \end{pmatrix}.
$$

Z poslednej matice vidíme, že $h(\mathbf{M}) = h(\mathbf{M}') = 4$, t.j. sústava má jediné riešenie. „Zrekonštruujeme“ sústavu s pôvodnou ekvivalentnú.

$$
\begin{aligned}
x_1 + x_4 + 4x_3 - 2x_2 &= -6, \\
-x_4 - 7x_3 + 9x_2 &= 20, \\
-9x_3 + 7x_2 &= 25, \\
-\frac{64}{9}x_2 &= -\frac{64}{9}.
\end{aligned}
$$

Z poslednej rovnice máme $x_2 = 1$, z predposlednej (po dosadení) $x_3 = -2$, z druhej $x_4 = 3$ a z prvej $x_1 = 1$. Jediným riešením pôvodnej sústavy je teda vektor $(1, 1, -2, 3) \in \boldsymbol{V}_4(Q)$.

Príklad 4.4. Vypočítajte súradnice vektora $\boldsymbol{\beta} = (-6, 13, 8, 1) \in \boldsymbol{V}_4(Q)$ vzhľadom na bázu $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3, \boldsymbol{\alpha}_4\}$, kde

$$
\boldsymbol{\alpha}_1 = (1, 2, 2, 3), \ \boldsymbol{\alpha}_2 = (-2, 3, 5, 1), \ \boldsymbol{\alpha}_3 = (4, -1, 1, 3), \ \boldsymbol{\alpha}_4 = (1, 2, 1, 1).
$$

Riešenie. Čitateľovi odporúčame, aby sa presvedčil, že vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3, \boldsymbol{\alpha}_4$ naozaj tvoria bázu $\boldsymbol{V}_4(Q)$. Ak súradnice vektora $\boldsymbol{\beta}$ označíme x_1, x_2, x_3, x_4, platí rovnica

$$
x_1(1, 2, 2, 3) + x_2(-2, 3, 5, 1) + x_3(4, -1, 1, 3) + x_4(1, 2, 1, 1) = (-6, 13, 8, 1),
$$

ktorá, ako sa čitateľ rýchlo presvedčí, vedie na sústavu rovníc, ktorú sme vyriešili v príklade 4.3. Teda $x_1 = 1$, $x_2 = 1$, $x_3 = -2$, $x_4 = 3$.

Príklad 4.5. Nad poľom racionálnych čísel riešte sústavu rovníc

$$
\begin{aligned}
x_1 + 2x_2 + 3x_3 - 2x_4 + x_5 &= 0, \\
x_1 - 2x_2 + 4x_3 - x_4 + 2x_5 &= 0, \\
2x_1 + x_2 - 3x_3 + 4x_4 - x_5 &= 0, \\
2x_1 + 5x_2 - 4x_3 + 3x_4 - 2x_5 &= 0, \\
2x_1 - 3x_2 - 2x_3 + 5x_4 \phantom{{}- 2x_5} &= 0.
\end{aligned}
$$

Riešenie. Hneď vidieť, že $h(\mathbf{M}) = h(\mathbf{M}')$, lebo rozšírenú maticu dostaneme z matice sústavy pridaním nulového stĺpca.

$$\begin{pmatrix} 1 & 2 & 3 & -2 & 1 & 0 \\ 1 & -2 & 4 & -1 & 2 & 0 \\ 2 & 1 & -3 & 4 & -1 & 0 \\ 2 & 5 & -4 & 3 & -2 & 0 \\ 2 & -3 & -2 & 5 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 & -2 & 1 & 0 \\ 0 & -4 & 1 & 1 & 1 & 0 \\ 0 & -3 & -9 & 8 & -3 & 0 \\ 0 & 1 & -10 & 7 & -4 & 0 \\ 0 & -7 & -8 & 9 & -2 & 0 \end{pmatrix} \to$$

Vymeníme druhý a piaty stĺpec (označiac stĺpce pre neznáme).

$$\to \begin{array}{c} \begin{matrix} x_1 & x_5 & x_3 & x_4 & x_2 & \end{matrix} \\ \begin{pmatrix} 1 & 1 & 3 & -2 & 2 & 0 \\ 0 & 1 & 1 & 1 & -4 & 0 \\ 0 & -3 & -9 & 8 & -3 & 0 \\ 0 & -4 & -10 & 7 & 1 & 0 \\ 0 & -2 & -8 & 9 & -7 & 0 \end{pmatrix} \end{array} \to \begin{pmatrix} 1 & 1 & 3 & -2 & 2 & 0 \\ 0 & 1 & 1 & 1 & -4 & 0 \\ 0 & 0 & -6 & 11 & -15 & 0 \\ 0 & 0 & -6 & 11 & -15 & 0 \\ 0 & 0 & -6 & 11 & -15 & 0 \end{pmatrix} \to$$

$$\to \begin{array}{c} \begin{matrix} x_1 & x_5 & x_3 & x_4 & x_2 & \end{matrix} \\ \begin{pmatrix} 1 & 1 & 3 & -2 & 2 & 0 \\ 0 & 1 & 1 & 1 & -4 & 0 \\ 0 & 0 & -6 & 11 & -15 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

Vidíme, že $h(\mathbf{M}) = h(\mathbf{M}') = 3$. Napíšeme sústavu ekvivalentnú s pôvodnou.

$$\begin{aligned} x_1 + x_5 + 3x_3 - 2x_4 + 2x_2 &= 0, \\ x_5 + x_3 + x_4 - 4x_2 &= 0, \\ -6x_3 + 11x_4 - 15x_2 &= 0. \end{aligned}$$

Zvolíme $x_2 = 6p_1, x_4 = 6p_2$, kde $p_1, p_2 \in Q$. Dostaneme

$$\begin{aligned} x_1 + x_5 + 3x_3 &= -12p_1 + 12p_2, \\ x_5 + x_3 &= 24p_1 - 6p_2, \\ -6x_3 &= 90p_1 - 66p_2. \end{aligned}$$

Vypočítame $x_3 = -15p_1 + 11p_2$, $x_5 = 39p_1 - 17p_2$, $x_1 = -6p_1 - 4p_2$. Teda všeobecné riešenie je $(-6p_1 - 4p_2,\ 6p_1,\ -15p_1 + 11p_2,\ 6p_2,\ 39p_1 - 17p_2)$, kde p_1, p_2 sú ľubovoľné racionálne čísla (parametre).

Poznámka 4.2. Tým, že sme v predchádzajúcom príklade za neznáme zvolili parametre v tvare $6p_1$ resp. $6p_2$, sme sa vo vyjadreniach pre jednotlivé neznáme vyhli výrazom so zlomkami. Nedopustili sme sa tým nijakej chyby, lebo ak parameter p_i prebieha všetky racionálne čísla, tak aj jeho šesťnásobok ich prebieha (premyslite to).

Príklad 4.6. Zistite, či nasledujúce vektory priestoru $\boldsymbol{V}_5(Q)$ sú lineárne závislé. Ak áno, určte koeficienty lineárnej závislosti.

$$\begin{aligned}\boldsymbol{\alpha}_1 &= (1,1,2,2,2),\\ \boldsymbol{\alpha}_2 &= (2,-2,1,5,-3),\\ \boldsymbol{\alpha}_3 &= (3,4,-3,-4,-2),\\ \boldsymbol{\alpha}_4 &= (-2,-1,4,3,5),\\ \boldsymbol{\alpha}_5 &= (1,2,-1,-2,0).\end{aligned}$$

Riešenie. Ak sú vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3, \boldsymbol{\alpha}_4, \boldsymbol{\alpha}_5$ lineárne závislé, existuje päť racionálnych čísel c_1, c_2, c_3, c_4, c_5, ktoré nie sú všetky rovné nule, že platí rovnica $c_1(1,1,2,2,2) + c_2(2,-2,1,5,-3) + c_3(3,4,-3,-4,-2) + c_4(-2,-1,4,3,5) + {} + c_5(1,2,-1,-2,0) = (0,0,0,0,0)$.
Ľahko sa presvedčíme, že táto rovnica vedie na sústavu, ktorú sme riešili v predchádzajúcom príklade 4.5. Tam sme zistili, že sústava má aj nenulové riešenie. To znamená, že dané vektory sú lineárne závislé. Ak napr. zvolíme $p_1 = \frac{1}{3}$, $p_2 = 0$, dostaneme riešenie $(-2,2,-5,0,13)$, t.j. za koeficienty lineárnej závislosti môžeme brať $c_1 = -2$, $c_2 = 2$, $c_3 = -5$, $c_4 = 0$, $c_5 = 13$.

Príklad 4.7. Riešte nasledujúcu sústavu 3 rovníc o 3 neznámych, vykonajúc diskusie vzhľadom na parametre $a, b, c \in Q$.

$$\begin{aligned} x + {}\ \ y + {}\ \ z &= 1,\\ ax + ay + bz &= c,\\ a^2x + a^2y + b^2z &= c^2.\end{aligned}$$

Riešenie. Napíšeme príslušnú rozšírenú maticu sústavy

$$\begin{pmatrix} 1 & 1 & 1 & 1\\ a & a & b & c\\ a^2 & a^2 & b^2 & c^2\end{pmatrix} \to \begin{pmatrix} 1 & 1 & 1 & 1\\ 0 & 0 & b-a & c-a\\ 0 & 0 & b^2-a^2 & c^2-a^2\end{pmatrix}$$

Z poslednej matice vidieť, že sústava nemá riešenie keď $a = b$ a súčasne $c \neq a$.

1) Nech $a = b$ a súčasne $c = a$. Potom $h(\mathsf{M}) = h(\mathsf{M}') = 1$ a máme jedinú rovnicu

$$x + y + z = 1,$$

riešením ktorej dostaneme všeobecné riešenie $(1 - p_1 - p_2, p_1, p_2)$, kde $p_1, p_2 \in Q$.

2) Nech $a \neq b$. Potom rozšírenú maticu sústavy upravíme na tvar

$$\begin{pmatrix} 1 & 1 & 1 & 1\\ 0 & 0 & b-a & c-a\\ 0 & 0 & 0 & (c-a)(c-b)\end{pmatrix}$$

Z tejto matice vidieť, že ak $c \neq a$ a súčasne $c \neq b$, sústava riešenie nemá. Čitateľ ľahko overí, že nemôže súčasne nastať $c = a$ aj $c = b$, lebo potom by bolo aj $a = b$, čo nie je. Máme tak buď ($c = a \wedge c \neq b$) alebo ($c \neq a \ \wedge c = b$). V oboch prípadoch je $h(M) = h(M') = 2$.

a) V prípade $c = a$ a zároveň $c \neq b$ máme sústavu

$$\begin{aligned} x + y + \quad z &= 1, \\ (b-a)z &= 0, \end{aligned}$$

ktorej všeobecné riešenie je $(1-p,\, p,\, 0)$, kde $p \in Q$.

b) V prípade $c \neq a$ a zároveň $c = b$ máme sústavu

$$\begin{aligned} x + y + \quad z &= 1, \\ (b-a)z &= b - a, \end{aligned}$$

ktorej všeobecné riešenie je $(-p,\, p,\, 1)$, kde $p \in Q$.

Zhrnieme:

(1) Ak $(a = b \wedge c \neq a) \vee (a \neq b \wedge c \neq a \wedge c \neq b)$, tak množina riešení sústavy je $S = \emptyset$.
(2) Ak $(a = b \wedge c = a)$, tak $S = \{(1 - p_1 - p_2,\, p_1,\, p_2);\ p_1, p_2 \in Q\}$.
(3) Ak $(a \neq b \wedge c = a \wedge c \neq b)$, tak $S = \{(1-p,\, p,\, 0);\ p \in Q\}$.
(4) Ak $(a \neq b \wedge c \neq a \ \wedge c = b)$, tak $S = \{(-p,\, p,\, 1);\ p \in Q\}$.

Cvičenia

4.1. Gaussovou eliminačnou metódou riešte nasledujúce sústavy lineárnych rovníc (nad poľom racionálnych čísel).

a)
$$\begin{aligned} x_1 + x_2 + 2x_3 - x_4 + x_5 &= 3, \\ 2x_1 + 5x_2 - 3x_3 - 2x_4 - x_5 &= -5, \\ 3x_1 + 4x_2 - 5x_3 - x_4 + 2x_5 &= 18, \\ 3x_1 + 5x_2 + 2x_3 - 2x_4 + x_5 &= 3, \\ 3x_1 + 6x_2 + 2x_3 + 5x_4 - 2x_5 &= 1, \end{aligned}$$

b)
$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 &= 15, \\ 2x_1 + 3x_2 + 4x_3 - x_4 - x_5 &= 11, \\ x_1 + 3x_2 - 4x_3 + 5x_4 + 2x_5 &= 7, \\ 2x_1 + x_2 + 9x_3 - 5x_4 - 2x_5 &= 10, \\ x_1 + 2x_2 - x_3 + x_4 - 7x_5 &= 5, \end{aligned}$$

c)
$$\begin{aligned} 2x_1 + 3x_2 - 4x_3 + x_4 + x_5 &= 10, \\ x_1 - 2x_2 + 3x_3 - 4x_4 + x_5 &= 11, \\ 3x_1 + 3x_2 - 4x_3 + 5x_4 - 2x_5 &= 7, \\ -2x_2 + 3x_3 - 8x_4 + 4x_5 &= 14, \\ 6x_1 + 4x_2 - 5x_3 + 2x_4 \qquad &= 28. \end{aligned}$$

d)
$$\begin{aligned} x_1 + x_2 + x_3 - x_4 - x_5 &= 3, \\ 2x_1 + 3x_2 + 4x_3 - 5x_4 + x_5 &= 5, \\ -2x_2 - 2x_3 + 3x_4 + 3x_5 &= -6, \\ x_1 - 2x_2 + 3x_3 + x_4 \qquad &= 0, \\ 4x_1 + x_2 \qquad - 3x_4 - 2x_5 &= 5, \end{aligned}$$

f)
$$\begin{aligned} x_1 - 2x_2 - 3x_3 + x_4 + x_5 &= -1, \\ 2x_1 + 2x_2 - x_3 + 3x_4 - x_5 &= -1, \\ x_1 + x_2 - 2x_3 - 2x_4 + 3x_5 &= 5, \\ 3x_1 - 2x_2 + x_3 - 2x_4 + x_5 &= 10, \\ x_1 - x_2 + x_3 - 2x_4 - 5x_5 &= 0. \end{aligned}$$

4.2. Riešte sústavy rovníc (nad Q):

$$a)\qquad \begin{aligned} ax_1 + ax_2 + ax_3 + bx_4 &= c_1,\\ ax_1 + ax_2 + bx_3 + ax_4 &= c_2,\\ ax_1 + bx_2 + ax_3 + ax_4 &= c_3,\\ bx_1 + ax_2 + ax_3 + ax_4 &= c_4, \end{aligned}$$

kde $a, b, c_1, c_2, c_3, c_4 \in Q$ a $a \neq b$.

$$b)\quad \begin{aligned} x_1 + x_2 + \cdots + x_{n-1} + 2x_n &= 1,\\ x_1 + x_2 + \cdots + 2x_{n-1} + x_n &= 2,\\ &\vdots\\ x_1 + 2x_2 + \cdots + x_{n-1} + x_n &= n-1,\\ 2x_1 + x_2 + \cdots + x_{n-1} + x_n &= n. \end{aligned}$$

$$c)\quad \begin{aligned} ax_1 + x_2 + \cdots + x_{n-1} + x_n &= 1,\\ x_1 + ax_2 + \cdots + x_{n-1} + x_n &= 1,\\ &\vdots\\ x_1 + x_2 + \cdots + ax_{n-1} + x_n &= 1,\\ x_1 + x_2 + \cdots + x_{n-1} + ax_n &= 1, \end{aligned}$$

kde $a \in Q$, pričom $a \neq 1$, $n \geqq 2$.

4.3. Dokážte, že množina B_i $(i = 1, 2)$ je báza priestoru $\boldsymbol{V}_4(R)$ a vypočítajte súradnice vektora $\boldsymbol{\alpha}_i$ vzhľadom na túto bázu.

a) $B_1 = \{(1,\ 2,\ 3,\ 4),\ (2,\ 1,\ 2,\ 3),\ (3,\ 2,\ 1,\ 2),\ (4,\ 3,\ 2,\ 1)\}$,
$\boldsymbol{\alpha}_1 = (5,\ 1,\ 1,\ -5)$.

b) $B_2 = \{(2,\ 1,\ 3,\ -1),\ (-3,\ 2,\ 2,\ 4),\ (2,\ -3,\ -2,\ 1),\ (4,\ -2,\ 1,\ -5)\}$,
$\boldsymbol{\alpha}_2 = (8,\ -4,\ 2,\ -5)$.

4.4. Nájdite súradnice vektora $3 - 6x + 2x^2 \in \boldsymbol{P}(R)$ vzhľadom na bázu $\{3, (2x-1), (2x-1)^2\}$.

4.5. Dokážte, že vektory nasledujúcich množín vektorov sú lineárne závislé a nájdite koeficienty lineárnej závislosti v rovnosti (2.1).

a) $\{(1,\ 2,\ 3),\ (-4,\ 5,\ 1),\ (0,\ 0,\ 0)\} \subset \boldsymbol{V}_3(R)$,
b) $\{(1,\ 2,\ 3), (2,\ 4,\ 6),\ (1,\ -1,\ 7)\} \subset \boldsymbol{V}_3(R)$,
c) $\{(1,\ -2,\ 3),\ (2,\ 4,\ -2),\ (-1,\ -11,\ 17) \subset \boldsymbol{V}_3(R)$,
d) $\{(1,\ 2,\ 3),\ (1,\ -1,\ 1),\ (4,\ 0,\ 5),\ (3,\ 2,\ 1)\} \subset \boldsymbol{V}_3(R)$,
e) $\{2 + x - x^2,\ 1 + x,\ 1 - x^2,\ 2 + x + 2x^2\}$ z vektorového priestoru všetkých polynómov s racionálnymi koeficientami stupňa najviac dva.
f) $\left\{\begin{pmatrix} 1 & -2\\ 3 & 1\end{pmatrix}, \begin{pmatrix} 0, & -3\\ 2 & 2\end{pmatrix}, \begin{pmatrix} 1 & -1\\ 3 & 4\end{pmatrix}, \begin{pmatrix} 0 & -4\\ 2 & -1\end{pmatrix}\right\} \subset \mathcal{M}_2(Q)$ pozri príklad 4.5).

4.6. Riešte sústavy rovníc (nad Q) a urobte diskusiu vzhľadom na dané parametre

$$a)\quad \begin{aligned} ax + y + z &= b,\\ x + ay + z &= b,\\ x + y + az &= c, \end{aligned} \qquad b)\quad \begin{aligned} ax + 2y + z &= 1,\\ x + 2ay + z &= 2,\\ x + 2y + az &= 1, \end{aligned}$$

kde $a, b, c \in Q$.

4.7. Nasledujúce sústavy rovníc riešte najprv nad poľom zvyškových tried Z_3, potom nad Z_5 a Z_7.

$$a)\quad \begin{aligned} \bar{1}x + \bar{2}y + \bar{2}z &= \bar{1},\\ \bar{2}x + \bar{1}y + \bar{1}z &= \bar{2},\\ \bar{2}x + \bar{2}y + 1z &= \bar{0}, \end{aligned}$$

$$b)\quad \begin{aligned} \bar{2}x_1 + \bar{2}x_2 + \bar{1}x_3 + \bar{1}x_4 + \bar{1}x_5 &= \bar{2},\\ \bar{1}x_1 + \qquad\ \bar{1}x_3 + \bar{2}x_4 + \bar{1}x_5 &= \bar{2},\\ \bar{2}x_1 + \bar{1}x_2 + \bar{2}x_3 + \bar{1}x_4 + \bar{1}x_5 &= \bar{0},\\ \bar{1}x_1 + \bar{2}x_2 + \bar{1}x_3 + \bar{2}x_4 \qquad\ &= \bar{1},\\ \bar{1}x_3 + \bar{1}x_4 + \bar{2}x_5 &= \bar{2}. \end{aligned}$$

§ 5. Sústavy homogénnych lineárnych rovníc

Definícia 5.1. Ak v sústave (2.2) platí $b_1 = b_2 = \cdots = b_m = 0$, tak sústavu (2.2) nazývame sústavou m *homogénnych* rovníc s n neznámymi nad poľom F. Máme tak sústavu

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0,\\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0,\\ &\vdots\\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0. \end{aligned} \tag{5.1}$$

Sústavu (5.1) môžeme v zhode s (4.3) stručne zapísať v tvare

$$\mathbf{M}.\vec{x} = \vec{0}, \tag{5.2}$$

kde $\mathbf{M}$ je matica sústavy (5.1). Keďže posledný stĺpec matice $\mathbf{M}'$ obsahuje len nuly (nulové prvky poľa F), zrejme je $h(\mathbf{M}) = h(\mathbf{M}')$ a tak sústava (5.1) má vždy (aspoň jedno) riešenie. Na prvý pohľad vidieť, že n-tica $(0, 0, \ldots, 0)$ je riešením sústavy (5.1). Toto riešenie voláme *nulové* (alebo *triviálne*) riešenie sústavy (5.1). Platí nasledujúca veta.

Veta 5.1. *Sústava (5.1) má netriviálne riešenie práve vtedy, keď* $h(\mathbf{M}) < n$.

Dôkaz vety 5.1 vyplýva bezprostredne z dôsledkov 2 a 3 vety 4.1. $\square$

Veta 5.2. *Množina* $\boldsymbol{S}$ *všetkých riešení sústavy (5.1) je podpriestor vektorového priestoru* $\boldsymbol{V}_n(F)$.

Dôkaz. Ak $\boldsymbol{\alpha} \in \boldsymbol{V}_n(F)$ je riešením sústavy (5.1), t.j. $\boldsymbol{\alpha} \in \boldsymbol{S}$, tak platí

$$\mathbf{M} \cdot \boldsymbol{\alpha} = \vec{\mathbf{0}}.$$

Podľa vety 3.1 kapitoly 2, $\boldsymbol{S}$ bude podpriestor priestoru $\boldsymbol{V}_n(F)$, keď sú splnené podmienky
1) Ak $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{S}$, tak $\boldsymbol{\alpha} + \boldsymbol{\beta} \in \boldsymbol{S}$,
2) ak $\boldsymbol{\alpha} \in \boldsymbol{S}$, $s \in F$, tak $s\boldsymbol{\alpha} \in \boldsymbol{S}$.
Prvá podmienka je splnená, lebo $\mathbf{M}(\boldsymbol{\alpha} + \boldsymbol{\beta}) = \mathbf{M} \cdot \boldsymbol{\alpha} + \mathbf{M}\boldsymbol{\beta} = \vec{\mathbf{0}} + \vec{\mathbf{0}} = \vec{\mathbf{0}}$. Analogicky sa dokáže i platnosť druhej podmienky. $\square$

Veta 5.3. *Nech hodnosť matice* $\mathbf{M}$ *sústavy (5.1)* m *homogénnych rovníc o* n *neznámych je* $h(\mathbf{M}) = h$. *Potom dimenzia vektorového priestoru* $\boldsymbol{S}$ *všetkých riešení sústavy (5.1) je* $d(\boldsymbol{S}) = n - h$.

Dôkaz. Ak je $h = n$ podľa dôsledku 2 vety 4.1 má sústava (5.1) jediné riešenie. Tak $\boldsymbol{S} = \{(0, 0, \dots, 0)\}$ a teda $d(\boldsymbol{S}) = 0 = n - n$.

Nech teda $h < n$. Danú sústavu riešme Gaussovou eliminačnou metódou. Po vykonaní príslušných úprav dostaneme sústavu ekvivalentnú so sústavou (5.1) v tvare (4.12), kde pravda $d_1 = d_2 = \dots = d_h = 0$. Ak položíme $x_{h+1} = p_1$, $x_{h+2} = p_2, \dots, x_n = p_{n-h}$, môžeme vypočítať neznáme $x_1, x_2, \dots, x_h$ vyjadrené pomocou parametrov $p_1, p_2, \dots, p_{n-h}$

$$\begin{aligned}
x_1 &= b_{11}p_1 + b_{12}p_2 + \dots + b_{1,n-h}p_{n-h} = \sum_{i=1}^{n-h} b_{1i}p_i,\\
x_2 &= b_{21}p_1 + b_{22}p_2 + \dots + b_{2,n-h}p_{n-h} = \sum_{i=1}^{n-h} b_{2i}p_i,\\
&\vdots\\
x_h &= b_{h1}p_1 + b_{h2}p_2 + \dots + b_{h,n-h}p_{n-h} = \sum_{i=1}^{n-h} b_{hi}p_i.
\end{aligned}$$

Dostávame tak podpriestor riešení sústavy (5.1)

$$\boldsymbol{S} = \left\{ \left(\sum_{i=1}^{n-h} b_{1i}p_i, \sum_{i=1}^{n-h} b_{2i}p_i, \dots, \sum_{i=1}^{n-h} b_{hi}p_i,\ p_1,\ p_2, \dots, p_{n-h} \right); p_1,\ p_2, \dots, p_{n-h} \in F \right\}.$$

V podpriestore $\boldsymbol{S}$ zvoľme $n - h$ vektorov $\boldsymbol{\varepsilon}_i$ položiac
$p_1 = p_2 = \dots = p_{i-1} = 0, p_i = 1$, $p_{i+1} = \dots p_{n-h} = 0$. Dostaneme:

$$\begin{aligned}
\boldsymbol{\varepsilon}_1 &= (b_{11}, \quad b_{21}, \quad \dots, \quad b_{h1}, \quad 1, 0, \dots, 0),\\
\boldsymbol{\varepsilon}_2 &= (b_{12}, \quad b_{22}, \quad \dots, \quad b_{h2}, \quad 0, 1, \dots, 0),\\
&\vdots\\
\boldsymbol{\varepsilon}_{n-h} &= (b_{1,n-h},\ b_{2,n-h}, \dots, b_{h,n-h},\ 0,\ 0, \dots, 1).
\end{aligned}$$

Je evidentné, že vektory $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_{n-h}$ sú lineárne nezávislé. Na druhej strane ľahko zistíme, že ľubovoľný vektor $\boldsymbol{\alpha} \in \boldsymbol{S}$, daný pevnou voľbou parametrov $p_1, p_2, \ldots, p_{n-h}$, môžeme vyjadriť takto: $\boldsymbol{\alpha} = p_1\boldsymbol{\varepsilon}_1 + p_2\boldsymbol{\varepsilon}_2 + \cdots + p_{n-h}\boldsymbol{\varepsilon}_{n-h}$. To znamená, že vektory $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_{n-h}$ sú bázou podpriestoru $\boldsymbol{S}$. Z toho vyplýva $d(\boldsymbol{S}) = n - h$, čo sme mali dokázať. □

Dôkaz vety 5.3 nám súčasne poskytuje návod ako nájsť bázu priestoru všetkých riešení sústavy homogénnych rovníc. Ukážeme si to na príkladoch.

Príklad 5.1. Nájdime bázu podpriestoru riešení nasledujúcej sústavy lineárnych rovníc (nad poľom racionálnych čísel)

$$
\begin{aligned}
x_1 + \ \ 3x_2 - 4x_3 + \ \ 5x_4 + \ \ 7x_5 &= 0,\\
2x_1 + \ \ 7x_2 + \ \ x_3 - \ \ 7x_4 + \ \ 5x_5 &= 0,\\
3x_1 + 10x_2 - 3x_3 - \ \ 2x_4 + 12x_5 &= 0,\\
x_1 + \ \ 4x_2 + 5x_3 - 12x_4 - \ \ 2x_5 &= 0.
\end{aligned}
$$

Riešenie. Sústavu upravíme na nasledujúcu s ňou ekvivalentnú sústavu (ľahko zistíme, že $h(\mathbf{M}) = 2$):

$$
\begin{aligned}
x_1 + x_2 - 22x_3 + 39x_4 + 25x_5 &= 0,\\
x_2 + \ \ 9x_3 - 17x_4 - \ \ 9x_5 &= 0.
\end{aligned}
$$

Čitateľ si skontroluje, že riešenie sústavy (vektor podpriestoru $\boldsymbol{S}$) je tvaru

$$\boldsymbol{\alpha} = (31p_1 - 56p_2 - 34p_3,\ -9p_1 + 17p_2 + 9p_3,\ p_1,\ p_2,\ p_3),$$

kde $p_1, p_2, p_3 \in Q$. Podpriestor $\boldsymbol{S}$ má dimenziu $d(\boldsymbol{S}) = n - h = 5 - 2 = 3$ a vektory bázy sú

$$
\begin{aligned}
\boldsymbol{\varepsilon}_1 &= (\ \ \ 31,\ -9,\ 1,\ 0,\ 0),\\
\boldsymbol{\varepsilon}_2 &= (-56,\ 17,\ 0,\ 1,\ 0),\\
\boldsymbol{\varepsilon}_3 &= (-34,\ \ \ 9,\ 0,\ 0,\ 1).
\end{aligned}
$$

Príklad 5.2. Pri riešení sústavy homogénnych rovníc v príklade 4.5 sme našli, že podpriestor riešení sústavy je

$$\boldsymbol{S} = \{(-6p_1 - 4p_2,\ 6p_1,\ -15p_1 + 11p_2,\ 6p_2,\ 39p_1 - 17p_2);\ p_1, p_2 \in Q\}.$$

Dimenzia podpriestoru je $d(\boldsymbol{S}) = n - h = 5 - 3 = 2$. Za vektory bázy môžeme zvoliť

$$
\begin{aligned}
\boldsymbol{\varepsilon}_1 &= (-6,\ 6,\ -15,\ 0,\ \ \ 39),\\
\boldsymbol{\varepsilon}_2 &= (-4,\ 0,\ \ \ 11,\ 6,\ -17).
\end{aligned}
$$

Nasledujúca veta hovorí o vzťahu medzi riešeniami nehomogénnej sústavy lineárnych rovníc a príslušnej sústavy homogénnych rovníc.

Veta 5.4. *Nech*

$$\mathbf{M} \cdot \vec{\boldsymbol{x}} = \vec{\boldsymbol{b}} \tag{5.3}$$

je sústava lineárnych rovníc nad poľom F*. Nech ďalej*

$$\mathbf{M} \cdot \vec{\boldsymbol{x}} = \vec{\mathbf{0}} \tag{5.4}$$

je sústava homogénnych rovníc nad F*, majúca tú istú maticu sústavy. Nech sústava (5.3) je riešiteľná a* $\boldsymbol{\alpha} \in \boldsymbol{V}_n$ *je pevne zvolené riešenie sústavy (5.3). Nech ďalej* $\boldsymbol{S}$ *je podpriestor riešení sústavy (5.4). Potom množina všetkých riešení* S^* *sústavy (5.3) je*

$$S^* = \{\boldsymbol{\alpha} + \boldsymbol{\xi};\ \boldsymbol{\xi} \in \boldsymbol{S}\}.$$

Dôkaz. I. Dokážeme, že každý vektor tvaru $\boldsymbol{\alpha} + \boldsymbol{\xi}$ je riešením sústavy (5.3). Skutočne, platí $\mathbf{M} \cdot \boldsymbol{\alpha} = \vec{\boldsymbol{b}}$ a súčasne $\mathbf{M} \cdot \boldsymbol{\xi} = \vec{\mathbf{0}}$, odkiaľ $\mathbf{M} \cdot \boldsymbol{\alpha} + \mathbf{M} \cdot \boldsymbol{\xi} = \vec{\boldsymbol{b}} + \vec{\mathbf{0}}$, čiže $\mathbf{M} \cdot (\boldsymbol{\alpha} + \boldsymbol{\xi}) = \vec{\boldsymbol{b}}$, čo znamená, že $\boldsymbol{\alpha} + \boldsymbol{\xi}$ je riešenie sústavy (5.3).

II. Dokážeme, že každé riešenie sústavy (5.3) je tvaru $\boldsymbol{\alpha} + \boldsymbol{\xi}$. Nech $\boldsymbol{\beta}$ je ľubovoľné riešenie sústavy (5.3). Píšeme $\boldsymbol{\beta} = \boldsymbol{\alpha} + (\boldsymbol{\beta} - \boldsymbol{\alpha})$. Stačí dokázať, že $\boldsymbol{\beta} - \boldsymbol{\alpha}$ je riešením sústavy (5.4). To vyplýva takto: Je $\mathbf{M} \cdot \boldsymbol{\beta} = \vec{\boldsymbol{b}}$ a tiež $\mathbf{M} \cdot \boldsymbol{\alpha} = \vec{\boldsymbol{b}}$, odkiaľ $\mathbf{M} \cdot \boldsymbol{\beta} = \mathbf{M} \cdot \boldsymbol{\alpha}$, čiže $\mathbf{M}(\boldsymbol{\beta} - \boldsymbol{\alpha}) = \vec{\mathbf{0}}$. □

Príklad 5.3. Nad poľom racionálnych čísel riešme nasledujúcu sústavu lineárnych rovníc a množinu riešení sústavy vyjadrime pomocou podpriestoru riešení príslušnej sústavy homogénnych rovníc.

$$\begin{aligned}
x_1 - 2x_2 + 4x_3 + x_4 &= -6,\\
2x_1 + 3x_2 - x_3 + 2x_4 &= 13,\\
3x_1 + x_2 + 3x_3 + 3x_4 &= 7,\\
x_1 + 5x_2 - 5x_3 + x_4 &= 19.
\end{aligned}$$

Riešenie. Odčítaním násobkov prvej rovnice od ostatných rovníc získame ekvivalentný sústavu

$$\begin{aligned}
x_1 - 2x_2 + 4x_3 + x_4 &= -6,\\
7x_2 - 9x_3 &= 25.
\end{aligned} \tag{5.5}$$

Príslušná sústava homogénnych rovníc je

$$\begin{aligned}
x_1 - 2x_2 + 4x_3 + x_4 &= 0,\\
7x_2 - 9x_3 &= 0.
\end{aligned} \tag{5.6}$$

Položiac $x_3 = p_1, x_4 = p_2$ ľahko zistíme, že množina všetkých riešení sústavy (5.5) je

$$S^* = \Big\{\Big(\frac{8}{7} - \frac{10}{7}p_1 - p_2,\ \frac{25}{7} + \frac{9}{7}p_1,\ p_1,\ p_2\Big);\ p_1, p_2 \in Q\Big\}$$

a podpriestor riešení sústavy (5.6) je

$$\boldsymbol{S} = \Big\{\Big(-\frac{10}{7}p_1 - p_2,\ \frac{9}{7}p_1,\ p_1,\ p_2\Big);\ p_1,\ p_2 \in Q\Big\}.$$

Ak zvolíme vektor $\boldsymbol{\alpha} \in S^*$ tak, že položíme $p_1 = p_2 = 0$, t.j. $\boldsymbol{\alpha} = \big(\frac{8}{7}, \frac{25}{7}, 0, 0\big)$, hneď vidíme, že

$$\Big(\frac{8}{7} - \frac{10}{7}p_1 - p_2,\ \frac{25}{7} + \frac{9}{7}p_1,\ p_1,\ p_2\Big) = \Big(\frac{8}{7}, \frac{25}{7}, 0, 0\Big) + \Big(-\frac{10}{7}p_1 - p_2,\ \frac{9}{7}p_1,\ p_1,\ p_2\Big)$$

a teda

$$S^* = \{\boldsymbol{\alpha} + \boldsymbol{\xi},\ \boldsymbol{\xi} \in \boldsymbol{S}\}.$$

Ak v priestore $\boldsymbol{S}$ (čitateľ si skontroluje, že $d(\boldsymbol{S}) = 2$) zvolíme bázu

$$\boldsymbol{\varepsilon}_1 = \Big(-\frac{10}{7}, \frac{9}{7}, 1, 0\Big) \qquad \boldsymbol{\varepsilon}_2 = (-1, 0, 0, 1),$$

vidíme, že

$$S^* = \{\boldsymbol{\alpha} + p_1\boldsymbol{\varepsilon}_1 + p_2\boldsymbol{\varepsilon}_2;\ p_1,\ p_2 \in Q\}.$$

Príklad 5.4. Nad poľom $(Z_5, +, \cdot)$ riešte nasledujúcu sústavu lineárnych rovníc. Určte počet riešení sústavy. Množinu S^* všetkých riešení sústavy vyjadrite pomocou podpriestoru riešení príslušnej sústavy homogénnych rovníc.

$$\begin{aligned}
\bar{1}x_1 + \bar{4}x_2 + \bar{1}x_3 + \bar{1}x_4 + \bar{3}x_5 &= \bar{0},\\
\bar{2}x_1 + \bar{1}x_2 + \bar{4}x_3 + \bar{4}x_4 + \bar{1}x_5 &= \bar{1},\\
\bar{3}x_1 + \bar{3}x_2 + \bar{2}x_3 + \bar{2}x_4 + \bar{4}x_5 &= \bar{2},\\
\bar{4}x_1 \qquad\qquad\qquad\qquad\quad + \bar{2}x_5 &= \bar{3}.
\end{aligned}$$

Riešenie.

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

Prvý riadok sme násobili postupne $\bar{3}, \bar{2}, \bar{1}$ a pripočítali k druhému, tretiemu a štvrtému riadku. Podobne postupujeme ďalej: druhý riadok násobíme $\bar{3}$ a pripočítame k tretiemu potom $\bar{2}$ a pripočítame ku štvrtému

$$\to \begin{pmatrix} \bar{1} & \bar{4} & \bar{1} & \bar{1} & \bar{3} & \bar{0}\\ \bar{0} & \bar{3} & \bar{2} & \bar{2} & \bar{0} & \bar{1}\\ \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0}\\ \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} \end{pmatrix} \to \begin{pmatrix} \bar{1} & \bar{4} & \bar{1} & \bar{1} & \bar{3} & \bar{0}\\ \bar{0} & \bar{3} & \bar{2} & \bar{2} & \bar{0} & \bar{1} \end{pmatrix}.$$

Vidíme, že $h(\mathbf{M}) = h(\mathbf{M}') = 2$. Napíšeme sústavu ekvivalentnú s pôvodnou.

$$\begin{aligned}
\bar{1}x_1 + \bar{4}x_2 + \bar{1}x_3 + \bar{1}x_4 + \bar{3}x_5 &= \bar{0},\\
\bar{3}x_2 + \bar{2}x_3 + \bar{2}x_4 &= \bar{1}.
\end{aligned}$$

Položíme $x_3 = p_1,\ x_4 = p_2,\ x_5 = p_3$, kde $p_1,\ p_2,\ p_3 \in Z_5$.
Počítame $\bar{3}x_2 = \bar{1} - \bar{2}p_1 - \bar{2}p_2 = \bar{1} + \bar{3}p_1 + \bar{3}p_2$, odkiaľ $x_2 = \bar{2} + p_1 + p_2$.
Podobne $x_1 = -\bar{4}x_2 - x_3 - x_4 - \bar{3}x_5 = x_2 + \bar{4}x_3 + \bar{4}x_4 + \bar{2}x_5 =$
$= \bar{2} + p_1 + p_2 + \bar{4}p_1 + \bar{4}p_2 + \bar{2}p_3 = \bar{2} + \bar{2}p_3$.
Teda $S^* = \{(\bar{2} + \bar{2}p_3,\ \bar{2} + p_1 + p_2,\ p_1,\ p_2,\ p_3);\ p_1,\ p_2,\ p_3 \in Z_5\}$.

Podpriestor riešení príslušnej sústavy homogénnych rovníc je

$$\boldsymbol{S} = \{(\bar{2}p_3,\ p_1 + p_2,\ p_1,\ p_2,\ p_3);\ p_1,\ p_2,\ p_3 \in Z_5\}$$

Ak v S^* zvolíme pevný vektor $\boldsymbol{\alpha} = (\bar{2},\ \bar{2},\ \bar{0},\ \bar{0},\ \bar{0})$ a v $\boldsymbol{S}$ bázu

$$\begin{aligned} \boldsymbol{\varepsilon}_1 &= (\bar{0},\ \bar{1},\ \bar{1},\ \bar{0},\ \bar{0}), \\ \boldsymbol{\varepsilon}_2 &= (\bar{0},\ \bar{1},\ \bar{0},\ \bar{1},\ \bar{0}), \\ \boldsymbol{\varepsilon}_3 &= (\bar{2},\ \bar{0},\ \bar{0},\ \bar{0},\ \bar{1}), \end{aligned}$$

vidíme, že

$$S^* = \{\boldsymbol{\alpha} + p_1\boldsymbol{\varepsilon}_1 + p_2\boldsymbol{\varepsilon}_2 + p_3\boldsymbol{\varepsilon}_3;\ p_1,\ p_2,\ p_3 \in Z_5\}.$$

Keďže pre voľbu každého z parametrov máme 5 možností, sústava má $5^3 = 125$ riešení (t.j. množina S^* má 125 prvkov).

Cvičenia

5.1. Nájdite bázu podpriestoru riešení nasledujúcich sústav homogénnych lineárnych rovníc (na poľom racionálnych čísel).

a)
$$\begin{aligned} x_1 \phantom{{}-x_2} + 2x_3 + 5x_4 &= 0, \\ 3x_1 - x_2 + x_3 \phantom{{}+2x_4} &= 0, \\ 2x_1 - 3x_2 + 2x_3 + 2x_4 &= 0, \\ 2x_2 - x_3 - 7x_4 &= 0, \end{aligned}$$

b)
$$\begin{aligned} x_1 + x_2 - 3x_4 - x_5 &= 0, \\ x_1 - x_2 + 2x_3 - x_4 &= 0, \\ 4x_1 - 2x_2 + 6x_3 + 3x_4 - 4x_5 &= 0, \\ 2x_1 + 4x_2 - 2x_3 + 4x_4 - 7x_5 &= 0, \end{aligned}$$

c)
$$\begin{aligned} 3x_1 + 4x_2 - 5x_3 + 7x_4 &= 0, \\ 2x_1 - 3x_2 + 3x_3 - 2x_4 &= 0, \\ 4x_1 + 11x_2 - 13x_3 + 16x_4 &= 0, \\ 7x_1 - 2x_2 + x_3 + 3x_4 &= 0, \end{aligned}$$

d)
$$\begin{aligned} 3x_1 - x_2 - 2x_3 + x_4 + 8x_5 &= 0, \\ 9x_1 - 3x_2 + 4x_3 + 8x_4 + 9x_5 &= 0, \\ 3x_1 - x_2 + 2x_3 + 3x_4 + 2x_5 &= 0, \\ 3x_1 - x_2 + 4x_3 + 4x_4 - x_5 &= 0. \end{aligned}$$

5.2. Množinu riešení tých sústav z cvičení 4.1 a 4.7, ktoré majú riešenie, vyjadrite pomocou podpriestoru riešení príslušných sústav homogénnych rovníc.

***5.3.** Nech vektory

$$\begin{aligned} \alpha_1 &= (a_{11}, a_{12}, \dots, a_{1n}) \\ \alpha_2 &= (a_{21}, a_{22}, \dots, a_{2n}) \\ &\vdots \\ \alpha_h &= (a_{h1}, a_{h2}, \dots, a_{hn}) \end{aligned}$$

generujú podpriestor $\boldsymbol{S} = [\alpha_1, \alpha_2, \dots, \alpha_h]$ vektorového priestoru $\boldsymbol{V}_n(F)$. Potom existuje sústava $\mathcal{S}$ homogénnych rovníc nad poľom F taká, že podpriestor riešení sústavy $\mathcal{S}$ je práve $\boldsymbol{S}$. Dokážte to.

Návod. Je jasné, že keď taká sústava $\mathcal{S}$ existuje, existuje tiež sústava $\mathcal{S}'$ lineárne nezávislých homogénnych rovníc majúci ten istý podpriestor riešení $\boldsymbol{S}$. Dokážte, že riadky matice tejto sústavy sú práve vektory bázy riešení sústavy $\mathbf{A}\overline{x} = \overline{0}$, kde $\mathbf{A} = (a_{ij})$, pričom $i = 1, 2, \dots, n \quad j = 1, 2, \dots, h$.

5.4. Na základe predchádzajúceho cvičenia nájdite sústavy homogénnych rovníc, ktorých podpriestory riešení sú

(1) $[(1, -1, 3), (2, 2, 5), (1, -5, 4)] \subseteq\subseteq \boldsymbol{V}_3(Q)$
(2) $(1, 2, 3, 1), (1, -1, 1, -1), (2, 1, 4, 1) \subseteq\subseteq \boldsymbol{V}_4(Q)$
(3) $[(1, 1, 1, -1, 2), (1, 1, 2, 0, 3), (0, 0, -1, -1, -1)] \subseteq\subseteq \boldsymbol{V}_5(Q)$.

5.5. Nájdite podpriestor $\boldsymbol{S} \cap \boldsymbol{T}$, keď je dané

a) $\boldsymbol{S} = [(1, 2, -1, 3, 1), (-1, 0, -2, 1, -3), (1, 4, -4, 7, -1)]$,
$\boldsymbol{T} = [(0, 2, -3, 4, -2), (2, 2, 1, 2, 4), (2, 6, -5, 12, 3)]$
v priestore $\boldsymbol{V}_5(Q)$.

b) $\boldsymbol{S} = [(\overline{1}, \overline{3}, \overline{0}, \overline{2}), (\overline{0}, \overline{2}, \overline{3}, \overline{1}), (\overline{1}, \overline{0}, \overline{1}, \overline{2})]$, $\qquad \boldsymbol{T} = [(\overline{1}, \overline{0}, \overline{2}, \overline{2}), (\overline{3}, \overline{3}, \overline{0}, \overline{1})]$
v priestore $\boldsymbol{V}_4(Z_5)$.

Návod. Najprv nájdite sústavu homogénnych rovníc pre $\boldsymbol{S}$, potom pre $\boldsymbol{T}$, nakoniec riešte sústavu, ktorá vznikne zjednotením týchto sústav.

***5.6.** Ukážte, že jednorozmerných podpriestorov vektorového priestoru $V_4(Z_5)$ je práve toľko, ako trojrozmerných podpriestorov tohto priestoru. Koľko ich je?

5.7. Riešte sústavy rovníc (nad Q) a urobte diskusiu vzhľadom na dané parametre

$$a)\quad \begin{aligned} px - 4y - z &= 0, \\ 4x - 6y - 3z &= 0, \\ x + y - pz &= 0, \end{aligned} \qquad b)\quad \begin{aligned} ax + y + z &= 0, \\ x + qy + z &= 0, \\ x + y + rz &= 0, \end{aligned}$$

kde $p, q, r \in Q$.

5.8. V nasledujúcej sústave rovníc (nad Q) zistite, za akej podmienky je možné voliť parametre práve za neznáme z a t. Pri platnosti tejto podmienky sústavu rozriešte.

$$\begin{aligned} y + az + bt &= 0, \\ -x \qquad + cz + dt &= 0, \\ ax + cy \qquad - et &= 0, \\ bx + dy + ez \qquad &= 0, \end{aligned}$$

kde $a, b, c, d, e \in Q$.

5.9. Nech je daná sústava homogénnych lineárnych rovníc s n neznámymi nad poľom Q majúca len celočíselmé koeficienty. Predpokladajme ďalej, že sústava má aj netriviálne riešenie. Dokážte, že každú zložku parametrického riešenia sústavy možno vyjadriť ako lineárnu kombináciu racionálnych parametrov tak, že koeficienty sú len celé čísla.
Návod. Všimnite si riešenie príkladu 4.5 a poznámku 4.2.

5.10. Podľa predchádzajúceho cvičenia vyjadrite každú zložku parametrických riešení nasledujúcich sústav ako lineárnu kombináciu racionálnych parametrov s celočíselnými koeficientami.

$a)$
$$\begin{aligned} 2x_1 - x_2 + 5x_3 + 7x_4 &= 0, \\ 4x_1 - 2x_2 + 7x_3 + 5x_4 &= 0, \\ 2x_1 - x_2 + x_3 - 5x_4 &= 0, \end{aligned}$$

$b)$
$$\begin{aligned} 2x_1 + 7x_2 + 4x_3 + 5x_4 + 8x_5 &= 0, \\ 4x_1 + 4x_2 + 8x_3 + 5x_4 + 4x_5 &= 0, \\ x_1 - 9x_2 - 3x_3 - 5x_4 - 14x_5 &= 0, \\ 3x_1 + 5x_2 + 7x_3 + 5x_4 + 6x_5 &= 0, \end{aligned}$$

$c)$
$$\begin{aligned} 3x_1 + 4x_2 + 3x_3 + 9x_4 + 6x_5 &= 0, \\ 9x_1 + 8x_2 + 5x_3 + 6x_4 + 9x_5 &= 0, \\ 3x_1 + 8x_2 + 7x_3 + 30x_4 + 15x_5 &= 0, \\ 6x_1 + 6x_2 + 4x_3 + 7x_4 + 5x_5 &= 0. \end{aligned}$$

Kapitola 4

DETERMINANTY

Teória determinantov je ďalšou časťou lineárnej algebry, jej základy vyložíme v tomto paragrafe. Začneme príkladom.

Príklad 1.1. Predpokladajme, že nasledujúca sústava dvoch rovníc s dvoma neznámymi nad poľom reálnych čísel má práve jedno riešenie, t.j. $h(\mathbf{M}) = h(\mathbf{M}') = 2$.

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 &= b_1, \\ a_{21}x_1 + a_{22}x_2 &= b_2. \end{aligned}$$

Keď danú sústavu vyriešime, dostaneme

$$x_1 = \frac{b_1a_{22} - b_2a_{12}}{a_{11}a_{22} - a_{12}a_{21}}, \qquad x_2 = \frac{a_{11}b_2 - b_1a_{21}}{a_{11}a_{22} - a_{12}a_{21}}. \tag{1.1}$$

Oba uvedené zlomky majú zmysel. O tom sa presvedčíme takto: Najskôr uvažujme o prípade, keď jedno z čísel $a_{11}, a_{12}, a_{21}, a_{22}$ sa rovná nule. Nech napr. $a_{11} = 0$. Potom čísla a_{12}, a_{21} sú rôzne od nuly. Naozaj, ak by aj $a_{12} = 0$, bolo by tiež $b_1 = 0$, mali by sme najviac jednu „nenulovú" rovnicu a daná sústava by mal viac ako jedno riešenie. Ak by $a_{21} = 0$, nemali by sme sústavu s dvoma neznámymi. Za týchto podmienok je výraz $a_{11}a_{22} - a_{12}a_{21} \neq 0$. Nech teda sú všetky koeficienty na ľavých stranách rovníc sústavy rôzne od nuly. Ak by $a_{11}a_{22} - a_{12}a_{21} = 0$, tak $\frac{a_{11}}{a_{21}} = \frac{a_{12}}{a_{22}} = k$, čiže $a_{11} = ka_{21}, a_{12} = ka_{22}$, odkiaľ $h(\mathbf{M}) \leqq 1$, čo nie je.

Teraz označme

$$ad - bc = \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

Použitím tohoto označenia napíšeme (1.1) v tvare

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}} \qquad x_2 = \frac{\begin{vmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}} \tag{1.2}$$

Riešenie je napísané prehľadne, lebo koeficienty sú v menovateli usporiadané tak, ako v matici sústavy a v čitateli stĺpec pri neznámej, ktorú sme vypočítali je nahradený stĺpcom „z druhých strán".

Zápis $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ nazývame determinant druhého stupňa a vypočítame ho, keď od súčinu prvkov hlavnej diagonály odčítame súčin prvkov vedľajšej diagonály. Je to tzv. „krížové pravidlo“.

V nasledujúcom paragrafe ukážeme, že podobným spôsobom možno vyjadriť aj riešenie sústavy rovníc s n neznámymi. Ak je $h(\mathbf{M}) = h(\mathbf{M}') = n$, musíme použiť determinanty n-tého stupňa. Prv však než si takýto determinant definujeme a naučíme sa ho vypočítať musíme si povedať niečo o permutáciách.

Definícia 1.1. Nech je daná množina $A = \{1, 2, \dots, n\}$. *Permutáciou* n prvkov budeme nazývať bijekciu $\pi : A \to A$. Permutáciu budeme zapisovať

$$\pi = \begin{pmatrix} 1, & 2, & \dots, & i, & \dots, & n \\ k_1, & k_2, & \dots, & k_i, & \dots, & k_n \end{pmatrix}, \tag{1.3}$$

kde $k_i = \pi(i)$ pre $i = 1, 2, \dots, n$.

