ŽILINSKÁ UNIVERZITA
FAKULTA RIADENIA A INFORMATIKY

Stanislav Palúch, Ida Stankovianska

ALGEBRA

VYDALA ŽILINSKÁ UNIVERZITA V ŽILINE, 2007

Recenzenti: Xxxxxxxxx Xxxxxxxxxx
Xxxxxxxx Xxxxxxxxxxxx

Schválil rektor ŽU výmerom XX/2007

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

ISBN-80-XXXX-XXX-X

Úvod

O algebre

V Žiline, 26. októbra 2006 Autori.

Obsah

Kapitola 1

Binárne relácie

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

Definícia 1.2. **Karteziánsky súčin** $A \times B$ **dvoch množín** A**,** B je množina všetkých usporiadaných dvojíc tvaru (a, b), kde $a \in A$, $b \in B$. **Karteziánsky súčin** $A_1 \times A_2 \times \cdots \times A_n$ **množín** $A_1, A_2, \ldots, A_n$ je množina všetkých usporiadaných n-tíc $(a_1, a_2, \ldots, a_n)$, kde $a_i \in A_i$ pre $i = 1, 2, \ldots, n$.

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

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

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

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

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

Definícia 1.3. **Binárna relácia** ρ **na množine** V je podmnožina karteziánskeho súčinu $V \times V$. Všeobecnejšie: Ľubovoľnú podmnožinu karteziánskeho súčinu V^n nazveme **n-árnou reláciou na množine** V.

Definícia 1.4. Hovoríme, že binárna relácia ρ na množine V je

reflexívna, ak pre každé $v \in V$ platí $v \,\rho\, v$,

irreflexívna, ak pre žiadne $v \in V$ neplatí $v \, \rho \, v$,
symetrická, ak pre každé $u, v \in V$ z platnosti $u \, \rho \, v$ vyplýva platnosť $v \, \rho \, u$,
antisymetrická, ak pre každé $u, v \in V$ z platnosti $u \, \rho \, v$ a $v \, \rho \, u$ vyplýva $u = v$,
tranzitívna, ak pre každé $u, v, w \in V$ z platnosti $u \, \rho \, v$ a $v \, \rho \, w$ vyplýva $u \, \rho \, w$.

Definícia 1.5. **Zobrazenie** F je taká binárna relácia z X do Y, že pre každé $x \in X$ existuje nanajvýš jedno $y \in Y$ také, že $x \, F \, y$. (Vtedy namiesto $x \, F \, y$ píšeme $y = F(x)$.)
Definujme množiny $\mathcal{D}_F \subseteq X$, $\mathcal{H}_F \subseteq Y$

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

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

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

1.1 Ekvivalencia a rozklad množiny

Definícia 1.6. **Ekvivalencia** alebo **relácia ekvivalencie** na množine V je binárna relácia na V ktorá je reflexívna, symetrická a tranzitívna.

Definícia 1.7. **Rozkladom množiny** V nazveme systém podmnožín $A_i \subseteq V$, $i \in I$ taký, že $A_i \cap A_j = \emptyset$ pre $i, j \in I$, $i \neq j$ a $\bigcup_{i \in I} A_i = V$. Množiny A_i, $i \in I$ nazveme **triedami rozkladu**.

Definícia 1.8. Nech P je relácia ekvivalencie na množine V, nech $a \in V$. **Triedou ekvivalencie** P **k prvku** a nazveme množinu

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

Prvok a nazveme reprezentantom triedy $[a]$.

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

Dôkaz.
Najprv ukážeme, že ak $[a] \cap [b] \neq \emptyset$, potom $[a] = [b]$. Nech $s \in [a] \cap [b]$. Nech

$x \in [a]$. Potom podľa definície $[a]$, $[b]$ je

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

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

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

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

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

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

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

Reflexivita a symetria relácie P vyplývajú priamo z definície.

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

1.2 Usporiadanie

Definícia 1.9. Hovoríme, že relácia $\preceq$ je **usporiadanie** na množine V, ak $\preceq$ je reflexívna, tranzitívna a antisymetrická relácia. Dvojicu $(V, \preceq)$, kde $\preceq$ je usporiadanie na V voláme **čiastočne usporiadaná množina** .
Nech $\preceq$ je usporiadanie na množine V, nech pre prvky $u \in V$, $v \in V$ neplatí ani $u \preceq v$, ani $v \preceq u$. Potom hovoríme, že prvky u, v sú **neporovnateľné**.
Lineárne usporiadanie je také usporiadanie $\preceq$ na V, že pre každú dvojicu prvkov $u, v \in V$ je $u \preceq v$ alebo $v \preceq u$. Dvojicu $(V, \preceq)$, kde P je lineárne usporiadanie na V, voláme **lineárne usporiadaná množina** alebo **reťazec**.

Kapitola 2

Algebraické štruktúry

2.1 Algebraické štruktúry s jednou binárnou operáciou

Pod algebraickou štruktúrou rozumieme množinu M

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

Definícia 2.2. Pod algebraickou štruktúrou rozumieme neprázdnu množinu M spolu s niekoľkými binárnymi operáciami. Presnejšie: Algebraická štruktúra je usporiadaná n-tica $\mathcal{A} = (M, \circ_1, \circ_2, \ldots, \circ_{n-1})$, kde M je neprázdna množina a $\circ_1, \circ_2, \ldots, \circ_{n-1}$ sú binárne oprácie na množine M.

Definícia 2.3. Grupoid je algebraická štruktúra $(M, \circ)$ s jednou operáciou.

Definícia 2.4. Nech $\circ$ je binárna operácia na neprázdnej množine M, $e \in M$. Hovoríme, že e je

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

Definícia 2.5. Nech $\circ$ je binárna operácia na neprázdnej množine M. Nech existuje neutrálny prvok $e \in M$, nech $a, b \in M$. Hovoríme, že a je

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

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

Veta 2.1. *Nech $(M, \circ)$ je grupoid, v ktorom existuje ľavý neutrálny prvok $e_l \in M$ a aj pravý neutrálny prvok $e_p \in M$. Potom $e_l = e_p$, a teda v M existuje neutrálny prvok $e = e_l = e_p$.*

Dôkaz. Platí
$$e_l \circ e_p = e_p, \tag{2.1}$$
pretože e_l je ľavý neutrálny prvok. Súčasne platí
$$e_l \circ e_p = e_l, \tag{2.2}$$
pretože e_p je pravý neutrálny prvok. Z rovnosti ľavých strán (2.1) (2.2) vyplýva $e_l = e_p$. ∎

Dôsledkom vety 2.1 je skutočnosť, že v grupoide môže existovať nanajvýš jeden neutrálny prvok.

Definícia 2.6. Majme grupoid $(M, \circ)$. Hovoríme, že binárna operácia $\circ$ je

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

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

- operácia $\otimes$ je sprava distributívna vzhľadom k operácii $\otimes$, ak pre všetky $a, b, c \in M$ platí
$$(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c) \tag{2.3}$$
- operácia $\otimes$ je zľava distributívna vzhľadov k operácii $\otimes$, ak pre všetky $a, b, c \in M$ platí
$$c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b) \tag{2.4}$$
- operácia $\otimes$ distributívna vzhľadov k operácii $\otimes$ ak $\otimes$ je súčasne distributívna k $\oplus$ súčasne sprava i zľava.

Definícia 2.7. Grupoid $(M, \circ)$ je

- pologrupa, ak jej operácia $\circ$ je asociatívna
- monoid, ak jej operácia $\circ$ je asociatívna a v M existuje neutrálny prvok

- grupa, ak jej operácia $\circ$ je asociatívna, v M existuje neutrálny prvok a ku každému prvku $a \in M$ existuje symetrizačný prvok.

Ak je v grupe $(M, \circ)$ naviac operácia $\circ$ komutatívna, hovoríme, že $(M, circ)$ je komutatívna grupa,. Pre komutatívnu grupu sa v literatúre používa tiež termín ábelovská grupa.

Veta 2.2. *Nech $(M, \circ)$ je pologrupa s neutrálnym prvkom $e \in M$. nech a_p resp. a_l je pravý, resp. ľavý symetrizačný prvok k prvku $b \in M$. Potom $a_p = a_l$, a teda existuje symetrizačný prvok k prvku b.*

Dôkaz. Platí $a \circ a_p = e$ a súčasne $a_l \circ a = e$. Potom

$$a_l = a_l \circ e = a_l \circ (a \circ a_p) = (a_l \circ a) \circ a_p = e \circ a_p = a_p. \tag{2.5}$$

■

Veta 2.3. *Nech $(G, \circ)$ je grupa, $a, \underset{\text{-}}{,}\, q \in G$.*

$$\text{Ak platí} \quad q \circ a = q \circ b, \qquad \text{potom platí } a = b. \tag{2.6}$$
$$\text{Ak platí} \quad a \circ q = b \circ q, \qquad \text{potom platí } a = b. \tag{2.7}$$

Dôkaz. Dokážeme (2.6).

$$\begin{aligned} q \circ a &= q \circ b && (2.8)\\ \overline{q} \circ (q \circ a) &= \overline{q} \circ (q \circ b) && (2.9)\\ (\overline{q} \circ q) \circ a &= (\overline{q} \circ q) \circ b && (2.10)\\ e \circ a &= e \circ b && (2.11)\\ a &= b && (2.12) \end{aligned}$$

Implikácia (2.7) sa dokáže analogicky.

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

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

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

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

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

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

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

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

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

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

$$x \diamond y = x \circ y, \tag{2.13}$$

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

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

Dôkaz. Platí $e_B = e_B \diamond e_B$. Pretože $(B, \diamond)$ je podgrupou grupy $(A, \circ)$,

$$e_B = e_B \circ e_B. \tag{2.14}$$

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

$$e_B = e_B \circ e_A. \tag{2.15}$$

Z posledných dvoch rovností máme

$$e_B \circ e_B = e_B \circ e_A, \tag{2.16}$$

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

2.2 Okruhy a telesá

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

- $(M, \oplus)$ je komutatívna grupa
- $(M, \otimes)$ je pologrupa

- Operácia $\otimes$ je distributávna vzhľadom k operácii $\oplus$, t.j. platia distributívne zákony:

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) \qquad (a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c) \tag{2.17}$$

Grupu $(M, \oplus)$ budme volať aditívnou grupou okruhu $\mathcal{O}$, pologrupu $(M, \otimes)$ multiplikatívnou pologrupou okruhu $\mathcal{O}$.
Neutrálny prvok aditívnej grupy okruhu $\mathcal{O}$ budeme označovať symbolom 0 a budeme ho volať nulovým prvkom aditívnej grupy, resp. okruhu $\mathcal{O}$.

Veta 2.8. *Nech $\mathcal{O} = (M, \oplus, \otimes)$ je okruh. Potom pre všetky $a \in M$ platí*

$$a \otimes 0 = 0 \otimes a = 0 \tag{2.18}$$

Dôkaz.

$$\begin{aligned} b \oplus 0 &= b \\ (b \oplus 0) \otimes a &= b \otimes a \\ (b \otimes a) \oplus (0 \otimes a) &= b \otimes a \\ (0 \otimes a) &= 0 \end{aligned} \tag{2.19}$$

■

Definícia 2.10. Nech $\mathcal{T} = (M, \oplus, \otimes)$ je okruh. Hovoríme, že $\mathcal{T}$ je teleso , ak algebraická štruktúra $(M - \{0\}, \otimes)$ je grupou. Ak je naviac operácia $\otimes$ komutatívna na množine M, hovoríme, že $\mathcal{T}$ je komutatívne teleso, alebo tiež pole .
Neutrálny prvok grupy $(M - \{0\}, \otimes)$ budeme označovať symbolom 1 a budeme ho volať jednotkovým prvkom telesa $\mathcal{T}$.
Symetrizačný prvok k prvku a v aditívnej grupe telesa $\mathcal{T}$ nazveme opačný prvok k prvku a a budeme ho označovať $\ominus a$.
Symetrizačný prvok k prvku a v grupe $(M - \{0\}, \otimes)$ nazveme inverzný prvok k prvku a a budeme ho označovať a^{-1}.

Veta 2.9. *Nech $a,\ b$ sú ľubovoľné prvky telesa $\mathcal{T}$. Potom*

$$(\ominus a) \otimes b = a \otimes (\ominus b) = \ominus(a \otimes b) \tag{2.20}$$

$$(\ominus a) \otimes (\ominus b) = a \otimes b \tag{2.21}$$

Dôkaz.

$$\begin{aligned} a \oplus (\ominus a) &= \quad 0 \\ [a \oplus (\ominus a)] \otimes b &= \quad 0 \otimes b = 0 \\ (a \otimes b) \oplus [(\ominus a) \otimes b] &= \quad 0 \\ [(\ominus a) \otimes b] &= \quad \ominus(a \otimes b) \end{aligned} \tag{2.22}$$

$$\begin{aligned} [a \oplus (\ominus a)] \otimes b &= 0 \\ (a \otimes b) \oplus [(\ominus a) \otimes b] &= 0 \\ (a \otimes b) &= \ominus[(\ominus a) \otimes b] \\ (a \otimes b) &= (\ominus a) \otimes (\ominus b) \end{aligned} \tag{2.23}$$

■

Veta 2.10. *V telese $\mathcal{T} = (M, \oplus, \otimes)$ platí pre každé $a,\ b \in M$*

$$\text{ak } a \otimes b = 0 \quad \text{potom} \quad a = 0 \text{ alebo } b = 0. \tag{2.24}$$

Dôkaz. Nech platí

$$a \otimes b = 0 \tag{2.25}$$

Nech $a \neq 0$ Potom existuje inverzný prvok a^{-1} a platí

$$\begin{aligned} a^{-1} \otimes (a \otimes b) = &\ 0 \\ (a^{-1} \otimes a) \otimes b = &\ 0 \\ 1 \otimes b = &\ 0 \\ b = &\ 0 \end{aligned} \tag{2.26}$$

■

Definícia 2.11. Nech $\mathcal{O}$ je okruh s aspň dvoma prvkami. Ak pre každé dva prvky $a,\ b$ okruhu $\mathcal{O}$ platí

$$\text{ak } a \otimes b = 0 \quad \text{potom} \quad a = 0 \text{ alebo } b = 0, \tag{2.27}$$

potom hovorím, že $\mathcal{O}$ je obor integrity .

