

Kapitola 2

Množiny a zobrazenia

2.1 Dôkazy

2.1.1 Základné typy dôkazov

Tvrdenie 2.1.1. *Nech n je celé číslo. Potom zvyšok čísla n^2 po delení 4 je 0 alebo 1. Pritom ak n je párne, tak n^2 je deliteľné 4 a ak n je nepárne tak n^2 má zvyšok 1.*

Tvrdenie 2.1.2. *Ak pre celé čísla a, b, c platí rovnosť $a^2 + b^2 = c^2$, tak aspoň jedno z čísel a, b je párne.*

Tvrdenie 2.1.3. *Nech n je prirodzené číslo. Ak n^2 je deliteľné štyrmi, tak n je párne.*

2.1.2 Matematická indukcia

2.1.3 Drobné rady ako dokazovať

2.1.4 Výroky, logické spojky, tautológie

Definícia 2.1.4. *Negáciou výroku P rozumieme výrok „neplatí P “. Označujeme ju $\neg P$.*

Pre dva výroky P a Q nazývame ich konjunkciou výrok „ P a Q “, označujeme $P \wedge Q$.

Disjunkcia je výrok „ P alebo Q “, označujeme $P \vee Q$.

Pod implikáciou rozumieme výrok „ak platí P , tak platí Q “, označujeme $P \Rightarrow Q$.

Ekvivalencia výrokov P a Q je výrok „ P platí práve vtedy, keď platí Q “, označujeme $P \Leftrightarrow Q$.

2.1.5 Negácia výrokov s kvantifikátormi

2.2 Množiny a zobrazenia

2.2.1 Množiny

Definícia 2.2.1. *Vzťah byť prvok množiny zapisujeme ako $x \in A$, čítame „ x patrí A “.*

Hovoríme, že množiny A a B sa rovnajú (označujeme $A = B$), ak platí

$$(x \in A) \quad \Leftrightarrow \quad (x \in B)$$

pre ľubovoľný prvok x .

Množiny, ktorá nemá nijaké prvky nazývame prázdna množina a označujeme \emptyset .

Definícia 2.2.2. Hovoríme, že A je *podmnožinou* B , ak každý prvok množiny A patrí aj do B , označujeme $A \subseteq B$. Inak povedané, $A \subseteq B$ ak pre každé x platí

$$(x \in A) \quad \Rightarrow \quad (x \in B).$$

Vzťah množín A a B , pre ktoré platí $A \subseteq B$ sa tiež zvykne nazývať *inklúzia*.

Definícia 2.2.3. *Zjednotenie* dvoch množín A a B je množina

$$A \cup B = \{x; x \in A, x \in B\}.$$

Prienik dvoch množín A a B je množina

$$A \cap B = \{x \in A; x \in B\}.$$

Rozdiel dvoch množín A a B je množina

$$A \setminus B = \{x \in A; x \notin B\}$$

Definícia 2.2.4. Ak A, B sú množiny, tak ich *karteziánsky súčin* je množina všetkých usporiadaných dvojíc (a, b) takých, že $a \in A$ a $b \in B$. Označujeme ho

$$A \times B = \{(a, b); a \in A, b \in B\}.$$

2.2.2 Zobrazenia

Definícia 2.2.5. *Zobrazenie* $f: X \rightarrow Y$ z množiny X do množiny Y je podmnožina f množiny $X \times Y$ taká, že ku každému $x \in X$ existuje práve jedno $y \in Y$ s vlastnosťou $(x, y) \in f$.

Množinu X budeme tiež nazývať *definičný obor* zobrazenia f a množina Y je *obor hodnôt* zobrazenia f .

Namiesto zápisu $(x, y) \in f$ budeme používať zápis $y = f(x)$.

Definícia 2.2.6. Hovoríme, že dve zobrazenia $f: X \rightarrow Y$ a $g: Z \rightarrow W$ sa *rovnajú*, ak $X = Z$, $Y = W$ a $f(x) = g(x)$ pre každé $x \in X$. (Inými slovami, ak sa rovnajú ich definičné obory, obory hodnôt a obe zobrazenia nadobúdajú v každom bode rovnakú hodnotu.) Rovnosť zobrazení označujeme $f = g$.

Definícia 2.2.7 (Skladanie zobrazení). Ak $f: X \rightarrow Y$, $g: Y \rightarrow Z$ sú zobrazenia, tak *zložením zobrazení* f a g nazývame zobrazenie $g \circ f: X \rightarrow Z$ také, že pre každé $x \in X$ platí

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

Tvrdenie 2.2.8 (Asociatívnosť skladania zobrazení). *Nech* $f: X \rightarrow Y$, $g: Y \rightarrow Z$, $h: Z \rightarrow W$ *sú zobrazenia, potom*

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

Definícia 2.2.9. Nech $f: X \rightarrow Y$ je zobrazenie. Hovoríme, že f je *injektívne (prsté) zobrazenie* (alebo tiež injekcia), ak pre všetky $x, y \in X$ také, že $x \neq y$ platí $f(x) \neq f(y)$.

Hovoríme, že f je *surjektia* (*surjektívne zobrazenie, zobrazenie na*), ak pre každé $y \in Y$ existuje také, $x \in X$, že $f(x) = y$.

Hovoríme, že f je *bijekcia* (*bijekatívne zobrazenie*), ak f je súčasne injekcia aj surjektia.

Tvrdenie 2.2.10. *Zloženie dvoch injekcií je injekcia, zloženie dvoch surjekcií je surjektia, zloženie dvoch bijekcií je bijekcia.*

Definícia 2.2.11. Zobrazenie $id_X: X \rightarrow X$ také, že $id_X(x) = x$ pre každé $x \in X$ sa nazýva *identické zobrazenie (identita)*.

Definícia 2.2.12. Nech $f: X \rightarrow Y$ a $g: Y \rightarrow X$ sú zobrazenia. Ak platí

$$\begin{aligned} g \circ f &= id_X \\ f \circ g &= id_Y \end{aligned}$$

tak hovoríme, že zobrazenie g je *inverzné zobrazenie k f* . Inverzné zobrazenie k zobrazeniu f označujeme f^{-1} .

Tvrdenie 2.2.13. *Inverzné zobrazenie k f existuje práve vtedy, keď f je bijekcia.*

Tvrdenie 2.2.14. *Nech $f: X \rightarrow Y$ a $g: Y \rightarrow Z$ sú bijekcie. Potom*

$$\begin{aligned} (f^{-1})^{-1} &= f \\ (g \circ f)^{-1} &= f^{-1} \circ g^{-1} \end{aligned}$$

Dôsledok 2.2.15. *Ak f je bijekcia, tak aj f^{-1} je bijekcia.*

2.2.3 Vzor a obraz množiny*

Definícia 2.2.16. Nech $f: X \rightarrow Y$ je zobrazenie, $A \subseteq X$, $B \subseteq Y$. Množinu

$$f[A] = \{f(a); a \in A\}$$

nazývame *obrazom* množiny A v zobrazení f . Množinu

$$f^{-1}(B) = \{x \in X; f(x) \in B\}$$

nazývame *vzorom* množiny B v zobrazení f .