Permutáciu teda úplne určuje poradie prvkov (usporiadaná n-tica rôznych prvkov) druhého riadku (1.3). Zo strednej školy vieme, že počet všetkých permutácií n prvkov (počet všetkých rôznych poradí n prvkov) je $n!$. Napr. počet permutácií 3 prvkov je $3! = 6$. Sú to tieto permutácie, ktoré sme už uviedli v príklade 2.3 kapitoly 2

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ x_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Množinu všetkých permutácií n prvkov budeme označovať P_n. Ako sme povedali, permutáciu (1.3) úplne určuje poradie $(k_1, k_2, \dots, k_n)$. Budeme hovoriť, že na danom poradí je *inverzia* ak pre $i < j$ platí $k_i > k_j$. Počet inverzií na danom poradí určíme napr. takto: škrtneme 1 a určíme počet s_1 prvkov, ktoré sa v poradí nachádzajú pred 1, škrtneme 2 a určíme počet s_2 (neškrtnutých) prvkov nachádzajúcich sa pred 2 atď. Počet inverzií je $s_1 + s_2 + \dots + s_n$. Napr. v poradí 7 prvkov $(3, 1, 7, 5, 2, 4, 6)$ je $1 + 3 + 0 + 2 + 1 + 1 + 0 = 8$ inverzií. Budeme hovoriť, že permutácia je *párna (nepárna)* ak na poradí, ktoré ju určuje je párny (nepárny) počet inverzií. Predpokladajme $n \geqq 2$. Čitateľ nech si premyslí, že ak na danom poradí vykonáme výmenu prvkov 1 a 2 počet inverzií vzrastie alebo klesne o jeden. Teda touto výmenou z párnej permutácie dostaneme nepárnu a naopak. Odtiaľ vyplýva, že ak označíme počet nepárnych permutácií $n(\geqq 2)$ prvkov l_1 a počet párnych permutácií l_2, platí $l_1 = l_2 = \frac{1}{2}n!$. Skutočne, ak v druhom riadku každej nepárnej permutácie vymeníme prvky 1 a 2, dostaneme párnu permutáciu, t.j. $l_1 \leqq l_2$, analogicky je $l_2 \leqq l_1$. Čitateľ si skontroluje, že uvedené permutácie 3 prvkov π_1, π_2, π_3 sú párne, π_4, π_5, π_6 sú nepárne. Počet inverzií v permutácii π budeme označovať $s(\pi)$. Teraz sme už pripravení na definíciu determinantu n-tého stupňa.

Definícia 1.2. Nech je daná štvorcová matica typu $n \times n$ nad poľom F:

$$\mathbf{A} = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \vdots & & & \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} \end{pmatrix}.$$

Determinantom $d(\mathbf{A})$ matice $\mathbf{A}$ nazývame sumu

$$d(\mathbf{A}) = \sum_{\pi \in P_n} (-1)^{s(\pi)} a_{1i_1} a_{2i_2} \dots a_{ni_n},$$

kde $\pi = \begin{pmatrix} 1, & 2, & \dots, & n \\ i_1, & i_2, & \dots, & i_n \end{pmatrix}$. Sčíta sa teda „cez všetky permutácie stĺpcových indexov“ pri pevnom poradí riadkových indexov. Znamienko sčítanca je „plus“, ak príslušná permutácia je párna, „mínus“ v opačnom prípade.

Determinant $d(\mathbf{A})$ tiež označujeme

$$d(\mathbf{A}) = |\mathbf{A}| = \begin{vmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \vdots & & & \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} \end{vmatrix}$$

a nazývame ho determinantom n-tého stupňa.

Príklad 1.2. Podľa definície 1.2 vypočítame determinanty matíc

$$\mathbf{A} = (a_{11}), \qquad \mathbf{B} = \begin{pmatrix} a_{11}, & a_{12} \\ a_{21}, & a_{22} \end{pmatrix}, \qquad \mathbf{C} = \begin{pmatrix} a_{11}, & a_{12}, & a_{13} \\ a_{21}, & a_{22}, & a_{23} \\ a_{31}, & a_{32}, & a_{33} \end{pmatrix}.$$

$|\mathbf{A}| = (-1)^0 a_{11} = a_{11}$, t.j. determinant matice typu 1×1 sa rovná (jedinému) prvku matice.

$$|\mathbf{B}| = \begin{vmatrix} a_{11}, & a_{12} \\ a_{21}, & a_{22} \end{vmatrix} = \sum_{\pi \in P_2} (-1)^{s(\pi)} \cdot a_{1i_1} \cdot a_{2i_2} =$$

$$= (-1)^0 a_{11} a_{22} + (-1)^1 a_{12} a_{21} = a_{11} a_{22} - a_{12} a_{21}.$$

Je vidieť, že sme dostali „krížové pravidlo“:

$$\begin{matrix} a_{11} & a_{12} \\ & \\ a_{21} & a_{22} \\ - & & + \end{matrix}$$

Od súčinu prvkov hlavnej diagonály odčítame súčin prvkov vedľajšej diagonály.

Napríklad:

$$\begin{vmatrix} 1 & -2 \\ 3 & 2 \end{vmatrix} = 1 \cdot 2 - (-2) \cdot 3 = 2 + 6 = 7.$$

Podobne vypočítame $d(\mathsf{C})$.

$$|\mathsf{C}| = \begin{vmatrix} a_{11}a_{12}a_{13} \\ a_{21}a_{22}a_{23} \\ a_{31}a_{32}a_{33} \end{vmatrix} = \sum_{\pi \in P_3} (-1)^{s(\pi)} a_{1i_1} a_{2i_2} a_{3i_3} =$$

$$= (-1)^0 a_{11}a_{22}a_{33} + (-1)^2 a_{12}a_{23}a_{31} + (-1)^2 a_{13}a_{21}a_{32} +$$

$$+ (-1)^3 a_{13}a_{22}a_{31} + (-1)^1 a_{12}a_{21}a_{33} + (-1)^1 a_{11}a_{23}a_{32}.$$

Práve vypočítaný výsledok sa používa aj pri praktickom výpočte hodnoty determinantu tretieho stupňa. Na jeho lepšie zapamätanie uvedieme mnemotechnickú pomôcku známu ako Sarrusovo pravidlo:

$$\begin{array}{ccccc} & a_{11} & a_{12} & a_{13} & \\ & a_{21} & a_{22} & a_{23} & \\ & a_{31} & a_{32} & a_{33} & \\ - & a_{11} & a_{12} & a_{13} & + \\ - & a_{21} & a_{22} & a_{23} & + \\ - & & & & + \end{array}$$

Prvé dva riadky determinantu napíšeme pod determinant ešte raz. Hodnotu determinantu dostaneme, ak od súčtu súčinov trojíc označených znamienkom „+“ odčítame súčet súčinov trojíc označených znamienkom „−“.

Sarrusovo pravidlo sa často používa aj v zjednodušenej forme. Nemusíme žiadne riadky znovu vypisovať, ak výber príslušných trojíc a ich znamienok vykonáme podľa nasledovnej schémy.

Súčinom spojených prvkov determinantu priradíme znamienko „+“. Zvýraznený smer je „smer hlavnej diagonály“.

Súčinom spojených prvkov determinantu priradíme znamienko „−“. Zvýraznený smer je „smer vedľajšej diagonály“.

Napríklad:

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

$$= 4 + 0 - 12 - 0 - 12 - 4 = -24.$$

Z definície 1.2 vyplýva, že determinant n-tého stupňa má $n!$ členov, ktorých polovici priraďujeme znamienko „+“, druhej polovici „−“. Príklad 1.2. ukazuje, že v prípade $n = 2, 3$ determinant pohodlne vypočítame podľa definície, t.j. krížovým alebo Sarrusovým pravidlom. Keďže $4! = 24$, už počítanie determinantu štvrtého stupňa podľa definície by bolo zdĺhavé. V ďalšom dokážeme také vlastnosti determinantu, ktoré umožnia počítať ho oveľa pohodlnejšie.

Veta 1.1. *Nech $\mathbf{A}$ je štvorcová matica (nad poľom F) a $\mathbf{A}^T$ je transponovaná matica k matici $\mathbf{A}$. Potom $d(\mathbf{A}) = d(\mathbf{A}^T)$.*

Inými slovami: *Determinant sa nezmení, ak v ňom vymeníme stĺpce za riadky.*

Dôkaz. Nech pre určitosť $\mathbf{A} = (a_{ij})$, $\mathbf{A}^T = (b_{ij})$, kde $i, j = 1, 2, \dots, n$, pričom platí $a_{ij} = b_{ji}$. Podľa definície

$$d(\mathbf{A}) = \sum_{\pi \in P_n} (-1)^{s(\pi)} a_{1i_1} a_{2i_2} \dots a_{ni_n}, \tag{1.4}$$

$$d(\mathbf{A}^T) = \sum_{\pi' \in P_n} (-1)^{s(\pi')} b_{1j_1} b_{2j_2} \dots b_{nj_n}. \tag{1.5}$$

Zoberme ľubovoľný člen $(-1)^{s(\pi)} a_{1i_1} a_{2i_2} \dots a_{ni_n}$ determinantu $d(\mathbf{A})$. Usporiadajme ho podľa stĺpcových indexov. Máme

$$(-1)^{s(\pi)} a_{1i_1} a_{2i_2} \dots a_{n1_n} = (-1)^{s(\pi)} \cdot a_{j_1 1} \cdot a_{j_2 2} \dots a_{j_n n} = (-1)^{s(\pi)} b_{1j_1} b_{2j_2} \dots b_{nj_n}.$$

Aby sme dokončili dôkaz, musíme dokázať $s(\pi) = s(\pi')$. To je ale zrejmé, lebo každej inverzii $i_s > i_t$ pri $s < t$ v permutácii π zodpovedá inverzia $j_{i_t} > j_{i_s}$ v permutácii π', pričom $j_{i_t} = t$, $j_{i_s} = s$. Teda platí $(-1)^{s(\pi)} b_{1j_1} \cdot b_{2j_2} \dots b_{nj_n} = (-1)^{s(\pi')} b_{1j_1} b_{2j_2} \dots b_{nj_n}$. □

Dôsledok. *Každé tvrdenie dokázané pre riadky determinantu platí aj pre jeho stĺpce.*

Veta 1.2. *Nech $\mathbf{B}$ je štvorcová matica, ktorá vznikne z matice $\mathbf{A}$ výmenou i-tého a j-tého riadku. Potom $d(\mathbf{B}) = -d(\mathbf{A})$.*

Dôkaz. Nech matice $\mathbf{A}, \mathbf{B}$ sú

$$\mathbf{A} = \begin{pmatrix} a_{11}, & \dots, & a_{1n} \\ \vdots & & \\ a_{i1}, & \dots, & a_{in} \\ \vdots & & \\ a_{j1}, & \dots, & a_{jn} \\ \vdots & & \\ a_{n1}, & \dots, & a_{nn} \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} b_{11}, & \dots, & b_{1n} \\ \vdots & & \\ b_{i1}, & \dots, & b_{in}, \\ \vdots & & \\ b_{j1}, & \dots, & b_{jn} \\ \vdots & & \\ b_{n1}, & \dots, & b_{nn} \end{pmatrix},$$

kde $i < j$ a platí $b_{ik} = a_{jk}$, $b_{jk} = a_{ik}$ pre $k = 1, 2, \dots, n$ a $a_{rs} = b_{rs}$ pre $r \neq i$, $r \neq j$.

Vezmime ľubovoľný člen determinantu $d(\mathbf{B})$:

$$\begin{aligned} c' &= (-1)^{s(\pi')} b_{1k_1} \cdot b_{2k_2} \dots b_{ik_i} \dots b_{jk_j} \dots b_{nk_n} = \\ &= (-1)^{s(\pi')} a_{1k_1} \cdot a_{2k_2} \dots a_{jk_i} \dots a_{ik_j} \dots a_{nk_n} = \\ &= (-1)^{s(\pi')} a_{1k_1} a_{2k_2} \dots a_{ik_j} \dots a_{jk_i} \dots a_{nk_n}, \end{aligned}$$

kde

$$\pi' = \begin{pmatrix} 1, & 2, & \dots, & i, & \dots, & j, & \dots, & n \\ k_1, & k_2, & \dots, & k_i, & \dots, & k_j, & \dots, & k_n \end{pmatrix}.$$

Tomuto členu však jednoznačne zodpovedá (t.j. líši sa od neho najviac ak znamienkom) nasledujúci člen determinantu $d(\mathbf{A})$.

$$c = (-1)^{s(\pi)} a_{1k_1} \cdot a_{2k_2} \dots a_{ik_j} \dots a_{jk_i} \dots a_{nk_n},$$

kde

$$\pi = \begin{pmatrix} 1, & 2, & \dots, & i, & \dots, j, & \dots, & n \\ k_1, & k_2, & \dots, & k_j, & \dots, k_i, & \dots, & k_n \end{pmatrix}.$$

Dokážeme, že $(-1)^{s(\pi')} \neq (-1)^{s(\pi)}$, t.j. že $c' = -c$. Skutočne, čísla $s(\pi')$, $s(\pi)$ sú rôznej parity. To dokážeme takto: Vidieť, že permutácie π' a π sa líšia len tým, že v druhom riadku sú vymenené čísla k_i a k_j. Budeme rozoznávať dva prípady.

a) Nech $j = i + 1$, potom ak $k_i < k_j$, tak $k_j > k_i$ a naopak. To jest permutácia π má práve o jednu inverziu menej alebo viac ako π'.

b) Nech $j = i + u$ potom výmenu k_i za k_j v druhom riadku π' možno uskutočniť takýmito výmenami: k_i za k_{i+1}, k_i za $k_{i+2}, \dots,$, k_i za k_{i+u}, spolu u výmen, potom spätnou výmenou $k_j = k_{i+u}$ za k_{i+u-1}, k_j za $k_{i+u-2}, \dots$, k_j za k_{i+1}, spolu $u - 1$ spätných výmen. Máme tak spolu $2u - 1$ výmen (nepárny počet). Pri každej klesne alebo vzrastie počet inverzií o 1. Teda permutácie π a π' sú opačnej parity. Dokázali sme, že každému členu determinantu $d(\mathbf{B})$ zodpovedá práve jeden*) člen determinantu $d(\mathbf{A})$ rovnakej absolútnej hodnoty ale rôzneho znamienka. Odtiaľ vyplýva $d(\mathbf{B}) = -d(\mathbf{A})$, čo sme chceli dokázať. □

Dôsledok. *Ak štvorcová matica* $\mathbf{A}$ *má dva riadky rovnaké, tak* $d(\mathbf{A}) = 0$.

Dôkaz. Ak vymeníme v danej matici tieto dva riadky (povedzme i-tý a j-tý), determinant sa vôbec nezmení. Odtiaľ vyplýva, že každý člen determinantu „priradený“ permutácii π' sa ruší s členom „priradeným“ permutácii π opačnej parity, ktorú sme z nej dostali výmenou čísel k_i a k_j. Teda $d(\mathbf{A}) = 0$. □

Príklad 1.3. Presvedčte sa, že

$$\begin{vmatrix} 3 & 1 & 2 \\ 4 & -1 & 3 \\ 1 & 1 & -1 \end{vmatrix} = 11, \quad \begin{vmatrix} 3 & 1 & 2 \\ 1 & 1 & -1 \\ 4 & -1 & 3 \end{vmatrix} = -11, \quad \begin{vmatrix} 3 & -2 & 1 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{vmatrix} = 0.$$

*) Čitateľ si rozmyslí, že ak v druhom riadku každej permutácie z P vykonáme výmenu prirodzených čísel k a k, dostaneme opäť všetky permutácie množiny P.

Definícia 1.3. Nech je daná štvorcová matica $\mathbf{A}$ typu $n \times n$, kde $n \geqq 2$.

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & & & & & \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & & & & & \\ a_{n1} & a_{n2} & \dots & a_{nj} & \dots & a_{nn} \end{pmatrix}, \tag{1.6}$$

nech matica $\mathbf{A}_{ij}$ typu $(n-1)\times(n-1)$ vznikne z matice $\mathbf{A}$ vynechaním i-teho riadku a j-teho stĺpca. Determinant $|\mathbf{A}_{ij}|$ nazývame *subdeterminantom* $(n-1)$-ho stupňa matice $\mathbf{A}$. Hovoríme tiež, že subdeterminant $|\mathbf{A}_{ij}|$ *patrí* k prvku a_{ij}. *Algebraický doplnok* A_{ij} *patriaci k prvku* a_{ij} definujeme takto:

$$A_{ij} = (-1)^{i+j}|\mathbf{A}_{ij}|.$$

Veta 1.3. *Nech je daná matica* $\mathbf{A}$ *typu* $n \times n$ *(matica (1.6)). Potom*

$$d(\mathbf{A}) = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in}. \tag{1.7}$$

Inými slovami: *Determinant sa rovná súčtu súčinov prvkov i-teho (teda ľubovoľného) riadku a príslušných algebraických doplnkov.*

Poznámka 1.1. Ak determinant $d(\mathbf{A})$ napíšeme vo forme (1.7) hovoríme, že sme ho rozvinuli podľa i-teho riadku.

Dôkaz vety 1.3. Podľa definície máme

$$d(\mathbf{A}) = \sum_{\pi \in P_n} (-1)^{s(\pi)} a_{1j_1} \cdot a_{2j_2} \dots a_{ij_i} \dots a_{nj_n}. \tag{1.8}$$

V každom člene sumy (1.8) sa nachádza práve jeden prvok i-teho riadku matice $\mathbf{A}$, pričom a_{i1} sa nachádza v $n!/n = (n-1)!$ členoch. Podobne aj ďalšie prvky $a_{i2}, a_{i3}, \dots, a_{ij}, \dots, a_{in}$. Preto $d(\mathbf{A})$ sa dá vyjadriť v tvare

$$\begin{aligned} d(\mathbf{A}) = {} & a_{i1}\sum(-1)^{s(\pi_1)} a_{1j_1} a_{2j_2} \dots a_{i-1,j_{i-1}} a_{i+1,j_{i+1}} \dots a_{nj_n} + \\ & + a_{i2}\sum(-1)^{s(\pi_2)} a_{1j_1} a_{2j_2} \dots a_{i-1,j_{i-1}} a_{i+1,j_{i+1}} \dots a_{nj_n} + \\ & \vdots \\ & + a_{ij}\sum(-1)^{s(\pi_j)} a_{1j_1} a_{2j_2} \dots a_{i-1,j_{i-1}} a_{i+1,j_{i+1}} \dots a_{nj_n} + \\ & \vdots \\ & + a_{in}\sum(-1)^{s(\pi_n)} a_{1j_1} a_{2j_2} \dots a_{i-1,j_{i-1}} a_{i+1,j_{i+1}} \dots a_{nj_n}, \end{aligned}$$

kde prvá suma sa vykoná cez všetky permutácie tvaru

$$\pi_1 = \begin{pmatrix} 1, & 2, & \dots, & i-1, & i & i+1, & \dots, & n \\ j_1, & j_2, & \dots, & j_{i-1}, & 1, & j_{i+1}, & \dots, & j_n \end{pmatrix},$$

druhá cez permutácie tvaru

$$\pi_2 = \begin{pmatrix} 1, & 2, & \dots, & i-1, & i, & i+1, & \dots, & n \\ j_1, & j_2, & \dots, & j_{i-1}, & 2, & j_{i+1}, & \dots, & j_n \end{pmatrix},$$

$$\vdots$$

j-tá cez permutácie tvaru

$$\pi_j = \begin{pmatrix} 1, & 2, & \dots, & i-1, & i, & i+1, & \dots, & n \\ j_1, & j_2, & \dots, & j_{i-1}, & j, & j_{i+1}, & \dots, & j_n \end{pmatrix}. \tag{1.9}$$

Takto postupujeme ďalej až po permutáciu π_n.

Teda $d(\mathbf{A})$ môžeme vyjadriť

$$d(\mathbf{A}) = \sum_{j=1}^{n} a_{ij} \sum_{\pi_j} (-1)^{s(\pi_j)} a_{1j_1} \cdot a_{2j_2} \dots a_{i-1,j_{i-1}} a_{i+1,j_{i+1}} \dots a_{nj_n}, \tag{1.10}$$

kde druhá suma sa vykoná cez všetky permutácie (1.9), ktoré majú fixovaný prvok j na i-tom mieste v druhom riadku.

Na druhej strane subdeterminant $|\mathbf{A}_{ij}|$ vypočítame

$$|\mathbf{A}_{ij}| = \sum (-1)^{s(\pi')} a_{ij_1} a_{2j_2} \dots a_{i-1,j_{i-1}} a_{i+1,j_{i+1}} \dots a_{nj_n},$$

kde sa sčíta cez všetky permutácie tvaru

$$\pi' = \begin{pmatrix} 1, & 2, & \dots, & i-1, & i+1, & \dots, & n \\ j_1, & j_2, & \dots, & j_{i-1}, & j_{i+1}, & \dots, & j_n \end{pmatrix}.$$

Aby sme dokončili dôkaz, treba nám vyjadriť paritu permutácie π_j pomocou parity permutácie π'. Uvažujeme takto: Z poradia $j_1, j_2, \dots, j_{i-1}, j, j_{i+1}, \dots, j_n$ dostaneme poradie $j, j_1, j_2, \dots, j_{i-1}, j_{i+1}, \dots, j_n$ pomocou $i-1$ výmen susedných prvkov. Parita poradia sa tým zmenila $i-1$ razy. Ak teraz prvok j na začiatku poradia zrušíme, stratí sa tým $j-1$ inverzií. Paritu permutácie π' teda dostaneme z parity permutácie π_j, ak na nej vykonáme $i-1+j-1 = i+j-2$ zmien parity, čiže $(-1)^{s(\pi')} = (-1)^{s(\pi_j)+i+j-2}$. Máme teda $(-1)^{s(\pi_j)} = (-1)^{i+j} \cdot (-1)^{s(\pi')}$. Preto z (1.10) dostaneme

$$d(\mathbf{A}) = \sum_{j=1}^{n} a_{ij} \sum (-1)^{i+j} \cdot (-1)^{s(\pi')} a_{ij_1} a_{ij_2} \dots a_{i-1,j_{i-1}} a_{i+1,j_{i+1}} \dots a_{nj_n} =$$

$$= \sum_{j=1}^{n} a_{ij} (-1)^{i+j} |\mathbf{A}_{ij}| = \sum_{j=1}^{n} a_{ij} A_{ij},$$

čo sme chceli dokázať. □

Príklad 1.4. Nasledujúci determinant rozvinieme podľa prvého riadku.

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

$$+2(-1)^{1+3}\begin{vmatrix} 4 & -1 \\ 1 & 1 \end{vmatrix} = 3(-2) + 1(-1)\cdot(-7) + 2\cdot 5 = 11.$$

Ďalší determinant rozvinieme podľa tretieho stĺpca.

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

$$+3(-1)^{3+3}\begin{vmatrix} 1 & -1 & 2 \\ 4 & 1 & 2 \\ 1 & 0 & 3 \end{vmatrix} + 0\cdot(-1)^{4+3}\begin{vmatrix} 1 & -1 & 2 \\ 4 & 1 & 2 \\ 1 & -1 & 1 \end{vmatrix} = 3\cdot(-12) + 3\cdot 11 = -3.$$

Vidíme, že veta 1.3 nám umožňuje vypočítať determinant ľubovoľne vysokého stupňa postupným prevodom na výpočet determinantov nižších stupňov. Takýto výpočet nie je vždy výhodný. Môže byť značne zdĺhavý. Za chvíľu uvedieme postup značne efektívnejší. Najprv však sformulujeme niekoľko dôsledkov vety 1.3.

Dôsledok 1. *Nech matica* $\mathbf{B}$ *vznikne zo štvorcovej matice* $\mathbf{A}$ *tak, že* i*-tý riadok matice* $\mathbf{A}$ *vynásobíme prvkom* $c \in F$. *Potom* $d(\mathbf{B}) = c \cdot d(\mathbf{A})$.

Dôsledok 2. *Nech každý prvok* i*-teho riadku štvorcovej matice* $\mathbf{A}$ *je súčtom dvoch sčítancov takto:*

$$\begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ \vdots & & & \\ a_{i1}+a'_{i1}, & a_{i2}+a'_{i2}, & \dots, & a_{in}+a'_{in} \\ \vdots & & & \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} \end{pmatrix}.$$

Potom

$$d(\mathbf{A}) = \begin{vmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ \vdots & & & \\ a_{i1}, & a_{i2}, & \dots, & a_{in} \\ \vdots & & & \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ \vdots & & & \\ a'_{i1}, & a'_{i2}, & \dots, & a'_{in} \\ \vdots & & & \\ a_{n1}, & a_{n2}, & \dots, & a_{in} \end{vmatrix}$$

Dôsledok 3. *Hodnota determinantu sa nezmení, ak* i*-temu riadku determinantu pripočítame lineárnu kombináciu ostatných riadkov determinantu.*

Dôsledok 4. *Súčet súčinov prvkov i-teho riadku determinantu a algebraických doplnkov patriacich k j-temu riadku $(j \neq i)$ sa rovná nule, t.j.*

$$0 = a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn},$$

kde $i \neq j$.

Dôkazy dôsledkov ponecháme na čitateľa. Na dôkaz dôsledku 1 a 2 stačí rozvinúť determinant podľa i-teho riadku. Je jasné, že dôsledok 2 možno zovšeobecniť tak, že prvky i-teho riadky sú súčty $k(\geqq 2)$ sčítancov (vykonajte!). Dôkazy dôsledkov 3 a 4 vyplývajú z dôsledkov 1, 2 a z dôsledku vety 1.2.

Veta 1.4. *Determinant sa rovná nule práve vtedy, keď jeho riadky sú lineárne závislé.*

Dôkaz. I. Ak riadky determinantu D sú lineárne závislé, tak aspoň jeden z nich je lineárnou kombináciou ostatných. Podľa dôsledku 3 ľahko nájdeme determinant rovnakej hodnoty majúci jeden riadok nulový. Odtiaľ rozvinutím podľa nulového riadku dostaneme $D = 0$.

II. Na dokončenie dôkazu je treba dokázať, že ak sa determinant rovná nule, tak jeho riadky sú lineárne závislé. Toto tvrdenie je jednoduchým dôsledkom vety 2.1, ktorú dokážeme v nasledujúcom paragrafe. □

Poznámka 1.2. Poznamenávame, že vetu 1.4 možno preformulovať takto: *Determinant sa rovná nule práve vtedy, keď aspoň jeden jeho riadok je lineárnou kombináciou ostatných riadkov.*

Veta 1.3 spolu s dôsledkami nám dáva prostriedky na „výhodný“ výpočet determinantu. Podobne ako pri výpočte hodnosti matice aj tu budeme používať elementárne riadkové (stĺpcové) operácie. Musíme si však uvedomiť, že výmenou dvoch riadkov (stĺpcov) sa zmení znamienko determinantu (veta 1.2). Ak násobíme jeden riadok determinantu prvkom poľa $c \in F$, tak celý determinant násobíme týmto prvkom (dôsledok vety 1.3). Konečne z dôsledku 3 vety 1.3 vyplýva, že ero typu 3 nemení hodnotu determinantu. Výpočet determinantu vykonáme tak, že najprv pomocou ero alebo eso dosiahneme, že v niektorom riadku (stĺpci) je práve jeden prvok rôzny od nuly. Potom rozvinieme determinant podľa tohoto riadku (stĺpca). Dostaneme determinant so stupňom o 1 menším. Tak postupujeme ďalej až kým nedostaneme determinant stupňa tri alebo dva, ktorý vypočítame Sarrusovým alebo krížovým pravidlom.

Príklad 1.5. Vypočítajme determinant

$$\begin{vmatrix} 1 & -1 & 3 & 2 \\ 4 & 1 & 0 & 2 \\ 1 & -1 & 3 & 1 \\ 1 & 0 & 0 & 3 \end{vmatrix}.$$

Prvý riadok vynásobíme -1 a pripočítame k tretiemu, dostaneme:

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

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

Príklad 1.6. Vypočítajte determinant

$$\begin{vmatrix} 5 & -10 & -10 & 15 & 25 & 5 \\ 2 & 1 & 0 & 3 & 2 & -1 \\ 4 & 5 & 3 & 0 & 8 & 3 \\ -1 & 4 & 2 & -3 & 5 & 8 \\ 2 & 2 & 0 & 6 & 2 & 2 \\ 1 & 0 & 5 & 3 & 2 & 0 \end{vmatrix}.$$

Z prvého riadku možno 5 „vyložiť pred determinant“ (t.j. riadok vynásobiť 1/5 a celý determinant 5-timi). Ďalej z piateho riadku vyložíme 2 a zo štvrtého stĺpca 3. Dostaneme

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

Pripočítaním štvrtého riadku k prvému, druhému, piatemu a šiestemu dostaneme

$$= 30 \cdot \begin{vmatrix} 0 & 2 & 0 & 0 & 10 & 9 \\ 1 & 5 & 2 & 0 & 7 & 7 \\ 4 & 5 & 3 & 0 & 8 & 3 \\ -1 & 4 & 2 & -1 & 5 & 8 \\ 0 & 5 & 2 & 0 & 6 & 9 \\ 0 & 4 & 7 & 0 & 7 & 8 \end{vmatrix} =$$

$$= -30 \begin{vmatrix} 0 & 2 & 0 & 10 & 9 \\ 1 & 5 & 2 & 7 & 7 \\ 4 & 5 & 3 & 8 & 3 \\ 0 & 5 & 2 & 6 & 9 \\ 0 & 4 & 7 & 7 & 8 \end{vmatrix} = -30 \begin{vmatrix} 0 & 2 & 0 & 10 & 9 \\ 1 & 5 & 2 & 7 & 7 \\ 0 & -15 & -5 & -20 & -25 \\ 0 & 5 & 2 & 6 & 9 \\ 0 & 4 & 7 & 7 & 8 \end{vmatrix} =$$

Pripočítali sme $-4-$násobok druhého riadku k tretiemu. Rozvinutím podľa prvého stĺpca dostaneme

$$= 30 \begin{vmatrix} 2 & 0 & 10 & 9 \\ -15 & -5 & -20 & -25 \\ 5 & 2 & 6 & 9 \\ 4 & 7 & 7 & 8 \end{vmatrix} = -150 \begin{vmatrix} 2 & 0 & 10 & 9 \\ 3 & 1 & 4 & 5 \\ 5 & 2 & 6 & 9 \\ 4 & 7 & 7 & 8 \end{vmatrix} =$$

Analogickým spôsobom si pripravíme rozvinutie podľa druhého stĺpca:

$$= -150 \begin{vmatrix} 2 & 0 & 10 & 9 \\ 3 & 1 & 4 & 5 \\ -1 & 0 & -2 & -1 \\ -17 & 0 & -21 & -27 \end{vmatrix} = -150 \cdot \begin{vmatrix} 2 & 10 & 9 \\ -1 & -2 & -1 \\ -17 & -21 & -27 \end{vmatrix} =$$

$$= -150 \begin{vmatrix} 2 & 10 & 9 \\ 1 & 2 & 1 \\ 17 & 21 & 27 \end{vmatrix} = -150 \cdot (-151) = 22650.$$

Pri výpočte determinantu je niekedy vhodné upraviť ho na tvar, v ktorom pod alebo nad hlavnou diagonálou sú samé nuly. Hodnota takého determinantu sa rovná súčinu prvkov hlavnej diagonály (presvedčte sa o tom!).

Príklad 1.7. Vypočítajte determinant

$$\begin{vmatrix} 1, & 2, & 3, & \dots, & n-1, & n \\ 1, & 3, & 3, & \dots, & n-1, & n \\ 1, & 2, & 5, & \dots, & n-1, & n \\ \dots \\ 1, & 2, & 3, & \dots, & 2n-3, & n \\ 1, & 2, & 3, & \dots, & n-1, & 2n-1 \end{vmatrix}.$$

Ako prvý riadok odčítame od ostatných dostaneme

$$\begin{vmatrix} 1, & 2, & 3, & \dots, & n-1, & n \\ 0, & 1, & 0, & \dots, & 0, & 0 \\ 0, & 0, & 2, & \dots, & 0, & 0 \\ \dots \\ 0, & 0, & 0, & \dots, & n-2, & 0 \\ 0, & 0, & 0, & \dots, & 0, & n-1 \end{vmatrix} = 1 \cdot 2 \cdot \ldots \cdot (n-2)(n-1) = (n-1)!$$

Cvičenia

1.1. Určte koľko inverzií je v nasledujúcich poradiach:

a) $(n, n-1, \dots, 2, 1)$,
b) $(1, 2, \dots, m, n, n-1, \dots, m+1)$,
c) $(n, n-1, \dots, m+1, 1, 2, \dots, m)$,
d) $(m, m-1, \dots, 1, n, n-1, \dots, m+1)$,
e) $(1, 3, \dots, 2n-1, 2, 4, \dots, 2n)$,
f) $(1, 3, \dots, 2n-1, 2n, 2n-2, \dots, 4, 2)$,
g) $(2n, 2n-2, \dots, 4, 2, 1, 3, \dots, 2n-1)$,
h) $(2n-1, 2n-3, \dots, 3, 1, 2n, 2n-2, \dots, 4, 2)$,

kde $n, m \in N$, pričom $m < n$.

1.2. Poradie $(n_1, n_2, \dots, n_k)$ má i inverzií. Koľko ich má poradie:

a) $(n_2, n_3, \dots, n_k, n_1)$,
b) $(n_k, n_{k-1}, \dots, n_2, n_1)$,
c) $(n_2, n_1, n_3, \dots, n_k)$,
d) $(n_m, n_{m-1}, \dots, n_{m+1}, \dots, n_k)$,

kde $n_i, m, k \in N$, pričom $m < k$.

1.3. Vypočítajte determinanty:

$$\begin{vmatrix} 2 & -1 \\ 3 & 2 \end{vmatrix}, \quad \begin{vmatrix} 126 & 385 \\ 105 & 620 \end{vmatrix}, \quad \begin{vmatrix} \sin x & \cos x \\ -cos x & \sin x \end{vmatrix} \begin{vmatrix} a+b_i & a\sqrt{3} \\ a\sqrt{3} & a-b_i \end{vmatrix}, \quad \begin{vmatrix} \cos x & \sin x \\ \sin x & \cos x \end{vmatrix},$$

$$\begin{vmatrix} 1 & 2 & 3 \\ -4 & 5 & 8 \\ 12 & 2 & 0 \end{vmatrix}, \quad \begin{vmatrix} a & 0 & b \\ 0 & c & c \\ a & c & b \end{vmatrix}, \quad \begin{vmatrix} 1 & a & b \\ 1 & a+x & b \\ 1 & a & b+y \end{vmatrix}$$

$$\begin{vmatrix} a & -1 & 0 \\ ax & a & -1 \\ ax^2 & ax & a \end{vmatrix}, \quad \begin{vmatrix} 2+3i & 2-2i & 1-i \\ 2+i & 7-3i & 3-i \\ 1+i & 4-6i & 2-3i \end{vmatrix}.$$

1.4. Dokážte, že platí:

$$\begin{vmatrix} 1 & x & x^2 \\ 1 & y & y^2 \\ 1 & z & z^2 \end{vmatrix} = (x-y)(x-z)(y-z), \qquad \begin{vmatrix} 1 & x & x^2 \\ 1 & x & ax \\ 1 & x^2 & ax^2 \end{vmatrix} = x^2(x-1)(x-a).$$

1.5. Nasledujúce výrazy vyjadrite v tvare determinantu tretieho stupňa: $a^3+b^3+c^3-3abc$, $abc+ax^2+by^2+cz^2$, $2x^2y-x^3-xy^2$, $abc+b^2-ab-bc$.

1.6. Vypočítajte

$$\begin{vmatrix} 2 & -5 & 1 & 2 \\ -3 & 7 & -1 & 4 \\ 5 & -9 & 2 & 7 \\ 4 & -6 & 1 & 2 \end{vmatrix}, \quad \begin{vmatrix} 8 & 6 & 5 & 2 \\ 3 & 3 & 2 & 1 \\ 4 & 2 & 3 & 1 \\ 5 & 5 & 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} x & a & b & 0 & c \\ 0 & y & 0 & 0 & d \\ 0 & e & z & 0 & f \\ g & h & k & u & l \\ 0 & 0 & 0 & 0 & v \end{vmatrix},$$

$$\begin{vmatrix} 24 & -14 & -11 & 6 & 0 \\ 0 & 24 & -14 & -11 & 6 \\ 10 & 3 & -4 & 0 & 0 \\ 0 & 10 & 3 & -4 & 0 \\ 0 & 0 & 10 & 3 & -4 \end{vmatrix}, \quad \begin{vmatrix} 2 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 4 & 1 & 1 & 1 \\ 1 & 1 & 1 & 5 & 1 & 1 \\ 1 & 1 & 1 & 1 & 6 & 1 \\ 1 & 1 & 1 & 1 & 1 & 7 \end{vmatrix},$$

1.7. Vypočítajte nasledujúce determinanty (prípadne skúste najprv pre $n = 3, 4$ alebo 5).

$$a) \begin{vmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ a_{31} & a_{32} & a_{33} & \dots & 0 \\ & \vdots & & & \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix}, \qquad b) \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1,n-1} & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2,4-1} & 0 \\ a_{31} & a_{32} & \dots & 0 & 0 \\ & \vdots & & & \\ a_{n1} & 0 & \dots & 0 & 0 \end{vmatrix},$$

$$c) \begin{vmatrix} a_0 & b_1 & 0 & \dots & 0 & 0 \\ a_0 & a_1 & b_2 & \dots & 0 & 0 \\ a_0 & a_1 & a_2 & \dots & 0 & 0 \\ & \vdots & & & & \\ a_0 & a_1 & a_2 & \dots & a_{n-1} & b_n \\ a_0 & a_1 & a_2 & \dots & a_{n-1} & a_n \end{vmatrix}, \qquad d) \begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1,n-1} & a_{1n} \\ a_{21} & 0 & 0 & \dots & 0 & 0 \\ a_{31} & a_{32} & 0 & \dots & 0 & 0 \\ & \vdots & & & & \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{n,n-1} & 0 \end{vmatrix},$$

$$e)\ \begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1,n-1} & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2,n-1} & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3,n-1} & a_{3n} \\ 0 & 0 & 0 & \dots & a_{4,n-1} & a_{4n} \\ \vdots \\ 0 & 0 & 0 & \dots & 0 & a_{nn} \end{vmatrix}, \qquad f)\ \begin{vmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ -1 & 0 & 1 & \dots & 1 & 1 \\ -1 & -1 & 0 & \dots & 1 & 1 \\ & \vdots \\ -1 & -1 & -1 & \dots & 0 & 1 \\ -1 & -1 & -1 & \dots & -1 & 0 \end{vmatrix}.$$

1.8. Vypočítajte determinanty:

$$a)\ \begin{vmatrix} x_1 & x_2 & x_3 & \dots & x_{n-1} & x_n \\ x_2 & x_2 & x_3 & \dots & x_{n-1} & x_n \\ x_3 & x_3 & x_3 & \dots & x_{n-1} & x_n \\ & \vdots \\ x_{n-1} & x_{n-1} & x_{n-1} & \dots & x_{n-1} & x_n \\ x_n & x_n & x_n & \dots & x_n & x_n \end{vmatrix}, \quad b)\ \begin{vmatrix} a_1 & b_2 & b_3 & \dots & b_{n-2} & b_{n-1} & b_n \\ c_1 & a_2 & b_3 & \dots & b_{n-2} & b_{n-1} & b_n \\ c_1 & c_2 & a_3 & \dots & b_{n-2} & b_{n-1} & b_n \\ & \vdots \\ c_1 & c_2 & c_3 & \dots & c_{n-2} & a_{n-1} & b_n \\ c_1 & c_2 & c_3 & \dots & c_{n-2} & c_{n-1} & b_n \end{vmatrix}.$$

1.9. Vypočítajte determinant:

$$D(n) = \begin{vmatrix} x & 1 & 1 & \dots & 1 & 1 \\ 1 & x & 1 & \dots & 1 & 1 \\ 1 & 1 & x & \dots & 1 & 1 \\ & \vdots \\ 1 & 1 & 1 & \dots & x & 1 \\ 1 & 1 & 1 & \dots & 1 & x \end{vmatrix}.$$

Návod. Po odčítaní prvého riadku od ostatných, rozviňte determinant podľa posledného stĺpca. Dostanete tak rekurentný vzorec

$$D(n) = (x-1)^{n-1} + (n-1)D(n-1).$$

Potom matematickou indukciou dokážte, že $D(n) = (x+n-1)(x-1)^{n-1}$.

1.10. Vypočítajte Vandermondov determinant:

$$V(n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}.$$

Návod. Predposledný stĺpec vynásobíme x_1 a odčítame ho od posledného stĺpca, potom stĺpec druhý od konca vynásobíme x_1 a odčítame ho od predposledného. Takto postupujeme ďalej. Dostaneme rekurentný vzťah

$$V(n) = (x_2 - x_1)(x_3 - x_1)\dots(x_n - x_1)V(n-1).$$

Matematickou indukciou ľahko dokážeme, že

$$\begin{aligned} V(n) = (x_2 - x_1)(x_3 - x_1)\dots(x_n - x_1) \\ (x_3 - x_2)\dots(x_n - x_2) \\ \vdots \\ (x_n - x_{n-1}). \end{aligned}$$

1.11. Dokážte, že platí

$$a)\quad \begin{vmatrix} b_1 & a & a & \dots & a & a \\ a & b_2 & a & \dots & a & a \\ a & a & b_3 & \dots & a & a \\ & \vdots & & & & \\ a & a & a & \dots & b_{n-1} & a \\ a & a & a & \dots & a & b_n \end{vmatrix} = \prod_{n=1}^{n}(b_i - a)\left(1 + \sum_{j=1}^{n} \frac{a}{b_j - a}\right)$$

kde $b_j \neq a$ pre $j = 1, 2, \dots, n$.

$$b)\quad \begin{vmatrix} x_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \\ a_1 & x_2 & a_3 & \dots & a_{n-1} & a_n \\ a_1 & a_2 & x_3 & \dots & a_{n-1} & a_n \\ & \vdots & & & & \\ a_1 & a_2 & a_3 & \dots & x_{n-1} & a_n \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & x_n \end{vmatrix} = \prod_{i=1}^{n}(x_i - a_i)\left(1 + \sum_{j=1}^{n} \frac{a_j}{x_j - a_j}\right),$$

kde $x_j \neq a_j$ $j = 1, 2, \dots, n$.

§ 2. Niektoré aplikácie determinantov

V tomto paragrafe si ukážeme niektoré aplikácie determinantov v lineárnej algebre. Čitateľ v priebehu štúdia zistí, že determinanty majú mnohé aplikácie aj v ďalších oblastiach matematiky. Najprv si ukážeme, ako možno využiť pojem determinantu v definícii hodnosti matice. Hovorí o tom veta 2.1. Prv však než ju vyslovíme, musíme definovať pojem subdeterminantu matice.

Definícia 2.1. Nech $\boldsymbol{\varrho}_{i_1}, \boldsymbol{\varrho}_{i_2}, \dots, \boldsymbol{\varrho}_{i_h}$ a $\boldsymbol{\sigma}_{j_1}, \boldsymbol{\sigma}_{j_2}, \dots, \boldsymbol{\sigma}_{j_h}$ je h vybratých riadkov a h vybratých stĺpcov matice $\mathbf{A} = (a_{i_h})$ typu $m \times n$ nad poľom F. (Zrejme je $1 \leqq h \leqq \min(m, n)$.) Potom determinant

$$\begin{vmatrix} a_{i_1 j_1}, & a_{i_1 j_2}, & \dots, & a_{i_1 j_h} \\ \vdots & & & \\ a_{i_h j_1}, & a_{i_h j_2}, & \dots, & a_{i_h j_h} \end{vmatrix}$$

nazývame *subdeterminantom* h-teho stupňa matice $\mathbf{A}$ patriacim h vybratým riadkom a h vybratým stĺpcom.

Poznámka 2.1. Hodnosť matice sa rovná nule práve vtedy, keď je to nulová matica.

Veta 2.1. *Nech $\mathbf{A} = (a_{ik})$ je matica typu $m \times n$ nad poľom F. Matica $\mathbf{A}$ má hodnosť $h \geqq 1$ práve vtedy, keď existuje subdeterminant matice $\mathbf{A}$ $h-$teho stupňa rôzny od nuly, pričom všetky subdeterminanty matice $\mathbf{A}$, ktoré sú stupňa vyššieho ako h (ak také vôbec existujú), sa rovnajú nule.*

Dôkaz. I. Predpokladajme, že v matici $\mathbf{A}$ existuje subdeterminant h-teho stupňa $D \neq 0$, pričom $h \geqq 1$ a všetky subdeterminanty matice $\mathbf{A}$ vyšších stupňov (ak také existujú), sa rovnajú nule. Bez ujmy na všeobecnosti môžeme predpokladať, že determinant D pozostáva z prvých h riadkov a z prvých h stĺpcov (pozri (4.1) kapitoly 3). Prvých h riadkov matice $\mathbf{A}$ je lineárne nezávislých. Naozaj, ak tieto riadky boli lineárne závislé, tak podľa vety 1.4 by platilo $D = 0$. Aby sme dokázali, že $h(\mathbf{A}) = h$ (v zmysle definície 1.4 kapitoly 3), stačí dokázať, že každý napr. j-ty riadok matice $\mathbf{A}$ je lineárnou kombináciou prvých h riadkov matice. Ak $1 \leqq j \leqq h$, je to zrejmé. Aby sme to dokázali aj pre $j > h$, uvažujme o nasledujúcom determinante $(h+1)$-ho stupňa

$$D^* = \begin{vmatrix} a_{11}, & a_{12}, & \dots, & a_{1h}, & a_{1k} \\ a_{21}, & a_{22}, & \dots, & a_{2h}, & a_{2k} \\ \vdots & & & & \\ a_{h1}, & a_{h2}, & \dots, & a_{hh}, & a_{hk} \\ a_{j1}, & a_{j2}, & \dots, & a_{jh}, & a_{jk} \end{vmatrix},$$

kde $h < j \leqq m$, $1 \leqq k \leqq n$, pričom „v ľavom hornom rohu“ determinantu D^* sa nachádza determinant D, o ktorom vieme, že je rôzny od nuly. Ďalej platí $D^* = 0$, lebo ak $k \leqq h$, D^* má dva rovnaké stĺpce; ak $k > h$, D^* je subdeterminantom matice $\mathbf{A}$ $(h+1)$-ho stupňa, teda sa rovná nule podľa predpokladu. Rozvinutím D^* podľa posledného stĺpca dostaneme:

$$a_{1h}A_{1h} + a_{2h}A_{2k} + \cdots + a_{hk}A_{hk} + a_{jk}(-1)^{j+k}D = D^* = 0.$$

Vzhľadom na $D \neq 0$, máme

$$a_{jk} = -\frac{A_{1k}}{(-1)^{j+k}D}a_{1k} - \frac{A_{2k}}{(-1)^{j+k}D}a_{2k} - \cdots - \frac{A_{hk}}{(-1)^{j+k}D}a_{hk}.$$

Keďže k bol ľubovoľný stĺpec, j-tý riadok $(h < j \leqq m)$ je lineárnou kombináciou prvých h riadkov matice.

II. Nech $h(\mathbf{A}) = h$, kde $h \geqq 1$. (Ide teda o nenulovú maticu.) Najprv dokážeme, že každý subdeterminant stupňa vyššieho ako h (ak taký v matici existuje) sa rovná nule, potom existenciu nenulového subdeterminantu stupňa h.

a) Nech matica obsahuje subdeterminanty vyššieho stupňa ako h. Vyberme hociktorý z nich. Riadky matice, z ktorých je tento subdeterminant vybratý sú lineárne závislé, lebo ich je viac ako h. Potom z dôsledku 4 vety 1.3 vyplýva, že tento subdeterminant sa rovná nule.

b) Nech g je najväčšie prirodzené číslo také, že subdeterminant g-teho stupňa vybratý z matice je $\neq 0$. Z toho, že $\mathbf{A}$ nie je nulová matica a z bodu a) plynie $1 \leqq g \leqq h$. Ak by $g < h$ podľa I. by platilo $h(\mathbf{A}) = g < h$, čo nie je. Teda $g = h$. □

Dôsledok. *Ak sa determinant D rovná nule, tak jeho riadky sú lineárne závislé.*

Dôkaz. Nech sa determinant D stupňa s rovná nule. Uvažujme maticu $\mathbf{A}$ typu $s \times s$, ktorá má tie isté riadky (teda aj stĺpce) ako determinant D, čiže $d(\mathbf{A}) = D$. Podľa vety 2.1 je zrejme $h(\mathbf{A}) < s$, čiže riadky matice $\mathbf{A}$ (a tým aj riadky determinantu D) sú lineárne závislé. □

Poznámka 2.2. Dôkazom dôsledku sme dokončili dôkaz vety 1.4.

Ďalšia aplikácia determinantov sa týka výpočtu inverznej matice.

Definícia 2.2. Štvorcová matica $\mathbf{A}$, pre ktorú $d(\mathbf{A}) \neq 0$, sa nazýva *regulárna.* Matica, ktorá nie je regulárna, sa nazýva *singulárna.*

Definícia 2.3. Nech $\mathbf{A}$ je štvorcová matica typu $n \times n$. Matica $\mathbf{A}^{-1}$, pre ktorú platí

$$\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{J}_n$$

sa nazýva *inverzná matica* matice $\mathbf{A}$.

Poznámka 2.3. Je jasné, že aj $\mathbf{A}^{-1}$ je typu $n \times n$. Čitateľ nech si tiež uvedomí, že $\mathbf{A}$ je inverznou maticou matice $\mathbf{A}^{-1}$.

Veta 2.2. *Nech*

$$\mathbf{A} = \begin{pmatrix} a_{11}, & a_{12}, & a_{13}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & a_{23}, & \dots, & a_{2n} \\ a_{31}, & a_{32}, & a_{33}, & \dots, & a_{3n} \\ \vdots & & & & \\ a_{n1}, & a_{n2}, & a_{n3}, & \dots, & a_{nn} \end{pmatrix}$$

je regulárna matica. Potom maticu $\mathbf{A}^{-1}$ *vypočítame takto:*

$$\mathbf{A}^{-1} = \frac{1}{d(\mathbf{A})} \begin{pmatrix} A_{11}, & A_{21}, & A_{31}, & \dots, & A_{n1} \\ A_{12}, & A_{22}, & A_{32}, & \dots, & A_{n2} \\ A_{13}, & A_{23}, & A_{33}, & \dots, & A_{n_3} \\ \vdots & & & & \\ A_{1n}, & A_{2n}, & A_{3n}, & \dots, & A_{nn} \end{pmatrix},$$

kde algebraické doplnky $A_{i1}, A_{i2}, \dots, A_{in}$ *patriace k* i*-temu riadku píšeme do* i*-teho stĺpca.*

Dôkaz. Prvok c_{ik} matice $\mathbf{A} \cdot \mathbf{A}^{-1}$ je tvaru

$$c_{ik} = \frac{1}{d(\mathbf{A})}(a_{i1}A_{k1} + a_{i2}A_{k2} + \dots + a_{in}A_{kn}).$$

Podľa vety 1.3 a jej dôsledku 4 vidíme, že

$$c_{ik} = \begin{cases} 1 & \text{ak } \ i = k, \\ 0 & \text{ak } \ i \neq k. \end{cases}$$

Teda $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{J}_n$. Analogicky sa presvedčíme, že aj $\mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{J}_n$. $\square$

Príklad 2.1. Nad poľom Q je daná matica

$$\mathbf{A} = \begin{pmatrix} 6 & 3 & 5 \\ 4 & 6 & 4 \\ 7 & 4 & 6 \end{pmatrix}.$$

Vypočítajme maticu $\mathbf{A}^{-1}$. Ľahko sa presvedčíme, že $d(\mathbf{A}) = 2$. Ďalej vypočítame

$$\begin{array}{lll} A_{11} = 20, & A_{12} = 4, & A_{13} = -26, \\ A_{21} = 2, & A_{22} = 1, & A_{23} = -\ 3, \\ A_{31} = -18, & A_{32} = -4, & A_{33} = 24. \end{array}$$

Máme tak

$$\mathbf{A}^{-1} = \frac{1}{2} \begin{pmatrix} 20 & 2 & -18 \\ 4 & 1 & -4 \\ -26 & -3 & 24 \end{pmatrix} = \begin{pmatrix} 10 & 1 & -9 \\ 2 & \frac{1}{2} & -2 \\ -13 & -\frac{3}{2} & 12 \end{pmatrix}.$$

Čitateľ si skontroluje, že $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{J}_3$.

Príklad 2.2. Nech $\mathbf{A}$ je matica typu 2×2 nad poľom F. Dokážeme, že matica $\mathbf{A}^{-1}$ existuje práve vtedy, keď $\mathbf{A}$ je regulárna.

Skutočne: I. Ak $\mathbf{A}$ je regulárna matica, tak $\mathbf{A}^{-1}$ vypočítame podľa vety 2.2.

II. Nech $\mathbf{A}$ je singulárna matica. Pre určitosť nech

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{pričom } \ ad - bc = 0.$$

Ak by existovala matica $\mathbf{A}^{-1} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$, platilo by $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{J}_3$ a teda

$$d(\mathbf{A} \cdot \mathbf{A}^{-1}) = 1. \tag{2.1}$$

Počítajme

$$\mathbf{A} \cdot \mathbf{A}^{-1} = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix}$$

a tak $d(\mathbf{A} \cdot \mathbf{A}^{-1}) = (ax + bz)(cy + dw) - (ay + bw)(cx + dz) = \dots$ $\dots = (xw - yz)(ad - bc) = (xw - yz) \cdot 0 = 0$, čo je spor s rovnosťou (2.1).

Príklad 2.3. Nájdeme všetky matice $\mathbf{A}$ typu 2×2 nad Q také, že $\mathbf{A} = \mathbf{A}^{-1}$.