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

- $$B \subseteq A \tag{2.28}$$

- $$\text{Pre každé } a,\ b \in B \qquad \text{platí} \quad a \boxplus b = a \oplus b \qquad a \boxtimes b = a \otimes b. \tag{2.29}$$

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

Veta 2.11. *Nech $(A, \oplus, \otimes)$ je teleso, nech $B \subset A$. Potom $(B, \oplus, \otimes)$ je podtelesom telesa $(A, \oplus, \otimes)$ práve vtedy, keď platí*

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

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

iii) Pre každý prvok $a \in B$ je aj $a^{-1} \in B$.

Dôkaz. Ak je $(B, \oplus, \otimes)$ podtelesom telesa $(A, \oplus, \otimes)$, je samo telesom, a preto i), ii), iii) platia.

Je $B \subset A$ a nech platia i), ii), iii). Vlastnosť (2.28) je splnená podľa predpokladu $B \subset A$, vlastnosť (2.29) takisto platí.

Treba ukázať, že $(B, \oplus, \otimes)$ je teleso, t.j. že $(B, \oplus)$ je komutatívna grupa, $(B - \{0\}, \otimes)$ je grupa a platia distributívne zákony.

Kapitola 3

Polynómy

3.1 Definícia polynómu a operácie s polynómami

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

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

Nech $a_0, a_1, \ldots, a_n$ sú pevne zvolené prvky telesa $\mathcal{T}$. Potom zobrazenie $p_n : T \to T$, ktoré každému $x \in T$ priradí hodnotu

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

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

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

- $a_0 + a_1 x$, kde $a_1 \neq 0$ – polynóm 1. stupňa
- a_0, kde $a_0 \neq 0$ – polynóm nulého stupňa
- 0 – polynóm stupňa -1

Definícia 3.2. Hovoríme, že dva polynómy nad telesom $\mathcal{T}$

$$p_n(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \tag{3.4}$$
$$q_m(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m \tag{3.5}$$

sú si rovné a píšeme $p_n = q_m$, ak pre všetky $x \in T$ platí $p_n(x) = q_m(x)$.

Odteraz predpokladajme, že $m \leq n$.

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

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

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

$$x_{n+m}(x) = p_n(x).q_m(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n+m}x^{n+m}, \tag{3.7}$$

kde

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

Násobok polynómu $p_n(x)$ prvkom $\alpha \in T$ definujeme ako polynóm $t_n(x)$

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

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

Veta 3.1 (Základná veta algebry)**.** *Nech $\mathcal{C} = (C, +, \ .)$ je teleso komplexných čísel. Každý polynóm $p_n(x)$ stupňa $n \geq 1$ má aspoň jeden koreň.*

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

$$p_n(x) = p_n(c) + (x - c).q_{n-1}(x), \tag{3.10}$$

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

Dôkaz.

$$\begin{aligned} p_n(x) - p_n(c) &= \\ &= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n - (a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n) = \\ &= (a_0 - a_0) + a_1(x - c) + a_2(x^2 - c^2) + \cdots + a_n(x^n - c^n) = \\ &= (x - c).\underbrace{\left[a_1 + a_2(x + c) + \cdots + a_n(x^{n-1} + x^{n-2}c + \cdots + c_{n-1})\right]}_{q_{n-1}(x)} \end{aligned} \tag{3.11}$$

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

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

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

$$p_n(x) = a_n.(x - c_1).(x - c_2). \ldots .(x - c_n), \tag{3.13}$$

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

Definícia 3.4. Vzťah (3.13) nazývame rozklad polynómu $p_n(x)$ na súčin koreňových činiteľov, každý polynóm prvého stupňa $x - c_i$ zo vzťahu (3.13) nazývame koreňovým činiteľom .
Ak

$$p_n(x) = (x - c)^k.q_{n-k}(x), \tag{3.14}$$

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

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

$$p_n(x) = a_n.(x - c_1)^{k_1}.(x - c_2)^{k_2}. \ldots .(x - c_r)^{k_r} \tag{3.15}$$

Veta 3.6. *Nech $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm s celočíselnými koeficientami. Ak racionálne číslo $r = \dfrac{p}{p}$, kde p, q sú nesúdeliteľné čísla je jeho koreňom, potom p delí a_0 a q delí a_n.*

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

$$\begin{aligned}
0 &= a_0 + a_1\frac{p}{q} + a_2\frac{p^2}{q^2} + \cdots + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + a_n\frac{p^n}{q^n} \\
0 &= a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_{n-1}p^{n-1}q + a_np^n \\
a_0q^n &= -\big(a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_{n-1}p^{n-1}q + a_np^n\big) && (3.16) \\
a_np^n &= -\big(a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_{n-1}p^{n-1}q\big) && (3.17)
\end{aligned}$$

Definícia 3.5. Hovoríme, že polynóm $p(x)$ nad telesom $\mathcal{T}$ je reducibilný, ak existujú dva polynómy $q(x)$, $r_(x)$ oba aspoň prvého stupňa také, že

$$p(x) = q(x).r(x). \tag{3.18}$$

V opačnom prípade hovorím, že $p(x)$ je ireducibilný polynóm,

Veta 3.7. *Rovnosť polynómov*

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

nad telesom komplexných čísel $\mathcal{C}$ *nastáva práve vtedy, keď* $m = n$ *a* $a_i = b_i$ *pre* $i = 1, 2, \ldots, n$.

Dôkaz. Predpokladajme $m \leq n$. Položme $r(x) = p_n(x) - q_m(x)$

$$r(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_m - b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n. \quad (3.19)$$

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

3.2 Hornerova schéma

Nech $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm n-tého stupňa nad telesom komplexných čísel. Podľa (3.10) platí

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

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

$$q_{n-1}(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}$$

Našou úlohou bude určiť koeficienty b_i polynómu $q_{n-1}(x)$.

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

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

$$\begin{aligned}
b_{n-1} &= a_n \\
b_{n-2} &= a_{n-1} + cb_{n-1} \\
b_{n-3} &= a_{n-2} + cb_{n-2} \\
&\dots \\
b_{n-j} &= a_{n-j+1} + cb_{n-j+1} \\
&\dots \\
b_0 &= a_1 + cb_1 \\
p_n(c) &= a_0 + cb_0
\end{aligned}$$

3.3 Polynómy s reálnymi koeficientami

Veta 3.8. *Nech $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm n-tého stupňa nad telesom komplexných čísel. Nech všetky koeficienty polynómu $p_n(x)$ sú reálne čísla.*
Ak komplexné číslo $c = \alpha + i\beta$ je koreňom polynómu $p_n(x)$, potom aj komplexne združené číslo $\overline{c} = \alpha - i\beta$ je koreňom polynómu $p_n(x)$.

Dôkaz.

$$\begin{aligned}
a_0 + a_1c + a_2c^2 + \cdots + a_nc^n &= 0 && (3.20) \\
\overline{a_0 + a_1c + a_2c^2 + \cdots + a_nc^n} &= 0 && (3.21) \\
\overline{a_0} + \overline{a_1c} + \overline{a_2c^2} + \cdots + \overline{a_nc^n} &= 0 && (3.22) \\
a_0 + a_1\overline{c} + a_2(\overline{c})^2 + \cdots + a_n(\overline{c})^n &= 0 && (3.23)
\end{aligned}$$

■

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

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

Veta 3.9. *Nech $p_n(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm n-tého stupňa s reálnymi koeficientami. Nech $c_1, c_2, \ldots, c_r$ sú všetky navzájom rôzne reálne korene s násobnosťami $n_1, n_2, \ldots, n_r$ a čísla $(\alpha_1 + i\beta_1), (\alpha_2 + i\beta_2), \ldots, (\alpha_s + i\beta_s)$ všetky rôzne komlexné korene také, že $\beta_k > 0$ pre $k = 1, 2, \ldots, s$ s násobnosťami*

$m_1, m_2, \dots, m_s$. Potom aj čísla $(\alpha_1 - i\beta_1), (\alpha_2 - i\beta_2), \dots, (\alpha_s - i\beta_s)$ sú porade $m_1, m_2, \dots, m_s$ - násobné korene polynomu $p_n(x)$ a platí

$$\begin{aligned} p_n(x) = a_n.(x-c_1)^{n_1}.(x-c_2)^{n_2}.\dots.(x-c_r)^{n_r}. \\ .(x^2+p_1x+q_1)^{m_1}.(x^2+p_2x+q_2)^{m_2}.\dots.(x^2+p_sx+q_s)^{m_s}, \end{aligned} \tag{3.24}$$

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

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

Vzťah (3.24) môžeme skrátene zapísať nasledovne

$$p_n(x) = a_n.\prod_{j=1}^{r}(x-c_j)^{n_j}.\prod_{k=1}^{s}(x^2+p_kx+q_k)^{m_k}. \tag{3.25}$$

3.4 Deliteľnosť polynómov

Definícia 3.6. Hovoríme, že polynóm $q(x)$ delí polynóm $p(x)$, ak existuje taký polynóm $r(x)$, že platí

$$p(x) = q(x).r(x). \tag{3.26}$$

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

Hovoríme, že $r(x)$ je najväčším spoločným deliteľom polynómov $p(x)$, $q(x)$, ak je spoločným deliteľom polynómov $p(x)$, $q(x)$ a je deliteľný každým iným spoločným deliteľom týchto polynómov.

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

Ako deliť polynómy. Majme polynómy:

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

kde $m \le n$

$$\begin{aligned} p_n(x) = \underbrace{\left[p_n(x) - \frac{a_n}{b_m}.q_m(x).x^{n-m}\right]}_{p_{n-1}(x)} + q_m(x).\left(\frac{a_n}{b_m}.x^{n-m}\right) = \\ = p_{n-1}(x) + q_m(x).c_{n-m}.x^{n-m} \end{aligned} \tag{3.27}$$

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

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

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

$$\begin{aligned}
p_n(x) &= \underbrace{p_{n-1}(x)}_{p_{n-2}(x)+q_m(x).c_{n-m-1}.x^{n-m-1}} + q_m(x).c_{n-m}.x^{n-m} = \\
&= \underbrace{p_{n-2}(x)}_{p_{n-3}(x)+q_m(x).c_{n-m-2}.x^{n-m-2}} + q_m(x).c_{n-m}.x^{n-m} + q_m(x).c_{n-m-1}.x^{n-m-1} = \\
&\dots \\
&= \underbrace{p_{n-k}(x)}_{r(x)} + q_m(x).\underbrace{(c_{n-m}.x^{n-m} + c_{n-m-1}.x^{n-m-1} + \dots + c_1.x + c_0)}_{s(x)-\text{ polynóm stupňa } n-m} \qquad (3.28)
\end{aligned}$$

Práve popísaný postup vedie ku vzťahu

$$p_n(x) = q_m(x).s(x) + r(x), \qquad (3.29)$$

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

3.5 Euklidov algoritmus

Postupne vyjadrujme

$$\begin{aligned}
p(x) &= q(x).s(x) + r_1(x) && (3.30)\\
q(x) &= r_1(x).s_1(x) + r_2(x) && (3.31)\\
r_1(x) &= r_2(x).s_2(x) + r_3(x) \\
r_2(x) &= r_3(x).s_3(x) + r_4(x) \\
&\dots \\
r_{k-2}(x) &= r_{k-1}(x).s_{k-1}(x) + r_k(x) && (3.32)\\
&\dots \\
r_{m-2}(x) &= r_{m-1}(x).s_{m-1}(x) + r_m(x) && (3.33)\\
r_{m-1}(x) &= r_m(x).s_m(x) + 0 && (3.34)
\end{aligned}$$

Teraz ukážeme, že $r_m(x)$ je najväčší spoločný deliteľ polynómov $q(x)$, $p(x)$.

Zo vzťahu (3.34) vyplýva, že $r_m(x)$ delí $r_{m-1}(x)$. Z tejto skutočnosti a zo vzťahu (3.33) vyplýva, že $r_m(x)$ delí aj $r_{m-2}(x)$ atď. až dospejeme k záveru, že $r_m(x)$ delí $q(x)$ aj $p(x)$.

Naopak, nech $t(x)$ delí $q(x)$ aj $p(x)$. Podľa (3.30) $r_1(x) = p(x) - q(x).s(x)$, a preto $t(x)$ delí aj $r_1(x)$. Podľa (3.31) $r_2(x) = q(x) - r_1(x).s_1(x)$, a preto $t(x)$ delí aj $r_2(x)$. Takto postupne dokážeme, že $t(x)$ delí $r_m(x)$.

Veta 3.10 (Bezoutova rovnosť)**.** *Nech $p(x)$ a $q(x)$ sú nenulové polnómy a nech $r(x)$ je ich najväčší spoločný deliteľ. Potom existujú také polynómy $u(x)$ a $v(x)$, že platí*

$$r(x) = p(x).u(x) + q(x).v(x). \qquad (3.35)$$

Dôkaz. V Euklidovom algoritme (3.34) je najväčší spoločný deliteľ $r(x) = r_m(x)$. Zo vzťahu (3.33) máme

$$r(x) = r_{m-2}(x) - r_{m-1}(x).\underbrace{s_{m-1}(x)}_{-v_1(x)} \qquad (3.36)$$

Ak položíme $u_1(x) = 1$ a $v_1(x) = -s_{m-1}(x)$, prepíšeme (3.36) takto

$$r(x) = r_{m-2}(x).u_1(x) + r_{m-1}.v_1(x). \qquad (3.37)$$

Zo vzťahu (3.32) pre $k = m-1$ máme $r_{m-1}(x) = r_{m-3}(x) - r_{m-2}(x)s_{m-2}(x)$, z čoho po dosadení za $r_{m-1}(x)$ do (3.37)

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

Takto po $(m-1)$ krokoch dostaneme

$$r(x) = p(x).u_{m-1}(x) + q(x).v_{m-1}(x). \tag{3.38}$$

■

Dôkaz predchádzajúcej vety dáva návod, ako k ľubovoľnému polynómu $p(x)$ zostrojiť polynóm $u(x)$ tak, aby súčin polynómov $p(x).u(x)$ po vydelení polynómom $q(x)$ dal zvyšok $r(x)$, ktorý je najväčším spoločným deliteľom polynómov $p(x)$, $q(x)$. Vzťah (3.36) možno totiž prepísať

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

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

Definícia 3.7. Polynómy $r(x)$ a $s(x)$ sú kongruentné modulo $q(x)$, píšeme

$$r(x) \equiv s(x) \mod q(x), \tag{3.39}$$

ak polynóm $r(x) - s(x)$ je deliteľný polynómom $q(x)$.