2.3 Permutácie

Definícia 2.3.1. Ak M je konečná množina, tak bijekciu $\varphi: M \rightarrow M$ budeme nazývať *permutáciou* množiny M .

2.3.1 Rozklad na súčin disjunktných cyklov*

Definícia 2.3.2. Permutáciu φ konečnej množiny M nazveme *cyklus*, ak existujú prvky a_1, a_2, \dots, a_k také, že

$$\begin{cases} \varphi(a_i) = a_{i+1} \text{ pre } i = 1, 2, \dots, k-1, \\ \varphi(a_k) = a_1, \\ \varphi(a) = a \text{ pre ostatné prvky } a \neq a_i. \end{cases}$$

Pre cyklus tohoto tvaru budeme používať zápis $(a_1 a_2 \dots a_k)$.

V definícii cyklu pripúšťame aj nulový počet prvkov. *Prázdny cyklus*, ktorý označujeme $()$, sa rovná identickej permutácii.

Definícia 2.3.3. Dve permutácie φ a τ tej istej množiny M nazveme *disjunktné*, ak pre každý prvok $a \in M$ platí $\varphi(a) = a$ alebo $\tau(a) = a$. (Teda každý prvok zostáva nezmenený pri aspoň jednej z týchto dvoch permutácií.)

Lema 2.3.4. Ak φ a τ sú disjunktné permutácie, tak

$$\varphi \circ \tau = \tau \circ \varphi.$$

Tvrdenie 2.3.5. Každú permutáciu možno zapísať ako zloženie disjunktných cyklov. Tento zápis je jednoznačný až na poradie cyklov (a vynechanie prázdneho cyklu). Nazývame ho rozklad permutácie na súčin disjunktných cyklov.

Definícia 2.3.6. Ak φ je permutácia konečnej množiny M , tak *řád permutácie* φ je najmenšie prirodzené číslo $n \geq 1$ také, že

$$\varphi^n = id_M.$$

Lema 2.3.7. Rád cyklu je rovný jeho dĺžke, t.j. ak $\varphi = (a_1 \dots a_n)$, tak rád φ je rovný n .

Veta 2.3.8. Rád permutácie je najmenší spoločný násobok dĺžok disjunktných cyklov, ktoré vystupujú v jej rozklade.

Kapitola 3

Grupy a polia

3.1 Binárne operácie

Definícia 3.1.1. Binárna operácia $*$ na množine A je zobrazenie z množiny $A \times A$ do A .

Namiesto $*(a, b)$ budeme používať označenie $a * b$, tento zápis budeme niekedy skracovať ako ab .

Definícia 3.1.2. Nech $*$ je binárna operácia na množine M . Hovoríme, že $e \in M$ je *neutrálny prvok* operácie $*$, ak pre všetky $m \in M$ platí

$$e * m = m * e = m.$$

Tvrdenie 3.1.3. Ak má binárna operácia $*$ na množine M neutrálny prvok, tak tento neutrálny prvok je jediný.

Definícia 3.1.4. Binárna operácia $*$ na množine M je *komutatívna*, ak pre všetky $x, y \in M$ platí

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

Definícia 3.1.5. Binárna operácia $*$ na množine M je *asociatívna*, ak pre všetky $x, y, z \in M$ platí

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

Definícia 3.1.6. Nech $*$ je binárna operácia na množine M . Nech $a \in M$ a nech e je neutrálny prvok operácie $*$. Prvok $b \in M$ je *inverzný* k prvku a , ak platí

$$a * b = b * a = e.$$

Tvrdenie 3.1.7. Nech $*$ je asociatívna operácia na množine M a $*$ má neutrálny prvok e . Ak existuje inverzný prvok k a , tak je jednoznačne určený.

3.1.1 Zovšeobecnený asociatívny zákon*

Tvrdenie 3.1.8 (Zovšeobecnený asociatívny zákon). Nech \cdot je asociatívna binárna operácia na množine A . Potom súčin $a_1 * a_2 * \dots * a_n$ nezávisí od spôsobu uzátvorkovania.

3.2 Grupy

Definícia 3.2.1. Dvojica $(G, *)$, kde G je množina a $*$ je binárna operácia na G , sa nazýva *grupa*, ak

- (i) operácia $*$ je asociatívna,
- (ii) operácia $*$ má neutrálny prvok, (neutrálny prvok budeme spravidla označovať e)
- (iii) ku každému prvku $g \in G$ existuje inverzný prvok vzhľadom na operáciu $*$. (Tento inverzný prvok budeme označovať g^{-1} .)

Definícia 3.2.2. Grupa $(G, *)$ sa nazýva *komutatívna*, ak operácia $*$ na G je komutatívna. (Tiež sa používa termín *abelovská grupa*.)

Veta 3.2.3 (Zákony o krátení). Ak $(G, *)$ je grupa, tak pre ľubovoľné $a, b, c \in G$ platí

$$\begin{aligned} a * b = a * c &\Rightarrow b = c \\ b * a = c * a &\Rightarrow b = c \end{aligned}$$

Veta 3.2.4. Nech $(G, *)$ je grupa. Potom pre ľubovoľné $a, b \in G$ platí

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

3.3 Polia

Definícia 3.3.1. Nech F je množina, $+$ a \cdot sú binárne operácie na F . Hovoríme, že trojica $(F, +, \cdot)$ je *pole*, ak

- (i) $(F, +)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 0 ;
- (ii) $(F \setminus \{0\}, \cdot)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 1 ;
- (iii) pre ľubovoľné $a, b, c \in F$ platí

$$\begin{aligned} a(b + c) &= ab + ac, \\ (a + b)c &= ac + bc. \end{aligned}$$

(Túto vlastnosť nazývame *distributívnosť*.)

Pre inverzný prvok v grupe $(F, +)$ budeme používať označenie $-a$, t.j. pre túto grupu používame aditívny zápis. Prvok $-a$ nazývame *opačný prvok* k prvku a .

Pre grupu $(F \setminus \{0\}, \cdot)$ budeme používať multiplikatívny zápis, teda inverzný prvok k prvku $a \neq 0$ poľa F vzhľadom na operáciu \cdot budeme značiť a^{-1} . Ak použijeme termín *inverzný prvok* v súvislosti s poľom a nešpecifikujeme binárnu operáciu, myslí sa tým práve prvok a^{-1} .

Namiesto $b + (-c)$ budeme používať stručnejší zápis $b - c$.

Definícia 3.3.2. Pole je množina F , na ktorej sú definované 2 binárne operácie $+$ a \cdot spĺňajúce:

- (i) pre všetky $a, b, c \in F$ platí $a + (b + c) = (a + b) + c$,
- (ii) pre všetky $a, b \in F$ platí $a + b = b + a$,

- (iii) existuje prvok $0 \in F$ taký, že pre každé $a \in F$ sa $a + 0 = a$,
- (iv) ku každému $a \in F$ existuje $b \in F$ tak, že $a + b = 0$,
- (v) pre všetky $a, b, c \in F$ platí $a.(b.c) = (a.b).c$,
- (vi) pre všetky $a, b \in F$ platí $a.b = b.a$,
- (vii) existuje prvok $1 \in F$ taký, že pre každé $a \in F$ sa $a.1 = a$,
- (viii) ku každému $a \in F$, $a \neq 0$ existuje $b \in F$ tak, že $a.b = 1$,
- (ix) pre všetky $a, b, c \in F$ sa $a.(b + c) = a.b + a.c$.