Riešenie. Z príkladu 2.2 vieme, že $\mathbf{A}$ musí byť regulárna matica. Nech pre určitosť

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ \text{pričom } \ ad - bc \neq 0.$$

Potom

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

Z rovnosti $\mathbf{A} = \mathbf{A}^{-1}$ vyplýva

$$a = \frac{d}{ad - bc}, \quad b = \frac{-b}{ad - bc}, \quad c = \frac{-c}{ad - bc}, \quad d = \frac{a}{ad - bc}.$$

Budeme rozoznávať dva prípady:

1) Nech je, po prvé, $b \cdot c \neq 0$. Potom z druhej a tretej rovnosti máme

$$\text{(a)} \qquad ad - bc = -1$$

Ak je $ad = 0$, z prvej rovnosti máme $a = d = 0$. Ak je $ad \neq 0$, z prvej rovnosti a zo vzťahu (a) máme $a = -d$. Keďže $0 = -0$, v každom prípade je $a = -d$. Dosadením do (a) dostaneme

$$\text{(b)} \qquad bc + a^2 = 1.$$

Keď si teraz zvolíme a, c ľubovoľne (pričom zrejme $c \neq 0$), z (b) dostaneme $b = (1 - a^2)/c$. Keďže $d = -a$, matica $\mathbf{A}$ má tvar

$$\mathbf{A} = \begin{pmatrix} a & \frac{1-a^2}{c} \\ c & -a \end{pmatrix}.$$

2) Po druhé predpokladajme $b \cdot c = 0$, t.j. $b = 0$ alebo $c = 0$. Potom musí byť $a \neq 0$, $d \neq 0$. Z prvej a štvrtej rovnosti vyjde $a^2 = 1$, $d^2 = 1$, t.j. $a = \pm 1$, $d = \pm 1$. Teraz máme tri podprípady:

2a) Ak je $b \neq 0$, $c = 0$, z druhej rovnosti vychádza $ad = -1$, t.j. matica $\mathbf{A}$ je tvaru

$$\begin{pmatrix} \pm 1 & b \\ 0 & \mp 1 \end{pmatrix},$$

kde $b \neq 0$ je ľubovoľné racionálne číslo.

2b) Ak je $c \neq 0$, $b = 0$, z tretej rovnosti vychádza $ad = -1$, t.j. matica $\mathbf{A}$ má tvar

$$\begin{pmatrix} \pm 1 & 0 \\ c & \mp 1 \end{pmatrix},$$

kde $c \neq 0$ je ľubovoľné racionálne číslo.

2c) Ak je $c = b = 0$, tak $\mathbf{A}$ má tvar

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \quad \text{alebo} \quad \begin{pmatrix} \pm 1 & 0 \\ 0 & \mp 1 \end{pmatrix}.$$

Keďže viac možností neexistuje, našli sme všetky požadované matice.

V príklade 2.2 sme dokázali, že matica typu 2×2 má inverznú maticu vtedy, keď je regulárna. Platí toto tvrdenie všeobecne, t.j. pre maticu typu $n \times n$, kde $n \geqq 2$ je ľubovoľné prirodzené číslo? Povedzme hneď, že odpoveď je áno. Toto tvrdenie je dôsledkom nasledujúcej vety.

Veta 2.3. *Nech* $\mathbf{A}, \mathbf{B}$ *sú dve matice typu* $n \times n$ *nad poľom* F. *Nech* $\mathbf{C} = \mathbf{A} \cdot \mathbf{B}$. *Potom*

$$d(\mathbf{C}) = d(\mathbf{A}) \cdot d(\mathbf{B}).$$

Dôkaz možno vykonať priamo, využitím definície násobenia matíc, definície determinantu a niektorých vlastností determinantov. My vykonáme dôkaz uvedený v [10, str. 112].

Nech $\mathbf{A} = (a_{ij}), \mathbf{B} = (b_{ij}),\ i, j = 1, 2, \dots, n$. Dôkaz je založený na tom, že pre istý determinant D platí $D = d(\mathbf{A} \cdot \mathbf{B}) = d(\mathbf{C})$ i $D = d(\mathbf{A}) \cdot d(\mathbf{B})$.

Determinant D definujeme nasledujúcim spôsobom:

$$(2.2) \qquad D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & 0 & \dots & 0 \\ \vdots & & & & & & & \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 & 0 & \dots & 0 \\ -1 & 0 & \dots & 0 & b_{11} & b_{12} & \dots & b_{1n} \\ 0 & -1 & \dots & 0 & b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & & & & & & & \\ 0 & 0 & \dots & -1 & b_{n1} & b_{n2} & \dots & b_{nn} \end{vmatrix}$$

Vidíme, že v „ľavom hornom rohu“ determinantu D je matica $\mathbf{A}$, zatiaľ čo $\mathbf{B}$ je v „pravom dolnom rohu“. Schematicky to môžeme zapísať takto:

$$D = \begin{vmatrix} \mathbf{A} & \mathbf{0}_n \\ -\mathbf{J}_n & \mathbf{B} \end{vmatrix}.$$

Teraz pripočítame vhodné násobky prvých n stĺpcov determinantu D k posledným n stĺpcom tak, aby sme na mieste matice $\mathbf{B}$ dostali nulovú maticu $\mathbf{0}_n$. Konkrétne: K $(n+k)$-temu stĺpcu $(k = 1, 2, \dots, n)$ pripočítame b_{1k}-násobok 1. stĺpca, b_{2k}-násobok 2. stĺpca, $\dots, b_{nk}$-násobok n-tého stĺpca. Tým sa $(n+k)$-ty stĺpec v posledných n riadkoch „vynuloval“. Aké prvky bude mať $(n+k)$-ty stĺpec na prvých n riadkoch? Ľahko sa možno presvedčiť, že na i-tom mieste bude prvok

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk} = \sum_{j=1}^{n} a_{ij}b_{jk},$$

kde $i = 1, 2, \dots, n$. Čitateľ nech si uvedomí, že determinant sme upravili tak, že v pravom hornom rohu je matica $\mathbf{C} = \mathbf{A} \cdot \mathbf{B}$.
Teda (schématicky napísané):

$$D = \begin{vmatrix} \mathbf{A} & \mathbf{C} \\ -\mathbf{J}_n & \mathbf{0}_n \end{vmatrix}$$

V determinante D teraz vymeníme 1. riadok a $(n+1)$-ný riadok, 2. riadok a $(n+2)$-hý riadok, $\dots, n$-tý riadok a $2n$-tý riadok. Dostaneme tak (vykonali sme n výmen riadkov):

$$D = (-1)^n \begin{vmatrix} -1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & -1 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \dots & -1 & 0 & 0 & \dots & 0 \\ a_{11} & a_{12} & \dots & a_{1n} & c_{11} & c_{12} & \dots & c_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} & c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & & & & & & & \\ a_{n1} & a_{n2} & \dots & a_{nn} & c_{n1} & c_{n2} & \dots & c_{nn} \end{vmatrix}$$

Ak tento determinant rozvinieme podľa prvého, druhého až n-tého riadku, dostaneme

$$D = (-1)^n \cdot (-1)^n \cdot d(\mathbf{C}) = d(\mathbf{A} \cdot \mathbf{B}).$$

Aby sme vykonali druhú časť dôkazu, determinant (2.2) upravíme pomocou ero a eso tak, že nad hlavnou diagonálou budú v prvých n riadkoch samé nuly. To sa vždy dá urobiť tak, že operácie vykonávame len s prvými n riadkami a s prvými n stĺpcami. Ak sme pri tom vybrali nejaký činiteľ pred determinant, vynásobíme nakoniec týmto činiteľom hoci prvý riadok determinantu. Čitateľ nech si preverí, že pri tomto postupe „v pravom dolnom rohu“ zostala matica $\mathbf{B}$ a determinant matice „v ľavom hornom rohu“ sa rovná $d(\mathbf{A})$. Dostaneme determinant

$$D = \begin{vmatrix} d_{11} & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ d_{21} & d_{22} & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & & \\ d_{n1} & d_{n2} & \dots & d_{nn} & 0 & 0 & \dots & 0 \\ e_{11} & e_{12} & \dots & e_{1n} & b_{11} & b_{12} & \dots & b_{1n} \\ e_{21} & e_{22} & \dots & e_{2n} & b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & & & & & & & \\ e_{n1} & e_{n2} & \dots & e_{nn} & b_{n1} & b_{n2} & \dots & b_{nn} \end{vmatrix}$$

Ak tento determinant rozvinieme podľa prvého, druhého až n-tého riadku dostaneme

$$D = d_{11} \cdot d_{22} \dots d_{nn} \cdot d(\mathbf{B}) = d(\mathbf{A}) \cdot d(\mathbf{B}).$$

Tým je dôkaz ukončený. □

Dôsledok 1. *Súčin dvoch regulárnych matíc (typu $n \times n$) je regulárna matica. Súčin singulárnej a ľubovoľnej matice je singulárna matica*

Dôkaz. Stačí zobrať do úvahy vetu 2.3 a uvedomiť si, že $d(\mathbf{A})$, $d(\mathbf{B})$, $d(\mathbf{A} \cdot \mathbf{B})$ sú prvky poľa F (pole nemá netriviálne delitele nuly). □

Dôsledok 2. *K matici $\mathbf{A}$ typu $n \times n$ nad poľom F existuje inverzná matica $\mathbf{A}^{-1}$ práve vtedy, keď $\mathbf{A}$ je regulárna matica.*

Dôkaz. Ak je regulárna, inverznú maticu vypočítame podľa vety 2.2. Nech $\mathbf{A}$ je singulárna matica. Predpokladajme, že k nej existuje inverzná matica $\mathbf{A}^{-1}$, t.j. $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{J}_n$. Potom $d(\mathbf{A} \cdot \mathbf{A}^{-1}) = 1$, to však nemôže byť, lebo podľa dôsledku 1 je $d(\mathbf{A} \cdot \mathbf{A}^{-1}) = 0$. Predpoklad existencie matice $\mathbf{A}^{-1}$ vedie teda k sporu. □

Veta 2.4. *Nech $\boldsymbol{M}_n$ je množina všetkých regulárnych matíc typu $n \times n$ nad poľom F. Potom štruktúra $(\boldsymbol{M}_n, \cdot)$ je grupa.*

Dôkaz. Podľa dôsledku 1 vety 2.3 je $(\boldsymbol{M}_n, \cdot)$ grupoid. Keďže násobenie matíc je asociatívne (lema 1.1 kapitoly 3), je $(\boldsymbol{M}_n, \cdot)$ pologrupa, dokonca monoid (jednotkový prvok je $\mathbf{J}_n$). Podľa dôsledku 2 vety 2.3 je tento monoid grupou. □

Poznámka 2.4. Výpočet inverznej matice podľa vety 2.3 je zdĺhavý, treba počítať n^2 algebraických doplnkov, čo je už pri $n = 4$ dosť dlhé počítanie. Oveľa efektívnejší je spôsob pomocou súčasnej úpravy danej matice a matice $\mathbf{J}_n$ elementárnymi riadkovými úpravami, ktorý uvedieme v piatej kapitole (pozri príklad 3.9).

Teraz použijeme determinanty pri riešení sústavy lineárnych rovníc.

Veta 2.5. *Nech je daná sústava n lineárnych rovníc s n neznámymi*

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1i}x_i + \cdots + a_{1n}x_n &= b_1, \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2i}x_i + \cdots + a_{2n}x_n &= b_2, \\
&\ \vdots \\
a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{ni}x_i + \cdots + a_{nn}x_n &= b_n
\end{aligned}
\tag{2.3}
$$

nad poľom F, v ktorom $h(\mathbf{M}) = h(\mathbf{M}') = n$. Potom riešením sústavy je n-tica

$$
\left(\frac{D_{x_1}}{D}, \frac{D_{x_2}}{D}, \ldots, \frac{D_{x_n}}{D} \right),
\tag{2.4}
$$

kde $D = d(\mathbf{M})$ a D_{x_i} je determinant, ktorý dostaneme z determinantu D tak, že v ňom zameníme i-tý stĺpec stĺpcom

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

Poznámka 2.5. Vzorce pre jednotlivé neznáme v n-tici (2.4) sa nazývajú *Cramerove vzorce.* Determinant matice sústavy D skrátene nazývame *determinant sústavy.*

Dôkaz vety 2.5. Aby sme vypočítali i-tú neznámu ($i = 1, 2, \ldots, n$) budeme postupovať nasledovne. Rovnice v sústave (2.3) násobíme postupne algebraickými doplnkami $A_{1i}, A_{2i}, \ldots A_{ni}$ prvkov i-tého stĺpca matice $\mathbf{M}$ a sčítame:

$$
\begin{aligned}
&(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1i}x_i + \cdots + a_{1n}x_n)A_{1i} + \\
&+(a_{21}x_1 + a_{22}x_2 + \cdots + a_{2i}x_i + \cdots + a_{2n}x_n)A_{2i} + \\
&\qquad \vdots \\
&+(a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{ni}x_i + \cdots + a_{nn}x_n)A_{ni} = \\
&= b_1A_{1i} + b_2A_{2i} + \cdots + b_nA_{ni}
\end{aligned}
$$

Po úprave

$$\begin{aligned} &x_1(a_{11}A_{1i} + a_{21}A_{2i} + \cdots + a_{n1}A_{ni}) + \\ &+x_2(a_{12}A_{1i} + a_{22}A_{2i} + \cdots + a_{n2}A_{ni}) + \\ &\qquad\vdots \\ &+x_i(a_{1i}A_{1i} + a_{2i}A_{2i} + \cdots + a_{ni}A_{ni}) + \\ &\qquad\vdots \\ &+x_n(a_{1n}A_{1i} + a_{2n}A_{2i} + \cdots + a_{nn}A_{ni}) = \\ &= \; b_1A_{1i} + b_2A_{2i} + \cdots + b_nA_{ni} \end{aligned}$$

Súčty v zátvorkách na ľavej strane rovnosti pri neznámych x_k, kde $k \neq i$ sú podľa dôsledku 4 vety 1.3 rovné nule, zatiaľ čo súčet pri neznámej x_i je rozvoj determinantu D podľa i-teho stĺpca. Na pravej strane rovnosti je determinant D_{x_i}. Máme tak $x_i \cdot D = D_{xi}$. Podľa podmienok vety je $h(\mathbf{M}) = n$, čiže podľa vety 2.1 $D \neq 0$. Preto $x_i = D_{xi}/D$. Tým je dôkaz vety skončený. □

Veta nám hovorí, že neznáme je možné vyjadriť pomocou koeficientov sústavy rovníc použitím základných operácií v poli (sčítania a násobenia) a operácií k nim inverzných (odčítania a delenia). Cramerove vzorce sa na praktický výpočet veľmi nehodia. Pri trochu väčšom n je nepohodlné počítať $n+1$ determinantov stupňa n. Ak ich použijeme, je vhodné najprv vypočítať determinant $D = d(\mathbf{M})$. Ak $D = 0$, Cramerove vzorce priamo použiť nemožno.

Príklad 2.4. Pomocou Cramerových vzorcov vyriešime nasledujúcu sústavu rovníc nad poľom Q.

$$\begin{aligned} x_1 - 3x_2 + x_3 - 4x_4 &= 3, \\ 2x_1 + x_2 - 4x_3 + x_4 &= -3, \\ 5x_1 - x_2 + 2x_3 - 3x_4 &= 4, \\ 3x_1 + 2x_2 + x_3 + 2x_4 &= 2. \end{aligned}$$

Vypočítame determinant sústavy

$$D = \begin{vmatrix} 1 & -3 & 1 & -4 \\ 2 & 1 & -4 & 1 \\ 5 & -1 & 2 & -3 \\ 3 & 2 & 1 & 2 \end{vmatrix} = 43.$$

Vidíme, že $D \neq 0$. To znamená $h(\mathbf{M}) = h(\mathbf{M}') = 4$, sústava má jediné riešenie a možno použiť Cramerove vzorce.
Vypočítame

$$D_{x_1} = \begin{vmatrix} 3 & -3 & 1 & -4 \\ -3 & 1 & -4 & 1 \\ 4 & -1 & 2 & -3 \\ 2 & 2 & 1 & 2 \end{vmatrix} = 43, \quad D_{x_2} = \begin{vmatrix} 1 & 3 & 1 & -4 \\ 2 & -3 & -4 & 1 \\ 5 & 4 & 2 & -3 \\ 3 & 2 & 1 & 2 \end{vmatrix} = -129,$$

$$D_{x_3} = \begin{vmatrix} 1 & -3 & 3 & 4 \\ 2 & 1 & -3 & 1 \\ 5 & -1 & 4 & -3 \\ 3 & 2 & 2 & 2 \end{vmatrix} = 43, \quad D_{x_4} = \begin{vmatrix} 1 & -3 & 1 & 3 \\ 2 & 1 & -4 & -3 \\ 5 & -1 & 2 & 4 \\ 3 & 2 & 1 & 2 \end{vmatrix} = 86.$$

Teda

$$x_1 = \frac{D_{x_1}}{D} = 1,\ x_2 = \frac{D_{x_2}}{D} = -3,\ x_3 = \frac{D_{x_3}}{D} = 1,\ x_4 = \frac{D_{x_4}}{D} = 2.$$

Riešením je štvorica $(1, -3, 1, 2)$.

Cramerove vzorce môžeme použiť i v prípade $h(\mathbf{M}) = h(\mathbf{M}') < n$. Sústavu nahradíme ekvivalentnou sústavou, v ktorej máme h lineárne nezávislých rovníc. Ukážeme si to na nasledujúcom príklade, v ktorom znova vypočítame sústavu z príkladu 4.1 kapitoly 3.

Príklad 2.5. V príklade 4.1 kapitoly 3 bola nad poľom Q daná sústava ekvivalentná so sústavou

$$\begin{aligned} 2x_1 + 3x_2 - x_3 + 2x_4 &= 13, \\ x_1 - 2x_2 + 4x_3 + x_4 &= -\ 6, \end{aligned}$$

ktorá obsahuje dve lineárne nezávislé rovnice, t.j. $h(\mathbf{M}) = h(\mathbf{M}') = 2$. Keďže prvé dva stĺpce matice sústavy sú lineárne nezávislé, položíme $x_3 = p_1$, $x_4 = p_2$, $p_1, p_2 \in Q$. Dostaneme

$$\begin{aligned} 2x_1 + 3x_2 &= 13 + p_1 - 2p_2, \\ x_1 - 2x_2 &= -6 - 4p_1 - p_2. \end{aligned}$$

Pri pevnej voľbe parametrov p_1, p_2, sústavu možno považovať za sústavu 2 rovníc s dvoma neznámymi s determinantom sústavy

$$D = \begin{vmatrix} 2 & 3 \\ 1 & -2 \end{vmatrix} = -7.$$

Vypočítame

$$D_{x_1} = \begin{vmatrix} 13 + p_1 - 2p_2, & 3 \\ -6 - 4p_1 - p_2, & -2 \end{vmatrix} = -26-2p_1+4p_2+18+12p_1+3p_2 = -8+10p_1+7p_2,$$

$$D_{x_2} = \begin{vmatrix} 2, & 13 + p_1 - 2p_2 \\ 1, & -6 - 4p_1 - p_2 \end{vmatrix} = -12 - 8p_1 - 2p_2 - 13 - p_1 + 2p_2 = -25 - 9p_1.$$

Máme tak

$$x_1 = \frac{-8 + 10p_1 + 7p_2}{-7}, \quad x_2 = \frac{-25 - 9p_1}{-7}.$$

(Porovnajte s výsledkom v príklade 4.1 kapitoly 3.)

Príklad 2.6. Keď použijeme Cramerove vzorce pre prípad sústavy rovníc nad konečným poľom, nemusíme používať zlomky (pozri poznámku 4.4 v kapitole 1). Vypočítajme znova sústavu

$$\begin{aligned}\bar{2}x + \bar{3}y &= \bar{1},\\ \bar{4}x + \bar{1}y &= \bar{3},\end{aligned}$$

nad poľom Z_7, ktorú sme uviedli v poznámke 2.2 kapitoly 3 a vypočítali v príklade 2.1 tej istej kapitoly. Determinant sústavy je $D = \begin{vmatrix} \bar{2} & \bar{3} \\ \bar{4} & \bar{1} \end{vmatrix} = \bar{2} \cdot \bar{1} + (-\bar{3} \cdot \bar{4}) = = \bar{2} + (-\bar{5}) = \bar{2} + \bar{2} = \bar{4}$. Podobne vypočítame $D_x = \begin{vmatrix} \bar{1} & \bar{3} \\ \bar{3} & \bar{1} \end{vmatrix} = \bar{6}$, $D_y = \begin{vmatrix} \bar{2} & \bar{1} \\ \bar{4} & \bar{3} \end{vmatrix} = \bar{2}$. Uplatnením Cramerových vzorcov dostaneme $x = D_x \cdot D^{-1} = \bar{6} \cdot \bar{4}^{-1} = \bar{6} \cdot \bar{2} = \bar{5}$, $y = D_y \cdot D^{-1} = \bar{2} \cdot \bar{4}^{-1} = \bar{2} \cdot \bar{2} = \bar{4}$, čo je v zhode s výsledkom z príkladu 2.1 kapitoly 3.

Ukážeme si ešte dve aplikácie inverznej matice. Najprv riešenie sústavy lineárnych rovníc pomocou inverznej matice, potom jej použitie pri transformácii súradníc vektora.

Sústavu (2.3) môžeme písať v tvare

$$\begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \vdots & & & \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

alebo

$$\mathbf{M} \cdot \vec{\boldsymbol{x}} = \vec{\boldsymbol{b}}. \tag{2.5}$$

Platí veta:

Veta 2.6. *Nech v sústave (2.1) resp. (2.3) platí* $h(\mathbf{M}) = h(\mathbf{M}') = n$. *Potom*

$$\vec{\boldsymbol{x}} = \mathbf{M}^{-1} \cdot \vec{\boldsymbol{b}} \tag{2.6}$$

je jediné riešenie danej sústavy.

Dôkaz. Podľa dôsledku 2 vety 4.1 (Frobeniova veta) sústava (2.5) má jediné riešenie. Keďže $\mathbf{M}$ je regulárna matica, existuje matica $\mathbf{M}^{-1}$. Ak (2.5) násobíme zľava maticou $\mathbf{M}^{-1}$, dostaneme (2.6). □

Príklad 2.7. Vyriešime sústavu rovníc (nad poľom Q)

$$\begin{aligned}6x_1 + 3x_2 + 5x_3 &= 1,\\ 4x_1 + 6x_2 + 4x_3 &= -3,\\ 7x_1 + 4x_2 + 6x_3 &= 2.\end{aligned}$$

Sústavu prepíšeme do tvaru

$$\begin{pmatrix} 6 & 3 & 5 \\ 4 & 6 & 4 \\ 7 & 4 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ -3 \\ 2. \end{pmatrix}. \tag{2.7}$$

V príklade 2.1 sme zistili, že matica tejto sústavy $\mathbf{M}$ je regulárna a vypočítali sme jej inverznú maticu $\mathbf{M}^{-1}$. Ak ňou vynásobíme (2.7) zľava, dostaneme

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 10 & 1 & -9 \\ 2 & \frac{1}{2} & -2 \\ -13 & -\frac{3}{2} & 12 \end{pmatrix} \begin{pmatrix} 1 \\ -3 \\ 2 \end{pmatrix} = \begin{pmatrix} -11 \\ -\frac{7}{2} \\ \frac{31}{2} \end{pmatrix}.$$

Vidíme, že trojica $(-11, -\frac{7}{2}, \frac{31}{2})$ je jediné riešenie danej sústavy.

Matica resp. inverzná matica budú základnými prostriedkami aj pri nájdení vzorcov pre transformáciu súradníc vektora pri zmene bázy. Vo vete 4.1 kapitoly 2 sme dokázali, že ak $B = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ je báza priestoru $\boldsymbol{V}(F)$, tak každý vektor $\boldsymbol{\alpha} \in \boldsymbol{V}(F)$ môžeme jednoznačne vyjadriť v tvare $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n$. Vektor $(x_1, x_2, \dots, x_n) \in \boldsymbol{V}_n(F)$ nazývame vektor súradníc vektora $\boldsymbol{\alpha}$ vzhľadom na bázu B. Vyjadrenie vektora $\boldsymbol{\alpha}$ zapíšeme „maticovo“ takto:

$$\boldsymbol{\alpha} = (x_1, x_2, \dots, x_n) \begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_n \end{pmatrix}. \tag{2.8}$$

Nech teraz $B_1 = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ a $B_2 = \{\boldsymbol{\varepsilon}'_1, \boldsymbol{\varepsilon}'_2, \dots, \boldsymbol{\varepsilon}'_n\}$ sú dve bázy priestoru $\boldsymbol{V}(F)$. Nech vektory $\boldsymbol{\varepsilon}'_i$ sú vyjadrené pomocou vektorov prvej bázy rovnicami

$$\begin{aligned} \boldsymbol{\varepsilon}'_1 &= a_{11}\boldsymbol{\varepsilon}_1 + a_{12}\boldsymbol{\varepsilon}_2 + \dots + a_{1n}\boldsymbol{\varepsilon}_n, \\ \boldsymbol{\varepsilon}'_2 &= a_{21}\boldsymbol{\varepsilon}_1 + a_{22}\boldsymbol{\varepsilon}_2 + \dots + a_{2n}\boldsymbol{\varepsilon}_n, \\ &\vdots \\ \boldsymbol{\varepsilon}'_n &= a_{n1}\boldsymbol{\varepsilon}_1 + a_{n2}\boldsymbol{\varepsilon}_2 + \dots + a_{nn}\boldsymbol{\varepsilon}_n. \end{aligned} \tag{2.9}$$

Definícia 2.4. Matica $\mathbf{A} = (a_{ik})$ $i, k = 1, 2, \dots, n$ sa nazýva *matica prechodu* od bázy B_1 (starej) k báze B_2 (novej).

Rovnosti (2.9) zapíšeme „maticovo“ takto:

$$\begin{pmatrix} \boldsymbol{\varepsilon}'_1 \\ \boldsymbol{\varepsilon}'_2 \\ \vdots \\ \boldsymbol{\varepsilon}'_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_n \end{pmatrix},$$

alebo kratšie:

$$\begin{pmatrix} \boldsymbol{\varepsilon}'_1 \\ \boldsymbol{\varepsilon}'_2 \\ \vdots \\ \boldsymbol{\varepsilon}'_n \end{pmatrix} = \mathbf{A} \cdot \begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_n \end{pmatrix}. \tag{2.10}$$

Veta 2.7. *Nech* $B_1 = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ a $B_2 = \{\boldsymbol{\varepsilon}'_1, \boldsymbol{\varepsilon}'_2, \dots, \boldsymbol{\varepsilon}'_n\}$ *sú dve bázy priestoru* $\boldsymbol{V}$ *a nech* $\mathbf{A}$ *je matica prechodu od bázy* B_1 *k báze* B_2. *Nech* $\boldsymbol{\alpha}$ *je ľubovoľný vektor priestoru* $\boldsymbol{V}$, *nech* $(x_1, x_2, \dots, x_n)$ *je vektor súradníc vektora* $\boldsymbol{\alpha}$ *vzhľadom na bázu* B_1 a $(x'_1, x'_2, \dots, x'_n)$ *je vektor súradníc vektora* $\boldsymbol{\alpha}$ *vzhľadom na bázu* B_2. *Potom matica* $\mathbf{A}$ *je regulárna a platí*

$$(x_1, x_2, \dots, x_n) = (x'_1, x'_2, \dots, x'_n) \cdot \mathbf{A}, \tag{2.11}$$

$$(x'_1, x'_2, \dots, x'_n) = (x_1, x_2, \dots, x_n) \cdot \mathbf{A}^{-1}. \tag{2.12}$$

Dôkaz. Keby matica $\mathbf{A}$ bola singulárna, bol by jeden jej riadok lineárnou kombináciou ostatných riadkov. To by ale vzhľadom na (2.9) znamenalo, že jeden z vektorov $\boldsymbol{\varepsilon}'_1, \boldsymbol{\varepsilon}'_2, \dots, \boldsymbol{\varepsilon}'_n$ by bol lineárnou kombináciou ostatných, čo nie je možné, lebo B_2 je báza.

Podľa (2.8) píšeme

$$\boldsymbol{\alpha} = (x_1, x_2, \dots, x_n) \begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_n \end{pmatrix} = (x'_1, x'_2, \dots, x'_n) \begin{pmatrix} \boldsymbol{\varepsilon}'_1 \\ \boldsymbol{\varepsilon}'_2 \\ \vdots \\ \boldsymbol{\varepsilon}'_n \end{pmatrix}.$$

Dosadením z (2.10) máme

$$(x_1, x_2, \dots, x_n) \cdot \begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_n \end{pmatrix} = (x'_1, x'_2, \dots, x'_n) \cdot \mathbf{A} \begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_n \end{pmatrix},$$

odkiaľ vzhľadom na to, že súradnice vektora $\boldsymbol{\alpha}$ sú dané jednoznačne, vyplýva (2.11). Ak (2.11) násobíme sprava maticou $\mathbf{A}^{-1}$ dostaneme (2.12). □

Príklad 2.8 Nech $B_1 = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_3\}$ a $B_2 = \{\boldsymbol{\varepsilon}'_1, \boldsymbol{\varepsilon}'_2, \boldsymbol{\varepsilon}'_3\}$ sú dve bázy priestoru $\boldsymbol{V}_3(R)$, kde

$$\boldsymbol{\varepsilon}_1 = (1,1,1), \qquad \boldsymbol{\varepsilon}_2 = (0,1,1), \qquad \boldsymbol{\varepsilon}_3 = (0,0,1),$$

$$\boldsymbol{\varepsilon}'_1 = (3,2,1), \qquad \boldsymbol{\varepsilon}'_2 = (-1,0,4), \qquad \boldsymbol{\varepsilon}'_3 = (2,2,4).$$

Čitateľ nech si skontroluje, že

$$\begin{aligned} \boldsymbol{\varepsilon}'_1 &= 3\boldsymbol{\varepsilon}_1 + (-1)\boldsymbol{\varepsilon}_2 + (-1)\boldsymbol{\varepsilon}_3, \\ \boldsymbol{\varepsilon}'_2 &= (-1)\boldsymbol{\varepsilon}_1 + 1\boldsymbol{\varepsilon}_2 + 4\boldsymbol{\varepsilon}_3, \\ \boldsymbol{\varepsilon}'_3 &= 2\boldsymbol{\varepsilon}_1 + 0\boldsymbol{\varepsilon}_2 + 2\boldsymbol{\varepsilon}_3. \end{aligned}$$

Máme tak

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

Vypočítame $\mathbf{A}^{-1}$. Keďže $d(\mathbf{A}) = -2$, je

$$\mathbf{A}^{-1} = -\frac{1}{2}\begin{pmatrix} 2 & 2 & -3 \\ 10 & 8 & -11 \\ -2 & -2 & 2 \end{pmatrix} = \begin{pmatrix} -1 & -1 & \frac{3}{2} \\ -5 & -4 & \frac{11}{2} \\ 1 & 1 & -1 \end{pmatrix}.$$

Nech vektor $\boldsymbol{\alpha} \in \boldsymbol{V}_3(R)$ má v báze B_1 súradnice $x_1 = 2$, $x_2 = -1$, $x_3 = 5$. Súradnice x'_1, x'_2, x'_3 vektora $\boldsymbol{\alpha}$ v báze B_2 budú (podľa 2.12):

$$(x'_1, x'_2, x'_3) = (2, -1, 5)\begin{pmatrix} -1 & -1 & \frac{3}{2} \\ -5 & -4 & \frac{11}{2} \\ 1 & 1 & -1 \end{pmatrix} = (8, 7, -\frac{15}{2}).$$

Presvedčme sa, že súradnice x_i resp. x'_i určujú ten istý vektor:

$$\boldsymbol{\alpha} = 2\boldsymbol{\varepsilon}_1 - 1\boldsymbol{\varepsilon}_2 + 5\boldsymbol{\varepsilon}_3 = (2,2,2) + (0,-1,-1) + (0,0,5) = (2,1,6)$$

a analogicky

$$\boldsymbol{\alpha} = 8 \cdot \boldsymbol{\varepsilon}'_1 + 7\boldsymbol{\varepsilon}'_2 + (-\frac{15}{2}) \cdot \boldsymbol{\varepsilon}'_3 = (24, 16, 8) + (-7, 0, 28) + (-15, -15, -30) = (2, 1, 6).$$

Cvičenia

2.1. Nech $\mathbf{A}, \mathbf{B}$ sú regulárne štvorcové matice typu $n \times n$. Dokážte

a) $(\mathbf{A} \cdot \mathbf{B})^{-1} = \mathbf{B}^{-1} \cdot \mathbf{A}^{-1}$ b) $((\mathbf{A})^{-1})^{-1} = \mathbf{A}$.

2.2. Vypočítajte inverzné matice nasledujúcim maticiam (nad poľom komplexných čísel)

$$\begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix}, \quad \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 2 \\ 3 & 1 & 0 \\ 0 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 3i & 1 & 2-i \\ 0 & 3 & 5 \\ 2i & i & 3+i \end{pmatrix}.$$

2.3. Vypočítajte neznámu maticu $\mathbf{X}$:

a) $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \mathbf{X} = \begin{pmatrix} 3 & 5 \\ 5 & 9 \end{pmatrix}$, b) $\begin{pmatrix} 3 & -1 \\ 5 & -2 \end{pmatrix} \cdot \mathbf{X} \cdot \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 14 & 16 \\ 9 & 10 \end{pmatrix}$,

c) $\begin{pmatrix} 4 & 6 \\ 6 & 9 \end{pmatrix} \cdot \mathbf{X} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, d) $\mathbf{X} \cdot \begin{pmatrix} 3 & 6 \\ 4 & 8 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 9 & 18 \end{pmatrix}$.

e) $\mathbf{X} \cdot \begin{pmatrix} 5 & 3 & 1 \\ 1 & -3 & -2 \\ -5 & 2 & 1 \end{pmatrix} = \begin{pmatrix} -8 & 3 & 0 \\ -5 & 9 & 0 \\ -2 & 15 & 0 \end{pmatrix}$,

f) $\begin{pmatrix} 2 & -3 & 1 \\ 4 & -5 & 2 \\ 5 & -7 & 3 \end{pmatrix} \cdot \mathbf{X} \cdot \begin{pmatrix} 9 & 7 & 6 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & -2 \\ 18 & 12 & 9 \\ 23 & 15 & 11 \end{pmatrix}$.

2.4. Nech $\mathbf{A}, \mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_s$ sú regulárne štvorcové matice typu $n \times n$. Pomocou cvičenia 2.1 dokážte

a) $$(\mathbf{A}_1 \cdot \mathbf{A}_i \cdot \ldots \cdot \mathbf{A}_s)^{-1} = \mathbf{A}_s^{-1} \cdot \mathbf{A}_{s-1}^{-1} \cdot \ldots \cdot \mathbf{A}_1^{-1}.$$

b) $$(\mathbf{A}^s)^{-1} = (\mathbf{A}^{-1})^s.$$

2.5. Zistite, ako sa zmení inverzná matica $\mathbf{A}^{-1}$, keď v matici $\mathbf{A}$ (s prvkami z poľa F):

a) zameníme i-tý a j-tý riadok,
b) i-tý riadok vynásobíme nenulovým prvkom c poľa F,
c) k i-temu riadku pripočítame c-násobok j-teho riadku, kde c je nenulový prvok poľa F.

2.6. Vypočítajte inverznú maticu k súčinom

a) $\begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix} \cdot \begin{pmatrix} \cos y & -\sin y \\ \sin y & \cos y \end{pmatrix}$ b) $\begin{pmatrix} 1 & -3 & 0 \\ 2 & -5 & 2 \\ 1 & -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 & 1 \\ 5 & 1 & 1 \\ -2 & 0 & 1 \end{pmatrix}.$

2.7. Pomocou vety 2.3 určte determinant, ktorý sa rovná súčinu determinantov

a) $\begin{vmatrix} 2 & -1 \\ 3 & 2 \end{vmatrix} \cdot \begin{vmatrix} 2 & -4 \\ 8 & 5 \end{vmatrix}$ b) $\begin{vmatrix} 1 & 0 & -3 & 5 \\ 4 & 2 & -1 & 0 \\ 0 & 0 & 1 & -4 \\ 3 & 2 & 0 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 & 1 & -1 & 2 \\ 0 & 3 & -1 & 4 \\ 5 & 0 & 5 & 1 \\ 0 & 0 & -1 & 8 \end{vmatrix}$

2.8. Dokážte, že všetky diagonálne regulárne matice tvoria podgrupu grupy všetkých regulárnych matíc typu $n \times n$.

2.9. Nájdite podgrupu grupy všetkých regulárnych matíc typu 2×2 nad poľom reálnych čísel generovanú maticou $\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$.

2.10. Pomocou Cramerových vzorcov riešte nasledujúce sústavy rovníc:

a) $$\begin{aligned} 2x + 3y &= 5, \\ 4x - 8y &= 10, \end{aligned}$$
b) $$\begin{aligned} 2x + 3y &= 8, \\ 6x - 2y &= 2. \end{aligned}$$

c) $$\begin{aligned} 2x_1 - 4x_2 + x_3 &= -9, \\ x_1 + 3x_2 - x_3 &= 13, \\ -x_1 + 2x_2 - 3x_3 &= 17, \end{aligned}$$
d) $$\begin{aligned} 2x_1 - 3x_2 + 6x_3 &= 10, \\ 4x_1 + x_2 - 2x_3 &= -1, \\ 2x_1 - 4x_2 + 5x_3 &= 13, \end{aligned}$$

e) $$\begin{aligned} 3x_1 + 2x_2 + x_3 &= 5, \\ 2x_1 + 3x_2 + x_3 &= 1, \\ 2x_1 + x_2 + 3x_3 &= 11, \end{aligned}$$
f) $$\begin{aligned} x_1 + 2x_2 + 4x_3 &= 31, \\ 5x_1 + x_2 + 2x_3 &= 29, \\ 3x_1 - x_2 + x_3 &= 10, \end{aligned}$$

$g)$
$$\begin{aligned} 2x_1 - 3x_2 + 2x_3 + 4x_4 &= 8, \\ x_1 + 2x_2 - 3x_3 - 2x_4 &= -4, \\ 3x_1 + 2x_2 - 2x_3 + x_4 &= 2, \\ -x_1 + 4x_2 + x_3 - 5x_4 &= -5, \end{aligned}$$

$h)$
$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0, \\ 2x_1 - 3x_2 + 4x_3 - 2x_4 &= 17, \\ -x_1 \qquad + 3x_3 - x_4 &= 7, \\ 3x_1 + 4x_2 + 2x_3 - 3x_4 &= 9. \end{aligned}$$

$i)$
$$\begin{aligned} 2x_1 + 2x_2 - x_3 + x_4 &= 4, \\ 4x_1 + 3x_2 - x_3 + 2x_4 &= 6, \\ 8x_1 + 5x_2 - 3x_3 + 4x_4 &= 12, \\ 3x_1 + 3x_2 - 2x_3 + 2x_4 &= 6, \end{aligned}$$

$j)$
$$\begin{aligned} 2x_1 + 3x_2 + 11x_3 + 5x_4 &= 2, \\ x_1 + x_2 + 5x_3 + 2x_4 &= 1, \\ 2x_1 + x_2 + 3x_3 + 2x_4 &= -3, \\ x_1 + x_2 + 3x_3 + 4x_4 &= -3. \end{aligned}$$

2.11. Ako v príklade 2.5 vyriešte nasledovné sústavy pomocou Cramerových vzorcov, keď viete, že rovnice každej zo sústav sú lineárne nezávislé.

$a)$
$$\begin{aligned} 2x_1 + 3x_2 + 4x_3 - 2x_4 &= 5, \\ 4x_1 + 6x_2 + 6x_3 - 2x_4 &= 12, \end{aligned}$$

$b)$
$$\begin{aligned} x_1 - 2x_2 + 3x_3 - 4x_4 &= 4, \\ x_1 - x_2 + 2x_3 - 3x_4 &= 1, \\ x_1 - 2x_2 + 5x_3 - 8x_4 &= 16. \end{aligned}$$

2.12. Podľa vzorca (2.12) transformujte súradnice vektora $\boldsymbol{\alpha} \in \boldsymbol{V}$ v báze B_1 na súradnice v báze B_2.

a)
$$\begin{aligned} \boldsymbol{V} &= \boldsymbol{V}_4(R), \qquad \boldsymbol{\alpha} = (3,2,2,-7), \\ B_1 &= \{(1,0,0,0),(1,1,0,0),(1,1,1,0),(1,1,1,1)\}, \\ B_2 &= \{(2,1,-5,1),(1,-3,0,-6),(0,2,-1,2),(1,4,-7,6)\}. \end{aligned}$$

b)
$$\begin{aligned} \boldsymbol{V} &= \mathbf{P}_3(R), \qquad \boldsymbol{\alpha} = 3 - 2x + x^2, \\ B_1 &= \{1, x, x^2\}, \\ B_2 &= \{3, (2x-1), (2x-1)^2\}. \end{aligned}$$

c) $\boldsymbol{V}$ je priestor matíc typu 2×2 nad poľom reálnych čísel.

$$\begin{aligned} \boldsymbol{\alpha} &= \begin{pmatrix} 3 & -1 \\ 2 & 0 \end{pmatrix}, \\ B_1 &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}, \\ B_2 &= \left\{ \begin{pmatrix} 1 & 4 \\ -1 & 9 \end{pmatrix}, \begin{pmatrix} 0 & -10 \\ 2 & 14 \end{pmatrix}, \begin{pmatrix} -2 & 6 \\ -5 & 4 \end{pmatrix}, \begin{pmatrix} 5 & -3 \\ 8 & -6 \end{pmatrix} \right\}. \end{aligned}$$

Kapitola 5

LINEÁRNE ZOBRAZENIA

§ 1. Základné vlastnosti lineárnych zobrazení

Príklad 1.1. Nech $\boldsymbol{V}$ je vektorový priestor orientovaných úsečiek v rovine vychádzajúcich z daného pevného bodu P. (Pozri príklad 1.1 kapitoly 2.) Nech $\boldsymbol{S}$ je podpriestor tých orientovaných úsečiek, ktoré ležia na priamke p prechádzajúcej bodom P. Nech $\varphi : \boldsymbol{V} \to \boldsymbol{S}$ je zobrazenie, ktoré každému vektoru $\vec{\boldsymbol{a}} \in \boldsymbol{V}$ priradí jeho priemet $\vec{\boldsymbol{a}}_p$ na priamku p. Zrejme platí $\varphi(\vec{\boldsymbol{a}} + \vec{\boldsymbol{b}}) = (\vec{\boldsymbol{a}} + \vec{\boldsymbol{b}})_p = \vec{\boldsymbol{a}}_p + \vec{\boldsymbol{b}}_p = \varphi(\vec{\boldsymbol{a}}) + \varphi(\vec{\boldsymbol{b}})$, to po prvé, a po druhé $\varphi(s\vec{\boldsymbol{a}}) = s\varphi(\vec{\boldsymbol{a}})$, kde $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}} \in \boldsymbol{V}$, $\varphi(\vec{\boldsymbol{a}})$, $\varphi(\vec{\boldsymbol{b}}) \in \boldsymbol{S}$ a $s \in R$ (pole reálnych čísel). Všimnime si, že zobrazenie φ nám zachováva ako sčítanie vektorov, tak aj skalárny násobok vektora.

Príklad 1.2. Nech $\boldsymbol{M}_2(Q)$ je vektorový priestor matíc typu 2×2 s racionálnymi prvkami. Uvažujme ďalej vektorový priestor $\boldsymbol{V}_3(Q)$. Nech je dané zobrazenie $\varphi : \boldsymbol{M}_2(Q) \to \boldsymbol{V}_3(Q)$ tak, že každej matici z $\boldsymbol{M}_2$ je priradený ten vektor z $\boldsymbol{V}_3(Q)$, ktorého prvé dve zložky sú rovné prvkom prvého riadku matice a tretia zložka je nulová. Teda

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a, b, 0). \tag{1.1}$$

Čitateľ rýchlo skontroluje, že opäť pre ľubovoľné $\mathbf{A}, \mathbf{B} \in \boldsymbol{M}_2(Q)$, $s \in Q$ platí $\varphi(\mathbf{A} + \mathbf{B}) = \varphi(\mathbf{A}) + \varphi(\mathbf{B})$, ako aj $\varphi(s\mathbf{A}) = s\varphi(\mathbf{A})$. Teda zobrazenie φ „zachováva“ súčet vektorov i skalárny násobok.

Definícia 1.1. Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ je také zobrazenie vektorového priestoru $\boldsymbol{V}(F)$ do vektorového priestoru $\boldsymbol{W}(F)$, že sú splnené nasledujúce podmienky:

$$\varphi(\boldsymbol{\alpha} + \boldsymbol{\beta}) = \varphi(\boldsymbol{\alpha}) + \varphi(\boldsymbol{\beta}), \tag{i}$$

$$\varphi(s\boldsymbol{\alpha}) = s\varphi(\boldsymbol{\alpha}), \tag{ii}$$

kde $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}(F)$ sú ľubovoľné vektory a $s \in F$ ľubovoľný skalár. Potom φ nazývame *morfizmus* alebo *lineárne zobrazenie* vektorového priestoru $\boldsymbol{V}$ do vektorového priestoru $\boldsymbol{W}$.

Poznámka 1.1. Ak je morfizmus φ z definície 1.1 injekcia (surjekcia, bijekcia), nazývame ho monomorfizmom (epimorfizmom, izomorfizmom). Ak budeme používať názov lineárne zobrazenie (obvyklý v lineárnej algebre), budeme hovoriť jednoducho o injektívnom (surjektívnom, bijektívnom) lineárnom zobrazení. Hneď vidieť, že lineárne zobrazenie z príkladu 1.1 je surjektívne, kým zobrazenie z príkladu 1.2 nie je ani injektívne ani surjektívne.

Príklad 1.3. Nech $\boldsymbol{V}_k(F)$ a $\boldsymbol{V}_n(F)$ sú vektorové priestory k-tíc resp. n-tíc nad telesom F a nech $2 \leqq k < n$. Zobrazenie $\psi : \boldsymbol{V}_k(F) \to \boldsymbol{V}_n(F)$ definované takto:

$$\psi[(x_1, x_2, \ldots, x_k)] = (x_1, x_2, \ldots, x_k, 0, \ldots, 0) \in \boldsymbol{V}_n(F)$$

je injektívnym lineárnym zobrazením (monomorfizmom). Dokážte to!

Príklad 1.4. Nech je daný pravouhlý súradnicový systém v rovine. Nech $\boldsymbol{V}$ je vektorový priestor orientovaných úsečiek vychádzajúcich z počiatku tohoto systému. Zobrazenie

$$\varphi : \boldsymbol{V} \to \boldsymbol{V}_2(R),$$

ktoré každému vektoru $\vec{\boldsymbol{a}} \in \boldsymbol{V}$ priradí tú dvojicu reálnych čísel, ktorá je dvojicou súradníc koncového bodu vektora $\vec{\boldsymbol{a}}$ je bijektívne lineárne zobrazenie (izomorfizmus).

Veta 1.1. *Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ je lineárne zobrazenie. Potom*

(i) $$\varphi(\vec{\mathbf{0}}) = \vec{\mathbf{0}}$$

(ii) $$\varphi(c_1\boldsymbol{\alpha}_1 + c_2\boldsymbol{\alpha}_2 + \cdots + c_k\boldsymbol{\alpha}_k) = c_1\varphi(\boldsymbol{\alpha}_1) + c_2\varphi(\boldsymbol{\alpha}_2) + \cdots + c_k\varphi(\boldsymbol{\alpha}_k),$$

*kde $\boldsymbol{\alpha}_i \in \boldsymbol{V}$, $\varphi(\boldsymbol{\alpha}_i) \in \boldsymbol{W}$, $c_i \in F$.**)

Inými slovami: Nulový vektor sa zobrazí na nulový vektor a lineárna kombinácia vektorov sa zobrazí na lineárnu kombináciu ich obrazov (s tými istými koeficientami lineárnej kombinácie).

Dôkaz ponecháme na čitateľa. Poznamenajme len, že morfizmus φ z definície 1.1 sa nazýva *lineárnym* zobrazením preto, lebo „zachováva“ *lineárnu* kombináciu. □

Veta 1.2 (hlavná veta o lineárnom zobrazení)**.** *Nech $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n\}$ je báza priestoru $\boldsymbol{V}(F)$ a nech $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_n$ sú ľubovoľné vektory vektorového priestoru $\boldsymbol{W}(F)$.***) *Potom existuje práve jedno lineárne zobrazenie φ také, že platí*

(1.2) $$\varphi(\boldsymbol{\varepsilon}_1) = \boldsymbol{\alpha}_1,\ \varphi(\boldsymbol{\varepsilon}_2) = \boldsymbol{\alpha}_2,\ \ldots,\ \varphi(\boldsymbol{\varepsilon}_n) = \boldsymbol{\alpha}_n.$$

Poznámka 1.2. Čitateľ nech si uvedomí, že v predpoklade vety 1.2 sa nežiada, aby vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_n$ boli lineárne nezávislé, ba ani to, aby boli rôzne.

Dôkaz vety 1.2. A. Existencia. Nech $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_n\boldsymbol{\varepsilon}_n$ je ľubovoľný vektor priestoru $\boldsymbol{V}$. Definujeme zobrazenie $\varphi : \boldsymbol{V} \to \boldsymbol{W}$ takto:

(1.3) $$\varphi(\boldsymbol{\alpha}) = \varphi(x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_n\boldsymbol{\varepsilon}_n) = x_1\boldsymbol{\alpha}_1 + x_2\boldsymbol{\alpha}_2 + \cdots + x_n\boldsymbol{\alpha}_n.$$

Dokážeme, že zobrazenie φ je lineárne. Ľubovoľné vektory $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}$ vyjadríme ako lineárne kombinácie vektorov bázy $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_2 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_n\boldsymbol{\varepsilon}_n$,

*) Zrejme nevadí, že symbol $\vec{\mathbf{0}}$ na ľavej strane (i) je nulový vektor priestoru $\boldsymbol{V}$, zatiaľ čo na pravej strane (i) ten istý symbol znamená nulový vektor priestoru $\boldsymbol{W}$.

**) Predpokladáme teda, že priestor $\boldsymbol{V}(F)$ je konečnorozmerný a oba priestory sú nad tým istým poľom.

$\boldsymbol{\beta} = y_1\boldsymbol{\varepsilon}_1 + y_2\boldsymbol{\varepsilon}_2 + \cdots + y_n\boldsymbol{\varepsilon}_n$. Potom

$$\begin{aligned}\varphi(\boldsymbol{\alpha}+\boldsymbol{\beta}) &= \varphi((x_1+y_1)\boldsymbol{\varepsilon}_1 + (x_2+y_2)\boldsymbol{\varepsilon}_2 + \cdots + (x_n+y_n)\boldsymbol{\varepsilon}_n) = \\ &= (x_1+y_1)\boldsymbol{\alpha}_1 + (x_2+y_2)\boldsymbol{\alpha}_2 + \cdots + (x_n+y_n)\boldsymbol{\alpha}_n = \\ &= x_1\boldsymbol{\alpha}_1 + x_2\boldsymbol{\alpha}_2 + \ldots x_n\boldsymbol{\alpha}_n + y_1\boldsymbol{\alpha}_1 + y_2\boldsymbol{\alpha}_2 + \cdots + y_n\boldsymbol{\alpha}_n = \varphi(\boldsymbol{\alpha}) + \varphi(\boldsymbol{\beta}).\end{aligned}$$

Podobne sa dokáže, že $\varphi(s\boldsymbol{\alpha}) = s\varphi(\boldsymbol{\alpha})$ pre ľubovoľný skalár $s \in F$. Čitateľ rýchlo zistí, že pre φ platia vzťahy (1.2).

B. Jednoznačnosť. Dokážeme jednoznačnosť zobrazenia φ. Nech $\psi : \boldsymbol{V} \to \boldsymbol{W}$ je ľubovoľné lineárne zobrazenie, pre ktoré platia vzťahy (1.2), t.j.

$$\psi(\boldsymbol{\varepsilon}_1) = \boldsymbol{\alpha}_1, \quad \psi(\boldsymbol{\varepsilon}_2) = \boldsymbol{\alpha}_2, \quad \ldots, \quad \psi(\boldsymbol{\varepsilon}_n) = \boldsymbol{\alpha}_n.$$

Nech $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_n\boldsymbol{\varepsilon}_n$ je ľubovoľný vektor priestoru $\boldsymbol{V}$. Potom

$$\begin{aligned}\psi(\boldsymbol{\alpha}) &= \psi(x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_n\boldsymbol{\varepsilon}_n) = \\ &= x_1\psi(\boldsymbol{\varepsilon}_1) + x_2\psi(\boldsymbol{\varepsilon}_2) + \cdots + x_n\psi(\boldsymbol{\varepsilon}_n) = x_1\boldsymbol{\alpha}_1 + x_2\boldsymbol{\alpha}_2 + \ldots x_n\boldsymbol{\alpha}_n = \varphi(\boldsymbol{\alpha}),\end{aligned}$$

kde sme najskôr použili vetu 1.1, potom (1.3). Vidíme, že $\psi = \varphi$, t.j. zobrazenie φ uvedených vlastností je jediné. □

Definícia 1.2. Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ je lineárne zobrazenie. *Jadrom* lineárneho zobrazenia nazývame množinu

$$\operatorname{Ker}\varphi = \{\boldsymbol{\alpha} \in \boldsymbol{V};\ \varphi(\boldsymbol{\alpha}) = \vec{\mathbf{0}} \in \boldsymbol{W}\}.$$

Obrazom lineárneho zobrazenia je množina

$$\operatorname{Im}\varphi = \{\boldsymbol{\beta} \in \boldsymbol{W};\ \text{existuje } \boldsymbol{\alpha} \in \boldsymbol{V} \text{ tak, že } \varphi(\boldsymbol{\alpha}) = \boldsymbol{\beta}\}.$$

Príklad 1.5. Vráťme sa k zobrazeniu $\varphi : \boldsymbol{M}_2(Q) \to \boldsymbol{V}_3(Q)$ z príkladu 1.2. Ihneď vidieť, že

$$\operatorname{Ker}\varphi = \left\{ \begin{pmatrix} 0 & 0 \\ x & y \end{pmatrix};\ x, y \in Q \right\},$$

$$\operatorname{Im}\varphi = \{(a, b, 0);\ a, b \in Q\}.$$

Veta 1.3. *Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ je lineárne zobrazenie. Jadro zobrazenia je podpriestor priestoru $\boldsymbol{V}$, obraz zobrazenia je podpriestor priestoru $\boldsymbol{W}$.*

Dôkaz. 1. Nech $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \operatorname{Ker}\varphi$, potom $\varphi(\boldsymbol{\alpha}) = \varphi(\boldsymbol{\beta}) = \vec{\mathbf{0}}$. Počítame $\varphi(\boldsymbol{\alpha}+\boldsymbol{\beta}) = \varphi(\boldsymbol{\alpha}) + \varphi(\boldsymbol{\beta}) = \vec{\mathbf{0}} + \vec{\mathbf{0}} = \vec{\mathbf{0}}$, čiže $\boldsymbol{\alpha}+\boldsymbol{\beta} \in \operatorname{Ker}\varphi$. Analogicky sa dokáže, že pre ľubovoľné $\boldsymbol{\alpha} \in \operatorname{Ker}\varphi$, $s \in F$ platí $s\boldsymbol{\alpha} \in \operatorname{Ker}\varphi$. Potom podľa vety 3.1 kapitoly 2 $\operatorname{Ker}\varphi$ je podpriestor priestoru $\boldsymbol{V}$.