Vieme teda riešiť rovnicu

$$p(x).y(x) \equiv r(x) \mod q(x). \tag{3.40}$$

Ak najväčším spoločným deliteľom polynómov $p(x)$, $q(x)$ je polynóm $r(x) = 1$, rovnica (3.40) má tvar

$$p(x).y(x) \equiv 1 \mod p(x). \tag{3.41}$$

```
nsd(a,b)
r[0]=a, r[1]=b, t[0]=0, t[1]=1;
i=0;
while r[i+1]!=0
{q[i+1]=r[i]/[i+1];
 r[i+2]=r[i]%r[i+1];
 t[i+2]=(t[i]-q[i+1].t[i+1])%r[0];
 i++;}
return r[i];
```

3.6 Racionálna funkcia a jej rozklad na elementárne zlomky

Definícia 3.8. Nech $p(x)$, $q(x)$ sú dva polynómy. Funkciu

$$f(x) = \frac{p(x)}{q(x)} \tag{3.42}$$

nazveme racionálnou funkciou.
Nech $\operatorname{st}\big(p(x)\big) = m$, $\operatorname{st}\big(q(x)\big) = n$. Ak $m < n$, hjovoríme, že (3.42) je rýdzo racionálna funkcia.

Poznámka. Každá racionálna funkcia (3.42) sa dá vyjadriť ako súčet

$$f(x) = r(x) + \frac{z(x)}{q(x)}, \tag{3.43}$$

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

Definícia 3.9. Funkcie tvaru

$$\frac{A}{(x-a)^k} \qquad \text{alebo } \frac{Bx+C}{(x^2+bx+c)^k}, \tag{3.44}$$

kde A, B, C, a, b sú reálne čísla, k prirodzené číslo a (x^2+bx+c) nemá reálne korene, (tj. $(b^2-4c) < 0$), nazývame elementárnymi zlomkami.

Veta 3.11. *Nech funkcia $f(x) = \frac{p(x)}{q(x)}$ je rýdzo racionálna. Nech c je k-násobným koreňom polynómu $q(x)$. Potom existuje také číslo A a taký polynóm $p_1(x)$ stupňa nižšieho než stupeň polynómu $(x-c)^{k-1}.q_1(x)$, že platí*

$$\frac{p(x)}{q(x)} = \frac{A}{(x-c)^k} + \frac{p_1(x)}{(x-c)^{k-1}.q_1(x)}. \tag{3.45}$$

Veta 3.12. *Nech $f(x) = \frac{p(x)}{q(x)}$ je rýdzo racionálna funkcia. Nech koeficienty $q(x)$ sú reálne čísla. Nech komplexné číslo $\alpha + i\beta$, ($\alpha \in R$, $\beta \in R$, $\beta \neq 0$) je k-násobným koreňom polynómu $q(x)$. Označme $a = -2\alpha$, $b = \alpha^2 + \beta^2$.*
Potom existujú čísla M, N a taký polynóm $p_1(x)$ stupňa nižšieho než stupeň polynómu $(x^2+ax+c)^{k-1}.q_1(x)$, že platí

$$\frac{p(x)}{q(x)} = \frac{Mx+N}{(x^2+ax+c)^k} + \frac{p_1(x)}{(x^2+ax+c)^{k-1}.q_1(x)}. \tag{3.46}$$

Nech $q(x) = (x-c)^k.q_1(x)$. Postupnou aplikáciou vety 3.11 dostaneme:

$$\begin{aligned}
\frac{p(x)}{q(x)} &= \frac{A_k}{(x-c)^k} + \frac{p_1(x)}{(x-c)^{k-1}.q_1(x)} = \\
&= \frac{A_k}{(x-c)^k} + \frac{A_{k-1}}{(x-c)^{k-1}} + \frac{p_2(x)}{(x-c)^{k-2}.q_1(x)} = \\
&= \dots \\
&= \frac{A_k}{(x-c)^k} + \frac{A_{k-1}}{(x-c)^{k-1}} + \dots + \frac{A_1}{(x-c)^1} + \frac{p_k(x)}{(x-c)^{k-k}.q_1(x)} = \\
&= \frac{A_k}{(x-c)^k} + \frac{A_{k-1}}{(x-c)^{k-1}} + \dots + \frac{A_1}{(x-c)^1} + \frac{p_k(x)}{q_1(x)} \qquad (3.47)
\end{aligned}$$

Uvedením (3.47) na spoločného menovateľa, ktorým je $q(x) = (x-c)^k.q_1(x)$ dostaneme vyjadrenie čitateľa zlomku $f(x) = \dfrac{p(x)}{q(x)}$ pomocou čísel $A_1, A_2, \dots, A_k$. Provnaním koeficientov u rovnakých mocnín oboch vyjadrení dostaneme sústavu lineárnych rovníc pre $A_1, A_2, \dots, A_k$.

Analogickym, ak $q(x) = (x^2+ax+c)^k.q_1(x)$ potom postupnou aplikáciou vety 3.12 dostaneme:

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

Uvedením posledného výrazu na spoločného menovateľa, ktorým je $q(x) = (x^2 + ax+c)^k.q_1(x)$ dostaneme vyjadrenie čitateľa zlomku $f(x) = \dfrac{p(x)}{q(x)}$ pomocou čísel $M_1, N_1, M_2, N_2 \dots, M_k, N_k$. Provnaním koeficientov u rovnakých mocnín oboch vyjadrení dostaneme sústavu lineárnych rovníc pre $M_1, N_1, M_2, N_2 \dots, M_k, N_k$.

3.7 Konečné telesá*

Definícia 3.10. Nech $q > 1$ je prirodzené číslo. Faktorový okruh Z_q je q-prvková množina $\{0, 1, 2, \ldots, q-1\}$ spolu s operáciami $\oplus$, $\otimes$ definovannými pre $r,\ s \in Z_q$ nasledovne

$$r \oplus s = r + s \mod q \tag{3.48}$$
$$r \otimes s = r.s \mod q \tag{3.49}$$

Veta 3.13. *Faktorový okruh modulo q Z_q je teleso práve vtedy, keď q je prvočíslo.*

Definícia 3.11. Nech T je komutatívne teleso, $q(x)$ polynóm nad stupňa $n \geq 0$ telesom T. Definujme okruh polynómov modulo $q(x)$ $T/q(x)$ s operáciami $\oplus$, $\otimes$ nasledovne:

- Prvkami okruhu $T/q(x)$ sú všetky polynómy $q(z)$ nad telesom T stupňa nanajvýš $n-1$.
- Pre $a(z),\ b(z) \in T/q(x)$ definujeme
$$a(z) \oplus b(z) = a(z) + b(z), \tag{3.50}$$
t.j. ako obvyklý súčet polynómov.
- Pre $a(z),\ b(z) \in T/q(x)$ definujeme
$$a(z) \otimes b(z) = a(z).b(z) \mod q(z), \tag{3.51}$$
t.j. ako zvyšok po delení polynómu $(z).b(z)$ polynómom $q(z)$.

Veta 3.14. *Pre každý ireducibilný polynóm $q(x)$ nad telesom T je okruh polynómov $T/q(x)$ telesom.*

Definícia 3.12. Teleso $Z_p/q(x)$, kde p je prvočíslo a $q(x)$ ireducibilný polynóm stupňa n nad telesom Z_p, sa nazýva Galoisovo pole (alebo Galoisovo teleso) a označuje sa $GF(p^n)$.

Veta 3.15. *Každé konečné teleso je izomorfné s niektorým Galoisovým telesom.*

Kapitola 4

Lineárne priestory

V tejto kapitole budeme pracovať s pojmom lineárneho priestoru, ktorý je založený na dvoch algebraických štruktúrach, a to komutatívnom telese $\mathcal{T} = (T, \boxplus, \boxdot)$ a komutatívnej grupe $\mathcal{V} = (V, \oplus)$. Prvky množiny V nazveme vektormi , grupu $\mathcal{V}$ grupou vektorov Prvky telesa $\mathcal{T}$ budeme značiť italikou – napríklad $t \in T$, $s \in T$, vektory – prvky grupy $\mathcal{V}$ tučnými malými písmenami, napríklad $\mathbf{u} \in V$, $\mathbf{v} \in V$.

Pri tomto značení budeme pre jednoduchosť písať pre $t,\ s \in T$ $t+s$ namiesto $t \boxplus s$, ts resp. $t.s$ namiesto $t \boxdot s$. Pre $\mathbf{u}, \mathbf{v} \in V$ budeme písať $\mathbf{u}+\mathbf{v}$ namiesto $\mathbf{u} \oplus \mathbf{v}$.

Toto si môžeme dovoliť bez ujmy na presnosti, pretože podľa príslušnosti operandov k množine T resp. k množine V bude jasné, o ktorú operáciu sa jedná. Vždy však majme na pamäti, že operácia $+$ je iná v zápise $t + s$ ako v zápise $\mathbf{u} + \mathbf{v}$.

4.1 Lineárny priestor a podpriestor

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

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

ktorá každej usporiadanej dvojici $(t, \mathbf{v})$, $t \in T$, $\mathbf{v} \in V$ priradí prvok $t \otimes \mathbf{v} \in V$. Hovoríme, že množina V s operáciou $+$ a vonkajšou operáciou $\otimes$ je lineárny priestor nad telesom $\mathcal{T}$, ako platí

$$\begin{aligned}
\forall t, s \in T, \quad \forall \mathbf{v} \in V \qquad t \otimes (s \otimes \mathbf{v}) &= (ts) \otimes \mathbf{v} && (4.2)\\
\forall t, s \in T, \quad \forall \mathbf{v} \in V \qquad (t + s) \otimes \mathbf{v} &= (t \otimes \mathbf{v}) + (s \otimes \mathbf{v}) && (4.3)\\
\forall t \in T, \quad \forall \mathbf{u}, \mathbf{v}, \in V \qquad t \otimes (\mathbf{u} + \mathbf{v}) &= (t \otimes \mathbf{u}) + (t \otimes \mathbf{v}) && (4.4)\\
\forall \mathbf{v}, \in V \qquad 1_T \otimes \mathbf{v} &= \mathbf{v} && (4.5)\\
& && (4.6)
\end{aligned}$$

Pre jednoduchosť zápisu budeme písať $t.\mathbf{v}$ alebo len $t\mathbf{v}$ namiesto $t \otimes \mathbf{v}$ pre $t \in T$, $v \in V$; namiesto 1_T len 1. Podobne

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

$$\begin{aligned}
\forall t, s \in T, \quad \forall \mathbf{v} \in V \qquad t.(s.\mathbf{v}) &= (ts).\mathbf{v} && (4.7)\\
\forall t, s \in T, \quad \forall \mathbf{v} \in V \qquad (t + s).\mathbf{v} &= (t.\mathbf{v}) + (s.\mathbf{v}) && (4.8)\\
\forall t \in T, \quad \forall \mathbf{u}, \mathbf{v}, \in V \qquad t.(\mathbf{u} + \mathbf{v}) &= (t.\mathbf{u}) + (t.\mathbf{v}) && (4.9)\\
\forall \mathbf{v}, \in V \qquad 1.\mathbf{v} &= \mathbf{v} && (4.10)\\
& && (4.11)
\end{aligned}$$

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

Veta 4.1. *Majme lineárny priestor s grupovu vektorov $\mathcal{V} = (V, +)$ nad telesom $\mathcal{T}$. Potom platí*

$$\begin{aligned}
0.\mathbf{v} &= \mathbf{o} && (4.12)\\
(-1).\mathbf{v} &= -\mathbf{v} && (4.13)
\end{aligned}$$

Dôkaz. Dokážeme (4.12). Platí:

$$\mathbf{v} + 0.\mathbf{v} = 1.\mathbf{v} + 0.\mathbf{v} = (1 + 0).\mathbf{v} = \mathbf{v} \tag{4.14}$$

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

Dokážeme (4.13).

$$\mathbf{v} + (-1.)\mathbf{v} = 1.\mathbf{v} + (-1).\mathbf{v} = (1 - 1).\mathbf{v} = 0.\mathbf{v} = \mathbf{o}. \tag{4.15}$$

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

Definícia 4.2. Lineárny priestor $(U, \boxplus, \boxtimes)$ nad telesom T nazveme lineárnym podpriestorom priestoru $(V, \oplus, \otimes)$ nad telesom T, ak $U \subseteq V$ a pre všetky $\mathbf{u},\ \mathbf{v} \in U$ a všetky $t \in T$ platí:

i) $\mathbf{u} \boxplus \mathbf{v} = \mathbf{u} \oplus \mathbf{v}$

ii) $t \boxtimes \mathbf{v} = t \otimes \mathbf{v}$

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

i) $\mathbf{u} + \mathbf{v} \in U$

ii) $t\mathbf{u} \in U$

Dôkaz. Ak $(U, +, .)$ je lineárnym podpriestorom priestoru $(V, +, .)$, i), ii) platia.

Ak platia i), ii), potom $0\mathbf{u} = \mathbf{o} \in U$ a pre každé $\mathbf{v} \in U$ je aj $-1.\mathbf{v} = -\mathbf{v} \in U$, čo spolu s asociativitou a komutativitou operácie + hovorí, že $(V, +)$ je komutatívna grupa. Keďže vlastnosti lineárneho priestoru 4.7 až 4.10 (pozri str. 32) platia pre všetky $t \in T$ a všetky $\mathbf{u},\ \mathbf{v} \in V$, musia platiť aj pre všetky $\mathbf{u},\ \mathbf{v} \in U$. ■

4.2 Lineárna nezávislosť

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

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

Definícia 4.4. Hovoríme, že vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne nezávislé, ak z rovnosti

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{o} \tag{4.17}$$

vyplýva

$$a_1 = 0, \quad a_2 = 0, \quad \ldots, \quad a_n = 0. \tag{4.18}$$

Veta 4.3. *Nech vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne nezávislé, nech $t \neq 0$, $t_2, t_3, \ldots, t_n$ sú prvky telesa T. Potom aj vektory*

$$t.\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \tag{4.19}$$

a

$$\left[\mathbf{v}_1 + (t_2.\mathbf{v}_2 + t_3.\mathbf{v}_3 + \cdots + t_n.\mathbf{v}_n)\right], \mathbf{v}_2, \ldots, \mathbf{v}_n \tag{4.20}$$

sú lineárne nezávislé.