Tvrdenie 3.3.3. *Nech $(F, +, \cdot)$ je pole. Potom pre $a, b, c \in F$ platí*

- (i) $a.0 = 0$, $0.a = 0$,
- (ii) $a.b = b.a$,
- (iii) $(-a).b = -a.b$,
- (iv) $(-a).(-b) = a.b$,
- (v) $a.b = 0 \Rightarrow a = 0 \vee b = 0$,
- (vi) $a.b = a.c \wedge a \neq 0 \Rightarrow b = c$,
- (vii) $a.a = a \Rightarrow a = 0 \vee a = 1$.

Definícia 3.3.4. Nech $n \in \mathbb{N}$, $n \geq 2$. Množinu \mathbb{Z}_n definujeme ako $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$. (Teda množina \mathbb{Z}_n obsahuje všetky možné zvyšky po delení číslom n .)

Na množine \mathbb{Z}_n zavedieme operácie \oplus a \odot predpisom

$$\begin{aligned} a \oplus b &= (a + b) \pmod{n}, \\ a \odot b &= (ab) \pmod{n}, \end{aligned}$$

kde operácia \pmod{n} označuje zvyšok po delení číslom n (pozri dodatok ??).

Definícia 3.3.5. Číslo $n \in \mathbb{N}$, $n > 1$, nazývame *zloženým číslom*, ak $n = m.k$ pre nejaké $m, k \in \mathbb{N}$ také, že $1 < m, k < n$.

Ak $n \in \mathbb{N}$, $n > 1$, nie je zložené, tak ho nazývame *prvočíslo*.

Číslo 1 nepovažujeme ani za prvočíslo ani za zložené číslo.

Veta 3.3.6. *Ak p je prvočíslo, tak $(\mathbb{Z}_p, \oplus, \odot)$ je pole.*

Definícia 3.3.7. Ak n je celé číslo a a, b sú prvky poľa F , tak definujeme $n \times a$ takto:

$$0 \times a = 0,$$

$$(n + 1) \times a = n \times a + a \text{ (zatiaľ sme to indukciou definovali pre prirodzené čísla),}$$

Ak $n > 0$ tak definujeme $(-n) \times a = -(n \times a)$ (tým sme rozšírili definíciu aj na záporné čísla).

Podobne definujeme pre $a \neq 0$:

$$a^0 = 1,$$

$$a^{n+1} = a^n . a,$$

$$a^{-n} = (a^n)^{-1} \text{ (} n > 0 \text{)}.$$

Kapitola 4

Vektorové priestory

4.1 Vektorový priestor

Definícia 4.1.1. Nech F je pole a $V \neq \emptyset$ je množina. Nech $+$ je binárna operácia na V a každej dvojici $c \in F$, $\vec{\alpha} \in V$ je priradený prvok $c.\vec{\alpha} \in V$, pričom platí pre ľubovoľné $c, d \in F$ a $\vec{\alpha}, \vec{\beta} \in V$:

- (i) $(V, +)$ je komutatívna grupa,
- (ii) $c.(\vec{\alpha} + \vec{\beta}) = c.\vec{\alpha} + c.\vec{\beta}$,
- (iii) $(c + d).\vec{\alpha} = c.\vec{\alpha} + d.\vec{\alpha}$,
- (iv) $(c.d).\vec{\alpha} = c.(d.\vec{\alpha})$,
- (v) $1.\vec{\alpha} = \vec{\alpha}$.

Potom hovoríme, že V je *vektorový priestor* nad poľom F .

Veta 4.1.2. Nech V je vektorový priestor nad poľom F , $c \in F$ a $\vec{\alpha} \in V$.

- (a) $0.\vec{\alpha} = \vec{0}$,
- (b) $c.\vec{0} = \vec{0}$,
- (c) $c.\vec{\alpha} = \vec{0}$ práve vtedy, keď $c = 0$ alebo $\vec{\alpha} = \vec{0}$,
- (d) $(-c).\vec{\alpha} = -c.\vec{\alpha}$.

4.2 Podpriestory

Definícia 4.2.1. Ak V je vektorový priestor nad poľom F , $S \neq \emptyset$ a $S \subseteq V$, tak S nazveme *podpriestorom* (alebo tiež *vektorovým podpriestorom*) priestoru V , ak

- (i) pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in S$ platí $\vec{\alpha} + \vec{\beta} \in S$,
- (ii) pre ľubovoľné $\vec{\alpha} \in S$ a $c \in F$ platí $c.\vec{\alpha} \in S$.

Tvrdenie 4.2.2 (Kritérium vektorového podpriestoru). *Nech V je vektorový priestor nad poľom F a $S \subseteq V$, $S \neq \emptyset$. Potom S je podpriestor V práve vtedy, keď pre ľubovoľné $c, d \in F$ a $\vec{\alpha}, \vec{\beta} \in V$ platí*

$$\vec{\alpha}, \vec{\beta} \in S \quad \Rightarrow \quad c\vec{\alpha} + d\vec{\beta} \in S. \quad (4.1) \quad \{\text{ppr:EQKRIT}\}$$

Veta 4.2.3. *Ak S a T sú podpriestory vektorového priestoru V , tak aj $S \cap T$ je podpriestor V .*

Dôsledok 4.2.4. *Nech $n \in \mathbb{N}$. Ak S_1, S_2, \dots, S_n sú podpriestory priestoru V , tak aj $\bigcap_{i=1}^n S_i$ je podpriestor priestoru V .*

Veta 4.2.5. *Nech I je ľubovoľná množina a S_i je podpriestor priestoru V pre každé $i \in I$. Potom aj $\bigcap_{i \in I} S_i$ je podpriestor priestoru V .*

4.3 Lineárna kombinácia, lineárna nezávislosť

4.3.1 Lineárna kombinácia a lineárny obal

Definícia 4.3.1. *Nech V je vektorový priestor nad poľom F . Hovoríme, že vektor $\vec{\alpha}$ je lineárnou kombináciou vektorov $\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n$, ak existujú skaláry $c_1, c_2, \dots, c_n \in F$ také, že*

$$\vec{\alpha} = c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \dots + c_n\vec{\alpha}_n.$$

Skaláry c_1, c_2, \dots, c_n nazývame *koeficienty lineárnej kombinácie*.

Tvrdenie 4.3.2. *Nech V je vektorový priestor nad poľom F . Ak $\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n \in V$, tak množina*

$$M = \{c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \dots + c_n\vec{\alpha}_n; n \in \mathbb{N}, c_i \in F, \vec{\alpha}_i \in V \text{ pre } i = 1, 2, \dots, n\}$$

je podpriestor vektorového priestoru V .

Tento podpriestor nazývame lineárny obal vektorov $\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n$ alebo podpriestor generovaný vektormi $\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n$. Označujeme ho

$$M =: [\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n].$$

Ak platí $[\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n] = V$, hovoríme, že vektory $\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n$ generujú vektorový priestor V .

