Algebra 1

slidy k přednáškám

KMI/ALG1

Zpracováno dle přednášek prof. Ivana Chajdy.

Obsah

Obsah

Obsah

Definice

Nechť A, B jsou neprázdné množiny. **Kartézský součin množin A a B** (označujeme $A \times B$) je množina všech uspořádaných dvojic $\langle a, b \rangle$, kde $a \in A$, $b \in B$. Každou podmnožinu $R \subseteq A \times B$ nazveme **binární relace mezi množinami A a B**. Je-li $A = B$, pak $R \subseteq A \times A$ nazveme **binární relace na množině A**.

Relaci vyjadřujeme buď výčtem uspořádaných dvojic, např. pro $A = \{a, b, c\}$, $R = \{\langle a, a \rangle, \langle b, b \rangle, \langle a, c \rangle\}$ nebo nějakým předpisem. Známé binární relace: $\leq, =, \neq, \|, \perp$, býti dělitelno, atd. Někdy místo $\langle a, b \rangle \in R$ zapisujeme aRb, např. $a = b$ místo $\langle a, b \rangle \in =$, $a \leq b$ místo $\langle a, b \rangle \in \leq$, atp.

Definice

Binární relace R na množině $A \neq \emptyset$ se nazývá:

- **reflexivní**, jestliže pro každé $a \in A$ platí $\langle a, a \rangle \in R$
- **symetrická**, jestliže pro každé $a, b \in A$, pokud $\langle a, b \rangle \in R$, pak také $\langle b, a \rangle \in R$
- **tranzitivní**, jestliže pro každé $a, b, c \in A$, pokud $\langle a, b \rangle \in R$ a $\langle b, c \rangle \in R$, pak také $\langle a, c \rangle \in R$
- **antisymetrická**, jestliže pro každé $a, b \in A$, pokud $\langle a, b \rangle \in R$ a $\langle b, a \rangle \in R$, pak $a = b$.

Některé relace: **identita** neboli **rovnost** (někdy označujeme ω): $\langle a, b \rangle \in \omega$, právě když $a = b$. **Úplná relace** neboli **úplný čtverec** (označení $\imath$ nebo $A \times A$): pro každé $a, b \in A$ platí $\langle a, b \rangle \in \imath$. **Prázdná relace** $\emptyset$: pro každé $a, b \in A$ platí $\langle a, b \rangle \notin \emptyset$.

Definice

Nechť R je binární relace mezi množinami A a B a nechť S je binární relace mezi množinami B a C. **Inverzní relací** R^{-1} k relaci R nazýváme binární relaci mezi množinami B a A takovou, že $\langle a,b\rangle \in R^{-1}$, právě když $\langle b,a\rangle \in R$. **Součinem (složením) relací** R **a** S nazýváme binární relaci $R \circ S$ mezi množinami A a C definovanou takto: $\langle a,c\rangle \in R \circ S$, právě když existuje $b \in B$ tak, že $\langle a,b\rangle \in R$ a $\langle b,c\rangle \in S$.

Věta 1.1

Relační součin je asociativní, t.j. je-li R binární relace mezi množinami A a B, S je binární relace mezi množinami B a C, T je binární relace mezi množinami C a D, pak $(R \circ S) \circ T = R \circ (S \circ T)$.

Důkaz. Libovolná uspořádaná dvojice $\langle a,d \rangle \in (R \circ S) \circ T$, právě když existuje $c \in C$ tak, že $\langle a,c \rangle \in R \circ S$, $\langle c,d \rangle \in T$, právě když existuje $b \in B$ a existuje $c \in C$ tak, že $\langle a,b \rangle \in R$, $\langle b,c \rangle \in S$, $\langle c,d \rangle \in T$, právě když existuje $b \in B$ tak, že $\langle a,b \rangle \in R$, $\langle b,d \rangle \in S \circ T$, právě když $\langle a,d \rangle \in R \circ (S \circ T)$, odkud dostáváme, že $(R \circ S) \circ T = R \circ (S \circ T)$.

Věta 1.2

Nechť R je binární relace mezi množinami A a B a nechť S je binární relace mezi množinami B a C. Pak

(a) $(R^{-1})^{-1} = R$

(b) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

Důkaz.

(a) $\langle a,b\rangle \in (R^{-1})^{-1}$, právě když $\langle b,a\rangle \in R^{-1}$, což platí právě když $\langle a,b\rangle \in R$. Tedy $(R^{-1})^{-1} = R$.

(b) Libovolná uspořádaná dvojice $\langle a,c\rangle \in (R \circ S)^{-1}$, právě když $\langle c,a\rangle \in R \circ S$, právě když existuje $b \in B$ tak, že $\langle c,b\rangle \in R$, $\langle b,a\rangle \in S$, právě když existuje $b \in B$ tak, že $\langle b,c\rangle \in R^{-1}$, $\langle a,b\rangle \in S^{-1}$, právě když $\langle a,c\rangle \in S^{-1} \circ R^{-1}$, odkud $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

Věta 1.3

Nechť R je binární relace na množině A. Pak

(a) R je reflexivní, právě když $\omega \subseteq R$

(b) R je symetrická, právě když $R = R^{-1}$

(c) R je tranzitivní, právě když $R \circ R \subseteq R$.

Důkaz.

(a) $\forall a \in A$ platí $\langle a,a \rangle \in \omega$. Tedy $\omega \subseteq R$, právě když $\forall a \in A$ platí $\langle a,a \rangle \in R$ neboli R je reflexivní.

(b) Nechť R je symetrická. Jestliže $\langle a,b \rangle \in R$, pak ze symetrie $\langle b,a \rangle \in R$, což je ekvivalentní s tím, že $\langle a,b \rangle \in R^{-1}$, tedy $R = R^{-1}$. Obráceně, nechť $R = R^{-1}$. Jestliže $\langle a,b \rangle \in R$, pak $\langle b,a \rangle \in R^{-1} = R$, t.j. R je symetrická.

(c) Nechť R je tranzitivní a $\langle a,b \rangle \in R \circ R$. Pak existuje $c \in A$ tak, že $\langle a,c \rangle \in R$, $\langle c,b \rangle \in R$. Z tranzitivity plyne $\langle a,b \rangle \in R$, tedy $R \circ R \subseteq R$. Obráceně, nechť $R \circ R \subseteq R$ a nechť $\langle a,c \rangle \in R$, $\langle c,b \rangle \in R$. Pak $\langle a,b \rangle \in R \circ R \subseteq R$, tedy R je tranzitivní.

Podobně lze dokázat následující tvrzení:

(1) **Monotonie relací**: nechť R, S, T jsou binární relace na množině A, $R \subseteq S$. Pak $R^{-1} \subseteq S^{-1}$ a $R \circ T \subseteq S \circ T$, $T \circ R \subseteq T \circ S$.

(2) Nechť R je binární relace na množině A. Má-li R některou z vlastností: reflexivita, symetrie, tranzitivita, antisymetrie, pak má tuto vlastnost i R^{-1}.

(3) Jsou-li R, S reflexivní binární relace na množině A, pak $R \subseteq R \circ S$, $S \subseteq R \circ S$.

(4) Binární relace R na množině A je antisymetrická, právě když $R \cap R^{-1} \subseteq \omega$.

Příklad

Najděte dvě konkrétní binární relace R, S tak, aby $R \circ S \neq S \circ R$, t.j. dokažte, že součin binárních relací není komutativní.

Řešení: jednoduché.

Definice

Binární relace R na množině A se nazývá **ekvivalence**, je-li reflexivní, symetrická a tranzitivní.

Například ω a ι jsou ekvivalence.

Lemma

Nechť R, S jsou reflexivní binární relace na množině A. Pak $R \circ S$ je také reflexivní binární relace na A.

Důkaz. Jelikož R, S jsou reflexivní, je dle Věty 1.3 $\omega \subseteq R$, $\omega \subseteq S$ a tedy i $\omega = \omega \circ \omega \subseteq R \circ S$, t.j. $R \circ S$ je také reflexivní.

Věta 1.4

Nechť R, S jsou ekvivalence na množině A. Pak $R \circ S$ je ekvivalence na A, právě když $R \circ S = S \circ R$.

Důkaz. Předpokládejme, že $R \circ S$ je ekvivalence na A. Zřejmě $R \circ S$ je symetrická a tedy dle Věty 1.3 platí, že $R \circ S = (R \circ S)^{-1}$. Podobně platí, že $R = R^{-1}$ a $S = S^{-1}$ (neboť R, S jsou symetrické, protože jsou ekvivalence). S využitím Věty 1.2 odtud dostáváme, že

$$R \circ S = (R \circ S)^{-1} = S^{-1} \circ R^{-1} = S \circ R.$$

Předpokládejme nyní, že $R \circ S = S \circ R$. Jestliže $\langle a, b \rangle \in R \circ S$, pak $\exists x \in A$ tak, že $\langle a, x \rangle \in R$, $\langle x, b \rangle \in S$. Ze symetrie R a S plyne $\langle b, x \rangle \in S$, $\langle x, a \rangle \in R$, tedy $\langle b, a \rangle \in S \circ R = R \circ S$, neboli $R \circ S$ je symetrická.

Nechť dále $\langle a, b \rangle \in R \circ S$, $\langle b, c \rangle \in R \circ S$. Pak (v důsledku asociativity součinu relací a dle Věty 1.3.) platí $\langle a, c \rangle \in (R \circ S) \circ (R \circ S) = R \circ (S \circ R) \circ S = R \circ (R \circ S) \circ S = (R \circ R) \circ (S \circ S) \subseteq R \circ S$, tedy $R \circ S$ je tranzitivní. Dle předchozího Lemma je $R \circ S$ i reflexivní. Dohromady $R \circ S$ je ekvivalence na A.

Obsah

Definice

Nechť A, B jsou neprázdné množiny a f je binární relace mezi množinami A a B. Relace f se nazývá **zobrazení** A **do** B, má-li tyto vlastnosti:

(i) $\forall a \in A\ \exists b \in B$ tak, že $\langle a, b \rangle \in f$

(ii) jestliže $\langle x, y_1 \rangle \in f$ a $\langle x, y_2 \rangle \in f$, pak $y_1 = y_2$.

Je-li f zobrazením množiny A do B, budeme tento fakt zapisovat symbolem $f : A \to B$. Místo $\langle x, y \rangle \in f$ budeme zapisovat $y = f(x)$. Prvek y nazveme **obraz prvku** x, prvek x nazveme **vzor prvku** y. Množinu $f(A) = \{f(x); x \in A\}$ nazveme **úplný obraz množiny** A.

Věta 1.5

Nechť A, B, C jsou neprázdné množiny a $f : A \to B$, $g : B \to C$ jsou zobrazení. Pak součin relací $h = f \circ g$ je zobrazení z A do C.

Důkaz. Stačí ověřit podmínky (i) a (ii) z definice zobrazení.

(i) Nechť $a \in A$. Pak $\exists b \in B$ tak, že $\langle a, b \rangle \in f$ a $\exists c \in C$ tak, že $\langle b, c \rangle \in g$, tedy $\langle a, c \rangle \in f \circ g = h$.

(ii) Nechť $\langle a, c_1 \rangle \in h$, $\langle a, c_2 \rangle \in h$ pro $c_1, c_2 \in C$. Pak $\exists b_1, b_2 \in B$ tak, že $\langle a, b_1 \rangle \in f$, $\langle b_1, c_1 \rangle \in g$, $\langle a, b_2 \rangle \in f$, $\langle b_2, c_2 \rangle \in g$. Ale f je zobrazení, tedy $b_1 = b_2$. Avšak i g je zobrazení, tedy $c_1 = c_2$, neboli i h splňuje (ii).

Definice

Jsou-li $f : A \to B$, $g : B \to C$ zobrazení, pak relaci $f \circ g$, která je dle Věty 1.5. také zobrazením, nazveme **složené zobrazení** f, g. Tedy $f \circ g(x) = g(f(x))$.

Důsledek (Věty 1.1 a 1.5)

Skládání zobrazení je asociativní, t.j. $f \circ (g \circ h) = (f \circ g) \circ h$.

Definice

Nechť $f : A \to B$ je zobrazení. f se nazývá

(a) **surjekce**, je-li $f(A) = B$

(b) **injekce**, jestliže $\forall x_1, x_2 \in A$ platí $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

(c) **bijekce**, je-li f současně surjekce a injekce.

Bijekce $f : A \to A$ se také nazývá **permutace množiny** A.

Věta 1.6

Nechť $f : A \to B$, $g : B \to C$ jsou zobrazení. Jsou-li f, g surjekce (resp. injekce, resp. bijekce), je i $f \circ g$ surjekce (resp. injekce, resp. bijekce).

Důkaz.

(a) Nechť f, g jsou surjekce, $h = f \circ g$. Pak pro každý prvek $c \in C$ existuje $b \in B$ tak, že $g(b) = c$, a pro každý prvek $b \in B$ existuje $a \in A$ tak, že $f(a) = b$, tedy $\forall c \in C$ existuje $a \in A$ tak, že $h(a) = f \circ g(a) = g(f(a)) = g(b) = c$, t.j. h je surjekce.

(b) Nechť $a_1, a_2 \in A$, $a_1 \neq a_2$. Jelikož f je injekce, je $f(a_1) \neq f(a_2)$. Dále, g je injekce, tedy $f \circ g(a_1) = g(f(a_1)) \neq g(f(a_2)) = f \circ g(a_2)$, odkud $f \circ g$ je injekce.

(c) Jsou-li f, g bijekce, pak dle (a), (b) je $f \circ g$ surjekce i injekce, t.j. bijekce.

Věta 1.7

Nechť $f : A \to B$ je zobrazení. Inverzní relace f^{-1} je zobrazením $B \to A$ tehdy a jen tehdy, je-li f bijekce.

Důkaz.

(a) Nechť f je bijekce. Pak f je surjektivní, t.j. $\forall b \in B$ existuje $a \in A$ tak, že $b = f(a)$, t.j. $\langle a, b \rangle \in f$, neboli $\langle b, a \rangle \in f^{-1}$, t.j. f^{-1} splňuje podmínku (i) z definice zobrazení. Dokážeme (ii): nechť $\langle b, a_1 \rangle \in f^{-1}$, $\langle b, a_2 \rangle \in f^{-1}$, pak $\langle a_1, b \rangle \in f$, $\langle a_2, b \rangle \in f$, t.j. $f(a_1) = b = f(a_2)$. Jelikož f je injekce, plyne odtud $a_1 = a_2$. Tedy f^{-1} je zobrazení.

(b) Nechť relace $f^{-1} : B \to A$ je zobrazení. Pak pro každé $b \in B$ existuje $a \in A$ tak, že $f^{-1}(b) = a$, t.j. $\langle b, a \rangle \in f^{-1}$, neboli $\langle a, b \rangle \in f$, t.j. $f(a) = b$, takže f je surjekce. Dále, nechť $a_1, a_2 \in A$, $a_1 \neq a_2$. Kdyby $f(a_1) = f(a_2) = b$, pak $\langle a_1, b \rangle \in f$, $\langle a_2, b \rangle \in f$, tedy $\langle b, a_1 \rangle \in f^{-1}$, $\langle b, a_2 \rangle \in f^{-1}$, což je spor s tím, že f^{-1} je zobrazení. Tedy $f(a_1) \neq f(a_2)$, t.j. f je injekce. Dohromady, f je bijekce.

Důsledek

Nechť $f : A \to B$, $g : B \to C$ jsou bijekce. Pak

(a) $f^{-1} : B \to A$ je bijekce

(b) $g^{-1} \circ f^{-1}$ je bijekce C na A a platí $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Důkaz. Dle Věty 1.7 je f^{-1} zobrazení, a dále f^{-1} je bijekce, právě když $(f^{-1})^{-1}$ je zobrazení. Dle Věty 1.2 je ale $(f^{-1})^{-1} = f$, což je zobrazení, t.j. f^{-1} je bijekce.

Dále, dle Věty 1.2 je $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. Dle Věty 1.7 je ale $(f \circ g)^{-1}$ zobrazením C do A. Dle (a) a Věty 1.6 je tedy $g^{-1} \circ f^{-1} = (f \circ g)^{-1}$ bijekce.

Definice

Nechť $A \neq \emptyset$ je množina. Zobrazení $id_A : A \to A$ dané předpisem $id_A(x) = x$ pro každé $x \in A$ se nazývá **identické zobrazení**.

Je ihned zřejmé, že id_A je bijekce, t.j. permutace množiny A.

Věta 1.8

Nechť $f : A \to B$ je zobrazení. Pak

(a) $f = f \circ id_B = id_A \circ f$

(b) f je bijekce tehdy a jen tehdy, když existuje zobrazení $g : B \to A$ tak, že $f \circ g = id_A$, $g \circ f = id_B$.

Důkaz. Tvrzení (a) je zřejmé. Dokážeme (b):

(1) Je-li f bijekce, pak položíme $g = f^{-1}$. Zřejmě $f \circ g = f \circ f^{-1} = id_A$, $g \circ f = f^{-1} \circ f = id_B$.

(2) Nechť pro $f : A \to B$ existuje $g : B \to A$ tak, že $f \circ g = id_A$, $g \circ f = id_B$. Nechť $b \in B$. Pak $f(g(b)) = g \circ f(b) = id_B(b) = b$, tedy f je surjekce, neboť každé $b \in B$ má vzor v zobrazení f, totiž prvek $g(b) \in A$.

Nechť $a_1, a_2 \in A$. Je-li $f(a_1) = f(a_2)$, pak $a_1 = id_A(a_1) = f \circ g(a_1) = g(f(a_1)) = g(f(a_2)) = f \circ g(a_2) = id_A(a_2) = a_2$, tedy f je injekce. Dohromady, f je bijekce.

Obsah

Definice

Nechť I je některá množina a pro každé $i \in I$ je A_i množina. Pak množinu $\{A_i; i \in I\}$ nazveme **systém množin indexovaný množinou** I, nebo jen **indexovaný systém množin**.

Příklad

Je-li $I = \{1, 2, 3\}$, pak $\{A_i; i \in I\} = \{A_1, A_2, A_3\}$.

Definice

Nechť $A \neq \emptyset$. Indexovaný systém neprázdných množin $\pi = \{B_i; i \in I\}$ nazveme **rozklad množiny** A, jestliže

(i) množiny z π jsou vzájemně disjunktní, t.j. $\forall i, j \in I$, $i \neq j$ je $B_i \cap B_j = \emptyset$

(ii) π tvoří pokrytí A, t.j. $\bigcup\{B_i; i \in I\} = A$.

Množiny B_i nazýváme **třídy rozkladu** π.

Je-li $\{C_i; i \in I\}$ některý indexovaný systém množin, pak řekneme, že množiny tohoto systému jsou **po dvou různé**, jestliže $i, j \in I$, $i \neq j \Rightarrow C_i \neq C_j$.

Definice

Nechť E je ekvivalence na množině A. Pro každé $a \in A$ nazveme množinu

$$E(a) = \{b \in A; \langle a, b \rangle \in E\}$$

třídou ekvivalence E obsahující prvek a.

Věta 1.9

Nechť E je ekvivalence na množině A, nechť $a,b \in A$. Pak $E(a) = E(b)$ nebo $E(a) \cap E(b) = \emptyset$.

Důkaz. Nechť $a,b \in A$ a nechť $E(a) \cap E(b) \neq \emptyset$. Tedy existuje $c \in A$ tak, že $c \in E(a)$, $c \in E(b)$. Pak $\langle a,c \rangle \in E$, $\langle b,c \rangle \in E$, ze symetrie $\langle c,b \rangle \in E$, z tranzitivity $\langle a,b \rangle \in E$. Nechť $x \in E(a)$. Pak $\langle x,a \rangle \in E$, ale $\langle a,b \rangle \in E$, tedy z tranzitivity $\langle x,b \rangle \in E$ a ze symetrie $\langle b,x \rangle \in E$, tedy $x \in E(b)$. Dokázali jsme $E(a) \subseteq E(b)$. Podobně lze dokázat, že $E(b) \subseteq E(a)$, odkud $E(a) = E(b)$.

Poznámka. Tedy, je-li E ekvivalence na A, pak pro každé $a \in A$ utvoříme $E(a)$. Pro $b \in A$ pak je buď $E(b) = E(a)$, nebo $E(b) \cap E(a) = \emptyset$, tedy z indexovaného systému $\{E(a); a \in A\}$ lze vybrat podsystém po dvou různých množin, který ale už bude systémem vzájemně disjunktních množin.

Věta 1.10

Nechť E je ekvivalence na množině $A \neq \emptyset$. Ze systému $\{E(a); a \in A\}$ všech tříd E lze vybrat systém π_E po dvou různých množin tak, že π_E je **rozklad množiny** A, nazvaný **indukovaný ekvivalencí** E. Třídy π_E jsou třídy ekvivalence E.

Důkaz. Jelikož E je reflexivní, platí $\langle a, a \rangle \in E$ pro každé $a \in A$, t.j. $a \in E(a)$. Tedy $\{a\} \subseteq E(a)$. Dále $A = \bigcup\{\{a\}; a \in A\} \subseteq \bigcup\{E(a); a \in A\} \subseteq A$, neboť $E(a) \subseteq A$, tedy $A = \bigcup\{E(a); a \in A\}$. Vybereme-li ze systému $\{E(a); a \in A\}$ po dvou různé množiny, dostaneme podsystém π_E. To jsme ale vynechali jen „opakující se“ množiny, t.j. opět $A = \bigcup\{E(a); E(a) \in \pi_E\}$, neboli π_E tvoří pokrytí množiny A. Podle předchozí poznámky (a Věty 1.9) je π_E systém vzájemně disjunktních množin, který je rozkladem A a jehož třídy jsou třídy $E(a)$ ekvivalence E.

Věta 1.11

Nechť $\pi = \{B_i; i \in I\}$ je rozklad množiny $A \neq \emptyset$. Definujme relaci E_π takto:

$$\langle a,b\rangle \in E_\pi, \text{ právě když } \exists i \in I \text{ tak, že } a,b \in B_i.$$

Pak E_π je **ekvivalence** na A nazvaná **indukovaná rozkladem** π. Její třídy jsou třídy rozkladu π.

Důkaz. Jelikož π je rozklad, je pokrytím, t.j. pro každé $a \in A$ existuje $i \in I$ tak, že $a \in B_i$, t.j. $\langle a,a\rangle \in E_\pi$, tedy E_π je reflexivní. Jestliže $\langle a,b\rangle \in E_\pi$, pak $a,b \in B_i$ pro některé $i \in I$, tedy $b,a \in B_i$, t.j. $\langle b,a\rangle \in E_\pi$, neboli E_π je symetrická. Jestliže $\langle a,b\rangle \in E_\pi$, $\langle b,c\rangle \in E_\pi$, pak existují $i,j \in I$ tak, že $a,b \in B_i$, $b,c \in B_j$. Tedy $b \in B_i \cap B_j$. Ale třídy π jsou vzájemně disjunktní, tedy $B_i \cap B_j \neq \emptyset \Rightarrow B_i = B_j$, tedy $a,c \in B_i \Rightarrow \langle a,c\rangle \in E_\pi$. Tedy E_π je také tranzitivní, t.j. E_π je ekvivalence. Dále, $x \in E_\pi(a)$ právě když $\langle a,x\rangle \in E_\pi$, což je právě když $a,x \in B_i$ pro některé $i \in I$. Tedy třídy E_π jsou právě třídy rozkladu π.

Věta 1.12

Nechť $A \neq \emptyset$, nechť E je ekvivalence na A a π nechť je rozklad na A. Pak, je-li π_E rozklad indukovaný ekvivalencí E a E_{π_E} je ekvivalence indukovaná rozkladem π_E, platí $E_{\pi_E} = E$. Dále, je-li E_π ekvivalence indukovaná rozkladem π a π_{E_π} rozklad indukovaný ekvivalencí E_π, platí $\pi_{E_\pi} = \pi$.

Důkaz.

(a) $\langle x, y \rangle \in E \Leftrightarrow$ existuje třída B_i rozkladu π_E tak, že $x, y \in B_i \Leftrightarrow \langle x, y \rangle \in E_{\pi_E}$, tedy $E = E_{\pi_E}$.

(b) $B \in \pi \Leftrightarrow B$ je třídou ekvivalence $E_\pi \Leftrightarrow B \in \pi_{E_\pi}$.

Podle Vět 1.10, 1.11, 1.12 lze každému rozkladu **jednoznačně** přiřadit ekvivalenci a každé ekvivalenci lze **jednoznačně** přiřadit rozklad. Tedy ekvivalence a rozklady na množině A vzájemně korespondují. Budeme-li hovořit o ekvivalenci na A, je to totéž, jako kdybychom hovořili o indukovaném rozkladu, hovoříme-li o rozkladu, je to totéž, jako kdybychom hovořili o indukované ekvivalenci.

Obsah

Věta 1.13

Nechť $f : A \to B$ je zobrazení. Relace E_f na A definovaná předpisem:

$$\langle x, y \rangle \in E_f, \quad \text{právě když} \quad f(x) = f(y)$$

je ekvivalence, tzv. **ekvivalence indukovaná zobrazením** f.

Důkaz. $\forall a \in A$ je $f(a) = f(a)$, t.j. $\langle a, a \rangle \in E_f$, tedy E_f je reflexivní. Jestliže $\langle a, b \rangle \in E_f$, pak $f(a) = f(b)$, tedy $f(b) = f(a)$, neboli $\langle b, a \rangle \in E_f$, odkud E_f je symetrická. Jesliže $\langle a, b \rangle \in E_f$ a $\langle b, c \rangle \in E_f$, pak $f(a) = f(b)$, $f(b) = f(c)$, tedy $f(a) = f(c)$, t.j. $\langle a, c \rangle \in E_f$, tedy E_f je tranzitivní a dohromady ekvivalence.

Definice

Nechť E je ekvivalence na $A \neq \emptyset$, nechť $\pi_E = \{B_i; i \in I\}$ indukovaný rozklad (t.j. každá B_i je třídou E). Množinu π_E všech tříd E nazveme **faktorová množina** A **dle** E a označíme A/E.

Definice

Nechť E je ekvivalence na $A \neq \emptyset$. Definujme zobrazení $f_E : A \to A/E$ takto: $a \to B_i$, je-li B_i třída rozkladu π_E obsahující a. Zobrazení f_E se nazývá **kanonické zobrazení** A do A/E.

Poznamenejme, že jelikož π_E je rozklad, je zřejmě f_E skutečně zobrazení, neboť a padne právě do jediné třídy rozkladu π_E. Je zřejmé, že f_E je surjekce.

Věta 1.14

Nechť E je ekvivalence na A, f_E je kanonické zobrazení A do A/E, nechť E_{f_E} je ekvivalence, indukovaná zobrazením f_E. Pak $E_{F_E} = E$.

Důkaz. $\langle a,b\rangle \in E_{f_E} \Leftrightarrow f_E(a) = f_E(b)$, což je ekvivalentní s tím, že a,b padnou do téže třídy rozkladu π_E, t.j. do téže třídy ekvivalence E. t.j. $\langle a,b\rangle \in E$.

Věta 1.15

Nechť $f : A \to B$ je zobrazení. Pak $f = g \circ h$, kde $g : A \to A/E_f$ je kanonické zobrazení (a tedy surjekce), a $h : A/E_f \to B$ je injekce.

Důkaz. Nechť $E_f(a)$ je třída ekvivalence E_f obsahující prvek a. Jestliže $x,y \in E_f(a)$, pak $f(x) = f(y)$ a také naopak $f(x) = f(y) \Rightarrow x,y$ patří do téže třídy E_f. Tedy zobrazení $h : E_f(a) \to f(a)$ je injekce. Nechť $g : A \to A/E_f$ je kanonické zobrazení. Pak $g \circ h(a) = h(g(a)) = h(E_f(a)) = f(a)$, tudíž $f = g \circ h$.

Důsledek

Každé zobrazení $f : A \to B$ lze vyjádřit jako složené zobrazení $f = g \circ h$, kde g je surjekce a h je injekce.

Obsah

Věta 1.16

Nechť B, C jsou neprázdné množiny, $A = B \times C$. Nechť E_1, E_2 jsou relace na A definované takto:

$$\langle (x_1,x_2),(y_1,y_2)\rangle \in E_1, \quad \text{právě když} \quad x_1 = y_1,$$

$$\langle (x_1,x_2),(y_1,y_2)\rangle \in E_2, \quad \text{právě když} \quad x_2 = y_2.$$

Pak E_1, E_2 jsou ekvivalence na A a platí

$$E_1 \cap E_2 = \omega_A, \quad E_1 \circ E_2 = \iota_A = E_2 \circ E_1.$$

Důkaz. Je ihned patrné, že E_1, E_2 jsou ekvivalence. Předpokládejme $\langle (x_1,x_2),(y_1,y_2)\rangle \in E_1 \cap E_2$. Pak $x_1 = y_1$, neboť $\langle (x_1,x_2),(y_1,y_2)\rangle \in E_1$, $x_2 = y_2$, neboť $\langle (x_1,x_2),(y_1,y_2)\rangle \in E_2$, tedy $(x_1,x_2) = (y_1,y_2)$, odtud $E_1 \cap E_2 = \omega_A$. Nechť (x_1,x_2), (y_1,y_2) jsou libovolné prvky z A. Pak $\langle (x_1,x_2),(x_1,y_2)\rangle \in E_1$, $\langle (x_1,y_2),(y_1,y_2)\rangle \in E_2$ tedy $\langle (x_1,x_2),(y_1,y_2)\rangle \in E_1 \circ E_2$, t.j. $E_1 \circ E_2 = \iota_A$. Analogicky se ukáže $E_2 \circ E_1 = \iota_A$.

Věta 1.17

Nechť A je množina a E_1, E_2 jsou ekvivalence na A takové, že $E_1 \cap E_2 = \omega_A$ a $E_1 \circ E_2 = \iota_A = E_2 \circ E_1$. Pak existují množiny B, C a bijekce $f : A \to B \times C$, přičemž $B = A/E_1$, $C = A/E_2$.

Důkaz. Označme $E(a)$ třídu ekvivalence E obsahující prvek $a \in A$. Nechť E_1, E_2 jsou ekvivalence na A takové, že $E_1 \cap E_2 = \omega_A$ a $E_1 \circ E_2 = \iota_A$. Nechť f je zobrazení A do $A/E_1 \times A/E_2$, které přiřazuje $x \mapsto \langle E_1(x), E_2(x)\rangle$. Pak

(a) Nechť $x, y \in A$, $f(x) = f(y)$. Pak Tedy $E_1(x) = E_1(y)$, $E_2(x) = E_2(y)$, t.j. $\langle x, y\rangle \in E_1$, $\langle x, y\rangle \in E_2$, tedy $\langle x, y\rangle \in E_1 \cap E_2 = \omega_A$, neboli $x = y$. Tedy f je injekce.