Dôkaz. Nech

$$a_1.(t.\mathbf{v}_1) + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{o} \tag{4.21}$$

$$(a_1.t).\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{o} \tag{4.22}$$

Pretože vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne nezávislé, je

$$a_1.t = 0, \quad a_2 = 0, \quad \ldots, \quad a_n = 0, \tag{4.23}$$

a teda, (keďže $t \neq 0$), aj

$$a_1 = 0, \quad a_2 = 0, \quad \ldots, \quad a_n = 0 \tag{4.24}$$

z čoho vyplýva nezávislosť vektorov (4.19).

Nech

$$a_1.\left[\mathbf{v}_1 + (t_2.\mathbf{v}_2 + t_3.\mathbf{v}_3 + \cdots + t_n.\mathbf{v}_n)\right] + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{o}, \tag{4.25}$$

čo je sa dá upraviť na tvar

$$a_1.\mathbf{v}_1 + (a_2 + a_1t_2)\mathbf{v}_2 + (a_3 + a_1t_3)\mathbf{v}_3 + \cdots + (a_n + a_1t_n)\mathbf{v}_n = \mathbf{o}. \tag{4.26}$$

Pretože vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne nezávislé, je

$$a_1 = 0 \tag{4.27}$$

$$a_i + a_1t_i = 0 \quad \text{pre } i = 2, 3, \ldots, n, \tag{4.28}$$

z čoho vyplýva, že $a_i = 0$ pre $i = 1, 2, \ldots, n$, a teda aj lineárna nezávislosť vektorov (4.20). ■

Veta 4.4. *Vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne závislé práve vtedy, keď jeden z nich je lineárnou kombináciou ostatných.*

Dôkaz. Nech vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ sú lineárne závislé, nech

$$\mathbf{o} = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_n\mathbf{v}_n = \sum_{i=1}^{n} t_i\mathbf{v}_i, \tag{4.29}$$

kde pre niektoré k platí $t_k \neq 0$. Potom

$$t_k\mathbf{v}_k = \sum_{\substack{i=1\\ i\neq k}}^{n} t_i\mathbf{v}_i \tag{4.30}$$

$$\mathbf{v}_k = \sum_{\substack{i=1\\ i\neq k}}^{n} (t_k^{-1}t_i)\mathbf{v}_i. \tag{4.31}$$

Nech na druhej strane je niektorý z vektorov $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ lineárnou kombi- náciou ostatných, t.j. nech

$$\mathbf{v}_k = \sum_{\substack{i=1\\k\neq 0}}^{n} t_i \mathbf{v}_i. \tag{4.32}$$

Potom

$$\mathbf{o} = \sum_{\substack{i=1\\i\neq k}}^{n} t_i \mathbf{v}_i + (-1)\mathbf{v}_k = \sum_{i=1}^{n} t_i \mathbf{v}_i, \tag{4.33}$$

kde $t_k = -1$. ■

Definícia 4.5. Množinu $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ vektorov lineárneho priestoru nazveme bázou lineárneho priestoru, ak platí:

i) vektory $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ sú linárne nezávislé

ii) pre ľubovoľný vektor $\mathbf{a}$ sú vektory $\mathbf{a}, \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ lineárne závislé.

Podmienku ii) možno vzhľadom na vetu 4.4 preformulovať nasledovne:

ii') Každý vektor $\mathbf{a}$ možno napísať ako lineárnu kombináciou vektorov $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$.

Poznámka. Nie v každom linárnom priestore existuje báza.

Veta 4.5. *Nech $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ je báza lineárneho priestoru $\mathcal{L}$, $\mathbf{w} \in V$. Potom existuje aspoň jeden vektor $\mathbf{b}_k$ bázy $\mathbf{B}$ taký, že*

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{w}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n \tag{4.34}$$

je tiež bázou lineárneho priestoru $\mathcal{L}$.

Dôkaz. Nech $\mathbf{w} \neq \mathbf{o}$

$$\mathbf{w} = \sum_{i=1}^{n} a_i \mathbf{b}_i = \sum_{\substack{i=1\\i\neq k}}^{n} a_i \mathbf{b}_i + a_k \mathbf{b}_k = a_k^{-1}\left[\sum_{\substack{i=1\\i\neq k}}^{n} (a_k^{-1} a_i)\mathbf{b}_i + \mathbf{b}_k\right] \tag{4.35}$$

kde $a_k \neq 0$. (Také k musí existovať, inak by $\mathbf{w} = \mathbf{o}$.)
Podľa vety 4.4 sú vektory

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{w}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$$

lineárne nezávislé.

$$a_k \mathbf{b}_k = \mathbf{w} - \sum_{\substack{i=1 \\ i \neq k}}^{n} a_i \mathbf{b}_i \tag{4.36}$$

$$\mathbf{b}_k = a_k^{-1} \mathbf{w} - \sum_{\substack{i=1 \\ i \neq k}}^{n} a_k^{-1} a_i \mathbf{b}_i \tag{4.37}$$

Ak

$$\mathbf{x} = x_1 \mathbf{b}_1 + x_2 \mathbf{b}_2 + \cdots + x_n \mathbf{b}_n \tag{4.38}$$

$$\mathbf{x} = \sum_{\substack{i=1 \\ i \neq k}}^{n} x_i \mathbf{b}_i + x_k \mathbf{b}_k \tag{4.39}$$

$$\mathbf{x} = \sum_{\substack{i=1 \\ i \neq k}}^{n} x_i \mathbf{b}_i + x_k \left[a_k^{-1} \mathbf{w} - \sum_{\substack{i=1 \\ i \neq k}}^{n} a_k^{-1} a_i \mathbf{b}_i \right] \tag{4.40}$$

$$\mathbf{x} = \sum_{\substack{i=1 \\ i \neq k}}^{n} (x_i - a_k^{-1} a_i x_k) \mathbf{b}_i + a_k^{-1} x_k \mathbf{w}. \tag{4.41}$$

Podľa posledného vzťahu možno každý vektor $\mathbf{x}$ vyjadriť ako lineárnu kombináciu vektorov

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{w}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$$

.

Vektory $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{w}, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$ tvoria bázu lineárneho priestoru. ■

Poznámka. Z dôkazu vety 4.5 vyplýva, že vektorom $\mathbf{w}$ možno nahradiť ktorýkoľvek z vektorov $\mathbf{b}_k$, ktorý sa v lineárnej kombinácii (4.35) vyskytuje s nenulovým koeficientom a_k.

Veta 4.6. *Nech* $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$, $\mathbf{C} = (\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m)$ *sú dve bázy lineárneho priestoru* $\mathcal{L}$. *Potom* $m = n$, *t.j. obe bázy majú rovnaký počet prvkov.*

Dôkaz. Predpokladajme $m \leq n$. Podla vety 4.5 existuje k, $1 \leq k \leq n$ také, že vektory $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{c}_1, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$ tvoria tiež bázu lineárneho priestoru $\mathcal{L}$, ktorú označíme symbolom $\mathbf{B}_1$.

Nech má báza $\mathbf{B}_j = (\mathbf{b}_1^j, \mathbf{b}_2^j, \ldots, \mathbf{b}_n^j)$, kde $(n-j)$ prvkov je z bázy $\mathbf{B}$ a j prvkov je z bázy $\mathbf{C}$ – sú to práve vektory $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_j$. Nech

$$\mathbf{c}_{j+1} = \sum_{i=1}^{n} t_i \mathbf{b}_i^j \tag{4.42}$$

Medzi sčítancami 4.42 musí byť aspoň jeden vektor $\mathbf{b}_{k_1}$ pôvodnej bázy $\mathbf{B}$ s nenulovým koeficientom, inak by bol vektor $\mathbf{c}_{j+1}$ lineárnou kombináciou prvkov bázy $\mathbf{C}$, čo by bolo v spore s lineárnou nezávislosťou prvkov bázy $\mathbf{C}$. Podla vety 4.5 a podľa poznámky za touto vetou možno vytvoriť bázu $\mathbf{B}_{j+1}$ nahradením vektora $\mathbf{b}_{k_1}$ vektorom $\mathbf{c}_{j+1}$. Táto báza bude obsahovať vektory $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_j, \mathbf{c}_{j+1}$ a $(n-j-1)$ vektorov z bázy $\mathbf{B}$.
Báza $\mathbf{B}_n$ bude obsahovať vektory $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$. Keby bolo $n < m$, vektor $\mathbf{c}_{n+1}$ by sa dal vyjadriť ako lineárna kombinácia ostatných vektorov z $\mathbf{C}$, čo by bolo v spore s linárnou nezávislosťou vektorov bázy $\mathbf{C}$. ■

Definícia 4.6. Hovoríme, že lineárny priestor $\mathcal{L}$ má konečnú dimenziu n, ak existuje báza $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ s počtom prvkom n.

Veta 4.7. *Nech $\mathcal{L}$ je lineárny priestor s konečnou dimenziou n. Nech $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ je báza lineárneho priestoru $\mathcal{L}$. Potom ľubovoľný vektor $\mathbf{x} \in V$ sa dá jednoznačne vyjadriť v tvare*

$$\mathbf{x} = t_1\mathbf{b}_1 + t_2\mathbf{b}_2 + \cdots + t_n\mathbf{b}_n = \sum_{i=1}^{n} t_i\mathbf{b}_i. \tag{4.43}$$

Dôkaz. Nech

$$\mathbf{x} = t_1\mathbf{b}_1 + t_2\mathbf{b}_2 + \cdots + t_n\mathbf{b}_n \tag{4.44}$$
$$\mathbf{x} = s_1\mathbf{b}_1 + s_2\mathbf{b}_2 + \cdots + s_n\mathbf{b}_n \tag{4.45}$$

Potom

$$\mathbf{o} = (t_1 - s_1)\mathbf{b}_1 + (t_2 - s_2)\mathbf{b}_2 + \cdots + (t_n - s_n)\mathbf{b}_n \tag{4.46}$$

Z lineárnej nezávislosti vektorov bázy $\mathbf{B}$ vyplýva $(t_i - s_i) = 0$, a teda $t_i = s_i$ pre $i = 1, 2, \ldots, n$. ■

Definícia 4.7. Nech $\mathcal{L}$ je lineárny priestor s konečnou dimenziou n. Nech $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ je báza lineárneho priestoru $\mathcal{L}$, $\mathbf{x} \in V$. Nech

$$\mathbf{x} = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_n\mathbf{v}_n = \sum_{i=1}^{n} t_i\mathbf{v}_i. \tag{4.47}$$

Prvky $t_1, t_2, \ldots, t_n$ nazývame súradnice vektora $\mathbf{x}$ v báze $\mathbf{B}$.

4.3 Izomorfizmus lineárnych priestorov

Definícia 4.8. Nech $(U, +, .)$, $V, +, .$ sú dva lineárne priestory nad tým istým telesom $(T, +, .)$ Zobrazenie $f : U \to V$ nazveme izmorfizmom, ak platí

i) f je vzájomne jednoznačné zobrazenie U na V

ii) pre každé $\mathbf{x},\ \mathbf{y} \in U \quad f(\mathbf{x}+\mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$

iii) pre každé $\mathbf{x} \in U$ a pre každé $t \in T \quad f(t\mathbf{x}) = tf(\mathbf{x})$

Ak medzi dvoma linárnymi priestormi existuje izomorfizmus, hovoríme, že tieto lineárne priestory sú izomorfné.

Definícia 4.9. Nech $(T, +, .)$ je komutatívne teleso, T^n množina všetkých usporiadaných n-tíc prvkov z T. Pre $\mathbf{t} = (t_1, t_2, \ldots, t_n) \in T^n$, $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in T^n$ a $t \in T$ definujeme vnútornú operáciu sčítania a vonkajšiu operáciu násobenia nasledovne

$$\mathbf{t} + \mathbf{s} = (t_1 + s_1, t_2 + s_2, \ldots, t_n + s_n) \tag{4.48}$$

$$r\mathbf{t} = (rt_1, rt_2, \ldots, rt_n) \tag{4.49}$$

Potom $(T^n, +, .)$ je lineárny priestor dimenzie n a nazveme ho aritmetický priestor nad telesom T.

Veta 4.8. *Nech $\mathcal{L} = (V.+, .)$ je lineárny priestor s konečnou dimenziou n je izomorfný s aritmetickým priestorom $(T^n, +, .)$ nad telesom T.*

Dôkaz. Nech $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ je báza lineárneho priestoru $\mathcal{L}$. Podľa vety 4.7 ľubovoľný vektor $\mathbf{v} \in V$ sa dá jednoznačne vyjadriť v tvare

$$\mathbf{v} = v_1\mathbf{b}_1 + v_2\mathbf{b}_2 + \cdots + v_n\mathbf{b}_n = \sum_{i=1}^{n} t_i\mathbf{b}_i.$$

Definujme zobrazenie $f : V \to T^n$ predpisom

$$f(\mathbf{v}) = (v_1, v_2, \ldots, v_n), \tag{4.50}$$

kde $(v_1, v_2, \ldots, v_n)$ sú súradnice vektora $\mathbf{v}$ v báze $\mathbf{B}$.

Pre takto definované zobrazenie f sa ľahko overí platnosť podmienok i), ii), iii) z definície 4.8. ■

Definícia 4.10. Lineárny priestor $(U, \boxplus, \boxtimes)$ nad telesom T nazveme lineárnym podpriestorom priestoru $(V, \oplus, \otimes)$ nad telesom T, ak $U \subseteq V$ a pre všetky $\mathbf{u},\ \mathbf{v} \in U$ a všetky $t \in T$ platí:

i) $\mathbf{u} \boxplus \mathbf{v} = \mathbf{u} \oplus \mathbf{v}$

ii) $t \boxtimes \mathbf{v} = t \otimes \mathbf{v}$

Veta 4.9. *Nech $\mathcal{L} = (V, +, .)$ je lineárny priestor nad telesom T, $\emptyset \neq U \subseteq V$. Potom $(U, +, .)$ je lineárnym podpriestorom priestoru $\mathcal{L}$ práve vtedy, keď pre všetky $\mathbf{u},\ \mathbf{v} \in U$ a $t \in T$ platí*

i) $\mathbf{u} + \mathbf{v} \in U$

ii) $t\mathbf{u} \in U$

Dôkaz. Ak $(U, +, .)$ je lineárnym podpriestorom priestoru $(V, +, .)$, i), ii) platia.