Lema 4.3.3. *Ak $\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n \in S$, kde S je podpriestor vektorového priestoru V nad poľom F , aj ich ľubovoľná lineárna kombinácia $c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \dots + c_n\vec{\alpha}_n$ patrí do podpriestoru S .*

Veta 4.3.4. *Ak $\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n \in S$, kde S je podpriestor vektorového priestoru V nad poľom F , tak $[\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n] \subseteq S$.*

Veta 4.3.5. *Nech $\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n \in V$, $\vec{\beta} \in V$, kde V je vektorový priestor nad poľom F . Potom $\vec{\beta}$ je lineárnou kombináciou vektorov $\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n$ práve vtedy, keď*

$$[\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n] = [\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n, \vec{\beta}].$$

4.3.2 Lineárna nezávislosť

Definícia 4.3.6. Nech V je vektorový priestor nad poľom F . Vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sú *lineárne závislé*, ak existujú $c_1, \dots, c_n \in F$, ktoré nie sú všetky nulové a platí

$$c_1\vec{\alpha}_1 + \dots + c_n\vec{\alpha}_n = \vec{0}.$$

(Stručne: $\vec{0}$ je nenulovou lineárnou kombináciou vektorov $\vec{\alpha}_1, \dots, \vec{\alpha}_n$.)

V opačnom prípade hovoríme, že vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ *lineárne nezávislé*.

Veta 4.3.7. Nech V je vektorový priestor nad poľom F . Nech n je prirodzené číslo, $n \geq 2$ a $\vec{\alpha}_1, \dots, \vec{\alpha}_n \in V$. Vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sú *lineárne závislé práve vtedy*, keď niektorý z nich je lineárnou kombináciou ostatných.

Veta 4.3.8. Nech V je vektorový priestor nad poľom F . Nech $\vec{\alpha}_1, \dots, \vec{\alpha}_n \in V$ sú vektory také, že $\vec{\alpha}_1 \neq \vec{0}$. Vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sú *lineárne závislé práve vtedy*, keď niektorý z nich je lineárnou kombináciou predchádzajúcich.

Veta 4.3.9. Nech V je vektorový priestor nad poľom F . Vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n \in V$ sú *lineárne závislé práve vtedy*, keď niektorý z nich je lineárnou kombináciou predchádzajúcich.

Veta 4.3.10 (Steinitzova veta o výmene). Nech V je vektorový priestor nad poľom F . Ak $V = [\vec{\alpha}_1, \dots, \vec{\alpha}_n]$ (vektorový priestor V je generovaný vektormi $\vec{\alpha}_1, \dots, \vec{\alpha}_n$) a $\vec{\beta}_1, \dots, \vec{\beta}_s \in V$ sú *lineárne nezávislé vektory*, tak

(i) $s \leq n$,

(ii) z vektorov $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sa dá vybrať $n - s$ vektorov, ktoré spolu s vektormi $\vec{\beta}_1, \dots, \vec{\beta}_s$ generujú V .

4.4 Báza a dimenzia

Definícia 4.4.1. Nech V je vektorový priestor. Hovoríme, že V je *konečnorozmerný* ak existuje taká konečná množina vektorov $\{\vec{\alpha}_1, \dots, \vec{\alpha}_n\}$, že platí $[\vec{\alpha}_1, \dots, \vec{\alpha}_n] = V$.

Definícia 4.4.2. Nech V je vektorový priestor nad poľom F . Množinu vektorov $\{\vec{\alpha}_1, \dots, \vec{\alpha}_n\}$ nazývame *bázou* priestoru V , ak

(i) vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sú *lineárne nezávislé*,

(ii) $V = [\vec{\alpha}_1, \dots, \vec{\alpha}_n]$.

(Stručne: Báza je taká množina lineárne nezávislých vektorov, ktorá generuje celý priestor.)

Veta 4.4.3. *Lubovoľné dve bázy konečnorozmerného vektorového priestoru V majú rovnaký počet prvkov.*

Veta 4.4.4. Nech V je konečnorozmerný vektorový priestor. Ak $\vec{\beta}_1, \dots, \vec{\beta}_s \in V$ sú *lineárne nezávislé*, tak sa dajú doplniť na bázu priestoru V .

Dôsledok 4.4.5. Každý konečnorozmerný vektorový priestor $V \neq \{\vec{0}\}$ má bázu.

Definícia 4.4.6. *Dimenziou* konečnorozmerného vektorového priestoru V nazývame počet prvkov ľubovoľnej jeho bázy. (Pre nulový priestor dodefinojeme $d(\{\vec{0}\}) = 0$.) Toto číslo označujeme $d(V)$.

Dôsledok 4.4.7. Ak V je konečnorozmerný vektorový priestor a $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sú lineárne nezávislé vo V , tak $n \leq d(V)$.

Veta 4.4.8. Nech V je konečnorozmerný vektorový priestor a $d(V) = n$. Nasledujúce podmienky sú ekvivalentné:

- (i) $\{\vec{\alpha}_1, \dots, \vec{\alpha}_n\}$ je báza priestoru V ,
- (ii) vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sú lineárne nezávislé,
- (iii) $V = [\vec{\alpha}_1, \dots, \vec{\alpha}_n]$.

Veta 4.4.9. Nech V je vektorový priestor. Vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ tvoria bázu priestoru V práve vtedy, keď každý vektor $\vec{\beta}$ sa dá jednoznačne vyjadriť ako

$$\vec{\beta} = c_1\vec{\alpha}_1 + \dots + c_n\vec{\alpha}_n.$$

Veta 4.4.10. Ľubovoľný podpriestor S konečnorozmerného priestoru V je konečnorozmerný. Navyše, $d(S) \leq d(V)$.

Tvrdenie 4.4.11. Ak S je podpriestor konečnorozmerného vektorového priestoru V a $d(S) = d(V)$, tak $S = V$.

4.5 Lineárne a direktné súčty podpriestorov

Veta 4.5.1. Nech S, T sú vektorové podpriestory vektorového priestoru V nad poľom F . Potom

$$S + T = \{\vec{\alpha} + \vec{\beta}; \vec{\alpha} \in S, \vec{\beta} \in T\}$$

je podpriestorom vektorového priestoru V .

Definícia 4.5.2. Ak S, T sú podpriestory vektorového podpriestoru V , tak vektorový podpriestor $S + T$ sa nazýva *lineárny súčet* podpriestorov S a T .

Veta 4.5.3. Nech S a T sú podpriestory vektorového priestoru V nad poľom F . Nech $S = [\vec{\alpha}_1, \dots, \vec{\alpha}_n]$, $T = [\vec{\beta}_1, \dots, \vec{\beta}_m]$. Potom $S + T = [\vec{\alpha}_1, \dots, \vec{\alpha}_n, \vec{\beta}_1, \dots, \vec{\beta}_m]$.

Veta 4.5.4. Nech S, T sú podpriestory konečnorozmerného priestoru V . Potom¹

$$d(S) + d(T) = d(S + T) + d(S \cap T).$$

Definícia 4.5.5. Nech S, T sú podpriestory vektorového priestoru V nad poľom F a nech $S \cap T = \{\vec{0}\}$. Potom podpriestor $S + T$ nazývame *direktný (priamy) súčet* podpriestorov S a T a označujeme ho $S \oplus T$.