(b) Nechť $\langle a, b\rangle \in A/E_1 \times A/E_2$. Tedy a je některá třída ekvivalence E_1, b je některá třída ekvivalence E_2. Zvolme libovolně $x \in a$, $y \in b$. Jelikož $E_1 \circ E_2 = \iota_A$, je $\langle x, y\rangle \in E_1 \circ E_2$. Tedy existuje $t \in A$ tak, že $\langle x, t\rangle \in E_1$, $\langle t, y\rangle \in E_2$, t.j. $E_1(t) = a$, $E_2(t) = b$, a tedy $f(t) = \langle E_1(t), E_2(t)\rangle = \langle a, b\rangle$, t.j. f je surjekce.

Z (a) a (b) dostáváme, že f je bijekce.

Poznámka. Na každé $A \neq \emptyset$ existují ekvivalence E_1, E_2 takové, že $E_1 \cap E_2 = \omega_A$, $E_1 \circ E_2 = \iota_A = E_2 \circ E_1$. Stačí zvolit $E_1 = \omega_A$, $E_2 = \iota_A$. Pak ale A/E_1 je bijektivní s A, A/E_2 je jednoprvková. Tento rozklad je tzv. **triviální**. Rozklad A na $B \times C$ je tzv. **netriviální**, je-li E_1, E_2 různé od ω_A, ι_A.

Příklad

$A = \{a,b,c,x,y,z\}$, E_1 má rozklad $\{\{a,x\},\{b,y\},\{c,z\}\}$, E_2 má rozklad $\{\{a,b,c\},\{x,y,z\}\}$. Ověřte $E_1 \cap E_2 = \omega_A$, $E_1 \circ E_2 = \iota_A = E_2 \circ E_1$. Pak

$$
\begin{aligned}
a &\mapsto \langle \{a,x\},\{a,b,c\} \rangle \\
b &\mapsto \langle \{b,y\},\{a,b,c\} \rangle \\
c &\mapsto \langle \{c,z\},\{a,b,c\} \rangle \\
x &\mapsto \langle \{a,x\},\{x,y,z\} \rangle \\
y &\mapsto \langle \{b,y\},\{x,y,z\} \rangle \\
z &\mapsto \langle \{c,z\},\{x,y,z\} \rangle
\end{aligned}
$$

definuje bijekci f z A na $A/E_1 \times A/E_2$, t.j. $\{\{a,x\},\{b,y\},\{c,z\}\} \times \{\{a,b,c\},\{x,y,z\}\}$.

Obsah

Nechť M je množina. Označme Exp$M$ množinu všech podmnožin množiny M. Je-li tedy M konečná a má-li n prvků, pak Exp$M$ má 2^n prvků. Je-li M prázdná, pak Exp$M$ obsahuje jedinou množinu, a to $\emptyset$, tedy $\mathrm{Exp}\emptyset = \{\emptyset\}$. Je-li M nekonečná, je zřejmě i Exp$M$ nekonečná.

Definice

Nechť A je množina a $\mathscr{M}$ neprázdný systém (některých) jejích podmnožin, t.j. $\mathscr{M} \subseteq ExpA$. $\mathscr{M}$ se nazývá **uzávěrový systém na** A, jestliže pro libovolný podsystém $\mathscr{N} \subseteq \mathscr{M}$ platí $\bigcap \mathscr{N} \in \mathscr{M}$.

Poznámka. Je-li $\mathscr{M}_1 \subseteq \mathscr{M}_2$, pak snadno ukážeme, že $\bigcap \mathscr{M}_2 \subseteq \bigcap \mathscr{M}_1$. Je-li tedy $\mathscr{N}_0$ prázdný systém množin (t.j. neobsahuje žádnou množinu), pak $\mathscr{N}_0 \subseteq \mathscr{M}$ pro každý systém podmnožin $\mathscr{M}$ množiny A, a tedy $\bigcap \mathscr{M} \subseteq \bigcap \mathscr{N}_0$. Protože průnik libovolného systému podmnožin množiny A je opět podmnožina množiny A, je tedy $\bigcap \mathscr{N}_0$ nadmnožinou libovolné podmnožiny A (včetně A). Proto zavádíme pro prázdný systém $\mathscr{N}_0$ jeho průnik takto:

$$\bigcap \mathscr{N}_0 = A.$$

Poznámka. Nechť $\mathscr{M}$ je libovolný uzávěrový systém na množině $A \neq \emptyset$. Jelikož $\mathscr{N}_0 \subseteq \mathscr{M}$ a dle definice $\bigcap \mathscr{N}_0 \in \mathscr{M}$, musí tedy $\mathscr{M}$ obsahovat množinu A.

Příklad

(1) Celá množina Exp$A$ je uzávěrový systém, neboť průnik libovolného podsystému $\mathscr{N} \subseteq ExpA$ je opět podmnožina z A, t.j. $\bigcap \mathscr{N} \in ExpA$.

(2) $\mathscr{M} = \{\emptyset, A\}$ je uzávěrový systém na A neboť $\mathscr{N} \subseteq \mathscr{M}$ je buď $\mathscr{N}$ prázdný systém, nebo $\mathscr{N} = \{\emptyset\}$, nebo $\mathscr{N} = \{A\}$ nebo $\mathscr{N} = \{\emptyset, A\}$. Průnik prázdného systému je $A \in \mathscr{M}$, pro ostatní je $\bigcap \mathscr{N} = \emptyset$ nebo $\bigcap \mathscr{N} = A$, tedy vždy $\mathscr{N} \in \mathscr{M}$.

(3) Nechť $A = B \times B$, $\mathscr{M}$ je systém všech ekvivalencí na B (t.j. ekvivalence na B je podmnožina $B \times B = A$, tedy je to systém některých podmnožin A). Ukažte, že průnik libovolné množiny ekvivalencí je opět ekvivalence.

(4) Nechť $A = \{a, b, c\}$, pak Exp$A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$. Položme $\mathscr{M} = \{\{a\}, \{a, b\}, \{a, c\}, A\}$. Snadno lze ověřit, že $\mathscr{M}$ je uzávěrový systém na A.

Definice

Nechť $\mathscr{M}$ je uzávěrový systém na A a $X \subseteq A$. Označme $[X] = \bigcap\{B \in \mathscr{M}; X \subseteq B\}$. Množinu $[X]$ nazveme **člen uzávěrového systému generovaný** X, nebo jen stručně **uzávěr** X.

Věta 1.18

Nechť $\mathscr{M}$ je uzávěrový systém na A a nechť $X, Y \subseteq A$. Pak platí:

(a) $X \subseteq [X]$

(b) $[X]$ je nejmenší (vzhledem k $\subseteq$) prvek z $\mathscr{M}$ obsahující X

(c) $[[X]] = [X]$

(d) $X \subseteq Y \Rightarrow [X] \subseteq [Y]$.

Důkaz.

(a) Dle definice je $[X]$ průnik všech množin z $\mathscr{M}$, které obsahují X, tedy i tento průnik obsahuje X.

(b) Kdyby $[X]$ nebyl nejmenší (vzhledem k $\subseteq$) prvek z $\mathscr{M}$, který obsahuje X (dle (a) obsahuje X), pak by v $\mathscr{M}$ existoval menší, t.j. $Z \in \mathscr{M}$, $X \subseteq Z$, $Z \subseteq [X]$, $Z \neq [X]$. Pak ale $Z \in \{B \in \mathscr{M}; X \subseteq B\} = \mathscr{N}$ a tedy $[X] = \bigcap \mathscr{N} \subseteq Z$, t.j. $[X] = Z$, spor.

(c) Jelikož $[X] \in \mathscr{M}$, pak $[X] \in \{B \in \mathscr{M}; X \subseteq B\}$, (dle definice uzávěru) tedy $[[X]] \subseteq [X]$. Dle (a) ovšem $[X] \subseteq [[X]]$, tedy platí (c).

(d) Je-li $X \subseteq Y$, pak $\{B \in \mathscr{M}; X \subseteq B\} \supseteq \{B \in \mathscr{M}; Y \subseteq B\}$, a tedy $[X] = \bigcap\{B \in \mathscr{M}; X \subseteq B\} \subseteq \bigcap\{B \in \mathscr{M}; Y \subseteq B\} = [Y]$.

Věta 1.19

Nechť $f : ExpA \to ExpA$ je zobrazení splňující:

(i) $X \subseteq f(X)$

(ii) $X \subseteq Y \Rightarrow f(X) \subseteq f(Y)$

(iii) $f(f(X)) = f(X)$.

Pak $\mathscr{M} = \{f(X); X \subseteq A\}$ je uzávěrový systém na A a $[X] = f(X)$.

Důkaz. Chceme dokázat, že pro každý podsystém $\mathscr{N} \subseteq \mathscr{M}$ je $\bigcap \mathscr{N} \in \mathscr{M}$. Nechť $\mathscr{N} = \{B_i; i \in I\}$, t.j. $B_i = f(X_i)$ pro některou $X_i \subseteq A$. Označme $B = \bigcap \mathscr{N}$. Pak $B \subseteq f(X_i)$ pro každé $i \in I$, tedy dle (ii) platí $f(B) \subseteq f(f(X_i)) = f(X_i)$ dle (iii), a tedy $f(B) \subseteq \bigcap\{f(X_i); i \in I\} = \bigcap \mathscr{N} = B$. Dle (i) je ale $B \subseteq f(B)$, tedy $B = f(B)$, t.j. $B \in \mathscr{M}$.

Obsah

Definice

Nechť $A \neq \emptyset$. **Binární operací na množině** A nazveme každé zobrazení $f : A \times A \to A$.

Příklad

Nechť $\mathbb{Z}$ je množina všech celých čísel, $+$ přiřadí každé dvojici čísel $a, b \in \mathbb{Z}$ číslo $a + b \in \mathbb{Z}$. Je tedy $+$ binární operace. Místo $+(a, b)$ budeme, jak je zvykem, psát $a + b$. Bude-li $\circ$ některá binární operace na A, budeme místo $\circ(a, b)$ zapisovat $a \circ b$.

Definice

Nechť $A \neq \emptyset$ a $\circ$ je binární operace na A. Dvojici $\mathscr{A} = (A, \circ)$ budeme nazývat **grupoid**. Je-li operace $\circ$ **asociativní**, t.j. jestliže $\forall a, b, c \in A$ platí $a \circ (b \circ c) = (a \circ b) \circ c$, nazývá se grupoid $(A, \circ)$ **pologrupa**. Operace $\circ$ se nazývá **komutativní**, jestliže $a \circ b = b \circ a$ pro každé $a, b \in A$.

Budeme-li operaci v grupoidu zapisovat symbolem $+$, nazýváme grupoid $(A, +)$ **aditivní**, budeme-li operaci zapisovat $\circ$ (nebo vynechávat), nazývá se grupoid $(A, \circ)$ **multiplikativní**.

Definice

Jestliže v grupoidu $(A, \circ)$ existuje prvek e takový, že $a \circ e = e \circ a = a$ pro každé $a \in A$, nazývá se e **jednotkou** $(A, \circ)$. Jestliže v A existuje prvek n takový, že $a \circ n = n \circ a = n$, nazývá se n **nula** grupoidu $(A, \circ)$.

Věta 1.20

Každý grupoid má nejvýše jednu jednotku a nejvýše jednu nulu.

Důkaz. Nechť e, f jsou jednotky v grupoidu $\mathscr{A} = (A, \circ)$. Pak $e = e \circ f = f$. Analogicky, jsou-li n, m nuly v $\mathscr{A}$, pak $n = n \circ m = m$.

Definice

Nechť $\mathscr{A} = (A, \circ)$ je grupoid, nechť $\emptyset \neq B \subseteq A$. Jestliže $\forall a, b \in B$ platí $a \circ b \in B$, nazývá se $(B, \circ)$ **podgrupoid** grupoidu $\mathscr{A}$.

Věta 1.21

Množina všech podgrupoidů daného grupoidu spolu s $\emptyset$ tvoří uzávěrový systém.

Důkaz. Nechť $Sub\mathscr{A}$ je množina všech podgrupoidů grupoidu $\mathscr{A}$ spolu s $\emptyset$. Nechť $\mathscr{N} = \{B_i; i \in I\}$ je některý systém podgrupoidů $\mathscr{A}$. Pak buď $\bigcap \mathscr{N} = \emptyset$, a tedy $\bigcap \mathscr{N} \in Sub\mathscr{A}$, nebo $\bigcap \mathscr{N} \neq \emptyset$; pak nechť $a, b \in \bigcap \mathscr{N}$, tedy $a, b \in B_i$ pro každé $i \in I$, ale B_i je podgrupoid, t.j. $a \circ b \in B_i$ pro každé $i \in I$, a tedy $a \circ b \in \bigcap \mathscr{N}$. Tedy $\bigcap \mathscr{N}$ je podgrupoid, t.j. $\bigcap \mathscr{N} \in Sub\mathscr{A}$.

Důsledek

Nechť $\mathscr{A} = (A, \circ)$ je grupoid a nechť $X \subseteq A$. Pak existuje nejmenší podgrupoid grupoidu $\mathscr{A}$ obsahující X, t.j. $[X]$. Tento grupoid $[X]$ nazveme **podgrupoid generovaný množinou** X.

Důkaz plyne přímo z Věty 1.21 a Věty 1.18.

Definice

Nechť $(A, \circ)$ je pologrupa. Jestliže pro každé dva prvky $a, b \in A$ existují $x, y \in A$ tak, že platí $a \circ x = b$, $y \circ a = b$, pak se $(A, \circ)$ nazývá **grupa**.

Definice

Je-li $(A, \circ)$ grupoid s jednotkou e, nazveme prvek $b \in A$ **prvkem inverzním k** $a \in A$, jestliže $a \circ b = b \circ a = e$.

Zřejmě, je-li a inverzní k b, je také b inverzní k a. Inverzní prvek (pokud existuje!) k prvku $a \in A$ budeme označovat a^{-1}, tedy $(a^{-1})^{-1} = a$.

Věta 1.22

Nechť $\mathscr{G} = (G, \circ)$ je grupa. Pak v $\mathscr{G}$ existuje jednotka a pro každý prvek $a \in G$ existuje prvek inverzní.

Důkaz.

(i) Nechť $a \in G$. Dle definice existují prvky $e, f \in G$ tak, že $a \circ e = a$, $f \circ a = a$. Nechť dále $x \in G$ je libovolný prvek. Dle definice existuje $y \in G$ tak, že $x = y \circ a$, tedy

$$x \circ e = (y \circ a) \circ e = y \circ (a \circ e) = y \circ a = x.$$

Analogicky lze dokázat $f \circ x = x$.

Zvolme nyní za $x = f$. Pak tedy $f \circ e = f$. Zvolme $x = e$, pak $f \circ e = e$, tedy $e = f \circ e = f$. Dohromady, v G existuje prvek e takový, že $e \circ x = x = x \circ e$ pro každé $x \in G$, t.j. e je jednotkou $\mathscr{G}$.

(ii) Z definice plyne, že pro každé $a \in G$ existují $x, y \in G$ tak, že $a \circ x = e$, $y \circ a = e$. Potom

$$x = e \circ x = (y \circ a) \circ x = y \circ (a \circ x) = y \circ e = y,$$

tedy $x = y$, t.j. $x = a^{-1}$, prvek inverzní k a.

Věta 1.23

Nechť $\mathscr{G} = (G, \circ)$ je pologrupa s jednotkou e, kde $\forall a \in G$ existuje prvek inverzní k a. Pak $\mathscr{G}$ je grupa.

Důkaz. Nechť $a, b \in G$. Položme $x = a^{-1} \circ b$, $y = b \circ a^{-1}$. Pak

$$a \circ x = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b,$$

$$y \circ a = (b \circ a^{-1}) \circ a = b \circ (a \circ a^{-1}) = b \circ e = b.$$

Dle definice, $\mathscr{G}$ je grupa.

Definice

Grupa $\mathscr{G} = (G, \circ)$ se nazývá **abelovská**, je-li komutativní, t.j. pro každé $a, b \in G$ platí $a \circ b = b \circ a$.

Poznámka. Budeme-li grupu $(G, \circ)$ zapisovat v aditivním tvaru, t.j. $(G, +)$, pak její jednotku budeme značit 0 a inverzní prvek k prvku $a \in G$ symbolem $-a$; také jej budeme nazývat **prvek opačný** k prvku a. Často místo $a + (-b)$ zapisujeme $a - b$.

Příklad

- Nechť $\mathbb{Z}$ je množina všech čísel celých. Pak $(\mathbb{Z}, +)$ je abelovská grupa s jednotkou 0.
- Nechť $\mathbb{R}^+$ je množina všech kladných reálných čísel. Pak $(\mathbb{R}^+, \cdot)$ je abelovská grupa s jednotkou 1.
- Nechť A je libovolná množina, nechť $\mathscr{P}(A)$ je množina všech permutací na A. Nechť $\circ$ označuje skládání zobrazení. Pak $(\mathscr{P}(A), \circ)$ je grupa s jednotkou id_A; pokud $|A| > 2$, pak není abelovská.

Definice

Nechť $\mathscr{G} = (G, \circ)$ je grupa. Podgrupoid $(A, \circ)$ grupoidu $(G, \circ)$ se nazývá **podgrupa grupy** $\mathscr{G}$, je-li $(A; \circ)$ grupou.

Příklad

Grupa $(\mathbb{Z}, +)$ je podgrupou grupy $(\mathbb{R}, +)$ všech reálných čísel. Poznamenejme, že podgrupoid grupy ještě nemusí být podgrupa. Např. je-li $\mathbb{N}$ množina všech přirozených čísel, je $(\mathbb{N}, +)$ podgrupoid $(\mathbb{Z}, +)$, ale $(\mathbb{N}, +)$ není grupa.

Definice

Okruhem nazveme trojici $\mathscr{R} = (R, +, \cdot)$ takovou, že $R \neq \emptyset$ je množina, $+$ a $\cdot$ jsou binární operace na R a

(i) $(R, +)$ je abelovská grupa (0 její jednotka)

(ii) $(R, \cdot)$ je pologrupa

(iii) platí **distributivní zákony**, t.j. pro každé $a, b, c \in R$ platí

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Okruh $\mathscr{R}$ se nazývá **komutativní**, jestliže $a \cdot b = b \cdot a$ pro každé $a, b \in R$. Okruh $\mathscr{R}$ se nazývá **unitární**, má-li pologrupa $(R \setminus \{0\}, \cdot)$ jednotku. Je-li $\mathscr{R}$ unitární, budeme jeho jednotku označovat 1. Prvek 0 (jednotka $(R, +)$) se nazývá **nulou okruhu** $\mathscr{R}$.

Příklad

Komutativní unitární okruhy jsou například: okruh celých čísel $(\mathbb{Z}, +, \cdot)$, okruh reálných čísel $(\mathbb{R}, +, \cdot)$, okruh komplexních čísel $(\mathbb{C}, +, \cdot)$ a okruh racionálních čísel $(\mathbb{Q}, +, \cdot)$.

Poznámka. Název nula okruhu pro prvek 0 je oprávněný, neboť je nulou pologrupy $(R, \cdot)$, což snadno ověříme. Totiž, dle distributivních zákonů platí $\forall a \in R$:

$$a \cdot a = a \cdot (a + 0) = a \cdot a + a \cdot 0,$$

$$a \cdot a = (a + 0) \cdot a = a \cdot a + 0 \cdot a,$$

avšak $(R, +)$ je grupa, tedy $a \cdot 0 = 0 = 0 \cdot a$.

Definice

Prvek a okruhu $\mathscr{R} = (R, +, \cdot)$ se nazývá **dělitel nuly**, jestliže $a \neq 0$ a existuje $b \neq 0$, $b \in R$ tak, že $a \cdot b = 0$.

Příklad

Nechť A je množina všech funkcí jedné reálné proměnné na intervalu $[0,1]$, nechť $+$ a $\cdot$ je sčítání respektive násobení funkcí. Pak $\mathscr{A} = (A; +, \cdot)$ je komutativní unitární okruh (jednotkou je konstantní funkce $f(x) = 1$). Tento okruh má dělitele 0: nechť $g(x)$ je funkce: $g(x) = 0$ pro $x \in [0, \frac{1}{2}]$, $g(x) \neq 0$ pro $x \in (\frac{1}{2}, 1]$. Nechť $h(x)$ je funkce: $h(x) \neq 0$ pro $x \in [0, \frac{1}{2}]$, $h(x) = 0$ pro $x \in (\frac{1}{2}, 1]$. Pak $g(x)$ i $h(x)$ jsou nenulové, ale $g(x) \cdot h(x)$ je nulová funkce na $[0,1]$.

Definice

Okruh $\mathscr{R} = (R, +, \cdot)$ se nazývá **obor integrity**, je-li komutativní, unitární a neobsahuje-li dělitele nuly.

Příklad

Každý z okruhů $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ je obor integrity.

Definice

Okruh $\mathscr{R} = (R, +, \cdot)$ se nazývá **těleso**, je-li množina jeho nenulových prvků grupou vzhledem k operaci $\cdot$. Těleso $\mathscr{R}$ se nazývá **komutativní**, je-li $(R \setminus \{0\}, \cdot)$ abelovská grupa.

Příklad

Okruhy $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou komutativní tělesa.
Okruh $(\mathbb{Z}, +, \cdot)$ není těleso.

Věta 1.24

Každé komutativní těleso je obor integrity.

Důkaz. Zřejmě stačí dokázat, že komutativní těleso $\mathscr{R} = (R, +, \cdot)$ má jednotku a neobsahuje dělitele 0. Avšak, je-li R těleso, je $(R \setminus \{0\}, \cdot)$ grupa, ta má jednotku 1, což je zřejmě jednotkou okruhu $\mathscr{R}$. Dále, nechť $a, b \in R, a \neq 0 \neq b$. Pak $a, b \in R \setminus \{0\}$, to je ale grupa, tedy $a \cdot b \in R \setminus \{0\}$, a tedy $a \cdot b \neq 0$.

Definice

Je-li $\mathscr{R} = (R, +, \cdot)$ okruh, $A \subseteq R$ taková, že $(A, +, \cdot)$ je opět okruh, pak se $(A, +, \cdot)$ nazývá **podokruh okruhu** $\mathscr{R}$. Je-li $\mathscr{R}$ těleso, $A \subseteq R$ taková, že $(A, +, \cdot)$ je opět těleso, pak $(A, +, \cdot)$ nazveme **podtěleso tělesa** R. Každé podtěleso tělesa $\mathscr{C} = (C, +, \cdot)$ komplexních čísel nazveme **číselné těleso**. Každý podokruh okruhu $\mathscr{C}$ nazveme **číselný okruh**.

Příklad

$\mathscr{C} = (\mathbb{C}, +, \cdot)$, $\mathscr{R} = (\mathbb{R}, +, \cdot)$, $\mathscr{Q} = (\mathbb{Q}, +, \cdot)$ jsou číselná tělesa, $\mathscr{Z} = (\mathbb{Z}, +, \cdot)$ je číselný okruh, který není tělesem.

Obsah

Mějme dán okruh $\mathscr{R} = (R, +, \cdot)$.
Jak jsme již ukázali, $\forall a \in R$ platí $a \cdot 0 = 0 = 0 \cdot a$.
Ověříme, že $\forall a, b \in R$ platí $a \cdot (-b) = (-a) \cdot b = -a \cdot b$.
Totiž, $a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0 = 0$, odkud
$a \cdot (-b) = -a \cdot b$, analogicky se dá ukázat, že $(-a) \cdot b = -a \cdot b$.
V unitárním okruhu navíc $\forall a \in R$ platí $a \cdot (-1) = (-1) \cdot a = -a$.

Nechť $\mathscr{R} = (R, +\cdot)$ je komutativní okruh. Jelikož $(R, +)$ je grupa (je tedy asociativní), nemusíme součty ve tvaru $a_1 + a_2 + a_3 + \cdots + a_n$ závorkovat. Jsou-li $a_1, \ldots, a_n \in R$ budeme používat tzv. **sumační symbol**

$$a_1 + a_2 + a_3 + \cdots + a_n = \sum_{i=1}^{n} a_i.$$

Číslo i nazveme **součtový index**.

Snadno lze (použitím asociativního a komutativního zákona a distributivních zákonů) ověřit platnost následujících pravidel:

(i) $\sum_{i=1}^{m} a_i + \sum_{i=m+1}^{n} a_i = \sum_{i=1}^{n} a_i$

(ii) $\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (a_i + b_i)$

(iii) $c \cdot \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} c \cdot a_i$

(iv) $(\sum_{i=1}^{m} a_i) \cdot (\sum_{i=1}^{n} b_j) = \sum_{i=1}^{m} (a_i \cdot \sum_{j=1}^{n} b_j) = \sum_{i=1}^{m} (\sum_{j=1}^{n} a_i \cdot b_j)$

(v) $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij}$.

Obsah

Definice

Nechť $A \neq \emptyset \neq B$ jsou množiny. Zobrazení $\circ : A \times B \to B$ nazveme **levá vnější operace nad množinami** A, B (v tomto pořadí). Jsou-li $a \in A$, $b \in B$, pak prvek $\circ(a,b)$ budeme zapisovat $a \circ b$.

Definice

Nechť $(V,+)$ je abelovská grupa, nechť T je (číselné) těleso, nechť $\circ : T \times V \to V$ je levá vnější operace nad T, V. Pak čtveřici $\mathscr{V} = (V,+,T,\circ)$ nazveme **vektorový prostor nad** T, platí-li $\forall \mathbf{u}, \mathbf{v} \in V$, $\forall c, d \in T$

(i) $c \circ (\mathbf{u} + \mathbf{v}) = c \circ \mathbf{u} + c \circ \mathbf{v}$

(ii) $(c + d) \circ \mathbf{u} = c \circ \mathbf{u} + d \circ \mathbf{u}$

(iii) $(c \cdot d) \circ \mathbf{u} = c \circ (d \circ \mathbf{u})$

(iv) $1 \circ \mathbf{u} = \mathbf{u}$.

Prvky z V budeme nazývat **vektory**, čísla z tělesa T **skaláry**. Množinu V nazveme **pole** vektorového prostoru $\mathscr{V}$.

Poznámka. Protože není nebezpečí nedorozumění, budeme operaci v grupě $(V,+)$ i sčítání v tělese T označovat stejným symbolem „$+$“. Také levou vnější operaci ve $\mathscr{V}$ budeme označovat shodně jako násobení v T a budeme ji nazývat **násobení vektoru skalárem**.

Příklady

- Každé těleso T je vektorovým prostorem samo nad sebou. Sčítání vektorů definujeme jako sčítání prvků tělesa T a násobení vektorů skaláry jako násobení prvků tělesa T s prvky tělesa T.
- Nechť V je množina všech funkcí jedné reálné proměnné na intervalu $[a,b]$, $+$ je operace sčítání funkcí, kde $(f+g)(x)=f(x)+g(x)$. Nechť dále $\cdot$ je levá vnější operace násobení funkce reálným číslem. Pak $(V,+,\mathbb{R},\cdot)$ je vektorový prostor nad $\mathbb{R}$.
- Množina $P(T)$ všech polynomů s koeficienty z tělesa T je spolu s obvyklými operacemi sčítání polynomů a násobení prvkem z T vektorový prostor nad T.

Definice

Nechť $\mathscr{V}$ je vektorový prostor nad tělesem T, nechť $\mathbf{v}, \mathbf{u}_1, \ldots, \mathbf{u}_k \in V$. Řekneme, že vektor $\mathbf{v}$ je **lineární kombinací vektorů** $\mathbf{u}_1, \ldots, \mathbf{u}_k$, jestliže existují čísla $c_1, \ldots, c_k \in T$ tak, že

$$\mathbf{v} = c_1 \cdot \mathbf{u}_1 + \cdots + c_k \cdot \mathbf{u}_k.$$

Poznámka. Symbolem $\mathbf{o}$ budeme označovat tzv. **nulový vektor**, což je jednotka grupy $(V, +)$. Použitím podmínky (ii) dostaneme $\forall \mathbf{u} \in V$:

$$0 \cdot \mathbf{u} = (c + (-c)) \cdot \mathbf{u} = c \cdot \mathbf{u} + (-c \cdot \mathbf{u}) = \mathbf{o}.$$

Tedy nulový vektor je lineární kombinací libovolných vektorů z V: je-li $\mathbf{u}_1, \ldots, \mathbf{u}_k \in V$, pak

$$0 \cdot \mathbf{u}_1 + \cdots + 0 \cdot \mathbf{u}_k = \mathbf{o}.$$

Definice

Vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$ z vektorového prostoru $\mathscr{V}$ se nazývají **lineárně závislé**, jestliže existují čísla $c_1, \ldots, c_k \in T$, která nejsou všechna rovna nule tak, že nulový vektor $\mathbf{o}$ je roven netriviální lineární kombinaci vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_k$, t.j.

$$\mathbf{o} = c_1 \cdot \mathbf{u}_1 + \cdots + c_k \cdot \mathbf{u}_k,$$

kde aspoň jedno $c_i \neq 0$. Jestliže vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$ nejsou lineárně závislé, nazývají se **lineárně nezávislé**.

Poznámka. Zřejmě vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k \in \mathscr{V}$ jsou lineárně nezávislé, právě když

$$\mathbf{o} = c_1 \cdot \mathbf{u}_1 + \cdots + c_k \cdot \mathbf{u}_k \quad \Rightarrow \quad c_1 = c_2 = \cdots = c_k = 0.$$

Poznámka. Jeden vektor $\mathbf{u} \in \mathscr{V}$ je lineárně nezávislý, právě když $\mathbf{u} \neq \mathbf{o}$. Nulový vektor $\mathbf{o}$ je totiž lineárně závislý, neboť $\mathbf{o} = c \cdot \mathbf{o}$ pro každé $c \in T$, $c \neq 0$; dle (i), (ii), (iii): $c \cdot \mathbf{o} = c \cdot (0 \cdot \mathbf{u}) = (c \cdot 0) \cdot \mathbf{u} = 0 \cdot \mathbf{u} = (c + (-c)) \cdot \mathbf{u} = (c \cdot \mathbf{u}) + (-c \cdot \mathbf{u}) = \mathbf{o}$.