2. Dôkaz, že $\operatorname{Im}\varphi$ je podpriestor priestor $\boldsymbol{W}$ ponecháme na čitateľa. □

Veta 1.4. *Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ je lineárne zobrazenie. Potom*

(i) *φ je injektívne zobrazenie (monomorfizmus) práve vtedy, keď* $\operatorname{Ker}\varphi = \{\vec{\mathbf{0}}\}$,

(ii) *φ je surjektívne zobrazenie (epimorfizmus) práve vtedy, keď* $\operatorname{Im}\varphi = \boldsymbol{W}$,

(iii) *φ je bijektívne zobrazenie (izomorfizmus) práve vtedy, keď* $\operatorname{Ker}\varphi = \{\vec{\mathbf{0}}\}$ a $\operatorname{Im}\varphi = \boldsymbol{W}$.

Dôkaz. (i) I. Ak φ je injektívne lineárne zobrazenie, tak vzhľadom na (i) vo vete (1.1) je $\operatorname{Ker}\varphi = \{\vec{\mathbf{0}}\}$.

II. Naopak, nech φ je také zobrazenie, že $\operatorname{Ker}\varphi = \{\vec{\mathbf{0}}\}$. Nech $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$ sú vektory priestoru $\boldsymbol{V}$. Ak by $\varphi(\boldsymbol{\alpha}) = \varphi(\boldsymbol{\beta})$, bolo by $\varphi(\boldsymbol{\alpha}) - \varphi(\boldsymbol{\beta}) = \vec{\mathbf{0}}$, čiže $\varphi(\boldsymbol{\alpha}-\boldsymbol{\beta}) = \vec{\mathbf{0}}$ a tak $\boldsymbol{\alpha}-\boldsymbol{\beta} \in \operatorname{Ker}\varphi$. To by znamenalo, že $\boldsymbol{\alpha}-\boldsymbol{\beta} = \vec{\mathbf{0}}$ t.j. $\boldsymbol{\alpha} = \boldsymbol{\beta}$, čo je spor s predpokladom. Teda $\varphi(\boldsymbol{\alpha}) \neq \varphi(\boldsymbol{\beta})$, čiže φ je injekcia.

Dôkaz (ii) je triviálny, (iii) vyplýva z (i) a (ii). □

Veta 1.5. *Nech* $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ *je báza vektorového priestoru* $\boldsymbol{V}(F)$ a $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n \in \boldsymbol{W}(F)$. *Nech* $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ *je lineárne zobrazenie také, že* $\varphi(\boldsymbol{\varepsilon}_i) = \boldsymbol{\alpha}_i$, $i = 1, 2, \dots, n$. *Potom*

(i) φ *je injektívne (monomorfizmus) práve vtedy, keď vektory* $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$ *sú lineárne nezávislé.*

(ii) φ *je surjektívne (epimorfizmus) práve vtedy, keď* $[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] = \boldsymbol{W}$.

(iii) φ *je bijektívne (izomorfizmus) práve vtedy, keď* $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n\}$ *je báza priestoru* $\boldsymbol{W}$.

Dôkaz. (i) I. Nech φ je injektívne, potom podľa vety 1.4 $\operatorname{Ker}\varphi = \{\vec{\mathbf{0}}\}$. Ak by vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n \in \boldsymbol{W}$ boli lineárne závislé, tak by platilo $x_1\boldsymbol{\alpha}_1 + x_2\boldsymbol{\alpha}_2 + \dots + x_n\boldsymbol{\alpha}_n = \vec{\mathbf{0}}$, pričom pre niektoré i by $x_i \neq 0$. Uvažujme o vektore $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n \in \boldsymbol{V}$. Zrejme $\boldsymbol{\alpha} \neq \vec{\mathbf{0}}$ (prečo?), ale $\varphi(\boldsymbol{\alpha}) = \varphi(x_1\boldsymbol{\varepsilon}_1 + \dots + x_n\boldsymbol{\varepsilon}_n) = x_1\boldsymbol{\alpha}_1 + \dots + x_n\boldsymbol{\alpha}_n = \vec{\mathbf{0}}$, teda $\boldsymbol{\alpha} \in \operatorname{Ker}\varphi$, čo je nemožné.

II. Nech vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$ sú lineárne nezávislé. Nech $\boldsymbol{\alpha} \in \operatorname{Ker}\varphi$. Vektor $\boldsymbol{\alpha}$ vyjadríme v tvare $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n$. Platí $\vec{\mathbf{0}} = \varphi(\boldsymbol{\alpha}) = x_1\boldsymbol{\alpha}_1 + x_2\boldsymbol{\alpha}_2 + \dots + x_n\boldsymbol{\alpha}_n$. Nakoľko $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$ sú lineárne nezávislé, je $x_1 = x_2 = \dots = x_n = 0$ a teda $\boldsymbol{\alpha} = \vec{\mathbf{0}}$. Preto $\operatorname{Ker}\varphi = \{\vec{\mathbf{0}}\}$ a podľa vety 1.4 je φ injektívne zobrazenie.

(ii) I. Nech φ je surjektívne lineárne zobrazenie. Keďže podľa (1.3) obrazom každého vektora $\boldsymbol{\alpha} \in \boldsymbol{V}$ je lineárna kombinácia vektorov $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n$ podľa vety 3.4 kapitoly 2 musí byť $[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] = \boldsymbol{W}$.

II. Nech naopak $[\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n] = \boldsymbol{W}$. Potom ľubovoľný vektor $\boldsymbol{\beta} \in \boldsymbol{W}$ sa dá vyjadriť v tvare $\boldsymbol{\beta} = y_1\boldsymbol{\alpha}_1 + y_2\boldsymbol{\alpha}_2 + \dots + y_n\boldsymbol{\alpha}_n$. To znamená, že $\boldsymbol{\beta}$ je obrazom vektora $y_1\boldsymbol{\varepsilon}_1 + y_2\boldsymbol{\varepsilon}_2 + \dots + y_n\boldsymbol{\varepsilon}_n \in \boldsymbol{V}$, čiže φ je surjektívne zobrazenie.

(iii) Ak si uvedomíme, že báza je množina lineárne nezávislých vektorov, ktorá generuje celý priestor, tvrdenie (iii) okamžite vyplýva z (i) a (ii). $\square$

Veta 1.6. *Nech* $\boldsymbol{V}$ a $\boldsymbol{W}$ *sú dva priestory konečnej dimenzie nad poľom* F. *Potom* $d(\boldsymbol{V}) = d(\boldsymbol{W})$ *práve vtedy, keď* $\boldsymbol{V}$ a $\boldsymbol{W}$ *sú izomorfné priestory.*

Dôkaz. I. Nech $d(\boldsymbol{V}) = d(\boldsymbol{W}) = n$ a nech $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ je báza priestoru $\boldsymbol{V}$ a $\{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, , \dots, \boldsymbol{\eta}_n\}$ je báza priestoru $\boldsymbol{W}$. Ľubovoľný vektor $\boldsymbol{\alpha} \in \boldsymbol{V}$ vyjadríme v tvare

$$\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n.$$

Bijekciu $f : \boldsymbol{V} \to W$ definujeme rovnosťou

$$f(\boldsymbol{\alpha}) = x_1\boldsymbol{\eta}_1 + x_2\boldsymbol{\eta}_2 + \dots + x_n\boldsymbol{\eta}_n. \tag{1.4}$$

Čitateľ ľahko zistí, že f je izomorfizmus.

II. Nech priestory $\boldsymbol{V}$ a $\boldsymbol{W}$ sú izomorfné a $f : \boldsymbol{V} \to \boldsymbol{W}$ je príslušný izomorfizmus. Nech $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ je báza priestoru $\boldsymbol{V}$. Potom podľa (iii) vety 1.5 je $\{f(\boldsymbol{\varepsilon}_1), f(\boldsymbol{\varepsilon}_2), \dots, f(\boldsymbol{\varepsilon}_n)\}$ báza priestoru $\boldsymbol{W}$ t.j. $d(\boldsymbol{W}) = n$. $\square$

Dôsledok. *Všetky vektorové priestory nad tým istým poľom* F *rovnakej dimenzie* n *sú navzájom izomorfné t.j. izomorfné priestoru* $\boldsymbol{V}_n(F)$.

Poznámka 1.3 (dôležitá) Nech $\boldsymbol{V}(F)$ je vektorový priestor dimenzie n. Izomorfizmus $f : \boldsymbol{V}(F) \to \boldsymbol{V}_n(F)$ často definujeme takto: V priestore $\boldsymbol{V}$ zvolíme bázu $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$. Ľubovoľnému vektoru $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n \in \boldsymbol{V}$ priradíme n-ticu $f(\boldsymbol{\alpha}) = (x_1, x_2, \dots, x_n) \in \boldsymbol{V}_n(F)$. Hovoríme, že vektoru $\boldsymbol{\alpha}$ sme priradili vektor jeho súradníc $f(\boldsymbol{\alpha})$. Čitateľ si dokáže sám, že f je bijektívne lineárne zobrazenie. Teda z algebraického hľadiska je jedno, či máme vektory $\boldsymbol{\alpha}$ z $\boldsymbol{V}$ alebo vektory ich súradníc z $\boldsymbol{V}_n(F)$.

Príklad 1.6. Ľahko dokážeme, že množiny $\boldsymbol{V} = \{(x, y, z); x, y, z \in R, 2x + y = 0\}$, $\boldsymbol{W} = \{(r, s, t); r, s, t \in R, r - s + t = 0\}$ sú podpriestory priestoru $\boldsymbol{V}_3(R)$ a že platí $d(\boldsymbol{V}) = d(\boldsymbol{W}) = 2$. Ak zvolíme vo $\boldsymbol{V}$, resp. $\boldsymbol{W}$ bázy $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2\}$, resp. $\{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2\}$, môžeme definovať izomorfizmus f podľa (1.4) t.j. že obrazom ľubovoľného vektora $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2$ bude vektor $f(\boldsymbol{\alpha}) = x_1\boldsymbol{\eta}_1 + x_2\boldsymbol{\eta}_2$. Konkrétne ak $\boldsymbol{\varepsilon}_1 = (1, -2, 0)$, $\boldsymbol{\varepsilon}_2 = (2, -4, 1)$, $\boldsymbol{\eta}_1 = (1, 2, 1)$, $\boldsymbol{\eta}_2 = (3, 3, 0)$, $\boldsymbol{\alpha} = (3, -6, -1) = 5\boldsymbol{\varepsilon}_1 - \boldsymbol{\varepsilon}_2$ tak $f(\boldsymbol{\alpha}) = 5\boldsymbol{\eta}_1 - \boldsymbol{\eta}_2 = 5(1, 2, 1) - -(3, 3, 0) = (2, 7, 5)$.

Čitateľa prosíme, aby si zopakoval pojem komplementárnych podpriestorov, definovaný v cvičení 4.8 kapitoly 2.

Veta 1.7. *Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ je lineárne zobrazenie. Nech podpriestor $\boldsymbol{L}$ je komplement jadra* $\operatorname{Ker}\varphi$ *a nech $d(\boldsymbol{V}) = n$. Nech $\psi : \boldsymbol{L} \to \operatorname{Im}\varphi$ je zobrazenie definované takto:*

$$\textit{Pre všetky } \boldsymbol{\alpha} \in \boldsymbol{L} \ \ \psi(\boldsymbol{\alpha}) = \boldsymbol{\beta} \ \textit{ práve vtedy, keď } \ \varphi(\boldsymbol{\alpha}) = \boldsymbol{\beta}.$$

Potom ψ je bijektívne lineárne zobrazenie (izomorfizmus) $\boldsymbol{L}$ na $\operatorname{Im}\varphi$.

Dôkaz. Keďže $\operatorname{Ker}\varphi$ a $\boldsymbol{L}$ sú komplementárne, t.j. $\operatorname{Ker}\varphi \cap \boldsymbol{L} = \{\vec{\mathbf{0}}\}$, vektor $\vec{\mathbf{0}}$ je jediný vektor z $\boldsymbol{L}$, ktorý sa zobrazí na $\vec{\mathbf{0}} \in \operatorname{Im}\varphi$. Preto $\operatorname{Ker}\psi = \{\vec{\mathbf{0}}\}$ a podľa vety 1.4 zobrazenie ψ je injekcia.

Ak $\operatorname{Ker}\varphi = \{\vec{\mathbf{0}}\}$ alebo $\boldsymbol{V}$, tak ψ je surjekcia (overte). Nech $\operatorname{Ker}\varphi \neq \{\vec{\mathbf{0}}\}, \boldsymbol{V}$. Nech $\boldsymbol{\beta}$ je ľubovoľný vektor z $\operatorname{Im}\varphi$. Potom existuje $\boldsymbol{\alpha} \in \boldsymbol{V}$ tak, že $\varphi(\boldsymbol{\alpha}) = \boldsymbol{\beta}$. Nech $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_k\}$ je báza $\operatorname{Ker}\varphi$. Podľa vety 4.2 kapitoly 2 ju možno doplniť na bázu celého priestoru $B = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_k, \boldsymbol{\varepsilon}_{k+1}, \dots, \boldsymbol{\varepsilon}_n\}$. Potom (kapitola 2, cvičenie 4.8b) je $\{\boldsymbol{\varepsilon}_{k+1}, \dots, \boldsymbol{\varepsilon}_n\}$ báza doplnku $\boldsymbol{L}$. Nech

$$\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + \dots + x_k\boldsymbol{\varepsilon}_k + x_{k+1}\boldsymbol{\varepsilon}_{k+1} + \dots + x_n\boldsymbol{\varepsilon}_n$$

je vyjadrenie vektora $\boldsymbol{\alpha}$ ako lineárna kombinácia vektorov bázy B. Vektor $\boldsymbol{\alpha}$ môžeme písať v tvare $\boldsymbol{\alpha} = (x_1\boldsymbol{\varepsilon}_1 + \dots + x_k\boldsymbol{\varepsilon}_k) + (x_{k+1}\boldsymbol{\varepsilon}_{k+1} + \dots x_n\boldsymbol{\varepsilon}_n) = \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2$, kde $\boldsymbol{\alpha}_1 \in \operatorname{Ker}\varphi$ a $\boldsymbol{\alpha}_2 \in \boldsymbol{L}$. Tvrdíme, že $\psi(\boldsymbol{\alpha}_2) = \boldsymbol{\beta}$. Skutočne $\boldsymbol{\beta} = \varphi(\boldsymbol{\alpha}) = = \varphi(\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2) = \varphi(\boldsymbol{\alpha}_1) + \varphi(\boldsymbol{\alpha}_2) = \vec{\mathbf{0}} + \varphi(\boldsymbol{\alpha}_2) = \varphi(\boldsymbol{\alpha}_2) = \psi(\boldsymbol{\alpha}_2)$. To znamená, že ψ je surjekcia. □

Veta 1.8. *Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ je lineárne zobrazenie a nech $d(\boldsymbol{V}) = n$, kde n je prirodzené číslo. Potom*

$$d(\operatorname{Ker}\varphi) + d(\operatorname{Im}\varphi) = n. \tag{1.5}$$

Dôkaz. Nech $\boldsymbol{L}$ je komplement podpriestoru $\operatorname{Ker}\varphi$ v priestore $\boldsymbol{V}$. Potom podľa cvičenia 4.8 kapitoly 2 je $d(\operatorname{Ker}\varphi) + d(\boldsymbol{L}) = n$. Vo vete 1.7 sme dokázali existenciu izomorfizmu $\psi : \boldsymbol{L} \to \operatorname{Im}\varphi$. Podľa vety 1.6 $d(\boldsymbol{L}) = d(\operatorname{Im}\varphi)$. Dostali sme (1.5). □

Cvičenia

1.1. Zistite, ktoré z nasledujúcich zobrazení je lineárne zobrazenie

a) $\varphi : \boldsymbol{V}_2(R) \to \boldsymbol{V}_3(R)$, kde $\varphi((x_1, x_2)) = (x_1, x_2, 0)$,
b) $\varphi : \boldsymbol{V}_3(R) \to \boldsymbol{V}_4(R)$, kde $\varphi((x_1, x_2, x_3)) = (x_1, x_2, x_3, x_3)$,
c) $\varphi : \boldsymbol{V}_4(R) \to \boldsymbol{V}_3(R)$, kde $\varphi((x_1, x_2, x_3, x_4)) = (x_1, x_2, x_3)$,
d) $\varphi : \boldsymbol{V}_3(R) \to \boldsymbol{V}_4(R)$, kde $\varphi((x_1, x_2, x_3)) = (x_1, x_2, x_3, 2)$,
e) $\varphi : \boldsymbol{V}_3(R) \to \boldsymbol{V}_3(R)$, kde $\varphi((x_1, x_2, x_3)) = (x_1, 3x_1 + x_2, x_3 + 2)$,
f) $\varphi : \boldsymbol{V}_3(R) \to \boldsymbol{V}_3(R)$, kde $\varphi((x_1, x_2, x_3)) = (x_1, 3x_1 + x_2, x_3)$.

1.2. Určte, ktoré z lineárnych zobrazení cvičenia 1.1 je injektívne, ktoré surjektívne a ktoré bijektívne a nájdite jadro a obraz daných zobrazení.

1.3. Nech $\varphi : \boldsymbol{V} \to \boldsymbol{W}$ je lineárne zobrazenie vektorových priestorov. Dokážte, že pre všetky $\boldsymbol{\alpha} \in \boldsymbol{V}$: $\varphi(-\boldsymbol{\alpha}) = -\varphi(\boldsymbol{\alpha})$.

1.4. Nech $\varphi_i : \boldsymbol{V}_3(R) \to \boldsymbol{V}_4(R)$ sú také lineárne zobrazenia, že platí

a) $\varphi_1((1,0,0)) = (3,-1,2,8)$, $\varphi_1((0,1,0)) = (2,1,1,0)$,
$\varphi_1((0,0,1)) = (1,-2,1,8)$,
b) $\varphi_2((1,2,2)) = (3,1,1,0)$, $\varphi_2((1,1,2)) = (1,1,3,2)$,
$\varphi_2((2,3,5)) = (4,2,4,3)$,
c) $\varphi_3((1,0,0)) = (1,2,3,1)$ $\varphi_3((0,1,1)) = (1,2,3,1)$,
$\varphi_3((2,1,-1)) = (2,4,6,2)$.

Vypočítajte $\varphi_i((x_1, x_2, x_3))$, kde $\boldsymbol{\alpha} = (x_1, x_2, x_3)$ je ľubovoľný vektor priestoru $\boldsymbol{V}_3(R)$. Ďalej určte, ktoré zo zobrazení φ_i je injektívne (surjektívne, bijektívne), nájdite jadro a obraz daných zobrazení a overte, že $d(\operatorname{Ker}\varphi_i) + d(\operatorname{Im}\varphi_i) = 3$.

1.5. Nech $\varphi_i : \boldsymbol{V}_4(R) \to \boldsymbol{V}_3(R)$ sú také lineárne zobrazenia, že platí

a) $\varphi_1((1,0,0,0)) = (1,1,1)$, $\varphi_1((0,1,0,0)) = (0,1,1)$,
$\varphi_1((0,0,1,0)) = (0,0,1)$, $\varphi_1((0,0,0,1)) = (1,-1,3)$,
b) $\varphi_2((1,-1,1,0)) = (1,3,-1)$, $\varphi_2((0,1,1,0)) = (1,3,-1)$,
$\varphi_2((-2,2,3,-1)) = (1,3,-1)$, $\varphi_2((3,-2,2,-3)) = (1,3,-1)$,
c) $\varphi_3((1,2,0,0)) = (1,1,3)$, $\varphi_3((0,1,1,0)) = (1,2,3)$,
$\varphi_3((1,0,0,-1)) = (0,-1,0)$, $\varphi_3((1,1,-1,1)) = (2,3,6)$.

Analogicky ako v predchádzajúcom cvičení, vypočítajte $\varphi_i(x_1, x_2, x_3, x_4)$, kde $\boldsymbol{\alpha} = (x_1, x_2, x_3, x_4)$ je ľubovoľný vektor priestoru $\boldsymbol{V}_4(R)$, určte, ktoré zo zobrazení φ_i je injektívne (surjektívne, bijektívne), nájdite jadro a obraz uvedených zobrazení a overte, že $d(\operatorname{Ker}\varphi_i) + d(\operatorname{Im}\varphi_i) = 4$.

1.6. Nech $\boldsymbol{V}(F)$ je vektorový priestor a $\boldsymbol{S}$ je podpriestor priestoru $\boldsymbol{V}$. Nech ďalej $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ je lineárne zobrazenie. Nech $\boldsymbol{W}_0$ je taká podmnožina priestoru $\boldsymbol{W}$, pre ktorú platí

$$\boldsymbol{W}_0 = \{\boldsymbol{\beta};\ \text{existuje taký vektor } \boldsymbol{\alpha} \in \boldsymbol{S},\ \text{že platí } \varphi(\boldsymbol{\alpha}) = \boldsymbol{\beta}\}.$$

Dokážte, že $\boldsymbol{W}_0$ je podpriestor priestoru $\boldsymbol{W}$.

1.7. Nech $\boldsymbol{P}_5(R)$ je vektorový priestor všetkých polynómov (s reálnymi koeficientami) stupňa najviac štvrtého. Definujme zobrazenie $\varphi : \boldsymbol{P}_5(R) \to \boldsymbol{V}_5(R)$ takto: Ak f je polynóm z $\boldsymbol{P}_5(R)$, tak $\varphi(f) = (f(0), f'(0), f''(0), f^{(3)}(0), f^{(4)}(0))$. Dokážte, že φ je izomorfizmus priestorov $\boldsymbol{P}_5$ a $\boldsymbol{V}_5$.

1.8. Nájdite jadrá a obrazy nasledujúcich lineárnych zobrazení vektorových priestorov:

a) $\varphi_1 : \boldsymbol{V}_2(R) \to \boldsymbol{V}_6(R)$, kde $\varphi_1((x_1, x_2)) = (x_1, x_2, x_1, x_2, x_1, x_2)$,
b) $\varphi_r : \boldsymbol{V}_3(R) \to \boldsymbol{V}_3(R)$, kde $\varphi_2((x_1, x_2, x_3)) = (x_1,\ x_1 + x_2,\ x_1 + x_2 + x_3)$,
c) $\varphi_3 : \boldsymbol{V}_3(R) \to \boldsymbol{M}_2(R)$, kde $\varphi_3((x_1, x_2, x_3)) = \begin{pmatrix} x_1, & x_2 \\ 0, & 0 \end{pmatrix}$.

§ 2. Matica lineárneho zobrazenia

V tomto paragrafe si ukážeme, že medzi maticami a lineárnymi zobrazeniami vektorových priestorov konečných dimenzií je úzky vzťah.

Definícia 2.1. Nech $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_m\}$ je báza priestoru $\boldsymbol{V}(F)$ a $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2 \dots, \boldsymbol{\eta}_n\}$ báza priestoru $\boldsymbol{W}(F)$. Nech $\varphi : \boldsymbol{V} \to \boldsymbol{W}$ je lineárne zobrazenie, pričom

$$\begin{aligned}
\varphi(\boldsymbol{\varepsilon}_1) &= a_{11}\boldsymbol{\eta}_1 + a_{12}\boldsymbol{\eta}_2 + \dots + a_{1n}\boldsymbol{\eta}_n, \\
\varphi(\boldsymbol{\varepsilon}_2) &= a_{21}\boldsymbol{\eta}_1 + a_{22}\boldsymbol{\eta}_2 + \dots + a_{2n}\boldsymbol{\eta}_n, \\
&\vdots \\
\varphi(\boldsymbol{\varepsilon}_m) &= a_{m1}\boldsymbol{\eta}_1 + a_{m2}\boldsymbol{\eta}_2 + \dots + a_{mn}\boldsymbol{\eta}_n.
\end{aligned} \tag{2.1}$$

Maticu $\mathbf{A} = (a_{ij})$ $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$ nazývame *maticou lineárneho zobrazenia* $\varphi : \boldsymbol{V} \to \boldsymbol{W}$ *vzhľadom na bázy* M a N.

Poznámka 2.1. Rovnice (2.1) možno pomocou sumy zapísať takto:

$$\varphi(\boldsymbol{\varepsilon}_i) = \sum_{j=1}^{n} a_{ij}\boldsymbol{\eta}_j, \quad i = 1, 2, \dots, m \tag{2.2}$$

a maticovo takto:

$$\begin{pmatrix} \varphi(\boldsymbol{\varepsilon}_1) \\ \varphi(\boldsymbol{\varepsilon}_2) \\ \vdots \\ \varphi(\boldsymbol{\varepsilon}_m) \end{pmatrix} = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \vdots & & & \\ a_{m1}, & a_{m2}, & \dots, & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{\eta}_1 \\ \boldsymbol{\eta}_2 \\ \vdots \\ \boldsymbol{\eta}_n \end{pmatrix} \tag{2.3}$$

Vidieť, že riadky matice $\mathbf{A}$ sú súradnice vektorov (v báze N), do ktorých sa zobrazujú vektory bázy M.

Poznámka 2.2. Z vety 1.2 vyplýva, že zobrazenie φ je rovnicami (2.1) resp. rovnicou (2.3) a teda aj maticou $\mathbf{A}$ jednoznačne určené. Každá matica typu $m \times n$ nad poľom F určuje (nejaké) lineárne zobrazenie priestoru $\boldsymbol{V}$ do $\boldsymbol{W}$ pri daných bázach M a N. Naopak ku každému lineárnemu zobrazeniu $\varphi : \boldsymbol{V} \to \boldsymbol{W}$ prislúcha matica typu $m \times n$ nad F. Čitateľ nech si rozmyslí, že dvom rôznym zobrazeniam prislúchajú dve rôzne matice a naopak dvom rôznym maticiam dve rôzne zobrazenia. Iným slovami: existuje bijekcia medzi množinou všetkých matíc typu $m \times n$ nad poľom F a množinou všetkých zobrazení priestoru $\boldsymbol{V}(F)$ do $\boldsymbol{W}(F)$ pri daných bázach M a N.

Veta 2.1. *Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ je lineárne zobrazenie, pre ktoré platí* (2.1)*. Nech $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_m\boldsymbol{\varepsilon}_m$ je ľubovoľný vektor priestoru $\boldsymbol{V}$, $\boldsymbol{\beta} = y_1\boldsymbol{\eta}_1 + y_2\boldsymbol{\eta}_2 + \cdots + y_n\boldsymbol{\eta}_n$ je taký vektor priestoru $\boldsymbol{W}$, pre ktorý platí $\boldsymbol{\beta} = \varphi(\boldsymbol{\alpha})$. Potom*

$$(y_1, y_2, \dots, y_n) = (x_1, x_2, \dots, x_m) \cdot \mathbf{A}. \tag{2.4}$$

Dôkaz. Počítajme

$$\begin{aligned}
y_1\boldsymbol{\eta}_1 + y_2\boldsymbol{\eta}_2 + \cdots + y_n\boldsymbol{\eta}_n &= \boldsymbol{\beta} = \varphi(\boldsymbol{\alpha}) = \varphi(x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_m\boldsymbol{\varepsilon}_m) = \\
&= x_1\varphi(\boldsymbol{\varepsilon}_1) + x_2\varphi(\boldsymbol{\varepsilon}_2) + \cdots + x_m\varphi(\boldsymbol{\varepsilon}_m) = \\
&= x_1 \sum_{j=1}^{n} a_{1j}\boldsymbol{\eta}_j + x_2 \sum_{j=1}^{n} a_{2j}\boldsymbol{\eta}_j + \cdots + x_m \sum_{j=1}^{n} a_{mj}\boldsymbol{\eta}_j = \\
&= \sum_{i=1}^{m} x_i \sum_{j=1}^{n} a_{ij}\boldsymbol{\eta}_j = \sum_{i=1}^{m}\sum_{j=1}^{n} x_i a_{ij}\boldsymbol{\eta}_j = \sum_{j=1}^{n}\sum_{i=1}^{m} x_i a_{ij}\boldsymbol{\eta}_j = \\
&= \boldsymbol{\eta}_1 \sum_{i=1}^{m} x_i a_{i1} + \boldsymbol{\eta}_2 \sum_{i=1}^{m} x_i a_{i2} + \cdots + \boldsymbol{\eta}_n \sum_{i=1}^{m} x_i a_{in}.
\end{aligned}$$

Porovnaním vidíme, že

$$\begin{aligned}
y_1 &= \sum_{i=1}^{m} x_i a_{i1} = x_1 a_{11} + x_2 a_{21} + \cdots + x_m a_{m1}, \\
y_2 &= \sum_{i=1}^{m} x_i a_{i2} = x_1 a_{12} + x_2 a_{22} + \cdots + x_m a_{m2}, \\
&\vdots \\
y_n &= \sum_{i=1}^{m} x_i a_{in} = x_1 a_{1n} + x_2 a_{2n} + \cdots + x_m a_{mn}.
\end{aligned}$$

Posledné rovnosti možno „maticovo“ zapísať v tvare

$$(y_1, y_2, \dots, y_n) = (x_1, x_2, \dots, x_m) \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \vdots & & & \\ a_{m1}, & a_{m2}, & \dots, & a_{mn} \end{pmatrix},$$

čo je (2.4). $\square$

Poznámka 2.3. Ak porovnáme (2.3) a (2.4), vidíme, že vektory bázy M sa zobrazujú pomocou riadkov matice $\mathbf{A}$, zatiaľ čo súradnice ľubovoľného vektora pomocou stĺpcov matice $\mathbf{A}$.

Príklad 2.1. Uvažujme o lineárnom zobrazení $\varphi : \boldsymbol{M}_2(Q) \to \boldsymbol{V}_3(Q)$ z príkladu 1.2. Rýchlo sa presvedčíme, že $d(\boldsymbol{M}_2(Q)) = 4$. V $\boldsymbol{M}_2(Q)$ zvolíme bázu $M = \{\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3, \mathbf{E}_4\}$ napr. takto:

$$\mathbf{E}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \mathbf{E}_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad \mathbf{E}_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{E}_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Bázu $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \boldsymbol{\eta}_3\}$ v priestore $\boldsymbol{V}_3(Q)$ zvolíme napr. takto:

$$\boldsymbol{\eta}_1 = (1,1,0), \quad \boldsymbol{\eta}_2 = (1,0,1), \quad \boldsymbol{\eta}_3 = (0,1,1).$$

Čitateľ sa môže presvedčiť, že M, N sú skutočne bázy. Podľa ((1.1)) v príklade 1.2 je $\varphi(\mathbf{E}_1) = (1,0,0)$, $\varphi(\mathbf{E}_2) = (1,1,0)$, $\varphi(\mathbf{E}_3) = (1,1,0)$, $\varphi(\mathbf{E}_4) = (1,1,0)$. Vypočítame, že

$$\begin{aligned}
\varphi(\mathbf{E}_1) &= \frac{1}{2} \cdot \boldsymbol{\eta}_1 + \frac{1}{2} \cdot \boldsymbol{\eta}_2 - \frac{1}{2} \cdot \boldsymbol{\eta}_3, \\
\varphi(\mathbf{E}_2) &= 1 \cdot \boldsymbol{\eta}_1 + 0 \cdot \boldsymbol{\eta}_2 + 0 \cdot \boldsymbol{\eta}_3, \\
\varphi(\mathbf{E}_3) &= 1 \cdot \boldsymbol{\eta}_1 + 0 \cdot \boldsymbol{\eta}_2 + 0 \cdot \boldsymbol{\eta}_3, \\
\varphi(\mathbf{E}_4) &= 1 \cdot \boldsymbol{\eta}_1 + 0 \cdot \boldsymbol{\eta}_2 + 0 \cdot \boldsymbol{\eta}_3.
\end{aligned}$$

Teda

$$\begin{pmatrix} \varphi(\mathbf{E}_1) \\ \varphi(\mathbf{E}_2) \\ \varphi(\mathbf{E}_3) \\ \varphi(\mathbf{E}_4) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{\eta}_1 \\ \boldsymbol{\eta}_2 \\ \boldsymbol{\eta}_3 \end{pmatrix}.$$

Tým sme určili maticu $\mathbf{A}$ zobrazenia φ. Vezmeme si napr. maticu

$$\mathbf{A} = \begin{pmatrix} -1 & \frac{2}{3} \\ 1 & \frac{3}{5} \end{pmatrix}$$

z vektorového priestoru $\boldsymbol{M}_2(Q)$ a určme $\varphi(\mathbf{A})$. Vypočítame, že

$$\mathbf{A} = -\frac{5}{3}\mathbf{E}_1 - \frac{1}{3}\mathbf{E}_2 + \frac{2}{5}\mathbf{E}_3 + \frac{3}{5}\mathbf{E}_4.$$

Pomocou (2.3) zistíme súradnice $\varphi(\mathbf{A})$ v báze N

$$(y_1, y_2, y_3) = \left(-\frac{5}{3}, -\frac{1}{3}, \frac{2}{5}, \frac{3}{5}\right) \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \left(-\frac{1}{6}, -\frac{5}{6}, \frac{5}{6}\right).$$

Ide teda o vektor $\varphi(\mathbf{A}) = -\frac{1}{6}\boldsymbol{\eta}_1 - \frac{5}{6}\boldsymbol{\eta}_2 + \frac{5}{6}\boldsymbol{\eta}_3 = -\frac{1}{6}(1,1,0) - \frac{5}{6}(1,0,1) + \frac{5}{6}(0,1,1) =$ $= (-1, \frac{2}{3}, 0)$. Tak to vychádza aj priamo: použitím (1.1) v príklade 1.2.

Veta 2.2. *Nech* $\varphi_1 : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ *a* $\varphi_2 : \boldsymbol{W}(F) \to \boldsymbol{U}(F)$ *sú lineárne zobrazenia. Potom aj zložené zobrazenie* $\varphi_2 \circ \varphi_1 : \boldsymbol{V}(F) \to \boldsymbol{U}(F)$ *je lineárne zobrazenie.*

Dôkaz. Nech $\boldsymbol{\alpha}, \boldsymbol{\beta}$ sú ľubovoľné vektory z vektorového priestoru $\boldsymbol{V}(F)$. Počítame $\varphi_2 \circ \varphi_1(\boldsymbol{\alpha} + \boldsymbol{\beta}) = \varphi_2[\varphi_1(\boldsymbol{\alpha} + \boldsymbol{\beta})] = \varphi_2[\varphi_1(\boldsymbol{\alpha}) + \varphi_1(\boldsymbol{\beta})] = \varphi_2[\varphi_1(\boldsymbol{\alpha})] + \varphi_2[\varphi_1(\boldsymbol{\beta})] = = \varphi_2 \circ \varphi_1(\boldsymbol{\alpha}) + \varphi_2 \circ \varphi_1(\boldsymbol{\beta})$. Vidíme, že prvá vlastnosť lineárneho zobrazenia je pre zobrazenie $\varphi_2 \circ \varphi_1$ splnená. Analogicky sa dokáže druhá vlastnosť. □

V nasledujúcej vete ukážeme, že „matica zloženého lineárneho zobrazenia je súčin matíc jednotlivých lineárnych zobrazení". Vlastne potreba vypočítať maticu zloženého zobrazenia pomocou matíc jednotlivých zložiek je jeden z dôvodov pre zavedenie súčinu matíc.

Veta 2.3. *Nech* $\varphi_1 : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ *a* $\varphi_2 : \boldsymbol{W}(F) \to \boldsymbol{U}(F)$ *sú lineárne zobrazenia. Nech dimenzie vektorových priestorov* $\boldsymbol{V}(F)$, $\boldsymbol{W}(F)$, $\boldsymbol{U}(F)$ *sú* m, n, p *a matice zobrazení* φ_1 *a* φ_2 *sú* $\mathbf{A}$ *(typu* $m \times n$*) a* $\mathbf{B}$ *(typu* $n \times p$*). Potom matica zloženého zobrazenia* $\varphi_2 \circ \varphi_1$ *je* $\mathbf{A} \cdot \mathbf{B}$ *(typu* $m \times p$*).*

Dôkaz. Nech bázy vektorových priestorov sú (po rade) $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_m\}$, $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \dots, \boldsymbol{\eta}_n\}$, $P = \{\boldsymbol{\vartheta}_1, \boldsymbol{\vartheta}_2, \dots, \boldsymbol{\vartheta}_p\}$ a matice

$$\mathbf{A} = (a_{ij}) \ i = 1, 2, \dots, m; \ j = 1, 2, \dots, n,$$
$$\mathbf{B} = (b_{jk}) \ j = 1, 2, \dots, n; \ k = 1, 2, \dots, p.$$

Podľa (2.2) máme pre φ_1:

$$\varphi_1(\boldsymbol{\varepsilon}_i) = \sum_{j=1}^{n} a_{ij} \boldsymbol{\eta}_j, \ i = 1, 2, \dots, m,$$

pre φ_2:

$$\varphi_2(\boldsymbol{\eta}_j) = \sum_{k=1}^{p} b_{jk} \boldsymbol{\vartheta}_k, \ j = 1, 2, \dots, n.$$

Počítajme

$$(\varphi_2 \circ \varphi_1)(\boldsymbol{\varepsilon}_i) = \varphi_2[\varphi_1(\boldsymbol{\varepsilon}_i)] = \varphi_2[\sum_{j=1}^{n} a_{ij} \boldsymbol{\eta}_j] = \sum_{j=1}^{n} a_{ij} \varphi_2(\boldsymbol{\eta}_j) =$$
$$= \sum_{j=1}^{n} a_{ij} \sum_{k=1}^{p} b_{jk} \boldsymbol{\vartheta}_k = \sum_{k=1}^{p} (\sum_{j=1}^{n} a_{ij} b_{jk}) \boldsymbol{\vartheta}_k = \sum_{k=1}^{p} c_{ik} \boldsymbol{\vartheta}_k,$$

kde sme dosadili $c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$. Vypočítali sme

$$(\varphi_2 \circ \varphi_1)(\boldsymbol{\varepsilon}_i) = \sum_{k=1}^{p} c_{ik} \boldsymbol{\vartheta}_k, \ i = 1, 2, \dots, n,$$

čo je vlastne vzťah (2.2) pre zobrazenie $\varphi_2 \circ \varphi_1 : \boldsymbol{V}(F) \to \boldsymbol{U}(F)$. Súčasne sme zistili, že matica

$$\mathbf{C} = (c_{ik}), \ i = 1, 2, \dots, m, \ k = 1, 2, \dots, p$$

je maticou tohto zobrazenia. Keď si čitateľ uvedomí definíciu súčinu matíc (pozri (1.6) v kapitole 3) vidí, že $\mathbf{C} = \mathbf{A} \cdot \mathbf{B}$, čo sme mali dokázať. □

Poznámka 2.4. Všimnime si, že v súčine $\mathbf{C} = \mathbf{A} \cdot \mathbf{B}$ vystupuje ako ľavý činiteľ matica zobrazenia φ_1, ktoré pri realizácii zloženého zobrazenia $\varphi_2 \circ \varphi_1$ pôsobí na vektor ako prvé. Ak by sme miesto zápisu $(\varphi_2 \circ \varphi_1)(\boldsymbol{\alpha})$ používali $\boldsymbol{\alpha}(\varphi_1 \circ \varphi_2)$ (čo sa často robí), bolo by poradie v súčine matíc v zhode s poradím pri kompozícii zobrazení.

V nasledujúcej vete ukážeme, ako sa zmení matica zobrazenia, ak sa zmenia bázy oboch priestorov.

Veta 2.4. *Nech $\mathbf{A}$ je matica lineárneho zobrazenia $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ vzhľadom na bázy $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_m\}$ a $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \dots, \boldsymbol{\eta}_n\}$. Nech $\mathbf{P}$ je matica prechodu od bázy M k báze $M' = \{\boldsymbol{\varepsilon}'_1, \boldsymbol{\varepsilon}'_2, \dots, \boldsymbol{\varepsilon}'_m\}$ a $\mathbf{Q}$ matica prechodu od bázy N k báze $N' = \{\boldsymbol{\eta}'_1, \boldsymbol{\eta}'_2, \dots, \boldsymbol{\eta}'_n\}$. Potom matica zobrazenia φ vzhľadom na bázy M' a N' je $\mathbf{P} \cdot \mathbf{A} \cdot \mathbf{Q}^{-1}$.*

Dôkaz. Podľa (2.10) kapitoly 4 vektory bázy M' vyjadríme pomocou vektorov bázy M takto:

$$\begin{pmatrix} \boldsymbol{\varepsilon}'_1 \\ \boldsymbol{\varepsilon}'_2 \\ \vdots \\ \boldsymbol{\varepsilon}'_m \end{pmatrix} = \mathbf{P} \cdot \begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_m \end{pmatrix}$$

alebo ak $\mathbf{P} = (p_{ri})$ $r, i = 1, 2, \dots, m$ takto:

$$\boldsymbol{\varepsilon}'_r = \sum_{i=1}^{m} p_{ri} \boldsymbol{\varepsilon}_i, \ r = 1, 2, \dots, m. \tag{2.5}$$

Podobne vektory bázy N' vyjadríme pomocou bázy N takto:

$$\begin{pmatrix} \boldsymbol{\eta}'_1 \\ \boldsymbol{\eta}'_2 \\ \vdots \\ \boldsymbol{\eta}'_n \end{pmatrix} = \mathbf{Q} \cdot \begin{pmatrix} \boldsymbol{\eta}_1 \\ \boldsymbol{\eta}_2 \\ \vdots \\ \boldsymbol{\eta}_n \end{pmatrix}$$

Keďže podľa vety 2.7 kapitoly 4 je matica $\mathbf{Q}$ regulárna, môžeme danú rovnosť vynásobiť zľava maticou $\mathbf{Q}^{-1}$. Dostaneme tak vyjadrenie bázy N pomocou bázy N':

$$\begin{pmatrix} \boldsymbol{\eta}_1 \\ \boldsymbol{\eta}_2 \\ \vdots \\ \boldsymbol{\eta}_n \end{pmatrix} = \mathbf{Q}^{-1} \cdot \begin{pmatrix} \boldsymbol{\eta}'_1 \\ \boldsymbol{\eta}'_2 \\ \vdots \\ \boldsymbol{\eta}'_n \end{pmatrix},$$

alebo ak $\mathbf{Q}^{-1} = (q^*_{js})$ $j, s = 1, 2, \dots, n$ takto:

$$\boldsymbol{\eta}_j = \sum_{s=1}^{n} q^*_{js} \boldsymbol{\eta}'_s, \ j = 1, 2, \dots, n. \tag{2.6}$$

Podľa (2.2) je

$$\varphi(\boldsymbol{\varepsilon}_i) = \sum_{j=1}^{n} a_{ij}\boldsymbol{\eta}_j, \ i = 1, 2, \ldots, m. \tag{2.7}$$

Počítame

$$\varphi(\boldsymbol{\varepsilon}'_r) = \varphi(\sum_{i=1}^{m} p_{ri}\boldsymbol{\varepsilon}_i) = \sum_{i=1}^{m} p_{ri}\varphi(\boldsymbol{\varepsilon}_i) = \sum_{i=1}^{m} p_{ri} \sum_{j=1}^{n} a_{ij}\boldsymbol{\eta}_j =$$
$$= \sum_{i=1}^{m}\sum_{j=1}^{n} p_{ri}a_{ij}\boldsymbol{\eta}_j = \sum_{j=1}^{n}\sum_{i=1}^{m} p_{ri}a_{ij}\boldsymbol{\eta}_j = \sum_{j=1}^{n}\sum_{i=1}^{m} p_{ri}a_{ij}\sum_{s=1}^{n} q^*_{js}\boldsymbol{\eta}'_s =$$
$$= \sum_{s=1}^{n}\left[\sum_{j=1}^{n}\left(\sum_{i=1}^{m} p_{ri}a_{ij}\right) q^*_{js}\right]\boldsymbol{\eta}'_s = \sum_{s=1}^{n} d_{rs}\boldsymbol{\eta}'_s,$$

kde sme pri výpočte dosadili postupne (2.5), (2.7) a (2.6). Keďže výraz v hranatej zátvorke $d_{rs} = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} p_{ri}a_{ij}\right) q^*_{js}$ je prvok matice $\mathbf{D} = \mathbf{P}\cdot\mathbf{A}\cdot\mathbf{Q}^{-1}$, vidíme, že matica $\mathbf{D} = (d_{rs})$, $r = 1, 2, \ldots, n$, $s = 1, 2, \ldots, n$ je maticou zobrazenia φ vzhľadom na bázy M' a N'. □

Príklad 2.2. V priestore $\boldsymbol{V}_3(Q)$ je daná báza $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_3\}$ a v priestore $\boldsymbol{V}_4(Q)$ báza $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \boldsymbol{\eta}_3, \boldsymbol{\eta}_4\}$, kde $\boldsymbol{\varepsilon}_1 = (1, -1, 2)$, $\boldsymbol{\varepsilon}_2 = (2, -1, 5)$, $\boldsymbol{\varepsilon}_3 = (3, -3, 4)$, $\boldsymbol{\eta}_1 = (1, 1, 1, 1)$, $\boldsymbol{\eta}_2 = (1, 1, 1, 0)$, $\boldsymbol{\eta}_3 = (1, 1, 0, 0)$, $\boldsymbol{\eta}_4 = (1, 0, 0, 0)$. Lineárne zobrazenie $\varphi : \boldsymbol{V}_3(Q) \to \boldsymbol{V}_4(Q)$ je dané takto:

$$\varphi(\boldsymbol{\varepsilon}_1) = (3, 2, -1, 0),$$
$$\varphi(\boldsymbol{\varepsilon}_2) = (1, -4, 5, 7),$$
$$\varphi(\boldsymbol{\varepsilon}_3) = (4, -2, 4, 7).$$

Nájdeme maticu $\mathbf{A}$ zobrazenia φ vzhľadom na bázy M a N a potom maticu $\mathbf{P}\cdot\mathbf{A}\cdot\mathbf{Q}^{-1}$ vzhľadom na kanonické bázy týchto priestorov (pozri poznámku 4.1 v kapitole 2). Ľahko zistíme (zostavením a vyriešením 3 sústav rovníc), že platí:

$$\varphi(\boldsymbol{\varepsilon}_1) = 0\cdot\boldsymbol{\eta}_1 + (-1)\cdot\boldsymbol{\eta}_2 + 3\cdot\boldsymbol{\eta}_3 + 1\cdot\boldsymbol{\eta}_4$$
$$\varphi(\boldsymbol{\varepsilon}_2) = 7\cdot\boldsymbol{\eta}_1 + (-2)\cdot\boldsymbol{\eta}_2 + (-9)\cdot\boldsymbol{\eta}_3 + 5\cdot\boldsymbol{\eta}_4$$
$$\varphi(\boldsymbol{\varepsilon}_3) = 7\cdot\boldsymbol{\eta}_1 + (-3)\cdot\boldsymbol{\eta}_2 + (-6)\cdot\boldsymbol{\eta}_3 + 6\cdot\boldsymbol{\eta}_4$$

Vidíme, že

$$\mathbf{A} = \begin{pmatrix} 0 & -1 & 3 & 1 \\ 7 & -2 & -9 & 5 \\ 7 & -3 & -6 & 6 \end{pmatrix}.$$

Kanonickú bázu priestoru $\boldsymbol{V}_3(Q)$ označíme $M' = \{\boldsymbol{\varepsilon}'_1, \boldsymbol{\varepsilon}'_2, \boldsymbol{\varepsilon}'_3\}$, kanonickú bázu priestoru $\boldsymbol{V}_4(Q)$ označíme $N' = \{\boldsymbol{\eta}'_1, \boldsymbol{\eta}'_2, \boldsymbol{\eta}'_3, \boldsymbol{\eta}'_4\}$.

Vypočítame

$$(1, 0, 0) = \boldsymbol{\varepsilon}'_1 = -\frac{11}{2}\boldsymbol{\varepsilon}_1 + 1\cdot\boldsymbol{\varepsilon}_2 + \frac{3}{2}\boldsymbol{\varepsilon}_3,$$
$$(0, 1, 0) = \boldsymbol{\varepsilon}'_2 = -\frac{7}{2}\boldsymbol{\varepsilon}_1 + 1\cdot\boldsymbol{\varepsilon}_2 + \frac{1}{2}\boldsymbol{\varepsilon}_3,$$
$$(0, 0, 1) = \boldsymbol{\varepsilon}'_3 = \frac{3}{2}\boldsymbol{\varepsilon}_1 + 0\cdot\boldsymbol{\varepsilon}_2 + (-\frac{1}{2})\boldsymbol{\varepsilon}_3,$$

čiže matica prechodu od bázy M, k báze M' je

$$\mathbf{P} = \begin{pmatrix} -\frac{11}{2} & 1 & \frac{3}{2} \\ -\frac{7}{2} & 1 & \frac{1}{2} \\ \frac{3}{2} & 0 & -\frac{1}{2} \end{pmatrix}.$$

Matica prechodu $\mathbf{Q}^{-1}$ od bázy N' k báze N by sme mohli vypočítať ako maticu inverznú k matici $\mathbf{Q}$ (prechodu od N k N').
Oveľa jednoduchšie však bude vypočítať maticu $\mathbf{Q}^{-1}$ priamo. Čitateľ si skontroluje, že

$$\mathbf{Q}^{-1} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Podľa vety 2.4 matica zobrazenia φ vzhľadom na (kanonické) bázy M' a N'' je

$$\mathbf{P} \cdot \mathbf{A} \cdot \mathbf{Q}^{-1} = \begin{pmatrix} -\frac{11}{2}, & 1 & \frac{3}{3} \\ -\frac{7}{2} & 1 & \frac{1}{2} \\ \frac{3}{2} & 0 & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 & 3 & 1 \\ 7 & -2 & -9 & 5 \\ 7 & -3 & -6 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} \frac{35}{2} & -1 & -\frac{69}{2} & \frac{17}{2} \\ \frac{21}{2} & 0 & -\frac{45}{2} & \frac{9}{2} \\ -\frac{7}{2} & 0 & \frac{15}{2} & -\frac{3}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -\frac{19}{2} & -18 & \frac{33}{2} & \frac{35}{2} \\ -\frac{15}{2} & -12 & \frac{21}{2} & \frac{21}{2} \\ \frac{5}{2} & 4 & -\frac{7}{2} & -\frac{7}{2} \end{pmatrix}.$$

Aby sme demonštrovali zobrazenia vektora pomocou matíc $\mathbf{A}$ resp. $\mathbf{PAQ}^{-1}$ zoberme hoci vektor $\boldsymbol{\alpha} = (5, -1, 18) \in \boldsymbol{V}_3(R)$. Čitateľ ľahko skontroluje, že $\boldsymbol{\alpha} = 3\boldsymbol{\varepsilon}_1 + 4\boldsymbol{\varepsilon}_2 - 2\boldsymbol{\varepsilon}_3$, čiže vektor súradníc vektora $\boldsymbol{\alpha}$ v báze M je $(3, 4, -2)$. Pomocou (2.3) zistíme súradnice vektora $\varphi(\boldsymbol{\alpha})$ v báze N:

$$(y_1, y_2, y_3, y_4) = (3, 4, -2) \begin{pmatrix} 0 & -1 & 3 & 1 \\ 7 & -2 & -9 & 5 \\ 7 & -3 & -6 & 6 \end{pmatrix} = (14, -5, -15, 11).$$

Teda $\varphi(\boldsymbol{\alpha}) = y_1\boldsymbol{\eta}_1 + y_2\boldsymbol{\eta}_2 + y_3\boldsymbol{\eta}_3 + y_4\boldsymbol{\eta}_4 =$
$= 14(1, 1, 1, 1) - 5(1, 1, 1, 0) - 15(1, 1, 0, 0) + 11(1, 0, 0, 0) = (5, -6, 9, 14).$
Kvôli kontrole vypočítajme $\varphi(\boldsymbol{\alpha})$ priamo:
$\varphi(\boldsymbol{\alpha}) = \varphi(3\boldsymbol{\varepsilon}_1 + 4\boldsymbol{\varepsilon}_2 - 2\boldsymbol{\varepsilon}_3) = 3\varphi(\boldsymbol{\varepsilon}_1) + 4\varphi(\boldsymbol{\varepsilon}_2) - 2\varphi(\boldsymbol{\varepsilon}_3) =$
$= 3(3, 2, -1, 0) + 4(1, -4, 5, 7) - 2(4, -2, 4, 7) = (5, -6, 9, 14).$
Je jasné, že vektor $\boldsymbol{\alpha}$ má v báze M' vektor súradníc $(5, -1, 18)$, a vektor $\varphi(\boldsymbol{\alpha})$ v báze N' vektor súradníc $(5, -6, 9, 14)$. Preto musí platiť

$$(5, -6, 9, 14) = (5, -1, 18) \cdot \mathbf{P} \cdot \mathbf{A} \cdot \mathbf{Q}^{-1}.$$

Čitateľ sa môže tom presvedčiť.