Veta 4.5.6. Nech S, T, P sú podpriestory konečnorozmerného vektorového priestoru V nad poľom F . Tieto podmienky sú potom ekvivalentné:

- (i) $P = S \oplus T$
- (ii) $P = S + T$ a $d(P) = d(S) + d(T)$
- (iii) Ak $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ je báza podpriestoru S a $\vec{\beta}_1, \dots, \vec{\beta}_m$ je báza podpriestoru T , tak $\vec{\alpha}_1, \dots, \vec{\alpha}_n, \vec{\beta}_1, \dots, \vec{\beta}_m$ je báza podpriestoru P .
- (iv) $P = S + T$ a každý vektor $\vec{\gamma} \in P$ sa dá jediným spôsobom vyjadriť v tvare $\vec{\alpha} + \vec{\beta}$, kde $\vec{\alpha} \in S$ a $\vec{\beta} \in T$. (T.j. ak $\vec{\gamma} = \vec{\alpha}_1 + \vec{\beta}_1 = \vec{\alpha}_2 + \vec{\beta}_2$, pričom $\vec{\alpha}_1, \vec{\alpha}_2 \in S$ a $\vec{\beta}_1, \vec{\beta}_2 \in T$, tak $\vec{\alpha}_1 = \vec{\alpha}_2$ a $\vec{\beta}_1 = \vec{\beta}_2$.)

¹Tento vzorec pripomína vzorec pre počet prvkov zjednotenia dvoch množín $|S \cup T| = |S| + |T| - |S \cap T|$.

Kapitola 5

Lineárne zobrazenia a matice

5.1 Matice

Definícia 5.1.1. *Maticou* typu $m \times n$ nad poľom F nazývame ľubovoľnú tabuľku pozostávajúcu z prvkov poľa F , ktorá má m riadkov a n stĺpcov.

Definícia 5.1.2. Nech A, B sú matice typu $m \times n$ nad poľom F a $c \in F$.

(a) Súčet matíc $A = \|a_{ij}\|$ a $B = \|b_{ij}\|$ je matica $A + B = \|a_{ij} + b_{ij}\|$.

(b) Matica $c.A = \|ca_{ij}\|$ sa nazýva *c-násobok* matice A .

(Teda sčítovanie matíc a násobenie matice skalárom definujeme po súradniciach.)

Veta 5.1.3. *Matice typu $m \times n$ nad poľom F s takto definovaným sčítovaním a násobením skalármi tvoria vektorový priestor nad poľom F .*

Definícia 5.1.4. Maticu typu $n \times n$ (teda takú, ktorá má rovnaký počet riadkov a stĺpcov) nazývame *štvorcová matica*.

Maticu

$$I = I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

typu $n \times n$, ktorá má na diagonále jednotky a mimo diagonály nuly, nazývame *jednotková matica*.

Štvorcová matica, ktorá má mimo diagonály iba nuly (t.j. $a_{ij} = 0$ pre $i \neq j$) sa nazýva *diagonálna matica*. (Príkladom diagonálnej matice je jednotková matica.)

Definícia 5.1.5. *Transponovaná matica* k matici A typu $m \times n$ je matica A^T typu $n \times m$ určená ako

$$A^T = \|a_{ji}\|.$$

Štvorcová matica A sa nazýva *symetrická*, ak $A = A^T$ a *antisymetrická*, ak $A = -A^T$.

5.2 Riadková ekvivalencia a hodnosť matice

Definícia 5.2.1. Podpriestorom prislúchajúcim matici A typu $m \times n$ nad poľom F nazývame podpriestor priestoru F^n generovaný riadkami matice A . Označujeme ho V_A .

Definícia 5.2.2. Elementárne riadkové operácie na matici A nad poľom F sú:

1. výmena 2 riadkov matice,
2. vynásobenie niektorého riadku matice nenulovým prvkom c poľa F ,
3. pripočítanie násobku niektorého riadku k inému riadku.

Hovoríme, že matice A a B sú *riadkovo ekvivalentné* ak maticu B možno z A dostať pomocou konečnej postupnosti elementárnych riadkových operácií. Ak matice A a B sú riadkovo ekvivalentné, zapisujeme to ako $A \sim B$.

Veta 5.2.3. Elementárne riadkové operácie nemenia podpriestor prislúchajúci danej matici. (Teda riadkovo ekvivalentným maticiam zodpovedá rovnaký podpriestor.)

Definícia 5.2.4. Matica A je *redukovaná trojuholníková matica*, ak:

- (i) Vedúci (=prvý nenulový) prvok každého riadku matice je 1.
- (ii) Každý stĺpec obsahujúci vedúci prvok niektorého riadku má prvky v ostatných riadkoch nulové.
- (iii) Nulové riadky ležia pod nenulovými riadkami.
- (iv) Vedúci prvok ľubovoľného nenulového riadku je napravo od vedúcich prvkov všetkých nenulových riadkov pod ním a naľavo od vedúcich prvkov riadkov nad ním (t.j. vedúce riadky sú usporiadané zľava doprava).

Veta 5.2.5. Každá matica nad poľom F je riadkovo ekvivalentná s nejakou redukovanou trojuholníkovou maticou.

Veta 5.2.6. Nenulové riadky redukovanej trojuholníkovej matice sú lineárne nezávislé.

Definícia 5.2.7. Hodnosť matice A je dimenzia priestoru V_A prislúchajúceho tejto matici. Označujeme ju $h(A)$.

Lema 5.2.8. Nech A je redukovaná trojuholníková matica typu $m \times n$ nad poľom F . Označme jej nenulové riadky $\vec{\alpha}_1, \dots, \vec{\alpha}_k$ a ako i_1, \dots, i_k označme čísla stĺpcov, v ktorých sú vedúce jednotky. Potom $\vec{\alpha} = (c_1, \dots, c_k) \in V_A$ práve vtedy, keď $\vec{\alpha} = c_{i_1}\vec{\alpha}_1 + c_{i_2}\vec{\alpha}_2 + \dots + c_{i_k}\vec{\alpha}_k$.

Veta 5.2.9. Ak A a B sú redukované trojuholníkové matice rovnakého typu $m \times n$ nad poľom F a $V_A = V_B$, tak $A = B$.

Dôsledok 5.2.10. Nech A a B sú matice typu $m \times n$ nad poľom F . Nasledovné podmienky sú ekvivalentné:

- (i) A a B sú riadkovo ekvivalentné,
- (ii) $V_A = V_B$,
- (iii) A a B sú riadkovo ekvivalentné s tou istou redukovanou trojuholníkovou maticou.