Věta 2.1

Jsou-li mezi vektory $\mathbf{u}_1, \ldots, \mathbf{u}_m \in \mathscr{V}$ některé lineárně závislé, pak jsou $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárně závislé.

Důkaz. Předpokládejme, že $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně závislé pro $k < m$ (jsou-li to jiné vektory, zaměníme pořadí). Pak existují $c_1, \ldots, c_k \in T$ tak, že

$$\mathbf{o} = c_1 \cdot \mathbf{u}_1 + \cdots + c_k \cdot \mathbf{u}_k,$$

kde $c_i \neq 0$ aspoň pro jedno $i \in \{1, \ldots, k\}$. Pak ale platí

$$\mathbf{o} = c_1 \cdot \mathbf{u}_1 + \cdots + c_k \cdot \mathbf{u}_k + 0 \cdot \mathbf{u}_{k+1} + \cdots + 0 \cdot \mathbf{u}_m,$$

kde aspoň jedno $c_i \neq 0$, tedy $\mathbf{u}_1, \ldots, \mathbf{u}_m$ jsou lineárně závislé.

Důsledek 1

Je-li mezi vektory $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektor nulový $\mathbf{o}$, pak jsou $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárně závislé.

Důsledek 2

Jsou-li vektory $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárně nezávislé a je-li $\{\mathbf{u}_{j_1}, \ldots, \mathbf{u}_{j_k}\} \subseteq \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$, pak jsou $\mathbf{u}_{j_1}, \ldots, \mathbf{u}_{j_k}$ opět lineárně nezávislé.

Věta 2.2

Nechť $\mathbf{u}_1, \ldots, \mathbf{u}_k \in \mathscr{V}$. Pak $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně závislé, právě když je aspoň jeden z nich lineární kombinací ostatních vektorů.

Důkaz.

(a) Nechť $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně závislé. Pak existují $c_1, \ldots, c_k \in T$ tak, že $c_1 \cdot \mathbf{u}_1 + \cdots + c_k \cdot \mathbf{u}_k = \mathbf{o}$ a existuje $j \in \{1, \ldots, k\}$ tak, že $c_j \neq 0$. Pak ale

$$\mathbf{u}_j = (-\frac{c_1}{c_j}) \cdot \mathbf{u}_1 + \cdots + (-\frac{c_{j-1}}{c_j}) \cdot \mathbf{u}_{j-1} + (-\frac{c_{j+1}}{c_j}) \cdot \mathbf{u}_{j+1} + \cdots + (-\frac{c_k}{c_j}) \cdot \mathbf{u}_k,$$

tedy $\mathbf{u}_j$ je lineární kombinací ostatních vektorů.

(b) Je-li $\mathbf{u}_j$ lineární kombinací vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_{j-1}, \mathbf{u}_{j+1}, \ldots, \mathbf{u}_k$, pak existují $c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_k \in T$ tak, že $\mathbf{u}_j = c_1 \cdot \mathbf{u}_1 + \cdots + c_{j-1} \cdot \mathbf{u}_{j-1} + c_{j+1} \cdot \mathbf{u}_{j+1} + \cdots + c_k \cdot \mathbf{u}_k$, odkud $\mathbf{o} = c_1 \cdot \mathbf{u}_1 + \cdots + c_{j-1} \cdot \mathbf{u}_{j-1} + (-1)\mathbf{u}_j + c_{j+1} \cdot \mathbf{u}_{j+1} + \cdots + c_k \cdot \mathbf{u}_k$, t.j. $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně závislé.

Definice

Nechť $\mathscr{V} = (V, +, T, \cdot)$ je vektorový prostor nad tělesem T, nechť $\emptyset \neq W \subseteq V$. Pak $\mathscr{W} = (W, +, T, \cdot)$ nazveme **podprostor vektorového prostoru** $\mathscr{V}$, jestliže

(i) $\forall \mathbf{u}, \mathbf{v} \in W$ je $\mathbf{u} + \mathbf{v} \in W$

(ii) $\forall \mathbf{u} \in W, \forall c \in T$ je $c \cdot \mathbf{u} \in W$.

Poznámka. Je-li $\mathscr{W}$ podprostor $\mathscr{V}$, $\mathbf{o}$ nulový vektor ve $\mathscr{V}$, pak zřejmě $\mathbf{o} \in \mathscr{W}$, neboť W je neprázdná, t.j. existuje $\mathbf{u} \in W$, dle (ii) ale $c \cdot \mathbf{u} \in W$, $(-c) \cdot \mathbf{u} \in W$, dle (i) pak $c \cdot \mathbf{u} + (-c) \cdot \mathbf{u} = (c + (-c)) \cdot \mathbf{u} = 0 \cdot \mathbf{u} = \mathbf{o} \in W$.

Příklady

(a) Je-li $\mathscr{V}$ vektorový prostor, pak $\mathscr{V}$ je podprostor $\mathscr{V}$, také $\{\mathbf{o}\}$ je podprostor $\mathscr{V}$.

(b) Je-li $\mathscr{V}$ vektorový prostor všech funkcí reálné proměnné na intervalu $[a, b]$, pak např. množina všech funkcí z V splňujících $f(a) = 0$ je podprostor $\mathscr{V}$.

Věta 2.3

Neprázdná podmnožina W vektorového prostoru $\mathscr{V}$ je polem podprostoru $\mathscr{W}$, právě když s každými prvky $\mathbf{u}_1, \ldots, \mathbf{u}_k$ obsahuje i jejich lineární kombinaci.

Důkaz. Jestliže $\mathbf{u}_1, \ldots, \mathbf{u}_k \in W$, pak dle (ii) také $c_1 \cdot \mathbf{u}_1, \ldots, c_k \cdot \mathbf{u}_k \in W$ pro libovolné $c_1, \ldots, c_k \in T$ a dle (i) tedy i $c_1 \cdot \mathbf{u}_1 + c_2 \cdot \mathbf{u}_2 \in W$, tedy i $c_1 \cdot \mathbf{u}_1 + c_2 \cdot \mathbf{u}_2 + c_3 \cdot \mathbf{u}_3 \in W$ atd. až $c_1 \cdot \mathbf{u}_1 + \cdots + c_k \cdot \mathbf{u}_k \in W$.
Obráceně, jestliže W obsahuje s každými $\mathbf{u}_1, \ldots, \mathbf{u}_k$ i jejich lineární kombinaci, pak pro $\mathbf{u}, \mathbf{v} \in W$ a $c \in T$ zřejmě i $\mathbf{u} + \mathbf{v} \in W$, $c \cdot \mathbf{u} \in W$, tedy dle (i), (ii) je W polem prostoru $\mathscr{V}$.

Věta 2.4

Podprostory vektorového prostoru $\mathscr{V}$ tvoří uzávěrový systém, t.j. je-li $\{\mathscr{W}_\gamma; \gamma \in \Gamma\}$ některý podsystém podprostorů $\mathscr{V}$, pak i $\mathscr{W} = \bigcap\{\mathscr{W}_\gamma; \gamma \in \Gamma\}$ je podprostor $\mathscr{V}$.

Důkaz. Nechť $W = \bigcap\{W_\gamma; \gamma \in \Gamma\}$ a nechť $\mathbf{u}, \mathbf{v} \in W$, $c \in T$. Pak $\mathbf{u}, \mathbf{v} \in W_\gamma$ pro každé $\gamma \in \Gamma$, ale W_γ je podprostor $\mathscr{V}$, tedy i $\mathbf{u} + \mathbf{v} \in W_\gamma$, $c \cdot \mathbf{u} \in W_\gamma$ pro každé $\gamma \in \Gamma$, a odtud $\mathbf{u} + \mathbf{v} \in W, c \cdot \mathbf{u} \in W$, t.j. W splňuje (i), (ii), je tedy (polem) podprostoru $\mathscr{V}$.

Poznámka. Vzhledem k $\subseteq$ je $\{\mathbf{o}\}$ nejmenší a $\mathscr{V}$ největší podprostor $\mathscr{V}$. Je-li $A \subseteq V$, pak existuje nejmenší podprostor prostoru $\mathscr{V}$ obsahující A, t.j. **podprostor** $[A]$ **generovaný množinou** A. Je-li $A = \emptyset$, pak zřejmě $[\emptyset] = \{\mathbf{o}\}$.

Definice

Nechť M je podmnožina vektorového prostoru $\mathscr{V}$. **Lineárním obalem množiny M ve $\mathscr{V}$** rozumíme množinu všech lineárních kombinací vektorů z M.

Věta 2.5

Nechť $M \neq \emptyset$ je podmnožina vektorového prostoru $\mathscr{V}$. Pak lineární obal M je právě podprostor $[M]$ generovaný M.

Důkaz. Nechť $L(M)$ je lineární obal M. Pak zřejmě $M \subseteq L(M)$. Dle Věty 2.3 je $L(M)$ podprostor $\mathscr{V}$, tedy $[M] \subseteq L(M)$.
Obráceně, nechť $\mathbf{u} \in L(M)$. Pak dle definice existují $\mathbf{u}_1, \ldots, \mathbf{u}_k \in M$ a $c_1, \ldots, c_k \in T$ tak, že $\mathbf{u} = c_1 \cdot \mathbf{u}_1 + \cdots + c_k \cdot \mathbf{u}_k$. Tedy $\mathbf{u}$ padne do každého podprostoru prostoru $\mathscr{V}$ obsahujícího M, tedy i do jejich průniku, t.j. $\mathbf{u} \in [M]$, neboli $L(M) \subseteq [M]$. Dokázali jsme $[M] = L(M)$.

Poznámka. Jsou-li tedy $\mathscr{W}_1, \mathscr{W}_2$ podprostory vektorového prostoru $\mathscr{V}$, pak nejmenší podprostor, obsahující současně $\mathscr{W}_1$ a $\mathscr{W}_2$ je dle Věty 2.5 lineárním obalem množiny $W_1 \cup W_2$. Následující věta ukazuje, že tento podprostor lze vyjádřit i jednodušeji.

Věta 2.6

Jsou-li $\mathscr{W}_1, \mathscr{W}_2$ podprostory vektorového prostoru $\mathscr{V}$, pak polem nejmenšího podprostoru, obsahujícího $\mathscr{W}_1$ a $\mathscr{W}_2$ je množina $W_1 + W_2 = \{\mathbf{v} \in V; \mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2, \text{ kde } \mathbf{v}_1 \in W_1, \mathbf{v}_2 \in W_2\}$.

Důkaz. Dle Věty 2.5 je zřejmé, že $W_1 + W_2 \subseteq [W_1 \cup W_2]$. Dále, pro libovolné $\mathbf{v}_1 \in W_1$ platí $\mathbf{v}_1 = \mathbf{v}_1 + \mathbf{o}$, ale $\mathbf{o} \in W_2$, tedy $\mathbf{v}_1 \in W_1 + W_2$, t.j. $W_1 \subseteq W_1 + W_2$. Analogicky se ověří $W_2 \subseteq W_1 + W_2$.
Stačí tedy dokázat, že $W_1 + W_2$ je polem podprostoru prostoru $\mathscr{V}$.
Nechť $\mathbf{u}, \mathbf{v} \in W_1 + W_2$, $c \in T$. Pak existují $\mathbf{u}_1, \mathbf{v}_1 \in W_1$, $\mathbf{u}_2, \mathbf{v}_2 \in W_2$ tak, že $\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2$, $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$. Jelikož grupa $(V, +)$ je komutativní, platí $\mathbf{u} + \mathbf{v} = (\mathbf{u}_1 + \mathbf{u}_2) + (\mathbf{v}_1 + \mathbf{v}_2) = (\mathbf{u}_1 + \mathbf{v}_1) + (\mathbf{u}_2 + \mathbf{v}_2)$. Dle definice ale $\mathbf{u}_1 + \mathbf{v}_1 \in W_1$, $\mathbf{u}_2 + \mathbf{v}_2 \in W_2$, tedy $\mathbf{u} + \mathbf{v} \in W_1 + W_2$.
Dále, $c \cdot \mathbf{u} = c \cdot (\mathbf{u}_1 + \mathbf{u}_2) = c \cdot \mathbf{u}_1 + c \cdot \mathbf{u}_2$, avšak $c \cdot \mathbf{u}_1 \in W_1$, $c \cdot \mathbf{u}_2 \in W_2$, tedy $c \cdot \mathbf{u} \in W_1 + W_2$, t.j. $W_1 + W_2$ je polem podprostoru (obsahujícího W_1, W_2), tedy $[W_1 \cup W_2] \subseteq W_1 + W_2$.

Definice

Nechť $\mathscr{V}$ je vektorový prostor, $\mathscr{W}_1, \mathscr{W}_2$ jeho podprostory. Podprostor $\mathscr{W}_1 + \mathscr{W}_2$, jehož pole je množina $W_1 + W_2$ nazveme **součet podprostorů** $\mathscr{W}_1, \mathscr{W}_2$. Je-li navíc $\mathscr{W}_1 \cap \mathscr{W}_2 = \{\mathbf{o}\}$, nazveme $\mathscr{W}_1 + \mathscr{W}_2$ **přímý součet podprostorů** $\mathscr{W}_1, \mathscr{W}_2$.

Věta 2.7

Je-li vektorový prostor $\mathscr{V}$ přímý součet podprostorů $\mathscr{W}_1, \mathscr{W}_2$, pak každý vektor $\mathbf{v} \in \mathscr{V}$ lze vyjádřit jediným způsobem ve tvaru $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$, kde $\mathbf{v}_1 \in \mathscr{W}_1$, $\mathbf{v}_2 \in \mathscr{W}_2$.

Důkaz. Dle Věty 2.6 lze $\mathbf{v} \in \mathscr{V}$ vyjádřit aspoň jedním způsobem ve tvaru $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$, $\mathbf{v}_1 \in \mathscr{W}_1$, $\mathbf{v}_2 \in \mathscr{W}_2$. Předpokládejme, že $\mathbf{v} = \mathbf{u}_1 + \mathbf{u}_2$, $\mathbf{u}_1 \in \mathscr{W}_1$, $\mathbf{u}_2 \in \mathscr{W}_2$. Pak $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{u}_1 + \mathbf{u}_2$, a tedy $\mathbf{v}_1 - \mathbf{u}_1 = \mathbf{u}_2 - \mathbf{v}_2$, t.j. $\mathbf{v}_1 - \mathbf{u}_1$ i $\mathbf{u}_2 - \mathbf{v}_2$ patří do téhož podprostoru. Avšak $\mathbf{v}_1 - \mathbf{u}_1 \in \mathscr{W}_1$, $\mathbf{u}_2 - \mathbf{v}_2 \in \mathscr{W}_2$, tedy $\mathbf{v}_1 - \mathbf{u}_1 \in W_1 \cap W_2 = \{\mathbf{o}\}$, analogicky $\mathbf{u}_2 - \mathbf{v}_2 \in W_1 \cap W_2 = \{\mathbf{o}\}$, tedy $\mathbf{v}_1 = \mathbf{u}_1$, $\mathbf{u}_2 = \mathbf{v}_2$. Neboli vyjádření $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$ je jednoznačné.

Definice

Nechť $\mathscr{V}$ je vektorový prostor, $M \neq \emptyset$ jeho podmnožina. Je-li $[M] = \mathscr{V}$, nazývá se M **množina generátorů** $\mathscr{V}$.

Poznámka. Dle Věty 2.5 je tedy každý vektor z $\mathscr{V}$ lineární kombinací generátorů. Zřejmě má každý vektorový prostor množinu generátorů, např. $M = V$.

Definice

Řekneme, že vektorový prostor $\mathscr{V}$ je **konečné dimenze**, má-li aspoň jednu konečnou množinu generátorů.

Definice

Bází vektorového prostoru $\mathscr{V}$ konečné dimenze rozumíme libovolnou lineárně nezávislou konečnou množinu $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ jeho generátorů.

Věta 2.8

Nechť $M = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ je bází $\mathscr{V}$. Pak každý vektor $\mathbf{v} \in \mathscr{V}$ lze jediným způsobem vyjádřit jako lineární kombinaci vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_n$.

Důkaz. Protože M je množinou generátorů, lze dle Věty 2.5 každý $\mathbf{v} \in \mathscr{V}$ zapsat ve tvaru

$$\mathbf{v} = c_1 \cdot \mathbf{u}_1 + \cdots + c_n \cdot \mathbf{u}_n = \sum_{i=1}^{n} c_i \mathbf{u}_i .$$

Jestliže

$$\mathbf{v} = d_1 \cdot \mathbf{u}_1 + \cdots + d_n \cdot \mathbf{u}_n = \sum_{i=1}^{n} d_i \mathbf{u}_i ,$$

pak

$$\mathbf{o} = \mathbf{v} - \mathbf{v} = \sum_{i=1}^{n} c_i \mathbf{u}_i - \sum_{i=1}^{n} d_i \mathbf{u}_i = \sum_{i=1}^{n} (c_i - d_i) \mathbf{u}_i .$$

Jelikož $\mathbf{u}_1, \ldots, \mathbf{u}_n$ jsou lineárně nezávislé, je $c_i - d_i = 0$ pro $i = 1, \ldots, n$, odkud $c_1 = d_1, \ldots, c_n = d_n$.

Příklad

Nechť $\mathscr{V}$ je množina všech čtveřic $\mathbf{a} = (a_1, a_2, a_3, a_4)$ reálných čísel. Položme

$$\begin{aligned} \mathbf{a} + \mathbf{b} &= (a_1, a_2, a_3, a_4) + (b_1, b_2, b_3, b_4) \\ &= (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4), \\ c \cdot \mathbf{a} &= (c \cdot a_1, c \cdot a_2, c \cdot a_3, c \cdot a_4), \end{aligned}$$

tedy $\mathscr{V}$ je vektorový prostor nad tělesem reálných čísel. Zřejmě $\mathbf{e}_1 = (1,0,0,0)$, $\mathbf{e}_2 = (0,1,0,0)$, $\mathbf{e}_3 = (0,0,1,0)$, $\mathbf{e}_4 = (0,0,0,1)$ tvoří jeho bázi, neboť

$$\mathbf{a} = (a_1, a_2, a_3, a_4) = a_1 \cdot \mathbf{e}_1 + a_2 \cdot \mathbf{e}_2 + a_3 \cdot \mathbf{e}_3 + a_4 \cdot \mathbf{e}_4.$$

Tato báze zřejmě není jediná, bází je v tomto prostoru nekonečně mnoho.

Věta 2.9

Je-li $M = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ množina generátorů vektorového prostoru $\mathscr{V}$, pak existuje $M' \subseteq M$ tak, že M' je bází $\mathscr{V}$.

Důkaz. Není-li M, kde $[M] = \mathscr{V}$, přímo bází $\mathscr{V}$, pak jsou vektory $\mathbf{u}_1, \ldots, \mathbf{u}_n$ lineárně závislé, a dle Věty 2.2 existuje aspoň jeden $\mathbf{u}_i \in M$, který je lineární kombinací ostatních. Tedy můžeme $\mathbf{u}_i$ vynechat, neboť $M_1 = M \setminus \{\mathbf{u}_i\}$ opět generuje $\mathscr{V}$. Je-li nyní M_1 lineárně nezávislá, je bází. Není-li M_1 lineárně nezávislá, lze opět jeden vektor vynechat, obdržíme M_2 a tak dále. Po konečném počtu kroků (neboť M je konečná), obdržíme lineárně nezávislou $M' \subseteq M$, která generuje $\mathscr{V}$, t.j. M' je báze $\mathscr{V}$.

Věta 2.10 (Steinitzova věta o výměně bazí)

Nechť $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ je množina generátorů vektorového prostoru $\mathscr{V} \neq \{\mathbf{o}\}$ a nechť $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ jsou lineárně nezávislé vektory z $\mathscr{V}$. Pak $k \leq n$ a při vhodném očíslování vektorů $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ je množina $\{\mathbf{v}_1, \ldots, \mathbf{v}_k, \mathbf{u}_{k+1}, \ldots, \mathbf{u}_n\}$ opět množinou generátorů $\mathscr{V}$.

Důkaz. Indukcí dle počtu k vektorů $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$.

(a) Nechť $k = 1$. Jelikož $\mathbf{v}_1$ je lineárně nezávislý, je $\mathbf{v}_1 \neq \mathbf{o}$. Dle předpokladu je $[\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}] = \mathscr{V}$, ale $\mathbf{v}_1 \in \mathscr{V}$, tedy dle Věty 2.5 existují skaláry $c_1, \ldots, c_n \in T$ tak, že

$$\mathbf{v}_1 = \sum_{i=1}^{n} c_i \mathbf{u}_i,$$

přičemž aspoň jeden $c_i \neq 0$ (jinak by $\mathbf{v}_1 = \mathbf{o}$). Předpokládejme např. $c_1 \neq 0$ (jinak bychom $\mathbf{u}_1, \ldots, \mathbf{u}_n$ přečíslovali). Pak platí

$$\mathbf{u}_1 = \frac{1}{c_1}\mathbf{v}_1 - \sum_{j=2}^{n} \frac{c_j}{c_1}\mathbf{u}_j,$$

odkud zřejmě $[\{\mathbf{v}_1, \mathbf{u}_2 \ldots, \mathbf{u}_n\}] = \mathscr{V}$. Přitom $1 \leq n$.

(b) Nechť $k > 1$ a předpokládejme, že tvrzení platí pro všechna čísla $1, \ldots, k-1$. Jelikož $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ jsou lineárně nezávislé, jsou dle Důsledku 2 (Věty 2.1) také $\{\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}\}$ lineárně nezávislé. Dle indukčního předpokladu platí $k-1 \leq n$ a po vhodném očíslování $\mathbf{u}_1, \ldots, \mathbf{u}_n$ je $\{\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}, \mathbf{u}_k, \ldots, \mathbf{u}_n\}$ množinou generátorů $\mathscr{V}$. Tedy existují $c_1, \ldots, c_{k-1}, d_k, \ldots, d_n \in T$ tak, že

$$\mathbf{v}_k = \sum_{i=1}^{k-1} c_i \mathbf{v}_i + \sum_{j=k}^{n} d_j \mathbf{u}_j, \qquad (*)$$

přičemž aspoň jeden ze skalárů $d_k, \ldots, d_n$ je nenulový (jinak by $\mathbf{v}_k = \sum_{i=1}^{k-1} c_i \mathbf{v}_i$, spor s lineární nezávislostí $\mathbf{v}_1, \ldots, \mathbf{v}_k$). Očíslujme $\mathbf{u}_k, \ldots, \mathbf{u}_n$ vhodně tak, aby $d_k \neq 0$. Pak z $(*)$ vyplývá $k \leq n$ a

$$\mathbf{u}_k = -\sum_{i=1}^{k-1} \frac{c_i}{d_k} \mathbf{v}_i + \frac{1}{d_k} \mathbf{v}_k - \sum_{j=k+1}^{n} \frac{d_j}{d_k} \mathbf{u}_j,$$

tedy $[\{\mathbf{v}_1, \ldots, \mathbf{v}_k, \mathbf{u}_{k+1}, \ldots, \mathbf{u}_n\}] = \mathscr{V}$.

Indukcí jsme dokázali tvrzení pro každé k.

Důsledek 1

Nechť $\mathscr{V} \neq \{\mathbf{o}\}$ je vektorový prostor konečné dimenze. Pak každé jeho dvě báze mají stejný počet prvků.

Důkaz. Jsou-li $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$, $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ dvě báze $\mathscr{V}$, pak dle Steinitzovy věty $k \leq n$ a $n \leq k$, t.j. $n = k$.

Definice

Je-li $\mathscr{V} \neq \{\mathbf{o}\}$ vektorový prostor konečné dimenze, pak počet prvků jeho libovolné báze nazýváme **dimenze** $\mathscr{V}$ a značíme $\dim\mathscr{V}$. Je-li $\mathscr{V} = \{\mathbf{o}\}$, položíme $\dim\mathscr{V} = 0$.

Důsledek 2

Nechť $[\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}] = \mathscr{V}$, nechť $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathscr{V}$. Je-li $k > n$, jsou $\mathbf{v}_1, \ldots, \mathbf{v}_k$ lineárně závislé.

Důkaz. Kdyby $\mathbf{v}_1, \ldots, \mathbf{v}_k$ byly lineárně nezávislé, muselo by dle Steinitzovy věty platit $k \leq n$.

Důsledek 3

Nechť $[\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}] = \mathscr{V}$, pak $\dim \mathscr{V} \leq n$.

Důkaz. Plyne přímo ze Steinitzovy věty a z definice dimenze.

Věta 2.11

Nechť $\dim \mathscr{V} = n$, nechť $\mathbf{u}_1, \ldots, \mathbf{u}_n \in \mathscr{V}$. Pak následující podmínky jsou ekvivalentní:

(i) $\mathbf{u}_1, \ldots, \mathbf{u}_n$ jsou lineárně nezávislé

(ii) $[\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}] = \mathscr{V}$

(iii) $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ je báze $\mathscr{V}$.

Důkaz.

(i) $\Rightarrow$ (ii): Je-li $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ libovolná báze $\mathscr{V}$, pak dle Steinitzovy věty $[\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}] = [\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}] = \mathscr{V}$.

(ii) $\Rightarrow$ (iii): Je-li $[\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}] = \mathscr{V}$, pak $\mathbf{u}_1, \ldots, \mathbf{u}_n$ jsou lineárně nezávislé, jinak by dle Steinitzovy věty platilo $n = \dim \mathscr{V} < n$, spor.

(iii) $\Rightarrow$ (i): Dle definice báze.

Věta 2.12

Nechť $\dim \mathscr{V} = n$. Pak každá množina $\mathbf{u}_1, \ldots, \mathbf{u}_k$ lineárně nezávislých vektorů z $\mathscr{V}$ je obsažena v některé bázi prostoru $\mathscr{V}$.

Důkaz. Plyne ihned ze Steinitzovy věty.

Věta 2.13

Nechť $\mathscr{W}$ je podprostor prostoru $\mathscr{V}$ konečné dimenze. Pak $\dim \mathscr{W} \leq \dim \mathscr{V}$, přičemž rovnost platí právě když $\mathscr{W} = \mathscr{V}$.

Důkaz. Zřejmě, jsou-li některé vektory nezávislé ve $\mathscr{W}$, jsou lineárně nezávislé i ve $\mathscr{V}$. Je-li tedy $\dim \mathscr{V} = n$, pak má každá lineárně nezávislá množina ve $\mathscr{W}$ nejvýše n prvků, t.j. $\dim \mathscr{W} \leq \dim \mathscr{V}$. Zbytek důkazu plyne z Věty 2.11.

Věta 2.14 (O dimenzi spojení a průniku)

Nechť $\mathscr{W}_1, \mathscr{W}_2$ jsou podprostory prostoru $\mathscr{V}$ konečné dimenze. Pak $\dim\mathscr{W}_1 + \dim\mathscr{W}_2 = \dim(\mathscr{W}_1 + \mathscr{W}_2) + \dim(\mathscr{W}_1 \cap \mathscr{W}_2)$.

Důkaz. Nechť $\dim\mathscr{W}_1 = k$, $\dim\mathscr{W}_2 = h$, $\dim(\mathscr{W}_1 \cap \mathscr{W}_2) = m$. Zřejmě $m \leq k$, $m \leq h$. Nechť $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ je báze $\mathscr{W}_1$, $\{\mathbf{v}_1, \ldots, \mathbf{v}_h\}$ je báze $\mathscr{W}_2$, a $\{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ je báze $\mathscr{W}_1 \cap \mathscr{W}_2$. Dle Steinitzovy věty platí, že při vhodném očíslování je $\{\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_{m+1}, \ldots, \mathbf{u}_k\}$ bází $\mathscr{W}_1$ a $\{\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{v}_{m+1}, \ldots, \mathbf{v}_h\}$ je bází $\mathscr{W}_2$. Ukážeme, že $M = \{\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_{m+1}, \ldots, \mathbf{u}_k, \mathbf{v}_{m+1}, \ldots, \mathbf{v}_h\}$ je bází $\mathscr{W}_1 + \mathscr{W}_2$.

Nechť $\mathbf{z} \in \mathscr{W}_1 + \mathscr{W}_2$, tedy $\mathbf{z} = \mathbf{z}_1 + \mathbf{z}_2$ pro $\mathbf{z}_i \in \mathscr{W}_i$, tedy $\mathbf{z}_1$ je lineární kombinace $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_{m+1}, \ldots, \mathbf{u}_k$, $\mathbf{z}_2$ je lineární kombinace $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{v}_{m+1}, \ldots, \mathbf{v}_h$, tedy $\mathbf{z}$ je lineární kombinací vektorů z M.

Stačí tedy dokázat, že vektory z M jsou lineárně nezávislé.

Nechť

$$\sum_{i=1}^{m} c_i \cdot \mathbf{w}_i + \sum_{j=m+1}^{k} d_j \cdot \mathbf{u}_j + \sum_{k=m+1}^{h} b_k \cdot \mathbf{v}_k = \mathbf{o}.$$

Pak $\sum_{i=1}^{m} c_i \cdot \mathbf{w}_i + \sum_{j=m+1}^{k} d_j \cdot \mathbf{u}_j = \sum_{k=m+1}^{h} (-b_k) \cdot \mathbf{v}_k$. Avšak vektor na levé straně patří do $\mathscr{W}_1$, na pravé do $\mathscr{W}_2$, a proto oba vektory patří do $\mathscr{W}_1 \cap \mathscr{W}_2$. Tedy existují $a_1, \ldots, a_m \in T$ tak, že

$$(-b_{m+1}) \cdot \mathbf{v}_{m+1} + \cdots + (-b_h) \cdot \mathbf{v}_h = a_1 \cdot \mathbf{w}_1 + \cdots + a_m \cdot \mathbf{w}_m.$$

Ovšem $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{v}_{m+1}, \ldots, \mathbf{v}_h$ jsou lineárně nezávislé, tedy $a_1 = \cdots = a_m = b_{m+1} = \cdots = b_h = 0$. Odtud

$$c_1 \cdot \mathbf{w}_1 + \cdots + c_m \cdot \mathbf{w}_m + d_{m+1} \cdot \mathbf{u}_{m+1} + \cdots + d_k \cdot \mathbf{u}_k = \mathbf{o}.$$

Avšak $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_{m+1}, \ldots, \mathbf{u}_k$ jsou také lineárně nezávislé, tedy $c_1 = \cdots = c_m = d_{m+1} = \cdots = d_k = 0$.
Dohromady, všechny vektory z M jsou lineárně nezávislé, tedy M je báze $\mathscr{W}_1 + \mathscr{W}_2$. Podle definice dimenze dostaneme tvrzení věty.