Ak platia i), ii), potom $0\mathbf{u} = \mathbf{o} \in U$ a pre každé $\mathbf{v} \in U$ je aj $-1.\mathbf{v} = -\mathbf{v} \in U$, čo spolu s asociativitou a komutativitou operácie $+$ hovorí, že $(V, +)$ je komutatívna grupa. Keďže vlastnosti lineárneho priestoru 4.7 až 4.10 (pozri str. 32) platia pre všetky $t \in T$ a všetky $\mathbf{u},\ \mathbf{v} \in V$, musia platiť aj pre všetky $\mathbf{u},\ \mathbf{v} \in U$. ∎

4.4 Skalárny súčin vektorov

V tejto časti práce budeme pracovať s aritmetickými lineárnymi priestormi nad telesom T, ktoré je podtelesom reálnych čísel. Teleso T bude najčastejšie alebo telesom reálnych čísel, alebo telesom racionálnych čísel alebo konečným telesom typu $\mathbb{Z}_q$, kde q je prvočíslo.
Vektory budú pre nás usporiadané n-tice čísel z telesa T s vnútornou operáciou sčítania a vonkajšou operáciou násobenia definovanými v defnícii 4.9.

Teória skalárnych súčinov sa robí aj všeobecné lineárne priestory nad telesom komplexných čísel. Všeobecnejší prístup však nesie so sebou isté komplikácie, ktorým sa vyhneme, ak sa budeme venovať len reálnemu prípadu.

Definícia 4.11. Nech T je podteleso telesa reálnych čísel. Nech $(T^n, +, .)$ je aritmetický lineárny priestor nad telesom T, $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in T^n$, $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in T^n$. Skalárny súčin $\mathbf{u}.\mathbf{v}$ vektorov $\mathbf{u}$, $\mathbf{v}$ definujeme predpisom

$$\mathbf{u}.\mathbf{v} = (u_1v_1 + u_2v_2 + \cdots + u_nv_n) = \sum_{i=1}^{n} u_iv_i. \tag{4.51}$$

Skalárny súčin je vlastne zobrazenie $g : T^n \times T^n \to T$, kde $g(\mathbf{u}, \mathbf{v}) = \mathbf{uv}$.

Veta 4.10. *Nech* $\mathbf{u} \in T^n$, $\mathbf{v} \in T^n$, $\mathbf{w} \in T^n$, $t \in T$. *Potom platí*

$$\begin{aligned} \mathbf{uv} &= \mathbf{vu} && (4.52)\\ (\mathbf{u}+\mathbf{v})\mathbf{w} &= \mathbf{uw} + \mathbf{vw} && (4.53)\\ (t\mathbf{u})\mathbf{v} &= t(\mathbf{uv}) && (4.54)\\ \mathbf{uu} \geq 0, \mathbf{uu} = 0, & \quad \textit{práve vtedy, keď } \mathbf{u} = \mathbf{o}. && (4.55) \end{aligned}$$

Kapitola 5

Matice a determinanty

5.1 Matice

Definícia 5.1. Nech T je komutatatívne teleso. Obdĺžnikovú schému $m\dot{n}$ prvkov telesa T usporiadanú do m riadkov a n stĺpcov nazývame maticou typu $m \times n$ (nad telesom T). Detailný zápis matice $\mathbf{A}$ je

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \tag{5.1}$$

Používajú sa tiež skrátené zápisy matice $\mathbf{A}$ z (5.1)

$$\mathbf{A} = \left(a_{ij}\right)_{i=1,2,\dots,m}^{i=1,2,\dots,n} = \left(a_{ij}\right)_{m,n} = \left(a_{ij}\right)_{m\times n} = \left(a_{ij}\right)_{mn} = \left(a_{ij}\right)$$

Definícia 5.2. Špeciálne typy matíc. Nech $\mathbf{A}$ je matica definovaná v (5.1).

a) Ak $m = n$, hovoríme, že $\mathbf{A}$ je štvorcová matica stupňa (alebo rádu) n.

b) Ak $a_{ij} = 0$ pre všetky $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$, hovoríme, že $\mathbf{A}$ je nulová matica a značíme ju $\mathbf{O}_{m\times n}$, $\mathbf{O}_{m,n}$, $\mathbf{O}_{mn}$, alebo len $\mathbf{O}$.

c) Ak v štvorcovej matici $\mathbf{A}$ rádu n je $a_{ij} = 0$ pre všetky $i \neq j$, $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$, hovoríme, že $\mathbf{A}$ je diagonálna matica.

d) Ak v štvorcovej matici $\mathbf{A}$ rádu n je $a_{ii} = 1$ a $a_{ij} = 0$ pre všetky $i \neq j$, $i = 1, 2, \dots, n$, $j = 1, 2, \dots, n$, hovoríme, že $\mathbf{A}$ je jednotková matica a značíme ju $\mathbf{E}_n$ alebo len $\mathbf{E}$.

e) Ak v štvorcovej matici $\mathbf{A}$ rádu n je $a_{ij} = 0$ pre všetky $i > j$, $i = 1, 2, \dots, n$, $j = 1, 2, \dots, n$, hovoríme, že $\mathbf{A}$ je horná trojuholníková matica. Ak $a_{ij} = 0$ pre všetky $i < j$, $i = 1, 2, \dots, n$, $j = 1, 2, \dots, n$, hovoríme, že $\mathbf{A}$ je dolná trojuholníková matica.

f) Ak v štvorcovej matici $\mathbf{A}$ rádu n je $a_{ij} = a_{ji}$ pre všetky $i = 1, 2, \dots, n$, $j = 1, 2, \dots, n$, hovoríme, že $\mathbf{A}$ je symetrická matica. Ak $a_{ij} = -a_{ji}$ pre všetky $i = 1, 2, \dots, n$, $j = 1, 2, \dots, n$, hovoríme, že $\mathbf{A}$ je antisymetrická matica. (V antisymetrickej matici musí byť $a_{ii} = 0$ pre všetky $i = 1, 2, \dots, n$.)

g) Každý vektor $\mathbf{v} \in T^n$ n-dimenzionálneho aritmetického linárneho priestoru nad komutatívnym telesom T možno považovať za maticu typu $n \times 1$, t.j. maticu obsahujúcu jediný stĺpec typu

$$\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \tag{5.2}$$

Niekedy sa na maticu (5.2) budeme odvolávať ako na stĺpcový vektor.

h) Ak z danej matice $\mathbf{A}$ vytvoríme inú maticu $\mathbf{B}$ tak, že z matice $\mathbf{A}$ vylúčime niektoré riadky a niektoré stĺpce, hovoríme, že matica $\mathbf{B}$ je podmatica matice $\mathbf{A}$.

i) Ak rozdelíme maticu $\mathbf{A}$ na niekoľko podmatíc tak, že spolu tvoria celú maticu, hovoríme o blokovej matici a jednotlivé podmatica nazývame bloky. Majme maticu $\mathbf{A}$

$$\mathbf{A} = \left(\begin{array}{cc|ccc|c} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} \\ a_{41} & a_{32} & a_{43} & a_{44} & a_{45} & a_{46} \end{array}\right) \tag{5.3}$$

Vyššie vyznačnými zvislými a vodorovnými čiarami sme maticu a rozdelili na bloky

$$\mathbf{A} = \begin{pmatrix} \mathbf{A_{11}} & \mathbf{A_{12}} & \mathbf{A_{13}} \\ \mathbf{A_{21}} & \mathbf{A_{22}} & \mathbf{A_{23}} \end{pmatrix}, \tag{5.4}$$

pričom jednotlivé bloky sú

$$\mathbf{A_{11}} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \mathbf{A_{12}} = \begin{pmatrix} a_{13} & a_{14} & a_{15} \\ a_{23} & a_{24} & a_{25} \end{pmatrix} \quad \mathbf{A_{13}} = \begin{pmatrix} a_{16} \\ a_{26} \end{pmatrix}$$

$$\mathbf{A_{21}} = \begin{pmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{pmatrix} \quad \mathbf{A_{22}} = \begin{pmatrix} a_{33} & a_{34} & a_{35} \\ a_{43} & a_{44} & a_{45} \end{pmatrix} \quad \mathbf{A_{23}} = \begin{pmatrix} a_{36} \\ a_{46} \end{pmatrix}$$

Definícia 5.3. Hovoríme, že dve matice $\mathbf{A} = \left(a_{ij}\right)_{i=1,2,\ldots,m}^{i=1,2,\ldots,n}$ $\mathbf{B} = \left(b_{ij}\right)_{i=1,2,\ldots,p}^{i=1,2,\ldots,q}$ sú si rovné, a píšeme $\mathbf{A} = \mathbf{B}$, ak sú rovnakého typu, t.j. $m = p$ a $n = q$ a pre všetky $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$ je $a_{ij} = b_{ij}$.

Definícia 5.4. Nech $\mathbf{A} = \left(a_{ij}\right)_{m\times n}$, $\mathbf{B} = \left(b_{ij}\right)_{m\times n}$ sú dve matice rovnakého typu $m \times n$. Súčtom $\mathbf{A} + \mathbf{B}$ matice $\mathbf{A}$ a matice $\mathbf{B}$ rozumieme maticu $\mathbf{C} = \left(c_{ij}\right)_{m\times n}$ typu $m \times n$, pre ktorú je

$$c_{ij} = a_{ij} + c_{ij}. \tag{5.5}$$

Skalárnym násobkom $t\mathbf{A}$ matice $\mathbf{A} = \left(a_{ij}\right)_{m\times n}$ typu $m \times n$ prvkom telesa $t \in T$ nazveme maticu $\mathbf{C} = \left(c_{ij}\right)_{m\times n}$ typu $m \times n$, pre ktorú je

$$c_{ij} = ta_{ij}. \tag{5.6}$$

Definícia 5.5. Nech $\mathbf{A} = \left(a_{ij}\right)_{m\times n}$ je matica typu $m\times n$ $\mathbf{B} = \left(b_{ij}\right)_{n\times p}$ je matica typu $n \times p$. Súčinom $\mathbf{A}.\mathbf{B}$ matíc $\mathbf{A}$ a $\mathbf{B}$ rozumieme maticu $\mathbf{C} = \left(c_{ij}\right)_{m\times p}$ typu $m \times p$, pre ktorú je

$$c_{ij} = \sum_{k=1}^{n} a_{ik}.b_{kj} \tag{5.7}$$

pre všetky $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, p$.

Veta 5.1. *Nech $\mathbf{A}_{m\times n}$, $\mathbf{B}_{n\times p}$, $\mathbf{C}_{n\times p}$, $\mathbf{D}_{p\times r}$ sú matice nad komutatívnym telesom T, $t, s, \in T$. Potom platí*

- $\mathbf{A}_{m\times n}(\mathbf{B}_{n\times p}\mathbf{D}_{p\times r}) = (\mathbf{A}_{m\times n}\mathbf{B}_{n\times p})\mathbf{D}_{p\times r}$
- $(\mathbf{B}_{n\times p} + \mathbf{C}_{n\times p})\mathbf{D}_{p\times r} = \mathbf{B}_{n\times p}\mathbf{D}_{p\times r} + \mathbf{C}_{n\times p}\mathbf{D}_{p\times r}$
- $\mathbf{A}_{m\times n}(\mathbf{B}_{n\times p} + \mathbf{C}_{n\times p}) = \mathbf{A}_{m\times n}\mathbf{B}_{n\times p} + \mathbf{A}_{m\times n}\mathbf{C}_{n\times p}$
- $t(s\mathbf{A}) = (ts)\mathbf{A}$
- $\mathbf{E}_m\mathbf{A}_{m\times n} = \mathbf{A}_{m\times n}\mathbf{E}_n$
- $\mathbf{O}_{m\times n} + \mathbf{A}_{m\times n} = \mathbf{A}_{m\times n}$
- $\mathbf{O}_{m\times n}\mathbf{B}_{n\times p} = \mathbf{O}_{m\times n}$
- $\mathbf{B}_{n\times p}\mathbf{O}_{p\times r} = \mathbf{O}_{n\times r}$

Dôkaz. Platnosť každej z uvedených rovností sa overí rozpísaním pravej a ľavej strany. ∎

Definícia 5.6. Nech matica $\mathbf{A}_{m\times n} = \big(a_{ij}\big)_{m\times n}$ je typu $m \times n$. Matica $\mathbf{A}^T = \big(a^T_{ij}\big)_{m\times n}$ typu $n \times m$, pre prvky ktorej platí

$$a^T_{ij} = a_{ji} \tag{5.8}$$

sa nazýva transponovaná matica k matici $\mathbf{A}$.

Veta 5.2. *Pre ľubovoľné matice $\mathbf{A}_{m\times n}$, $\mathbf{B}_{m\times n}$, $\mathbf{C}_{n\times p}$ a $t \in T$ platí*

- $\left(\mathbf{A}^T\right)^T = \mathbf{A}$
- $(\mathbf{A}_{m\times n} + \mathbf{B}_{m\times n})^T = (\mathbf{A}_{m\times n})^T + (\mathbf{B}_{m\times n})^T$
- $(t\mathbf{A}_{m\times n})^T = t(\mathbf{A}_{m\times n})^T$
- $(\mathbf{B}_{m\times n}\mathbf{C}_{n\times p})^T = (\mathbf{C}_{n\times p})^T(\mathbf{B}_{m\times n})^T$

Dôkaz. Platnosť každej z uvedených rovností sa overí rozpísaním pravej a ľavej strany. ■

V definícii 5.2 pod písmenom g) sme konštatovlai, že vektory aritmetického priestoru $(T^n, +, .)$ môžeme interpretovať ako maticu o jednom stĺpci

$$\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

Potom vektor $\mathbf{v}^T$ je maticou typu $1 \times n$

$$\mathbf{v}^T = \big(v_1, v_2, \dots, v_n\big)$$

Nech $\mathbf{u}, \mathbf{v} \in T^n$ sú dva vektory aritmetického lineárneho priestoru $(T^n, +, .)$, $\mathbf{u}^T = (u_1, u_2, \dots, u_n)$, $\mathbf{v}^T = (v_1, v_2, \dots, v_n)$ oba uvažované ako jednostĺpcové matice. Potom pre ich maticový súčin platí

$$\mathbf{u}^T.\mathbf{v} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} . \begin{pmatrix} v_1 & v_2 & \dots & v_n \end{pmatrix} = \left(\sum_{i=1}^n u_i v_i\right) \tag{5.9}$$

Výsledkom je matica typu 1×1 s jediným prvkom, ktorého hodnota je rovná skalárnemu súčinu vektorov $\mathbf{u}$, $\mathbf{v}$. Takúto maticu $\big(a\big)_{1\times 1}$ ztotožňujeme s prvkom $a \in T$.