5.3 Lineárne zobrazenia

Definícia 5.3.1. Ak V a W sú vektorové priestory nad poľom F a $f: V \rightarrow W$ je zobrazenie z V do W , tak hovoríme, že f je *lineárne zobrazenie*, ak pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in V$ a ľubovoľné $c \in F$ platí

$$(i) f(\vec{\alpha} + \vec{\beta}) = f(\vec{\alpha}) + f(\vec{\beta}),$$

$$(ii) f(c\vec{\alpha}) = cf(\vec{\alpha}).$$

Veta 5.3.2. Nech V, W sú vektorové priestory nad poľom F a $f: V \rightarrow W$ je zobrazenie. Nasledujúce podmienky sú ekvivalentné:

(a) zobrazenie f je lineárne,

$$(b) f(c\vec{\alpha} + d\vec{\beta}) = cf(\vec{\alpha}) + df(\vec{\beta}) \text{ pre ľubovoľné } c, d \in F \text{ a ľubovoľné } \vec{\alpha}, \vec{\beta} \in V,$$

$$(c) f(c_1\vec{\alpha}_1 + \dots + c_n\vec{\alpha}_n) = c_1f(\vec{\alpha}_1) + \dots + c_nf(\vec{\alpha}_n) \text{ pre ľubovoľné } c_1, \dots, c_n \in F, \vec{\alpha}_1, \dots, \vec{\alpha}_n \in V.$$

Tvrdenie 5.3.3. Ak f je lineárne zobrazenie, tak $f(\vec{0}) = \vec{0}$.

Veta 5.3.4. Nech V, W sú vektorové priestory. Nech $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ je báza priestoru V a nech $\vec{\beta}_1, \dots, \vec{\beta}_n \in W$. Potom existuje práve jedno lineárne zobrazenie $f: V \rightarrow W$ také, že

$$f(\vec{\alpha}_i) = \vec{\beta}_i$$

pre $i = 1, 2, \dots, n$.

Definícia 5.3.5. Nech F je pole. Matica lineárneho zobrazenia $f: F^m \rightarrow F^n$ je matica typu $m \times n$ ktorej k -ty riadok je vektor $f(\vec{\varepsilon}_k)$.

Veta 5.3.6. Nech U, V, W sú vektorové priestory nad tým istým poľom F . Ak $f: U \rightarrow V$ a $g: V \rightarrow W$ sú lineárne zobrazenia, tak aj $g \circ f$ je lineárne zobrazenie.

5.4 Súčin matíc

Definícia 5.4.1. Ak A je matica typu $m \times n$ a B je matica typu $n \times k$ nad poľom F , tak maticu $C = \|c_{ij}\|$ typu $m \times k$, kde

$$c_{ij} = \sum_{t=1}^n a_{it}b_{tj}$$

pre $i = 1, 2, \dots, m$ a $j = 1, 2, \dots, k$, nazývame *súčin matíc* A a B . Označujeme ju $A.B$.

Veta 5.4.2. Nech F je pole, $f: F^m \rightarrow F^n$ a $g: F^n \rightarrow F^k$ sú lineárne zobrazenia. Potom platí

$$A_{g \circ f} = A_f.A_g$$

Dôsledok 5.4.3. Násobenie matíc je asociatívne, teda

$$A.(B.C) = (A.B).C$$

pre ľubovoľné matice také, že ich možno násobiť v uvedenom poradí.

Veta 5.4.4. Nech matice A, B, C nad poľom F sú majú také rozmery, že uvedené súčty a súčiny majú zmysel.

$$\begin{aligned} I_m A &= A = A I_n \\ A(B + C) &= AB + AC \\ (B + C)D &= BC + BD \end{aligned}$$

5.5 Inverzná matica

Veta 5.5.1. Ak $f: V \rightarrow W$ je lineárne zobrazenie a existuje inverzné zobrazenie $f^{-1}: W \rightarrow V$, tak f^{-1} je lineárne zobrazenie.

Lema 5.5.2. Nech $f: V \rightarrow W$ je lineárne zobrazenie a $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ je báza priestoru V .

- (i) Zobrazenie f je injekcia práve vtedy, keď vektory $f(\vec{\alpha}_1), \dots, f(\vec{\alpha}_n)$ sú lineárne nezávislé.
- (ii) Zobrazenie f je surjekcia práve vtedy, keď $[f(\vec{\alpha}_1), \dots, f(\vec{\alpha}_n)] = W$ (teda ak vektory $f(\vec{\alpha}_1), \dots, f(\vec{\alpha}_n)$ generujú celý priestor W).

Veta 5.5.3. Nech $f: V \rightarrow W$ je lineárne zobrazenie a $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ je báza priestoru V . Zobrazenie f je bijekcia práve vtedy, keď vektory $f(\vec{\alpha}_1), \dots, f(\vec{\alpha}_n)$ tvoria bázu vektorového priestoru W .

Dôsledok 5.5.4. Nech $f: F^n \rightarrow F^n$ je lineárne zobrazenie. Nasledujúce podmienky sú ekvivalentné:

- (i) f je bijekcia,
- (ii) f je prosté,
- (iii) f je surjektívne.

Dôsledok 5.5.5. Nech $f: F^n \rightarrow F^n$ je lineárne zobrazenie. Nasledujúce podmienky sú ekvivalentné:

- (a) zobrazenie f je bijekcia,
- (b) existuje inverzné zobrazenie f^{-1} ,
- (c) $h(A_f) = n$.

Definícia 5.5.6. Nech A je matica typu $n \times n$. Hovoríme, že matica B je inverzná k matici A , ak platí

$$AB = BA = I_n.$$

Označujeme ju $B =: A^{-1}$.

Definícia 5.5.7. Štvorcová matica typu $n \times n$ sa nazýva regulárna, ak $h(A) = n$.

Veta 5.5.8. Nech A je matica typu $n \times n$. K matici A existuje inverzná matica práve vtedy, keď A je regulárna.

Definícia 5.5.9. Bijektívne lineárne zobrazenie $f: V \rightarrow W$ nazývame izomorfismus vektorových priestorov V a W (alebo tiež lineárny izomorfizmus).

Ak existuje bijektívne zobrazenie $f: V \rightarrow W$, hovoríme, že vektorové priestory V a W sú izomorfné. Fakt, že V a W sú izomorfné označujeme $V \cong W$.

Veta 5.5.10. Nech V je vektorový priestor nad poľom F a $d(V) = n$. Potom V je izomorfný s priestorom F^n .

5.6 Elementárne riadkové operácie a súčin matic*

Definícia 5.6.1. Pre ľubovoľnú elementárnu riadkovú operáciu na matici typu $m \times n$ nazveme *maticou elementárnej riadkovej operácie* maticu typu $m \times m$, ktorá vznikne vykonaním tejto operácie na jednotkovej matici I_m .

Tvrdenie 5.6.2. Ak matica B vznikne z matice A vykonaním nejakej elementárnej riadkovej operácie a E je matica tejto riadkovej operácie, tak $B = E.A$.

Tvrdenie 5.6.3. Ak matica B vznikne z matice A vykonaním nejakej elementárnej stĺpcovej operácie a E je matica tejto stĺpcovej operácie, tak $B = A.E$.

5.7 Sústavy lineárnych rovníc

Definícia 5.7.1. *Sústavou lineárnych rovníc* rozumieme systém rovníc tvaru

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= c_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= c_2 \\ &\dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= c_m \end{aligned} \tag{5.1} \quad \{\text{sust:EQSUST}\}$$

kde $a_{ij}, c_i \in F$ pre všetky prípustné hodnoty indexov i a j .

Riešenie sústavy lineárnych rovníc je n -ticia (x_1, \dots, x_n) ktorá spĺňa všetky uvedené rovnice. Ak existuje aspoň jedno riešenie sústavy lineárnych rovníc, hovoríme, že táto sústava je *riešiteľná*. Skaláry c_1, \dots, c_n nazývame *pravé strany*, a_{ij} sú *koefficienty* a x_i sú *neznáme*.