Důsledek

Je-li vektorový prostor konečné dimenze $\mathscr{V}$ přímým součtem podprostorů $\mathscr{W}_1$ a $\mathscr{W}_2$, pak $\dim\mathscr{W}_1+\dim\mathscr{W}_2=\dim\mathscr{V}$.

Důkaz. Plyne z Věty 2.14, neboť $\mathscr{W}_1\cap\mathscr{W}_2=\{\mathbf{o}\}$.

Obsah

Nechť T je číselné těleso, n přirozené číslo. Na n-násobném kartézském součinu $T^n = V$ definujeme operaci $+$ takto: je-li $(a_1,\ldots,a_n),(b_1,\ldots,b_n) \in V$, pak

$$(a_1,\ldots,a_n)+(b_1,\ldots,b_n) = (a_1+b_1,\ldots,a_n+b_n).$$

Zřejmě $(V,+)$ je abelovská grupa, prvek $\mathbf{o} = (0,\ldots,0)$ je její jednotkou, prvek $(-a_1,\ldots,-a_n)$ je inverzní k prvku $(a_1,\ldots,a_n)$. Definujme levou vnější operaci: $c \in T$, $(a_1,\ldots,a_n) \in V$,

$$c \cdot (a_1,\ldots,a_n) = (c \cdot a_1,\ldots,c \cdot a_n).$$

Jednoduše lze ověřit, že $\mathscr{V} = (V,+,T,\cdot)$ je vektorový prostor dimenze n. Tento vektorový prostor nazveme **aritmetický** a budeme jej značit T^n. Snadno se dokáže, že jedna z jeho (nekonečně mnoha) bází je $\mathbf{e}_1,\ldots,\mathbf{e}_n$, kde $\mathbf{e}_1 = (1,0,\ldots,0)$, $\mathbf{e}_2 = (0,1,\ldots,0)$, $\ldots$, $\mathbf{e}_n = (0,0,\ldots,1)$. Skutečně: $(a_1,a_2,\ldots,a_n) = a_1 \cdot \mathbf{e}_1 + a_2 \cdot \mathbf{e}_2 + \cdots + a_n \cdot \mathbf{e}_n$.

Označme $\mathscr{V}_i = \{(0,\ldots,0,a_i,0,\ldots,0); a_i \in T\}$. Zřejmě $\mathscr{V}_i$ je podprostor dimenze 1 ve $\mathscr{V}$ a $\mathscr{V}$ je přímým součtem $\mathscr{V}_1 + \mathscr{V}_2 + \cdots + \mathscr{V}_n$.

Zapisujeme-li aritmetický vektor **a** ve tvaru $(a_1, a_2, \ldots, a_n)$, nazýváme tento zápis **řádkový vektor**. Zapisujeme-li **a** ve tvaru $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$, nazýváme jej **sloupcový vektor**.

Je-li $\mathscr{V}$ vektorový prostor dimenze n, $\{\mathbf{u}_1,\ldots,\mathbf{u}_n\}$ jeho báze, pak $\mathscr{V}$ lze reprezentovat aritmetickým vektorovým prostorem takto: je-li $\mathbf{a} \in \mathscr{V}$, pak $\mathbf{a} = a_1 \cdot \mathbf{u}_1 + \cdots + a_n \cdot \mathbf{u}_n$ je jednoznačné vyjádření vektoru **a** v bázi $\{\mathbf{u}_1,\ldots,\mathbf{u}_n\}$. Přiřaďme vektoru **a** n-tici koeficientů $(a_1,\ldots,a_n)$. Je-li $\mathbf{b} = b_1 \cdot \mathbf{u}_1 + \cdots + b_n \cdot \mathbf{u}_n$, $\mathbf{b} \to (b_1,\ldots,b_n)$, $c \in T$. Pak zřejmě $c \cdot \mathbf{a} \to (c \cdot a_1,\ldots,c \cdot a_n)$, $\mathbf{a} + \mathbf{b} \to (a_1 + b_1,\ldots,a_n + b_n)$.

Obsah

Ve vektorovém prostoru nad tělesem T můžeme vektory sčítat, odčítat a násobit skaláry z tělesa T (levá vnější operace). Nemáme však zaveden pojem délky vektoru, úhlu mezi vektory apod. Zavedeme proto další pojem.

Definice

Nechť $\mathscr{V} = (V, +, \mathbb{R}, \cdot)$ je vektorový prostor nad tělesem reálných čísel $\mathbb{R}$. **Skalárním součinem** $\circ$ nazveme zobrazení $V \times V$ do tělesa $\mathbb{R}$, které má tyto vlastnosti:

(i) $\forall \mathbf{u}, \mathbf{v} \in V$, $\mathbf{u} \circ \mathbf{v} = \mathbf{v} \circ \mathbf{u}$

(ii) $\forall \mathbf{u} \in V$, $\mathbf{u} \neq \mathbf{o}$, $\mathbf{u} \circ \mathbf{u} > 0$

(iii) $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, $(\mathbf{u} + \mathbf{v}) \circ \mathbf{w} = \mathbf{u} \circ \mathbf{w} + \mathbf{v} \circ \mathbf{w}$

(iv) $\forall \mathbf{u}, \mathbf{v} \in V$, $\forall c \in \mathbb{R}$, $(c \cdot \mathbf{u}) \circ \mathbf{v} = c \cdot (\mathbf{u} \circ \mathbf{v})$.

Příklady

(1) Je-li $\mathscr{V} = (\mathbb{R}^n, +, \mathbb{R}, \cdot)$ aritmetický (n-dimenzionální) vektorový prostor nad $\mathbb{R}$, $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n)$, pak $\mathbf{x} \circ \mathbf{y} = \sum_{i=1}^{n} x_i \cdot y_i$ definuje skalární součin $\circ$.

(2) Je-li $\mathscr{V}$ vektorový prostor všech funkcí jedné reálné proměnné nad intervalem $[a, b]$, pak $\mathbf{f} \circ \mathbf{g} = \int_a^b f(x)g(x)dx$ definuje skalární součin $\circ$.

Definice

Nechť $\mathscr{V} = (V, +, \mathbb{R}, \cdot)$ je vektorový prostor nad tělesem reálných čísel, ve kterém je definován skalární součin. Pak se $\mathscr{V}$ nazývá **Eukleidovský vektorový prostor**.

Definice

Nechť $\mathscr{V}$ je Eukleidovský vektorový prostor, nechť $\mathbf{u} \in V$. Číslo $\|\mathbf{u}\| = \sqrt{\mathbf{u} \circ \mathbf{u}}$ nazveme **délka vektoru u**.

Věta 2.15

Nechť $\mathscr{V}$ je Eukleidovský vektorový prostor, $\mathbf{u},\mathbf{v} \in V$. Pak

(a) $\forall c \in \mathbb{R}$ je $\|c \cdot \mathbf{u}\| = |c| \cdot \|\mathbf{u}\|$

(b) $\|\mathbf{o}\| = 0$ a pro $\mathbf{u} \neq \mathbf{o}$ je $\|\mathbf{u}\| > 0$

(c) $|\mathbf{u} \circ \mathbf{v}| \leq \|\mathbf{u}\| \cdot \|\mathbf{v}\|$ (Schwarzova nerovnost).

Důkaz. (a) $\|c \cdot \mathbf{u}\| = \sqrt{c \cdot \mathbf{u} \circ c \cdot \mathbf{u}} = \sqrt{c^2 \cdot \mathbf{u} \circ \mathbf{u}} = |c| \cdot \|\mathbf{u}\|$.
(b) $\mathbf{o} = \mathbf{u} - \mathbf{u}$, tedy $\|\mathbf{o}\| = \|\mathbf{u} - \mathbf{u}\| = \sqrt{(\mathbf{u} - \mathbf{u}) \circ (\mathbf{u} - \mathbf{u})} = \sqrt{\mathbf{u} \circ \mathbf{u} - \mathbf{u} \circ \mathbf{u} - \mathbf{u} \circ \mathbf{u} + \mathbf{u} \circ \mathbf{u}} = \sqrt{0} = 0$. Je-li $\mathbf{u} \neq \mathbf{o}$, pak dle (ii) platí $\mathbf{u} \circ \mathbf{u} > 0$, a tedy $\|\mathbf{u}\| = \sqrt{\mathbf{u} \circ \mathbf{u}} > 0$.
(c) Dle (ii) a (b) platí $\|\mathbf{u} - c \cdot \mathbf{v}\| \geq 0 \ \forall c \in \mathbb{R}$. Rozepsáním dostaneme $0 \leq (\mathbf{u} - c \cdot \mathbf{v}) \circ (\mathbf{u} - c \cdot \mathbf{v}) = \mathbf{u} \circ (\mathbf{u} - c \cdot \mathbf{v}) + (-c \cdot \mathbf{v}) \circ (\mathbf{u} - c \cdot \mathbf{v}) = \mathbf{u} \circ \mathbf{u} + \mathbf{u} \circ (-c \cdot \mathbf{v}) + (-c \cdot \mathbf{v}) \circ \mathbf{u} + (-c \cdot \mathbf{v}) \circ (-c \cdot \mathbf{v}) = c^2 \cdot \mathbf{v} \circ \mathbf{v} - 2c \cdot \mathbf{u} \circ \mathbf{v} + \mathbf{u} \circ \mathbf{u}$, což je kvadratická funkce pro c. Jelikož je nezáporná, nemůže mít pravá strana dva různé reálné kořeny (neprotíná osu x ve dvou bodech), a tedy pro diskriminant platí $4 \cdot (\mathbf{u} \circ \mathbf{v})^2 - 4 \cdot (\mathbf{u} \circ \mathbf{u}) \cdot (\mathbf{v} \circ \mathbf{v}) \leq 0$, odtud $(\mathbf{u} \circ \mathbf{v})^2 \leq (\mathbf{u} \circ \mathbf{u}) \cdot (\mathbf{v} \circ \mathbf{v})$, tedy po odmocnění $|\mathbf{u} \circ \mathbf{v}| \leq \|\mathbf{u}\| \cdot \|\mathbf{v}\|$.

Definice

Nechť $\mathscr{V}$ je Eukleidovský vektorový prostor a $\mathbf{u}, \mathbf{v} \in V$, $\mathbf{u} \neq \mathbf{o} \neq \mathbf{v}$. **Úhlem φ vektorů $\mathbf{u}, \mathbf{v}$** nazveme číslo

$$\varphi = \arccos \frac{\mathbf{u} \circ \mathbf{v}}{\|\mathbf{u}\| \cdot \|\mathbf{v}\|}.$$

Platí tedy $\cos \varphi = \frac{\mathbf{u} \circ \mathbf{v}}{\|\mathbf{u}\| \cdot \|\mathbf{v}\|}$, kde $0 \leq \varphi \leq \pi$. Je-li $\mathbf{u} = \mathbf{o}$ nebo $\mathbf{v} = \mathbf{o}$, položíme $\cos \varphi = 0$. Ze Schwarzovy nerovnosti plyne, že úhel φ je určen jednoznačně.

Definice

Vektory $\mathbf{u}, \mathbf{v}$ nazveme **ortogonální** (**kolmé**), ozn. $\mathbf{u} \perp \mathbf{v}$, je-li $\varphi = \frac{\pi}{2}$, t.j. $\cos\varphi = 0$, t.j. $\mathbf{u} \circ \mathbf{v} = 0$.

Věta 2.16

Jsou-li $\mathbf{u}, \mathbf{v}_1, \ldots, \mathbf{v}_m$ vektory z Eukleidovského vektorového prostoru a platí-li $\mathbf{u} \perp \mathbf{v}_i$ pro $i = 1, \ldots, m$, pak $\mathbf{u} \perp \mathbf{w}$ pro každý vektor $\mathbf{w} \in [\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}]$.

Důkaz. Nechť $\mathbf{w} \in [\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}]$. Pak $\mathbf{w} = c_1\mathbf{v}_1 + \cdots + c_m\mathbf{v}_m$ pro některá čísla $c_1, \ldots, c_m \in \mathbb{R}$. Potom
$\mathbf{u} \circ \mathbf{w} = \mathbf{u} \circ (c_1\mathbf{v}_1 + \cdots + c_m\mathbf{v}_m) = \mathbf{u} \circ (c_1\mathbf{v}_1) + \cdots + \mathbf{u} \circ (c_m\mathbf{v}_m) =$
$c_1(\mathbf{u} \circ \mathbf{v}_1) + \cdots + c_m(\mathbf{u} \circ \mathbf{v}_m) = 0 + \cdots + 0 = 0.$

Definice

Vektory $\mathbf{u}_1, \ldots, \mathbf{u}_m$ jsou **vzájemně ortogonální**, platí-li $\mathbf{u}_i \perp \mathbf{u}_j$ pro každé $i \neq j$.

Věta 2.17

Nenulové vzájemně ortogonální vektory $\mathbf{u}_1, \ldots, \mathbf{u}_m$ jsou lineárně nezávislé.

Důkaz. Nechť $\mathbf{o} = c_1\mathbf{u}_1 + \cdots + c_m\mathbf{u}_m$ pro $c_i \in \mathbb{R}$. Pak $\forall k \in \{1, \ldots, m\}$ platí

$0 = \mathbf{o} \circ \mathbf{u}_k = (c_1\mathbf{u}_1 + \cdots + c_m\mathbf{u}_m) \circ \mathbf{u}_k = c_1(\mathbf{u}_1 \circ \mathbf{u}_k) + \cdots + c_m(\mathbf{u}_m \circ \mathbf{u}_k) =$
$0 + \cdots + 0 + c_k(\mathbf{u}_k \circ \mathbf{u}_k) + 0 + \cdots + 0 = c_k \|\mathbf{u}_k\|^2 > 0$ pro $c_k \neq 0$. Tedy $c_k = 0$. Tedy $\forall k \in \{1, \ldots, m\}$ je $c_k = 0$, t.j. $\mathbf{u}_1, \ldots, \mathbf{u}_m$ jsou lineárně nezávislé.

Důsledek a definice

Jsou-li $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vzájemně ortogonální vektory, přičemž $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ generuje celý prostor $\mathscr{V}$, pak je to báze $\mathscr{V}$ (tzv. **ortogonální báze**).

Příklad

Je-li $\mathscr{V} = (\mathbb{R}^n, +, \mathbb{R}, \cdot)$ aritmetický vektorový prostor, pak např. vektory $\mathbf{e}_1 = (1, 0, \ldots, 0), \mathbf{e}_2 = (0, 1, \ldots, 0), \ldots, \mathbf{e}_n = (0, \ldots, 0, 1)$ tvoří ortogonální bázi prostoru $\mathscr{V}$.

Dále ukážeme metodu, tzv. **Schmidtův ortogonalizační proces**, pomocí které lze každou bázi vektorového prostoru $\mathscr{V}$ převést na bázi ortogonální.

Věta 2.18

Nechť $\mathscr{V}$ je Eukleidovský vektorový prostor konečné dimenze, nechť $\mathbf{v}_1, \ldots, \mathbf{v}_m$ je jeho báze. Pak existují čísla d_{ik} tak, že vektory

$$\mathbf{u}_i = \mathbf{v}_i - \sum_{k=1}^{i-1} d_{ik}\mathbf{u}_k \qquad (i = 1, \ldots, m)$$

tvoří ortogonální bázi.

Důkaz. Indukcí. Je-li $\dim\mathscr{V} = 1$, je $\mathbf{u}_1 = \mathbf{v}_1$. Nechť $\dim\mathscr{V} = m > 1$ a předpokládejme, že jsme již sestrojili vektory $\mathbf{u}_1, \ldots, \mathbf{u}_{n-1}$, které jsou vzájemně ortogonální a platí $[\{\mathbf{u}_1, \ldots, \mathbf{u}_{n-1}\}] = [\{\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}\}]$. Položme nyní $\mathbf{u}_n = \mathbf{v}_n - \sum_{k=1}^{n-1} c_{nk}\mathbf{u}_k$, kde $c_{nk} = \frac{\mathbf{v}_n \circ \mathbf{u}_k}{\mathbf{u}_k \circ \mathbf{u}_k}$. Pak pro $j = 1, \ldots, n-1$ platí
$\mathbf{u}_n \circ \mathbf{u}_j = \mathbf{v}_n \circ \mathbf{u}_j - \sum_{k=1}^{n-1} c_{nk}(\mathbf{u}_k \circ \mathbf{u}_j) = \mathbf{v}_n \circ \mathbf{u}_j - c_{nj}(\mathbf{u}_j \circ \mathbf{u}_j)$ (neboť $\mathbf{u}_s \perp \mathbf{u}_r$ pro $r \neq s$). Dosazením za c_{nj} dostaneme $\mathbf{u}_n \circ \mathbf{u}_j = 0$, tedy $\mathbf{u}_n$ je také kolmý na $\mathbf{u}_1, \ldots, \mathbf{u}_{n-1}$. Indukcí jsme dokázali, že $\mathbf{u}_1, \ldots, \mathbf{u}_m$ jsou vzájemně ortogonální. Dle Věty 2.17 jsou tedy lineárně nezávislé, a dle Steinitzovy věty tvoří bázi $\mathscr{V}$.

Postup ortogonalizace

Nechť $\mathbf{v}_1, \ldots, \mathbf{v}_n$ jsou lineárně nezávislé vektory ve $\mathscr{V}$. Položme

$$\mathbf{u}_1 = \mathbf{v}_1$$
$$\mathbf{u}_2 = \mathbf{v}_2 - \left(\frac{\mathbf{v}_2 \circ \mathbf{u}_1}{\mathbf{u}_1 \circ \mathbf{u}_1}\right)\mathbf{u}_1$$
$$\mathbf{u}_3 = \mathbf{v}_3 - \left(\frac{\mathbf{v}_3 \circ \mathbf{u}_2}{\mathbf{u}_2 \circ \mathbf{u}_2}\right)\mathbf{u}_2 - \left(\frac{\mathbf{v}_3 \circ \mathbf{u}_1}{\mathbf{u}_1 \circ \mathbf{u}_1}\right)\mathbf{u}_1$$
$$\ldots$$
$$\mathbf{u}_n = \mathbf{v}_n - \left(\frac{\mathbf{v}_n \circ \mathbf{u}_{n-1}}{\mathbf{u}_{n-1} \circ \mathbf{u}_{n-1}}\right)\mathbf{u}_{n-1} - \cdots - \left(\frac{\mathbf{v}_n \circ \mathbf{u}_1}{\mathbf{u}_1 \circ \mathbf{u}_1}\right)\mathbf{u}_1.$$

Pak $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ jsou vzájemně ortogonální.

Obsah

Definice

Nechť T je číselné těleso, m,n jsou čísla přirozená a nechť $a_{ij} \in T$ pro $i = 1,\ldots,m$, $j = 1,\ldots,n$. Dvojindexované schéma

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

se nazývá **matice typu** $m \times n$ **nad** T. Číslo a_{ij} se nazývá **prvek matice** A z i-tého řádku a j-tého sloupce. Číslo i se nazývá **řádkový**, číslo j **sloupcový index** prvku a_{ij}.

Někdy budeme matici A označovat jen stručně $A = \|a_{ij}\|$. Nechť $r = \min(m,n)$; pak řekneme, že prvky $a_{11}, a_{22}, \ldots, a_{rr}$ tvoří **hlavní diagonálu matice** A.

Příklad

$A = \begin{pmatrix} 2 & 0 & -1 & 0 \\ 1 & \frac{1}{4} & -2 & -\frac{2}{3} \\ 0 & 0 & 7 & 1 \end{pmatrix}$ je matice typu 3×4 nad tělesem $\mathbb{Q}$, kde prvky $2, \frac{1}{4}$ a 7 tvoří hlavní diagonálu.

Definice

Matice $A = \|a_{ij}\|$ typu $m \times n$, kde $m = n$, se nazývá **čtvercová matice (stupně n)**. Čtvercová matice A se nazývá **diagonální**, pokud všechny její prvky, které neleží na hlavní diagonále jsou rovny 0. Diagonální matice se nazývá **skalární**, jestliže všechny její prvky na hlavní diagonále jsou si rovny. Skalární matice se nazývá **jednotková matice stupně** n, jsou-li všechny její prvky na hlavní diagonále rovny 1 (budeme ji označovat E_n). Matici $N = \|n_{ij}\|$ typu $m \times n$ nazveme **nulová matice**, jestliže $n_{ij} = 0$ pro každé $i = 1, \ldots, m$, $j = 1, \ldots, n$.

Příklad

Nechť A, B, C, D, E_2 jsou čtvercové matice stupně 2 nad tělesem $\mathbb{Q}$: $A = \begin{pmatrix} 2 & 1 \\ 0 & -3 \end{pmatrix}$, $B = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$, $C = \begin{pmatrix} -3 & 0 \\ 0 & -3 \end{pmatrix}$, $D = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Pak A není diagonální, B je diagonální, ale není skalární, C, D, E_2 jsou skalární, přičemž D je nulová a E_2 je jednotková.

Označení. Symbolem $\mathscr{M}_{m\times n}(T)$ resp. $\mathscr{M}_n(T)$ označíme množinu všech matic typu $m \times n$ resp. všech čtvercových matic stupně n nad tělesem T.

Definice

Dvě matice $A = \|a_{ij}\|$, $B = \|b_{ij}\|$ z $\mathscr{M}_{m\times n}(T)$ jsou si **rovny**, jestliže $a_{ij} = b_{ij}$ pro každé $i = 1,\ldots,m$, $j = 1,\ldots,n$. Zapisujeme $A = B$.

Definice

Nechť $A = \|a_{ij}\|$, $B = \|b_{ij}\| \in \mathscr{M}_{m\times n}(T)$. **Součtem matic** A **a** B rozumíme matici $A+B = \|c_{ij}\|$, kde $c_{ij} = a_{ij} + b_{ij}$ pro každé $i = 1,\ldots,m$, $j = 1,\ldots,n$.

Příklad

Součtem matic $A = \begin{pmatrix} 1 & 0 & 2 \\ 2 & -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} -1 & -1 & -1 \\ 0 & 2 & 0 \end{pmatrix}$ je matice $A+B = \begin{pmatrix} 0 & -1 & 1 \\ 2 & 1 & 0 \end{pmatrix}$.

Věta 3.1

Množina $\mathscr{M}_{m\times n}(T)$ spolu se zavedenou operací sčítání matic tvoří abelovskou grupu.

Důkaz. Nechť $A=\|a_{ij}\|, B=\|b_{ij}\|, C=\|c_{ij}\| \in \mathscr{M}_{m\times n}(T)$. Jelikož sčítání v T je asociativní, t.j.

$$a_{ij}+(b_{ij}+c_{ij})=(a_{ij}+b_{ij})+c_{ij}, \quad \forall i,j,$$

platí také $A+(B+C)=(A+B)+C$, t.j. $(\mathscr{M}_{m\times n}(T),+)$ je pologrupa. Nechť $N=\|n_{ij}\| \in \mathscr{M}_{m\times n}(T)$ je nulová matice, t.j. $n_{ij}=0$ pro každé i,j. Pak $a_{ij}+0=0+a_{ij}=a_{ij}$, odtud $A+N=N+A=A$, tedy N je jednotkou v $(\mathscr{M}_{m\times n}(T),+)$. Označme $-A$ matici, jejíž prvky jsou $-a_{ij}$, t.j. $-A=\|-a_{ij}\|$. Snadno se přesvědčíme, že $A+(-A)=(-A)+A=N$, tedy $-A$ je prvek inverzní k A, tedy $(\mathscr{M}_{m\times n}(T),+)$ je grupa. Jelikož sčítání v T je komutativní: $a_{ij}+b_{ij}=b_{ij}+a_{ij}$, je také $A+B=B+A$, tedy tato grupa je abelovská.

Matici $-A$ budeme nazývat **matice opačná k** A.

Definice

Nechť T je číselné těleso, $A \in \mathscr{M}_{m\times n}(T)$. Prvky z T budeme nazývat skaláry. Zavedeme levou vnější operaci $\cdot\colon T \times \mathscr{M}_{m\times n}(T) \to \mathscr{M}_{m\times n}(T)$ takto: $c \in T$, $A = \|a_{ij}\|$, pak $cA = \|c \cdot a_{ij}\|$ je tzv. **násobení matice skalárem**.

Příklad

Nechť $T = \mathbb{Q}$, $A = \begin{pmatrix} 0 & 0 & 1 \\ -2 & 1 & 0{,}5 \end{pmatrix} \in \mathscr{M}_{2\times 3}(\mathbb{Q})$, pak

$4A = \begin{pmatrix} 0 & 0 & 4 \\ -8 & 4 & 2 \end{pmatrix}$ a $-2A = \begin{pmatrix} 0 & 0 & -2 \\ 4 & -2 & -1 \end{pmatrix}$.

Věta 3.2

Nechť T je číselné těleso, $\mathscr{M}_{m\times n}(T)$ množina všech matic typu $m \times n$ nad T, $+$ sčítání matic, $\cdot$ levá vnější operace násobení matice skalárem. Pak $(\mathscr{M}_{m\times n}(T), +, T, \cdot)$ je vektorový prostor dimenze $m \times n$ nad T.

Důkaz. Dle Věty 3.1 je $(\mathscr{M}_{m\times n}(T), +)$ abelovská grupa, stačí tedy ověřit (i), (ii), (iii), (iv) z definice vektorového prostoru. Snadno lze dokázat, že pro každé $A, B \in \mathscr{M}_{m\times n}(T)$, $c, d \in T$ platí

(i) $c(A+B) = cA + cB$

(ii) $(c+d)A = cA + dA$

(iii) $(cd)A = c(dA)$

(iv) $1A = A$

a tedy $(\mathscr{M}_{m\times n}(T); +, T, \cdot)$ je vektorový prostor nad T.
Dále, označme J_{ij} matici takovou, že prvek v i-tém řádku a j-tém sloupci je roven 1 a všechny ostatní prvky jsou rovny 0:

$$J_{ij} = \begin{pmatrix} 0 & \dots & 0 & \dots & 0 \\ \vdots & & & & \\ 0 & \dots & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix}.$$

Pak $\{J_{ij}; i = 1, \dots, m, j = 1, \dots, n\}$ tvoří bázi tohoto vektorového prostoru, neboť zřejmě pro $A = \|a_{ij}\|$ platí

$$A = a_{11}J_{11} + a_{12}J_{12} + \cdots + a_{1n}J_{1n} + a_{21}J_{21} + \cdots + a_{mn}J_{mn}.$$

Dle Důsledků Steinitzovy věty je dimenze tohoto vektorového prostoru rovna počtu prvků báze, t.j. $m \times n$. (Ověření, že J_{ij} jsou lineárně nezávislé je snadné.)

Definice

Nechť $A = \|a_{ij}\|$ je matice typu $m \times n$. **Matici transponovanou k matici** A nazýváme matici $A^T = \|a_{ji}\|$ typu $n \times m$, která vznikne z A vzájemnou záměnou řádků a sloupců (t.j. otočením A podle hlavní diagonály).

Příklad

Je-li $A = \begin{pmatrix} -1 & 0 & 3 \\ 4 & 10 & -2 \end{pmatrix}$, pak $A^T = \begin{pmatrix} -1 & 4 \\ 0 & 10 \\ 3 & -2 \end{pmatrix}$.

Snadno lze ověřit, že $(A+B)^T = A^T + B^T$ a $(cA)^T = cA^T$.

Nyní zavedeme tzv. součin matic:

Definice

Nechť $A = \|a_{ij}\|$ je typu $m \times n$, nechť $B = \|b_{jk}\|$ je typu $n \times p$ jsou matice nad tělesem T. **Součinem matic** A **a** B (v tomto pořadí) nazveme matici $AB = \|c_{ik}\|$ typu $m \times p$, pro jejíž prvky platí:

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk} = \sum_{j=1}^{n} a_{ij}b_{jk}$$

pro každé $i = 1, \ldots, m$, $k = 1, \ldots, p$.

Poznámka. Můžeme tedy násobit matice A a B jen tehdy, je-li počet sloupců matice A roven počtu řádků matice B. Tedy, jestliže existuje součin AB, nemusí existovat součin BA.

Poznámka. Pravidlo o násobení A a B si lze zapamatovat takto: násobíme i-tý řádek matice A k-tým sloupcem matice B, abychom obdrželi prvek c_{ik} matice AB.

Příklad

Mějme matice $A = \begin{pmatrix} 2 & 3 & 1 \\ -1 & 1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & -1 & 2 \\ 2 & -2 & 1 & -1 \\ 3 & 1 & 2 & 1 \end{pmatrix}$,

A typu 2×3, B typu 3×4. Zřejmě součin matic B a A neexistuje. Lze ale násobit matice A a B, přičemž AB je typu 2×4 a

$$AB = \begin{pmatrix} 11 & -5 & 3 & 2 \\ 7 & 0 & 6 & -1 \end{pmatrix},$$

kde

$c_{11} = 2 \cdot 1 + 3 \cdot 2 + 1 \cdot 3 = 2 + 6 + 3 = 11,$

$c_{12} = 2 \cdot 0 + 3 \cdot (-2) + 1 \cdot 1 = 0 - 6 + 1 = -5,$

$\vdots$

$c_{21} = (-1) \cdot 1 + 1 \cdot 2 + 2 \cdot 3 = -1 + 2 + 6 = 7,$

$\vdots$

Věta 3.3

Násobení matic je asociativní, t.j. jestliže $A \in \mathscr{M}_{m\times n}(T)$, $B \in \mathscr{M}_{n\times p}(T)$, $C \in \mathscr{M}_{p\times r}(T)$, pak

$$(AB)C = A(BC).$$

Důkaz. Nechť $A = \|a_{ij}\|$, $B = \|b_{jk}\|$, $C = \|c_{kl}\|$. Označme $D = AB = \|d_{ik}\|$ (je typu $m \times p$), $F = BC = \|f_{jl}\|$ (je typu $n \times r$). Tedy $d_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}$, $f_{jl} = \sum_{k=1}^{p} b_{jk}c_{kl}$. Dále vypočítáme prvek v i-tém řádku a l-tém sloupci matic $(AB)C$ a $A(BC)$. Pro $(AB)C$ je to

$$\sum_{k=1}^{p} d_{ik}c_{kl} = \sum_{k=1}^{p}(\sum_{j=1}^{n} a_{ij}b_{jk})c_{kl} = \sum_{k=1}^{p}\sum_{j=1}^{n}(a_{ij}b_{jk})c_{kl},$$

a pro matici $A(BC)$ je to prvek

$$\sum_{j=1}^{n} a_{ij}f_{jl} = \sum_{j=1}^{n} a_{ij}(\sum_{k=1}^{p} b_{jk}c_{kl}) = \sum_{j=1}^{n}\sum_{k=1}^{p} a_{ij}(b_{jk}c_{kl}).$$

Protože sčítání v T je komutativní a asociativní, násobení v T je asociativní, oba tyto prvky se sobě rovnají (pro každé i, l), tedy dle definice rovnosti matic platí $(AB)C = A(BC)$.