V definícii 5.2 pod písmenom i) sme hovorili o rozdelení matice **A** na bloky. Často sa ukazuje vhodným nasledujúce rozdelenie

$$\mathbf{A} = \left(\begin{array}{c|c|cc|c} a_{11} & a_{12} & \dots & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & \dots & a_{mn} \end{array}\right) = \begin{pmatrix} \mathbf{s_1} & \mathbf{s_2} & \dots & \dots & \mathbf{s_n}, \end{pmatrix} \tag{5.10}$$

kde $\mathbf{s_i} = (a_{1i}, a_{2i}, \dots, a_{mi})^T$ sú stĺpce matice **A**.

$$\mathbf{A} = \left(\begin{array}{ccccc} \hline a_{11} & a_{12} & \dots & \dots & a_{1n} \\ \hline a_{21} & a_{22} & \dots & \dots & a_{2n} \\ \hline \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \hline a_{m1} & a_{m2} & \dots & \dots & a_{mn} \\ \hline \end{array}\right) = \begin{pmatrix} \mathbf{r_1} \\ \mathbf{r_2} \\ \dots \\ \dots \\ \mathbf{r_m} \end{pmatrix}, \tag{5.11}$$

kde $\mathbf{r_i} = \begin{pmatrix} a_{i1}, a_{i2}, \dots, a_{in} \end{pmatrix}^T$ je i-tý riadok matice **A**

Nech $\mathbf{A} = \begin{pmatrix} a_{ij} \end{pmatrix}_{m\times n}$ je matica typu $m \times n$, $\mathbf{B} = \begin{pmatrix} b_{ij} \end{pmatrix}_{n\times p}$ matica typu $n \times p$, $\mathbf{a_i}$ pre $i = 1, 2, \dots, m$ riadkové vektory matice **A**, $\mathbf{b_i}$ pre $j = 1, 2, \dots, p$ stĺpcové vektory matice **B**. potom

$$\mathbf{A}.\mathbf{B} = \begin{pmatrix} \mathbf{a_1} \\ \\ \mathbf{a_2} \\ \\ \dots \\ \\ \mathbf{a_m} \end{pmatrix} . \begin{pmatrix} \mathbf{b_1} & \mathbf{b_2} & \dots & \mathbf{b_p} \end{pmatrix} = \begin{pmatrix} \mathbf{a_1^T b_1} & \mathbf{a_1^T b_2} & \dots & \mathbf{a_1^T b_p} \\ \\ \mathbf{a_2^T b_1} & \mathbf{a_2^T b_2} & \dots & \mathbf{a_2^T b_p} \\ \\ \dots & \dots & \dots & \dots \\ \\ \mathbf{a_m^T b_1} & \mathbf{a_m^T b_2} & \dots & \mathbf{a_m^T b_p} \end{pmatrix} \tag{5.12}$$

5.2 Determinant matice

Definícia 5.7. Permutácia množiny $\langle n \rangle = \{1, 2, \dots, n\}$ je vzájomne jednoznačné zobrazenie množiny $\langle n \rangle$ na seba. Permutáciu zapisujeme ako

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix} \tag{5.13}$$

alebo len

$$\pi = \begin{pmatrix} \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix} \tag{5.14}$$

Ak pre $i < j$ $i, j \in \{1, 2, \ldots, n\}$ je $\pi[i] > \pi[j]$, hovoríme, že dvojica (i, j) predstavuje inverziu v permutácii π.

Znamienko permutácie π je číslo

$$\mathrm{zn}\pi = (-1)^k,$$

kde k je počet inverzií v permutácii π. Ak má permutácia π párny počet inverzií, hovoríme, že π je párna permutácia. V opačnom prípade hovoríme, že π je nepárna permutácia.

Pretože π je vzájomne jednoznačné zobrazenie – bijekcia, existuje k nemu inverzné zobrazenie π^{-1}, ktoré je tiež permutáciou a ktoré nazveme inverznou permutáciou k permutácii π.

Veta 5.3. *Nech π je permutácia na množine $\{1, 2, \ldots, n\}$, π^{-1} k nej inverzná permutácia. Potom platí*

a) $\mathrm{zn}\pi = \mathrm{zn}\pi^{-1}$

b) Nech permutácia ϕ je definovaná nasledevne

$$\phi[k] = \begin{cases} \pi[k] & ak\ k \neq i, k \neq j \\ \pi[j] & ak\ k = i \\ \pi[i] & ak\ k = j \end{cases} \tag{5.15}$$

Potom $\mathrm{zn}\phi = -\mathrm{zn}\pi$.

Definícia 5.8. Nech $\mathbf{A} = \left(a_{ij}\right)$ je štvorcová matica rádu n nad komutatívnym telesom $(T, +, .)$. Determinant matice $\mathbf{A}$ je definovaný ako

$$\det\mathbf{A} = \sum_{\pi \in \Pi} \mathrm{zn}\pi . a_{\pi[1]} a_{\pi[2]} \ldots a_{\pi[n]}, \tag{5.16}$$

kde Π je množina všetkých permutácií mnjožiny $\{1, 2, \ldots, n\}$.

Veta 5.4. *Nech $\mathbf{A}$ je štvorcová matica $\mathbf{A}^T$ k nej transponovaná matica. Potom*

$$\det\mathbf{A} = \det\mathbf{A}^T \tag{5.17}$$

Veta 5.5. *Nech matica $\mathbf{B}$ vznikla zo štvorcovej matice $\mathbf{A}$ vzájomnou výmenou i-teho a j-teho riadku (alebo stĺpca). Potom*

$$\det\mathbf{B} = -\det\mathbf{A} \tag{5.18}$$

Veta 5.6. *Nech matica* $\mathbf{B}$ *vznikla zo štvorcovej matice* $\mathbf{A}$ *vynásobením jej* i*-teho riadku prvkom* $t \in T$*. Potom*

$$\det\mathbf{B} = t.\det\mathbf{A} \tag{5.19}$$

Veta 5.7. *Ak má štvorcová matica* $\mathbf{A}$ *dva stĺpce rovnaké, potom*

$$\det\mathbf{A} = 0. \tag{5.20}$$

Veta 5.8. *Ak má štvorcová matica* $\mathbf{A}$ *jeden riadok alebo jeden stĺpec nulový, potom*

$$\det\mathbf{A} = 0. \tag{5.21}$$

Veta 5.9. *Ak matica* $\mathbf{B}$ *vznikla zo štvorcovej matice* $\mathbf{A}$ *pripočítaním* t*-násobku* i*-teho riadku k ľubovoľnému inému riadku, alebo pripočítaním* t*-násobku* i*-teho stĺpca k ľubovoľnému inému stĺpcu, potom*

$$\det\mathbf{B} = \det\mathbf{A} \tag{5.22}$$

Veta 5.10. *Ak matica* $\mathbf{B}$ *vznikla zo štvorcovej matice* $\mathbf{A}$ *tak, že k riadku (resp. k stĺpcu)* i *bola pripočítaná lineáírna kombinácia iných riadkov (resp. stĺpcov), potom*

$$\det\mathbf{B} = \det\mathbf{A} \tag{5.23}$$

Veta 5.11. *Nech* $\mathbf{A}$ *je štvorcovná horná alebo dolná trojuholníková matica. Potom*

$$\det\mathbf{A} = a_{11}.a_{22}.\dots.a_{nn} \tag{5.24}$$

Definícia 5.9. Nech $\mathbf{A} = \left(a_{ij}\right)$ je štvorcová matica rádu n. Pre $i,\ j \in \{1, 2, \dots, n\}$ označme $\mathbf{A_{ij}}$ štvorcovú maticu, ktorá vznikne z matice $\mathbf{A}$ vynechaním i-teho riadku a j-teho stĺpca. Číslo

$$A_{ij} = \det\mathbf{A_{ij}} \tag{5.25}$$

nazveme algebraický doplnok prvku a_{ij}.

Veta 5.12. *Nech* $\mathbf{A} = \left(a_{ij}\right)$ *je štvorcová matica rádu* n*. Potom*

$$\sum_{k=1}^{n} a_{ik}A_{jk} = a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = \begin{cases} \det\mathbf{A} & ak\ i = j \\ 0 & ak\ i \neq j \end{cases} \tag{5.26}$$

$$\sum_{k=1}^{n} a_{ki}A_{kj} = a_{1i}A_{1j} + a_{2i}A_{2j} + \cdots + a_{ni}A_{nj} = \begin{cases} \det\mathbf{A} & ak\ i = j \\ 0 & ak\ i \neq j \end{cases} \tag{5.27}$$

Ľavej strane vzťahu (5.26) resp. (5.27) hovoríme Laplaceov rozvoj determinantu podľa i-teho riadku (resp. podľa j-teho stĺpca) matice $\mathbf{A}$

Veta 5.13. *Nech* $\mathbf{A} = \left(a_{ij}\right)$, $\mathbf{B} = \left(b_{ij}\right)$ *sú štvorcové matice rádu* n. *Potom*

$$\det(\mathbf{A}.\mathbf{B}) = \det\mathbf{A}.\det\mathbf{B} \tag{5.28}$$

5.2.1 Hodnosť matice

Definícia 5.10. Elementárne úpravy matice sú

a) vzájomná výmena dvoch riadkov (resp. stĺpcov)

b) vynásobenie riadku (resp. stĺpca) nenulovým číslom

c) pripočítanie riadku (resp. stĺpca) k inému riadku (resp stĺpcu)

Elementárne úpravy matice $\mathbf{A}$ možno interpretovať, ako vynásobenie tejto matice vhodnou štvorcovaou regulárnou maticou B.

$$\mathbf{A} = \begin{pmatrix} t & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} ta_{11} & ta_{12} & \dots & ta_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \tag{5.29}$$

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & \dots & 1 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+a_{j1} & a_{12}+a_{j2} & \dots & a_{1n}+a_{jn} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \tag{5.30}$$

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & \dots & 1 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} =$$

$$\begin{pmatrix} a_{21} & a_{22} & \dots & a_{2n} \\ a_{11} & a_{12} & \dots & a_{1n} \\ a_{31} & a_{32} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \tag{5.31}$$

Veta 5.14 (Gaussova eliminačná metóda)**.** *Každú maticu typu $m \times n$ možno pomocou elementárnych úprav previesť na práve jeden z nasledujúcich tvarov*

$$\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2m} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b_{mm} & \dots & b_{mn} \end{pmatrix} \tag{5.32}$$

$$\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2m} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & 0 & b_{nn} \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{5.33}$$

$$\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1k} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b_{kk} & 0 & b_{kn} \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{5.34}$$

Veta 5.15 (Jordanova eliminačná metóda)**.** *Každú maticu typu $m \times n$ možno pomocou elementárnych úprav previesť na práve jeden z nasledujúcich tvarov*

$$\begin{pmatrix} b_{11} & 0 & 0 & \dots & \dots & 0 & 0 & \dots & 0 \\ 0 & b_{22} & 0 & \dots & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & \dots & 0 & b_{mm} & 0 & \dots & 0 \end{pmatrix} \tag{5.35}$$

$$\begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & b_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b_{nn} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix} \tag{5.36}$$

$$\begin{pmatrix} b_{11} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & b_{22} & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & 0 & \dots & 0 \\ 0 & 0 & \dots & b_{kk} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix} \tag{5.37}$$

Definícia 5.11. Hodnosť $h(\mathbf{A})$ matice $\mathbf{A}$ rozumieme maximum z počtu lineárne nezávislých riadkov matice $\mathbf{A}$.

Definícia 5.12. Nech $\mathbf{A}$ je štvorcová matica rádu n. Nulita matice je číslo $n - h(\mathbf{A})$.

Veta 5.16. *Elementárne úpravy matice $\mathbf{A}$ nemenia jej hodnosť.*

Veta 5.17. *Pre každú maticu $\mathbf{A}$ platí*

$$h(\mathbf{A}) = h(\mathbf{A}^T). \tag{5.38}$$

Definícia 5.13. Nech $\mathbf{A}$ je štvorcová matica rádu n. Hovoríme, že matica $\mathbf{A}$ je regulárna, ak $h(\mathbf{A}) = n$. Ak $h(\mathbf{A}) < n$ hovoríme, že matica $\mathbf{A}$ je singulárna.

Veta 5.18. *Nech $\mathbf{A}$ je štvorcová matica rádu n.*
Matica $\mathbf{A}$ je regulárna práve vtedy, keď

$$\det\mathbf{A} \neq 0. \tag{5.39}$$

Matica $\mathbf{A}$ je singuylárna, práve keď

$$\det\mathbf{A} = 0. \tag{5.40}$$

Definícia 5.14. Ak matica $\mathbf{B}$ vznikne z matice $\mathbf{A}$ konečným počtom elementárnych úprav, hovoríme, že matica $\mathbf{A}$ je ekvivalentná s maticou $\mathbf{B}$ a píšeme $\mathbf{A} \sim \mathbf{B}$.

Relácia $\sim$ je reflexívna ($\mathbf{A} \sim \mathbf{A}$), symetrická ($\mathbf{A} \sim \mathbf{B} \Leftrightarrow \mathbf{B} \sim \mathbf{A}$) a tranzitívna ($\mathbf{A} \sim \mathbf{B}$, $\mathbf{B} \sim \mathbf{C} \Rightarrow \mathbf{A} \sim \mathbf{C}$) – je to relácia ekvivalencie.