Maticu

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

nazývame *matica sústavy* (5.1).

Maticu

$$A' = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & c_1 \\ a_{21} & a_{22} & \dots & a_{2n} & c_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} & c_m \end{pmatrix}$$

nazývame *rozšírená matica sústavy* (5.1).

Veta 5.7.2. Ak rozšírené matice dvoch sústav lineárnych rovníc sú riadkovo ekvivalentné, tak tieto dve sústavy majú rovnakú množinu riešení.

5.7.1 Homogénne sústavy lineárnych rovníc

Veta 5.7.3. Množina všetkých riešení homogénnej sústavy lineárnych rovníc tvorí vektorový priestor priestoru F^n .

$$\begin{aligned} x_1 + c_{1,r+1}x_{r+1} + c_{1,r+2}x_{r+2} + \dots + c_{1,n}x_n &= 0 \\ x_2 + c_{2,r+1}x_{r+1} + c_{2,r+2}x_{r+2} + \dots + c_{2,n}x_n &= 0 \\ &\dots \\ x_r + c_{r,r+1}x_{r+1} + c_{r,r+2}x_{r+2} + \dots + c_{r,n}x_n &= 0 \end{aligned} \tag{5.2} \quad \{\text{sust:EQHOM}\}$$

Veta 5.7.4. Vektory $\vec{\gamma}_{r+1}, \vec{\gamma}_{r+2}, \dots, \vec{\gamma}_n$ tvoria bázu priestoru riešení homogénnej sústavy (5.2).

Dôsledok 5.7.5. Nech A je matica typu $m \times n$ a S je priestor riešení homogénnej sústavy lineárnych rovníc s maticou A . Potom

$$d(S) = n - h(A).$$

Dôsledok 5.7.6. Homogénna sústava lineárnych rovníc s n neznámymi, ktorej matica má hodnotu n , má len triviálne riešenie.

Veta 5.7.7. Každý podpriestor priestoru F^n je množinou riešení nejakého homogénneho systému lineárnych rovníc.

5.7.2 Gaussova eliminačná metóda

5.7.3 Frobeniova veta

Veta 5.7.8. Pre každú maticu A nad poľom F platí $h(A) = h(A^T)$.

Veta 5.7.9 (Frobeniova). Nehomogénna sústava lineárnych rovníc (5.1) je riešiteľná práve vtedy, keď matica sústavy a rozšírená matica sústavy majú rovnakú hodnotu, t.j.

$$h(A) = h(A').$$

Veta 5.7.10. Nech $\vec{\alpha}$ je riešenie sústavy lineárnych rovníc

$$A \cdot \vec{\alpha}^T = \vec{\gamma}^T \tag{N} \quad \{\text{sust:EQN}\}$$

a S je podpriestor pozostávajúci zo všetkých riešení homogénneho systému

$$A \cdot \vec{\alpha}^T = \vec{0}^T. \tag{H} \quad \{\text{sust:EQH}\}$$

Potom $T = \{\vec{\alpha} + \vec{\beta}; \vec{\beta} \in S\}$ je množina všetkých riešení (N).

5.8 Jadro a obraz lineárneho zobrazenia[△]

Definícia 5.8.1. Nech V a W sú vektorové priestory nad poľom F a $f: V \rightarrow W$ je lineárne zobrazenie. Potom *jadrom lineárneho zobrazenia f* nazývame množinu

$$\text{Ker } f = \{\vec{\alpha} \in V; f(\vec{\alpha}) = \vec{0}\}$$

a *obrazom lineárneho zobrazenia f* nazývame množinu

$$\text{Im } f = \{f(\vec{\alpha}); \vec{\alpha} \in V\}.$$

Tvrdenie 5.8.2. Nech V a W sú vektorové priestory nad poľom F a $f: V \rightarrow W$ je lineárne zobrazenie. Potom $\text{Ker } f$ je vektorový podpriestor priestoru V a $\text{Im } f$ je vektorový podpriestor priestoru W .

Tvrdenie 5.8.3. Nech V a W sú vektorové priestory nad poľom F a $f: V \rightarrow W$ je lineárne zobrazenie.

Zobrazenie f je injektívne práve vtedy, keď $\text{Ker } f = \{\vec{0}\}$.

Tvrdenie 5.8.4. *Nech V a W sú vektorové priestory nad poľom F a $f: V \rightarrow W$ je lineárne zobrazenie.*

Zobrazenie f je surjektívne práve vtedy, keď $\text{Im } f = W$.

Dôsledok 5.8.5. *Lineárne zobrazenie $f: V \rightarrow W$ je izomorfizmus práve vtedy, keď $\text{Im } f = W$ a $\text{Ker } f = \{\vec{0}\}$.*

Veta 5.8.6. *Nech V a W sú konečnorozmerné vektorové priestory a $f: V \rightarrow W$ je lineárne zobrazenie. Potom*

$$d(V) = d(\text{Ker } f) + d(\text{Im } f).$$

5.9 Hodnosť transponovanej matice

Kapitola 6

Determinanty

6.1 Motivácia

6.2 Definícia determinantu

Definícia 6.2.1. V tejto kapitole budeme označovať ako S_n množinu všetkých permutácií množiny $\{1, 2, \dots, n\}$.

Dvojica $(\varphi(k), \varphi(s))$ sa volá *inverzia* permutácie φ , ak $k < s$ ale $\varphi(k) > \varphi(s)$. Počet inverzií permutácie φ budeme označovať $i(\varphi)$.

Definícia 6.2.2. Nech A je matica typu $n \times n$ nad poľom F , $A = \|a_{ij}\|$. *Determinant matice* A je

$$|A| = \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} a_{2\varphi(2)} \cdots a_{n\varphi(n)}. \quad (6.1) \quad \{\text{det:EQDEF}\}$$

Veta 6.2.3. Nech A je matica typu $n \times n$. Potom

$$|A| = |A^T|.$$

6.3 Výpočet determinantov

6.3.1 Laplaceov rozvoj

Veta 6.3.1. Pre algebraický doplnok prvku a_{rs} štvorcovej matice A platí

$$A_{rs} = (-1)^{r+s} |M_{rs}|$$

Dôsledok 6.3.2 (Laplaceov rozvoj determinantu). Nech A je matica typu $n \times n$. Potom

$$|A| = (-1)^{i+1} a_{i1} |M_{i1}| + (-1)^{i+2} a_{i2} |M_{i2}| + \dots + (-1)^{i+n} a_{in} |M_{in}| \quad (6.2) \quad \{\text{det:EQ LAPR}\}$$

$$|A| = (-1)^{j+1} a_{1j} |M_{1j}| + (-1)^{j+2} a_{2j} |M_{2j}| + \dots + (-1)^{j+n} a_{nj} |M_{nj}| \quad (6.3) \quad \{\text{det:EQ LAPS}\}$$

6.3.2 Výpočet pomocou riadkových a stĺpcových operácií

Veta 6.3.3. Ak maticu B získame z A vynásobením k -teho riadku skalárom $c \in F$, tak

$$|B| = c|A|.$$

Dôsledok 6.3.4. Ak matica A má nulový riadok, tak $|A| = 0$.