Poznámka. Vzhledem k asociativitě násobení matic není nutné součiny závorkovat, t.j. místo $(AB)C$ budeme psát jen ABC.

Poznámka. Násobení matic není obecně komutativní, a to ani v případě, že oba součiny AB i BA existují! Například pro čtvercové matice stupně 2

$$A = \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

je

$$AB = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} = BA.$$

Věta 3.4

Násobení matic je distributivní vzhledem ke sčítání, t.j. pro $A \in \mathscr{M}_{m\times n}(T)$, $B,C \in \mathscr{M}_{n\times p}(T)$ platí $A(B+C) = AB+AC$, pro $D \in \mathscr{M}_{p\times r}(T)$ platí $(B+C)D = BD+CD$.

Důkaz. Nechť $A = \|a_{ij}\|$, $B = \|b_{jk}\|$, $C = \|c_{jk}\|$. Označme $A(B+C) = F = \|f_{ik}\|$, $AB+AC = G = \|g_{ik}\|$. Pak $f_{ik} = \sum_{j=1}^{n} a_{ij}(b_{jk}+c_{jk}) = \sum_{j=1}^{n}(a_{ij}b_{jk}+a_{ij}c_{jk}) = g_{ik}$ pro každé i,k, tedy $A(B+C) = AB+AC$. Druhý distributivní zákon $(B+C)D = BD+CD$ se dokazuje analogicky.

Tvrzení. Platí, že $(AB)^T = B^T A^T$.

Věta 3.5

Nechť T je těleso, $n \in \mathbb{N}$. Pak $\mathscr{M}_n(T) = (\mathscr{M}_n(T), +, \cdot)$ je unitární okruh, jehož jednotkou je jednotková matice. Je-li $n > 1$, pak tento okruh není komutativní a obsahuje dělitele nuly. Je-li $n = 1$, pak $\mathscr{M}_1(T)$ je komutativní těleso.

Důkaz. Dle Věty 3.1 je $(\mathscr{M}_n(T), +)$ abelovská grupa, dle Věty 3.3 je $(\mathscr{M}_n(T), \cdot)$ pologrupa, zřejmě E_n je její jednotkou. Dle Věty 3.4 platí distributivní zákony, tedy $(\mathscr{M}_n(T); +, \cdot)$ je okruh. Je-li $n > 1$ a

$$A, B \in \mathscr{M}_n(T),\ A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & & & \\ 0 & 0 & \dots & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 0 & 1 \\ \vdots & & & \\ 0 & \dots & 0 & 1 \end{pmatrix}, \text{ pak}$$

$$AB = \begin{pmatrix} 0 & \dots & 0 & n \\ 0 & \dots & 0 & 0 \\ \vdots & & & \\ 0 & \dots & 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & 0 \\ \vdots & & & \\ 0 & \dots & 0 & 0 \end{pmatrix} = BA, \text{ t.j. } AB \neq BA,$$

přičemž B je levý a A je pravý dělitel 0.

Je-li $n = 1$, pak $A = \|a_{11}\|$, $B = \|b_{11}\|$, tedy pro sčítání i násobení platí pravidla z T, t.j. $\mathscr{M}_1(T)$ je komutativní těleso.

Obsah

Definice

Nechť $A = \{a_1, a_2, \ldots, a_n\}$ je konečná (n-prvková) množina. **Pořadím** π množiny A nazveme libovolnou posloupnost $\pi = (a_{k_1}, a_{k_2}, \ldots, a_{k_n})$ prvků z A takovou, že každý prvek z A se v π vyskytuje právě jedenkrát. **Permutací na** A rozumíme každou bijekci A na A. Permutaci P množiny A lze zapisovat ve tvaru

$$P = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_{\pi(1)} & a_{\pi(2)} & \ldots & a_{\pi(n)} \end{pmatrix},$$

kde π je některé pořadí množiny indexů.

Věta 4.1

Pro každou n-prvkovou množinu ($n \geq 1$) je počet pořadí roven počtu permutací, t.j. $n!$.

Důkaz. Indukcí: pro $n = 1$ zřejmě tvrzení platí. Nechť $n > 1$ a nechť pro každou k-prvkovou množinu, kde $k \leq n-1$ již tvrzení platí. Nechť $A = \{a_1, \ldots, a_n\}$. Pak počet pořadí množiny A, které mají na 1. místě pevně zvolený prvek a_i je roven počtu pořadí $(n-1)$-prvkové množiny, t.j. $(n-1)!$ dle indukčního předpokladu. Máme právě n možností volby pevného prvního prvku a_i (totiž $a_1, a_2 \ldots, a_n$), celkem je tedy těchto pořadí $n \cdot (n-1)! = n!$. To je ale zřejmě i počet permutací.

Úmluva. Jelikož nezáleží na povaze prvků $a_1, \ldots, a_n$, budeme dále pracovat přímo s množinou $A = \{1, 2, \ldots, n\}$. **Základním pořadím** A pak rozumíme $\pi_0 = (1, 2, \ldots, n)$.

Permutaci P množiny A lze vyjádřit $P = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$, kde π_1, π_2 jsou pořadí A.

Příklad

Nechť $A = \{1,2,3,4,5\}$, pak $P = \begin{pmatrix} 2 & 1 & 3 & 5 & 4 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}$ a $Q = \begin{pmatrix} 3 & 5 & 1 & 4 & 2 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$ jsou dva zápisy téže permutace na A.

Nejčastěji budeme permutace zapisovat ve tvaru $P = \begin{pmatrix} \pi_0 \\ \pi_1 \end{pmatrix}$, kde π_0 je základní pořadí. Tedy v předchozím příkladě: $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}$. Tento tvar nazveme **základní tvar permutace**.

Definice

Nechť $\pi = (k_1, k_2, \ldots, k_n)$ je pořadí množiny $A = \{1, 2, \ldots, n\}$. Prvky k_i, k_j tvoří **inverzi v** π, jestliže $i < j$ a $k_i > k_j$. Označme $[\pi]$ počet všech inverzí v π. **Znaménkem pořadí** π nazveme číslo $\mathrm{sgn}\pi = (-1)^{[\pi]}$. Je-li $\mathrm{sgn}\pi = 1$, pořadí se nazývá **sudé**, je-li $\mathrm{sgn}\pi = -1$, π se nazývá **liché**.

Nechť $P = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$ je permutace množiny A. **Znaménkem permutace** P rozumíme číslo $\mathrm{sgn}P$, kde $\mathrm{sgn}P = 1$, je-li $\mathrm{sgn}\pi_1 = \mathrm{sgn}\pi_2$, $\mathrm{sgn}P = -1$, je-li $\mathrm{sgn}\pi_1 = -\mathrm{sgn}\pi_2$. Je-li $\mathrm{sgn}P = 1$, je P **sudá**. Je-li $\mathrm{sgn}P = -1$, je P **lichá**.

Příklad

Nechť $\pi = (2,4,3,5,1)$. Pak všechny jeho inverze jsou: 2,1; 4,3; 4,1; 3,1; 5,1. Tedy $[\pi] = 5$, t.j. $\operatorname{sgn}\pi = (-1)^5 = -1$, π je liché.

Nechť $P = \begin{pmatrix} 2 & 1 & 4 & 5 & 3 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix} = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$. Ověříme $[\pi_1] = 3$, $[\pi_2] = 5$, tedy $\operatorname{sgn}\pi_1 = -1 = \operatorname{sgn}\pi_2$, odkud $\operatorname{sgn}P = 1$, t.j. P je sudá permutace.

Poznámka. Je-li $P = \begin{pmatrix} \pi_0 \\ \pi_1 \end{pmatrix}$, kde π_0 je základní pořadí, pak zřejmě $\operatorname{sgn}P = \operatorname{sgn}\pi_1$.

Označení. Symbolem P_0 označíme **identickou permutaci**, t.j. $P_0 = \begin{pmatrix} \pi_0 \\ \pi_0 \end{pmatrix}$. Je-li $P = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$, symbolem P^{-1} označíme **inverzní permutaci**, t.j. $P^{-1} = \begin{pmatrix} \pi_2 \\ \pi_1 \end{pmatrix}$.

Věta 4.2

Platí $\operatorname{sgn} P_0 = 1$ a pro každou permutaci P je $\operatorname{sgn} P = \operatorname{sgn} P^{-1}$.

Důkaz. Plyne přímo z definice sgn, P_0 a P^{-1}.

Definice

Transpozicí na $A = \{1, \ldots, n\}$ rozumíme permutaci P takovou, že existují $i, j \in A$, $i \neq j$ tak, že $P(i) = j$, $P(j) = i$ a $P(k) = k$ pro každé $i \neq k \neq j$.

Tedy, je-li $P = \begin{pmatrix} \pi_0 \\ \pi_1 \end{pmatrix}$ transpozice, π_0 základní pořadí, pak π_1 má inverzi i, j, neboť P zaměňuje právě i s j (pro některé $i, j \in A$).

Příklad

$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$ je transpozice, zaměňuje 2 a 4.

Označení. Transpozici P zaměňující i a j budeme zapisovat $P = (i,j)$.

Přímo z definice transpozice plyne:

Věta 4.3

Každá transpozice je sama k sobě inverzní, t.j. je-li $P = (i,j)$, pak $P^{-1} = (i,j)$.

Věta 4.4

Každou permutaci je možné vyjádřit jako složení konečného počtu transpozic. Permutace P je sudá (resp. lichá), je-li tento počet transpozic sudý (resp. lichý).

Důkaz. Nechť P je v základním tvaru, t.j. $P = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$. Může být např. $1 = k_1$, $2 = k_2$ atd., pak buď $\forall i$ je $i = k_i$, t.j. $P = P_0$ (identická), t.j. je složena z 0 transpozic (0 je sudé číslo), nebo existuje $i \geq 1$ tak, že je to první číslo, pro které $i \neq k_i$. Tedy $k_i = j$ pro některé $j \in \{1, \dots, n\}$. Provedeme-li na základní pořadí $\pi_0 = (1, 2, \dots, n)$ transpozici (i, j), pak tedy pro $1, 2, \dots, i$ budou $k_1, k_2, \dots, k_i = j$ ve správné posloupnosti shodné s prvními i prvky z $\pi = (k_1, k_2, \dots, k_n)$. Je-li $i + 1 = k_{i+1}$, opět neprovádíme nic, zkoumáme $i + 2, \dots$ až narazíme na další číslo, např. r, pro které je $r \neq k_r = s$. Pak použijeme-li transpozici (r, s) na pořadí, vzniklé z π_0 pomocí (i, j), bude posloupnost $k_1, k_2, \dots, k_i, \dots, k_r$ shodná s prvními r prvky z π. Analogicky postupujeme dále. Jelikož A je konečná, po konečném počtu kroků dostaneme pořadí $\pi = (k_1, \dots, k_n)$ a obdržíme konečný počet transpozic. Bylo-li v π h inverzí, pak se dá dokázat, že je-li h liché číslo, je počet transpozic lichý, je-li h sudé číslo, je tento počet sudý.

Příklad

Nechť $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 7 & 6 & 5 & 2 \end{pmatrix} = \begin{pmatrix} \pi_0 \\ \pi \end{pmatrix}$. Zde $\pi_0 = (1,2,3,4,5,6,7)$. První i, pro které $i \neq k_i$ je 2, tedy máme transpozici $(2,k_2) = (2,4)$, jejíž aplikací na π_0 dostaneme pořadí $\pi_1 = (1,4,3,2,5,6,7)$, kde již první 3 prvky (t.j. 1, 4, 3) souhlasí s π. Toto pořadí π_1 se liší od π na 4. místě (neboť $2 \neq 7$). Dostaneme tedy transpozici $(2,7)$, jejímž použitím na π_1 obdržíme pořadí $\pi_2 = (1,4,3,7,5,6,2)$. Zřejmě π_2 se liší od π na 5. místě (neboť $5 \neq 6$); použitím transpozice $(5,6)$ na π_2, dostaneme $\pi_3 = \pi = (1,4,3,7,6,5,2)$, což je již pořadí z permutace P. Odkud

$$P = (2,4) \cdot (2,7) \cdot (5,6)$$

a tedy P je lichá. (To koresponduje s tím, že P má lichý počet inverzí; konkrétně devět.)

Důsledek

Je-li $n \geq 2$, pak mezi všemi $n!$ permutacemi n-prvkové množiny je právě $\frac{n!}{2}$ sudých a $\frac{n!}{2}$ lichých.

Důkaz. Složením transpozic dostaneme zřejmě permutaci. Dle Věty 4.4 je každá permutace složením transpozic. Nechť tedy M je množina všech transpozic z $A = \{1, \ldots, n\}$, pak vytvářejme všechny možné součiny. Zřejmě polovina bude lichých a polovina sudých. Všech permutací je ale $n!$.

Definice

Nechť $A = \|a_{ij}\|$ je čtvercová matice stupně n nad číselným tělesem T. **Determinantem** $detA$ matice A rozumíme číslo z T takové, že

$$detA = \sum_P \mathrm{sgn}P \cdot a_{1k_1} a_{2k_2} \dots a_{nk_n},$$

kde sčítáme přes všechny permutace $P = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$. Každý ze součinů $a_{1k_1} a_{2k_2} \dots a_{nk_n}$ nazýváme **člen determinantu** $detA$.

Tedy: determinant matice A je číslo z T, které je rovno součtu všech $n!$ součinů prvků matice A, kde v každém součinu je každý prvek právě z jednoho řádku a právě z jednoho sloupce, přičemž tento součin je opatřen znaménkem rovným znaménku permutace určené řádkovými a sloupcovými indexy prvků tohoto součinu.

Příklad

Určete determinant matice

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Jeho členy tedy budou součiny $a_{11}a_{22}$, $a_{12}a_{21}$. Určíme jejich znaménka:

$$sgn \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = 1, \quad sgn \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = -1.$$

Tedy

$$\det A = a_{11}a_{22} - a_{12}a_{21}.$$

Příklad

Určete determinant matice

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Jeho členy zřejmě budou: $a_{11}a_{22}a_{33}$, $a_{12}a_{23}a_{31}$, $a_{21}a_{32}a_{13}$, $a_{13}a_{22}a_{31}$, $a_{12}a_{21}a_{33}$, $a_{23}a_{32}a_{11}$. Pomocí permutací určíme u prvních tří znaménko $+$, u zbývajících bude znaménko $-$. Tedy

$$\begin{aligned} \det A &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{21}a_{32}a_{13} - \\ &= -a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{23}a_{32}a_{11}. \end{aligned}$$

Poznámka. Tato vyjádření determinantů matice 2. a 3. stupně se nazývají **Sarusovo pravidlo**. (Pozor: nelze použít pro stupeň větší než 3.)

Věta 4.5

Nechť $A \in \mathscr{M}_n(T)$. Pak $\det A = \det A^T$.

Důkaz. Zřejmě dle definice je $\det A$ roven součtu všech součinů $\operatorname{sgn} P \cdot a_{1k_1} a_{2k_2} \dots a_{nk_n}$, kde a_{ik_i} jsou vybrané právě z jednoho řádku a právě z jednoho sloupce a $P = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$. Avšak u transponované matice A^T jsou součiny stejné, pouze permutace jsou inverzní, t.j. u $a_{1k_1} a_{2k_2} \dots a_{nk_n}$ bude $P^{-1} = \begin{pmatrix} k_1 & k_2 & \dots & k_n \\ 1 & 2 & \dots & n \end{pmatrix}$. Dle definice sgn je ale $\operatorname{sgn} P^{-1} = \operatorname{sgn} P$.

Věta 4.6

Má-li čtvercová matice A v některém řádku (resp. sloupci) samé 0, je $\det A = 0$.

Důkaz. Zřejmě je každý člen determinantu roven nule, neboť obsahuje právě jeden prvek z tohoto řádku (event. sloupce).

Věta 4.7

Má-li $A \in \mathscr{M}_n(T)$ všechny prvky pod hlavní diagonálou rovny nule, pak $\det A = a_{11}a_{22}\ldots a_{nn}$.

Důkaz. Kromě členu $a_{11}a_{22}\ldots a_{nn}$ má každý další člen aspoň jeden prvek pod hlavní diagonálou, t.j. rovná se nule. U členu $a_{11}a_{22}\ldots a_{nn}$ je permutace identická, tedy se znaménkem $+$.

Věta 4.8

Vznikne-li matice B z matice $A \in \mathscr{M}_n(T)$ záměnou i-tého a j-tého řádku (resp. sloupce), přičemž $i \neq j$, pak $\det B = -\det A$.

Důkaz. Zřejmě členy determinantu (součiny), budou pro A i B shodné, až na znaménko. Každá permutace P ve členu $\det A$ se změní na P', kde P' je složením P a transpozice (i,j). Tedy sudá P se změní na lichou P' a obráceně, a to u každého členu, t.j. $\det B = -\det A$.

Věta 4.9

Vznikne-li matice B z matice $A \in \mathscr{M}_n(T)$ provedením některé permutace P na řádky (resp. sloupce) matice A, pak $\det B = \operatorname{sgn} P \cdot \det A$.

Důkaz. Analogicky jako u Věty 4.8.

Věta 4.10

Jestliže se v matici A rovnají i-tý a j-tý řádek (resp. sloupec) pro $i \neq j$, pak $\det A = 0$.

Důkaz. Zaměníme-li i-tý a j-tý řádek (resp. sloupec) v A, pak dle Věty 4.8 je $\det A = -\det A$ (neboť matice se nezmění). To ale implikuje $\det A = 0$.

Definice

Nechť $A = \|a_{ij}\| \in \mathscr{M}_{m\times n}(T)$. Pak každou matici, která vznikne z A vynecháním některých řádků a některých sloupců, nazýváme **dílčí maticí matice** A. Je-li dílčí matice matice A čtvercová, pak její determinant nazýváme **subdeterminant** A.

Definice

Je-li $A = \|a_{ij}\| \in \mathscr{M}_n(T)$, potom subdeterminant dílčí matice A_{ij} stupně $n-1$ vzniklé vynecháním i-tého řádku a j-tého sloupce nazveme **minor matice** A **příslušný k prvku** a_{ij} a značíme jej M_{ij}. **Algebraickým doplňkem prvku** a_{ij} nazýváme číslo $\mathscr{A}_{ij} = (-1)^{i+j} M_{ij}$.

Příklad

Určete minory a algebraické doplňky M_{12}, M_{33}, $\mathscr{A}_{12}$, $\mathscr{A}_{33}$ matice

$$A = \begin{pmatrix} 2 & 5 & 1 \\ 0 & -6 & 2 \\ 5 & 1 & -3 \end{pmatrix}.$$

Platí:

$$M_{12} = \begin{vmatrix} 0 & 2 \\ 5 & -3 \end{vmatrix} = -10, \quad M_{33} = \begin{vmatrix} 2 & 5 \\ 0 & -6 \end{vmatrix} = -12,$$

tedy

$$\mathscr{A}_{12} = (-1)^{1+2}(-10) = 10, \quad \mathscr{A}_{33} = (-1)^{3+3}(-12) = -12.$$

Nechť $A = \|a_{ij}\| \in \mathscr{M}_{m\times n}(T)$. Pak $\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in})$ nazýváme **řádkový vektor matice** A, $\mathbf{a}_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ nazýváme **sloupcový vektor matice** A (pro každé $i = 1, \ldots, m$, $j = 1, \ldots, n$).

Označení. Jsou-li $\mathbf{a}_1, \ldots, \mathbf{a}_n$ řádkové vektory a $\mathbf{b}_1, \ldots, \mathbf{b}_n$ sloupcové vektory matice $A \in \mathscr{M}_n(T)$, pak budeme také zkráceně zapisovat $A = \|\mathbf{b}_1, \ldots, \mathbf{b}_n\|$, resp. $A = \left\| \begin{matrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_n \end{matrix} \right\|$ a

$$\det A = |\mathbf{b}_1, \ldots, \mathbf{b}_n| = \begin{vmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_n \end{vmatrix}.$$

Věta 4.11 (Laplaceova)

Nechť $A = \|a_{ik}\| \in \mathscr{M}_n(T)$. Pak

(a) $\forall i = 1,\dots,n$ platí $\det A = a_{i1}\mathscr{A}_{i1} + a_{i2}\mathscr{A}_{i2} + \cdots + a_{in}\mathscr{A}_{in}$

(b) $\forall i,j = 1,\dots,n,\ i \neq j$ platí $a_{i1}\mathscr{A}_{j1} + \cdots + a_{in}\mathscr{A}_{jn} = 0$.

Důkaz. Dle definice je $detA = \sum_P \mathrm{sgn}P \cdot a_{1k_1}a_{2k_2}\dots a_{nk_n} = \sum_{k=1}^{n} a_{ik}\mathscr{B}_{ik}$, kde $\mathscr{B}_{ik} = \mathrm{sgn}P \cdot a_{2k_2}\dots a_{nk_n}$. Pokud v matici A zaměníme j-tý řádek i-tým (a i-tý ponecháme), má A dva shodné řádky a dle Věty 4.10 je

$$0 = \begin{vmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_i \\ \vdots \\ \mathbf{a}_i \\ \vdots \\ \mathbf{a}_n \end{vmatrix} = \sum_{k=1}^{n} a_{ik}\mathscr{B}_{jk}.$$

Abychom dokázali tvrzení věty, stačí tedy ukázat, že $\mathscr{B}_{ik} = \mathscr{A}_{ik}$ $(i = 1,\dots,n,\ k = 1,\dots,n)$.

(1) Je-li $i = 1 = k$, pak $a_{11}\mathscr{B}_{11} = \sum_P \mathrm{sgn}P \cdot a_{11}a_{2k_2}\dots a_{nk_n}$, kde sčítáme přes všechny permutace tvaru $P = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & k_2 & \dots & k_n \end{pmatrix}$. To tedy znamená, že $\mathscr{B}_{11} = \sum_{P'} \mathrm{sgn}P' \cdot a_{2k_2}a_{3k_3}\dots a_{nk_n}$, kde $P' = \begin{pmatrix} 2 & 3 & \dots & n \\ k_2 & k_3 & \dots & k_n \end{pmatrix}$, jelikož zřejmě $\mathrm{sgn}P = \mathrm{sgn}P'$. Tedy $\mathscr{B}_{11} = M_{11}$ a $\mathscr{A}_{11} = (-1)^2 M_{11} = M_{11}$, t.j. $\mathscr{B}_{11} = \mathscr{A}_{11}$.

(2) Nechť nyní jsou i, j libovolné indexy. Proveďme nejdříve permutaci $P_1 = \begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n \\ i & 1 & \dots & i-1 & i+1 & \dots & n \end{pmatrix}$ s řádky a $P_2 = \begin{pmatrix} 1 & 2 & \dots & j & j+1 & \dots & n \\ j & 1 & \dots & j-1 & j+1 & \dots & n \end{pmatrix}$ se sloupci matice A. Dostaneme matici:

$$C = \|c_{ik}\| = \begin{pmatrix} a_{ij} & a_{i1} & \dots & a_{i,j-1} & a_{i,j+1} & \dots & a_{in} \\ a_{1j} & a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i-1,j} & a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i+1,j} & a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{nj} & a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} \end{pmatrix}.$$

Snadno určíme: $\mathrm{sgn}P_1 = (-1)^{i-1}$, $\mathrm{sgn}P_2 = (-1)^{j-1}$, tedy dle Věty 4.9 a Věty 4.5 platí

$$\det C = (-1)^{i-1} \cdot (-1)^{j-1} \det A = (-1)^{i+j} \det A.$$

V matici C je ale $c_{11} = a_{ij}$, tedy dle (1) platí $\mathscr{B}_{ij} = \mathscr{D}_{11} = M_{ij}$. Tedy

$$a_{i1}\mathscr{B}_{i1} + \cdots + a_{in}\mathscr{B}_{in} = \det A =$$

$$= (-1)^{i+j} \det C = (-1)^{i+j}(c_{11}\mathscr{D}_{11} + \cdots + c_{1n}\mathscr{D}_{1n}) =$$

$$= (-1)^{i+j}(a_{ij}M_{ij} + a_{i1}\mathscr{D}_{12} + \cdots + a_{i,j-1}\mathscr{D}_{ij} + a_{i,j+1}\mathscr{D}_{i,j+1} + \cdots + a_{in}\mathscr{D}_{in}).$$

Přitom
$\mathscr{D}_{1k} = (-1)^{i+1}\mathscr{B}_{i,k-1}$ pro $k = 2, \ldots, j$ a
$\mathscr{D}_{1h} = (-1)^{i+1}\mathscr{B}_{ih}$ pro $h = j+1, \ldots, n$, odkud

$$\mathscr{B}_{ij} = (-1)^{i+j} M_{ij} = \mathscr{A}_{ij}.$$

Věta 4.12

Vznikne-li matice B z matice $A \in \mathscr{M}_n(T)$ vynásobením i-tého řádku (resp. sloupce) číslem $c \in T$, pak $\det B = c \cdot \det A$.

Důkaz. Dle Laplaceovy věty je

$$\det B = \sum_{k=1}^{n} c \cdot a_{ik} \mathscr{A}_{ik} = c \cdot \sum_{k=1}^{n} a_{ik} \mathscr{A}_{ik} = c \cdot \det A.$$

Důsledek. Jestliže $A \in \mathscr{M}_n(T)$, $c \in T$, pak

$$\det(cA) = c^n \cdot \det A.$$

Věta 4.13

Je-li i-tý řádek (resp. sloupec) matice $A \in \mathscr{M}_n(T)$ součtem vektorů $\mathbf{b}, \mathbf{c}$ pak

$$\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_i \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{b} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} + \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{c} \\ \vdots \\ \mathbf{a}_n \end{pmatrix}.$$

Důkaz. Dle Laplaceovy věty je

$\det A = \sum_{k=1}^{n} a_{ik} \mathscr{A}_{ik} = \sum_{k=1}^{n} (b_k + c_k) \mathscr{A}_{ik} = \sum_{k=1}^{n} b_k \mathscr{A}_{ik} + \sum_{k=1}^{n} c_k \mathscr{A}_{ik}$.

Věta 4.14

Nechť $A \in \mathscr{M}_n(T)$ a nechť B vznikne z A tak, že k některému řádku (sloupci) matice A přičteme libovolnou lineární kombinaci ostatních řádků (sloupců). Pak $\det B = \det A$.

Důkaz. Nechť k i-tému řádku matice A přičteme lineární kombinaci $\mathbf{b}$ ostatních. Pak $\det B =$

$$\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_i + \mathbf{b} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_i \\ \vdots \\ \mathbf{a}_n \end{pmatrix} + c_1 \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_n \end{pmatrix} + \cdots + c_n \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_n \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

$= \det A + 0 + \cdots + 0 = \det A.$

Věta 4.15

Jsou-li řádkové (sloupcové) vektory matice $A \in \mathscr{M}_n(T)$ lineárně závislé, pak $\det A = 0$.

Důkaz. Analogicky jako v předchozí větě. Nechť například $\mathbf{a}_i = c_1\mathbf{a}_1 + \cdots + c_{i-1}\mathbf{a}_{i-1} + c_{i+1}\mathbf{a}_{i+1} \cdots + c_n\mathbf{a}_n$ (neboť pak je jeden řádek lineární kombinací ostatních, viz Věta 2.2). Tedy $\det A =$

$$c_1 \begin{vmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_n \end{vmatrix} + \cdots + c_{i-1} \begin{vmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{i-1} \\ \mathbf{a}_{i-1} \\ \vdots \\ \mathbf{a}_n \end{vmatrix} + c_{i+1} \begin{vmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{i+1} \\ \mathbf{a}_{i+1} \\ \vdots \\ \mathbf{a}_n \end{vmatrix} + \cdots + c_n \begin{vmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_n \\ \vdots \\ \mathbf{a}_n \end{vmatrix} = 0 + \cdots + 0,$$

neboť každý má dva řádky shodné, t.j. $\det A = 0$.

Poznámka. Předchozích vět lze použít k praktickému výpočtu determinantů matic vyšších stupňů. Dle Laplaceovy věty lze determinant matice n-tého stupně převést na výpočet determinantů matic $(n-1)$-stupňů, atd. Dle Věty 4.14 lze v matici přičítat k řádku (respektive sloupci) lineární kombinace ostatních řádků (sloupců) a tak získat matici s mnoha nulami v některém řádku (či sloupci), kterou lze pak snadno dle Laplaceovy věty rozvinout, nebo lze získat matici, která má dva různé řádky (sloupce) shodné – pak je (dle Věty 4.10) $\det A = 0$.

Příklad

Vypočítejte determinant matice $A = \begin{pmatrix} -2 & 3 & -1 & 2 \\ 1 & -2 & 0 & 4 \\ 2 & -4 & -2 & 5 \\ -3 & 2 & 1 & -5 \end{pmatrix}$.

Řešení:

$$\begin{vmatrix} -2 & 3 & -1 & 2 \\ 1 & -2 & 0 & 4 \\ 2 & -4 & -2 & 5 \\ -3 & 2 & 1 & -5 \end{vmatrix} = \begin{vmatrix} 0 & -1 & -1 & 10 \\ 1 & -2 & 0 & 4 \\ 0 & 0 & -2 & -3 \\ 0 & -4 & 1 & 7 \end{vmatrix} =$$

$$= (-1)^{2+1} \begin{vmatrix} -1 & -1 & 10 \\ 0 & -2 & -3 \\ -4 & 1 & 7 \end{vmatrix} = (-1) \begin{vmatrix} -1 & 0 & 0 \\ 0 & -2 & -3 \\ -4 & 5 & -33 \end{vmatrix} =$$

$$(-1)(-1)^{1+1}(-1) \begin{vmatrix} -2 & -3 \\ 5 & -33 \end{vmatrix} = 66 + 15 = 81.$$

Nyní budeme zkoumat, jak lze vypočítat determinant součinu dvou čtvercových matic.