Veta 5.19. *Každú regulárnu maticu možno previesť na diagonálnu maticu Jordanovou eliminačnom metódou použitím iba riadkových elementárnych úprav (resp. použitím iba stĺpcových elementárnych úprav).*

Veta 5.20. *Nech $\mathbf{A}_{m\times n}$ je matica typu $m\times n$, $\mathbf{B}_{m\times m}$ regulárna štvorcová matica rádu m, $\mathbf{C}_{n\times n}$ regulárna štvorcová matica rádu n. Potom*

$$h(\mathbf{B}_{m\times m}.\mathbf{A}_{m\times n}) = h(\mathbf{A}_{m\times n}), \qquad h(\mathbf{A}_{m\times n}.\mathbf{C}_{n\times n}) = h(\mathbf{A}_{m\times n}). \tag{5.41}$$

Definícia 5.15. Nech $\mathbf{A}$ je štvorcová matica rádu n. Nech existuje štvorcová matica $\mathbf{B}$ rádu n taká, že

$$\mathbf{A}.\mathbf{B} = \mathbf{B}.\mathbf{A} = \mathbf{E_n}, \tag{5.42}$$

kde $\mathbf{E_n}$ je jednotková matica rádu n. Potom hovoríme, že $\mathbf{B}$ je inverzná matica matice $\mathbf{A}$ a značíme ju $\mathbf{A^{-1}}$.

Veta 5.21. *Štvorcová matica $\mathbf{A}$ má inverznú maticu práve vtedy, keď $\det\mathbf{A} \neq 0$ a v tomto prípade je*

$$\det\mathbf{A^{-1}} = \frac{1}{\det\mathbf{A}}. \tag{5.43}$$

Dôkaz. Nech existuje inverzná matica $\mathbf{A^{-1}}$. Platí $\mathbf{E} = \mathbf{A}.\mathbf{A^{-1}}$. Preto

$$1 = \det\mathbf{E} = \det\mathbf{A}\det\mathbf{A^{-1}} \tag{5.44}$$

Z posledného vzťahu vyplýva, že $\det\mathbf{A} \neq 0$ aj $\det\mathbf{A^{-1}} \neq 0$, a tiež vzťah (5.43).

Veta 5.22. *Pre regulárnu maticu $\mathbf{A}$ rádu n platí*

$$\mathbf{A^{-1}} = \begin{pmatrix} \frac{A_{11}}{\det\mathbf{A}} & \frac{A_{21}}{\det\mathbf{A}} & \dots & \frac{A_{n1}}{\det\mathbf{A}} \\ \frac{A_{12}}{\det\mathbf{A}} & \frac{A_{22}}{\det\mathbf{A}} & \dots & \frac{A_{n2}}{\det\mathbf{A}} \\ \dots & \dots & \dots & \dots \\ \frac{A_{1n}}{\det\mathbf{A}} & \frac{A_{2n}}{\det\mathbf{A}} & \dots & \frac{A_{nn}}{\det\mathbf{A}} \end{pmatrix} = \frac{1}{\det\mathbf{A}} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} \tag{5.45}$$

Praktický výpočet inverznej matice k štvorcovej matici $\mathbf{A}$ rádu n začneme z blokovej matice $\left(\mathbf{A}|\mathbf{E_n}\right)$. Túto postupne upravujeme Jordanovou elimináciou – riadkovými elementárnymi úpravami na tvar $\left(\mathbf{E_n}|\mathbf{B}\right)$. Tvrdíme, že

$$\mathbf{B} = \mathbf{A^{-1}}. \tag{5.46}$$

Dôkaz Jednotlivé elementárne úpravy možno zapísať, ako postupné násobenie matice $\left(\mathbf{A}|\mathbf{E_n}\right)$ štvorcovými maticami $\mathbf{B_1}, \mathbf{B_2}, \ldots \mathbf{B_k}$, tj

$$\begin{aligned}\left(\mathbf{A}|\mathbf{E_n}\right) \sim \mathbf{B_1}\left(\mathbf{A}|\mathbf{E_n}\right) \sim \mathbf{B_2}\mathbf{B_1}\left(\mathbf{A}|\mathbf{E_n}\right) \sim \cdots \sim \\ \sim \mathbf{B_k}\mathbf{B_{k-1}}\ldots\mathbf{B_2}\mathbf{B_1}\left(\mathbf{A}|\mathbf{E_n}\right) = \\ = \left(\mathbf{B_k}\mathbf{B_{k-1}}\ldots\mathbf{B_2}\mathbf{B_1}\mathbf{A}|\mathbf{B_k}\mathbf{B_{k-1}}\ldots\mathbf{B_2}\mathbf{B_1}\mathbf{E_n}\right) = \left(\mathbf{BA}|\mathbf{BE_n}\right) = \left(\mathbf{E_n}|\mathbf{B}\right)\end{aligned} \tag{5.47}$$

Odtiaľ

$$\mathbf{BA} = \mathbf{E_n} \tag{5.48}$$

$$\mathbf{B} = \mathbf{A^{-1}}. \tag{5.49}$$

■

Kapitola 6

Systémy linárnych rovníc

Definícia 6.1. Nech $\mathbf{A} = \left(a_{ij}\right)_{m,n} = \left(a_{ij}\right)_{m\times n}$ je matica nad komutatívnym telesom T. Majme m rovníc s neznámymi $x_1, x_2, \ldots, x_n$:

$$\begin{array}{l} a_{11}x_1 \;+\; a_{12}x_2 \;+\ldots+\; a_{1n}x_n \;=\; b_1 \\ a_{21}x_1 \;+\; a_{22}x_2 \;+\ldots+\; a_{2n}x_n \;=\; b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{array} \tag{6.1}$$

Systém (6.16) nazývame systémom alebo sústavou m lineárnych rovníc o n neznámych $x_1, x_2, \ldots, x_n$. Riešením systému rovníc nazveme sa nazýva každá usporiadaná n-tica $(u_1, u_2, \ldots, u_n)$ prvkov z telesa T taká, že po dosadení u_i za x_i do systému (6.16) dostaneme m rovností resp. identít. Riešit systém rovníc (6.16) znamená nájsť všetky takéto n-tice.

Označme $\mathbf{A} = \left(a_{ij}\right)_{m\times n}$, $\mathbf{b} = (b_1, b_2, \ldots, b_m)^T$. Systém (6.16) môžeme v maticovom tvare zapísať nasledovne:

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_m \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \ldots \\ b_m \end{pmatrix}$$

a skrátene

$$\mathbf{A}.\mathbf{x} = \mathbf{b} \tag{6.2}$$

Hľadanie riešenia systému rovníc (6.2) znamená nájsť všetky vektory $\mathbf{u} \in T^n$, pre ktoré je $\mathbf{A}.\mathbf{u} = \mathbf{b}$.

Maticu **A** nazveme maticou systému (6.16). . Rozšírenou maticou systému linárnych rovníc je matica **B** definovaná

$$\mathbf{B} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix} = \big(\mathbf{A}|\mathbf{b}\big) \tag{6.3}$$

Systém (6.16) resp. (6.2) nazveme homgénny , ak $\mathbf{b} = o$. Inak je sysém rovníc (6.16) resp. (6.2) nehomogénny. Nutnou podmienkou na to je, aby mali matice **A**, **C** rovnaký počet stĺpcov.

Dva systémy rovníc $\mathbf{Ax} = \mathbf{b}$, $\mathbf{Cx} = \mathbf{d}$ sa nazývajú ekvivalentné, ak majú rovnaké množiny riešení.

Veta 6.1. *Majme systémy lineárnych rovníc* $\mathbf{Ax} = \mathbf{b}$, $\mathbf{Cx} = \mathbf{d}$, *nech matica* $\big(\mathbf{C}|\mathbf{d}\big)$ *vznikla z matice* $\big(\mathbf{A}|\mathbf{b}\big)$ *konečným počtom riadkových elementárnych úprav. Potom sú systémy rovníc* $\mathbf{Ax} = \mathbf{b}$, $\mathbf{Cx} = \mathbf{d}$ *ekvivalentné.*

Dôkaz. Vzájomná výmena dvoch rovníc, vynásobenie rovnice nenulovým prvkom a pripočítanie násobku jednej rovnice k inej rovnici nezmenia množinu riešení. ■

Veta 6.2 (Frobeniova veta)**.** *Systém lineárnych rovníc o* n *neznámych*

$$\mathbf{Ax} = \mathbf{b}$$

má riešeni práve vtedy, keď hodnosť matice systému sa rovná hodnosti rozšírenej matice systému a platí

- *Ak* $h(\mathbf{A}) = h(\mathbf{A}|\mathbf{b})$, *potom má systém práve jedno riešenie*
- *Ak* $h(\mathbf{A}) = h(\mathbf{A}|\mathbf{b})$, *potom má systém nekonečne veľa riešení, pričom* $n-k$ *neznámych je ľubovoľne voliteľných.*

Dôkaz. Dôkaz vychádza z prevodu rozšírenej matice systému lineárnych rovníc $(\mathbf{A}|\mathbf{b})$ na tvar $(\mathbf{C}|\mathbf{c})$

$$\mathbf{D}(\mathbf{C}|\mathbf{c}) = \left(\begin{array}{ccccccc|c} c_{11} & 0 & \dots & 0 & c_{1,k+1} & \dots & c_{1n} & c_{1,n+1} \\ 0 & c_{22} & 0\dots & 0 & c_{1,k+1} & \dots & c_{2n} & c_{2,n+1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0\dots & c_{kk} & c_{k,k+1} & \dots & c_{kn} & c_{k,n+1} \\ 0 & 0 & 0\dots & 0 & 0 & \dots & 0 & c_{k+1,n+1} \\ 0 & 0 & 0\dots & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0\dots & 0 & 0 & \dots & 0 & 0 \end{array}\right) \tag{6.4}$$

Najprv konštatujme, že $\mathbf{A} \sim \mathbf{C}$ a $(\mathbf{A}|\mathbf{b}) \sim (\mathbf{C}|\mathbf{c})$.

Z tvaru (6.7) matice $(\mathbf{C}|\mathbf{c})$ vidieť, že $c_{k+1,n+1} \neq 0$, nastane práve vtedy, keď $h(\mathbf{C}) < h((\mathbf{C}|\mathbf{c}))$ čo je práve vtedy, keď $h(\mathbf{A}) < h((\mathbf{A}|\mathbf{b}))$.

Ak $c_{k+1,n+1} \neq 0$, potom z rovnice prislúchajúcej riadku $k+1$ matice $\mathbf{D}$ vyplýva, že systém nemá riešenie.

Ak $c_{k+1,n+1} = 0$, potom $h(\mathbf{C}) = h((\mathbf{C}|\mathbf{c}))$ a teda aj $h(\mathbf{A}) = h((\mathbf{A}|\mathbf{b}))$.

Ak $c_{k+1,n+1} = 0$ a $k = n$, potom má matica $\mathbf{D}$ po vynechaní posledných nulových riadkov tvar

$$\mathbf{D} = (\mathbf{C}|\mathbf{c}) = \begin{pmatrix} c_{11} & 0 & \dots & 0 & | & c_{1,n+1} \\ 0 & c_{22} & 0\dots & 0 & | & c_{2,n+1} \\ \dots & \dots & \dots & \dots & | & \dots \\ 0 & 0 & 0\dots & c_{nn} & | & c_{n,n+1} \end{pmatrix} \tag{6.5}$$

odkiaľ máme

$$y_i = \frac{c_{i,n+1}}{c_{ii}}. \tag{6.6}$$

Ak nakoniec $c_{k+1,n+1} = 0$ a $k < n$, potom má matica $\mathbf{D}$ po vynechaní posledných nulových riadkov tvar

$$\mathbf{D} = (\mathbf{C}|\mathbf{c}) = \begin{pmatrix} c_{11} & 0 & \dots & 0 & c_{1,k+1} & \dots & c_{1n} & | & c_{1,n+1} \\ 0 & c_{22} & 0\dots & 0 & c_{1,k+1} & \dots & c_{2n} & | & c_{2,n+1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & | & \dots \\ 0 & 0 & 0\dots & c_{kk} & c_{k,k+1} & \dots & c_{kn} & | & c_{k,n+1} \end{pmatrix} \tag{6.7}$$

Z tvaru matice $\mathbf{D}$ vyplýva, že každé y_i pre $i = 1, 2, \dots, k$ môžeme vyjadriť pomocou premenných $y_{k+1}, y_{k+2}, \dots, y_n$ nasledovne

$$y_i = \frac{c_{i,n+1}}{c_{ii}} - \frac{c_{i,k+1}}{c_{ii}} y_{k+1} - \frac{c_{i,k+2}}{c_{ii}} y_{k+2} - \dots - \frac{c_{i,n}}{c_{ii}} y_n \tag{6.8}$$

Čísla $y_{k+1}, y_{k+2}, \dots, y_n$ môžeme zvoliť ľubovoľne a k nim potom jednoznačne dopočítame hodnoty premenných $y_1, y_2, \dots, y_k$ podľa posledne uvedných vzťahov (6.8).

6.0.2 Homogénny systém lineárnych rovníc

Veta 6.3. *Nech vektory $\mathbf{x_1}, \mathbf{x_2}, \dots, \mathbf{x_l}$ sú riešenia homogénneho systému m lineárnych rovníc o n neznámych*

$$\mathbf{Ax} = \mathbf{o}.$$

Potom aj každá lineárna kombinácia vektorov $\mathbf{x_1}, \mathbf{x_2}, \dots, \mathbf{x_l}$ je riešením tohoto systému rovníc.

Dôkaz. Stačí ukázať, že ak $\mathbf{Au} = \mathbf{o}$, $\mathbf{Av} = \mathbf{o}$, potom aj $\mathbf{A}(\alpha\mathbf{u}+\beta\mathbf{v}) = o$. Podľa prvidiel násobenia matíc platí

$$\mathbf{A}(\alpha\mathbf{u} + \beta\mathbf{v}) = \mathbf{A}(\alpha\mathbf{u}) + \mathbf{A}(\beta\mathbf{v}) = \alpha(\mathbf{Au}) + \alpha(\mathbf{Av}) = \alpha\mathbf{o} + \beta\mathbf{o} = \mathbf{o}.$$

■

Veta 6.4. *Homogénny systém lineárnych rovníc*

$$\mathbf{Ax} = \mathbf{o} \tag{6.9}$$

má vždy aspoň jedno riešenie, a to tzv. triviálne riešenie $\mathbf{x} = \mathbf{o} = (0, 0, \dots, 0)$. *Pritom platí:*

- *Ak* $h(\mathbf{A}) = n$, *potom má tento systém iba triviálne riešenie.*
- *Ak* $h(\mathbf{A}) = k < n$, *potom má tento systém nekonečne veľa riešení, ktoré tvoria* $n - k$ *dimenzionálny podpriestor* n*-dimenzionálneho aritmetického priestoru* $(T^n, +, .)$ *nad telesom* T.