Veta 6.3.5. Ak má matica A dva rovnaké riadky, tak $|A| = 0$.

Veta 6.3.6. Nech matice A a B sú matice typu $n \times n$, ktoré sa líšia len v k -tom riadku. Potom $|A| + |B| = |C|$, kde $c_{ij} = a_{ij} = b_{ij}$ pre $i \neq k$ a $c_{kj} = a_{kj} + b_{kj}$.

Veta 6.3.7. Ak matica B vznikne z A pripočítaním c -násobku niektorého riadku k inému (pričom $c \in F$), tak $|B| = |A|$.

Veta 6.3.8. Ak matica B vznikne z A vzájomnou výmenou dvoch riadkov, tak $|B| = -|A|$. (Výmena 2 riadkov matice mení znamienko determinantu.)

Veta 6.3.9. Ak A je horná trojuholníková matica (pod hlavnou diagonálou má nuly), tak determinant matice A sa rovná súčinnu prvkov na diagonále.

$$|A| = a_{11}a_{22} \dots a_{nn}$$

Dôsledok 6.3.10. Determinant diagonálnej matice sa rovná súčinnu diagonálnych prvkov.

$$\begin{vmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{vmatrix} = d_1 d_2 \dots d_n$$

Veta 6.3.11. Nech A je štvorcová matica typu $n \times n$. Matica A je regulárna práve vtedy, keď $|A| \neq 0$.

6.4 Determinant súčinnu matíc

Veta 6.4.1. Nech A, B sú dve matice typu $n \times n$ nad poľom F . Potom platí

$$|A \cdot B| = |A| \cdot |B|.$$

6.5 Využitie determinantov

6.5.1 Výpočet inverznej matice

Veta 6.5.1. Ak A je regulárna matica typu $n \times n$, tak

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

kde A_{ij} označuje algebraický doplnok prvku a_{ij} .

6.5.2 Cramerovo pravidlo

Kapitola 7

Euklidovské vektorové priestory

7.1 Skalárny súčin

Definícia 7.1.1. Nech $(V, +, \cdot)$ je vektorový priestor nad poľom \mathbb{R} . Potom zobrazenie $g: V \times V \rightarrow \mathbb{R}$ sa nazýva *skalárny súčin* na V , ak pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in V$ a $c \in F$ platí

- (i) $g(\vec{\alpha}, \vec{\beta}) = g(\vec{\beta}, \vec{\alpha})$,
- (ii) $g(\vec{\alpha} + \vec{\beta}, \vec{\gamma}) = g(\vec{\alpha}, \vec{\gamma}) + g(\vec{\beta}, \vec{\gamma})$,
- (iii) $g(c\vec{\alpha}, \vec{\beta}) = cg(\vec{\alpha}, \vec{\beta})$,
- (iv) ak $\vec{\alpha} \neq \vec{0}$, tak $g(\vec{\alpha}, \vec{\alpha}) > 0$.

Vektorový priestor V spolu so skalárnym súčinom g nazývame *euklidovským vektorovým priestorom*.

Definícia 7.1.2. Nech V je euklidovský vektorový priestor. Potom pre $\vec{\alpha} \in V$ definujeme veľkosť vektora $\vec{\alpha}$ ako

$$|\vec{\alpha}| = \sqrt{\langle \vec{\alpha}, \vec{\alpha} \rangle}.$$

Tvrdenie 7.1.3. Nech V je euklidovský vektorový priestor. Pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in V$ a $c \in \mathbb{R}$ platí:

- (i) $|\vec{\alpha}| \geq 0$
- (ii) $|\vec{\alpha}| = 0 \Leftrightarrow \vec{\alpha} = \vec{0}$
- (iii) $|c\vec{\alpha}| = |c||\vec{\alpha}|$
- (iv) $|\langle \vec{\alpha}, \vec{\beta} \rangle| \leq |\vec{\alpha}||\vec{\beta}|$ (*Schwarzova nerovnosť*)
- (v) $|\vec{\alpha} + \vec{\beta}| \leq |\vec{\alpha}| + |\vec{\beta}|$ (*trojuholníková nerovnosť*)

Definícia 7.1.4. Nech V je euklidovský vektorový priestor.

Uhol dvoch nenulových vektorov definujeme ako taký uhol, pre ktorý platí

$$\cos \varphi = \frac{\langle \vec{\alpha}, \vec{\beta} \rangle}{|\vec{\alpha}||\vec{\beta}|}.$$

V prípade, že niektorý z vektorov je nulový, položíme $\varphi = 0$.

Definícia 7.1.5. Vektory $\vec{\alpha}, \vec{\beta} \in V$ nazveme *kolmé (ortogonálne)*, ak $\langle \vec{\alpha}, \vec{\beta} \rangle = 0$.

O k -tici vektorov $\vec{\alpha}_1, \dots, \vec{\alpha}_k$ hovoríme, že tieto vektory sú ortogonálne, ak ľubovoľné 2 z nich sú ortogonálne, t.j. $\langle \vec{\alpha}_i, \vec{\alpha}_j \rangle = 0$ pre každé $i \neq j$.

Tvrdenie 7.1.6. *Nech V je euklidovský vektorový priestor. Ak nenulové vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_k$ sú ortogonálne, tak sú lineárne nezávislé*

Definícia 7.1.7. Nech V je euklidovský priestor a $M \subseteq V$. Potom

$$M^\perp = \{\alpha \in V; \langle \vec{\alpha}, \vec{\beta} \rangle = 0 \text{ pre všetky } \beta \in M\}$$

sa nazýva *ortogonálny doplnok* množiny M .

Tvrdenie 7.1.8. *Nech V je euklidovský priestor a $M \subseteq V$. Potom M^\perp je vektorový priestor priestoru V .*

Tvrdenie 7.1.9. *Ak V je euklidovský priestor a $M \subseteq N \subseteq V$, tak*

$$N^\perp \subseteq M^\perp.$$

Lema 7.1.10. *Nech V je euklidovský priestor a $\vec{\alpha}_1, \dots, \vec{\alpha}_k \in V$. Nech $S = [\vec{\alpha}_1, \dots, \vec{\alpha}_k]$ je podpriestor vygenerovaný týmito vektormi. Potom $S^\perp = \{\vec{\alpha}_1, \dots, \vec{\alpha}_k\}^\perp$.*

Tvrdenie 7.1.11. *Ak V je euklidovský priestor a S, T sú podpriestory V , tak*

$$(S + T)^\perp = S^\perp \cap T^\perp.$$

7.2 Gram-Schmidtov ortogonalizačný proces

Definícia 7.2.1. Vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sa nazývajú *ortonormálne*, ak pre všetky i platí $|\vec{\alpha}_i| = 1$ a pre $i \neq j$ platí

$$\langle \vec{\alpha}_i, \vec{\alpha}_j \rangle = 0.$$

Definícia 7.2.2. Ak vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sú ortonormálne a tvoria bázu vektorového priestoru V , tak túto bázu nazývame *ortonormálna báza*.

Veta 7.2.3. *Nech V je euklidovský vektorový priestor a $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ je báza priestoru V . Potom existuje ortonormálna báza $\vec{\beta}_1, \dots, \vec{\beta}_n$ priestoru V .*