Věta 4.16

Nechť $A = \|a_{ij}\| \in \mathscr{M}_n(T)$, $n \geq 2$ je tvaru $A = \left\| \begin{matrix} B & D \\ N & C \end{matrix} \right\|$, kde B je čtvercová matice stupně r, C je čtvercová matice stupně s (t.j. $r+s=n$) a N je nulová matice. Pak $\det A = \det B \cdot \det C$.

Důkaz. Indukcí dle stupně matice A.

(a) $n = 2$, pak $A = \left\| \begin{matrix} a_{11} & a_{12} \\ 0 & a_{22} \end{matrix} \right\|$, tedy $\det A = a_{11} \cdot a_{22}$, t.j. tvrzení platí.

(b) Nechť tvrzení platí pro všechny matice daného typu a stupně $k \leq n-1$ ($n > 2$). Uvažujme zadanou matici A. Dle Laplaceovy věty platí

$$\det A = \sum_{j=1}^{n} a_{1j} \mathscr{A}_{1j} = \sum_{j=1}^{n} (-1)^{1+j} a_{1j} (\det M_{1j}),$$

kde M_{1j} je dílčí matice, která vznikne z A vynecháním 1. řádku a j-tého sloupce. Ovšem každá M_{1j} je stupně $n-1$ a přitom tvaru uvažovaného ve větě. Lze pro ni tedy použít indukční předpoklad.

Označme B_{1j} matici, která vznikne z B vynecháním 1. řádku a j-tého sloupce. Pak (dle předpokladu indukce) $\det M_{1j} = \det B_{1j} \cdot \det C$ ($j = 1, \ldots, r$). Ovšem matice $M_{1,r+1}, \ldots, M_{1n}$ můžeme vyjádřit ve tvaru, kdy levá horní čtvercová dílčí matice je stupně r, a tedy má v posledním řádku samé 0, t.j. determinant každé z těchto matic je roven nule, a dle indukčního předpokladu také $\det M_{1,r+k} = 0$ pro $k = 1, \ldots, s$. Dohromady:

$$\det A = \sum_{j=1}^{r} (-1)^{1+j} a_{1j} \cdot \det B_{1j} \cdot \det C =$$

$$= (\sum_{j=1}^{r} (-1)^{1+j} a_{1j} \cdot \det B_{1j}) \cdot \det C = \det B \cdot \det C.$$

Věta 4.17

Nechť $A, B \in \mathscr{M}_n(T)$. Pak $\det AB = \det A \cdot \det B$.

Důkaz. Nechť $A = \|a_{ij}\|$, $B = \|b_{ij}\|$. Uvažujme čtvercovou matici U stupně $2n$:

$$U = \left\| \begin{array}{cccc|cccc} & & & & 0 & 0 & \dots & 0 \\ & A & & & 0 & 0 & \dots & 0 \\ & & & & \vdots & \vdots & & \vdots \\ & & & & 0 & 0 & \dots & 0 \\ \hline -1 & 0 & \dots & 0 & & & & \\ 0 & -1 & \dots & 0 & & & & \\ \vdots & \vdots & & \vdots & & B & & \\ 0 & 0 & \dots & -1 & & & & \end{array} \right\|.$$

Dle Věty 4.5 a Věty 4.16 je $\det U = \det A \cdot \det B$. Nyní: k 1. ř. matice U přičteme lineární kombinaci řádků: $(n+1)$-ho, $(n+2)$-ho, ..., $2n$-tého s koeficienty $a_{11}, a_{12}, \dots, a_{1n}$. Analogicky přičteme ke 2. řádku matice U lineární kombinaci stejných řádků s koeficienty: $a_{21}, a_{22}, \dots, a_{2n}$, atd. až k n-tému řádku přičteme lineární kombinaci těchto řádků s koeficienty: $a_{n1}, a_{n2}, \dots, a_{nn}$. Dostaneme tak matici:

$$\left\|\begin{array}{cccc|ccc|c} 0 & 0 & \dots & 0 & \sum_{j=1}^{n} a_{1j}b_{j1} & \sum_{j=1}^{n} a_{1j}b_{j2} & \dots & \sum_{j=1}^{n} a_{1j}b_{jn} \\ 0 & 0 & \dots & 0 & \sum_{j=1}^{n} a_{2j}b_{j1} & \sum_{j=1}^{n} a_{2j}b_{j2} & \dots & \sum_{j=1}^{n} a_{2j}b_{jn} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & \sum_{j=1}^{n} a_{nj}b_{j1} & \sum_{j=1}^{n} a_{nj}b_{j2} & \dots & \sum_{j=1}^{n} a_{nj}b_{jn} \\ \hline -1 & 0 & \dots & 0 & & & & \\ 0 & -1 & \dots & 0 & & & & \\ \vdots & \vdots & & \vdots & & B & & \\ 0 & 0 & \dots & -1 & & & & \end{array}\right\| =$$

$= \left\| \begin{array}{cc} N & A\cdot B \\ -E & B \end{array} \right\|$. Nyní zaměníme: 1. sloupec s $(n+1)$., 2. sloupec s $(n+2)$. atd. až n. sloupec s $2n$. Získáme tak matici $\left\| \begin{array}{cc} A\cdot B & N \\ B & -E \end{array} \right\|$. Dle první části důkazu platí: $(-1)^n \cdot \det U = (-1)^n \cdot \det A \cdot \det B$. Dle Věty 4.16 je ale determinant poslední matice roven $\det AB \cdot \det(-E) = \det AB \cdot (-1)^n$. Porovnáním obou vztahů získáme $\det AB = \det A \cdot \det B$.

Obsah

Nechť $A \in \mathscr{M}_{m\times n}(T)$. Tedy její řádky jsou řádkové vektory a patří do aritmetického vektorového prostoru T^n.

Definice

Řádkovým podprostorem matice A rozumíme podprostor prostoru T^n generovaný všemi řádkovými vektory matice A.

Definice

Elementárními řádkovými transformacemi matice A nazýváme tyto operace:

(i) výměnu libovolných dvou řádků v A

(ii) vynásobení některého řádku v A číslem $c \in T$ různým od 0

(iii) přičtením libovolného násobku některého řádku z A k jinému řádku v A.

Definice

Řekneme, že $A, B \in \mathscr{M}_{m\times n}(T)$ jsou **řádkově ekvivalentní**, lze-li B získat z A pomocí konečného počtu elementárních řádkových transformací. Zapisujeme $A \sim B$.

Poznámka. Zřejmě pro každé $A, B, C \in \mathscr{M}_{m\times n}(T)$ platí: $A \sim A$, $A \sim B \Rightarrow B \sim A$, jestliže $A \sim B$ a $B \sim C$, pak $A \sim C$. Tedy řádková ekvivalence je relací ekvivalence na $\mathscr{M}_{m\times n}(T)$.

Věta 5.1

Jestliže $A, B \in \mathscr{M}_{m\times n}(T)$ a $A \sim B$, pak A i B určují stejné řádkové podprostory v T^n.

Důkaz. Nechť $\mathbf{a}_1, \ldots, \mathbf{a}_m$ jsou řádkové vektory matice A. Dle Věty 2.5 je řádkový podprostor matice A, t.j. $[\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}]$ roven lineárnímu obalu množiny $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$, což jsou všechny lineární kombinace vektorů $\mathbf{a}_1, \ldots, \mathbf{a}_m$. Je tedy zřejmé, že elementární transformací (i) se řádkový podprostor nezmění. Násobíme-li některý $\mathbf{a}_i$ číslem $c \in T$, $c \neq 0$, opět se řádkový podprostor nezmění, neboť vektor $c\mathbf{a}_i$ lze násobit $\frac{1}{c}$ ($c \neq 0$, je to lineární kombinace) a dostaneme $\frac{1}{c} \cdot c \cdot \mathbf{a}_i = \mathbf{a}_i$. Tedy transformací (ii) se řádkový podprostor nemění. Přičteme-li k $\mathbf{a}_i$ řádkový vektor $\mathbf{a}_j$, pak z množiny $\{\mathbf{a}_1, \ldots, \mathbf{a}_i + \mathbf{a}_j, \ldots, \mathbf{a}_j, \ldots, \mathbf{a}_m\}$ opět získáme $\mathbf{a}_i$ jako lineární kombinaci: $\mathbf{a}_i = (\mathbf{a}_i + \mathbf{a}_j) + (-1) \cdot \mathbf{a}_j$. Tedy ani transformací (iii) se řádkový podprostor nezmění. Jelikož $A \sim B$, jestliže B vznikne z A konečným počtem elementárních transformací, je důkaz hotov.

Definice

Vedoucím prvkem řádkového vektoru $\mathbf{a}_i$ nazveme první nenulový prvek v tomto vektoru (řádku). Matice A se nazývá **redukovaná**, je-li vedoucí prvek každého nenulového řádku v A roven 1 a jestliže jsou v každém sloupci A, který obsahuje vedoucí prvek některého řádku všechny zbývající prvky rovny 0. Redukovaná matice se nazývá **redukovaná trojúhelníková**, jestliže všechny její nulové řádky (pokud existují) jsou až za nenulovými a jestliže pro každé i, j, $i < j$ platí, že jsou-li $\mathbf{a}_i, \mathbf{a}_j$ nenulové řádky, vedoucí prvek v $\mathbf{a}_i$ je v k_i-tém sloupci, vedoucí prvek v $\mathbf{a}_j$ je v k_j-tém sloupci, pak $k_i < k_j$.

Příklad

Matice A je redukovaná, B redukovaná trojúhelníková:

$$A = \begin{pmatrix} 0 & 0 & 1 & 2 & -1 \\ 1 & 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 8 & 11 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 & 0 & 0 & 4 & -1 \\ 0 & 0 & 1 & 0 & 5 & 6 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Věta 5.2

Každá matice A je řádkově ekvivalentní s některou redukovanou maticí, kterou lze získat z A pomocí transformací (ii) a (iii). Každá matice je řádkově ekvivalentní s redukovanou trojúhelníkovou maticí.

Důkaz. Je-li A nulová, je redukovaná a trojúhelníková. Je-li A nenulová, pak existuje i-tý řádek, jehož vedoucí prvek $a_{ik} \neq 0$. Násobíme $\mathbf{a}_i$ prvkem $\frac{1}{a_{ik}}$, t.j. vedoucí prvek upraveného řádku bude roven 1. Nyní pro každé $j \neq i$ přičteme k $\mathbf{a}_j$ $(-a_{jk})$-tý násobek i-tého řádku. Tím dostaneme v k-tém sloupci 0 s výjimkou i-tého řádku, kde je 1. Tento postup opakujeme se všemi nenulovými řádky, výsledkem je redukovaná matice.

Jestliže nyní použijeme transformaci (i), můžeme „přeskládat“ řádky redukované matice, čímž získáme matici redukovanou trojúhelníkovou.

Věta 5.3

Nechť $A \in \mathscr{M}_{m\times n}(T)$ je redukovaná matice s nenulovými řádky $\mathbf{a}_1, \ldots, \mathbf{a}_r$. Pak pro každý vektor $\mathbf{u} = \sum_{i=1}^{r} c_i \mathbf{a}_i$ řádkového podprostoru matice A je c_i rovno k_i-té souřadnici vektoru $\mathbf{u}$.

Důkaz. Dle definice redukované matice je v k_i-tém sloupci 1 v i-tém řádku a 0 v ostatních řádcích. Odtud plyne tvrzení.

Důsledek 1

Nenulové řádky redukované matice jsou lineárně nezávislé.

Důsledek 2

Je-li $A \sim B$, kde B je redukovaná, pak nenulové řádky matice B tvoří bázi řádkového podprostoru matice A.

Důkaz. Plyne ihned z Věty 5.1 a 5.3.

Definice

Hodností matice $A \in \mathscr{M}_{m\times n}(T)$ rozumíme dimenzi řádkového podprostoru matice A v T^n. Hodnost matice A budeme značit $h(A)$.

Poznámka.

(a) Dle definice řádkového podprostoru je zřejmé, že $h(A)$ se rovná počtu lineárně nezávislých řádků matice $A \in \mathscr{M}_{m\times n}(T)$, t.j. $h(A) \leq m$

(b) $A \sim B \Rightarrow h(A) = h(B)$

(c) $h(A)$ se rovná počtu nenulových řádků libovolné redukované matice B takové, že $A \sim B$.

Připomeňme, že **subdeterminantem matice stupně k matice** $A \in \mathscr{M}_{m\times n}(T)$ (kde $k \leq \min(m,n)$) nazveme determinant libovolné čtvercové dílčí matice stupně k matice A.

Příklad

Je-li $A = \begin{pmatrix} 5 & 2 & -1 & 0 \\ -2 & 3 & 1 & -1 \\ 6 & -8 & 0 & 9 \end{pmatrix}$, pak jejími subdeterminanty 2. stupně jsou například determinanty $\begin{vmatrix} 5 & 2 \\ -2 & 3 \end{vmatrix} = 19$, $\begin{vmatrix} 2 & 0 \\ -8 & 9 \end{vmatrix} = 18$, subdeterminant 3. stupně je například $\begin{vmatrix} 5 & 2 & 0 \\ -2 & 3 & -1 \\ 6 & -8 & 9 \end{vmatrix} = 119$, atd.

Věta 5.4

Hodnost matice A je rovna maximálnímu stupni nenulového subdeterminantu matice A.

Důkaz. Zřejmě A je nulová právě když $h(A) = 0$, což je zřejmě ekvivalentní s tím, že každý subdeterminant stupně 1 (což je prvek z A) je roven 0. Nechť tedy A je nenulová.

Zřejmě dimenze podprostoru nezávisí na záměně souřadnic (t.j. sloupců), dle předchozí Poznámky (b) nezávisí dimenze, a tedy ani $h(A)$, na záměně řádků. Předpokládejme tedy, že maximální stupeň nenulového subdeterminantu je roven h a vzhledem k předchozímu, že je to subdeterminant $\mathscr{A}_h = \begin{vmatrix} a_{11} & \dots & a_{1h} \\ \vdots & & \vdots \\ a_{h1} & \dots & a_{hh} \end{vmatrix} \neq 0$. Chceme dokázat $[\{\mathbf{a}_1, \dots, \mathbf{a}_m\}] = [\{\mathbf{a}_1, \dots, \mathbf{a}_h\}]$. Nechť $\mathbf{a}_i$ je libovolný řádek matice A. Chceme dokázat, že pro $i = h+1, \dots, m$ je $\mathbf{a}_i$ lineární kombinací $\mathbf{a}_1, \dots, \mathbf{a}_h$.

Dle předpokladu je $\begin{vmatrix} a_{11} & \dots & a_{1h} & a_{1j} \\ \vdots & & \vdots & \vdots \\ a_{h1} & \dots & a_{hh} & a_{hj} \\ a_{i1} & \dots & a_{ih} & a_{ij} \end{vmatrix} = 0$, neboť je to již subdeterminant stupně $h+1$, a to pro každé j. Pomocí Laplaceovy věty rozvineme tento determinant dle posledního sloupce:

$$a_{1j}\mathscr{B}_1 + a_{2j}\mathscr{B}_2 + \cdots + a_{hj}\mathscr{B}_h + a_{ij}\mathscr{A}_h = 0,$$

kde $\mathscr{B}_1, \dots, \mathscr{B}_h, \mathscr{A}_h$ jsou stejné pro každé j, tedy i pro celé vektory platí $\mathscr{B}_1\mathbf{a}_1 + \mathscr{B}_2\mathbf{a}_2 + \cdots + \mathscr{B}_h\mathbf{a}_h + \mathscr{A}_h\mathbf{a}_i = \mathbf{o}$, kde $\mathbf{a}_i = (a_{i1}, a_{i2}, \dots, a_{im})$, odtud

$$\mathbf{a}_i = (-\frac{\mathscr{B}_1}{\mathscr{A}_h})\mathbf{a}_1 + (-\frac{\mathscr{B}_2}{\mathscr{A}_h})\mathbf{a}_2 + \cdots + (-\frac{\mathscr{B}_h}{\mathscr{A}_h})\mathbf{a}_h.$$

Tím jsme tedy dokázali $[\{\mathbf{a}_1, \dots, \mathbf{a}_m\}] \subseteq [\{\mathbf{a}_1, \dots, \mathbf{a}_h\}]$. Obrácená inkluze je zřejmá, tedy platí rovnost. Zbývá jen dokázat, že $\mathbf{a}_1, \dots, \mathbf{a}_h$ jsou lineárně nezávislé.
Předpokládejme, že $\mathbf{a}_1, \dots, \mathbf{a}_h$ jsou lineárně závislé. Pak dle Věty 4.15 je $\mathscr{A}_h = 0$, což je spor. Jsou tedy lineárně nezávislé.

Dokázali jsme tedy, že je-li maximální stupeň nenulového subdeterminantu roven h, je $h(A) = h$.

Obráceně: nechť $h(A) = h$, t.j. dle definice je dimenze podprostoru $[\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}] = h$. Pak pro každých h' řádků matice A, $h' > h$ platí, že tyto řádky jsou lineárně závislé a dle Věty 4.15 jsou tedy všechny subdeterminanty stupně h' rovny 0. Přitom však aspoň jeden subdeterminant stupně h je nenulový, jinak by $\mathbf{a}_1, \ldots, \mathbf{a}_h$ byly lineárně závislé, a tedy dimenze podprostoru by byla menší než h, spor.

Důsledek

Hodnost matice A je rovna maximálnímu počtu lineárně nezávislých sloupců matice A.

Důkaz. Plyne ihned z Věty 5.4 a Věty 4.5 ($\det A = \det A^T$).

Příklad

Určete $h(A)$, kde $A = \begin{pmatrix} 2 & 3 & -2 & 1 \\ 4 & 2 & 1 & -3 \\ -2 & 5 & -8 & 9 \end{pmatrix}$.

Řešení: Nejdříve pomocí elementárních transformací dostaneme

$$A \sim \begin{pmatrix} 2 & 3 & -2 & 1 \\ 0 & -4 & 5 & -5 \\ 0 & 8 & -10 & 10 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & -2 & 1 \\ 0 & -4 & 5 & -5 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Zřejmě $1 \leq h(A) < 3$, $\det \begin{vmatrix} 2 & 3 \\ 0 & -4 \end{vmatrix} \neq 0$, tedy $h(A) = 2$.

Definice

Nechť T je číselné těleso, $a_1, \ldots, a_n, b \in T$. Úloha určit všechny n-tice $(x_1, \ldots, x_n) \in T^n$ pro které platí

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b$$

se nazývá **lineární rovnice o n neznámých nad T**. Každá n-tice $(x_1, \ldots, x_n) \in T^n$ pro kterou tato rovnost platí se nazývá **řešení** této rovnice.

Rovnici $a_1 x_1 + \cdots + a_n x_n = b$ budeme zkráceně zapisovat $\sum_{i=1}^{n} a_i x_i = b$.

Definice

Nechť T je číselné těleso, $a_{ij} \in T$ pro $i = 1,\ldots,n$, $j = 1,\ldots,m$, $b_j \in T$. Úloha určit všechny n-tice $(x_1,\ldots,x_n) \in T^n$ pro které platí

$$\sum_{i=1}^{n} a_{1i}x_i = b_1 \qquad (R_1)$$

$$\vdots \qquad (S)$$

$$\sum_{i=1}^{n} a_{mi}x_i = b_m \qquad (R_m)$$

se nazývá **soustava** m **lineárních rovnic o** n **neznámých nad** T. Každá n-tice $(x_1,\ldots,x_n)$ splňující (S) se nazývá **řešení** této soustavy. Pokud $b_1 = b_2 = \cdots = b_m = 0$, soustava (S) se nazývá **homogenní**. Není-li (S) homogenní, nazývá se **nehomogenní**.

Poznámka. Jsou-li $M_1, \ldots, M_m$ množiny řešení rovnic $(R_1), \ldots, (R_m)$, pak pro množinu M řešení soustavy (S) platí $M = M_1 \cap M_2 \cap \cdots \cap M_m$.
Soustavu (S) můžeme zkráceně zapisovat

$$\sum_{i=1}^{n} a_{ji} x_i = b_j, \quad j = 1, \ldots, m. \qquad (S)$$

Definice

Nechť je dána soustava (S) lineárních rovnic. Pak matici

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \text{ resp. } \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{pmatrix}$$

nazýváme **matice soustavy (S)** resp. **rozšířená matice soustavy (S)**.

Poznámka. Buď (S) soustava lineárních rovnic, A její matice typu $m \times n$. Označíme-li sloupcové vektory: $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $\mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$, pak $\mathbf{x}$ je matice typu $n \times 1$, $\mathbf{b}$ je matice typu $m \times 1$; lze tedy soustavu (S) psát v tzv. **maticovém tvaru**

$$A \cdot \mathbf{x} = \mathbf{b}.$$

Řešením této soustavy je pak každý vektor $\mathbf{u} \in T^n$, pro který platí rovnost $A \cdot \mathbf{u} = \mathbf{b}$.
Rozšířenou matici soustavy (S) budeme také zapisovat symbolem $(A, \mathbf{b})$.

Definice

Soustava lineárních rovnic $A\mathbf{x} = \mathbf{b}$ se nazývá **řešitelná**, má-li aspoň jedno řešení. Dvě soustavy $A\mathbf{x} = \mathbf{b}$ a $B\mathbf{y} = \mathbf{c}$ se nazývají **ekvivalentní**, mají-li stejné množiny řešení.

Věta 5.5

Nehomogenní soustava lineárních rovnic $A\mathbf{x} = \mathbf{b}$ je řešitelná právě tehdy, je-li vektor $\mathbf{b}$ lineární kombinací sloupců matice A.

Důkaz. Označme $\mathbf{d}_1, \ldots, \mathbf{d}_n$ sloupcové vektory matice A. Soustavu $A\mathbf{x} = \mathbf{b}$ lze zřejmě zapsat ve tvaru $\sum_{i=1}^{n} x_i \mathbf{d}_i = \mathbf{b}$. Je-li tedy soustava řešitelná, existují $x_1, \ldots, x_n$ tak, že výše uvedená rovnost platí a tedy $\mathbf{b}$ je lineární kombinací $\mathbf{d}_1, \ldots, \mathbf{d}_n$ s koeficienty $x_1, \ldots, x_n$.
Obráceně, je-li $\mathbf{b}$ lineární kombinací $\mathbf{d}_1, \ldots, \mathbf{d}_n$, pak koeficienty této kombinace jsou složkami vektoru řešení této soustavy.

Věta 5.6 (Frobeniova)

Nehomogenní soustava lineárních rovnic $A\mathbf{x} = \mathbf{b}$ je řešitelná tehdy a jen tehdy, je-li $h(A) = h((A, \mathbf{b}))$.

Důkaz. Dle důsledku Věty 5.4 je hodnost matice rovna počtu lineárně nezávislých sloupců této matice. Označme $\mathbf{d}_1, \ldots, \mathbf{d}_n$ sloupcové vektory matice A. Je-li $A\mathbf{x} = \mathbf{b}$ řešitelná, je dle Věty 5.5 $h(A) = \dim[\{\mathbf{d}_1, \ldots, \mathbf{d}_n\}] = \dim[\{\mathbf{d}_1, \ldots, \mathbf{d}_n, \mathbf{b}\}] = h((A, \mathbf{b}))$. Obráceně, nechť $h(A) = h((A, \mathbf{b}))$. Pak $\dim[\{\mathbf{d}_1, \ldots, \mathbf{d}_n\}] = \dim[\{\mathbf{d}_1, \ldots, \mathbf{d}_n, \mathbf{b}\}]$. Jelikož $[\{\mathbf{d}_1, \ldots, \mathbf{d}_n\}]$ je zřejmě podprostor prostoru $[\{\mathbf{d}_1, \ldots, \mathbf{d}_n, \mathbf{b}\}]$, platí dle Věty 2.13

$$[\{\mathbf{d}_1, \ldots, \mathbf{d}_n\}] = [\{\mathbf{d}_1, \ldots, \mathbf{d}_n, \mathbf{b}\}],$$

tedy $\mathbf{b} \in [\{\mathbf{d}_1, \ldots, \mathbf{d}_n\}]$, t.j. dle Věty 2.5 je $\mathbf{b}$ lineární kombinací $\mathbf{d}_1, \ldots, \mathbf{d}_n$. Podle Věty 5.5 je tedy $A\mathbf{x} = \mathbf{b}$ řešitelná.

Věta 5.7

Nechť $A\mathbf{x} = \mathbf{b}$, $B\mathbf{x} = \mathbf{c}$ jsou dvě soustavy (nehomogenní) lineárních rovnic o n neznámých nad T. Je-li $(A, \mathbf{b}) \sim (B, \mathbf{c})$, pak jsou tyto soustavy ekvivalentní.

Důkaz. Matice jsou řádkově ekvivalentní, lze-li jednu získat z druhé konečným počtem elementáních transformací. Prověříme tedy tvrzení pro jednotlivé typy elementárních transformací.

(i) Je zřejmé, že záměnnou řádků se jen změní pořadí rovnic v soustavě, tedy množina řešení je stejná.

(ii) Násobíme-li k-tý řádek matice $(A, \mathbf{b})$ číslem $c \in T, c \neq 0$, změní se k-tá rovnice $\sum_{i=1}^{n} a_{ki} x_i = b_k$ na rovnici $c \cdot \sum a_{ki} x_i = c \cdot b_k$, která má zřejmě stejnou množinu řešení jako rovnice původní, t.j. množina řešení soustavy se nezmění.

(iii) Přičteme ke k-tému řádku matice $(A, \mathbf{b})$ j-tý řádek. Původní soustava $A\mathbf{x} = \mathbf{b}$ měla k-tou rovnici $\sum_{i=1}^{n} a_{ki}x_i = b_k$, v nové soustavě to bude rovnice $\sum_{i=1}^{n} a_{ki}x_i + \sum_{i=1}^{n} a_{ji}x_i = b_k + b_j$. Nechť $\mathbf{u} = (u_1, \ldots, u_n)$ je řešením $A\mathbf{x} = \mathbf{b}$. Pak platí $\sum_{i=1}^{n} a_{pi}u_i = b_p$ pro každé $p = 1, \ldots, m$, a proto také

$$\sum_{i=1}^{n} a_{ki}u_i + \sum_{i=1}^{n} a_{ji}u_i = b_k + b_j,$$

tedy $\mathbf{u}$ je i řešením upravené soustavy.

Obráceně, nechť $\mathbf{v} = (v_1, \ldots, v_n)$ je řešením upravené soustavy. Pak $\sum_{i=1}^{n} a_{ki}v_i + \sum_{i=1}^{n} a_{ji}v_i = b_k + b_j$, ale tato soustava obsahuje i j-tou rovnici (shodnou s původní), t.j. $\sum_{i=1}^{n} a_{ji}v_i = b_j$. Odtud $\sum_{i=1}^{n} a_{ki}v_i = (\sum_{i=1}^{n} a_{ki}v_i + \sum_{i=1}^{n} a_{ji}v_i) - \sum_{i=1}^{n} a_{ji}v_i = (b_k + b_j) - b_j = b_k$, tedy $\mathbf{v}$ je i řešením rovnice $\sum_{i=1}^{n} a_{ki}x_i = b_k$ a tedy i řešením původní soustavy.

Tedy jak soustava $A\mathbf{x} = \mathbf{b}$, tak soustava, jejíž matice je řádkově ekvivalentní s $(A, \mathbf{b})$ mají stejné množiny řešení, t.j. jsou ekvivalentní.

Na základě Věty 5.7 je založena tzv. **Gaussova eliminační metoda.** Nechť $A\mathbf{x} = \mathbf{b}$ je soustava m lineárních rovnic o n neznámých, jejíž rozšířená matice $(A, \mathbf{b})$ je:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}.$$

Předpokládejme, že $a_{11} \neq 0$ (kdyby $a_{11} = 0$, lze dle Věty 5.7. zaměnit řádky – rovnice tak, až bude levý horní prvek nenulový). Pro každé $k = 2, \dots, m$ přičteme ke k-tému řádku $(-\frac{a_{k1}}{a_{11}})$-násobek 1. řádku této matice. Ve vzniklé matici jsou všechny prvky 1. sloupce s výjimkou 1. řádku rovny 0. Pochopitelně lze ze soustavy vypustit všechny nulové řádky (řádky obsahující samé 0). Matice (získaná zřejmě elementárními řádkovými transformacemi) vypadá takto:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ 0 & a'_{22} & \dots & a'_{2n} & b'_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & a'_{r2} & \dots & a'_{rn} & b'_r \end{pmatrix},$$

kde $r \leq m$.

Nyní celý postup opakujeme (s dílčí maticí). Předpokládáme, že $a'_{22} \neq 0$ (jinak zaměníme řádky, jsou-li všechny $a'_{22} = \cdots = a'_{r2} = 0$, přejdeme rovnou ke 3. sloupci). Pro každé $j = 3, \ldots, r$ přičteme k j-tému řádku $(-\frac{a'_{j2}}{a'_{22}})$-násobek 2. řádku. Opět vynecháme nulové řádky. Získáme matici

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} & b_1 \\ 0 & a'_{22} & a'_{23} & \ldots & a'_{2n} & b'_2 \\ 0 & 0 & a''_{33} & \ldots & a''_{3n} & b''_3 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & a''_{s3} & \ldots & a''_{sn} & b''_s \end{pmatrix},$$

kde $s \leq r$. Takto pokračujeme dále, až nakonec získáme matici:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} & b_1 \\ 0 & a'_{22} & a'_{23} & \ldots & a'_{2n} & b'_2 \\ 0 & 0 & a''_{33} & \ldots & a''_{3n} & b''_3 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots c_{hh} \ldots & c_{hn} & d_h \end{pmatrix},$$

kde $h \leq n$, $h = h(A)$ a všechny prvky $a_{11}, a'_{22}, a''_{33}, \ldots, c_{hh}$ na hlavní diagonále jsou nenulové.

Z rovnice $c_{hh}x_h + \cdots + c_{hn}x_n = d_h$, která odpovídá poslednímu řádku, vyjádříme x_h pomocí $x_{h+1}, \ldots, x_n$. Z předposlední rovnice vypočítáme x_{h-1}, atd., až z 1. rovnice vypočítáme x_1.

Je zřejmé, že pokud $h = n$, má soustava jediné řešení, je-li $h < n$, pak má nekonečně mnoho řešení závislých na parametrech $x_{h+1}, \ldots, x_n$ (za tyto parametry lze volit libovolná čísla z T). Tedy:

Věta 5.8 (Frobeniova)

Nechť $A\mathbf{x} = \mathbf{b}$ je soustava m rovnic o n neznámých nad tělesem T. Tato soustava má řešení právě když $h(A) = h((A, \mathbf{b}))$. Je-li $h(A) = n$, soustava má jediné řešení. Je-li $h(A) = h < n$, soustava má nekonečně mnoho řešení závislých na $n - h$ parametrech.