Vyslovili sme už dve vety (veta 1.4 a 1.5) o tom, kedy je lineárne zobrazenie injektívne, surjektívne či bijektívne. Vyslovíme ešte jednu takúto vetu.

Veta 2.5. *Nech* $\mathbf{A}$ *je matica zobrazenia* $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$, *vzhľadom na bázy* M *a* N, *pričom dimenzie priestorov* $\boldsymbol{V}$ *i* $\boldsymbol{W}$ *sú konečné. Potom platí*

(i) φ *je injektívne (monomorfizmus) práve vtedy, keď* $h(\mathbf{A}) = d(\boldsymbol{V})$,
(ii) φ *je surjektívne (epimorfizmus) práve vtedy, keď* $h(\mathbf{A}) = d(\boldsymbol{W})$,
(iii) φ *je bijektívne (izomorfizmus) práve vtedy, keď* $h(\mathbf{A}) = d(\boldsymbol{V}) = d(\boldsymbol{W})$.

Dôkaz bezprostredne vyplýva z vety 1.5 a definície matice $\mathbf{A}$ z poznámky 1.3 za dôsledkom vety 1.6. Preto ho ponecháme na čitateľa. $\square$

Pripomíname, že relácia inverzná k zobrazeniu je zobrazením práve vtedy, keď dané zobrazenie je bijekcia. Čitateľa už iste napadla otázka, či inverzné zobrazenie k bijektívnemu lineárnemu zobrazeniu bude tiež lineárne. Nasledujúca veta odpovedá na túto otázku kladne.

Veta 2.6. *Nech* $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ *je bijektívne lineárne zobrazenie. Potom aj* $\varphi^{-1} : \boldsymbol{W}(F) \to \boldsymbol{V}(F)$ *je (bijektívne) lineárne zobrazenie.*

Dôkaz. Že zobrazenie φ^{-1} je bijekcia je jasné. Dokážeme, že je lineárne. Nech $\boldsymbol{\alpha}', \boldsymbol{\beta}' \in \boldsymbol{W}$ sú dva ľubovoľné vektory. Nech $\varphi^{-1}(\boldsymbol{\alpha}') = \boldsymbol{\alpha}$, $\varphi^{-1}(\boldsymbol{\beta}') = \boldsymbol{\beta}$. Potom $\varphi(\boldsymbol{\alpha}) = \boldsymbol{\alpha}'$, $\varphi(\boldsymbol{\beta}) = \boldsymbol{\beta}'$. Keďže φ lineárne je, dostaneme $\varphi(\boldsymbol{\alpha} + \boldsymbol{\beta}) = \varphi(\boldsymbol{\alpha}) + \varphi(\boldsymbol{\beta}) = \boldsymbol{\alpha}' + \boldsymbol{\beta}'$. Preto $\varphi^{-1}(\boldsymbol{\alpha}' + \boldsymbol{\beta}') = \boldsymbol{\alpha} + \boldsymbol{\beta} = \varphi^{-1}(\boldsymbol{\alpha}') + \varphi^{-1}(\boldsymbol{\beta}')$ a prvá vlastnosť lineárneho zobrazenia je dokázaná. Podobne sa dokáže i druhá vlastnosť. $\square$

Veta 2.7. *Nech izomorfné priestory* $\boldsymbol{V}(F)$ *a* $\boldsymbol{W}(F)$ *sú konečnej dimenzie a nech* $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ *je príslušné bijektívne lineárne zobrazenie. Nech* $\mathbf{A}$ *je matica zobrazenia* φ *vzhľadom na bázy* M *a* N. *Potom maticou inverzného lineárneho zobrazenia* $\varphi^{-1} : \boldsymbol{W}(F) \to \boldsymbol{V}(F)$ *(vzhľadom na bázy* N *a* M*) je* $\mathbf{A}^{-1}$.

Dôkaz. Najprv poznamenajme, že podľa vety 1.6 je $d(\boldsymbol{V}) = d(\boldsymbol{W})$. Ak položíme $d(\boldsymbol{V}) = d(\boldsymbol{W}) = n$, matica $\mathbf{A}$ je štvorcová matica typu $n \times n$. Ďalej z vety 2.5 vyplýva, že $h(\mathbf{A}) = n$, t.j. $\mathbf{A}$ je regulárna matica.

Nech $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ je báza priestoru $\boldsymbol{V}$ a $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \dots, \boldsymbol{\eta}_n\}$ je báza priestoru $\boldsymbol{W}$. Podľa (2.2) píšeme

$$\varphi(\boldsymbol{\varepsilon}_i) = \sum_{j=1}^{n} a_{ij} \boldsymbol{\eta}_j, \quad i = 1, 2, \dots, n. \tag{2.8}$$

Vektory oboch strán (2.8) zobrazíme zobrazením φ^{-1}. Dostaneme

$$\boldsymbol{\varepsilon}_i = \sum_{j=1}^{n} a_{ij} \varphi^{-1}(\boldsymbol{\eta}_j), \quad i = 1, 2, \dots, n. \tag{2.9}$$

Vzťah (2.9) zapíšeme „maticovo“:

$$\begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_n \end{pmatrix} = \mathbf{A} \cdot \begin{pmatrix} \varphi^{-1}(\boldsymbol{\eta}_1) \\ \varphi^{-1}(\boldsymbol{\eta}_2) \\ \vdots \\ \varphi^{-1}(\boldsymbol{\eta}_n) \end{pmatrix}. \tag{2.10}$$

Ak vzťah (2.10) násobíme zľava maticou $\mathbf{A}^{-1}$ dostaneme

$$\begin{pmatrix} \varphi^{-1}(\boldsymbol{\eta}_1) \\ \varphi^{-1}(\boldsymbol{\eta}_2) \\ \vdots \\ \varphi^{-1}(\boldsymbol{\eta}_n) \end{pmatrix} = \mathbf{A}^{-1} \begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_n \end{pmatrix}, \tag{2.11}$$

odkiaľ (porovnaním s (2.3)) vyplýva, že $\mathbf{A}^{-1}$ je maticou zobrazenia φ^{-1} vzhľadom na bázy N a M. □

Príklad 2.3. Nech $\boldsymbol{D}_2(Q)$ je priestor diagonálnych matíc typu 2×2 s racionálnymi prvkami. Nech $\varphi : \boldsymbol{D}_2(Q) \to \boldsymbol{V}_2(Q)$ je bijektívne lineárne zobrazenie dané maticou

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

vzhľadom na bázy $M = \{\mathbf{E}_1, \mathbf{E}_2\}$, $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2\}$, kde

$$\mathbf{E}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad \mathbf{E}_2 = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \boldsymbol{\eta}_1 = (5, 2), \quad \boldsymbol{\eta}_2 = (1, 7).$$

Potom môžeme písať (podľa (2.3)):

$$\begin{pmatrix} \varphi(\mathbf{E}_1) \\ \varphi(\mathbf{E}_2) \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} \boldsymbol{\eta}_1 \\ \boldsymbol{\eta}_2 \end{pmatrix}.$$

Vidíme, že

$$\varphi(\mathbf{E}_1) = 1 \cdot \boldsymbol{\eta}_1 + 3\boldsymbol{\eta}_2 = (5, 2) + 3(1, 7) = (8,\ 23),$$
$$\varphi(\mathbf{E}_2) = 1 \cdot \boldsymbol{\eta}_1 + 4\boldsymbol{\eta}_2 = (5, 2) + 4(1, 7) = (9,\ 30).$$

Keďže

$$\mathbf{A}^{-1} = \begin{pmatrix} 4 & -3 \\ -1 & 1 \end{pmatrix},$$

podľa (2.11) je

$$\begin{pmatrix} \varphi^{-1}(\boldsymbol{\eta}_1) \\ \varphi^{-1}(\boldsymbol{\eta}_2) \end{pmatrix} = \begin{pmatrix} 4 & -3 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix}.$$

Vypočítali sme, že $\varphi(\mathbf{E}_1) = (8, 23) = \boldsymbol{\alpha}$. Preto $\varphi^{-1}(\boldsymbol{\alpha}) = \mathbf{E}_1$. Vektor $\boldsymbol{\alpha}$ má v báze N vektor súradníc (1,3). Vypočítajme vektor súradníc (y_1, y_2) vektora $\varphi^{-1}(\boldsymbol{\alpha})$. Podľa (2.4)

$$(y_1, y_2) = (1, 3) \begin{pmatrix} 4 & -3 \\ -1 & 1 \end{pmatrix} = (1, 0),$$

teda $\varphi^{-1}(\boldsymbol{\alpha}) = 1 \cdot \mathbf{E}_1 + 0 \cdot \mathbf{E}_2 = \mathbf{E}_1$, čo je pravda. Aby sme urobili príklad viac poučným, skúsme izomorfizmus daný maticou $\mathbf{A}$ určiť všeobecne t.j. určiť, aký vektor je priradený priradený matici $\mathbf{X} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Urobíme to takto: Najprv určíme súradnice matice $\mathbf{X}$ vzhľadom na bázu M. Je

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = x \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + y \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix},$$

odkiaľ $x = \frac{a+3b}{7}$, $y = \frac{2a-b}{7}$. Vektor súradníc matice $\mathbf{X}$ je $\left(\frac{a+3b}{7}, \frac{2a-b}{7}\right)$. Vypočítame súradnice $\varphi(\mathbf{X})$ v báze N:

$$(x', y') = \left(\frac{a+3b}{7}, \frac{2a-b}{7}\right) \begin{pmatrix} 1, & 3 \\ 1, & 4 \end{pmatrix} = \left(\frac{3a+2b}{7}, \frac{11a+5b}{7}\right).$$

Preto

$$\varphi(\mathbf{X}) = \frac{3a+2b}{7}(5,2) + \frac{11a+5b}{7}(1,7) = \left(\frac{26a+15b}{7}, \frac{83a+39b}{7}\right).$$

Snaživému čitateľovi odporúčame, aby podobným spôsobom určil „všeobecný obraz“ $\varphi^{-1}(\boldsymbol{\alpha})$ ľubovoľného vektora $\boldsymbol{\alpha} = (u, v) \in \boldsymbol{V}_2(Q)$. Tiež si môže určiť matice zobrazení φ a φ^{-1} vzhľadom na kanonické bázy priestorov $\boldsymbol{V}(Q)$ a $\boldsymbol{V}_2(Q)$.

Na koniec tohoto paragrafu ukážeme, že množina všetkých lineárnych zobrazení dvoch priestorov nad poľom F je tiež vektorový priestor nad F. Za tým účelom musíme vysloviť definíciu súčtu a skalárneho násobku lineárneho zobrazenia.

Definícia 2.2. Nech φ a ψ sú dve lineárne zobrazenia vektorového priestoru $\boldsymbol{V}(F)$ do $\boldsymbol{W}(F)$. Nech ďalej zobrazenie $\omega : \boldsymbol{V} \to \boldsymbol{W}$ je definované takto:

(2.12) Pre všetky $\boldsymbol{\alpha} \in \boldsymbol{V}$ platí $\omega(\boldsymbol{\alpha}) = \varphi(\boldsymbol{\alpha}) + \psi(\boldsymbol{\alpha})$.

Potom zobrazenie ω nazývame *súčtom* zobrazení φ a ψ. Budeme ho označovať $\omega = \varphi + \psi$. Teda $(\varphi + \psi)(\boldsymbol{\alpha}) = \varphi(\boldsymbol{\alpha}) + \psi(\boldsymbol{\alpha})$. Podobne definujeme *skalárny násobok* $s\varphi$:

(2.13) $$(s\varphi)(\boldsymbol{\alpha}) = s\varphi(\boldsymbol{\alpha}),$$

kde $s \in F$ je ľubovoľný skalár a $\boldsymbol{\alpha} \in \boldsymbol{V}$ ľubovoľný vektor.

Lema 2.1. *Zobrazenia $\varphi + \psi : \boldsymbol{V} \to \boldsymbol{W}$ a $s\varphi : \boldsymbol{V} \to \boldsymbol{W}$ definované v definícii 2.2 sú lineárne zobrazenia.*

Dôkaz. Skutočne, pre dva ľubovoľné vektory $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}$ platí $(\varphi + \psi)(\boldsymbol{\alpha} + \boldsymbol{\beta}) = \varphi(\boldsymbol{\alpha}+\boldsymbol{\beta}) + \psi(\boldsymbol{\alpha}+\boldsymbol{\beta}) = \varphi(\boldsymbol{\alpha}) + \varphi(\boldsymbol{\beta}) + \psi(\boldsymbol{\alpha}) + \psi(\boldsymbol{\beta}) = (\varphi+\psi)(\boldsymbol{\alpha}) + (\varphi+\psi)(\boldsymbol{\beta})$. Prvá vlastnosť lineárneho zobrazenia je dokázaná. Podobne sa dokáže aj druhá vlastnosť prvého a obe vlastnosti druhého zobrazenia. □

Veta 2.8. *Nech $\boldsymbol{L}(F)$ je množina všetkých lineárnych zobrazení vektorového priestoru $\boldsymbol{V}(R)$ do $\boldsymbol{W}(F)$. Ak na $\boldsymbol{L}(F)$ definujme operáciu „+“ a skalárny násobok ako v definícii 2.2, tak $\boldsymbol{L}(F)$ je vektorový priestor nad F.*

Dôkaz ponecháme na čitateľa. Poznamenáme len, že neutrálnym prvkom v grupe $(\boldsymbol{L}(F), +)$ je zobrazenie $o : \boldsymbol{V} \to \boldsymbol{W}$ také, že pre každé $\boldsymbol{\alpha} \in \boldsymbol{V}$ je $o(\boldsymbol{\alpha}) = \vec{0}$. Teda $\operatorname{Ker} o = \boldsymbol{V}$, $\operatorname{Im} o = \{\vec{0}\}$. □

Veta 2.9. *Nech $\boldsymbol{L}(F)$ vektorový priestor lineárnych zobrazení priestoru $\boldsymbol{V}(F)$ dimenzie m do priestoru $\boldsymbol{W}(F)$ dimenzie n. Nech $\boldsymbol{M}_{m,n}(F)$ je vektorový priestor všetkých matíc typu $m \times n$ nad F. Potom priestory $\boldsymbol{L}(F)$ a $\boldsymbol{M}_{m,n}(F)$ sú izomorfné.*

Dôkaz. Zvoľme pevne bázu M v priestore $\boldsymbol{V}(F)$ a bázu N v priestore $\boldsymbol{W}(F)$. Potom existuje bijekcia

$$f : \boldsymbol{L}(F) \to \boldsymbol{M}_{m,n}(F),$$

ktorá priradí každému zobrazeniu $\varphi \in \boldsymbol{L}(F)$ jeho maticu $\mathbf{A}$ vzhľadom na bázy M, N (pozri poznámku 2.2).

Nech $\varphi, \psi \in \boldsymbol{L}(F)$ sú dve ľubovoľné zobrazenia. Nech $f(\varphi) = \mathbf{A}$, $f(\psi) = \mathbf{B}$. Ak $\boldsymbol{\varepsilon}_i \in M$, tak

$$\varphi(\boldsymbol{\varepsilon}_i) = \sum_{j=1}^{n} a_{ij}\boldsymbol{\eta}_j \qquad i = 1, 2, \ldots, m,$$

$$\psi(\boldsymbol{\varepsilon}_i) = \sum_{j=1}^{n} b_{ij}\boldsymbol{\eta}_j \qquad i = 1, 2, \ldots, m,$$

kde $\mathbf{A} = (a_{ij}), \mathbf{B} = (b_{ij})$ a $\boldsymbol{\eta}_j$ sú vektory bázy N, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$. Počítame:

$$(\varphi + \psi)(\boldsymbol{\varepsilon}_i) = \varphi(\boldsymbol{\varepsilon}_i) + \psi(\boldsymbol{\varepsilon}_i) = \sum_{j=1}^{n} a_{ij}\boldsymbol{\eta}_j + \sum_{j=1}^{n} b_{ij}\boldsymbol{\eta}_j = \sum_{j=1}^{n}(a_{ij} + b_{ij})\boldsymbol{\eta}_j.$$

Vidíme, že $f(\varphi + \psi) = \mathbf{A} + \mathbf{B} = f(\varphi) + f(\psi)$. Podobne sa dokáže

$$f(s\varphi) = s\mathbf{A} = sf(\varphi).$$

To znamená, že f je izomorfizmus. □

Veta 2.10. *Nech matica $\mathbf{A}$ (typu $m \times n$) je matica lineárneho zobrazenia $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$ vzhľadom na bázy M a N. Potom*

$$d(\operatorname{Im}\varphi) = h(\mathbf{A}), \tag{2.14}$$

$$d(\operatorname{Ker}\varphi) = m - h(\mathbf{A}). \tag{2.15}$$

Dôkaz. 1) Dokážeme rovnosť (2.14). Nech $\boldsymbol{\beta} \in \operatorname{Im}\varphi$ je ľubovoľný vektor. Potom existuje $\boldsymbol{\alpha} \in \boldsymbol{V}(F)$ tak, že $\varphi(\boldsymbol{\alpha}) = \boldsymbol{\beta}$. Predpokladajme ako obvykle, že $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_m\}$ ako aj $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \ldots, \boldsymbol{\eta}_n\}$. Ak vektor $\boldsymbol{\alpha}$ vyjadríme v tvare $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_m\boldsymbol{\varepsilon}_m$, hneď vidíme, že jeho obraz $\boldsymbol{\beta} = \varphi(\boldsymbol{\alpha}) = x_1\varphi(\boldsymbol{\varepsilon}_1) + x_2\varphi(\boldsymbol{\varepsilon}_2) + \cdots + x_m\varphi(\boldsymbol{\varepsilon}_m)$ je lineárnou kombináciou vektorov $\varphi(\boldsymbol{\varepsilon}_i)$. Inými slovami: podpriestor $\operatorname{Im}\varphi$ je generovaný vektormi $\varphi(\boldsymbol{\varepsilon}_i)$ (zapíšeme to $\operatorname{Im}\varphi = [\varphi(\boldsymbol{\varepsilon}_1), \varphi(\boldsymbol{\varepsilon}_2), \ldots, \varphi(\boldsymbol{\varepsilon}_m)]$). Každému z vektorov $\varphi(\boldsymbol{\varepsilon}_i)$ je priradený podľa (2.3) vektor súradníc $(a_{i1}, a_{i2}, \ldots, a_{in}) \in \boldsymbol{V}_n(F)$, ktorý je i-tym riadkom matice $\mathbf{A}$. Toto priradenie je podľa poznámky 1.3 izomorfizmom priestorov $\boldsymbol{W}(F)$ a $\boldsymbol{V}_n(F)$. Preto riadky matice $\mathbf{A}$ generujú podpriestor tej istej dimenzie ako vektory $\varphi(\boldsymbol{\varepsilon}_i)$, čiže platí (2.14).

2) Aby sme dokázali (2.15), stačí dosadiť (2.14) do (1.5). □

Dôsledok 1. *Nech matica* $\mathbf{A}$ *je maticou typu* $m \times n$*, matica* $\mathbf{B}$ *je regulárna typu* $m \times m$ *a matica* $\mathbf{C}$ *je regulárna typu* $n \times n$*. Potom*

$$h(\mathbf{A}) = h(\mathbf{BAC}).$$

Dôkaz. Maticu $\mathbf{A}$ môžeme považovať za maticu zobrazenia $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$, kde $d(\boldsymbol{V}) = m$, $d(\boldsymbol{W}) = n$ vzhľadom na bázy M a N. Ak $\mathbf{B}$ je matica prechodu od bázy M k báze M' (bázu M' zrejme môžeme tak zvoliť, lebo $\mathbf{B}$ je regulárna matica – dokážte to!) a analogicky $\mathbf{C}$ je matica prechodu od bázy N' k N (pozor, bázu N' musíme zvoliť tak, aby maticou prechodu od N k N' bola $\mathbf{C}^{-1}$) podľa vety 2.4 je $\mathbf{BAC}$ maticou zobrazenia φ vzhľadom na bázy M' a N'. Podľa (2.14) je $h(\mathbf{A}) = d(\operatorname{Im}\varphi) = h(\mathbf{BAC})$, čo sme mali dokázať. $\square$

Poznámka 2.5. Zobrazenie $\varphi : \boldsymbol{V} \to \boldsymbol{W}$ konečnorozmerných priestorov má rôzne matice podľa toho aké bázy sme zvolili v priestoroch $\boldsymbol{V}$ a $\boldsymbol{W}$. Ale podľa (2.14) všetky tieto matice majú rovnakú hodnosť rovnajúcu sa $d(\operatorname{Im}\varphi)$. Hodnosť matice zobrazenia teda nezávisí od bázy, ale len od zobrazenia φ (je invariantom zobrazenia φ).

Dôsledok 2. *Nech* $\mathbf{A}$ *je matica typu* $m \times n$ *nad* F*. Potom* $h(\mathbf{A}) = h(\mathbf{A}^T)$.

Dôkaz. Majme na mysli také zobrazenie $\varphi : \boldsymbol{V}(F) \to \boldsymbol{W}(F)$, ktorého matica je $\mathbf{A}$, vzhľadom na bázy M a N, kde $d(\boldsymbol{V}) = m$, $d(\boldsymbol{W}) = n$.

Zvoľme ľubovoľný vektor $\boldsymbol{\alpha} \in \operatorname{Ker}\varphi$. Nech vektor súradníc vektora $\boldsymbol{\alpha}$ je $(x_1, x_2, \ldots, x_m) \in \boldsymbol{V}_m(F)$, potom zrejme vektor súradníc vektora $\varphi(\boldsymbol{\alpha})$ je $(0, 0, \ldots, 0) \in \boldsymbol{V}_n(F)$. Podľa (2.4) je

$$(0, 0, \ldots, 0) = (x_1, x_2, \ldots, x_m)\mathbf{A}$$

alebo, čo je to isté

$$\mathbf{A}^T \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{2.16}$$

Posledná rovnica reprezentuje sústavu homogénnych lineárnych rovníc s maticou sústavy $\mathbf{A}^T$. Vo vete 6.3 kapitoly 3 sme dokázali, že podpriestor riešení $\boldsymbol{S}$ sústavy (2.16) má dimenziu $d(\boldsymbol{S}) = m - h(\mathbf{A}^T)$. Je jasné, že $d(\boldsymbol{S}) = d(\operatorname{Ker}\varphi)$. Vyplýva to z izomorfizmu medzi $\boldsymbol{W}(F)$ a $\boldsymbol{V}_n(F)$ a z toho, že riešenia sústavy (2.16) sú práve tie n-tice z $\boldsymbol{V}_n(F)$, ktoré sú súradnicami vektorov z $\operatorname{Ker}\varphi$. Máme tak $d(\operatorname{Ker}\varphi) = m - h(\mathbf{A}^T)$. Porovnaním so (2.15) dostávame $h(\mathbf{A}) = h(\mathbf{A}^T)$. $\square$

Poznámka 2.6. Izomorfizmus vo vete 2.9 znamená, že z algebraického hľadiska je jedno, či skúmame vektorový priestor zobrazení dvoch konečnorozmerných priestorov, alebo príslušný vektorový priestor matíc. Umožňuje nám to z vlastností zobrazení usudzovať na vlastnosti matíc a naopak. Príkladom takéhoto usudzovania boli predchádzajúce dva dôsledky vety 2.10, v ktorých sme tvrdenia o maticiach dokazovali pomocou lineárnych zobrazení. Dôsledok 2 sme, pravda, dokázali už predtým (pozri lemu 3.2 kapitoly 3).

Poznámka 2.7. Podľa dôsledku vety 1.6 všetky priestory nad tým istým poľom F rovnakej dimenzie sú izomorfné priestoru $\boldsymbol{V}_n(F)$. Preto sa môžeme obmedziť na vyšetrovanie vektorových priestorov $\boldsymbol{V}_n(F)$. Aj maticu $\mathbf{A}$ lineárneho zobrazenia $\varphi : \boldsymbol{V}_m(F) \to \boldsymbol{V}_n(F)$ možno definovať jednoznačne ak za bázy M a N zvolíme kanonické bázy (pozri poznámku za príkladom 4.1). Keďže v kanonickej báze sa súradnice vektorov rovnajú ich zložkám, riadky matice $\mathbf{A}$ sú priamo vektory priestoru $\boldsymbol{V}_n$, do ktorých sa zobrazujú „jednotkové" vektory kanonickej bázy priestoru $\boldsymbol{V}_m$. Napr. ak uvažujeme zobrazenie $\varphi : \boldsymbol{V}_2(Q) \to \boldsymbol{V}_3(Q)$ také, že $(1,0) \mapsto (2,3,-1)$, $(0,1) \mapsto (1,0,4)$, matica zobrazenia φ vzhľadom na kanonické bázy je

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

Cvičenia

2.1. Nech $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_m\}$ je báza priestoru $\boldsymbol{V}(R)$ a $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \dots, \boldsymbol{\eta}_n\}$ je báza priestoru $\boldsymbol{W}(R)$. Nájdite maticu $\mathbf{A}$ lineárneho zobrazenia $\varphi : \boldsymbol{V} \to \boldsymbol{W}$ vzhľadom na bázy M a N a obraz $\varphi(\boldsymbol{\alpha})$, ak je dané:

a) $\boldsymbol{V}(R) = \boldsymbol{V}_2(R)$, $\boldsymbol{W}(R) = \boldsymbol{V}_3(R)$ $m = 2$, $n = 3$, $\boldsymbol{\varepsilon}_1 = (1,0)$, $\boldsymbol{\varepsilon}_2 = (0,1)$, $\boldsymbol{\eta}_1 = (1,0,0)$, $\boldsymbol{\eta}_2 = (0,1,0)$, $\boldsymbol{\eta}_3 = (0,0,1)$,

$$\varphi(\boldsymbol{\varepsilon}_1) = (1,-3,8),$$
$$\varphi(\boldsymbol{\varepsilon}_2) = (3,-1,5)$$

a $\boldsymbol{\alpha} = (r,s)$, kde $r,s \in R$.

b) $\boldsymbol{V}(R) = \boldsymbol{V}_2(R)$, $\boldsymbol{V}(R) = \boldsymbol{V}_3(R)$, $m = 2, n = 3$, $\boldsymbol{\varepsilon}_1 = (2,-3)$, $\boldsymbol{\varepsilon}_2 = (4,1)$, $\boldsymbol{\eta}_1 = (1,-1,3)$, $\boldsymbol{\eta}_2 = (0,3,-5)$, $\boldsymbol{\eta}_3 = (1,2,-1)$,

$$\varphi(\boldsymbol{\varepsilon}_1) = (-7,-3,1),$$
$$\varphi(\boldsymbol{\varepsilon}_2) = (7,-13,37)$$

a $\boldsymbol{\alpha} = (r,s)$, kde $r,s \in R$

c) $\boldsymbol{V}(R) = \boldsymbol{V}_2(R)$, $\boldsymbol{W}(R) = \boldsymbol{V}_2(R)$, $m = n = 2$, $\boldsymbol{\varepsilon}_1 = (1,0)$, $\boldsymbol{\varepsilon}_2 = (0,1)$, $\boldsymbol{\eta}_1 = (1,0)$, $\boldsymbol{\eta}_2 = (0,1)$,

$$\varphi(\boldsymbol{\varepsilon}_1) = (1,3),$$
$$\varphi(\boldsymbol{\varepsilon}_2) = (2,5)$$

a $\boldsymbol{\alpha} = (r,s)$, kde $r,s \in R$.

d) $\boldsymbol{V}(R) = \boldsymbol{V}_2(R)$, $\boldsymbol{W}(R) = \boldsymbol{V}_2(R)$, $m = n = 2$, $\boldsymbol{\varepsilon}_1 = (1,0)$, $\boldsymbol{\varepsilon}_2 = (0,1)$, $\boldsymbol{\eta}_1 = (1,0)$, $\boldsymbol{\eta}_2 = (0,1)$,

$$\varphi(\boldsymbol{\varepsilon}_1) = (\ 1,\ 4),$$
$$\varphi(\boldsymbol{\varepsilon}_2) = (-2,-8)$$

a $\boldsymbol{\alpha} = (r,s)$, kde $r,s \in R$.

e) $\boldsymbol{V}(R) = \boldsymbol{V}_3(R)$, $\boldsymbol{W}(R)$ je vektorový priestor matíc typu 2×2 nad poľom reálnych čísel majúcich v „pravom dolnom rohu“ číslo nula, $m = 3$, $n = 3$, $\boldsymbol{\varepsilon}_1 = (1, 0, 0)$, $\boldsymbol{\varepsilon}_2 = (0, 1, 0)$, $\boldsymbol{\varepsilon}_3 = (0, 0, 1)$, $\boldsymbol{\eta}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\boldsymbol{\eta}_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\boldsymbol{\eta}_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$,

$$\varphi(\boldsymbol{\varepsilon}_1) = \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix},$$
$$\varphi(\boldsymbol{\varepsilon}_2) = \begin{pmatrix} 2 & 3 \\ -2 & 0 \end{pmatrix},$$
$$\varphi(\boldsymbol{\varepsilon}_3) = \begin{pmatrix} 3 & 5 \\ 1 & 0 \end{pmatrix},$$

a $\boldsymbol{\alpha} = (3, -7, 5)$.

f) $\boldsymbol{V}(R) = \boldsymbol{V}_3(R)$, $\boldsymbol{W}(R) = \boldsymbol{V}_2(R)$, $m = 3$, $n = 2$, $\boldsymbol{\varepsilon}_1 = (1, 0, 0)$, $\boldsymbol{\varepsilon}_2 = (0, 1, 0)$, $\boldsymbol{\varepsilon}_3 = (0, 0, 1)$, $\boldsymbol{\eta}_1 = (1, 1)$, $\boldsymbol{\eta}_2 = (1, 0)$,

$$\varphi(\boldsymbol{\varepsilon}_1) = (1,\ 2),$$
$$\varphi(\boldsymbol{\varepsilon}_2) = (3, -4),$$
$$\varphi(\boldsymbol{\varepsilon}_3) = (1, -1)$$

a $\boldsymbol{\alpha} = (2, -3, 5)$.

2.2. Pomocou hodnosti matice zobrazenia určte, ktoré z lineárnych zobrazení z cvičenia 2.1 je injektívne, surjektívne, bijektívne.

2.3. Porovnajte zobrazenia z cvičenia 2.1a a 2.1b.

2.4. U tých zobrazení cvičenia 2.1, ktoré sú bijektívne, nájdite inverzné lineárne zobrazenie a jeho maticu.

2.5. Lineárne zobrazenie $\varphi : \boldsymbol{V}(R) \to \boldsymbol{W}(R)$ je dané maticou zobrazenia $\mathbf{A}$ pri bázach M a N. Zistite, do ktorých vektorov priestoru $\boldsymbol{W}(R)$ sa zobrazia vektory bázy $\boldsymbol{M}$. Určte tiež súradnice vektora $\varphi(\boldsymbol{\alpha})$ vzhľadom na bázu N, ak je dané

a) $\boldsymbol{V}(R) = \boldsymbol{V}_2(R)$, $\boldsymbol{W}(R) = \boldsymbol{V}_3(R)$, $M = \{(1, 0), (0, 1)\}$, $N = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$, $\boldsymbol{\alpha} = (r, s)$, kde $r, s \in R$ a

$$\mathbf{A} = \begin{pmatrix} 1 & -1 & 3 \\ 2 & -2 & 5 \end{pmatrix}.$$

b) $\boldsymbol{V}(R) = \boldsymbol{V}_2(R)$, $\boldsymbol{W}(R) = \boldsymbol{V}_3(R)$, $M = \{(2, -3), (4, 1)\}$, $N = \{(1, -1, 3), (0, 3, -5), (1, 2, -1)\}$, $\boldsymbol{\alpha} = (r, s)$, kde $r, s \in R$ a

$$\mathbf{A} = \begin{pmatrix} 1 & -1 & 3 \\ 2 & -2 & 5 \end{pmatrix}$$

c) $\boldsymbol{V}(R) = \boldsymbol{V}_4(R)$, $\boldsymbol{W}(R) = \boldsymbol{V}_3(R)$ $M = \{(1, 2, 3, 4), (2, 1, 2, 3), (3, 2, 1, 2), (4, 3, 2, 1)\}$ $N = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$, $\boldsymbol{\alpha} = (5, 1, 1, -5)$ a

$$\mathbf{A} = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 0 & 0 \\ 3 & 8 & -7 \\ 1 & 1 & -2 \end{pmatrix}.$$

d) $\boldsymbol{V}(R)$, $\boldsymbol{W}(R)$, M, N a $\boldsymbol{\alpha}$ ako v cvičení c) ale matica sústavy

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

2.6. Lineárne zobrazenie $\varphi : \boldsymbol{V}(R) \to \boldsymbol{W}(R)$ je dané maticou $\mathbf{A}$ pri bázach M a N. Nájdite maticu tohto zobrazenia pri bázach M' a N', ak je dané:

a) $\boldsymbol{V}(R) = \boldsymbol{V}_3(R)$ $\boldsymbol{W}(R) = \boldsymbol{V}_3(R)$, $M = \{(1,2,3),\ (-1,-1,-1),\ (0,1,1)\}$
$N = \{(2,-1,5), (1,2,3),\ (1,-3,1)\}$ $M' = \{(1,2,-1),\ (3,2,1),\ (-2,0,1)\}$
$N' = \{(1,1,1),\ (1,1,0),\ (1,0,0)\}$

$$\mathbf{A} = \begin{pmatrix} 1, & 1, & -1 \\ 3, & 2 & -5 \\ 4, & -2, & 1 \end{pmatrix}.$$

b) $\boldsymbol{V}(R)$, $\boldsymbol{W}(R)$, $M, N, \mathbf{A}$, ako v cvičení 2.5 b, $M' = \{(1,0),(0,1)\}$, $N' = \{(1,0,0),(0,1,0),(0,0,1)\}$.

2.7. Pomocou matíc prechodu vyjadrite maticu lineárneho zobrazenia z cvičenia 2.1 b) pomocou matice (toho istého) zobrazenia z cvičenia 2.1 a).

2.8. Určte matice zloženého lineárneho zobrazenia:

a) zobrazenia z cvičenia 2.1a) a zobrazenia z cvičenia 2.1f).
b) zobrazenia z cvičenia 2.1a) a zobrazenia z cvičenia 2.1e).

2.9. Nech φ, ψ sú dve lineárne zobrazenia $\boldsymbol{V}_3(R) \to \boldsymbol{V}_2(R)$ a $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_3\}$, $N = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2\}$ sú kanonické bázy priestorov $\boldsymbol{V}_3(R)$ a $\boldsymbol{V}_2(R)$. Zobrazenia φ a ψ sú dané takto:

$$\begin{aligned} \varphi(\boldsymbol{\varepsilon}_1) &= (1,\ 2), & \psi(\boldsymbol{\varepsilon}_1) &= (1,\ 1), \\ \varphi(\boldsymbol{\varepsilon}_2) &= (3,-1), & \psi(\boldsymbol{\varepsilon}_2) &= (-1,-1), \\ \varphi(\boldsymbol{\varepsilon}_3) &= (0,\ 1), & \psi(\boldsymbol{\varepsilon}_3) &= (2,\ 2). \end{aligned}$$

Nájdite maticu zobrazenia $\varphi + \psi$ vzhľadom na bázy M a N.

2.10. Nájdite dimenzie jadra a obrazu zobrazení z cvičení 2.1 a 2.5.

2.11. Nájdite matice lineárnych zobrazení z cvičenia 1.1 a 1.8 vzhľadom na kanonické bázy.

§ 3. Lineárne transformácie

Špeciálnym prípadom lineárnych zobrazení sú lineárne zobrazenia (morfizmy) vektorového priestoru do seba (endomorfizmy).

Definícia 3.1. Ak v definícii 1.1 položíme $\boldsymbol{V}(F) = \boldsymbol{W}(F)$, lineárne zobrazenie φ nazývame *lineárna transformácia.* Inými slovami: Lineárna transformácia je také zobrazenie $\varphi : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$, že platí

(i) $$\varphi(\boldsymbol{\alpha} + \boldsymbol{\beta}) = \varphi(\boldsymbol{\alpha}) + \varphi(\boldsymbol{\beta}),$$

(ii) $$(s\boldsymbol{\alpha}) = s\varphi(\boldsymbol{\alpha}),$$

kde $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}(F)$ sú ľubovoľné vektory a $s \in F$ ľubovoľný skalár.

Príklad 3.1. Vo vektorovom priestore orientovaných úsečiek v rovine (pozri príklad 1.1) je lineárnou transformáciou otočenie o uhol ω okolo pevného bodu P. Podmienka (i) hovorí, že je jedno, či dva vektory najskôr sčítame a potom otočíme ich súčet, alebo naopak. Podmienka (ii) hovorí, že výsledok bude rovnaký, či vektor najprv vynásobíme skalárom a potom otočíme, alebo naopak, najskôr ho otočíme a potom vynásobíme skalárom.

Príklad 3.2. Nech $\boldsymbol{V}(F)$ je ľubovoľný vektorový priestor. Potom zobrazenie $\varphi : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$ definované vzťahom $\varphi(\boldsymbol{\alpha}) = -\boldsymbol{\alpha}$ je lineárnou transformáciou. Dokážte to.

Príklad 3.3. Nech $\boldsymbol{P}_n(R)$ je vektorový priestor polynómov stupňa najviac $n-1$ s reálnymi koeficientami (pozri cvičenie 1.6 kapitoly 2). Nech ďalej zobrazenie $d : \boldsymbol{P}_n(R) \to \boldsymbol{P}_n(R)$ je derivovanie, t.j. $d(f(x)) = f'(x)$. Ide o lineárnu transformáciu, lebo $(f(x) + g(x))' = f'(x) + g'(x)$, $(sf(x))' = sf'(x)$.

Veta 3.1. *Nech* $\varphi : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$ *je lineárna transformácia, pričom* $d(\boldsymbol{V}(F)) = n$. *Potom nasledovné tvrdenia sú ekvivalentné:*

(i) φ *je injektívna lineárna transformácia,*
(ii) φ *je surjektívna lineárna transformácia,*
(iii) φ *je bijektívna lineárna transformácia.*

Dôkaz. Je jasné, že tretie tvrdenie je ekvivalentné konjukcii prvých dvoch. Preto stačí dokázať ekvivalenciu prvých dvoch tvrdení.

a) Nech zobrazenie φ je injekcia. Ďalej nech $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ je báza $\boldsymbol{V}(F)$. Potom podľa vety 1.5 (i) sú vektory $\varphi(\boldsymbol{\varepsilon}_1), \varphi(\boldsymbol{\varepsilon}_i), \dots, \varphi(\boldsymbol{\varepsilon}_n)$ lineárne nezávislé, t.j. tvoria bázu priestoru $\boldsymbol{V}(F)$. Nech $\boldsymbol{\beta} \in \boldsymbol{V}$ je ľubovoľný vektor. Potom ho môžeme písať ako lineárnu kombináciu vektorov tejto bázy. Na základe toho máme $\boldsymbol{\beta} = y_1\varphi(\boldsymbol{\varepsilon}_1) + {} + y_2\varphi(\boldsymbol{\varepsilon}_2) + \cdots + y_n\varphi(\boldsymbol{\varepsilon}_n) = \varphi(y_1\boldsymbol{\varepsilon}_1 + y_2\boldsymbol{\varepsilon}_2 + \cdots + y_n\boldsymbol{\varepsilon}_n)$, t.j. $\boldsymbol{\beta}$ je obrazom, čo značí, že φ je surjekcia.

b) Nech zobrazenie φ je surjekcia. Potom $\operatorname{Im}\varphi = \boldsymbol{V}(F)$. Keďže podľa vety 1.8 je $d(\operatorname{Ker}\varphi) + d(\operatorname{Im}\varphi) = n$, máme $d(\operatorname{Ker}\varphi) + d(\boldsymbol{V}(F)) = n$, čiže $d(\operatorname{Ker}\varphi) = 0$, odkiaľ $\operatorname{Ker}\varphi = \{\vec{0}\}$ a teda podľa vety 1.4 zobrazenie φ je injekcia. □

Poznámka 3.1. Z vety 3.1 vyplýva, že injektívna lineárna transformácia konečnorozmerného priestoru je zároveň aj surjektívna a naopak. Preto pojmy injektívna, surjektívna a bijektívna lineárna transformácia pre konečnorozmerné priestory splývajú.

Definícia 3.2. Bijektívnu lineárnu transformáciu (endomorfizmus, ktorý je izomorfizmom) nazývame *automorfizmus.*

Príklad 3.4. Nech $\boldsymbol{V}(F)$ je ľubovoľný vektorový priestor. Definujeme dve lineárne transformácie $i : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$, $o : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$ takto:

$$\text{Pre všetky} \quad \boldsymbol{\alpha} \in \boldsymbol{V}(F): \qquad i(\boldsymbol{\alpha}) = \boldsymbol{\alpha}, \tag{3.1}$$

$$\text{pre všetky} \quad \boldsymbol{\alpha} \in \boldsymbol{V}(F): \qquad o(\boldsymbol{\alpha}) = \vec{\mathbf{0}}. \tag{3.2}$$

Čitateľ rýchlo dokáže, že i, o sú lineárne transformácie.

Definícia 3.3. Lineárnu transformáciu i nazývame *identická* a o *nulová* transformácia.

O lineárnych transformáciách platia všetky definície a vety paragrafu 1. Aby sme dostali formulácie pre lineárne transformácie vo väčšine viet a definícií stačí položiť $\boldsymbol{W}(F) = \boldsymbol{V}(F)$. Pravda vo vetách 1.4 a 1.5 body (i), (ii), (iii) splývajú. „Preformulovaná“ veta 1.4 bude znieť takto:

Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$ je lineárna transformácia. Potom φ je automorfizmus práve vtedy, keď $\operatorname{Ker}\varphi = \{\vec{0}\}$, *alebo* $\operatorname{Im}\varphi = \boldsymbol{V}$.

Podobne sa „preformuluje“ aj veta 1.5. Čitateľ iste sám postrehol, že veta 1.6 pre lineárnu transformáciu triviálne platí.

V paragrafe 2 sme pojednávali o maticiach lineárnych zobrazení konečnorozmerných priestorov. Definíciu matice lineárnej transformácie dostaneme z definície 2.1 ak položíme $\boldsymbol{W}(F) = \boldsymbol{V}(F)$. Keďže by bola zbytočná komplikácia mať v jedinom priestore $\boldsymbol{V}(F)$ dve bázy, je účelné položiť tiež $M = N$. Kvôli úplnosti si definíciu sformulujeme ešte raz.

Definícia 3.4. Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$ je lineárna transformácia priestoru dimenzie n. Nech $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ je báza priestoru $\boldsymbol{V}$. Nech pre obrazy vektorov bázy platí

$$\begin{aligned}
\varphi(\boldsymbol{\varepsilon}_1) &= a_{11}\boldsymbol{\varepsilon}_1 + a_{12}\boldsymbol{\varepsilon}_2 + \dots + a_{1n}\boldsymbol{\varepsilon}_n,\\
\varphi(\boldsymbol{\varepsilon}_2) &= a_{21}\boldsymbol{\varepsilon}_1 + a_{22}\boldsymbol{\varepsilon}_2 + \dots + a_{2n}\boldsymbol{\varepsilon}_n,\\
&\vdots\\
\varphi(\boldsymbol{\varepsilon}_n) &= a_{n1}\boldsymbol{\varepsilon}_1 + a_{n2}\boldsymbol{\varepsilon}_2 + \dots + a_{nn}\boldsymbol{\varepsilon}_n.
\end{aligned} \tag{3.3}$$

Maticu $\mathbf{A} = (a_{ij})$ $i, j = 1, 2, \dots, n$ nazývame *maticou lineárnej transformácie $\varphi : \boldsymbol{V} \to \boldsymbol{V}$ vzhľadom na bázu M.*

Podobne ako v paragrafe 2 rovnice (3.3) možno zapísať

$$\varphi(\boldsymbol{\varepsilon}_i) = \sum_{j=1}^{n} a_{ij}\boldsymbol{\varepsilon}_j \quad i = 1, 2, \dots, n \tag{3.4}$$

a tiež takto:

$$\begin{pmatrix} \varphi(\boldsymbol{\varepsilon}_1)\\ \varphi(\boldsymbol{\varepsilon}_2)\\ \vdots\\ \varphi(\boldsymbol{\varepsilon}_n) \end{pmatrix} = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n}\\ a_{21}, & a_{22}, & \dots, & a_{2n}\\ \vdots & & & \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} \end{pmatrix} \begin{pmatrix} \boldsymbol{\varepsilon}_1\\ \boldsymbol{\varepsilon}_2\\ \vdots\\ \boldsymbol{\varepsilon}_n \end{pmatrix}. \tag{3.5}$$

Je jasné, že matica lineárnej transformácie je štvorcová matica. Ak si čitateľ preformuluje vetu 2.1 (položí $\boldsymbol{W}(F) = \boldsymbol{V}(F)$, $m = n$, a $M = N$) zistí, že ak $\mathbf{A}$ je matica lineárnej transformácie $\varphi : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$ a $\boldsymbol{\beta} = \varphi(\boldsymbol{\alpha})$, tak súradnice vektora $\boldsymbol{\beta}$ vypočítame podľa vzťahu

$$(y_1, y_2, \dots, y_n) = (x_1, x_2, \dots, x_n)\mathbf{A}, \tag{3.6}$$

kde $(x_1, x_2, \dots, x_n)$ je vektor súradníc vektora $\boldsymbol{\alpha}$.

Príklad 3.5. Vo $\boldsymbol{V}_2(R)$ je daná lineárna transformácia φ vzhľadom na kanonickú bázu $\boldsymbol{\varepsilon}_1 = (1,0), \boldsymbol{\varepsilon}_2 = (0,1)$ takto:

$$\begin{aligned} \varphi(\boldsymbol{\varepsilon}_1) &= -\boldsymbol{\varepsilon}_1 = -1 \cdot \boldsymbol{\varepsilon}_1 + 0 \cdot \boldsymbol{\varepsilon}_2, \\ \varphi(\boldsymbol{\varepsilon}_2) &= \quad \boldsymbol{\varepsilon}_2 = \quad 0 \cdot \boldsymbol{\varepsilon}_1 + 1 \cdot \boldsymbol{\varepsilon}_2. \end{aligned}$$

Vidíme, že

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

Zistíme, do ktorého vektora sa transformuje napr. vektor $\boldsymbol{\alpha} = (3, -5)$. Keďže pri kanonickej báze sa súradnice vektora rovnajú jeho zložkám, máme podľa (3.6)

$$(y_1, y_2) = (3, -5)\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = (-3, -5).$$

t.j. $\varphi(\boldsymbol{\alpha}) = (-3, -5)$. Obraz $\varphi(\boldsymbol{\alpha})$ môžeme vypočítať priamo:
$\varphi(\boldsymbol{\alpha}) = \varphi(3\boldsymbol{\varepsilon}_1 - 5\boldsymbol{\varepsilon}_2) = 3\varphi(\boldsymbol{\varepsilon}_1) - 5\varphi(\boldsymbol{\varepsilon}_2) = 3(-\boldsymbol{\varepsilon}_1) - 5\boldsymbol{\varepsilon}_2 = -3\boldsymbol{\varepsilon}_1 - 5\boldsymbol{\varepsilon}_2$.

Príklad 3.6. Nech $\boldsymbol{P}_4(R)$ je vektorový priestor polynómov s reálnymi koeficientami stupňa najviac 3. Z príkladu 3.3 vieme, že derivovanie je lineárna transformácia tohoto priestoru. Nájdime jej maticu $\mathbf{D}$ vzhľadom na bázu $\{1, x, x^2, x^3\}$. Vidieť, že

$$\begin{aligned} (1)' &= \quad 0 = 0 \cdot 1 + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3, \\ (x)' &= \quad 1 = 1 \cdot 1 + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3, \\ (x^2)' &= \ 2x = 0 \cdot 1 + 2 \cdot x + 0 \cdot x^2 + 0 \cdot x^3, \\ (x^3)' &= 3x^2 = 0 \cdot 1 + 0 \cdot x + 3 \cdot x^2 + 0 \cdot x^3, \end{aligned}$$

čiže

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

Súradnice polynómu $f(x) = 7 - 3x + 4x^2 + 2x^3$ sú $x_1 = 7$, $x_2 = -3$, $x_3 = 4$, $x_4 = 2$. Ak súradnice $f'(x)$ sú y_1, y_1, y_3, y_4, tak $(y_1, y_2, y_3, y_4) = (7, -3, 4, 2)\mathbf{D} = $ $= (-3, 8, 6, 0)$, t.j. $f'(x) = -3 \cdot 1 + 8x + 6 \cdot x^2 + 0 \cdot x^3$.

Príklad 3.7. Čitateľ si ľahko preverí, že v ľubovoľnom vektorovom priestore dimenzie n má zobrazenie $\boldsymbol{i}$ resp. $\boldsymbol{o}$ maticu $\mathbf{J}_n$ resp. $\mathbf{0}_n$.

Vety 2.2 a 2.3 o skladaní lineárnych zobrazení a o matici zloženého zobrazenia zrejme platia, keď položíme $\boldsymbol{V} = \boldsymbol{W} = \boldsymbol{U}$. Poznamenajme len, že ak φ, ψ sú dve lineárne transformácie vektorového priestoru $\boldsymbol{V}$ do seba, má zmysel zložená transformácia $\varphi \circ \psi$ (tu pôsobí ψ ako prvé) aj $\psi \circ \varphi$. Ak priestor $\boldsymbol{V}$ má dimenziu n, matice zobrazení φ resp. ψ sú $\mathbf{A}$, $\mathbf{B}$ sú štvorcové matice typu $n \times n$. Zobrazenie $\varphi \circ \psi$ má maticu $\mathbf{B} \cdot \mathbf{A}$, zobrazenie $\psi \circ \varphi$ maticu $\mathbf{A} \cdot \mathbf{B}$.

Keďže skladanie lineárnych transformácií je asociatívna operácia, platí nasledovná veta.

Veta 3.2. *Nech $\mathcal{L}(F)$ je množina všetkých lineárnych transformácií $\boldsymbol{V}(F) \to \boldsymbol{V}(F)$. Potom štruktúra $(\mathcal{L}(F), \circ)$, kde operácia „$\circ$“ je skladanie transformácií, je monoid.*

Poznámka 3.2. Ak priestor $\boldsymbol{V}$ vo vete 3.2 má konečnú dimenziu n, tak monoid $\mathcal{L}(F)$ je izomorfný monoidu všetkých štvorcových matíc $\boldsymbol{M}_n(F)$ nad poľom F. Dokážte to.

Vetu 2.4 preformulujeme takto:

Veta 3.3. *Nech $\mathbf{A}$ je matica lineárnej transformácie $\varphi : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$ vzhľadom na bázu $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n\}$. Nech $\mathbf{P}$ je matica prechodu od bázy M k báze $M' = \{\boldsymbol{\varepsilon}'_1, \boldsymbol{\varepsilon}'_2, \ldots, \boldsymbol{\varepsilon}'_n\}$. Potom $\mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1}$ je matica zobrazenia φ vzhľadom na bázu M'.*

Príklad 3.8. Lineárna transformácia $\varphi : \boldsymbol{V}_2(R) \to \boldsymbol{V}_2(R)$, ktorú sme skúmali v príklade 3.5 má pri báze $\boldsymbol{\varepsilon}_1 = (1, 0)$, $\quad \boldsymbol{\varepsilon}_2 = (0, 1)$ maticu

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

Nájdeme maticu zobrazenia φ pri báze $\boldsymbol{\varepsilon}'_1 = (1, 1)$, $\boldsymbol{\varepsilon}'_2 = (2, 3)$. Platí

$$\begin{aligned} \boldsymbol{\varepsilon}'_1 &= 1 \cdot \boldsymbol{\varepsilon}_1 + 1 \cdot \boldsymbol{\varepsilon}_2, \\ \boldsymbol{\varepsilon}'_2 &= 2 \cdot \boldsymbol{\varepsilon}_3 + 3 \cdot \boldsymbol{\varepsilon}_2, \end{aligned}$$

Preto matica prechodu $\mathbf{P}$ a jej inverzná matica je

$$\mathbf{P} = \begin{pmatrix} 1, & 1 \\ 2, & 3 \end{pmatrix}, \qquad \mathbf{P}^{-1} = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}.$$

Matica zobrazenia v „novej“ báze bude

$$\mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & -1 \\ -2, & 1 \end{pmatrix} = \begin{pmatrix} -5 & 2 \\ -12 & 5 \end{pmatrix}.$$

V príklade 3.5 sme vypočítali $\varphi(\boldsymbol{\alpha})$, kde $\boldsymbol{\alpha} = (3, -5)$. V novej báze má súradnice $x'_1 = 19, x'_2 = -8$. Vektor súradníc vektora $\varphi(\boldsymbol{\alpha})$ je

$$(y_1, y_2) = (19, -8) \begin{pmatrix} -5 & 2 \\ -12 & 5 \end{pmatrix} = (1, -2),$$

teda $\varphi(\boldsymbol{\alpha}) = 1\boldsymbol{\varepsilon}'_1 + (-2)\boldsymbol{\varepsilon}'_2 = (-3, -5)$ v zhode s príkladom 3.5.