Dôkaz. Ľahko sa overí, že $\mathbf{x} = \mathbf{o}$ je riešením systému (6.9). Rozšírenú maticu $(\mathbf{A}|\mathbf{o})$ systému (6.9) možno previesť Jordanovou eliminačnou metódou a následným vynechaním nulových riadkov na tvar

$$\mathbf{D} = (\mathbf{C}|\mathbf{c}) = \begin{pmatrix} c_{11} & 0 & \dots & 0 & c_{1,k+1} & \dots & c_{1n} & | & 0 \\ 0 & c_{22} & 0\dots & 0 & c_{1,k+1} & \dots & c_{2n} & | & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & | & 0 \\ 0 & 0 & 0\dots & c_{kk} & c_{k,k+1} & \dots & c_{kn} & | & 0 \end{pmatrix} \tag{6.10}$$

Ak je $h(\mathbf{A}) = n$, potom $k = m$ a matica (6.10) má tvar

$$\mathbf{D} = (\mathbf{C}|\mathbf{c}) = \begin{pmatrix} c_{11} & 0 & \dots & 0 & | & 0 \\ 0 & c_{22} & 0\dots & 0 & | & 0 \\ \dots & \dots & \dots & \dots & | & 0 \\ 0 & 0 & 0\dots & c_{nn} & | & 0 \end{pmatrix} \tag{6.11}$$

odkiaľ vyplýva, že jediným riešením systému (6.9) je $\mathbf{x} = \mathbf{o}$.

Ak $k < n$, potom má matica $\mathbf{D}$ tvar

$$\mathbf{D} = (\mathbf{C}|\mathbf{o}) = \begin{pmatrix} c_{11} & 0 & \dots & 0 & c_{1,k+1} & \dots & c_{1n} & | & 0 \\ 0 & c_{22} & 0\dots & 0 & c_{1,k+1} & \dots & c_{2n} & | & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & | & 0 \\ 0 & 0 & 0\dots & c_{kk} & c_{k,k+1} & \dots & c_{kn} & | & 0 \end{pmatrix} \tag{6.12}$$

Z tvaru matice $\mathbf{D}$ vyplýva, že každé y_i pre $i = 1, 2, \ldots, k$ môžeme vyjadriť pomocou premenných $y_{k+1}, y_{k+2}, \ldots, y_n$ nasledovne

$$y_i = -\frac{c_{i,k+1}}{c_{ii}} y_{k+1} - \frac{c_{i,k+2}}{c_{ii}} y_{k+2} - \cdots - \frac{c_{i,n}}{c_{ii}} y_n \tag{6.13}$$

Čísla $y_{k+1}, y_{k+2}, \ldots, y_n$ môžeme zvoliť ľubovoľne a k nim potom jednoznačne dopočítame hodnoty premenných $y_1, y_2, \ldots, y_k$ podľa vzťahov (6.13).

Veta 6.5. *Nech $\mathbf{x_b}$ je jedno pevné konrétne riešenie nehomogéneho systému*

$$\mathbf{Ax} = \mathbf{b}. \tag{6.14}$$

Potom ľubovoľné riešenie tohoto nehomogénneho sytému sytému možno napísať ako

$$\mathbf{x} = \mathbf{x_b} + \mathbf{x_o}, \tag{6.15}$$

kde $\mathbf{x_o}$ je riešenie homogénneho systému $\mathbf{Ax} = \mathbf{o}$.

Dôkaz. Majme jedno pevne zvolené riešenie $\mathbf{x_b}$ systému (6.14). Nech $\mathbf{u}$ je ľubovoľné riešenie systému (6.14). Pretože $\mathbf{Au} = \mathbf{Ax_b} = \mathbf{b}$, je

$$\mathbf{o} = \mathbf{Au} - \mathbf{Ax_b} = \mathbf{A}(\mathbf{u} - \mathbf{x_b}),$$

čo znamená, že $\mathbf{u} - \mathbf{x_b}$ je riešením homogénneho systému $\mathbf{Ax} = \mathbf{o}$. Vyjadrenie $\mathbf{u} = \mathbf{x_b} + (\mathbf{u} - \mathbf{x_b})$ je už vyjadrenie riešenia $\mathbf{u}$ systému (6.14) v požadovanom tvare.

Každý vektor v tvare $\mathbf{u} = \mathbf{x_b} + \mathbf{x_o}$ je riešením nehomogénneho systému (6.14), pretože $\mathbf{Au} = \mathbf{A}.(\mathbf{x_b} + \mathbf{x_o}) = \mathbf{Ax_b} + \mathbf{Ax_o} = \mathbf{b} + \mathbf{o} = \mathbf{o}$. ■

6.0.3 Cramerovo pravidlo

Majme n rovníc o n neznámych

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n \end{array} . \tag{6.16}$$

Jeho skrátený zápis je

$$\mathbf{Ax} = \mathbf{b}, \tag{6.17}$$

kde $\mathbf{A}$ je štvorcová matica typu $n \times n$. Budeme študovať špeciálny prípad, keď je matica $\mathbf{A}$ regulárna.

Veta 6.6. *Majme nehomogénny systém n lineárnych rovníc o n neznámych v tvare* (6.0.3) *s regulárnou maticou* $\mathbf{A}$. *Potom jediné riešenie tohoto systému je*

$$\mathbf{x} = \mathbf{A^{-1}}\mathbf{x} \qquad \text{resp. } x_i = \frac{\det \mathbf{B_i}}{\det \mathbf{A}}, \tag{6.18}$$

kde $\mathbf{B_i}$ *je matica, ktorá vznikne z matice* $\mathbf{A}$ *nahradením jej i-teho stĺpca stĺpcovým vektorom* $\mathbf{b}$.

Dôkaz.

$$\mathbf{x} = \mathbf{E_n}\mathbf{x} = (\mathbf{A^{-1}}\mathbf{A})\mathbf{x} = \mathbf{A^{-1}}(\mathbf{A}\mathbf{x}) = \mathbf{A^{-1}}\mathbf{b}. \tag{6.19}$$

Po dosadení za $\mathbf{A^{-1}}$ zo vzťahu (5.22) na str. 51 dostávame

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \mathbf{A^{-1}}\mathbf{b} = \frac{1}{\det \mathbf{A}} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}. \tag{6.20}$$

Z posledného vzťahu vyplýva pre každé x_i, $i = 1, 2, \dots, n$

$$x_i = \frac{1}{\det \mathbf{A}}(b_1 A_{1i} + b_2 A_{2i} + \dots + b_n A_{ni}). \tag{6.21}$$

Výraz na pravej strane posledného vzťahu predstavuje Laplaceov rozvoj podľa i-teho stĺpca matice $\mathbf{B_i}$, ktorá vznikla nahradením nahradením i-teho stĺpca matice $\mathbf{A}$ stĺpcovým vektorom $\mathbf{b}$.

6.1 Vlastné hodnoty a vlastné vektory matice

Majme štvorcovú maticu $\mathbf{A}$ rádu n. Zobrazenie

$$\mathbf{y} = \mathbf{A}\mathbf{x} \tag{6.22}$$

je tzv. lineárne zobrazenie z T^n do T^n, t.j. platí

$$\mathbf{A}(\mathbf{x} + \mathbf{y}) = \mathbf{A}\mathbf{x} + \mathbf{A}\mathbf{y} \qquad \text{a} \qquad \mathbf{A}(t\mathbf{x}) = t\mathbf{A}\mathbf{x}. \tag{6.23}$$

Pri riešení mnohých matematických problémov vzniká otázka, kedy takto definované lineárne zobrazenie vektor $\mathbf{x}$ len „natiahne“ t.j. kedy

$$\mathbf{A}\mathbf{x} = \lambda\mathbf{x} = \lambda\mathbf{E_n}\mathbf{x}. \tag{6.24}$$

Vzťah (6.24) nastane práve vtedy, keď

$$(\mathbf{A} - \lambda\mathbf{E})\mathbf{x} = \mathbf{o}. \tag{6.25}$$

Z teórie linárnych rovníc vieme, že rovnica (6.25) má vždy jedno z riešení $\mathbf{x} = \mathbf{o}$. Nenulové riešenie má však len vtedy, keď je matica $(\mathbf{A} - \lambda\mathbf{E})$ singulárna, čo nastane práve vtedy, keď

$$\det(\mathbf{A} - \lambda\mathbf{E}) = 0. \tag{6.26}$$

Definícia 6.2. Nech $\mathbf{A}$ je štvorcová matica rádu n, ktorej prvky sú reálne čísla. Determinant

$$\det(\mathbf{A} - \lambda\mathbf{E}) \tag{6.27}$$

nazývame charakteristickým polynómom matice $\mathbf{A}$.
Rovnicu

$$\det(\mathbf{A} - \lambda\mathbf{E}) = b_0\lambda^n + b_1\lambda^{n-1} + \cdots + b_{n-1}\lambda + b_0 = 0 \tag{6.28}$$

nazývame charakteristickou rovnicou matice $\mathbf{A}$.
Korene charakteristickej rovnice (6.28) matice $\mathbf{A}$ nazveme chrakteristické hodnoty resp. charakteristické čísla matice $\mathbf{A}$.
Nech λ je vlastná hodnota matice $\mathbf{A}$. Stĺpcový vektor $\mathbf{x} \neq \mathbf{o}$, pre ktorý platí $\mathbf{Ax} = \lambda\mathbf{x}$ nazveme vlastným vektorom resp. charakteristickým vektorom prislúchajúcim vlastnej hodnote λ.

Veta 6.7. *Nech λ je vlastná hodnota matice $\mathbf{A}$. Všetky vlastné vektory prislúchajúce tej istej vlastnej hodnote λ spolu s nulovým vektorom $\mathbf{o}$ tvoria lineárny podpriestor s dimenziou $n - h(\mathbf{A} - \lambda\mathbf{E})$, kde $h(\mathbf{A} - \lambda\mathbf{E})$ je hodnosť matice $(\mathbf{A} - \lambda\mathbf{E})$.*

Veta 6.8. *Vlastné vektory $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}$ prislúchajúce rôznym vlastným hodnotám $\lambda_1, \lambda_2, \ldots, \lambda_k$ sú lineárne nezávislé.*

Dôkaz. Matematickou indukciou podľa k.
Majme vektory $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}$ prislúchajúce rôznym vlastným hodnotám $\lambda_1, \lambda_2, \ldots, \lambda_k$.

Nech

$$a_1\mathbf{x_1} + a_2\mathbf{x_2} + \cdots + a_k\mathbf{x_k} = \mathbf{o}. \tag{6.29}$$

Platí

$$\begin{aligned} \mathbf{o} = \mathbf{Ao} = \mathbf{A}(a_1\mathbf{x_1} + a_2\mathbf{x_2} + \cdots + a_k\mathbf{x_k}) &= \\ = a_1(\mathbf{Ax_1}) + a_2(\mathbf{Ax_2}) + \cdots + a_k(\mathbf{Ax_k}) &= \\ = a_1\lambda_1\mathbf{x_1} + a_2\lambda_2\mathbf{x_2} + \cdots + a_k\lambda_k\mathbf{x_k} & \end{aligned} \tag{6.30}$$

Vynásobme rovnicu (6.29) číslom λ_k a odčítajme od rovnice (6.30). Dostaneme

$$a_1(\lambda_1 - \lambda_k)\mathbf{x_1} + a_2(\lambda_2 - \lambda_k)\mathbf{x_2} + \cdots + a_{k-1}(\lambda_{k-1} - \lambda k)\mathbf{x_{k-1}} + a_k(\lambda_k - \lambda k)\mathbf{x_k} =$$
$$a_1(\lambda_1 - \lambda_k)\mathbf{x_1} + a_2(\lambda_2 - \lambda_k)\mathbf{x_2} + \cdots + a_{k-1}(\lambda_{k-1} - \lambda k)\mathbf{x_{k-1}} = \mathbf{o}. \quad (6.31)$$

Podľa indukčného predpokladu sú vektory $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_{k-1}}$ lineárne nezávislé, a preto $a_i(\lambda_i - \lambda_k) = 0$ pre $i = 1, 2, \ldots, k-1$, z čoho (keďže $\lambda_i \neq \lambda_k$) vyplýva $a_i = 0$ pre $i = 1, 2, \ldots, k-1$. Z posledného faktu a z (6.29) vyplýva $a_k\mathbf{x}_k = \mathbf{o}$, a teda aj $a_k = 0$. ■

Register

Literatúra

[1] Viliam Chvál, Milan Mikola: *Lineárna algebra*, Katolícka univerzita, Ružomberok, (2000), ISBN 80-89039-00-6

Za odbornú náplň tohto vydania zodpovedá vedúci katedry matematických metód Fakulty riadenia a informatiky ŽU doc. RNDr. Stanislav Palúch, CSc.

Autori:	Doc. RNDr. Stanislav Palúch, CSc.
	RNDr. Ida Stankovianska, CSc.
Názov:	**ALGEBRA**
Vydala:	Žilinská univerzita v EDIS-vydavateľstve ŽU
	v auguste 2007 ako svoju XXX. publikáciu
Zodpovedný redaktor:	PhDr. Albert Jurčišin
Technický redaktor:	doc. RNDR. Stanislav Palúch, CSc.
Určené:	pre študentov Fakulty riadenia a informatiky
Vedúci katedry:	doc. RNDr. Stanislav Palúch, CSc.
Povolené:	rektorom ŽU v Žiline výmerom XX/2001
Vydanie:	prvé
Náklad:	XXX výtlačkov
AH/VH:	XX/XX
Druh tlače:	ofset
Typografický systém:	LaTeX pod o. s. Linux
ISBN 80-XXXX-XX-X	

Rukopis neprešiel v ES redakčnou ani jazykovou úpravou.