Příklad

Řešte soustavu

$$\begin{aligned} 3x_1 - 5x_2 + 2x_3 + 4x_4 &= 2 \\ 7x_1 - 4x_2 + x_3 + 3x_4 &= 5 \\ 5x_1 + 7x_2 - 4x_3 - 6x_4 &= 3. \end{aligned}$$

Řešení. Rozšířená matice soustavy je

$$\begin{pmatrix} 3 & -5 & 2 & 4 & 2 \\ 7 & -4 & 1 & 3 & 5 \\ 5 & 7 & -4 & -6 & 3 \end{pmatrix} \sim \begin{pmatrix} 7 & -4 & 1 & 3 & 5 \\ -11 & 3 & 0 & -2 & -8 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Zřejmě tedy $h(A) = 2$, $h((A, \mathbf{b})) = 3$, tedy soustava nemá řešení.

Příklad

Řešte soustavu

$$\begin{aligned} x_1 + 2x_2 + 5x_3 &= -9 \\ x_1 - x_2 + 3x_3 &= 2 \\ 3x_1 - 6x_2 - x_3 &= 25. \end{aligned}$$

Řešení. Pomocí Gaussovy eliminační metody upravíme $(A, \mathbf{b})$:

$$\left(\begin{array}{cccc} 1 & 2 & 5 & -9 \\ 1 & -1 & 3 & 2 \\ 3 & -6 & -1 & 25 \end{array}\right) \sim \left(\begin{array}{cccc} 1 & 2 & 5 & -9 \\ 0 & -3 & -2 & 11 \\ 0 & -12 & -16 & 52 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc} 1 & 2 & 5 & -9 \\ 0 & 3 & 2 & -11 \\ 0 & 3 & 4 & -13 \end{array}\right) \sim \left(\begin{array}{cccc} 1 & 2 & 5 & -9 \\ 0 & 3 & 2 & -11 \\ 0 & 0 & 2 & -2 \end{array}\right).$$

Zřejmě $h(A) = h((A, \mathbf{b})) = 3$, tedy soustava má jediné řešení. Z poslední rovnice: $x_3 = -1$, z předposlední pak: $x_2 = -3$ a následně z první: $x_1 = 2$, tedy soustava má řešení $(2, -3, -1)$.

Další metodou řešení soustavy je:

Věta 5.9 (Cramerovo pravidlo)

Nechť $A\mathbf{x} = \mathbf{b}$ je soustava n lineárních rovnic o n neznámých ($n \geq 1$) nad T taková, že $\det A \neq 0$. Pak pro $j = 1, \ldots, n$ platí $x_j = \frac{\det A_j}{\det A}$, kde A_j je matice, která vznikne z A tak, že j-tý sloupec nahradíme vektorem $\mathbf{b}$.

Důkaz. Vynásobíme-li 1. rovnici algebraickým doplňkem $\mathscr{A}_{1j}$ prvku a_{1j}, 2. rovnici doplňkem $\mathscr{A}_{2j}$ prvku a_{2j}, atd., až n-tou rovnici doplňkem $\mathscr{A}_{nj}$ prvku a_{nj} a rovnice sečteme, dostaneme rovnici: $L = \sum_{i=1}^{n} \mathscr{A}_{ij} \sum_{k=1}^{n} a_{ik} x_k = \sum_{i=1}^{n} b_i \mathscr{A}_{ij} = P$. Pak lze L upravit: $L = \sum_{k=1}^{n} x_k \sum_{i=1}^{n} a_{ik} \mathscr{A}_{ij}$. Pro $k \neq j$ je člen $\sum a_{ik} \mathscr{A}_{ij} = 0$, tedy dle Laplaceovy věty: $L = x_j \det A$. Dále, dle Laplaceovy věty platí $P = \det A_j$, tedy $x_j \det A = \det A_j$.

Věta 5.10

Nechť $A\mathbf{x} = \mathbf{o}$ je homogenní soustava lineárních rovnic o n neznámých nad T, nechť $h(A) = h$. Pak všechna řešení této soustavy tvoří podprostor v aritmetickém vektorovém prostoru T^n. Dimenze tohoto podprostoru je $n - h$.

Důkaz. Protože homogenní soustava má vždy aspoň triviální řešení $\mathbf{o} = (0, \ldots, 0)$, je její množina řešení neprázdná. Nechť $\mathbf{u}, \mathbf{v}$ jsou řešení soustavy, t.j. $A\mathbf{u} = \mathbf{o}$, $A\mathbf{v} = \mathbf{o}$, pak $A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = \mathbf{o}$. Dále pro $c \in T$ je $A(c\mathbf{u}) = (Ac)\mathbf{u} = (cA)\mathbf{u} = c(A\mathbf{u}) = \mathbf{o}$, tedy množina všech řešení soustavy $A\mathbf{x} = \mathbf{o}$ je uzavřena na lineární kombinace, je tedy podprostorem T^n.

Nechť je $h(A) = h$. Pak má dle Věty 5.8 řešení závislé na $n - h$ parametrech. Je-li $h = n$, má jediné řešení, t.j. $\mathbf{o} = (0, \ldots, 0)$, ale $\{\mathbf{o}\}$ je zřejmě podprostor T^n dimenze $0 = h - n$. Je-li $h < n$, volme parametry $x_{h+1}, \ldots, x_n$ postupně takto:

$$x_{h+1} = 1, x_{h+2} = 0, \ldots, x_n = 0$$
$$x_{h+1} = 0, x_{h+2} = 1, \ldots, x_n = 0$$
$$\ldots$$
$$x_{h+1} = 0, x_{h+2} = 0, \ldots, x_n = 1.$$

Pro každou volbu parametrů $x_{h+1}, \ldots, x_n$ dostaneme hodnoty $x_1, \ldots, x_h$, tedy pro výše uvedené hodnoty parametrů získáme řešení:

$$\mathbf{u}_1 = (u_{11}, u_{12}, \ldots, u_{1h}, 1, 0, \ldots, 0)$$
$$\mathbf{u}_2 = (u_{21}, u_{22}, \ldots, u_{2h}, 0, 1, \ldots, 0)$$
$$\ldots$$
$$\mathbf{u}_{n-h} = (u_{n-h,1}, u_{n-h,2}, \ldots, u_{n-h,h}, 0, 0, \ldots, 1).$$

Jelikož $h(A) = h$, jsou $(u_{11}, \ldots, u_{1h}), \ldots, (u_{n-h,1}, \ldots, u_{n-h,h})$ lineárně nezávislé. Tedy dimenze podprostoru řešení je $\geq n - h$. Avšak každé další řešení je lineární kombinací těchto, tedy dimenze je rovna $n - h$.

Definice

Fundamentálním systémem řešení homogenní soustavy lineárních rovnic rozumíme libovolnou bázi prostoru řešení této soustavy.

Poznámka.

(a) Protože každá báze generuje tento podprostor, je fundamentálním řešením určena celá množina řešení homogenní soustavy.

(b) Příkladem fundamentálního systému řešení je množina $\mathbf{u}_1, \ldots, \mathbf{u}_{n-h}$ z předchozího důkazu.

(c) Je-li matice soustavy $A\mathbf{x} = \mathbf{o}$ čtvercová, pak má tato homogenní soustava jen triviální (t.j. nulové) řešení právě když $\det A \neq 0$.

Příklad

Určete fundamentální systém řešení soustavy:

$$\begin{array}{rrrrrl} x_1 & +2x_2 & -x_3 & +3x_4 & -2x_5 & =0 \\ 2x_1 & +x_2 & & +x_4 & -3x_5 & =0 \\ 5x_1 & +4x_2 & -x_3 & +5x_4 & -8x_5 & =0 \\ & 3x_2 & -2x_3 & +5x_4 & -x_5 & =0. \end{array}$$

Řešení. Matici soustavy upravíme:

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

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

Tedy $h(A) = 2$ a řešení bude záviset na 3 parametrech.

Příklad – dokončení

Za parametry zvolme například x_1, x_2, x_5. Pak z prvních dvou rovnic odvodíme snadno obecné řešení:

$$\begin{aligned} x_4 &= -2x_1 - x_2 + 3x_5 \\ x_3 &= -5x_1 - x_2 + 7x_5. \end{aligned}$$

Fundamentální systém řešení získáme (dle důkazu Věty 5.10) například tak, že budeme postupně volit:

x_1	x_2	x_5
1	0	0
0	1	0
0	0	1

.

Pak fundamentálním systémem řešení je:

$$\mathbf{u}_1 = (1,0,-5,-2,0), \mathbf{u}_2 = (0,1,-1,-1,0), \mathbf{u}_3 = (0,0,7,3,1).$$

Definice

Nechť $A\mathbf{x} = \mathbf{b}$ je nehomogenní soustava lineárních rovnic. Homogenní soustavu $A\mathbf{x} = \mathbf{o}$ nazveme **soustava přiřazená k** $A\mathbf{x} = \mathbf{b}$.

Věta 5.11

Nechť $A\mathbf{x} = \mathbf{b}$ je nehomogenní soustava lineárních rovnic, nechť $\mathbf{u}$ je některé její řešení. Pak množina všech řešení této soustavy je tvořena právě všemi vektory $\mathbf{u} + \mathbf{v}$, kde $\mathbf{v}$ je libovolné řešení přiřazené homogenní soustavy.

Důkaz. Jestliže platí $A\mathbf{v} = \mathbf{o}$, pak platí $A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = \mathbf{b} + \mathbf{o} = \mathbf{b}$, tedy $\mathbf{u} + \mathbf{v}$ je řešením $A\mathbf{x} = \mathbf{b}$. □

Tedy, známe-li jediné řešení nehomogenní soustavy a všechna řešení přiřazené homogenní soustavy (t.j. například fundamentální systém řešení této soustavy), pak známe všechna řešení i původní nehomogenní soustavy.

Obsah

Podle Věty 3.2 tvoří množina $\mathscr{M}_n(T)$ všech čtvercových matic nad tělesem T okruh, který pro $n > 1$ není komutativní a obsahuje dělitele nuly. Budeme blíže zkoumat vlastnosti tohoto okruhu.

Definice

Matice $A \in \mathscr{M}_n(T)$ se nazývá **regulární**, je-li $\det A \neq 0$. Matice A je **singulární**, je-li $\det A = 0$.

Definice

Jestliže $A \in \mathscr{M}_n(T)$ a existuje $B \in \mathscr{M}_n(T)$ tak, že $AB = E = BA$, pak se B nazývá **inverzní matice** k A a značí se $B = A^{-1}$.

Věta 6.1

K matici $A \in \mathscr{M}_n(T)$ existuje matice inverzní, právě když A je regulární.

Důkaz. (a) Je-li A singulární, t.j. $\det A = 0$, pak existuje-li inverzní matice A^{-1}, je $A \cdot A^{-1} = E$, t.j.
$0 = \det A \cdot \det A^{-1} = \det A \cdot A^{-1} = \det E = 1$, spor.
(b) Nechť $A = \|a_{ij}\|$ je regulární, t.j. $\det A \neq 0$. Je-li $\mathscr{A}_{ij}$ algebraický doplněk prvku a_{ij}, pak dle Laplaceovy věty platí:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} \mathscr{A}_{11} & \mathscr{A}_{21} & \dots & \mathscr{A}_{n1} \\ \mathscr{A}_{12} & \mathscr{A}_{22} & \dots & \mathscr{A}_{n2} \\ \vdots & \vdots & & \vdots \\ \mathscr{A}_{1n} & \mathscr{A}_{2n} & \dots & \mathscr{A}_{nn} \end{pmatrix} = \begin{pmatrix} \det A & 0 & \dots & 0 \\ 0 & \det A & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \det A \end{pmatrix}$$

$= \det A \cdot E$. Snadno ověříme, že i při obráceném pořadí těchto matic je jejich součin roven $\det A \cdot E$, tedy inverzní matice k A existuje a je to matice

$$\frac{1}{\det A} \cdot \begin{pmatrix} \mathscr{A}_{11} & \mathscr{A}_{21} & \dots & \mathscr{A}_{n1} \\ \vdots & \vdots & & \vdots \\ \mathscr{A}_{1n} & \mathscr{A}_{2n} & \dots & \mathscr{A}_{nn} \end{pmatrix}.$$

Věta 6.2

Množina všech regulárních čtvercových matic stupně n tvoří grupu vzhledem k násobení.

Důkaz. Dle Věty 3.3 je násobení matic asociativní a je-li $\det A \neq 0 \neq \det B$, pak $\det AB = \det A \cdot \det B \neq 0$, t.j. součin regulárních matic je regulární matice. Dále E je jednotka a dle Věty 6.1 existuje ke každé regulární čtvercové matici matice inverzní (zřejmě také regulární), tedy množina všech regulárních čtvercových matic stupně n tvoří grupu vzhledem k násobení.

Důsledek

Jestliže $A, B \in \mathscr{M}_n(T)$ jsou regulární, pak $(AB)^{-1} = B^{-1}A^{-1}$.

Důkaz. $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AEA^{-1} = AA^{-1} = E$, t.j. $B^{-1}A^{-1}$ je inverzní k AB, t.j. $(AB)^{-1} = B^{-1}A^{-1}$.

Příklad

Určete inverzní matici k matici $A = \begin{pmatrix} 2 & -1 & 3 \\ 1 & -1 & -2 \\ -3 & 2 & 1 \end{pmatrix}$.

Řešení. Zřejmě $\det A = -2$. Určíme všechny alg. doplňky:

$$\mathscr{A}_{11} = \begin{vmatrix} -1 & -2 \\ 2 & 1 \end{vmatrix} = 3,\ \mathscr{A}_{12} = -\begin{vmatrix} 1 & -2 \\ -3 & 1 \end{vmatrix} = 5,$$

$$\mathscr{A}_{13} = \begin{vmatrix} 1 & -1 \\ -3 & 2 \end{vmatrix} = -1,\ \mathscr{A}_{21} = -\begin{vmatrix} -1 & 3 \\ -2 & 1 \end{vmatrix} = 7,$$

$$\mathscr{A}_{22} = \begin{vmatrix} 2 & 3 \\ -3 & 1 \end{vmatrix} = 11,\ \mathscr{A}_{23} = -\begin{vmatrix} 2 & -1 \\ -3 & 2 \end{vmatrix} = -1,$$

$$\mathscr{A}_{31} = \begin{vmatrix} -1 & 3 \\ -1 & -2 \end{vmatrix} = 5,\ \mathscr{A}_{32} = -\begin{vmatrix} 2 & 3 \\ 1 & -2 \end{vmatrix} = 7,$$

$\mathscr{A}_{33} = \begin{vmatrix} 2 & -1 \\ 1 & -1 \end{vmatrix} = -1$. Tedy (dle důkazu Věty 6.1):

$$A^{-1} = -\tfrac{1}{2} \cdot \begin{pmatrix} 3 & 7 & 5 \\ 5 & 11 & 7 \\ -1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{3}{2} & -\frac{7}{2} & -\frac{5}{2} \\ -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Ukážeme si jednodušší způsob výpočtu inverzní matice. Je-li A regulární čtvercová matice, pak lze dle Věty 5.2 převést A pomocí elementárních řádkových transformací na jednotkovou matici E. Platí:

Věta 6.3

Je-li $A \in \mathscr{M}_n(T)$ regulární, pak je možné konečnou posloupností $t_1, t_2, \ldots, t_k$ elementárních řádkových transformací převést A na jednotkovou matici E, přičemž pomocí téže posloupnosti $t_1, t_2, \ldots, t_k$ lze E převést na A^{-1}.

Důkaz. Dle Věty 5.2 je A řádkově ekvivalentní s E neboť $h(A) = n$. Tedy existuje posloupnost $t_1, t_2, \ldots, t_k$ elementárních řádkových transformací převádějících A na E. Každé elementární řádkové transformaci lze přiřadit matici:

(i) násobíme-li BA, kde

$$B = \begin{pmatrix} 1 & & & & & & & & & \\ & \ddots & & & & & & & N & \\ & & 1 & & & & & & & \\ & & & 0 & & \cdots & & 1 & & \\ & & & & 1 & & & & & \\ & & & \vdots & & \ddots & & \vdots & & \\ & & & & & & 1 & & & \\ & & & 1 & & \cdots & & 0 & & \\ & & & & & & & & 1 & \\ & & & & & & & & & \ddots \\ & & N & & & & & & & \\ & & & & & & & & & 1 \end{pmatrix},$$

pak BA má vyměněný i-tý řádek s j-tým řádkem matice A.

(ii) násobíme-li BA, kde

$$B = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & N & \\ & & & c & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & N & & & & & \\ & & & & & & 1 \end{pmatrix},$$

pak BA má vynásobený i-tý řádek matice A číslem c, ostatní řádky shodné s A.

(iii) násobíme-li BA, kde

$$B = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & N & \\ & & 1 & \cdots & 1 & & \\ & & & \ddots & \vdots & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & N & & & & & 1 \end{pmatrix},$$

pak BA má i-tý řádek součet i-tého a j-tého řádku matice A, ostatní řádky shodné s A.

Jestliže tedy $t_1, t_2, \ldots, t_k$ transformuje A na E, pak $t_i \to B_j$ (matice transformace) a platí $E = B_1 B_2 \ldots B_k A$. Pak ale

$$A^{-1} = EA^{-1} = B_1 B_2 \ldots B_k A A^{-1} = B_1 B_2 \ldots B_k E,$$

tedy A^{-1} vznikne z E stejnou posloupností elementárních řádkových transformací.

Příklad

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

Řešení. Napíšeme vedle sebe matice A, E a budeme na obou provádět tytéž transformace. Poté, co A převedeme na E, bude E převedeno na A^{-1}:

$$\left(\begin{array}{ccc|ccc} 2 & -1 & 3 & 1 & 0 & 0 \\ 1 & -1 & -2 & 0 & 1 & 0 \\ -3 & 2 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & -1 & -2 & 0 & 1 & 0 \\ 0 & 1 & 7 & 1 & -2 & 0 \\ 0 & -1 & -5 & 0 & 3 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & -1 & -2 & 0 & 1 & 0 \\ 0 & 1 & 7 & 1 & -2 & 0 \\ 0 & 0 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & -1 & -2 & 0 & 1 & 0 \\ 0 & 1 & 0 & -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ 0 & 0 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & -2 & -\frac{5}{2} & -\frac{9}{2} & -\frac{7}{2} \\ 0 & 1 & 0 & -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ 0 & 0 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{3}{2} & -\frac{7}{2} & -\frac{5}{2} \\ 0 & 1 & 0 & -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ 0 & 0 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right).$$

Tedy $A^{-1} = -\frac{1}{2} \cdot \begin{pmatrix} 3 & 7 & 5 \\ 5 & 11 & 7 \\ -1 & -1 & -1 \end{pmatrix}$.

Obsah

Definice

Nechť $\mathscr{V}_1 = (V_1, +, T, \cdot)$ a $\mathscr{V}_2 = (V_2, +, T, \cdot)$ jsou vektorové prostory nad tělesem T. Zobrazení $f : V_1 \to V_2$ nazýváme **homomorfismus (lineární zobrazení) vektorového prostoru $\mathscr{V}_1$ do vektorového prostoru $\mathscr{V}_2$**, jestliže

(i) $\forall \mathbf{u}, \mathbf{v} \in V_1$ platí $f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v})$

(ii) $\forall c \in T, \forall \mathbf{u} \in V_1$ platí $f(c\mathbf{u}) = cf(\mathbf{u})$.

Bijektivní homomorfismus $\mathscr{V}_1$ na $\mathscr{V}_2$ se nazývá **izomorfismus**. Řekneme, že vektorový prostor $\mathscr{V}_1$ je **izomorfní** s $\mathscr{V}_2$, jestliže existuje izomorfismus $\mathscr{V}_1$ na $\mathscr{V}_2$.

Přímo z definice je zřejmé, že je-li h homomorfismus $\mathscr{V}_1$ do $\mathscr{V}_2$, pak libovolné lineární kombinaci vektorů z $\mathscr{V}_1$ přiřadí tutéž lineární kombinaci jejich obrazů ve $\mathscr{V}_2$.

Věta 7.1

Nechť $\mathscr{V}_1, \mathscr{V}_2, \mathscr{V}_3$ jsou vektorové prostory nad T a nechť $h_1 : \mathscr{V}_1 \to \mathscr{V}_2$, $h_2 : \mathscr{V}_2 \to \mathscr{V}_3$ jsou homomorfismy. Pak $h_1 \cdot h_2$ je homomorfismus z $\mathscr{V}_1$ do $\mathscr{V}_3$. Je-li $f : \mathscr{V}_1 \to \mathscr{V}_2$ izomorfismus, pak f^{-1} je izomorfismus z $\mathscr{V}_2$ na $\mathscr{V}_1$. Identické zobrazení id: $\mathscr{V}_1 \to \mathscr{V}_1$ je izomorfismus $\mathscr{V}_1$ na $\mathscr{V}_1$.

Důkaz. Jsou-li $h_1 : \mathscr{V}_1 \to \mathscr{V}_2$, $h_2 : \mathscr{V}_2 \to \mathscr{V}_3$ homomorfismy, pak $\forall \mathbf{u}, \mathbf{v} \in V_1, c \in T$ platí $h_1 \cdot h_2(\mathbf{u}+\mathbf{v}) = h_2(h_1(\mathbf{u})+h_1(\mathbf{v})) = h_2(h_1(\mathbf{u}))+h_2(h_1(\mathbf{v})) = h_1h_2(\mathbf{u})+h_1h_2(\mathbf{v})$ a dále $h_1h_2(c\mathbf{u}) = h_2(ch_1(\mathbf{u})) = c(h_2(h_1(\mathbf{u}))) = ch_1h_2(\mathbf{u})$, tedy h_1h_2 je homomorfismus z $\mathscr{V}_1$ do $\mathscr{V}_3$.

Je-li $f : \mathscr{V}_1 \to \mathscr{V}_2$ izomorfismus, pak f je bijekce, t.j. existuje $f^{-1} : \mathscr{V}_2 \to \mathscr{V}_1$. Nechť $\mathbf{u}', \mathbf{v}' \in \mathscr{V}_2$. Pak existují $\mathbf{u}, \mathbf{v} \in \mathscr{V}_1$ tak, že $f(\mathbf{u}) = \mathbf{u}'$, $f(\mathbf{v}) = \mathbf{v}'$. Tedy $f^{-1}(\mathbf{u}'+\mathbf{v}') = f^{-1}(f(\mathbf{u})+f(\mathbf{v})) = f^{-1}(f(\mathbf{u}+\mathbf{v})) = \mathbf{u}+\mathbf{v} = f^{-1}(\mathbf{u}')+f^{-1}(\mathbf{v}')$, analogicky $f^{-1}(c\mathbf{u}') = f^{-1}(cf(\mathbf{u})) = f^{-1}(f(c\mathbf{u})) = c\mathbf{u} = cf^{-1}(\mathbf{u}')$, tedy f^{-1} je homomorfismus. Jelikož je bijekce, je také izomorfismus $\mathscr{V}_2$ na $\mathscr{V}_1$.

Poslední tvrzení je zřejmé.

Definice

Nechť $f : \mathscr{V}_1 \to \mathscr{V}_2$ je homomorfismus. **Jádrem** f nazveme množinu $\mathrm{Ker} f = \{\mathbf{u} \in \mathscr{V}_1; f(\mathbf{u}) = \mathbf{o}\}$, kde $\mathbf{o}$ je nulový vektor ve $\mathscr{V}_2$.

Věta 7.2

Surjektivní homomorfismus $f : \mathscr{V}_1 \to \mathscr{V}_2$ je izomorfismus právě když $\mathrm{Ker} f = \{\mathbf{o}\}$, kde $\mathbf{o}$ je nulový vektor ve $\mathscr{V}_1$.

Důkaz. Jelikož $f : \mathscr{V}_1 \to \mathscr{V}_2$ je homomorfismus a surjekce, stačí dokázat, že f je injekce, abychom dokázali, že f je izomorfismus. Nechť $\mathrm{Ker} f = \{\mathbf{o}\}$ a nechť $\mathbf{u}, \mathbf{v} \in \mathscr{V}_1$. Jestliže $f(\mathbf{u}) = f(\mathbf{v})$, pak $f(\mathbf{u}) - f(\mathbf{v}) = \mathbf{o}$, ale $f(\mathbf{u}) - f(\mathbf{v}) = f(\mathbf{u} - \mathbf{v})$, tedy $\mathbf{u} - \mathbf{v} \in \mathrm{Ker} f = \{\mathbf{o}\}$, t.j. $\mathbf{u} - \mathbf{v} = \mathbf{o}$, odtud $\mathbf{u} = \mathbf{v}$, neboli f je injekce.

Obráceně, nechť f je injekce. Zřejmě pro $\mathbf{o}, \mathbf{u} \in \mathscr{V}_1$ platí $f(\mathbf{o}) = f(0 \cdot \mathbf{u}) = 0 \cdot f(\mathbf{u}) = \mathbf{o} \in \mathscr{V}_2$, tedy $\mathbf{o} \in \mathrm{Ker} f$ vždy. Jelikož f je injekce, má každý prvek jediný vzor, t.j. $\mathrm{Ker} f$ má jediný prvek. Dohromady $\mathrm{Ker} f = \{\mathbf{o}\}$.

Věta 7.3

Je-li $f : \mathscr{V}_1 \to \mathscr{V}_2$ izomorfismus a je-li $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ báze $\mathscr{V}_1$, pak $\{f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n)\}$ je báze $\mathscr{V}_2$.

Důkaz. Nechť $\mathbf{u}' \in \mathscr{V}_2$. Jelikož f je surjekce, existuje $\mathbf{u} \in \mathscr{V}_1$ tak, že $f(\mathbf{u}) = \mathbf{u}'$. Protože $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ je báze $\mathscr{V}_1$, existují $c_1, \ldots, c_n \in T$ tak, že $\mathbf{u} = c_1\mathbf{u}_1 + \cdots + c_n\mathbf{u}_n$. Tedy
$\mathbf{u}' = f(\mathbf{u}) = f(c_1\mathbf{u}_1 + \cdots + c_n\mathbf{u}_n) = c_1 f(\mathbf{u}_1) + \cdots + c_n f(\mathbf{u}_n)$. Neboli $\{f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n)\}$ generuje prostor $\mathscr{V}_2$. Zbývá dokázat, že $f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n)$ jsou lineárně nezávislé.
Nechť $d_1, \ldots, d_n \in T$ a předpokládejme

$$d_1 f(\mathbf{u}_1) + \cdots + d_n f(\mathbf{u}_n) = \mathbf{o}.$$

Pak $f(d_1\mathbf{u}_1 + \cdots + d_n\mathbf{u}_n) = \mathbf{o}$, tedy $d_1\mathbf{u}_1 + \cdots + d_n\mathbf{u}_n \in \mathrm{Ker} f$. Dle Věty 7.2 je $\mathrm{Ker} f = \{\mathbf{o}\}$, odtud $d_1\mathbf{u}_1 + \cdots + d_n\mathbf{u}_n = \mathbf{o}$. Ovšem $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ je báze $\mathscr{V}_1$, tedy vektory $\mathbf{u}_1, \ldots, \mathbf{u}_n$ jsou lineárně nezávislé, tedy $d_1 = \cdots = d_n = 0$. Neboli také $f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n)$ jsou lineárně nezávislé.

Příklad

Zobrazení $f : \mathbb{R}^2 \to \mathbb{R}^2$ dané předpisem

$$f_1((x_1, x_2)) = (2x_1 + x_2, x_1 + x_2)$$

je homomorfismus aritmetického vektorového prostoru $\mathbb{R}^2$ do $\mathbb{R}^2$.

Příklad

Zobrazení $f : \mathbb{R}^3 \to \mathbb{R}^3$ dané předpisem

$$f_2((x_1, x_2, x_3)) = (1, 1, 1)$$

není homomorfismus aritmetického vektorového prostoru $\mathbb{R}^3$ do $\mathbb{R}^3$.

Věta 7.4

Každý vektorový prostor nad T dimenze n je izomorfní s aritmetickým vektorovým prostorem T^n.

Důkaz. Nechť $\{\mathbf{u}_1,\ldots,\mathbf{u}_n\}$ je báze prostoru $\mathscr{V}$ nad T, nechť $f:\mathscr{V}\to T^n$ takové, že je-li $\mathbf{u}=c_1\mathbf{u}_1+\cdots+c_n\mathbf{u}_n$, pak $f(\mathbf{u})=(c_1,\ldots,c_n)$.

(a) Nechť $\mathbf{u},\mathbf{v}\in\mathscr{V}$, $c\in T$. Pak $\mathbf{v}=d_1\mathbf{u}_1+\cdots+d_n\mathbf{u}_n$ a platí $f(\mathbf{u}+\mathbf{v})=(c_1+d_1,c_2+d_2,\ldots,c_n+d_n)=$ $(c_1,\ldots,c_n)+(d_1,\ldots,d_n)=f(\mathbf{u})+f(\mathbf{v})$, $f(c\mathbf{u})=(cc_1,\ldots,cc_n)=c(c_1,\ldots,c_n)=cf(\mathbf{u})$, tedy f je homomorfismus.

(b) Jestliže $(c_1,\ldots,c_n)\in T^n$, pak $(c_1,\ldots,c_n)=f(c_1\mathbf{u}_1+\cdots+c_n\mathbf{u}_n)$, kde $\{\mathbf{u}_1,\ldots,\mathbf{u}_n\}$ je báze $\mathscr{V}$, tedy existuje $\mathbf{u}\in\mathscr{V}$, totiž $\mathbf{u}=c_1\mathbf{u}_1+\cdots+c_n\mathbf{u}_n$ tak, že $f(\mathbf{u})=(c_1,\ldots,c_n)$, t.j. f je surjekce.

(c) Jestliže $f(\mathbf{u})=(0,\ldots,0)=\mathbf{o}$, pak $\mathbf{u}=0\cdot\mathbf{u}_1+\cdots+0\cdot\mathbf{u}_n=\mathbf{o}$. Odtud $\mathrm{Ker}f=\{\mathbf{o}\}$ a dle Věty 7.2 je tedy f izomorfismus.

Důsledek

Každé dva vektorové prostory $\mathscr{V}_1, \mathscr{V}_2$ nad T, které jsou konečné dimenze jsou izomorfní tehdy a jen tehdy, mají-li stejnou dimenzi.