Podobne ako vo vetách 1.4 a 1.5 aj vo vete 2.5 body (i), (ii) a (iii) splynú. Vetu 2.5 preformulujeme takto:

Veta 3.4. *Nech* $\mathbf{A}$ *je matica lineárnej transformácie* $\varphi : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$, *vzhľadom na bázu* $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n\}$. *Potom* φ *je automorfizmus (bijektívna lineárna transformácia) práve vtedy, keď* $\mathbf{A}$ *je regulárna matica.*

Vety 2.6. a 2.7 platia aj pre prípad $\boldsymbol{V} = \boldsymbol{W}$. Veta 2.6 (preformulovaná pre lineárnu transformáciu) hovorí, že lineárna transformácia φ má inverznú lineárnu transformáciu φ^{-1} práve vtedy keď je automorfizmus. Keďže zložením dvoch automorfizmov dostaneme opäť automorfizmus (prečo?), platí nasledujúca veta.

Veta 3.5. *Nech* $\mathcal{A}(F)$ *je množina všetkých automorfizmov priestoru* $\boldsymbol{V}(F)$. *Potom štruktúra* $(\mathcal{A}(F), \circ)$ *je grupa. (Operácia „*$\circ$*" je skladanie automorfizmov.)*

Dôkaz sa ponecháva na čitateľa. Poznamenajme len, že neutrálnym prvkom grupy je automorfizmus $\boldsymbol{i} : \boldsymbol{V}(F) \to \boldsymbol{V}(F)$.

Poznámka 3.3. V prípade, že priestor $\boldsymbol{V}(F)$ vo vete 3.5 má konečnú dimenziu n, grupa $\mathcal{A}(F)$ je izomorfná grupe všetkých regulárnych matíc typu $n \times n$ nad F. Dokážte to.

Podľa vety 2.7 matice automorfizmov φ, φ^{-1} priestoru dimenzie n sú navzájom inverzné. V nasledujúcom príklade ukážeme ďalšiu možnosť výpočtu inverznej matice pomocou pojmu lineárnej transformácie.

Príklad 3.9 (dôležitý). Nech $\mathbf{A}$ je regulárna matica typu $n \times n$ nad poľom F. Na základe poznámky 3.3 ju môžeme považovať za maticu automorfizmu $\varphi : \boldsymbol{V}_n(F) \to \boldsymbol{V}_n(F)$ vzhľadom na kanonickú bázu. Ak vektory kanonickej bázy označíme $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n$, tak jednotlivé riadky matice $\mathbf{A}$ budú vektory $\varphi(\boldsymbol{\varepsilon}_1)$, $\varphi(\boldsymbol{\varepsilon}_2), \ldots, \varphi(\boldsymbol{\varepsilon}_n)$. (Čitateľ nech nestráca zo zreteľa, že súradnice vektora v kanonickej báze sa rovnajú jeho zložkám.) Napíšeme maticu typu $n \times 2n$ majúcu v každom riadku $i = 1, 2, \ldots, n$ najprv zložky vektora $\boldsymbol{\varepsilon}_i$, potom zložky vektora $\varphi(\boldsymbol{\varepsilon}_i) = \varrho_i$. Teda vľavo bude matica $\mathbf{J}_n$, vpravo matica $\mathbf{A}$.

$$
\begin{pmatrix}
1,0,0, & \ldots, & 0, & a_{11}, & a_{12}, & \ldots, & a_{1n} \\
0,1,0, & \ldots, & 0, & a_{21}, & a_{22}, & \ldots, & a_{2n} \\
0,0,1, & \ldots, & 0, & a_{31}, & a_{32}, & \ldots, & a_{3n} \\
\vdots & & & & & & \\
0,0,0, & \ldots, & 1, & a_{n1}, & a_{n2}, & \ldots, & a_{nn}
\end{pmatrix}. \tag{3.7}
$$

Keďže φ je automorfizmus ($\mathbf{A}$ je regulárna matica), vektory $\varrho_i = \varphi(\boldsymbol{\varepsilon}_i)$ tvoria podľa vety 1.5 bázu priestoru $\boldsymbol{V}_n(F)$. Z toho vyplýva, že inverzný automorfizmus φ^{-1} je určený rovnicami $\varphi^{-1}(\varrho_i) = \boldsymbol{\varepsilon}_i$. Matica (3.7) nám teda určuje aj automorfizmus φ^{-1}. Teraz si uvedomme toto: Ak na matici (3.7) uskutočníme ľubovoľnú ero dostaneme maticu, ktorá tiež určuje φ^{-1}. Skutočne:

1) Keď vymeníme riadky matice (3.7) je to zrejmé.

2) Keď vynásobíme i-tý riadok prvkom $c \in F$, $c \neq 0$ máme:
$c \cdot \boldsymbol{\varepsilon}_i = c \cdot \varphi^{-1}(\varrho_i)$, čiže $c\boldsymbol{\varepsilon}_i = \varphi^{-1}(c\varrho_i)$. Teda vektor vľavo bude obrazom vektora vpravo, ako predtým.

3) Keď zameníme i-tý riadok súčtom i-teho a j-teho riadku, bude v i-tom riadku $\boldsymbol{\varepsilon}_i + \boldsymbol{\varepsilon}_j = \varphi^{-1}(\varrho_i) + \varphi^{-1}(\varrho_j) = \varphi^{-1}(\varrho_i + \varrho_j)$. Zase v i-tom riadku máme vľavo obraz vektora vpravo.

Vidieť, že keď urobíme ľubovoľný počet ero, výsledná matica vždy bude určovať automorfizmus φ^{-1}. Ak teraz pomocou ero dosiahneme, že na pravej strane matice bude matica $\mathbf{J}_n$, riadky matice na ľavej strane určujú vektory, do ktorých sa zobrazujú vektory kanonickej bázy pri automorfizme φ^{-1}. Podľa vety 2.7 matica vľavo je matica $\mathbf{A}^{-1}$.

Aby sme si postup ozrejmili, ukážeme ho na konkrétnom príklade. Vypočítame inverznú maticu matici z príkladu 2.1. z kapitoly 4

$$\mathbf{A} = \begin{pmatrix} 6 & 3 & 5 \\ 4 & 6 & 4 \\ 7 & 4 & 6 \end{pmatrix}.$$

Počítame

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

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

$$\to \begin{pmatrix} -3 & -\frac{1}{2} & 3 & 1 & 0 & 1 \\ 2 & \frac{1}{2} & -2 & 0 & 1 & 0 \\ 13 & \frac{3}{2} & -12 & 0 & 0 & -1 \end{pmatrix} \to \begin{pmatrix} 10 & 1 & -9 & 1 & 0 & 0 \\ 2 & \frac{1}{2} & -2 & 0 & 1 & 0 \\ -13 & -\frac{3}{2} & 12 & 0 & 0 & 1 \end{pmatrix}.$$

Na ľavej strane matice sme určili $\mathbf{A}^{-1}$. Porovnajte s výsledkom príkladu 2.1 kapitoly 4. Čitateľ si môže sám určiť, aké ero sme uskutočnili pri jednotlivých krokoch.

Cvičenia

3.1. Nech $\varphi : \boldsymbol{V}(F) \to \boldsymbol{F}(F)$ je lineárna transformácia priestoru $\boldsymbol{V}(F)$. Potom platí: $\varphi(\vec{0}) = \vec{0}$, $\varphi(-\boldsymbol{\alpha}) = -\varphi(\boldsymbol{\alpha})$, kde $\boldsymbol{\alpha}, \vec{0} \in \boldsymbol{V}(F)$. Dokážte to.

3.2. Nech φ je zobrazenie priestoru $\boldsymbol{V}_3(R)$ do seba. V ktorých prípadoch je φ lineárna transformácia, keď $\boldsymbol{\alpha} = (x, y, z)$ je ľubovoľný vektor priestoru $\boldsymbol{V}_3(R)$:

a) $\varphi(\boldsymbol{\alpha}) = (x + 3, y + 3, z + 3)$, b) $\varphi(\boldsymbol{\alpha}) = (-x, -y, z)$,
c) $\varphi(\boldsymbol{\alpha}) = (x - y, y - z, z - x)$, d) $\varphi(\boldsymbol{\alpha}) = (x^2, x, z)$.

3.3. Nájdite matice týchto lineárnych zobrazení priestoru $\boldsymbol{V}_2(R)$ vzhľadom na bázu $\boldsymbol{\varepsilon}_1 = (1, 0)$, $\boldsymbol{\varepsilon}_2 = (0, 1)$.

a) Súmernosť podľa osi x,
b) súmernosť podľa osi y,
c) súmernosť podľa počiatku súradnicového systému,
d) otočenie o uhol $\frac{\pi}{2}$ (proti smeru hodinových ručičiek),
e) súmernosť podľa osi $y = x$,
f) súmernosť podľa osi $y = -x$,
g) priemet na os x,
h) otočenie o uhol ω.
i) súmernosť podľa osi zvierajúcej s osou x uhol $\frac{\omega}{2}$.

3.4. V priestore $\boldsymbol{V}_3(R)$ je daná transformácia φ vzhľadom na bázu $\boldsymbol{\varepsilon}_1 = (1,0,0)$, $\boldsymbol{\varepsilon}_2 = (0,1,0)$ $\boldsymbol{\varepsilon}_3 = (0,0,1)$ maticou

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

Definujte zobrazenie φ pomocou vektorov $\varphi(\boldsymbol{\varepsilon}_1)$, $\varphi(\boldsymbol{\varepsilon}_2)$, $\varphi(\boldsymbol{\varepsilon}_3)$ (rovností (3.4)) a transformujte vektor $\boldsymbol{\alpha} = (3,-2,5)$ ako podľa vzťahu (3.6), tak aj pomocou rovností (3.4).

3.5. Urobte cvičenie 3.4 ešte raz s tým rozdielom, že matica $\mathbf{A}$ definuje zobrazenie φ, vzhľadom na bázu $\boldsymbol{\varepsilon}'_1 = (1,2,1)$, $\boldsymbol{\varepsilon}'_2 = (1,2,0)$, $\boldsymbol{\varepsilon}'_3 = (1,0,0)$.

3.6. Nájdite maticu $\mathbf{D}^*$ lineárnej transformácie d^* vektorového priestoru $\boldsymbol{P}_4(R)$ (vektorový priestor polynómov s reálnymi koeficientami stupňa najviac tri) definovanej takto: $d^*(f(x)) = f''(x)$, kde $f''(x)$ je druhá derivácia polynómu $f(x) \in \boldsymbol{P}_4(R)$.

3.7. Lineárna transformácia $\varphi : \boldsymbol{V} \to \boldsymbol{V}$ je daná pri báze B maticou $\mathbf{A}$. Nájdite maticu $\mathbf{A}'$ zobrazenia φ vzhľadom na bázu B', ak je dané:

a) $\boldsymbol{V} = \boldsymbol{V}_2(R)$, $B = \{(1,0),(0,1)\}$, $B' = \{(2,-1),(2,3)\}$, $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$,

b) $\boldsymbol{V} = \boldsymbol{V}_2(R)$, $B = \{(2,3),(-1,-1)\}$, $B' = \{(1,1),(1,0)\}$, $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$,

c) $\boldsymbol{V} = \boldsymbol{V}_3(R)$, $B = \{(1,0,-1),(2,1,-1),(3,1,-3)\}$,
$B' = \{(1,0,0),(0,1,0),(0,0,1)\}$, $\mathbf{A} = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$,

d) $\boldsymbol{V} = \boldsymbol{V}_3(R)$, $B = \{(1,0,0),(0,1,0),(0,0,1)\}$,
$B' = \{(1,1,1),(1,1,0),(1,0,0)\}$, $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & -1 \\ 2 & 4 & 3 \end{pmatrix}$.

3.8. Metódou ako v príklade 3.9 vypočítajte inverzné matice matíc z cvičenia 2.2 kapitoly 4.

3.9. Metódou ako v príklade 3.9. vypočítajte inverzné matice nasledujúcich matíc:

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

3.10. V prípadoch, kde je to možné, určte maticu $\mathbf{A}^{-1}$ zobrazenia φ^{-1} z cvičenia 3.7.

§ 4. Invariantné podpriestory

V poznámke 2.5 sme uviedli, že hoci matica lineárneho zobrazenia závisí od báz, vzhľadom na ktoré ju uvažujeme, jej hodnosť od báz nezávisí, t.j. je invariantom lineárneho zobrazenia. Samozrejme toto platí aj v prípade lineárnej transformácie. Hodnosť matice lineárnej transformácie je invariantom lineárnej transformácie (nezávisí na voľbe bázy). V tomto paragrafe nájdeme ďalšie invarianty lineárnej transformácie: charakteristické vektory a charakteristické hodnoty.

Definícia 4.1. Nech φ je lineárna transformácia vektorového priestoru $\boldsymbol{V}$. Podpriestor $\boldsymbol{S}$ priestoru $\boldsymbol{V}$ sa nazýva *invariantným podpriestorom* vzhľadom na transformáciu φ, ak pre všetky vektory $\boldsymbol{\alpha} \in \boldsymbol{S}$ platí $\varphi(\boldsymbol{\alpha}) \in \boldsymbol{S}$.

Hneď vidieť, že podpriestory $\boldsymbol{V}$ a $\{\vec{\mathbf{0}}\}$ sú invariantnými priestormi priestoru $\boldsymbol{V}$.

Príklad 4.1. Uvažujme lineárnu transformáciu φ priestoru $\boldsymbol{V}_2(R)$, ktorej matica pri báze $\boldsymbol{\varepsilon}_1 = (1,0)$ $\boldsymbol{\varepsilon}_2 = (0,1)$ je

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

Podpriestor $\boldsymbol{R} = \{(x,y);\ 2x + y = 0\}$ nie je invariantný vzhľadom na transformáciu φ. Ak zvolíme napr. vektor $\boldsymbol{\alpha} = (-1,2) \in \boldsymbol{R}$, ľahko sa presvedčíme, že $\varphi(\boldsymbol{\alpha}) \notin \boldsymbol{R}$. Naozaj, keďže vzhľadom na kanonickú bázu súradnice vektora sú rovné jeho zložkám, máme

$$\varphi(\boldsymbol{\alpha}) = (-1,2)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (2,-1).$$

Vidíme, že $\varphi(\boldsymbol{\alpha}) = (2,-1) \notin \boldsymbol{R}$.

Podpriestor $\boldsymbol{S} = \{(x,y);\ x-y = 0\}$ je invariantný vzhľadom na transformáciu φ. Skutočne: nech $\boldsymbol{\beta} = (x,y)$ je ľubovoľný vektor z $\boldsymbol{S}$. Vypočítame vektor

$$\varphi(\boldsymbol{\beta}) = (x,y)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (y,x).$$

Vidieť, že $\varphi(\boldsymbol{\beta}) = (y,x) \in \boldsymbol{S}$, lebo ak $x-y=0$, tak $y-x=0$.

Príklad 4.2. Nech φ je otočenie okolo osi x v trojrozmernom priestore orientovaných úsečiek vychádzajúcich z počiatku súradnicového systému. Invariantné podpriestory tvoria:

1) všetky vektory ležiace na osi x,

2) všetky vektory ležiace v rovine yz.

Príklad 4.3. Nech $\boldsymbol{P}_n(R)$ je priestor polynómov stupňa najviac $n-1$. Nech transformácia δ je derivovanie a nech $k \leqq n$ je prirodzené číslo. Potom $\boldsymbol{P}_k(R)$ je invariantný podpriestor priestoru $\boldsymbol{P}_n(R)$ vzhľadom na transformáciu δ.

Príklad 4.4. Lineárna transformácia φ priestoru $\boldsymbol{V}_5(R)$ je daná maticou

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & 0 & 0 \\ a_{21} & a_{22} & a_{23} & 0 & 0 \\ a_{31} & a_{32} & a_{33} & 0 & 0 \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix}$$

vzhľadom na kanonickú bázu. $\boldsymbol{\varepsilon}_1 = (1,0,0,0,0)$, $\boldsymbol{\varepsilon}_2 = (0,1,0,0,0), \cdots$. Podpriestor $\boldsymbol{S} = [\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_3]$ (generovaný vektormi $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_3$) je invariantný podpriestor. Skutočne: vektory priestoru $\boldsymbol{S}$ majú posledné dve zložky nulové. Čitateľ ľahko skontroluje, že aj ich obrazy majú posledné dve zložky nulové.

Budeme uvažovať o jednorozmerných invariantných podpriestoroch. Nech $\boldsymbol{R}$ je jednorozmerný invariantný podpriestor priestoru $\boldsymbol{V}(F)$ vzhľadom na transformáciu φ. Nech $\boldsymbol{R}$ je generovaný vektorom $\boldsymbol{\alpha}$, t.j. $\boldsymbol{R} = [\boldsymbol{\alpha}]$, kde $\boldsymbol{\alpha} \neq \vec{0}$. Keďže $\boldsymbol{R}$ je invariantný podpriestor, platí

$$\varphi(\boldsymbol{\alpha}) \in \boldsymbol{R}.$$

To znamená, že $\varphi(\boldsymbol{\alpha})$ je tvaru

$$\varphi(\boldsymbol{\alpha}) = \lambda\boldsymbol{\alpha}, \tag{4.1}$$

kde $\lambda \in F$ je skalár.

Definícia 4.2. Vektor $\boldsymbol{\alpha}$, ktorý generuje jednorozmerný invariantný podpriestor $\boldsymbol{R}$ priestoru $\boldsymbol{V}(F)$ vzhľadom na transformáciu φ sa nazýva *charakteristický (vlastný) vektor* transformácie φ. Skalár λ v rovnosti (4.1) sa nazýva *charakteristická (vlastná) hodnota* transformácie φ.

Veta 4.1. *Nech $\boldsymbol{R}$ je jednorozmerný invariantný podpriestor priestoru $\boldsymbol{V}(F)$ vzhľadom na transformáciu φ. Nech $\boldsymbol{\alpha}, \lambda$ sú charakteristický vektor a charakteristická hodnota transformácie φ. Nech $\boldsymbol{\beta}$ je ľubovoľný vektor podpriestoru $\boldsymbol{R}$. Potom*

$$\varphi(\boldsymbol{\beta}) = \lambda\boldsymbol{\beta}. \tag{4.2}$$

Dôkaz. Keďže $\boldsymbol{\beta} \in \boldsymbol{R}$, platí $\boldsymbol{\beta} = k \cdot \boldsymbol{\alpha}$, kde $k \in F$. Počítame $\varphi(\boldsymbol{\beta}) = \varphi(k\boldsymbol{\alpha}) = k\varphi(\boldsymbol{\alpha}) = k(\lambda\boldsymbol{\alpha}) = \lambda(k\boldsymbol{\alpha}) = \lambda\boldsymbol{\beta}$. □

Teda každý vektor jednorozmerného invariantného podpriestoru sa transformuje pomocou charakteristickej hodnoty λ.

Veta 4.2. *Nech λ je charakteristická hodnota transformácie φ n-rozmerného vektorového priestoru $\boldsymbol{V}(F)$. Nech $\mathbf{A}$ je matica tejto transformácie (vzhľadom na nejakú bázu). Potom λ je koreň rovnice*

$$d(\mathbf{A} - \lambda \mathbf{J}_n) = 0. \tag{4.3}$$

Dôkaz. Nech $\boldsymbol{\alpha}$ je charakteristický vektor transformácie φ prislúchajúci charakteristickej hodnote λ. Nech $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n$ je nejaká báza priestoru $\boldsymbol{V}(F)$ a

$$\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n,$$
$$\varphi(\boldsymbol{\alpha}) = y_1\boldsymbol{\varepsilon}_1 + y_2\boldsymbol{\varepsilon}_2 + \dots + y_n\boldsymbol{\varepsilon}_n$$

sú vyjadrenia vektorov $\boldsymbol{\alpha}$ a $\varphi(\boldsymbol{\alpha})$ v tejto báze. Keďže je $\varphi(\boldsymbol{\alpha}) = \lambda\boldsymbol{\alpha}$, z týchto vyjadrení vyplýva

$$y_1 = \lambda x_1, \quad y_2 = \lambda x_2, \dots, \quad y_n = \lambda x_n.$$

Podľa (2.4) však máme

$$(y_1, y_2, \dots, y_n) = (x_1, x_2, \dots, x_n)\mathbf{A}$$

alebo (po dosadení)

$$(\lambda x_1, \lambda x_2, \dots, \lambda x_n) = (x_1, x_2, \dots, x_n)\mathbf{A}.$$

Čitateľ ľahko zistí, že posledná rovnica vedie na sústavu rovníc

$$\begin{aligned}
a_{11}x_1 + a_{21}x_2 + \dots + a_{n1}x_n &= \lambda x_1,\\
a_{12}x_1 + a_{22}x_2 + \dots + a_{n2}x_n &= \lambda x_2,\\
&\ \vdots\\
a_{1n}x_1 + a_{2n}x_2 + \dots + a_{nn}x_n &= \lambda x_n,
\end{aligned} \tag{4.4}$$

ktorú, keďže ide o sústavu homogénnych rovníc, napíšeme v tvare

$$\begin{aligned}
(a_{11} - \lambda)x_1 + a_{21}x_2 + \dots + a_{n1}x_n &= 0,\\
a_{12}x_1 + (a_{22} - \lambda)x_2 + \dots + a_{n2}x_n &= 0,\\
&\ \vdots\\
a_{1n}x_1 + a_{2n}x_2 + \dots + (a_{nn} - \lambda)x_n &= 0,
\end{aligned} \tag{4.5}$$

kde a_{ik} sú prvky matice $\mathbf{A}$. Vidíme, že matica sústavy (4.5) je $(\mathbf{A} - \lambda\mathbf{J}_n)^T$. Keďže $\boldsymbol{\alpha} \neq \vec{0}$ (prečo?), musí mať uvedená sústava aj nenulové riešenie. To však je možné iba vtedy keď determinant matice sústavy (teda aj determinant transponovanej matice sústavy) je rovný nule. Máme tak

$$\begin{vmatrix}
a_{11} - \lambda & a_{12} & \dots & a_{1n}\\
a_{21} & a_{22} - \lambda & \dots & a_{2n}\\
\vdots & & & \\
a_{n1} & a_{n2} & \dots & a_{nn} - \lambda
\end{vmatrix} = 0, \qquad \text{alebo} \qquad d(\mathbf{A} - \lambda\mathbf{J}_n) = 0.$$

Tým je dôkaz vety skončený. □

Ľahko sa ukáže, že rovnicu (4.3) môžeme písať v tvare

$$\lambda^n + a_1\lambda^{n-1} + \dots + a_{n-1}\lambda + a_n = 0. \tag{4.6}$$

Vidíme, že ide o rovnicu n-tého stupňa majúcu koeficienty z poľa F.

Definícia 4.3. Rovnicu (4.3) resp. (4.6) nazývame *charakteristickou rovnicou* a jej ľavú stranu *charakteristickým polynómom* transformácie φ. Charakteristický polynóm označíme $P(\lambda)$.

Poznámka 4.1. Môže sa stať, že rovnica (4.6) nemá v poli F žiaden koreň. Ako uvidíme neskoršie existencia koreňa je zaručená, keď F je tzv. algebraicky uzavreté pole. Napr. pole reálnych čísel nie je algebraicky uzavreté, lebo ako čitateľ vie zo strednej školy existujú rovnice 2-ho stupňa s reálnymi koeficientami nemajúce reálny koreň. Pole komplexných čísel je algebraicky uzavreté. (Toto tvrdenie dokázal K. F. Gauss v r. 1799.)

Z tejto poznámky a vety 4.2 vyplýva tvrdenie:

Každá lineárna transformácia vektorového priestoru nad algebraicky uzavretým poľom má aspoň jednu charakteristickú hodnotu a tým tiež aspoň jeden charakteristický vektor.

Poznámka 4.2. Keď chceme nájsť vlastné vektory nejakej lineárnej transformácie vektorového priestoru (konečnej dimenzie) nad poľom F postupujeme obyčajne tak, že riešime rovnicu (4.6) a vypočítame vlastné hodnoty transformácie. Ku každej vlastnej hodnote λ, ktorá je z poľa F (ak takáto vôbec existuje), napíšeme sústavu (4.4) alebo, čo je to isté, (4.5). (Pozor, matica tejto sústavy je $(\mathbf{A} - \lambda \mathbf{J}_n)^T$.) Sústavu vyriešime. Každé nenulové riešenie tejto sústavy je vektor súradníc charakteristického vektora, ktorý sa transformuje hodnotou λ.

Príklad 4.5. Lineárna transformácia $\varphi : \boldsymbol{V}_2(R) \to \boldsymbol{V}_2(R)$ je daná (vzhľadom na kanonickú bázu) touto maticou

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

Charakteristická rovnica transformácie φ je

$$d\left(\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) - \lambda \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) = 0.$$

Po úprave

$$\begin{vmatrix} -\lambda & 1 \\ -1 & -\lambda \end{vmatrix} = 0,$$

alebo

$$\lambda^2 + 1 = 0.$$

Vidíme, že rovnica nemá reálny koreň, t.j. transformácia φ nemá jednorozmerný invariantný podpriestor. Je to pochopiteľné, lebo transformácia φ zodpovedá v priestore orientovaných úsečiek v rovine (izomorfnom priestoru $\boldsymbol{V}_2(R)$) otočeniu o 90^o. Presvedčte sa o tom.

Príklad 4.6. Matica

$$\mathbf{B} = \begin{pmatrix} \frac{5}{4} & \frac{3}{4} \\ -\frac{3}{4} & -\frac{5}{4} \end{pmatrix}$$

nám určuje transformáciu ψ vektorového priestoru $\boldsymbol{V}_2(R)$ vzhľadom na bázu $\varepsilon_1 = (1,2)$, $\varepsilon_2 = (1,-2)$. Charakteristická rovnica transformácie ψ je

$$\begin{vmatrix} \frac{5}{4} - \lambda & \frac{3}{4} \\ -\frac{3}{4} & -\frac{5}{4} - \lambda \end{vmatrix} = 0$$

alebo

$$-(\frac{5}{4} - \lambda)(\frac{5}{4} + \lambda) + \frac{9}{16} = 0,$$

čo ľahko upravíme na

$$\lambda^2 - 1 = 0.$$

Korene tejto rovnice (vlastné hodnoty transformácie ψ) sú $\lambda_1 = 1$, $\lambda_2 = -1$.

Sústava (4.5) pre charakteristickú hodnotu $\lambda_1 = 1$ je

$$\begin{aligned} (\frac{5}{4} - 1)x_1 - \frac{3}{4}x_2 &= 0, \\ \frac{3}{4}x_1 - (\frac{5}{4} + 1)x_2 &= 0, \end{aligned}$$

po úprave

$$\begin{aligned} x_1 - 3x_2 &= 0, \\ x_1 - 3x_2 &= 0. \end{aligned}$$

Podpriestor riešení tejto sústavy je $\{(3p,p);\ p \in R\}$, čo znamená, že každý charakteristický vektor α, prislúchajúci vlastnej hodnote 1, má vektor súradníc $(3p,p)$, kde $p \in R$. Teda $\alpha = 3p\varepsilon_1 + p\varepsilon_2 = 3p(1,2) + p(1,-2) = (4p,4p) = (r,r)$, kde $r \in R$. Odtiaľ vyplýva, že charakteristickým vektorom je ľubovoľný nenulový vektor (x_1,x_2), pre ktorý platí $x_1 = x_2$. To znamená, že invariantným podpriestorom je množina $\boldsymbol{S} = \{(x_1,x_2);\ x_1 = x_2\}$ všetkých vektorov ležiacich na priamke $y = x$. Ďalej platí $\psi(\boldsymbol{\alpha}) = 1\boldsymbol{\alpha} = \boldsymbol{\alpha}$. Naozaj, vypočítali sme, že vektor súradníc ľubovoľného vlastného vektora je $(3p,p)$. Ak ho transformujeme maticou zobrazenia, dostaneme $(3p,p) \cdot \begin{pmatrix} \frac{5}{4} & \frac{3}{4} \\ -\frac{3}{4} & -\frac{5}{4} \end{pmatrix} = (\frac{15}{4}p - \frac{3}{4}p,\ \frac{9}{4}p - \frac{5}{4}p) = (3p,p)$. Vidíme, že vektor súradníc,teda ani samotný vektor, sa transformáciou nezmenil.

Sústava (4.5) pre $\lambda_2 = -1$ je

$$\begin{aligned} (\frac{5}{4} + 1)x_1 - \frac{3}{4}x_2 &= 0, \\ \frac{3}{4}x_1 + (-\frac{5}{4} + 1)x_2 &= 0, \end{aligned}$$

po úprave

$$\begin{aligned} 3x_1 - x_2 &= 0, \\ 3x_1 - x_2 &= 0. \end{aligned}$$

Podpriestor riešení tejto sústavy je $\{(p, 3p);\ p \in R\}$, čo znamená, že každý charakteristický vektor β prislúchajúci vlastnej hodnote -1 má vektor súradníc $(p, 3p)$, kde $p \in R$. Teda $\beta = p\varepsilon_1 + 3p\varepsilon_2 = p(1,2) + 3p(1,-2) = (4p, -4p) = (r, -r)$, kde $r \in R$. Odtiaľ vyplýva, že charakteristickým vektorom je ľubovoľný nenulový vektor (x_1, x_2), pre ktorý platí $x_1 + x_2 = 0$. Charakteristickým vektorom je napr. $\boldsymbol{\beta} = (1, -1)$ a invariantný jednorozmerný podpriestor $\boldsymbol{T} = \{(x_1, x_2); x_1 + x_2 = 0\}$ je množinou všetkých vektorov ležiacich na priamke $y = -x$. Podobne ako vyššie, čitateľ ľahko skontroluje, že platí $\psi(\boldsymbol{\beta}) = -1\boldsymbol{\beta} = -\boldsymbol{\beta}$.

V definícii 4.3 sme ľavú stranu rovnice (4.6) nazvali charakteristickým polynómom transformácie φ, vynechajúc slová „pri danej báze“. Tým sme naznačili, že charakteristický polynóm nezávisí od voľby bázy. To však treba dokázať.

Veta 4.3. *Charakteristický polynóm lineárnej transformácie n-rozmerného vektorového priestoru nezávisí na voľbe bázy.*

Dôkaz. Charakteristický polynóm (podľa 4.3) je

$$P(\lambda) = d(\mathbf{A} - \lambda \mathbf{J}_n),$$

kde matica transformácie $\mathbf{A}$ závisí od zvolenej bázy. Prejdeme k novej báze pomocou matice prechodu $\mathbf{P}$. Matica transformácie v novej báze podľa vety 2.4 je $\mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1}$. Charakteristický polynóm pre túto maticu je $d(\mathbf{PAP}^{-1} - \lambda \mathbf{J}_n) = d(\mathbf{PAP}^{-1} - \lambda \mathbf{PJ}_n\mathbf{P}^{-1}) = d(\mathbf{P}(\mathbf{A} - \lambda \mathbf{J}_n)\mathbf{P}^{-1}) = d(\mathbf{P})d(\mathbf{A} - \lambda \mathbf{J}_n)d(\mathbf{P}^{-1}) = d(\mathbf{PP}^{-1})d(\mathbf{A} - \lambda \mathbf{AJ}_n) = d(\mathbf{A} - \lambda \mathbf{J}_n) = P(\lambda)$. Vidíme, že prechodom k inej báze sa charakteristický polynóm nezmenil. $\square$

Poznámka 4.3. Z toho, že charakteristický polynóm nezávisí od voľby bázy vyplýva, že ani charakteristická rovnica ani charakteristické hodnoty a charakteristické vektory od nej nezávisia. Sú to *invarianty* lineárnej transformácie.

V príklade 4.6 každý charakteristický vektor prislúchajúci charakteristickej hodnote 1 generuje ten istý jednorozmerný invariantný priestor $\boldsymbol{S}$. Inými slovami: neexistujú dva lineárne nezávislé charakteristické vektory prislúchajúce hodnote 1. Podobne to je to aj s hodnotou -1. Nasledujúci príklad ukazuje, že tomu vždy tak nie je.

Príklad 4.7. Transformácia $\varphi : \boldsymbol{V}_3(R) \to \boldsymbol{V}_3(R)$ je daná maticou (vzhľadom na kanonickú bázu)

$$\mathbf{A} = \begin{pmatrix} 3 & -1 & 3 \\ 2 & 0 & 6 \\ 3 & -3 & 11 \end{pmatrix}.$$

Vypočítame charakteristickú rovnicu:

$$\begin{vmatrix} 3-\lambda & -1 & 3 \\ 2 & -\lambda & 6 \\ 3 & -3 & 11-\lambda \end{vmatrix} = 0,$$

po úprave

$$\lambda^3 - 14\lambda^2 + 44\lambda - 40 = 0,$$

alebo

$$(\lambda-2)^2(\lambda-10)=0.$$

Vidíme, že charakteristické hodnoty sú reálne čísla*) $\lambda_1=\lambda_2=2$, $\lambda_3=10$.

Napíšeme sústavu (4.4) pre hodnotu $\lambda_{1,2}=2$. Máme sústavu

$$\begin{aligned} x_1+2x_2+3x_3&=0,\\ -x_1-2x_2-3x_3&=0,\\ 3x_1+6x_2+9x_3&=0, \end{aligned}$$

ktorej podpriestor riešení je

$$\boldsymbol{S}=\{(-2p-3q,\ p,\ q);\ \ p,q\in R\}.$$

Ľubovoľný nenulový vektor priestoru $\boldsymbol{S}$ je charakteristický vektor prislúchajúci charakteristickej hodnote 2. Zvoľme napr. charakteristické vektory $\boldsymbol{\alpha}=(-2,1,0)$, $\boldsymbol{\beta}=(-3,0,1)$. Čitateľ nech si skontroluje, že vektory $\boldsymbol{\alpha},\boldsymbol{\beta}$ sú lineárne nezávislé a že $\varphi(\boldsymbol{\alpha})=(-2,1,0)\cdot\mathbf{A}=(-4,2,0)=2\boldsymbol{\alpha}$, $\varphi(\boldsymbol{\beta})=(-3,0,1)\cdot\mathbf{A}=(-6,0,2)=2\boldsymbol{\beta}$.

Podobne pre hodnotu $\lambda_3=10$ máme sústavu

$$\begin{aligned} -7x_1+2x_2+3x_3&=0,\\ -x_1-10x_2-3x_3&=0,\\ 3x_1+6x_2+x_3&=0, \end{aligned}$$

ktorej podpriestor riešení je $\{(p,\ -p,\ 3p);\ p\in R\}$. Keďže vzhľadom na kanonickú bázu sú súradnice vektora priestoru $\boldsymbol{V}_3(R)$ rovné jeho zložkám, tento podpriestor je zároveň jednorozmerným invariantným podpriestorom transformácie φ. Za charakteristický vektor zoberieme napr. $\boldsymbol{\gamma}=(1,-1,3)$. Čitateľ si overí, že $\varphi(\boldsymbol{\gamma})=(1,-1,3)\cdot A=(10,-10,30)=10\boldsymbol{\gamma}$.

Z príkladu 4.7 vyplýva, že charakteristické vektory, ktoré sa transformujú tým istým charakteristickým číslom, môžu byť lineárne závislé i lineárne nezávislé. Dokážeme, že charakteristické vektory prislúchajúce rôznym charakteristickým číslam sú vždy lineárne nezávislé.

Veta 4.4. *Nech $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\dots,\boldsymbol{\alpha}_k$ sú charakteristické vektory lineárnej transformácie $\varphi:\boldsymbol{V}(F)\to\boldsymbol{V}(F)$, tej vlastnosti, že im odpovedajúce charakteristické hodnoty $\lambda_1,\lambda_2,\dots,\lambda_k$ sú navzájom rôzne. Potom vektory $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\dots,\boldsymbol{\alpha}_k$ sú lineárne nezávislé.*

Dôkaz. Vetu dokážeme matematickou indukciou. Ak $k=1$, veta platí. Nech je veta správna pre $k-1$ vektorov ($k>1$). Predpokladajme nepriamo, že tvrdenie neplatí pre k vektorov, t.j.

$$c_1\boldsymbol{\alpha}_1+c_2\boldsymbol{\alpha}_2+\dots+c_k\boldsymbol{\alpha}_k=\vec{0}, \tag{4.7}$$

---

*) Miesto „charakteristická hodnota" môžeme hovoriť „charakteristické číslo" prípadne „vlastné číslo".

kde napr. $c_1 \neq 0$. Ak na rovnosť (4.7) aplikujeme transformáciu φ, dostaneme

$$c_1\varphi(\boldsymbol{\alpha}_1) + c_2\varphi(\boldsymbol{\alpha}_2) + \cdots + c_k\varphi(\boldsymbol{\alpha}_k) = \vec{0},$$

alebo

$$c_1\lambda_1\boldsymbol{\alpha}_1 + c_2\lambda_2\boldsymbol{\alpha}_2 + \cdots + c_k\lambda_k\boldsymbol{\alpha}_k = \vec{0}. \tag{4.8}$$

Ak rovnicu (4.7) vynásobíme λ_k a odčítame od rovnice (4.8), dostaneme

$$c_1(\lambda_1 - \lambda_k)\boldsymbol{\alpha}_1 + c_2(\lambda_2 - \lambda_k)\boldsymbol{\alpha}_2 + \cdots + c_{k-1}(\lambda_{k-1} - \lambda_k)\boldsymbol{\alpha}_{k-1} = \vec{0}.$$

Keďže $c_1 \neq 0$, $\lambda_1 - \lambda_k \neq 0$, z poslednej rovnosti vyplýva, že $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_{k-1}$ sú lineárne závislé vektory, čo je spor s indukčným predpokladom. $\square$

Dôsledok. *Nech lineárna transformácia φ n-rozmerného vektorového priestoru $\boldsymbol{V}(F)$ má n navzájom rôznych charakteristických hodnôt $\lambda_1, \lambda_2, \ldots, \lambda_n \in F$. Ak príslušné charakteristické vektory vezmeme za bázu priestoru $\boldsymbol{V}(F)$, matica transformácie φ je tvaru*

$$\mathsf{D} = \begin{pmatrix} \lambda_1, & 0, & 0, & \ldots, & 0 \\ 0, & \lambda_2, & 0, & \ldots, & 0 \\ \vdots & & & & \\ 0, & 0, & 0, & \ldots, & \lambda_n \end{pmatrix}. \tag{4.9}$$

Dôkaz. Podľa predchádzajúcej vety sú charakteristické vektory $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_n$ lineárne nezávislé, t.j. možno ich vziať za bázu priestoru $\boldsymbol{V}(F)$. Keďže $\boldsymbol{\varepsilon}_i$ sú charakteristické vektory, platí

$$\begin{aligned} \varphi(\boldsymbol{\varepsilon}_1) &= \lambda_1\boldsymbol{\varepsilon}_1, \\ \varphi(\boldsymbol{\varepsilon}_2) &= \lambda_2\boldsymbol{\varepsilon}_2, \\ &\vdots \\ \varphi(\boldsymbol{\varepsilon}_n) &= \lambda_n\boldsymbol{\varepsilon}_n, \end{aligned}$$

alebo

$$\begin{aligned} \varphi(\boldsymbol{\varepsilon}_i) &= \lambda_1\boldsymbol{\varepsilon}_1 + 0\cdot\boldsymbol{\varepsilon}_2 + \cdots + 0\cdot\boldsymbol{\varepsilon}_n, \\ \varphi(\boldsymbol{\varepsilon}_2) &= 0\cdot\boldsymbol{\varepsilon}_1 + \lambda_2\boldsymbol{\varepsilon}_2 + \cdots + 0\cdot\boldsymbol{\varepsilon}_n, \\ &\vdots \\ \varphi(\boldsymbol{\varepsilon}_n) &= 0\cdot\boldsymbol{\varepsilon}_1 + 0\cdot\boldsymbol{\varepsilon}_2 + \cdots + \lambda_n\boldsymbol{\varepsilon}_n, \end{aligned}$$

čo znamená, že matica lineárnej transformácie φ je tvaru (4.9). $\square$

Príklad 4.8. V príklade 4.6 sme mali lineárnu transformáciu $\psi : \boldsymbol{V}_2(R) \to \boldsymbol{V}_2(R)$ danú maticou

$$\mathbf{B} = \begin{pmatrix} \frac{5}{4} & \frac{3}{4} \\ -\frac{3}{4} & -\frac{5}{4} \end{pmatrix}$$

vzhľadom na bázu $\varepsilon_1 = (1,2)$, $\varepsilon_2 = (1,-2)$. Našli sme jej charakteristické čísla $\lambda_1 = 1, \lambda_2 = -1$ a charakteristické vektory napr. $\boldsymbol{\alpha} = (1,1)$, $\boldsymbol{\beta} = (1,-1)$. Keďže $\lambda_1 \neq \lambda_2$, vektory $\boldsymbol{\alpha}, \boldsymbol{\beta}$ sú lineárne nezávislé. Preto ich môžeme zvoliť za bázu priestoru $\boldsymbol{V}_2(R)$. Podľa dôsledku vety 4.4 matica transformácie ψ vzhľadom na bázu $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ je

$$\mathbf{B}^* = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Skutočne, ľahko vypočítame

$$\boldsymbol{\alpha} = (1,1) = \frac{3}{4} \cdot \boldsymbol{\varepsilon}_1 + \frac{1}{4} \cdot \boldsymbol{\varepsilon}_2$$

$$\boldsymbol{\beta} = (1,-1) = \frac{1}{4} \cdot \boldsymbol{\varepsilon}_1 + \frac{3}{4} \cdot \boldsymbol{\varepsilon}_2$$

Matica prechodu od bázy $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2\}$ k báze $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ a jej inverzná matica je

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

Preto podľa vety 3.3 máme

$$\mathbf{B}^* = \mathbf{P} \cdot \mathbf{B} \cdot \mathbf{P}^{-1} = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{4} \end{pmatrix} \cdot \begin{pmatrix} \frac{5}{4} & \frac{3}{4} \\ -\frac{3}{4} & -\frac{5}{4} \end{pmatrix} \cdot \begin{pmatrix} \frac{3}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{3}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Aby sme si naše úvahy zjednodušili, v ďalšom vždy budeme predpokladať lineárnu transformáciu $\varphi : \boldsymbol{V}_n(F) \to \boldsymbol{V}_n(F)$, t.j. v aritmetickom priestore n-tíc.

Bude účelné, keď vyslovíme nasledujúcu definíciu.

Definícia 4.4. Dve matice $\mathbf{A}, \mathbf{B}$ typu $n \times n$ nad poľom F sú *podobné*, ak existuje regulárna matica $\mathbf{P}$ typu $n \times n$ taká, že $\mathbf{B} = \mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1}$. Hovoríme, že sme maticu $\mathbf{A}$ transformovali (konjugáciou) maticou $\mathbf{P}$ na maticu $\mathbf{B}$.

Keď použijeme pojem podobné matice a vezmeme do úvahy vetu 3.3 dostaneme nasledujúcu vetu.

Veta 4.5. *Dve matice $\mathbf{A}, \mathbf{B}$ typu $n \times n$ nad poľom F reprezentujú tú istú lineárnu transformáciu $\varphi : \boldsymbol{V}_n(F) \to \boldsymbol{V}_n(F)$ práve vtedy keď sú podobné.*

Dôkaz. I. Skutočne ak si v priestore $\boldsymbol{V}_n(F)$ zvolíme bázu M a matica $\mathbf{A}$ reprezentuje transformáciu $\varphi : \boldsymbol{V}_n(F) \to \boldsymbol{V}_n(F)$ vzhľadom na túto bázu, tak táto transformácia bude vzhľadom na inú bázu M' reprezentovaná podľa vety 3.3 maticou $\mathbf{B} = \mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1}$, kde P je matica prechodu od bázy M k báze M'. To znamená: matice $\mathbf{A}, \mathbf{B}$ sú si podobné.

II. Naopak, ak máme dve podobné matice $\mathbf{B} = \mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1}$ a ak si zvolíme nejakú bázu, tak maticou $\mathbf{A}$ bude určená lineárna transformácia $\varphi : \boldsymbol{V}_n(F) \to \boldsymbol{V}_n(F)$. Podľa vety 3.3 ľahko prejdeme pomocou matice $\mathbf{P}$ k novej báze, kde zobrazenie φ bude reprezentované maticou $\mathbf{B}$. $\square$

Dôsledok. *Podobné matice majú rovnaké spektrum.*

Dôkaz vyplýva z vety 4.3 z vety 4.5. □

V istom zmysle najjednoduchšou maticou lineárnej transformácie je diagonálna matica. Je otázka, ktorá lineárna transformácia sa dá reprezentovať diagonálnou maticou.

Veta 4.6. *Matica* $\mathbf{A}$ *typu* $n \times n$ *je podobná diagonálnej matici* $\mathbf{D}$ *práve vtedy, keď charakteristické vektory, ktoré prislúchajú transformácii* φ *vektorového priestoru* $\boldsymbol{V}_n(F)$, *reprezentovanej maticou* $\mathbf{A}$, *generujú celý vektorový priestor* $\boldsymbol{V}_n(F)$.

Dôkaz. Nech $\mathbf{A}$ je matica transformácie φ vzhľadom na nejakú bázu M. Nech vlastné vektory transformácie φ generujú celý priestor $\boldsymbol{V}_n(F)$. Potom z nich možno vybrať novú bázu $\{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \dots, \boldsymbol{\eta}_n\}$. Podobne ako v dôkaze dôsledku vety 4.4 môžeme písať

$$\begin{aligned} \varphi(\boldsymbol{\eta}_1) &= \lambda_1 \boldsymbol{\eta}_1, \\ \varphi(\boldsymbol{\eta}_2) &= \lambda_2 \boldsymbol{\eta}_2, \\ &\vdots \\ \varphi(\boldsymbol{\eta}_n) &= \lambda_n \boldsymbol{\eta}_n, \end{aligned}$$

čiže matica transformácie φ vzhľadom na novú bázu je

$$\mathbf{D} = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$

Podľa vety 4.5 sú matice $\mathbf{A}$ a $\mathbf{D}$ podobné.

II. Naopak, nech $\mathbf{A}$ je podobná nejakej diagonálnej matici $\mathbf{D}$. Predpokladajme, že $\mathbf{A}$ je maticou zobrazenia φ vzhľadom na kanonickú bázu. Potom existuje báza $M = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \dots, \boldsymbol{\eta}_n\}$ taká, že vzhľadom na ňu je φ reprezentovaná maticou $\mathbf{D}$. To ale znamená, že vektory bázy M sú charakteristické vektory.
Naozaj

$$\begin{aligned} \varphi(\boldsymbol{\eta}_1) &= d_1 \boldsymbol{\eta}_1 + 0 \cdot \boldsymbol{\eta}_2 + \dots + 0 \cdot \boldsymbol{\eta}_n = d_1 \boldsymbol{\eta}_1, \\ \varphi(\boldsymbol{\eta}_2) &= 0 \cdot \boldsymbol{\eta}_1 + d_2 \boldsymbol{\eta}_2 + \dots + 0 \cdot \boldsymbol{\eta}_n = d_2 \boldsymbol{\eta}_2, \\ &\vdots \\ \varphi(\boldsymbol{\eta}_n) &= 0 \cdot \boldsymbol{\eta}_1 + 0 \cdot \boldsymbol{\eta}_2 + \dots + d_n \boldsymbol{\eta}_n = d_n \boldsymbol{\eta}_n. \end{aligned}$$

Teda $\mathbf{D}$ je tvaru

$$\mathbf{D} = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & d_n \end{pmatrix}$$

a diagonálne prvky $\mathbf{D}$ sú vlastné hodnoty $\mathbf{D}$ a teda aj $\mathbf{A}$. Keďže báza generuje $\boldsymbol{V}_n(F)$, aj vlastné vektory generujú $\boldsymbol{V}_n(F)$. □

Poznámka 4.4. Ak o matici $\mathbf{A}$ vieme, že je podobná diagonálnej matici, lebo možno vybrať n lineárne nezávislých vlastných vektorov transformácie, ktorú reprezentuje, vzniká otázka, ako určiť maticu prechodu $\mathbf{P}$, ktorá transformuje maticu $\mathbf{A}$ na diagonálnu maticu $\mathbf{D} = \mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1}$. Problém rieši nasledujúci dôsledok predchádzajúcej vety.

Dôsledok vety 4.6. *Nech matica $\mathbf{A}$ je maticou lineárnej transformácie φ (vzhľadom na bázu $M = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$) a nech $M' = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \dots, \boldsymbol{\eta}_n\}$ je báza lineárne nezávislých charakteristických vektorov transformácie φ. Potom maticou prechodu $\mathbf{P}$ od bázy M k báze M' je matica, ktorej riadky sú vektory súradníc vektorov $\boldsymbol{\eta}_i$ vzhľadom na bázu M.*

Dôkaz. Skutočne

$$\begin{aligned}
\boldsymbol{\eta}_1 &= p_{11}\boldsymbol{\varepsilon}_1 + p_{12}\boldsymbol{\varepsilon}_2 + \dots + p_{1n}\boldsymbol{\varepsilon}_n \\
\boldsymbol{\eta}_2 &= p_{21}\boldsymbol{\varepsilon}_1 + p_{22}\boldsymbol{\varepsilon}_2 + \dots + p_{2n}\boldsymbol{\varepsilon}_n \\
&\vdots \\
\boldsymbol{\eta}_n &= p_{n1}\boldsymbol{\varepsilon}_1 + p_{n2}\boldsymbol{\varepsilon}_2 + \dots + p_{nn}\boldsymbol{\varepsilon}_n,
\end{aligned}$$

čiže

$$\begin{pmatrix} \boldsymbol{\eta}_1 \\ \boldsymbol{\eta}_2 \\ \vdots \\ \boldsymbol{\eta}_n \end{pmatrix} = \mathbf{P} \cdot \begin{pmatrix} \boldsymbol{\varepsilon}_1 \\ \boldsymbol{\varepsilon}_2 \\ \vdots \\ \boldsymbol{\varepsilon}_n \end{pmatrix}.$$

(Porovnaj s (2.3) v kapitole 3.) Potom podľa vety 3.3 máme $\mathbf{D} = \mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1}$. $\square$

Iný dôkaz. Vektory súradníc vektorov $\boldsymbol{\eta}_i$ transformujme maticou $\mathbf{A}$. Dostaneme vektory súradníc vektorov $\varphi(\boldsymbol{\eta}_i)$. Keďže platí $\varphi(\boldsymbol{\eta}_i) = d_i\boldsymbol{\eta}_i$, kde d_i je vlastné číslo prislúchajúce vektoru $\boldsymbol{\eta}_i$, máme

$$\begin{pmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ \vdots & & \ddots & \\ p_{n1} & p_{n2} & \dots & p_{nn} \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & \ddots & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} =$$

$$= \begin{pmatrix} d_1p_{11} & d_1p_{12} & \dots & d_1p_{1n} \\ d_2p_{21} & d_2p_{22} & \dots & d_2p_{2n} \\ \vdots & & \ddots & \\ d_np_{n1} & d_np_{n2} & \dots & d_np_{nn} \end{pmatrix} =$$

$$= \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & d_n \end{pmatrix} \cdot \begin{pmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ \vdots & & \ddots & \\ p_{n1} & p_{n2} & \dots & p_{nn} \end{pmatrix}.$$

Vidieť, že $\mathbf{P} \cdot \mathbf{A} = \mathbf{D} \cdot \mathbf{P}$.
Keďže riadky matice P sú vektory súradníc lineárne nezávislých vektorov $\boldsymbol{\eta}_i$, je matica P regulárna a máme $\mathbf{D} = \mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1}$. $\square$

Poznámka 4.5. Vo vete 4.4 sme dokázali, že ak sú všetky vlastné hodnoty matice $\mathbf{A}$ navzájom rôzne, vlastné vektory k nim prislúchajúce sú nezávislé, tvoria bázu a podľa dôsledku tejto vety i podľa vety 4.5 je matica $\mathbf{A}$ podobná diagonálnej matici. Podmienka vzájomnej rôznosti vlastných hodnôt matice $\mathbf{A}$ nie je podmienkou nevyhnutnou. Ako ukazuje nasledujúci príklad, n lineárne nezávislých vektorov možno (niekedy) vybrať aj v tom prípade, keď vlastné hodnoty nie sú navzájom rôzne.

Príklad 4.9. V príklade 4.7 sme skúmali transformáciu

$$\varphi : \boldsymbol{V}_3(R) \to \boldsymbol{V}_3(R)$$

danú (vzhľadom na kanonickú bázu) maticou

$$\mathbf{A} = \begin{pmatrix} 3 & -1 & 3 \\ 2 & 0 & 6 \\ 3 & -3 & 11 \end{pmatrix}.$$

Vypočítali sme jej vlastné hodnoty $\lambda_1 = 2, \lambda_2 = 2, \lambda_3 = 10$. Našli sme dva lineárne nezávislé (!) vektory

$$\begin{aligned} \boldsymbol{\alpha} &= (-2, 1, 0) \\ \boldsymbol{\beta} &= (-3, 0, 1) \end{aligned}$$

prislúchajúce vlastnému číslu 2 a ďalší vektor

$$\boldsymbol{\gamma} = (1, -1, 3)$$

prislúchajúci vlastnému číslu 10. Ako sa možno ľahko presvedčiť, tieto tri charakteristické vektory sú lineárne nezávislé a teda generujú celý priestor $\boldsymbol{V}_3(R)$. Preto ak ich vezmeme za bázu, matica transformácie φ bude

$$\mathbf{D} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 10 \end{pmatrix}.$$

Presvedčíme sa o tom. Keďže $\mathbf{A}$ je maticou transformácie φ vzhľadom na kanonickú bázu, máme

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

a ako čitateľ vypočíta je

$$\mathbf{P}^{-1} = \begin{pmatrix} \frac{1}{8} & -\frac{3}{8} & \frac{1}{8} \\ \frac{10}{8} & -\frac{6}{8} & \frac{2}{8} \\ \frac{3}{8} & -\frac{1}{8} & \frac{3}{8} \end{pmatrix}.$$

Dostávame tak

$$\mathbf{D} = \mathbf{P} \cdot \mathbf{A} \cdot \mathbf{P}^{-1} = \begin{pmatrix} -2 & 1 & 0 \\ -3 & 0 & 1 \\ 1 & -1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & -1 & 3 \\ 2 & 0 & 6 \\ 3 & -3 & 11 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{8} & -\frac{3}{8} & \frac{1}{8} \\ \frac{10}{8} & -\frac{6}{8} & \frac{2}{8} \\ \frac{3}{8} & -\frac{1}{8} & \frac{3}{8} \end{pmatrix} =$$

$$= \begin{pmatrix} -4 & 2 & 0 \\ -6 & 0 & 2 \\ 10 & -10 & 30 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{8} & -\frac{3}{8} & \frac{1}{8} \\ \frac{10}{8} & -\frac{6}{8} & \frac{2}{8} \\ \frac{3}{8} & -\frac{1}{8} & \frac{3}{8} \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 10 \end{pmatrix}.$$

Príklad 4.10. V príklade 4.5 sme mali maticu transformácie φ vo $\boldsymbol{V}_2(R)$

$$\mathbf{A} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{4.10}$$

ktorej charakteristická rovnica je

$$\lambda^2 + 1 = 0. \tag{4.11}$$

Jej korene $\lambda_1 = i$, $\lambda_2 = -i$ sú vlastné čísla transformácie. Transformácia vôbec nemá jednorozmerný invariantný priestor. Matica nie je podobná diagonálnej matici nad R. Inak je to nad poľom komplexných čísel C. Majme na mysli transformáciu $\varphi : \boldsymbol{V}_2(C) \to \boldsymbol{V}_2(C)$, ktorej matica vzhľadom na kanonickú bázu je (4.10) a charakteristická rovnica (4.11). Vypočítame jej charakteristické vektory. Keďže $\mathbf{A} - \lambda \mathbf{J}_2 = \begin{pmatrix} -\lambda & 1 \\ -1 & -\lambda \end{pmatrix}$, pre $\lambda_1 = i$ máme sústavu rovníc:

$$\begin{aligned} -ix - y &= 0, \\ x - iy &= 0, \end{aligned}$$

po úprave

$$\begin{aligned} x - iy &= 0, \\ x - iy &= 0. \end{aligned}$$

Podpriestor riešení danej sústavy je $\boldsymbol{S} = \{(ip, p);\ p \in C\}$. Nakoľko máme kanonickú bázu, tento podpriestor je zároveň jednorozmerným invariantným podpriestorom transformácie φ. Vlastný vektor je napr. $\boldsymbol{\alpha} = (i, 1)$. Vidieť, že $\boldsymbol{S} = [(i, 1)]$.

Sústava rovníc pre $\lambda_2 = -i$ je

$$\begin{aligned} ix - y &= 0, \\ x + iy &= 0, \end{aligned}$$

po úprave

$$\begin{aligned} x + iy &= 0, \\ x + iy &= 0. \end{aligned}$$

Podpriestor riešení danej sústavy je $\boldsymbol{T} = \{(-ip, p);\ p \in C\}$, ktorý podobne ako vyššie je zároveň jednorozmerným invariantným podpriestorom transformácie φ. Vlastný vektor je napr. $\boldsymbol{\beta} = (-i, 1)$ a tiež $\boldsymbol{T} = [(-i, 1)]$.

Čitateľ skontroluje, že

$$\varphi(\boldsymbol{\alpha}) = (i, 1) \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (-1, i) = i(i, 1) = i\boldsymbol{\alpha}.$$

Teda vektor $\boldsymbol{\alpha}$ sa naozaj transformuje pomocou vlastnej hodnoty $\lambda_1 = i$. Podobne aj $\varphi(\boldsymbol{\beta}) = -i\boldsymbol{\beta}$. Keďže vlastné čísla sú rôzne, vlastné vektory α, β, sú lineárne nezávislé, teda tvoria bázu priestoru $\boldsymbol{V}_2(C)$. Keď kanonickú bázu označíme ako obyčajne $\{\varepsilon_1, \varepsilon_2\}$, vidíme, že

$$\begin{aligned} \alpha &= i \cdot \varepsilon_1 + 1 \cdot \varepsilon_2, \\ \beta &= -i \cdot \varepsilon_1 + 1 \cdot \varepsilon_2. \end{aligned}$$

Preto matica prechodu od bázy $\{\varepsilon_1, \varepsilon_2\}$, k báze $\{\alpha, \beta\}$, je

$$\mathbf{P} = \begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix}$$

a jej inverzná matica

$$\mathbf{P}^{-1} = \frac{1}{2i} \begin{pmatrix} 1 & -1 \\ i & i \end{pmatrix} = \begin{pmatrix} -\frac{i}{2} & \frac{i}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Podľa vety 2.4 matica transformácie φ vzhľadom na bázu $\{\alpha, \beta\}$ je

$$\mathbf{D} = \begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -\frac{i}{2} & \frac{i}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} -1 & i \\ -1 & -i \end{pmatrix} \cdot \begin{pmatrix} -\frac{i}{2} & \frac{i}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Vidieť, že v súlade s dôsledkom vety 4.4 ide o diagonálnu maticu majúcu na hlavnej diagonále vlastné čísla.

Matica $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ nebola podobná diagonálnej matici nad R ale nad C už je podobná matici $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. V nasledujúcom príklade uvedieme maticu, čo nie je (vôbec) podobná diagonálnej matici.

Príklad 4.11. Skúmajme maticu

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

transformácie $\varphi : \boldsymbol{V}_2(R) \to \boldsymbol{V}_2(R)$, vzhľadom na kanonickú bázu. Charakteristická rovnica

$$\begin{vmatrix} 1-\lambda & 2 \\ 0 & 1-\lambda \end{vmatrix} = 0$$

čiže

$$(1-\lambda)^2 = 0$$

má dvojnásobný koreň $\lambda_1 = \lambda_2 = 1$.

Sústava pre vlastný vektor

$$0 \cdot x + 0 \cdot y = 0$$
$$2 \cdot x + 0 \cdot y = 0$$

má podpriestor riešení $\boldsymbol{S} = \{(0,p);\ p \in R\}$, ktorý je pri kanonickej báze aj invariantným podpriestorom našej transformácie. Generuje ho napríklad vlastný vektor $\boldsymbol{\alpha} = (0,1)$. Vidieť, že všetky vlastné vektory sú násobky $\boldsymbol{\alpha}$. Nenájdeme dva lineárne nezávislé vlastné vektory. Matica nie je podobná diagonálnej matici.

Ako sme už poznamenali vyššie, existujú lineárne transformácie reálnych vektorových priestorov, ktoré nemajú jednorozmerný invariantný podpriestor. Také bolo napríklad zobrazenie z príkladu 4.10. Je jasné, že lineárna transformácia priestoru $\boldsymbol{V}_n(R)$ nemá jednorozmerný podpriestor práve vtedy, keď jej charakteristický polynóm $|\mathbf{A} - \lambda \mathbf{J}_n|$ nemá reálne korene. Platí nasledujúca veta.

Veta 4.7. *Lineárna transformácia $\varphi : \boldsymbol{V}_n(R) \to \boldsymbol{V}_n(R)$ má vždy jednorozmerný alebo dvojrozmerný invariantný podpriestor.*

Dôkaz. Nech $\mathbf{A}$ je matica transformácie φ vzhľadom na nejakú (napr. kanonickú) bázu. Ak má polynóm $|\mathbf{A} - \lambda \mathbf{J}_n|$ reálny koreň, tak vlastný vektor $\boldsymbol{\alpha}$ patriaci tomu koreňu generuje jednorozmerný invariantný podpriestor $[\boldsymbol{\alpha}]$.

Zostáva uvážiť prípad, keď charakteristický polynóm má len komplexné korene. Nech $\lambda_0 = r + si$ je taký koreň pričom $s \neq 0$. Ak napíšeme sústavu rovníc (4.4) pre tento koreň máme

$$\begin{aligned}
a_{11}x_1 + a_{21}x_2 + \cdots + a_{n1}x_n &= (r+si)\cdot x_1\\
a_{12}x_1 + a_{22}x_2 + \cdots + a_{n2}x_n &= (r+si)\cdot x_2\\
&\ \vdots\\
a_{1n}x_1 + a_{2n}x_2 + \cdots + a_{nn}x_n &= (r+si)\cdot x_n
\end{aligned}$$

Táto homogénna sústava má aspoň jedno nenulové (!) riešenie nad poľom komplexných čísel. Nech je to napr. n-tica

$$(4.12) \qquad (u_1 + v_1 i, u_2 + v_2 i, \ldots, u_n + v_n i),$$

v ktorej aspoň jedno $v_i \neq 0$. Ak ju dosadíme do sústavy, máme

$$(u_1 + v_1 i, u_2 + v_2 i, \ldots, u_n + v_n i) \cdot \mathbf{A} = (r+si)(u_1 + v_1 i, u_2 + v_2 i, \ldots, u_n + v_n i).$$

V poslednej rovnici oddelíme reálnu a imaginárnu časť. Tak máme

$$\begin{aligned}
(u_1, u_2, \ldots, u_n)\cdot \mathbf{A} = (ru_1 - sv_1, ru_2 - sv_2, \ldots, ru_n - sv_n) &=\\
= r(u_1, u_2, \ldots, u_n) - s(v_1, v_2, \ldots, v_n)&
\end{aligned}$$

a

$$\begin{aligned}
(v_1, v_2, \ldots, v_n)\mathbf{A} = (rv_1 + su_1, rv_2 + su_2, \ldots, rv_n + su_n) &=\\
= r(v_1, v_2, \ldots, v_n) + s(u_1, u_2, \ldots, u_n).&
\end{aligned}$$

Označme $\boldsymbol{\alpha} = (u_1, u_2, \ldots, u_n)$ a $\boldsymbol{\beta} = (v_1, v_2, \ldots, v_n)$. Vidieť, že $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{V}_n(R)$. Posledné rovnice vlastne hovoria, že obrazy daných vektorov sú

$$\begin{aligned} \varphi(\boldsymbol{\alpha}) &= r\boldsymbol{\alpha} - s\boldsymbol{\beta} \\ \varphi(\boldsymbol{\beta}) &= r\boldsymbol{\beta} + s\boldsymbol{\alpha} \end{aligned} \tag{4.13}$$

Dokážeme, že vektory $\boldsymbol{\alpha}, \boldsymbol{\beta}$ sú lineárne nezávislé.

Skutočne, ihneď vidíme, že $\boldsymbol{\beta} \neq \vec{0}$, lebo v opačnom prípade by n-tica (4.12) pozostávala z reálnych čísel, čo by znamenalo, že reálny vektor by sa transformoval pomocou komplexného vlastného čísla λ_0, čo nie je možné. Ak by vektory $\boldsymbol{\alpha}, \boldsymbol{\beta}$ boli závislé bolo by $\boldsymbol{\alpha} = c\boldsymbol{\beta}$. Potom z (4.13) máme

$$\begin{aligned} \varphi(c\boldsymbol{\beta}) &= rc\boldsymbol{\beta} - s\boldsymbol{\beta}, \\ \varphi(\boldsymbol{\beta}) &= r\boldsymbol{\beta} + sc\boldsymbol{\beta}. \end{aligned}$$

Ak druhú rovnicu vynásobíme číslom c a použijeme $\varphi(c\beta) = c\varphi(\beta)$, dostaneme

$$\begin{aligned} c\varphi(\boldsymbol{\beta}) &= rc\boldsymbol{\beta} - s\boldsymbol{\beta}, \\ c\varphi(\boldsymbol{\beta}) &= rc\boldsymbol{\beta} + sc^2\boldsymbol{\beta}, \end{aligned}$$

odkiaľ $s\boldsymbol{\beta} = -sc^2\boldsymbol{\beta}$, čiže $s(1+c^2)\boldsymbol{\beta} = \vec{0}$. Keďže $s \neq 0$, $1 + c^2 \neq 0$, máme $\boldsymbol{\beta} = \vec{\mathbf{0}}$, čo je spor s tým, že $\boldsymbol{\beta} \neq \vec{0}$. Zo (4.13) ale vyplýva, že $\varphi(\boldsymbol{\alpha}), \varphi(\boldsymbol{\beta}) \in [\boldsymbol{\alpha}, \boldsymbol{\beta}]$, teda $\boldsymbol{\alpha}, \boldsymbol{\beta}$ generujú invariantný podpriestor dimenzie 2. (Pozor, $\boldsymbol{\alpha}, \boldsymbol{\beta}$ nie sú vlastné vektory!) Tým je dôkaz skončený. □

Poznámka 4.6. Príklad 4.7 ukazuje, že invariantný podpriestor lineárnej transformácie $\boldsymbol{V}_n(R)$ dimenzie dva môžu generovať aj dva lineárne nezávislé vlastné vektory prislúchajúce tomu istému reálnemu vlastnému číslu, v tomto prípade číslu 2.

Naozaj, ľahko zistíme, že podpriestor

$$\boldsymbol{S} = \{(-2p - 3p, p, q); p, q \in R\} = [(-2, 1, 0), (-3, 0, 1)]$$

je invariantný podpriestor dimenzie dva.

Nasledujúci príklad ilustruje vetu 4.7.

Príklad 4.12. Nech je daná transformácia $\varphi : \boldsymbol{V}_4(R) \to \boldsymbol{V}_4(R)$ nasledujúcou maticou (vzhľadom na kanonickú bázu).

$$\mathbf{A} = \begin{pmatrix} -1 & 2 & -1 & 7 \\ -1 & 1 & 1 & -2 \\ 0 & 0 & 0 & 5 \\ 0 & 0 & -1 & 4 \end{pmatrix}.$$

Určíme charakteristický polynóm a vlastné čísla matice. Zistíme či existuje jednorozmerný invariantný podpriestor; ak nie, určíme dvojrozmerný. Počítame

$$P(\lambda) = \begin{vmatrix} -1-\lambda & 2 & -1 & 7 \\ -1 & 1-\lambda & 1 & -2 \\ 0 & 0 & -\lambda & 5 \\ 0 & 0 & -1 & 4-\lambda \end{vmatrix} =$$

$$= (-1-\lambda)\begin{vmatrix} 1-\lambda & 1 & -2 \\ 0 & -\lambda & 5 \\ 0 & -1 & 4-\lambda \end{vmatrix} + \begin{vmatrix} 2 & -1 & 7 \\ 0 & -\lambda & 5 \\ 0 & -1 & 4-\lambda \end{vmatrix} =$$

$$= -(1+\lambda)\cdot(1-\lambda)(\lambda^2-4\lambda+5) + 2(\lambda^2-4\lambda+5) =$$

$$= (\lambda^2-4\lambda+5)\cdot(\lambda^2+1) = \lambda^4-4\lambda^3+6\lambda^2-4\lambda+5.$$

Keďže v priebehu výpočtu sme polynóm $P(\lambda)$ mali rozložený na súčin dvoch kvadratických polynómov $P(\lambda) = (\lambda^2-4\lambda+5)\cdot(\lambda^2+1)$, jeho korene ľahko vypočítame:

$$\lambda_1 = i, \quad \lambda_2 = -i, \quad \lambda_3 = 2+i, \quad \lambda_4 = 2-i.$$

Vidieť, že charakteristický polynóm nemá reálny koreň. To znamená zobrazenie φ nemá jednorozmerný invariantný podpriestor. Určíme dvojrozmerný invariantný podpriestor určený vlastným číslom, napr. $\lambda_3 = 2+i$. Vidíme, že $r = 2$, $s = 1 \neq 0$.

Napíšeme sústavu rovníc (4.4) pre koreň λ_3.

$$\begin{aligned} -x_1 - x_2 &= (2+i)x_1, \\ 2x_1 + x_2 &= (2+i)x_2, \\ -x_1 + x_2 - x_4 &= (2+i)x_3, \\ 7x_1 - 2x_2 + 5x_3 + 4x_4 &= (2+i)x_4, \end{aligned}$$

po úprave

$$\begin{aligned} (-3-i)x_1 - x_2 &= 0, \\ 2x_1 + (-1-i)x_2 &= 0, \\ -x_1 + x_2 + (-2-i)x_3 - x_4 &= 0, \\ 7x_1 - 2x_2 + 5x_3 + (2-i)x_4 &= 0. \end{aligned}$$

Vidieť, že možno riešiť prvé dve rovnice zvlášť. Keď prvú vynásobíme dvoma a druhú komplexným číslom $3+i$, dostaneme

$$\begin{aligned} 2(-3-i)x_1 - 2x_2 &= 0, \\ 2(3+i)x_1 + (-2-4i)x_2 &= 0, \end{aligned}$$

odkiaľ vychádza $x_1 = 0$, $x_2 = 0$. Dosadením do 3. a 4. rovnice máme

$$\begin{aligned} (-2-i)x_3 - x_4 &= 0, \\ 5x_3 + (2-i)x_4 &= 0, \end{aligned}$$

Po vynásobení prvej rovnice číslom $-2+i$, dostaneme dve rovnaké rovnice

$$\begin{aligned} 5x_3 + (2-i)x_4 &= 0, \\ 5x_3 + (2-i)x_4 &= 0. \end{aligned}$$

Podpriestor riešení danej sústavy je $\boldsymbol{S} = \{(0,0,\frac{i-2}{5}p,p);\ p \in R\}$ Nájdeme jedno nenulové riešenie, napr. pre $p = 5$

$$(0+0i,\ 0+0i,\ -2+i,\ 5+0i)$$

Podľa úvahy v dôkaze vety 4.7 vektory $\boldsymbol{\alpha} = (0,0,-2,5)$ a $\boldsymbol{\beta} = (0,0,1,0)$ sú lineárne nezávislé a generujú dvojrozmerný invariantný podpriestor

$$[\boldsymbol{\alpha},\boldsymbol{\beta}] = \{x\boldsymbol{\alpha} + y\boldsymbol{\beta};\ x,y \in R\} = \{x(0,0,-2,5) + y(0,0,1,0);\ x,y \in R\} = \\ = \{(0,0,-2x+y,5x);\ x,y \in R\}.$$

Ďalej, podľa (4.13) platí

$$\varphi(\boldsymbol{\alpha}) = 2\boldsymbol{\alpha} - \boldsymbol{\beta} = (0,0,-4,10) - (0,0,1,0) = (0,0,-5,10),$$

$$\varphi(\boldsymbol{\beta}) = 2\boldsymbol{\beta} + \boldsymbol{\alpha} = (0,0,2,0) + (0,0,-2,5) = (0,0,0,5).$$

Keďže matica transformácie je vzhľadom na kanonickú bázu, môžeme vektory priamo transformovať pomocou matice

$$\varphi(\boldsymbol{\alpha}) = (0,0,-2,5)\begin{pmatrix} -1 & 2 & -1 & 7 \\ -1 & 1 & 1 & -2 \\ 0 & 0 & 0 & 5 \\ 0 & 0 & -1 & 4 \end{pmatrix} = (0,0,-5,10).$$

Podobne dostaneme $\varphi(\boldsymbol{\beta}) = (0,0,1,0) \cdot A = (0,0,0,5)$. Vykonali sme tak kontrolu výsledku. Prosíme čitateľa, aby si overil, že pre koreň $\lambda_4 = 2 - i$ dostaneme ten istý podpriestor. Ďalší invariantný podpriestor by sme mohli určiť pre korene $\lambda_1 = i$ resp. $\lambda_2 = -i$.

V nasledujúcich úvahách zistíme, aký je význam koeficientov charakteristického polynómu danej matice $\mathbf{A}$ (typu $n \times n$ nad poľom F). Charakteristický polynóm je tvaru

$$f(\lambda) = \begin{vmatrix} a_{11}-\lambda & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22-\lambda} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33}-\lambda & \dots & a_{3n} \\ \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn}-\lambda \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11}-\lambda & a_{12}-0 & a_{13}-0 & \dots & a_{1n}-0 \\ a_{21}-0 & a_{22}-\lambda & a_{23}-0 & \dots & a_{2n}-0 \\ a_{31}-0 & a_{32}-0 & a_{33}-\lambda & \dots & a_{3n}-0 \\ \vdots \\ a_{n1}-0 & a_{n2}-0 & a_{n3}-0 & \dots & a_{nn}-\lambda \end{vmatrix}.$$

Vidíme, že polynóm môžeme písať ako súčet 2^n determinantov, z ktorých prvý bude mať všetky stĺpce len z „pravých“ členov, ďalších $n = \binom{n}{n-1}$ determinantov bude mať $n-1$ stĺpcov z „pravých“ členov, ďalších $\binom{n}{2} = \binom{n}{n-2}$ determinantov bude mať $(n-2)$ stĺpcov z „pravých“ členov, $\dots$, $\binom{n}{n-k} = \binom{n}{k}$ determinantov bude mať (každý z nich) k stĺpcov z „pravých" členov, $\ldots, 1 = \binom{n}{0}$ determinant bude mať všetky stĺpce len z „ľavých" členov, tento bude rovný $d(\mathbf{A})$.

Pozrime sa na jeden z determinantov, nazvime ho hoci D_s, majúci k stĺpcov z pravých členov a teda $n-k$ stĺpcov z ľavých členov. Tieto „ľavé" stĺpce sú vlastne stĺpce matice $\mathbf{A}$. Takýchto determinantov bude $\binom{n}{k}$, teda $s = 1, 2, \ldots, \binom{n}{k}$.

Napríklad ak $n = 7$, $k = 3$ a vyberieme napr. druhý, piaty a šiesty stĺpec, dostaneme nasledujúci determinant D_s, kde s je niektoré z čísel $1, 2, \ldots, 35$.

$$D_s = \begin{vmatrix} a_{11} & 0 & a_{13} & a_{14} & 0 & 0 & a_{17} \\ a_{21} & -\lambda & a_{23} & a_{24} & 0 & 0 & a_{27} \\ a_{31} & 0 & a_{33} & a_{34} & 0 & 0 & a_{37} \\ a_{41} & 0 & a_{43} & a_{44} & 0 & 0 & a_{47} \\ a_{51} & 0 & a_{53} & a_{54} & -\lambda & 0 & a_{57} \\ a_{61} & 0 & a_{63} & a_{64} & 0 & -\lambda & a_{67} \\ a_{71} & 0 & a_{73} & a_{74} & 0 & 0 & a_{77} \end{vmatrix}.$$

Ak postupne rozvinieme determinant D_s podľa k stĺpcov z „pravých" členov, označme ich napr. $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}$, dostaneme

$$(-\lambda)^k \cdot M_s^{(n-k)},$$

kde symbol $M_s^{(n-k)}$ označuje „zvyšný" determinant, ktorý zostane po rozvinutí determinantu D podľa k stĺpcov. V našom príklade to bude

$$D_s = (-\lambda)^3 \cdot \begin{vmatrix} a_{11} & a_{13} & a_{14} & a_{17} \\ a_{31} & a_{33} & a_{34} & a_{37} \\ a_{41} & a_{43} & a_{44} & a_{47} \\ a_{71} & a_{73} & a_{74} & a_{77} \end{vmatrix} = (-\lambda)^3 \cdot M_s^{(7-3)}.$$

Ako vidíme na príklade determinant $M_s^{(n-k)}$ pozostáva z tých prvkov matice $\mathbf{A}$, ktoré zostanú po vyčiarknutí stĺpcov $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}$ a riadkov s tými istými indexami $\varrho_{i_1}, \varrho_{i_2} \ldots, \varrho_{i_k}$. Takýto subdeterminant nazývame hlavný minor matice $\mathbf{A}$ $(n-k)$-teho rádu.
Ak tento výpočet prevedieme v každom determinante D_s a spoločný činiteľ $(-\lambda)^k$ vyložíme pred zátvorku, dostaneme:

$$(-\lambda)^k (M_1^{(n-k)} + M_2^{(n-k)} + \cdots + M_{\binom{n}{k}}^{(n-k)}).$$

Súčet $\binom{n}{k}$ hlavných minorov označme c_k; dostaneme tým nasledujúci člen polynómu $f(\lambda)$

$$(-\lambda)^k (M_1^{(n-k)} + M_2^{(n-k)} + \cdots + M_{\binom{n}{k}}^{(n-k)}) = c_k(-\lambda)^k.$$

Ak vyššie uvedenú úvahu vykonáme pre $k = n, n-1, \ldots, 1, 0$, dostaneme charakteristický polynóm:

$$f(\lambda) = (-\lambda)^n + c_{n-1}(-\lambda)^{n-1} + c_{n-2}(-\lambda)^{n-2} + \cdots + c_k(-\lambda)^k + \cdots + c_1(-\lambda) + d(\mathbf{A}),$$

kde c_{n-1} je súčet hlavných minorov 1. stupňa t.j. prvkov matice $\mathbf{A}$ na jej hlavnej diagonále. Tento súčet sa nazýva *stopa matice*. Ďalej, c_{n-2} je súčet hlavných minorov 2. stupňa, ..., až posledný determinant má stĺpce len z „ľavých“ členov a teda je rovný $\mathrm{d}(\mathbf{A})$.

Charakteristický polynóm zvykneme písať v nasledujúcej forme

$$f(\lambda) = (-1)^n(\lambda^n - c_{n-1}\lambda^{n-1} + c_{n-2}\lambda^{n-2} + \cdots + (-1)^{n-1}c_1\lambda + (-1)^n \mathrm{d}(\mathbf{A})).$$

Nech $\lambda_1, \lambda_2, \ldots, \lambda_n$ sú korene polynómu $f(\lambda)$, vieme, že súčet týchto koreňov je záporne vzatý koeficient pri člene so stupňom $(n-1)$, teda platí $\lambda_1 + \lambda_2 + \cdots + \lambda_n = c_{n-1}$. Vidíme, že súčet charakteristických hodnôt je rovný stope matice.

Príklad 4.13. Uvažujme maticu

$$A = \begin{pmatrix} 1 & -1 & 2 \\ -2 & 0 & 4 \\ -1 & -1 & 4 \end{pmatrix}.$$

Jej vlastné hodnoty sú $\lambda_1 = 1, \lambda_2 = 2, \lambda_3 = 2$.
Pre súčet vlastných hodnôt platí $\lambda_1 + \lambda_2 + \lambda_3 = 1 + 2 + 2 = 5$ a stopa matice sa rovná súčtu prvkov na hlavnej diagonále, teda $1 + 0 + 4 = 5$.
Vidíme, že naozaj súčet vlastných hodnôt sa rovná stope matice.

Príklad 4.14. Postup výpočtu charakteristického polynómu si ukážeme na jeho výpočte pre maticu typu 3×3, pričom bude vidieť význam koeficientov.

$$f(\lambda) = \begin{vmatrix} a_{11}-\lambda & a_{12} & a_{13} \\ a_{21} & a_{22}-\lambda & a_{23} \\ a_{31} & a_{32} & a_{33}-\lambda \end{vmatrix} = \begin{vmatrix} a_{11}-\lambda & a_{12}-0 & a_{13}-0 \\ a_{21}-0 & a_{22}-\lambda & a_{23}-0 \\ a_{31}-0 & a_{32}-0 & a_{33}-\lambda \end{vmatrix} =$$

$$= \begin{vmatrix} -\lambda & 0 & 0 \\ 0 & -\lambda & 0 \\ 0 & 0 & -\lambda \end{vmatrix} + \begin{vmatrix} a_{11} & 0 & 0 \\ a_{21} & -\lambda & 0 \\ a_{31} & 0 & -\lambda \end{vmatrix} + \begin{vmatrix} -\lambda & a_{12} & 0 \\ 0 & a_{22} & 0 \\ 0 & a_{32} & -\lambda \end{vmatrix} + \begin{vmatrix} -\lambda & 0 & a_{13} \\ 0 & -\lambda & a_{23} \\ 0 & 0 & a_{33} \end{vmatrix} +$$

$$+ \begin{vmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & -\lambda \end{vmatrix} + \begin{vmatrix} a_{11} & 0 & a_{13} \\ a_{21} & -\lambda & a_{23} \\ a_{31} & 0 & a_{33} \end{vmatrix} + \begin{vmatrix} -\lambda & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} =$$

$$= -\lambda^3 + \lambda^2(a_{11} + a_{22} + a_{33}) - \lambda \left(\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} \right) + \mathrm{d}(\mathbf{A}) =$$

$$= (-1)^3 \left(\lambda^3 - \lambda^2(a_{11} + a_{22} + a_{33}) + \lambda \left(\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} \right) - \mathrm{d}(\mathbf{A}) \right) =$$

$$= (-1)^3(\lambda^3 - c_2\lambda^2 + c_1\lambda - \mathrm{d}(\mathbf{A})).$$

Poznámka 4.7. Majme na mysli štvorcovú maticu typu $n \times n$ nad poľom F, ktorej prvky sú polynómy v neurčitej λ stupňa najviac m-tého nad tým istým poľom. Označme ju $\mathbf{C}(\lambda)$ a zvykneme nazývať λ-maticou.(Pozri [5, str. 158].) Potom je zrejmé, že ju môžeme písať vo forme

$$\mathbf{C}(\lambda) = \mathbf{C}_0 + \mathbf{C}_1\lambda + \cdots + \mathbf{C}_m\lambda^m,$$

kde $\mathbf{C}_i$ sú matice typu $n \times n$ nad F Napr.

$$\begin{pmatrix} 2\lambda^2 + 3\lambda - 2 & \lambda + 5 \\ \lambda^2 - 7 & \lambda^2 + \lambda - 3 \end{pmatrix} = \begin{pmatrix} -2 & 5 \\ -7 & -3 \end{pmatrix} + \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix}\lambda + \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}\lambda^2.$$

Definícia 4.5. Nech

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

je nejaký polynóm nad F. Nech $\mathbf{A}$ je štvorcová matica typu $n \times n$ nad F. Potom výraz

$$f(\mathbf{A}) = a_m\mathbf{A}^m + a_{m-1}\mathbf{A}^{m-1} + \cdots + a_1\mathbf{A} + a_0\mathbf{J}_n$$

nazývame *polynóm matice* $\mathbf{A}$.

Veta 4.8 (Cayleyho - Hamiltonova). *Nech* $\mathbf{A}$ *je štvorcová matica typu* $n \times n$ *nad poľom* F. *Ďalej nech* $P(\lambda)$ *je charakteristický polynóm matice* $\mathbf{A}$. *Potom* $P(\mathbf{A}) = \mathbf{0}_n$.

Dôkaz. Najprv poznamenajme, že

$$P(\lambda) = |\mathbf{A} - \lambda\mathbf{J}_n| = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$$

je charakteristický polynóm matice $\mathbf{A}$.

K matici $(\mathbf{A} - \lambda\mathbf{J}_n)$ zostrojíme maticu $\mathbf{C}(\lambda)$ tak, že jej prvok $c_{ik}(\lambda)$ je algebraický doplnok patriaci k prvku stojacemu v k-tom riadku a i-tom stĺpci v matici $(\mathbf{A} - \lambda\mathbf{J}_n)$. Je jasné, že $c_{ik}(\lambda)$ je polynóm v neurčitej λ stupňa najviac $n-1$. Keďže

$$(\mathbf{A} - \lambda\mathbf{J}_n)^{-1} = \frac{1}{|\mathbf{A} - \lambda\mathbf{J}_n|} \cdot \mathbf{C}(\lambda),$$

je aj

$$(\mathbf{A} - \lambda\mathbf{J}_n) \cdot \frac{1}{|\mathbf{A} - \lambda\mathbf{J}_n|} \cdot \mathbf{C}(\lambda) = \mathbf{J}_n,$$

čiže

$$(\mathbf{A} - \lambda\mathbf{J}_n) \cdot \mathbf{C}(\lambda) = |\mathbf{A} - \lambda\mathbf{J}_n| \cdot \mathbf{J}_n,$$

alebo

$$P(\lambda) \cdot \mathbf{J}_n = (\mathbf{A} - \lambda\mathbf{J}_n)\mathbf{C}(\lambda), \tag{4.14}$$

Vidíme, že súčin matice $\mathbf{A} - \lambda\mathbf{J}_n$ a matice $\mathbf{C}(\lambda)$ je diagonálna matica majúca všetky prvky hlavnej diagonály rovné $P(\lambda)$.

Keďže maticu $\mathbf{C}(\lambda)$ je λ-maticou, v ktorej každý prvok je polynóm stupňa najviac $(n-1)$-ho, podľa poznámky 4.7 môžeme ju písať v tvare

$$\mathbf{C}(\lambda) = \mathbf{C}_0 + \mathbf{C}_1\lambda + \cdots + \mathbf{C}_{n-1}\lambda^{n-1},$$

kde $\mathbf{C}_i$ sú matice typu $n \times n$.

Vypočítame ľavú stranu (4.14):

$$P(\lambda)\cdot\mathbf{J}_n = a_n\mathbf{J}_n\cdot\lambda^n + a_{n-1}\mathbf{J}_n\lambda^{n-1} + \cdots + a_1\mathbf{J}_n\lambda + a_0\mathbf{J}_n.$$

Vypočítajme aj pravú stranu (4.14):
$(\mathbf{A}-\lambda\mathbf{J}_n)\mathbf{C}(\lambda) = (\mathbf{A}-\lambda\mathbf{J}_n)\cdot(\mathbf{C}_{n-1}\lambda^{n-1}+\mathbf{C}_{n-2}\lambda^{n-2}+\cdots+\mathbf{C}_1\lambda+\mathbf{C}_0) = -\mathbf{C}_{n-1}\lambda^n + (\mathbf{A}\mathbf{C}_{n-1}-\mathbf{C}_{n-2})\lambda^{n-1} + (\mathbf{A}\mathbf{C}_{n-2}-\mathbf{C}_{n-3})\lambda^{n-2} + \cdots + (\mathbf{A}\mathbf{C}_1-\mathbf{C}_0)\lambda + \mathbf{C}_0.$

Porovnaním koeficientov z ľavej i pravej strany (4.14) dostaneme

$$\begin{aligned}
a_n\mathbf{J}_n &= -\mathbf{C}_{n-1}\\
a_{n-1}\mathbf{J}_n &= \mathbf{A}\mathbf{C}_{n-1}-\mathbf{C}_{n-2}\\
a_{n-2}\mathbf{J}_n &= \mathbf{A}\mathbf{C}_{n-2}-\mathbf{C}_{n-3}\\
&\vdots\\
a_1\mathbf{J}_n &= \mathbf{A}\mathbf{C}_1-\mathbf{C}_0\\
a_0\mathbf{J}_n &= \mathbf{A}\mathbf{C}_0
\end{aligned}$$

Keď dané rovnosti vynásobíme zľava postupne $\mathbf{A}^n$, $\mathbf{A}^{n-1}$, $\mathbf{A}^{n-2}$, $\ldots$, $\mathbf{A}$, $\mathbf{A}^0 = \mathbf{J}_n$, dostaneme

$$\begin{aligned}
a_n\mathbf{A}^n &= -\mathbf{A}^n\mathbf{C}_{n-1}\\
a_{n-1}\mathbf{A}^{n-1} &= \mathbf{A}^n\mathbf{C}_{n-1}-\mathbf{A}^{n-1}\mathbf{C}_{n-2}\\
a_{n-2}\mathbf{A}^{n-2} &= \mathbf{A}^{n-1}\mathbf{C}_{n-2}-\mathbf{A}^{n-2}\mathbf{C}_{n-3}\\
&\vdots\\
A_1\mathbf{A} &= \mathbf{A}^2\mathbf{C}_1-\mathbf{A}\mathbf{C}_0\\
a_0\mathbf{J}_n &= \mathbf{A}\mathbf{C}_0
\end{aligned}$$

Rovnosti sčítame. Dostaneme $P(\mathbf{A}) = \mathbf{0}_n$, čo bolo treba dokázať. □

Poznámka 4.8. Mohlo by sa zdať, že do (4.14) stačí dosadiť za λ maticu $\mathbf{A}$, ale na pravej strane (4.14) máme číslo λ, nie maticu.

Veta 4.9. *Nech $\lambda \in F$ je vlastná hodnota nasledovnej lineárnej transformácie $\varphi : \mathcal{V}_n(F) \to \mathcal{V}_n(F)$ danej maticou A vzhľadom na kanonickú bázu. Nech $\alpha = (x_1, x_2, \ldots, x_n)$ je vlastný vektor transformácie prislúchajúci vlastnej hodnote λ. Nech ďalej*

$$\Phi(A) = a_mA^m + a_{m-1}A^{m-1} + \cdots + a_1A + a_0I_n$$

je ľubovoľný polynóm matice A, kde $a_i \in F$.
Nech $\psi : \mathcal{V}_n(F) \to \mathcal{V}_n(F)$ je lineárna transformácia určená maticou $\Phi(A)$ vzhľadom na kanonickú bázu. Potom

1) α *je vlastný vektor zobrazenia* ψ.

2) Vlastný vektor α *zobrazenia* ψ *sa transformuje vlastnou hodnotou*

$$\Phi(\lambda) = a_m\lambda^m + a_{m-1}\lambda^{m-1} + \cdots + a_1\lambda + a_0.$$

Dôkaz. Keďže matica A určuje φ vzhľadom na kanonickú bázu je

$$\varphi(\alpha) = (x_1, x_2, \dots, x_n) \cdot A = \lambda(x_1, x_2, \dots, x_n).$$

Vypočítame $\psi(\alpha)$

$$\begin{aligned}
\psi(\alpha) &= (x_1, x_2, \dots, x_n) \cdot \Phi(A) = \\
&= (x_1, x_2, \dots, x_n) \cdot (a_m A^m + a_{m-1}A^{m-1} + \cdots + a_1 A + a_0 \cdot I_n) = \\
&= a_m(x_1, x_2, \dots, x_n)A^m + a_{m-1}(x_1, x_2, \dots, x_n)A^{m-1} + \dots \\
&\cdots + a_1(x_1, x_2, \dots, x_n)A + a_0(x_1, x_2, \dots, x_n)I_n = \\
&= a_m(x_1, x_2, \dots, x_n) \cdot A \cdot A^{m-1} + a_{m-1}(x_1, x_2, \dots, x_n) \cdot A \cdot A^{m-2} + \dots \\
&\cdots + a_1(x_1, x_2, \dots, x_n)A + a_0(x_1, x_2, \dots, x_n) = \\
&= a_m\lambda(x_1, x_2, \dots, x_n \cdot)A^{m-1} + a_{m-1}\lambda(x_1, x_2, \dots, x_n)A^{m-2} + \\
&+ \cdots + a_1\lambda(x_1, x_2, \dots, x_n) + a_0 \cdot (x_1, x_2, \dots, x_n) = \dots \\
\dots &= a_m\lambda^m(x_1, x_2, \dots, x_n) + a_{m-1}\lambda^{m-1}(x_1, x_2, \dots, x_n) + \\
&+ \cdots + \lambda(x_1, x_2, \dots, x_n) + a_0(x_1, x_2, \dots, x_n) = \\
&= (a_m\lambda^m + a_{m-1}\lambda^{m-1} + \cdots + a_1\lambda + a_0)(x_1, x_2, \dots, x_n).
\end{aligned}$$

Vypočítali sme

$$\psi(\alpha) = \Phi(\lambda)(x_1, x_2, \dots, x_n) = \Phi(\lambda)\alpha.$$

Z tohto vzťahu vyplýva tvrdenie vety:

1) $\Phi(\lambda)$ je charakteristická hodnota ψ,

2) α je charakteristický vektor zobrazenia ψ transformujúci sa vlastnou hodnotou $\Phi(\lambda)$. □

Dôsledok 1. *Ak* λ *je charakteristická hodnota matice* A*, tak* λ^k *je charakteristická hodnota matice* A^k.

Dôsledok 2. *Nech* $\lambda_1, \lambda_2, \dots, \lambda_n$ *sú vlastné hodnoty matice* A *(t.j. spektrum matice), tak* $\lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k$ *je stopa matice* A^k.

Príklad 4.15. Uvažujme maticu

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

z príkladu 4.13. Jej vlastné čísla sú $\lambda_1 = 1, \lambda_2 = 2, \lambda_3 = 2$. Overme, že $\lambda_1^2 + \lambda_2^2 + \lambda_3^2$ je stopa matice A^2.

$$A^2 = \begin{pmatrix} 1 & -1 & 2 \\ -2 & 0 & 4 \\ -1 & -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 2 \\ -2 & 0 & 4 \\ -1 & -1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & -3 & 6 \\ -6 & -2 & 12 \\ -3 & -3 & 10 \end{pmatrix}.$$

Vidíme, že stopa matice A^2 je $1-2+10=9$ a súčet $\lambda_1^2+\lambda_2^2+\lambda_3^2 = 1+2^2+2^2 = = 1+4+4 = 9$, teda stopa druhej mocniny matice A sa rovná súčtu druhých mocnín vlastných čísel matice A.

Cvičenia

4.1. Zistite, ktoré z nasledujúcich podpriestorov sú invariantné priestory zobrazenia $\varphi : \boldsymbol{V}_3(R) \to \boldsymbol{V}_3(R)$ dané (vzhľadom na kanonickú bázu) maticou

$$A = \begin{pmatrix} \frac{\sqrt{2}}{2} & 0 & \frac{\sqrt{2}}{2} \\ 0 & 1 & 0 \\ -\frac{\sqrt{2}}{2} & 0 & \frac{\sqrt{2}}{2} \end{pmatrix}$$

a) $\boldsymbol{S} = \{(0,x,0);\ x \in R\}$,
b) $\boldsymbol{T} = \{(x_1,x_2,x_3);\ 2x_1+x_2-x_3=0\}$,
c) $\boldsymbol{U} = \{(x_1,0,x_2);\ x_1,x_2 \in R\}$.

4.2. Nájdite charakteristické hodnoty, charakteristické vektory (ak existujú) a jednorozmerné invariantné podpriestory lineárnych transformácií z cvičenia 3.3. Kde je to možné preveďte maticu týchto transformácií na diagonálnu formu.

4.3. Nájdite charakteristické hodnoty, charakteristické vektory (ak existujú) a jednorozmerné invariantné podpriestory lineárnych transformácií priestor $\boldsymbol{V}_2(R)$ danými nasledujúcimi maticami. Matice sú vzhľadom na kanonickú bázu. Kde je to možné preveďte maticu transformácie na diagonálnu formu.

$$\text{a)} \begin{pmatrix} 3 & 5 \\ 0 & 3 \end{pmatrix}, \qquad \text{b)} \begin{pmatrix} 33 & -24 \\ 48 & -35 \end{pmatrix}, \qquad \text{c)} \begin{pmatrix} -36 & 26 \\ -50 & 36 \end{pmatrix}.$$

4.4. Nech matica

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

je maticou lineárnej transformácie φ v priestore $\boldsymbol{V}_2(R)$. Nájdite podmienky, pri ktorých má charakteristický polynóm transformácie φ
a) reálne korene rôzne,
b) dvojnásobný koreň,
c) komplexne združené korene.
V ktorých prípadoch má zobrazenie jednorozmerný invariantný priestor?

4.5. V priestore $\boldsymbol{V}_3(R)$ je daná lineárna transformácia φ (vzhľadom na bázu $\boldsymbol{\varepsilon}_1 = (1,0,0)$, $\boldsymbol{\varepsilon}_2 = (0,1,0)$, $\boldsymbol{\varepsilon}_3 = (0,0,1)$ maticami:
a) maticou z cvičenia 4.1,

$$\text{b)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -4 & 0 \end{pmatrix}, \qquad \text{c)} \begin{pmatrix} 2 & -1 & 2 \\ 5 & -3 & 3 \\ -1 & 0 & -2 \end{pmatrix}, \qquad \text{d)} \begin{pmatrix} 5 & 6 & -3 \\ -1 & 0 & 1 \\ 1 & 2 & -1 \end{pmatrix}.$$

Nájdite charakteristický polynóm, charakteristické hodnoty, charakteristické vektory a jednorozmerné invariantné podpriestory danej transformácie. Ak transformácia φ má tri lineárne nezávislé vektory, nájdite maticu transformácie φ v diagonálnom tvare (4.9).

4.6. Nech $P(\lambda)$ je charakteristický polynóm matice $\mathbf{A}$. Na maticiach z cvičenia 4.2, 4.3 a 4.4 overte že platí $P(\mathbf{A}) = \mathbf{0}$.

4.7. Nech $\mathbf{A}$ je regulárna matica. Dokážte, že vlastné hodnoty matice $\mathbf{A}^{-1}$ sú prevrátené hodnoty vlastných hodnôt matice $\mathbf{A}$.

4.8. Nech $\mathbf{A}$ je štvorcová matica nad poľom reálnych (komplexných) čísel. Dokážte, že vlastné hodnoty matice $\mathbf{A}^2$ sú štvorce vlastných hodnôt matice $\mathbf{A}$.

4.9. Nech $\mathbf{A}$, $\mathbf{B}$ regulárne matice nad poľom reálnych čísel. Potom matice $\mathbf{AB}$, $\mathbf{BA}$ sú si podobné. Dokážte to. Pokúste sa dokázať to len za podmienky, že $\mathbf{A}$ je regulárna matica.

4.10. Je daná lineárna transformácia $\varphi : \boldsymbol{V}_4(R) \to \boldsymbol{V}_4(R)$ maticou z príkladu 4.12. Overte, že pre koreň $\lambda_4 = 2 - i$ dostaneme ten istý dvojrozmerný invariantný podpriestor ako pre koreň $\lambda_3 = 2 + i$, ktorý sme našli v príklade 4.12 a nájdite invariantný podpriestor pre ďalší koreň $\lambda_1 = i$ resp. $\lambda_2 = -i$.

§ 5. Ortogonálne a symetrické zobrazenia

Budeme pokračovať vo vyšetrovaní lineárnych transformácií. V euklidovskom priestore $\boldsymbol{E}(R)$ sa môžeme pýtať, ako tieto transformujú skalárny súčin.

Definícia 5.1. Lineárna transformácia $\varphi : \boldsymbol{E}(R) \to \boldsymbol{E}(R)$ sa nazýva *ortogonálna,* keď

$$\text{pre všetky} \quad \boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{E}(R) \quad \text{platí :} \quad (\varphi(\boldsymbol{\alpha}), \varphi(\boldsymbol{\beta})) = (\boldsymbol{\alpha}, \boldsymbol{\beta}),$$

to jest, keď zachováva skalárny súčin.

Príklad 5.1. Nech transformácia $\varphi : \boldsymbol{V}_2(R) \to \boldsymbol{V}_2(R)$ je daná maticou

$$\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix},$$

vzhľadom na bázu $\{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2\}$, kde $\boldsymbol{\eta}_1 = (1,1)$, $\boldsymbol{\eta}_2 = (1,0)$. Skalárny súčin vektorov $\boldsymbol{\alpha} = (r,s)$, $\beta = (u,v)$ definujeme ako obvykle takto: $(\boldsymbol{\alpha}, \boldsymbol{\beta}) = ru + sv$. Zistime, či φ je ortogonálna transformácia.

Najprv vypočítame súradnice vektora $\boldsymbol{\alpha}$. Z rovnice $(r,s) = x_1(1,1) + x_2(1,0)$ hneď vyjde $x_1 = s$, $x_2 = r - s$. Analogicky vypočítame súradnice vektora $\boldsymbol{\beta}$: $y_1 = v, \quad y_2 = u - v$. Súradnice vektora $\varphi(\boldsymbol{\alpha})$ sú

$$(x_1', x_2') = (s, r-s)\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} = (r, s-r),$$

odkiaľ dostaneme $\varphi(\boldsymbol{\alpha}) = r(1,1) + (s-r)(1,0) = (s,r)$. Podobne vypočítame: $\varphi(\boldsymbol{\beta}) = (v,u)$. Vidno, že $(\varphi(\boldsymbol{\alpha}), \varphi(\boldsymbol{\beta})) = vs + ru = (\boldsymbol{\alpha}, \boldsymbol{\beta})$. Ide zrejme o ortogonálnu transformáciu.

Veta 5.1. *Nech $\varphi : \boldsymbol{E}(R) \to \boldsymbol{E}(R)$ je ortogonálna transformácia priestoru $\boldsymbol{E}(R)$. Nech $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{E}(R)$ sú ľubovoľné vektory euklidovského priestoru. Potom platí:*

a) *φ zachováva veľkosť vektora, t.j. $|\varphi(\boldsymbol{\alpha})| = |\boldsymbol{\alpha}|$,*
b) *φ zachováva ortogonalitu, t.j. $\boldsymbol{\alpha} \perp \boldsymbol{\beta}$ implikuje $\varphi(\boldsymbol{\alpha}) \perp \varphi(\boldsymbol{\beta})$,*
c) *φ zachováva uhol, t.j. $\measuredangle(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \measuredangle(\varphi(\boldsymbol{\alpha}), \varphi(\boldsymbol{\beta}))$,*
d) *φ zachováva vzdialenosť, t.j. $|\boldsymbol{\alpha} - \boldsymbol{\beta}| = |\varphi(\boldsymbol{\alpha}) - \varphi(\boldsymbol{\beta})|$.*

Dôkaz priamo vyplýva z definície 5.1, lebo pojmy veľkosť, kolmosť, uhol, vzdialenosť sa definujú pomocou skalárneho súčinu. □

Napr. veľkosť: $|\varphi(\boldsymbol{\alpha})| = \sqrt{(\varphi(\boldsymbol{\alpha}), \varphi(\boldsymbol{\alpha}))} = \sqrt{(\boldsymbol{\alpha}, \boldsymbol{\alpha})} = |\boldsymbol{\alpha}|$.

Veta 5.2. *Nech $B = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ je ortonormálna báza euklidovského priestoru $\boldsymbol{E}(R)$. Matica $\mathbf{A}$ typu $n \times n$ je maticou ortogonálnej lineárnej transformácie $\varphi : \boldsymbol{E}(R) \to \boldsymbol{E}(R)$ vzhľadom na bázu B práve vtedy, keď*

$$\sum_{k=1}^{n} a_{ik} \cdot a_{jk} = \delta_{ij}, \tag{5.1}$$

kde δ_{ij} je Kroneckerova delta.

Poznámka 5.1. Kroneckerova delta je definovaná nasledovne:

$$\delta_{ij} = \begin{cases} 0, & \text{ak} \quad i \neq j, \\ 1, & \text{ak} \quad i = j. \end{cases}$$

Dôkaz vety 5.2. I. Nech $\boldsymbol{\varepsilon}_i$, $\boldsymbol{\varepsilon}_j \in B$ sú ľubovoľné vektory ortonormálnej bázy. Nech ďalej $\mathbf{A}$ je maticou ortogonálnej transformácie. Potom podľa (3.4)

$$\varphi(\boldsymbol{\varepsilon}_i) = \sum_{k=1}^{n} a_{ik} \boldsymbol{\varepsilon}_k, \qquad \varphi(\boldsymbol{\varepsilon}_j) = \sum_{k=1}^{n} a_{jk} \cdot \boldsymbol{\varepsilon}_k.$$

Keďže $\boldsymbol{\varepsilon}_i$, $\boldsymbol{\varepsilon}_j$ sú vektory ortonormálnej bázy, podľa vety 5.3 a definície 5.6 kapitoly 2 platí $(\boldsymbol{\varepsilon}_i, \boldsymbol{\varepsilon}_j) = \delta_{ij}$. Preto

$$\begin{aligned} 1 = |\boldsymbol{\varepsilon}_i| = (\boldsymbol{\varepsilon}_i, \boldsymbol{\varepsilon}_i) = (\varphi(\boldsymbol{\varepsilon}_i), \varphi(\boldsymbol{\varepsilon}_i)) = \\ = (a_{i1}\boldsymbol{\varepsilon}_1 + \boldsymbol{\varepsilon}_{i2}\boldsymbol{\varepsilon}_2 + \dots + a_{in}\boldsymbol{\varepsilon}_n,\ a_{i1}\boldsymbol{\varepsilon}_1 + a_{i2}\boldsymbol{\varepsilon}_2 + \dots + a_{in}\boldsymbol{\varepsilon}_n) = \\ = a_{i1}^2 + a_{i2}^2 + \dots + a_{in}^2 = \sum_{k=1}^{n} a_{ik}^2 = \sum_{k=1}^{n} a_{ik} \cdot a_{ik}. \end{aligned}$$

Ďalej, ak $i \neq j$, tak

$$\begin{aligned} 0 = (\boldsymbol{\varepsilon}_i, \boldsymbol{\varepsilon}_1) = (\varphi(\boldsymbol{\varepsilon}_i), \varphi(\boldsymbol{\varepsilon}_j)) = \\ = (a_{i1}\boldsymbol{\varepsilon}_1 + a_{i2}\boldsymbol{\varepsilon}_2 + \dots + a_{in}\boldsymbol{\varepsilon}_n,\ a_{j1}\boldsymbol{\varepsilon}_1 + a_{j2}\boldsymbol{\varepsilon}_2 + \dots + a_{jn}\boldsymbol{\varepsilon}_n) = \\ = a_{i1}a_{j1} + a_{i2}a_{j2} + \dots + a_{in}a_{jn} = \sum_{i=1}^{n} a_{ik} \cdot a_{jk}. \end{aligned}$$

Vidíme, že 5.1 platí.

II. Nech naopak $\mathbf{A}$ má vlastnosť (5.1). Nech $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{E}(R)$ sú ľubovoľné vektory

$$\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_n\boldsymbol{\varepsilon}_n,$$
$$\boldsymbol{\beta} = y_1\boldsymbol{\varepsilon}_1 + y_2\boldsymbol{\varepsilon}_2 + \cdots + y_n\boldsymbol{\varepsilon}_n.$$

Máme

$$(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \cdots + x_n\boldsymbol{\varepsilon}_n,\ y_1\boldsymbol{\varepsilon}_1 + y_2\boldsymbol{\varepsilon}_2 + \cdots + y_n\boldsymbol{\varepsilon}_n) =$$
$$= x_1y_1 + x_2y_2 + \cdots + x_ny_n = \sum_{i=1}^{n} x_iy_i,$$

lebo $(\boldsymbol{\varepsilon}_i, \boldsymbol{\varepsilon}_j) = \delta_{ij}$. Podľa (2.4) vektor súradníc $\varphi(\boldsymbol{\alpha})$ je

$$(x_1, x_2, \ldots, x_n)\mathbf{A} = \left(\sum_{i=1}^{n} x_ia_{i1}, \sum_{i=1}^{n} x_ia_{i2}, \ldots, \sum_{i=1}^{n} x_ia_{in}\right).$$

Podobne vektor súradníc $\varphi(\boldsymbol{\beta})$ je

$$(y_1, y_2, \ldots, y_n)\mathbf{A} = \left(\sum_{j=1}^{n} y_ja_{j1}, \sum_{j=1}^{n} y_ja_{j2}, \ldots, \sum_{j=1}^{n} y_ja_{jn}\right).$$

Tak isto ako $(\boldsymbol{\alpha}, \boldsymbol{\beta})$, vypočítame aj $(\varphi(\boldsymbol{\alpha}), \varphi(\boldsymbol{\beta}))$:

$$(\varphi(\boldsymbol{\alpha}), \varphi(\boldsymbol{\beta})) = \sum_{i=1}^{n} x_ia_{i1} \sum_{j=1}^{n} y_ja_{j1} + \sum_{i=1}^{n} x_ia_{i2} \sum_{j=1}^{n} y_ja_{j2} + \cdots + \sum_{i=1}^{n} x_ia_{in} \sum_{j=1}^{n} y_ja_{jn} =$$
$$= \sum_{i=1}^{n}\sum_{j=1}^{n} x_iy_ja_{i1}a_{j1} + \sum_{i=1}^{n}\sum_{j=1}^{n} x_iy_ja_{i2}a_{j2} + \cdots + \sum_{i=1}^{n}\sum_{j=1}^{n} x_iy_ja_{in}a_{jn} =$$
$$= \sum_{k=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n} x_iy_ja_{ik}a_{jk} = \sum_{i=1}^{n}\sum_{j=1}^{n} x_iy_j \sum_{k=1}^{n} a_{ik}a_{jk} =$$
$$= \sum_{i=1}^{n}\sum_{j=1}^{n} x_iy_j\delta_{ij} = \sum_{i=1}^{n} x_iy_i = (\boldsymbol{\alpha}, \boldsymbol{\beta}).$$

Vidíme, že φ zachováva skalárny súčin, preto je ortogonálnou transformáciou. $\square$

Príklad 5.2. Postup časti II dôkazu predchádzajúcej vety demonštrujeme na priestore $\boldsymbol{E}(R)$ dimenzie dva.

$$(\varphi(\boldsymbol{\alpha}), \varphi(\boldsymbol{\beta})) = \sum_{i=1}^{2} x_ia_{i1} \sum_{j=1}^{2} y_ja_{j1} + \sum_{i=1}^{2} x_ia_{i2} \sum_{i=1}^{2} y_ja_{j2} =$$
$$= (x_1a_{11} + x_2a_{21}) \cdot (y_1a_{11} + y_2a_{21}) + (x_1a_{12} + x_2a_{22}) \cdot (y_1a_{12} + y_2a_{22}) =$$
$$= x_1y_1a_{11}^2 + x_1y_2a_{11}a_{21} + x_2y_1a_{21}a_{11} + x_2y_2a_{21}^2 + x_1y_1a_{12}^2 + x_1y_2a_{12}a_{22} +$$
$$+ x_2y_1a_{22}a_{12} + x_2y_2a_{22}^2 = x_1y_1(\underbrace{a_{11}^2 + a_{12}^2}_{1}) + x_1y_2(\underbrace{a_{11}a_{21} + a_{12}a_{22}}_{0}) +$$
$$+ x_2y_1(\underbrace{a_{11}a_{21} + a_{12}a_{22}}_{0}) + x_2y_2(\underbrace{a_{21}^2 + a_{22}^2}_{1}) = x_1y_1 + x_2y_2 = (\boldsymbol{\alpha}, \boldsymbol{\beta}).$$

Príklad 5.3. V príklade 5.1 sme mali ortogonálnu transformáciu vektorového priestoru $\boldsymbol{V}_2(R)$ danú maticou

$$\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix},$$

ktorá evidentne nesplĺňa podmienku (5.1) z vety 5.2. Je to preto, lebo báza v danom prípade nie je ortonormálna (ani len ortogonálna). Ak prejdeme k ortonormálnej (kanonickej) báze

$$\begin{aligned} \boldsymbol{\varepsilon}_1 &= (1,0) = 0\cdot(1,1) + 1\cdot(1,0) = 0\cdot\eta_1 + 1\cdot\eta_2, \\ \boldsymbol{\varepsilon}_2 &= (0,1) = 1\cdot(1,1) - 1\cdot(1,0) = 1\cdot\eta_1 - 1\cdot\eta_2, \end{aligned}$$

vidíme, že matica prechodu a jej inverzná matica sú

$$\mathbf{P} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{a} \quad \mathbf{P}^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Podľa vety 2.4 matica zobrazenia φ vzhľadom na kanonickú bázu bude

$$\mathbf{B} = \mathbf{PAP}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

ktorá už podmienku (5.1) splĺňa.

Príklad 5.4. Zistime aké sú (všetky možné) ortogonálne zobrazenia v priestore $\boldsymbol{V}_2(R)$.

Nech ortogonálne zobrazenie $\varphi : \boldsymbol{V}_2(R) \to \boldsymbol{V}_2(R)$ je dané vzhľadom na kanonickú bázu maticou

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

Potom na základe vety 5.2 platí:

$$\sum_{k=1}^{2} a_{ik}\cdot a_{jk} = \delta_{ij}. \tag{5.2}$$

Pre voľbu indexov i, j máme len štyri možnosti: $i = j = 1$, alebo $i = j = 2$, alebo $i = 1$, $j = 2$, alebo $i = 2$, $j = 1$. Čitateľ ľahko preverí, že uplatnením prvej z (5.2) dostaneme (a), uplatnením druhej (b) a konečne uplatnením tretej alebo štvrtej máme (c). Teda

$$a_{11}^2 + a_{12}^2 = 1, \tag{a}$$

$$a_{21}^2 + a_{22}^2 = 1, \tag{b}$$

$$a_{11}a_{21} + a_{12}a_{22} = 0. \tag{c}$$

Zo vzťahu (a) hneď vidíme, že existuje uhol ω taký, že $\cos\omega = a_{11}$ a zároveň $\sin\omega = a_{12}$. Máme dve možnosti.

Po prvé: $a_{11} \neq 0$. Potom $a_{22} \neq 0$. Naozaj, ak by $a_{22} = 0$, tak z (c) máme $a_{21} = 0$, t.j. druhý riadok matice $\mathbf{A}$ by bol nulový, čo odporuje (b). Preto z (c) vyplýva

$$tg\omega = \frac{a_{12}}{a_{11}} = -\frac{a_{21}}{a_{22}}.$$

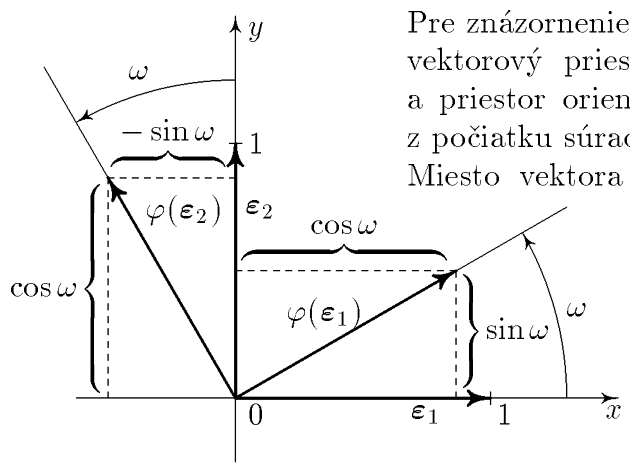
Odtiaľ dostávame $a_{21} = \pm\sin\omega$ $a_{22} = \pm\cos\omega$. Preto pre maticu $\mathbf{A}$ máme len dve možnosti:

$$\mathbf{A} = \begin{pmatrix} \cos\omega & \sin\omega \\ -\sin\omega & \cos\omega \end{pmatrix} \quad \text{alebo} \quad \mathbf{A} = \begin{pmatrix} \cos\omega & \sin\omega \\ \sin\omega & -\cos\omega \end{pmatrix}.$$

Prvá matica je maticou transformácie, ktorá je otočením o uhol ω.
Skutočne,

$$\varphi(\boldsymbol{\varepsilon}_1) = (1,0)\begin{pmatrix} \cos\omega & \sin\omega \\ -\sin\omega & \cos\omega \end{pmatrix} = (\cos\omega, \sin\omega),$$
$$\varphi(\boldsymbol{\varepsilon}_2) = (0,1)\begin{pmatrix} \cos\omega & \sin\omega \\ -\sin\omega & \cos\omega \end{pmatrix} = (-\sin\omega, \cos\omega),$$

ako to vidíme na obrázku:

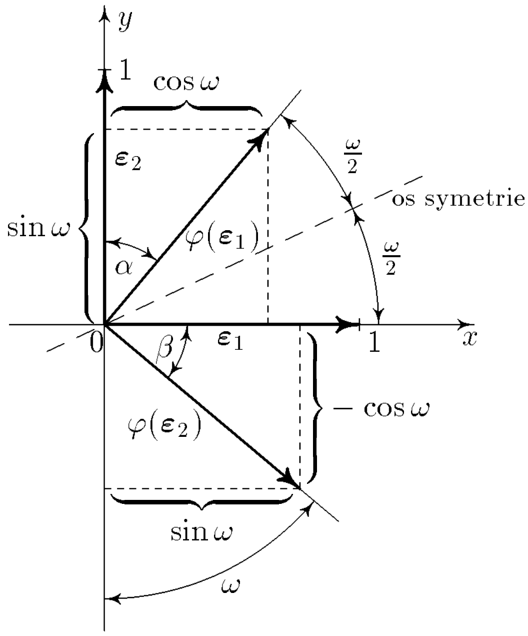


Pre znázornenie transformácie sa využíva fakt, že vektorový priestor dvojíc reálnych čísel $\boldsymbol{V}_2(R)$ a priestor orientovaných úsečiek vychádzajúcich z počiatku súradnicovej sústavy sú izomorfné. Miesto vektora (x_1, x_2) (aritmetický vektor) je znázornená orientovaná úsečka (geometrický vektor) vychádzajúca z počiatku súradníc, ktorej koncový bod má súradnice (x_1, x_2).

Druhá matica je maticou symetrie vzhľadom na os zvierajúcu s osou x uhol $\frac{\omega}{2}$.
Skutočne,

$$\varphi(\boldsymbol{\varepsilon}_1) = (1,0)\begin{pmatrix} \cos\omega & \sin\omega \\ \sin\omega & -\cos\omega \end{pmatrix} = (\cos\omega, \sin\omega),$$
$$\varphi(\boldsymbol{\varepsilon}_2) = (0,1)\begin{pmatrix} \cos\omega & \sin\omega \\ \sin\omega & -\cos\omega \end{pmatrix} = (\sin\omega, -\cos\omega),$$

ako to vidíme na obrázku:



Keďže vektor $\varphi(\boldsymbol{\varepsilon}_2)$ je obrazom vektora $\boldsymbol{\varepsilon}_2$ podľa osi symetrie zvierajúcej s kladným smerom osi x uhol $\frac{\omega}{2}$, pre veľkosti uhlov znázornených na obrázku platí: $\alpha + \frac{\omega}{2} = \frac{\omega}{2} + \beta$. Preto $\alpha = \beta$. Odtiaľ už vidieť, že uhol, ktorý zviera vektor $\varphi(\boldsymbol{\varepsilon}_2)$ so záporným smerom osi y má tiež veľkosť ω.

Po druhé: $a_{11} = 0$. Potom z (a) vyplýva $a_{12} = \pm 1$ a z (c) máme $a_{22} = 0$. Ďalej z (b) dostávame $a_{21} = \pm 1$. Ak zvolíme $a_{12} = 1$, máme dve možnosti:

1)

$$\mathbf{A} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\pi}{2} & \sin\frac{\pi}{2} \\ -\sin\frac{\pi}{2} & \cos\frac{\pi}{2} \end{pmatrix},$$

2)

$$\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\pi}{2} & \sin\frac{\pi}{2} \\ \sin\frac{\pi}{2} & -\cos\frac{\pi}{2} \end{pmatrix}.$$

Prvá možnosť znamená otočenie o uhol $\frac{\pi}{2}$, druhá symetriu vzhľadom na os $y = x$.

Ak zvolíme $a_{12} = -1$, opäť máme dve možnosti:

1)

$$\mathbf{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{3\pi}{2} & \sin\frac{3\pi}{2} \\ -\sin\frac{3\pi}{2} & -\cos\frac{3\pi}{2} \end{pmatrix},$$

ide o otočenie o uhol $\frac{3\pi}{2}$.

2)

$$\mathbf{A} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{3\pi}{2} & \sin\frac{3\pi}{2} \\ \sin\frac{3\pi}{2} & -\cos\frac{3\pi}{2} \end{pmatrix},$$

ide o symetriu vzhľadom na os $y = -x$, ktorá zviera s osou x uhol $\frac{3\pi}{4}$.

Vidieť, že všetky štyri prípady pre $a_{11} = 0$ sú len špeciálnymi prípadmi otočenia alebo symetrie. Máme teda len dvojaké ortogonálne transformácie v rovine dané maticami

$$\begin{pmatrix} \cos\omega & \sin\omega \\ -\sin\omega & \cos\omega \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} \cos\omega & \sin\omega \\ \sin\omega & -\cos\omega \end{pmatrix}.$$

Vypočítajme charakteristický polynóm prvej

$$f(\lambda) = \begin{vmatrix} \cos\omega - \lambda & \sin\omega \\ -\sin\omega & \cos\omega - \lambda \end{vmatrix} = \lambda^2 - 2\cos\omega\lambda + \cos^2\omega + \sin^2\omega = \lambda^2 - (2\cos\omega)\lambda + 1.$$

Jeho korene sú
$$\lambda_{12} = \cos\omega \pm \sqrt{\cos^2\omega - 1}\,.$$
Ak $\omega = 0 + 2k\pi$, kde $k \in Z$, tak $\lambda_{1,2} = 1$. Ide o otočenie o nulový uhol, čiže identické zobrazenie, ktorého matica je $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Ak $\omega \neq 0 + 2k\pi$, tak existujú komplexne združené korene a najmenším invariantným podpriestorom priestoru $\boldsymbol{V}_2(R)$ je on sám.

Vypočítajme charakteristický polynóm druhej:
$$f(\lambda) = \begin{vmatrix} \cos\omega - \lambda & \sin\omega \\ \sin\omega & -\cos\omega - \lambda \end{vmatrix} = \lambda^2 - \cos^2\omega - \sin^2\omega = \lambda^2 - 1.$$

Vidíme, že charakteristické čísla sú $\lambda_{1,2} = \pm 1$. Pre $\lambda_1 = 1$ máme sústavu
$$\begin{aligned} (\cos\omega - 1)x_1 + (\sin\omega)x_2 &= 0, \\ (\sin\omega)x_1 - (\cos\omega + 1)x_2 &= 0. \end{aligned}$$
Máme dve možnosti. Po prvé, $\omega = 0 + 2k\pi$, kde $k \in Z$. Potom ide o symetriu podľa osi x. Naša sústava má tvar
$$\begin{aligned} 0 \cdot x_1 + 0 \cdot x_2 &= 0, \\ 0 \cdot x_1 - 2 \cdot x_2 &= 0, \end{aligned}$$
ktorej podpriestor riešení je $\{(p, 0);\ p \in R\}$. Vidieť, že vlastným vektorom je každý vektor ležiaci na osi x, čiže jednorozmerný invariantný podpriestor tvoria všetky vektory ležiace na osi x.
Po druhé, $\omega \neq 0 + 2k\pi$. Potom ak prvú rovnicu vynásobíme číslom $\sin\omega$, druhú číslom $\cos\omega - 1$, dostaneme sústavu
$$\begin{aligned} \sin\omega(\cos\omega - 1)x_1 + (\sin^2\omega)x_2 &= 0, \\ \sin\omega(\cos\omega - 1)x_1 + (1 - \cos^2\omega)x_2 &= 0, \end{aligned}$$
ktorá má len jedinú lineárne nezávislú rovnicu a podpriestor riešení ktorrej je
$$\left\{(\frac{1 + \cos\omega}{\sin\omega}p,\, p);\ p \in R\right\}.$$
Keďže matica **A** je daná vzhľadom na kanonickú bázu, tento podpriestor je zároveň aj invariantným podpriestorom symetrie. Položiac $p = \sin\omega$, máme charakteristický vektor
$$\boldsymbol{\alpha} = (1 + \cos\omega,\, \sin\omega).$$
prináležiaci vlastnému číslu 1.

Pre $\lambda_2 = -1$ máme sústavu
$$\begin{aligned} (\cos\omega + 1)x_1 + (\sin\omega)x_2 &= 0, \\ (\sin\omega)x_1 - (\cos x - 1)x_2 &= 0. \end{aligned}$$

Znova máme dve možnosti. Po prvé, $\omega = 0 + 2k\pi$, kde $k \in Z$. Opäť ide o symetriu podľa osi x. Naša sústava má tvar

$$
\begin{aligned}
2 \cdot x_1 + 0 \cdot x_2 &= 0,\\
0 \cdot x_1 + 0 \cdot x_2 &= 0,
\end{aligned}
$$

ktorej podpriestor riešení je $\{(0,p);\ p \in R\}$. Vidieť, že vlastným vektorom je každý vektor ležiaci na osi y, čiže jednorozmerný invariantný podpriestor tvoria všetky vektory ležiace na osi y.
Po druhé, $\omega \neq 0 + 2k\pi$. Potom ak prvú rovnicu vynásobíme číslom $\sin\omega$, druhú číslom $1 + \cos\omega$, dostaneme sústavu

$$
\begin{aligned}
\sin\omega(\cos\omega + 1)x_1 + (\sin^2\omega)x_2 &= 0,\\
\sin\omega(\cos\omega + 1)x_1 + (1 - \cos^2\omega)x_2 &= 0
\end{aligned}
$$

Zasa ide len o jedinú lineárne nezávislú rovnicu. Podpriestor riešení sústavy je

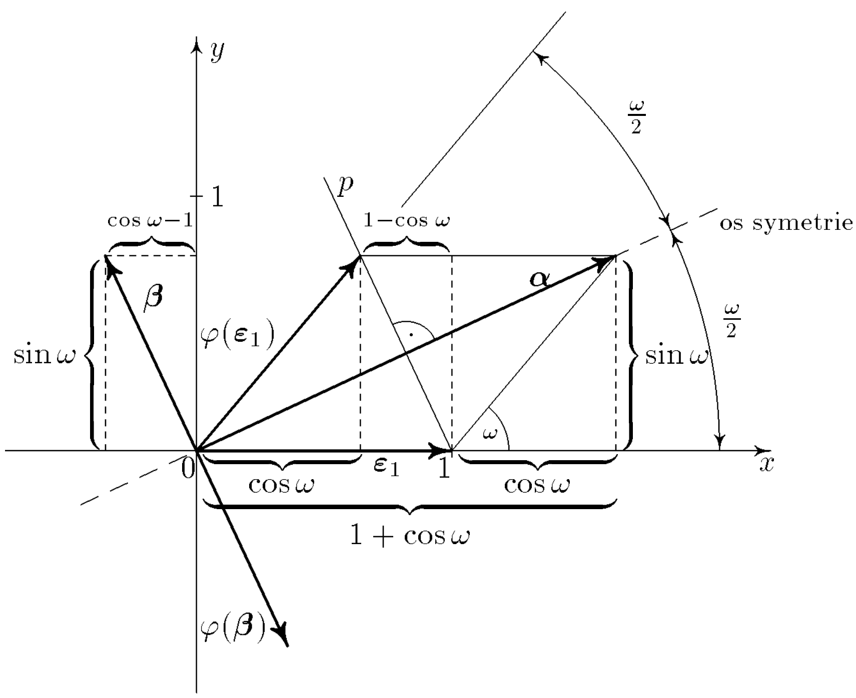
$$\left\{(\frac{\cos\omega - 1}{\sin\omega}p,\ p);\ p \in R\right\}.$$

Podobne ako predtým, tento podpriestor je zároveň aj invariantným podpriestorom symetrie. Pre $p = \sin\omega$, máme charakteristický vektor

$$\boldsymbol{\beta} = (\cos\omega - 1,\ \sin\omega).$$

prináležiaci vlastnému číslu -1.

Situáciu ilustrujeme na nasledujúcom obrázku.



Vidieť, že charakteristický vektor $\boldsymbol{\alpha} = (1 + \cos\omega, \sin\omega)$ leží na osi symetrie a charakteristický vektor $\boldsymbol{\beta} = (\cos\omega - 1, \sin\omega)$ leží na priamke kolmej na os symetrie.

Vo vete 5.2 sme dokázali, že reálna matica $\mathbf{A}$ typu $n \times n$ je maticou ortogonálneho zobrazenia ak je pre ňu splnená podmienka (5.1) t.j. $\sum_{k=1}^{n} a_{ik} \cdot a_{jk} = \delta_{ij}$. Ak si uvedomíme, že v matici $\mathbf{A}^T$ sú riadky matice $\mathbf{A}$ stĺpcami, podmienku (5.1) možno preformulovať a platí

Veta 5.3 (iné znenie vety 5.2). *Matica $\mathbf{A}$ typu $n \times n$ je maticou ortogonálnej transformácie $\varphi : \boldsymbol{E}(R) \to (R)$ vzhľadom na ortonormálnu bázu práve vtedy, keď*

$$\mathbf{A} \cdot \mathbf{A}^T = \mathbf{J}_n. \tag{5.3}$$

Definícia 5.2. Štvorcová matica typu $n \times n$ nad nejakým telesom sa nazýva *ortogonálna,* ak platí

$$\mathbf{A} \cdot \mathbf{A}^T = \mathbf{J}_n.$$

Poznámka 5.2. Z podmienky (5.1) vyplýva, že matica $\mathbf{A}$ nemá žiadny riadok nulový. Keďže (nenulové) riadky ortogonálnej matice $\mathbf{A}$ sú navzájom ortogonálne, sú aj lineárne nezávislé a teda $\mathbf{A}$ je regulárna matica. Ďalej hneď vidieť, že $\mathbf{A}^T = \mathbf{A}^{-1}$ a teda aj $\mathbf{A}^T \cdot \mathbf{A} = \mathbf{J}_n$ t.j. aj $\mathbf{A}^T$ je ortogonálna. Ďalej ak $\mathbf{A}, \mathbf{B}$ sú ortogonálne matice, tak $(\mathbf{A} \cdot \mathbf{B})^T = \mathbf{B}^T \cdot \mathbf{A}^T$ a tak $(\mathbf{A} \cdot \mathbf{B}) \cdot (\mathbf{A} \cdot \mathbf{B})^T = \mathbf{A} \cdot (\mathbf{B} \cdot \mathbf{B}^T) \cdot \mathbf{A}^T = \mathbf{J}_n$. To znamená: súčin ortogonálnych matíc je ortogonálna matica. Množina všetkých ortogonálnych matíc (typu $n \times n$) je podpologrupou multiplikatívnej grupy regulárnych matíc. Je aj jej podgrupou, lebo ak $\mathbf{A}, \mathbf{B}$ sú ortogonálne matice, tak $\mathbf{A} \cdot \mathbf{B}^{-1}$ je ortogonálna. Naozaj, $(\mathbf{AB}^{-1})(\mathbf{AB}^{-1})^T = (\mathbf{AB}^T)(\mathbf{AB}^T)^T = \mathbf{A}(\mathbf{B}^T\mathbf{B})\mathbf{A}^T = \mathbf{J}_n$. Čitateľ si premyslí, že vzhľadom na tento fakt je aj grupa ortogonálnych transformácií podgrupou grupy regulárnych transformácií euklidovského priestoru dimenzie n.

Prejdime k ďalšiemu typu transformácie euklidovského priestoru $\boldsymbol{E}(R)$.

Definícia 5.3. Ak pre lineárnu transformáciu $\varphi : \boldsymbol{E}(R) \to \boldsymbol{E}(R)$ euklidovského priestoru platí

$$\text{pre všetky} \quad \boldsymbol{\alpha}, \boldsymbol{\beta} \in \boldsymbol{E}(R) \qquad (\varphi(\boldsymbol{\alpha}), \boldsymbol{\beta}) = (\boldsymbol{\alpha}, \varphi(\boldsymbol{\beta})),$$

tak sa nazýva *symetrickou transformáciou.*

Príklad 5.5. Nech $\varphi : \boldsymbol{V}_2(R) \to \boldsymbol{V}_2(R)$ je transformácia určená vzhľadom na bázu $\{(1,1), (1,0)\}$ maticou

$$\mathbf{A} = \begin{pmatrix} -1 & 4 \\ 2 & -1 \end{pmatrix}.$$

Zistime, či φ je symetrická. V príklade 5.1 sme vypočítali, že vektor súradníc vektora $\boldsymbol{\alpha} = (r, s)$,vzhľadom na danú bázu je $(s, r - s)$. Podľa (2.4) vektor súradníc vektora $\varphi(\boldsymbol{\alpha})$ bude

$$(s, r - s) \begin{pmatrix} -1 & 4 \\ 2 & -1 \end{pmatrix} = (2r - 3s, -r + 5s).$$

Potom $\varphi(\boldsymbol{\alpha}) = (2r - 3s)(1,1) + (-r + 5s)(1,0) = (r + 2s, 2r - 3s)$. Ak zvolíme $\boldsymbol{\beta} = (u, v)$ analogicky zistíme, že $\varphi(\boldsymbol{\beta}) = (u + 2v, 2u - 3v)$. Počítajme teda

$$(\varphi(\boldsymbol{\alpha}), \boldsymbol{\beta}) = (r + 2s)u + (2r - 3s)v = ru + 2su + 2rv - 3sv,$$

$$(\boldsymbol{\alpha}, \varphi(\boldsymbol{\beta})) = r(u + 2v) + s(2u - 3v) = ru + 2rv + 2su - 3sv.$$

Dostali sme rovnaké výsledky, preto $(\varphi(\boldsymbol{\alpha}), \boldsymbol{\beta}) = (\boldsymbol{\alpha}, \varphi(\boldsymbol{\beta}))$. Ide teda o symetrickú transformáciu.

Veta 5.4. *Matica* $\mathbf{A}$ *typu* $n \times n$ *(nad* R*) je maticou symetrickej transformácie* $\varphi : \boldsymbol{E}(R) \to \boldsymbol{E}(R)$ *vzhľadom na ortonormálnu bázu práve vtedy, keď je symetrická.*

Dôkaz. Nech $\mathbf{A}$ je maticou nejakej transformácie vzhľadom na ortonormálnu bázu $\{\boldsymbol{\varepsilon}_1, \dots, \boldsymbol{\varepsilon}_n\}$. Nech $\boldsymbol{\alpha} = x_1\boldsymbol{\varepsilon}_1 + x_2\boldsymbol{\varepsilon}_2 + \dots + x_n\boldsymbol{\varepsilon}_n$ a $\boldsymbol{\beta} = y_1\boldsymbol{\varepsilon}_1 + y_2\boldsymbol{\varepsilon}_2 + \dots + y_n\boldsymbol{\varepsilon}_n$ sú ľubovoľné vektory priestoru $\boldsymbol{E}(R)$. Vypočítajme ich obrazy

$$\begin{aligned}\varphi(\boldsymbol{\alpha}) &= x_1\varphi(\boldsymbol{\varepsilon}_1) + x_2\varphi(\boldsymbol{\varepsilon}_2) + \dots + x_n\varphi(\boldsymbol{\varepsilon}_n) = \\ &= x_1\sum_{j=1}^{n} a_{1j}\boldsymbol{\varepsilon}_j + x_2\sum_{j=1}^{n} a_{2j}\boldsymbol{\varepsilon}_j + \dots + x_n\sum_{j=1}^{n} a_{nj}\boldsymbol{\varepsilon}_j = \\ &= \sum_{i=1}^{n} x_i \sum_{j=1}^{n} a_{ij}\boldsymbol{\varepsilon}_j = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i a_{ij}\boldsymbol{\varepsilon}_j = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} x_i a_{ij}\right)\cdot \boldsymbol{\varepsilon}_j.\end{aligned}$$

Analogicky dostaneme

$$\varphi(\boldsymbol{\beta}) = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} y_i a_{ij}\right)\boldsymbol{\varepsilon}_j.$$

Keďže báza $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \dots, \boldsymbol{\varepsilon}_n\}$ je ortonormálna, t.j. $(\varepsilon_i, \boldsymbol{\varepsilon}_j) = \delta_{ij}$, dostávame

$$(\varphi(\boldsymbol{\alpha}), \boldsymbol{\beta}) = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} x_i a_{ij}\right) y_j, \qquad (\boldsymbol{\alpha}, \varphi(\boldsymbol{\beta})) = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} y_i a_{ij}\right) x_j.$$

Z posledných dvoch rovností vyplýva, že $(\varphi(\boldsymbol{\alpha}), \boldsymbol{\beta}) = (\boldsymbol{\alpha}, \varphi(\boldsymbol{\beta}))$ práve vtedy, keď $a_{ij} = a_{ji}$. Čitateľ to hneď uvidí, keď si pravú stranu prvej rovnosti prepíše na $\sum\limits_{i=1}^{n}(\sum\limits_{j=1}^{n} x_j a_{ji}) y_i$. □

Príklad 5.6. V príklade 5.5 matica $\mathbf{A} = \begin{pmatrix} -1 & 4 \\ 2 & -1 \end{pmatrix}$ symetrickej transformácie $\varphi : \boldsymbol{V}_2(R) \to \boldsymbol{V}_2(R)$ nebola symetrická. To preto lebo báza $\{(1,1),(1,0)\}$ nie je ortonormálna. Tak ako v príklade 5.3 prejdeme ku kanonickej (ortonormálnej) báze pomocou matice prechodu (a jej inverznej matice) $\mathbf{P} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$, a $\mathbf{P}^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Preto

$$\mathbf{B} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 4 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -3 & 5 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & -3 \end{pmatrix}$$

je matica transformácie φ v ortonormálnej báze, ktorá je už symetrická.

Veta 5.5. *Nech* $\mathbf{A}$ *je symetrická matica typu* $n \times n$ *nad poľom reálnych čísel. Potom všetky jej vlastné čísla sú reálne.*

Dôkaz. Nech $\boldsymbol{E}(R)$ je euklidovský priestor dimenzie n. Podľa vety 5.4 maticu $\mathbf{A}$ môžeme považovať za maticu symetrickej transformácie

$$\varphi : \boldsymbol{E}(R) \to \boldsymbol{E}(R),$$

vzhľadom na ortonormálnu bázu.

Dokážeme, že polynóm

$$f(\lambda) = |\mathbf{A} - \lambda \mathbf{J}_n|$$

má len reálne korene. Predpokladajme nepriamo, že polynóm má komplexný koreň $\lambda = r+si$, $s \neq 0$. Potom ako v dôkaze vety 4.7 zostrojíme lineárne nezávislé vektory $\boldsymbol{\alpha}, \boldsymbol{\beta}$ také, že platí (4.13), t.j.

$$\varphi(\boldsymbol{\alpha}) = r\boldsymbol{\alpha} - s\boldsymbol{\beta},$$
$$\varphi(\boldsymbol{\beta}) = r\boldsymbol{\beta} + s\boldsymbol{\alpha}.$$

Potom máme

$$(\varphi(\boldsymbol{\alpha}), \boldsymbol{\beta}) = r(\boldsymbol{\alpha}, \boldsymbol{\beta}) - s(\boldsymbol{\beta}, \boldsymbol{\beta}),$$
$$(\boldsymbol{\alpha}, \varphi(\boldsymbol{\beta})) = r(\boldsymbol{\alpha}, \boldsymbol{\beta}) + s(\boldsymbol{\alpha}, \boldsymbol{\alpha}).$$

Odkiaľ

$$s((\boldsymbol{\alpha}, \boldsymbol{\alpha}) + (\boldsymbol{\beta}, \boldsymbol{\beta})) = 0$$

Keďže $s \neq 0$, $\boldsymbol{\alpha} \neq \vec{\mathbf{0}}$, $\boldsymbol{\beta} \neq \vec{\mathbf{0}}$ posledná rovnosť nemôže nastať - spor! □

Dôsledok. *Každá symetrická transformácia $\varphi : \boldsymbol{E}(R) \to \boldsymbol{E}(R)$ má aspoň jeden charakteristický vektor, t.j. aspoň jeden jednorozmerný invariantný podpriestor.*

Dôkaz. Je to jasné, lebo charakteristický polynóm má aspoň jeden reálny koreň (pozri vetu 4.7). □

Lema 5.1. *Nech $\varphi : \boldsymbol{E}(R) \to \boldsymbol{E}(R)$ je symetrická transformácia euklidovského priestoru dimenzie n. Nech $\boldsymbol{\alpha}$ je charakteristický vektor tejto transformácie prislúchajúci vlastnej hodnote λ. Nech $\boldsymbol{S}$ je množina všetkých vektorov priestoru $\boldsymbol{E}(R)$, ktoré sú ortogonálne k vektoru $\boldsymbol{\alpha}$. Potom $\boldsymbol{S}$ je podpriestor dimenzie $n-1$ invariantný k transformácii φ.*

Dôkaz. a) Dokážeme,že $\boldsymbol{S} \subseteq\subseteq \boldsymbol{E}(R)$. Nech $\boldsymbol{\mu}, \boldsymbol{\nu} \in \boldsymbol{S}$. Potom $(\boldsymbol{\mu} + \boldsymbol{\nu}, \boldsymbol{\alpha}) = (\boldsymbol{\mu}, \boldsymbol{\alpha}) + (\boldsymbol{\nu}, \boldsymbol{\alpha}) = 0 + 0 = 0$, čiže $\boldsymbol{\mu} + \boldsymbol{\nu} \in \boldsymbol{S}$. Podobne sa dokáže, že $c\boldsymbol{\mu} \in \boldsymbol{S}$, kde $c \in R$.

b) Ak v $\boldsymbol{E}(R)$ uplatníme ortogonalizačný proces tak, aby $\boldsymbol{\alpha}$ bol prvý vektor ortogonálnej bázy. $\{\boldsymbol{\alpha}, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3, \ldots, \boldsymbol{\alpha}_n\}$ vidíme, že $\boldsymbol{S} = [\boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3, \ldots, \boldsymbol{\alpha}_n]$ a teda $d(\boldsymbol{S}) = n - 1$.

c) Dokážeme, že $\boldsymbol{S}$ je invariantný podpriestor. Nech $\boldsymbol{\mu} \in \boldsymbol{S}$, t.j. $(\boldsymbol{\alpha}, \boldsymbol{\mu}) = 0$. Vidieť, že $\varphi(\boldsymbol{\mu}) \in \boldsymbol{S}$. Naozaj, $(\varphi(\boldsymbol{\mu}), \boldsymbol{\alpha}) = (\boldsymbol{\mu}, \varphi(\boldsymbol{\alpha})) = (\boldsymbol{\mu}, \lambda\boldsymbol{\alpha}) = \lambda(\boldsymbol{\mu}, \boldsymbol{\alpha}) = 0$. □

Veta 5.6. *Nech $\varphi : \boldsymbol{E}(R) \to \boldsymbol{E}(R)$ je symetrická transformácia. Potom existuje ortonormálna báza priestoru $\boldsymbol{E}(R)$ taká, že matica transformácie φ vzhľadom na ňu má diagonálny tvar.*

Dôkaz. Vzhľadom na vetu 4.6 stačí v $\boldsymbol{E}(R)$ zostrojiť ortonormálnu bázu pozostávajúcu z vlastných vektorov. To urobíme takto:

Zvolíme v $\boldsymbol{E}(R)$ vlastný vektor $\boldsymbol{\alpha}$, ktorý existuje podľa dôsledku vety 5.5. Potom aj $\boldsymbol{\alpha}_1 = \frac{\boldsymbol{\alpha}}{|\boldsymbol{\alpha}|}$ je vlastný vektor veľkosti jedna.

Podľa lemy 5.1 zostrojíme invariantný podpriestor $\boldsymbol{S}$, v ktorom podľa toho istého dôsledku existuje jednotkový vlastný vektor $\boldsymbol{\alpha}_2$ ortogonálny k $\boldsymbol{\alpha}_1$. Takto postupujeme ďalej až zostrojíme bázu $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_n\}$ navzájom ortogonálnych vlastných vektorov veľkosti jedna. □

Príklad 5.7. Vo vektorovom priestore $\boldsymbol{V}_4(R)$ je dané symetrické zobrazenie φ nasledovnou maticou (vzhľadom na kanonickú bázu, ktorá je zrejme ortonormálna)

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

Nájdeme ortogonálnu bázu priestoru $\boldsymbol{V}_4(R)$ pozostávajúcu z invariantných vektorov. Ak prejdeme na túto bázu, tak podľa vety 5.6 matica transformácie bude mať diagonálny tvar.

Najprv nájdeme vlastné čísla transformácie. Charakteristická rovnica je

$$\begin{vmatrix} 1-\lambda & 1 & 1 & 1 \\ 1 & 1-\lambda & -1 & -1 \\ 1 & -1 & 1-\lambda & -1 \\ 1 & -1 & -1 & 1-\lambda \end{vmatrix} = 0.$$

Ak prvý riadok determinantu odčítame od ostatných a determinant rozvinieme podľa posledného riadku, dostaneme

$$\begin{vmatrix} 1-\lambda & 1 & 1 & 1 \\ 2-\lambda & 2-\lambda & 0 & 0 \\ 2-\lambda & 0 & 2-\lambda & 0 \\ 2-\lambda & 0 & 0 & 2-\lambda \end{vmatrix} =$$

$$-(2-\lambda)\begin{vmatrix} 1 & 1 & 1 \\ 2-\lambda & 0 & 0 \\ 0 & 2-\lambda & 0 \end{vmatrix} + (2-\lambda)\begin{vmatrix} 1-\lambda & 1 & 1 \\ 2-\lambda & 2-\lambda & 0 \\ 2-\lambda & 0 & 2-\lambda \end{vmatrix} =$$

$$= -(2-\lambda)^3 + (2-\lambda)\big((1-\lambda)(2-\lambda)^2 - (2-\lambda)^2 - (2-\lambda)^2\big) = \cdots = (\lambda-2)^3(\lambda+2) = 0.$$

Dostali sme charakteristickú rovnicu $(\lambda-2)^3(\lambda+2) = 0$, ktorá má korene $\lambda_1 = -2$, $\lambda_2 = \lambda_3 = \lambda_4 = 2$. Podľa (4.5) sústava rovníc pre koreň λ_1 bude

$$\begin{aligned} 3x_1 + x_2 + x_3 + x_4 &= 0, \\ x_1 + 3x_2 - x_3 - x_4 &= 0, \\ x_1 - x_2 + 3x_3 - x_4 &= 0, \\ x_1 - x_2 - x_3 + 3x_4 &= 0, \end{aligned}$$

ktorý upravíme na

$$\begin{aligned} 3x_1 + x_2 + x_3 + x_4 &= 0, \\ x_1 + x_2 &= 0, \\ x_1 + x_3 &= 0. \end{aligned}$$

Vidíme, že sústava má len tri lineárne nezávislé rovnice. Položíme $x_1 = p$ a dostaneme podpriestor riešení danej sústavy $\{(p, -p, -p, -p);\ p \in R\}$. Pre $p = 1$ máme charakteristický vektor prislúchajúci vlastnému číslu -2

$$\alpha = (1, -1, -1, -1).$$

Pre vlastné číslo 2 (trojnásobný koreň) máme sústavu

$$\begin{aligned} -x_1 + x_2 + x_3 + x_4 &= 0, \\ x_1 - x_2 - x_3 - x_4 &= 0, \\ x_1 - x_2 - x_3 - x_4 &= 0, \\ x_1 - x_2 - x_3 - x_4 &= 0. \end{aligned}$$

Hneď vidieť, že sústava má len jednu lineárne nezávislú rovnicu. Preto podpriestor jeho riešení bude $\{(p_1 + p_2 + p_3,\ p_1,\ p_2,\ p_3);\ p_1, p_2, p_3 \in R\}$. Dostaneme tri vektory prislúchajúce vlastnému číslu 2.

$$\begin{aligned} \beta_1 &= (1, 1, 0, 0), \\ \beta_2 &= (1, 0, 1, 0), \\ \beta_3 &= (1, 0, 0, 1). \end{aligned}$$

Čitateľ nech sa presvedčí o tom, že tieto vektory sú lineárne nezávislé, ale nie navzájom ortogonálne. Na druhej strane, všetky sú ortogonálne k vektoru α. Preto podľa lemy 5.1 generujú invariantný podpriestor $[\beta_1, \beta_2, \beta_3]$. Ďalej, nech čitateľ skontroluje, že všetky štyri vlastné vektory $\alpha, \beta_1, \beta_2, \beta_3$ sú lineárne nezávislé a teda tvoria bázu priestoru $\boldsymbol{V}_4(R)$. Keby sme túto bázu použili už teraz, dostali by sme už podľa vety 4.6 diagonálnu maticu zobrazenia. My však chceme, aby bázu tvorili *navzájom ortogonálne* vlastné vektory, čo má ilustrovať vetu 5.6. Uplatníme preto ortogonalizačný proces popísaný v paragrafe 5 kapitoly 2 (pozri vetu 5.4) tak, aby vznikla ortogonálna báza $\{\eta_1, \eta_2, \eta_3, \eta_4\}$ pozostávajúca z vlastných vektorov. Zoberme bázu $\{\alpha, \beta_1, \beta_2, \beta_3\}$. Keďže vektory α a β_1 sú ortogonálne, môžeme prvý krok ortogonalizačného procesu vynechať a rovno položiť $\eta_1 = \alpha$, $\eta_2 = \beta_1$ a prikročiť k druhému kroku: $\eta_3 = \beta_2 + c_1\eta_1 + c_2\eta_2$. Ponecháme na čitateľa, aby zistil, že $c_1 = 0$, $c_2 = -\frac{1}{2}$ a vypočítal $\eta_3 = (\frac{1}{2}, -\frac{1}{2}, 1, 0)$. V ďalšom kroku položíme $\eta_4 = \beta_3 + d_1\eta_1 + d_2\eta_2 + d_3\eta_3$. Čitateľ znova zistí, že $d_1 = 0$, $d_2 = -\frac{1}{2}$, $d_3 = -\frac{1}{3}$ a vypočíta $\eta_4 = (\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}, 1)$. Keďže násobením vektora nenulovým skalárom sa zrejme ortogonalita neporuší, môžeme miesto vektora η_3 resp. η_4 vziať jeho dvojnásobok resp. trojnásobok. Máme tak ortogonálnu bázu

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

Je jednoduché sa uistiť, že vektory sú naozaj navzájom ortogonálne (teda aj lineárne nezávislé), že vektory η_3, η_4 a teda aj ich násobky sú vlastné vektory zobrazenia φ. Podľa vety 4.6 matica transformácie vzhľadom na bázu B je diagonálna. Môžeme sa o tom presvedčiť aj priamo. Naozaj podľa dôsledku vety 4.6 matica prechodu od kanonickej bázy k báze B je (jej inverznú maticu čitateľ vypočíta ako užitočné cvičenie)

$$\mathbf{P} = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 2 & 0 \\ 1 & -1 & -1 & 3 \end{pmatrix}, \qquad \mathbf{P}^{-1} = \begin{pmatrix} \frac{1}{4} & \frac{1}{2} & \frac{1}{6} & \frac{1}{12} \\ -\frac{1}{4} & \frac{1}{2} & -\frac{1}{6} & -\frac{1}{12} \\ -\frac{1}{4} & 0 & \frac{1}{3} & -\frac{1}{12} \\ -\frac{1}{4} & 0 & 0 & \frac{1}{4} \end{pmatrix}.$$

Matica transformácie vzhľadom na bázu B je

$$\begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 2 & 0 \\ 1 & -1 & -1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{4} & \frac{1}{2} & \frac{1}{6} & \frac{1}{12} \\ -\frac{1}{4} & \frac{1}{2} & -\frac{1}{6} & -\frac{1}{12} \\ -\frac{1}{4} & 0 & \frac{1}{3} & -\frac{1}{12} \\ -\frac{1}{4} & 0 & 0 & \frac{1}{4} \end{pmatrix} =$$

$$= \begin{pmatrix} -2 & 2 & 2 & 2 \\ 2 & 2 & 0 & 0 \\ 2 & -2 & 4 & 0 \\ 2 & -2 & -2 & 6 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{4} & \frac{1}{2} & \frac{1}{6} & \frac{1}{12} \\ -\frac{1}{4} & \frac{1}{2} & -\frac{1}{6} & -\frac{1}{12} \\ -\frac{1}{4} & 0 & \frac{1}{3} & -\frac{1}{12} \\ -\frac{1}{4} & 0 & 0 & \frac{1}{4} \end{pmatrix} = \begin{pmatrix} -2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Výsledná matica transformácie vzhľadom na ortogonálnu bázu B je diagonálna matica, na hlavnej diagonále ktorej sú vlastné čísla transformácie. Ponecháme čitateľovi, aby vykonal prechod na ortonormálnu bázu a určil maticu prechodu od kanonickej bázy priamo k ortonormálnej báze. Aká bude matica transformácie vzhľadom na túto bázu? Čitateľ iste vie, že bude taká istá, zatiaľ čo matica prechodu bude, pravdaže, iná.

Cvičenia

5.1 V priestore $\boldsymbol{V}_2(R)$ je daná lineárna transformácia $\varphi : V_2(R) \to V_2(R)$. Zistite priamo (bez použitia vety 5.2) či ide o ortogonálnu transformáciu.

a) $\varphi(\boldsymbol{\varepsilon}_1) = \boldsymbol{\varepsilon}_1, \quad \varphi(\boldsymbol{\varepsilon}_2) = -\boldsymbol{\varepsilon}_2,$
b) $\varphi(\boldsymbol{\varepsilon}_1) = -\boldsymbol{\varepsilon}_1, \quad \varphi(\boldsymbol{\varepsilon}_2) = \boldsymbol{\varepsilon}_2,$
c) $\varphi(\boldsymbol{\varepsilon}_1) = -\boldsymbol{\varepsilon}_1, \quad \varphi(\boldsymbol{\varepsilon}_2) = -\boldsymbol{\varepsilon}_2,$
d) $\varphi(\boldsymbol{\varepsilon}_1) = \boldsymbol{\varepsilon}_2, \quad \varphi(\boldsymbol{\varepsilon}_2) = \boldsymbol{\varepsilon}_1,$

kde $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2\}$ je kanonická báza priestoru $\boldsymbol{V}_2(R)$.

5.2 V priestore $\boldsymbol{V}_2(R)$ je daná báza $\boldsymbol{\eta}_1 = (3, 2)$, $\boldsymbol{\eta}_2 = (1, 1)$. Rozhodnite, či lineárne transformácie dané maticami sú ortogonálne transformácie.

$$\mathbf{A} = \begin{pmatrix} \sqrt{3} - 2 & \frac{-3\sqrt{3}+11}{2} \\ -1 & \frac{\sqrt{3}+5}{2} \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} 8 & 1 \\ 0 & 5 \end{pmatrix}.$$

5.3 V priestore $\boldsymbol{V}_2(R)$ je daná báza $\boldsymbol{\eta}_1 = (3, 2)$, $\boldsymbol{\eta}_2 = (1, 1)$. Rozhodnite, či lineárne transformácie dané maticami sú symetrické transformácie.

$$\mathbf{A} = \begin{pmatrix} -4 & 21 \\ -1 & 7 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} 3 & 1 \\ 2 & 5 \end{pmatrix}.$$

5.4 V priestore $\boldsymbol{V}_2(R)$ je daná lineárna transformácia $\varphi : V_2(R) \to V_2(R)$. Zistite či ide o symetrickú transformáciu.

a) $\varphi((x, y)) = (x + 5y,\ 5x + 2y)$,
b) $\varphi((x, y)) = (x + 2y,\ 3x + 4y)$.

5.5 Vo vektorovom priestore $\boldsymbol{V}_3(R)$ sú dané symetrické transformácie nasledovnými maticami (vzhľadom na kanonickú bázu). Pre každú z nich nájdite ortonormálnu bázu pozostávajúcu z invariantných vektorov, maticu prechodu k tejto báze, ako aj diagonálnu maticu transformácie vzhľadom na túto bázu.

$$\mathbf{A} = \begin{pmatrix} 1 & 3 & 0 \\ 3 & -2 & -1 \\ 0 & -1 & 1 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 1 & -2 \\ -1 & -2 & 1 \end{pmatrix}, \qquad \mathbf{C} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 1 \end{pmatrix},$$

$$\mathbf{D} = \begin{pmatrix} 1 & -3 & -1 \\ -3 & 1 & 1 \\ -1 & 1 & 5 \end{pmatrix}, \qquad \mathbf{E} = \begin{pmatrix} 14 & -2 & 4 \\ -2 & 17 & 2 \\ 4 & 2 & 14 \end{pmatrix}, \qquad \mathbf{F} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Návod. Matica $\mathbf{E}$ má charakteristický polynóm $-\lambda^3 + 45\lambda^2 - 648\lambda + 2916$, ktorý má korene $\lambda_1 = 9$, $\lambda_2 = \lambda_3 = 18$.

LITERATÚRA

[1] BICAN, L.: *Lineární algebra*, SNTL, Praha (1979).

[2] BIRKHOFF, G.- MAC LANE, S.: *Prehľad modernej algebry*, Alfa, Bratislava (1979).

[3] BLAŽEK, J. - CALDA, E.- KOMAN, M. - KUSSOVÁ, B.: *Algebra a teoretická aritmetika, I. díl*, SPN, Praha (1983).

[4] FADDEJEV, A. K.- SOMINSKIJ, J. S.: *Zbierka úloh z vyššej algebry*, Alfa, Bratislava (1968).

[5] GELFAND, I. M.: *Lineární algebra*, ČSAV, Praha (1953).

[6] HAVEL, V. - HOLENDA, J.: *Lineární algebra*, SNTL/Alfa, Praha/Bratislava (1984).

[7] CHUDÝ, J.: *Determinanty a matice*, SNTL, Praha (1974).

[8] JEŚMIANOWICZ, L.- ŁOŚ, J.: *Zbiór zadań z algebry*, PWN, Warszawa (1976).

[9] JAEGER, A. - WENKE, K.: *Lineárna hospodárska algebra*, Alfa, Bratislava (1978).

[10] KATRIŇÁK, T. a kol.: *Algebra a teoretická aritmetika (1)*, Alfa, Bratislava (1985).

[11] KLENOVČAN, P.- HAVIAR, A. - HAVIAR, M.: *Úvod do štúdia matematiky (skriptum)*, UMB, Banská Bystrica (1996).

[12] KOŘÍNEK, V. : *Základy algebry*, ČSAV, Praha (1956).

[13] LEGÉŇ, A.: *Grupy okruhy a zväzy*, Alfa, Bratislava (1980).

[14] MOSTOWSKI, A. - STARK, M.: *Algebra liniowa*, PWN, Warszawa (1975).

[15] PALUMBÍNY, D. - VRÁBEL, P.: *Teoretická aritmetika (skriptum)*, VŠPg, Nitra (1994).

[16] PROSKURJAKOV, I. V.: *Sbornik zadač po linejnoj algebre*, GITTL, Moskva (1957).

[17] SCHWARZ, Š.: *Základy náuky o riešení rovníc*, SAV, Bratislava (1968).

[18] SMITAL, J. - GEDEONOVÁ, E. - ZNÁM, Š.: *Úvod do lineárnej algebry (skriptum)*, UK, Bratislava (1978).

[19] SMITAL, J. - GEDEONOVÁ, E.: *Lineárna algebra (skriptum)*, UK, Bratislava (1983).