Důkaz. Je-li $\mathscr{V}_1$ dimenze n, $\mathscr{V}_2$ dimenze m, pak dle Věty 7.4 je $\mathscr{V}_1$ izomorfní s T^n a $\mathscr{V}_2$ s T^m. Je-li $n = m$, pak jsou oba izomorfní s T^n, a tedy jsou i navzájem izomorfní.

Obráceně, jsou-li $\mathscr{V}_1, \mathscr{V}_2$ izomorfní, pak dle Věty 7.3 mají báze o stejném počtu vektorů, tedy mají i stejnou dimenzi.

Definice

Nechť $\mathscr{V}$ je vektorový prostor nad T dimenze n, $M = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ je jeho báze. Nechť $\mathbf{u} \in \mathscr{V}$, $\mathbf{u} = c_1\mathbf{u}_1 + \cdots + c_n\mathbf{u}_n$. Potom koeficienty $c_1, \ldots, c_n$ nazýváme **souřadnice vektoru u vzhledem k bázi** M, což zapisujeme $\{\mathbf{u}\}_M = (c_1, \ldots, c_n)$.

Definice

Nechť $M_1 = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$, $M_2 = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ jsou dvě báze vektorového prostoru $\mathscr{V}$. Nechť $\{\mathbf{v}_i\}_{M_1} = (a_{i1}, \ldots, a_{in})$, $i = 1, \ldots, n$. Potom matici $A = \|a_{ij}\|$ nazýváme **matice přechodu od báze** M_1 **k bázi** M_2.

Věta 7.5

Jsou-li M_1, M_2 dvě báze vektorového prostoru $\mathscr{V}$ a A je matice přechodu od M_1 k M_2, pak $\forall \mathbf{u} \in \mathscr{V}$ platí $\{\mathbf{u}\}_{M_1} = \{\mathbf{u}\}_{M_2} \cdot A$.

Důkaz. Nechť $A = \|a_{ij}\|$, $M_1 = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$, $M_2 = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, $\{\mathbf{u}\}_{M_1} = (c_1, \ldots, c_n)$, $\{\mathbf{u}\}_{M_2} = (c'_1, \ldots, c'_n)$. Tedy
$\mathbf{u} = c_1\mathbf{u}_1 + \cdots + c_n\mathbf{u}_n = c'_1\mathbf{v}_1 + \cdots + c'_n\mathbf{v}_n$ a $\mathbf{v}_j = a_{j1}\mathbf{u}_1 + \cdots + a_{jn}\mathbf{u}_n$.
Odkud $\mathbf{u} = c'_1\mathbf{v}_1 + \cdots + c'_n\mathbf{v}_n = c'_1(a_{11}\mathbf{u}_1 + \cdots + a_{1n}\mathbf{u}_n) + c'_2(a_{21}\mathbf{u}_1 + \cdots + a_{2n}\mathbf{u}_n) + \cdots + c'_n(a_{n1}\mathbf{u}_1 + \cdots + a_{nn}\mathbf{u}_n)$, ale $\mathbf{u} = c_1\mathbf{u}_1 + \cdots + c_n\mathbf{u}_n$,

tedy $(c_1, \ldots, c_n) = (c'_1, \ldots, c'_n) \cdot \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$.

Věta 7.6

Jsou-li M_1, M_2, M_3 báze vektorového prostoru $\mathscr{V}$ a $A = \|a_{ij}\|$ je matice přechodu od M_1 k M_2, $B = \|b_{ij}\|$ je matice přechodu od M_2 k M_3, pak BA je matice přechodu od M_1 k M_3.

Důkaz. Nechť $M_1 = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}, M_2 = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}, M_3 = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$. Pak $\mathbf{v}_k = \sum_{j=1}^{n} a_{kj}\mathbf{u}_j$ $(k = 1, \ldots, n)$; $\mathbf{w}_i = \sum_{k=1}^{n} b_{ik}\mathbf{v}_k$ $(i = 1, \ldots, n)$, tedy $\mathbf{w}_i = \sum_{k=1}^{n} b_{ik}\mathbf{v}_k = \sum_{k=1}^{n} b_{ik} \sum_{j=1}^{n} a_{kj}\mathbf{u}_j = \sum_{j=1}^{n} (\sum_{k=1}^{n} b_{ik}a_{kj})\mathbf{u}_j$. Odtud plyne tvrzení, neboť $\sum_{k=1}^{n} b_{ik}a_{kj}$ jsou koeficienty matice BA.

Věta 7.7

Jsou-li M_1, M_2 báze vektorového prostoru $\mathscr{V}$ a je-li A matice přechodu od M_1 k M_2, pak A^{-1} je matice přechodu od M_2 k M_1.

Důkaz. Zřejmě matice přechodu od M_1 k M_1 je jednotková, t.j. E. Je-li B matice přechodu od M_2 k M_1, pak $BA = E = AB$, odtud $B = A^{-1}$.

Věta 7.8

Nechť $M = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ je báze vektorového prostoru $\mathscr{V}$, nechť A je regulární čtvercová matice stupně n. Pak $M' = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, kde $\mathbf{v}_i = a_{i1}\mathbf{u}_1 + \cdots + a_{in}\mathbf{u}_n$ $(i = 1, \ldots, n)$ je báze prostoru $\mathscr{V}$. Neboli, každá čtvercová regulární matice je maticí přechodu od jedné báze ke druhé.

Důkaz. Ukážeme, že vektory $\mathbf{v}_1, \ldots, \mathbf{v}_n$ jsou lineárně nezávislé. Předpokládejme $c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = \mathbf{o}$. Pak $\sum_{i=1}^n c_i(\sum_{j=1}^n a_{ij}\mathbf{u}_j) = \sum_{j=1}^n(\sum_{i=1}^n c_i a_{ij})\mathbf{u}_j = \mathbf{o}$. Protože M je báze, jsou $\mathbf{u}_1, \ldots, \mathbf{u}_n$ lineárně nezávislé, t.j.

$$\sum_{i=1}^{n} c_i a_{ij} = 0 \quad \text{pro každé} \quad j = 1, \ldots, n. \qquad (*)$$

Označme $A^{-1} = \|b_{ij}\|$. Násobme každou z rovností $(*)$ prvkem b_{jk}, tyto rovnosti sečtěme: $0 = \sum_{j=1}^n \sum_{i=1}^n c_i a_{ij} b_{jk} = \sum_{i=1}^n c_i(\sum_{j=1}^n a_{ij} b_{jk})$. Ale součin i-tého řádku A s k-tým řádkem A^{-1} je roven 1 pro $i = k$, a roven 0 pro $i \neq k$ (neboť $AA^{-1} = E$), t.j. $0 = \sum_{i=1}^n c_i(\sum_{j=1}^n a_{ij} b_{jk}) = c_k$, a to pro každé $k \in \{1, \ldots, n\}$. Tedy $\mathbf{v}_1, \ldots, \mathbf{v}_n$ jsou lineárně nezávislé. Dle Steinitzovy věty je tedy $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ báze $\mathscr{V}$.

Příklad

Určete matici A přechodu od báze
$M_1 = \{(2,3,1),(0,1,2),(1,2,1)\}$
k $M_2 = \{(3,5,2),(6,11,6),(-1,1,4)\}$ vektorového prostoru $\mathbb{R}^3$.

Řešení. Je $\mathbf{v}_i = a_{i1}\mathbf{u}_1 + a_{i2}\mathbf{u}_2 + a_{i3}\mathbf{u}_3$, $i = 1,2,3$. Dosadíme za $\mathbf{v}_1, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ a vyřešíme tuto lineární soustavu pro neznámé a_{11}, a_{12}, a_{13}. Pak dosadíme $\mathbf{v}_2, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$, řešíme $\rightarrow a_{21}, a_{22}, a_{23}$. Nakonec dosadíme $\mathbf{v}_3, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$, řešíme $\rightarrow a_{31}, a_{32}, a_{33}$. Např. pro $\mathbf{v}_1, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ máme $(A, \mathbf{b}) = \begin{pmatrix} 2 & 0 & 1 & 3 \\ 3 & 1 & 2 & 5 \\ 1 & 2 & 1 & 2 \end{pmatrix}$; řešení: $(1,0,1)$, t.j. $a_{11} = 1, a_{12} = 0, a_{13} = 1$. Analogicky pro $\mathbf{v}_2, \mathbf{v}_3$ (změníme vektor pravé strany); řešení $(2,1,2)$, respektive $(-1,2,1)$. Odtud $a_{21} = 2, a_{22} = 1, a_{23} = 2$;
$a_{31} = -1, a_{32} = 2, a_{33} = 1$, t.j. $A = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 2 \\ -1 & 2 & 1 \end{pmatrix}$ je matice přechodu od M_1 k M_2.

Příklad – pokračování

Určete vztah mezi souřadnicemi libovolného vektoru $\mathbf{u} \in \mathbb{R}^3$.

Řešení. Označme $\{\mathbf{u}\}_{M_1} = (x_1, x_2, x_3)$ a $\{\mathbf{u}\}_{M_2} = (x_1', x_2', x_3')$. Jelikož $\{\mathbf{u}\}_{M_1} = \{\mathbf{u}\}_{M_2} \cdot A$, platí:

$$\begin{aligned} x_1 &= x_1' + 2x_2' - x_3' \\ x_2 &= x_2' + 2x_3' \\ x_3 &= x_1' + 2x_2' + x_3'. \end{aligned}$$

Poznámka. Spočíteme-li inverzní matici k matici A, pak ze vztahu $\{\mathbf{u}\}_{M_2} = \{\mathbf{u}\}_{M_1} \cdot A^{-1}$ obdržíme:

$$\begin{aligned} x_1' &= -\frac{3}{2}x_1 - 2x_2 + \frac{5}{2}x_3 \\ x_2' &= x_1 + x_2 - x_3 \\ x_3' &= -\frac{1}{2}x_1 + \frac{1}{2}x_3. \end{aligned}$$

V následující části této sekce si doplníme (i trochu zopakujeme) některé užitečné pojmy a výsledky (tentokrát bez důkazů). Opřeme se přitom o doporučenou litaraturu:

- *Bican L.: Lineární algebra a geometrie. Praha, Academia, 2009.*
- *Bečvář J.: Lineární algebra. Praha, Matfyzpress, 2010.*

Definice

Buďte V a V' vektorové prostory nad tělesem T. Zobrazení f množiny V do množiny V' se nazývá **homomorfismus (lineární zobrazení)**, jestliže pro všechna $\mathbf{u}, \mathbf{v} \in V$, $r \in T$ platí

$$f(\mathbf{u}+\mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}),$$

$$f(r\mathbf{u}) = rf(\mathbf{u}).$$

Prostý (injektivní) homomorfismus se nazývá **monomorfismus**, surjektivní homomorfismus (zobrazení V na V') se nazývá **epimorfismus**. **Izomorfismus** je homomorfismus, který je současně monomorfismem a epimorfismem (prostý homomorfismus V na V'). Řekneme, že vektorové prostory V a V' jsou **izomorfní**, $V \cong V'$, jestliže existuje izomorfismus prostoru V na prostor V'. Homomorfismus f vektorového prostoru V do vektorového prostoru V' budeme značit symbolem $f : V \to V'$.

Definice

Buď $f : V \to V'$ homomorfismus vektorového prostoru V do vektorového prostoru V'. Podmnožinu $\mathrm{Ker} f = \{\mathbf{u} \in V; f(\mathbf{u}) = \mathbf{o}\}$ prostoru V nazýváme **jádrem homomorfismu** f a podmnožinu $\mathrm{Im} f = \{f(\mathbf{u}); \mathbf{u} \in V\} = f(V)$ prostoru V' nazýváme **obrazem homomorfismu** f.

Věta

Buď $f : V \to V'$ homomorfismus vektorového prostoru V do vektorového prostoru V'. Pak

(i) $\mathrm{Ker} f$ je podprostorem ve V, $\mathrm{Im} f$ je podprostorem ve V'

(ii) f je monomorfismus, právě když $\mathrm{Ker} f = \{\mathbf{o}\}$

(iii) f je epimorfismus, právě když $\mathrm{Im} f = V'$

(iv) f je izomorfismus, právě když $\mathrm{Ker} f = \{\mathbf{o}\}$ a $\mathrm{Im} f = V'$.

Příklad (Bečvář str. 101)

Zobrazení f prostoru $\mathbb{R}^2$ do prostoru $\mathbb{R}^3$, které vektoru $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$ přiřazuje vektor $f(\mathbf{x}) = (2x_1 + x_2, x_1 - 3x_2, -2x_1 - x_2) \in \mathbb{R}^3$, je homomorfismus.

Jádro Ker$f$ homomorfismu f je tvořeno všemi vektory $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$, pro které je $2x_1 + x_2 = 0$, $x_1 - 3x_2 = 0$, $-2x_1 - x_2 = 0$, tj. všemi řešeními této soustavy rovnic. Snadno se vypočte, že Ker$f$ obsahuje jen nulový vektor.

Obraz Imf homomorfismu f je tvořen všemi vektory $\mathbf{y} = (y_1, y_2, y_3) \in \mathbb{R}^3$, pro které existuje vektor $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$ vyhovující rovnicím $2x_1 + x_2 = y_1$, $x_1 - 3x_2 = y_2$, $-2x_1 - x_2 = y_3$, tj. všemi vektory (y_1, y_2, y_3), pro které je tato soustava rovnic řešitelná. Snadno se ukáže, že když je $y_3 = -y_1$, pak je možno ze zadaných čísel y_1, y_2 vypočítat neznámé x_1, x_2. Tedy Im$f = \{(y_1, y_2, y_3); y_3 = -y_1\} = [(1, 0, -1), (0, 1, 0)]$.

Příklad (Bečvář str. 102)

Zobrazení prostoru $\mathbb{R}^3$ do prostoru $\mathbb{R}^2$, která vektoru (x_1, x_2, x_3) přiřazují po řadě vektor $(0,1)$, $(x_1 + 3x_2, x_3 - 2)$, $(x_1^2, x_2 + x_3^2)$, $(x_2 - \sqrt{x_3}, x_1)$, $(x_1 \cdot x_2, x_3)$, (x_1, e^{x_2}) nejsou homomorfismy.

Příklad (Bečvář str. 102)

Nechť V je vektorový prostor všech vázaných vektorů prostoru, které mají společný počátek v pevně zvoleném bodě S.
Buď dána přímka p, která prochází bodem S. Otočení prostoru V kolem přímky p o pevný úhel α přirozeným způsobem určuje homomorfismus prostoru V do prostoru V. Jádro tohoto homomorfismu je triviální, obrazem je celý prostor V.
Nechť je dána rovina ρ, která prochází bodem S. Přiřadíme-li každému vektoru prostoru V jeho kolmou projekci na rovinu ρ, dostaneme homomorfismus prostoru V do prostoru V. Jádrem je množina všech vektorů prostoru V, které jsou kolmé k rovině ρ (leží na kolmé přímce k rovině ρ procházející bodem S). Obrazem je rovina ρ.

Příklad (Bečvář str. 102)

Nechť V je vektorový prostor všech funkcí, které jsou spojité na uzavřeném intervalu $\langle 0,1\rangle$. Zobrazení, které každé funkci $v \in V$ přiřazuje funkci w,

$$w(x) = \int_0^x v(t)dt, \quad x \in \langle 0,1\rangle,$$

je homomorfismus prostoru V do prostoru V.

Příklad (Bečvář str. 103)

Nechť V je vektorový prostor všech reálných funkcí definovaných na intervalu $(-\infty,\infty)$. Funkce v se nazývá **sudá**, resp. **lichá**, jestliže pro každé reálné číslo x platí $v(-x)=v(x)$, resp. $v(-x)=-v(x)$; tedy např. funkce sin je lichá a funkce cos je sudá. Snadno se ověří, že zobrazení f, které každé funkci $v\in V$ přiřazuje funkci w, $w(x)=\frac{1}{2}(v(x)+v(-x))$, je homomorfismus V do V a že Ker$f$ je množina všech lichých funkcí a Imf je množina všech sudých funkcí. Zobrazení g, které každé funkci $v\in V$ přiřazuje funkci w, $w(x)=\frac{1}{2}(v(x)-v(-x))$, je rovněž homomorfismus V do V; Ker$g$ je množina všech sudých funkcí a Imf množina všech lichých funkcí.

Věta

Nechť $f, h : V \to V'$ a $g : V' \to V''$ jsou homomorfismy vektorových prostorů a $r \in T$ buď libovolný prvek. Pak platí:

(i) zobrazení $fg : V \to V''$ definované $\forall \mathbf{u} \in V$ předpisem $(fg)(\mathbf{u}) = g(f(\mathbf{u}))$ je homomorfismus

(ii) zobrazení $f + h : V \to V'$ definované $\forall \mathbf{u} \in V$ předpisem $(f + h)(\mathbf{u}) = f(\mathbf{u}) + h(\mathbf{u})$ je homomorfismus

(iii) zobrazení $rf : V \to V'$ definované $\forall \mathbf{u} \in V$ předpisem $(rf)(\mathbf{u}) = rf(\mathbf{u})$ je homomorfismus.

Definice

Buďte $f, h : V \to V'$ a $g : V' \to V''$ homomorfismy vektorových prostorů. Homomorfismus $fg : V \to V''$ definovaný v předchozí větě se nazývá **součinem (složením)** homomorfismů f a g. **Součtem homomorfismů** f a h a **násobkem homomorfismu** f prvkem $r \in T$ rozumíme homomorfismy $f + h$, a rf z předchozí věty.

Příklad (Bečvář str. 108)

Zobrazení log prostoru $\mathbb{R}^+$ do prostoru $\mathbb{R}$, které každému kladnému reálnému číslu x přiřazuje číslo $\log_z x$, je izomorfismus prostoru $\mathbb{R}^+$ na prostor $\mathbb{R}$, neboť jde o bijekci a pro libovolně zvolená čísla $x, y \in \mathbb{R}^+$, $a \in \mathbb{R}$ platí

$$\log_z xy = \log_z x + \log_z y, \quad \log_z x^a = a \log_z x.$$

Prostory $\mathbb{R}^+$ a $\mathbb{R}$ jsou tedy izomorfní.

Příklad (Bečvář str. 108)

Zobrazení f prostoru $\mathbb{R}^3$ do prostoru $\mathbb{R}^2$, které vektoru (x, y, z) přiřazuje vektor $(x + y, 2y - z)$, je epimorfismus.

Příklad (Bečvář str. 108)

Zobrazení f prostoru $\mathbb{R}^3$ do prostoru $\mathbb{R}^4$, které vektoru (x,y,z) přiřazuje vektor $(x,x+y,x+y+z,x-y+2z)$, je monomorfismus.

Příklad (Bečvář str. 109)

Zobrazení f prostoru všech polynomů stupně nejvýše n nad tělesem T (n pevně zvoleno) do prostoru T^{n+1}, které každému polynomu $a_0 + a_1x + \cdots + a_nx^n$ přiřazuje $(n+1)$-tici $(a_0, a_1, \ldots, a_n)$ jeho koeficientů, je izomorfismus.

Věta

Nechť $f : V \to V'$ a $g : V' \to V''$ jsou homomorfismy vektorových prostorů. Pak platí:

(i) jsou-li f a g monomorfismy, je i fg monomorfismus

(ii) jsou-li f a g epimorfismy, je i fg epimorfismus

(iii) jsou-li f a g izomorfismy, je i fg izomorfismus

(iv) je-li fg monomorfismus, je i f monomorfismus

(v) je-li fg epimorfismus, je i g epimorfismus.

Věta

Buď $f : V^n \to V^m$ homomorfismus vektorového prostoru V^n (dimenze n) do vektorového prostoru V^m (dimenze m).
Pak $\dim \mathrm{Ker} f + \dim \mathrm{Im} f = n$.

Definice

Homomorfismus $f : V \to V$ vektorového prostoru V do V se nazývá **endomorfismus prostoru** V. V případě, že f je dokonce izomorfismus, hovoříme o **automorfismu prostoru** V.

Definice

Hodností $h(f)$ **homomorfismu** $f : V^n \to V^m$ rozumíme dimenzi obrazu Imf.

Věta

Buď M báze vektorového prostoru V^n (dimenze n), M' báze vektorového prostoru V^m (dimenze m) a buď A matice homomorfismu $f : V^n \to V^m$ vzhledem k bázím M a M'. Pak $h(f) = h(A)$.

Definice

Buď $A \in \mathscr{M}_n(T)$ čtvercová matice stupně n nad tělesem T. Polynom $f(\lambda) = \det(A - \lambda E)$ se nazývá **charakteristický polynom matice** A. Prvek $\lambda \in T$ takový, že $\det(A - \lambda E) = 0$ se nazývá **vlastní hodnota** matice A. V případě, že T je číselné těleso (např. těleso racionálních, reálných, komplexních čísel), pak místo vlastní hodnota obvykle říkáme **vlastní číslo**. Říkáme dále, že nenulový vektor $\mathbf{u} \in T^n$ je **vlastní vektor** matice A příslušný vlastní hodnotě λ, jestliže $A\mathbf{u}^T = \lambda\mathbf{u}^T$.

Buď $A \in \mathscr{M}_n(T)$ čtvercová matice stupně n nad tělesem T a buď $\mathbf{u} = (x_1, x_2, \ldots, x_n)$ vlastní vektor matice A příslušný vlastní hodnotě λ. To znamená, že platí rovnost $A\mathbf{u}^T = \lambda\mathbf{u}^T$, což rozepsáno ve složkách znamená

$$\begin{aligned}
(a_{11} - \lambda)x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0,\\
a_{21}x_1 + (a_{22} - \lambda)x_2 + \cdots + a_{2n}x_n &= 0,\\
&\vdots\\
a_{n1}x_1 + a_{n2}x_2 + \cdots + (a_{nn} - \lambda)x_n &= 0.
\end{aligned}$$

Vidíme tedy, že vlastní vektor $\mathbf{u}$ je řešením homogenní soustavy lineárních rovnic s maticí $A - \lambda E$. Uvědomme si, že tato soustava má netriviální řešení, právě když $\det(A - \lambda E) = 0$, tj. právě když λ je vlastní hodnota matice A.

Příklad

Určete vlastní čísla matice A nad $\mathbb{R}$, je-li $A = \begin{pmatrix} 4 & -2 \\ 1 & 1 \end{pmatrix}$.

Řešení. $\det(A - \lambda E) = \begin{vmatrix} 4-\lambda & -2 \\ 1 & 1-\lambda \end{vmatrix} = 0.$

Odtud $\lambda_1 = 2$, $\lambda_2 = 3$.

Obsah

Teorie grup

Grupa je algebraická struktura, která popisuje a formalizuje koncept symetrie. Matematická disciplína zabývající se studiem grup se nazývá teorie grup.
Teorie grup vznikla počátkem 19. století. U jejího zrodu stál matematik Évariste Galois, který dokázal, že polynomiální rovnice (stupně vyššího než 4) nelze obecně řešit pomocí odmocnin. Grupy našly později uplatnění také v geometrii, teorii čísel, algebraické topologii a dalších matematických oborech. Klasifikace jednoduchých konečných grup byla dokončena koncem 20. století a patří k největším výsledkům matematiky vůbec.

Teorie grup

Pojem grupy abstraktně popisuje či zobecňuje mnoho matematických objektů a má významné uplatnění i v příbuzných oborech – ve fyzice, informatice a chemii. Reprezentace grup hrají důležitou úlohu v teoriích jako jsou částicová fyzika, kvantová teorie pole anebo teorie strun. Chemie používá grupy pro popis symetrií molekul a krystalových mřížek v krystalografii. V informatice se grupy vyskytují například při zpracování obrazu, v kryptografii či kódování.
Konečné grupy symetrií, jako například Mathiovy grupy se využívají v kódování a v korekci chyb přenášených dat. Multiplikativní grupy konečných těles se využívají v cyklickém kódování, které se používá například v CD přehrávačích. Kryptografie kombinuje přístup abstraktní teorie grup s výpočetní teorií grup implementovanou pro konečné grupy.

Více například viz http://cs.wikipedia.org/wiki/Grupa.

Afinní prostor (Bican str. 128)

Lineární algebra má mnoho aplikací v geometrii. Nejjednodušší geometrickou strukturou je afinní prostor na který se nyní v krátkosti zaměříme. Idea tohoto pojmu spočívá na prostém faktu, že dva body určují jednoznačně vektor a naopak, „umístíme-li“ vektor do daného bodu, dostaneme jednoznačně určený „koncový“ bod.

Afinní prostor (Bican str. 128)

Definice

Afinním prostorem $A = A(V)$ nad vektorovým prostorem V (nad tělesem T) rozumíme trojici (A, V, f), kde A je neprázdná množina a $f : A \times V \to A$ je zobrazení splňující tyto dvě podmínky:

(a) $f(a,0) = a$, $f(f(a,\mathbf{u}),\mathbf{v}) = f(a,\mathbf{u}+\mathbf{v})$ pro všechna $a \in A$ a $\mathbf{u},\mathbf{v} \in V$;

(b) ke každé dvojici prvků $a,b \in A$ existuje právě jeden vektor $\mathbf{u} \in V$ tak, že $f(a,\mathbf{u}) = b$.

Dimenzí afinního prostoru $A(V)$ rozumíme dimenzi příslušného vektorového prostoru V, místo $A(V^n)$ budeme někdy používat kratší zápis A_n. Prvky množiny A se nazývají **body** příslušného afinního prostoru.

Afinní prostor (Bican str. 128)

Afinní prostor jsme definovali jako trojici (A, V, f). Protože jak zobrazení f, tak vektorový prostor V bývají zpravidla pevně dány, používáme pro afinní prostor zkrácené označení A.
V některých případech, zejména u zobrazení mezi afinními prostory, kde se mohou vyskytovat různé vektorové prostory (nad týmž tělesem, pochopitelně), pak používáme označení $A(V)$. Dále, zápis a vlastnosti zobrazení f jsou dosti těžkopádně zapisovatelné, a proto budeme místo $f(a, \mathbf{u})$ psát krátce $a + \mathbf{u}$. Při tomto způsobu zápisu dostávají podmínky $(a), (b)$ z předchozí definice tento tvar:

(a) $a + 0 = a$, $(a + \mathbf{u}) + \mathbf{v} = a + (\mathbf{u} + \mathbf{v})$ pro všechna $a \in A$ a $\mathbf{u}, \mathbf{v} \in V$;

(b) ke každé dvojici bodů $a, b \in A$ existuje právě jeden vektor $\mathbf{u} \in V$ tak, že $a + \mathbf{u} = b$. Pro tento jednoznačně určený vektor $\mathbf{u}$ můžeme tedy zvolit zápis $\mathbf{u} = b - a$.

Afinní prostor (Bican str. 128)

Přirozenost tohoto zápisu vysvitne z tohoto jednoduchého příkladu. Pro $A = V = \mathbb{R}^2$, kde $\mathbb{R}$ značí jako obvykle těleso reálných čísel, snadno ověříme, že zobrazení $f(a, \mathbf{u}) = a + \mathbf{u}$ definuje na množině A strukturu afinního prostoru. Přitom $a + \mathbf{u}$ značí obvyklé sčítání v aritmetickém vektorovém prostoru $\mathbb{R}^2$. Podmínky (a) a (b) v tomto případě neříkají nic jiného než vlastnost nulového vektoru, asociativní zákon pro sčítání a vlastnost opačného vektoru. Takže např. pro $a = (3, 5)$, $b = (7, 1)$, $\mathbf{u} = (4, 2)$ máme $a + \mathbf{u} = (7, 7)$ a $b - a = (4, -4)$.

Eukleidovské a projektivní prostory, Bican str. 148

Speciálním případem afinních prostorů jsou Eukleidovské prostory, které už trochu známe. Díky nim můžeme studovat tzv. metrické vlastnosti (vzdálenosti, úhly, atp.), což je umožněno přítomností skalárního součinu.

Afinní prostor A_n můžeme zkoumat také pomocí směrů v afinním prostoru o jednotku větší dimenze. Popis tohoto obecného postupu vynecháme. Zaměříme-li se na práci se směry ve vektorovém prostoru, mluvíme o tzv. projektivních prostorech.

Definice

Řekneme, že je dán n-rozměrný **projektivní prostor** $P_n(V^{n+1})$, je-li dáno:

(1) množina P_n;

(2) vektorový prostor V^{n+1};

(3) vzájemně jednoznačné zobrazení φ množiny $\{\langle \mathbf{u} \rangle \mid 0 \neq \mathbf{u} \in V^{n+1}\}$ na množinu P_n.

Prvky množiny P_n se nazývají **aritmetické body**. Vektorový prostor V^{n+1} se nazývá **aritmetický základ** prostoru P_n. Každý vektor $0 \neq \mathbf{u} \in V^{n+1}$ se nazývá **aritmetický zástupce** geometrického bodu $\varphi(\langle \mathbf{u} \rangle)$.

V projektivním prostoru $P_n(V^{n+1})$ tedy každému aritmetickému bodu $0 \neq \mathbf{u} \in V^{n+1}$ odpovídá jediný geometrický bod $\varphi(\langle \mathbf{u} \rangle)$, zatímco geometrické body mohou mít více aritmetických zástupců. Přitom je-li $\mathbf{u}$ jeden z nich, jsou všechny ostatní tvaru $r\mathbf{u}$, kde $0 \neq r \in T$. Například je-li V^{n+1} reálný vektorový prostor, má každý geometrický bod nekonečně mnoho aritmetických zástupců.

Definice

Je-li $M = \{\mathbf{u_0}, \mathbf{u_1}, \ldots, \mathbf{u_n}\}$ báze vektorového prostoru V^{n+1}, pak množinu M nazýváme **aritmetickou bází** projektivního podprostoru $P_n(V^{n+1})$. Je-li $0 \neq \mathbf{u} \in V^{n+1}$, pak $\{\mathbf{u}\}_M$ nazýváme **homogenními souřadnicemi** geometrického bodu $\langle \mathbf{u} \rangle$ vzhledem k bázi M.

Název homogenní souřadnice pochází z toho, že dva aritmetické vektory lišící se pouze násobkem, jsou homogenními souřadnicemi téhož geometrického bodu.

Počítačová grafika

Počítačová grafika je obor informatiky, který používá počítače k tvorbě umělých grafických objektů a dále také na úpravu zobrazitelných a prostorových informací, nasnímaných z reálného světa (například digitální fotografie a jejich úprava, filmové triky).
Nyní se podíváme jen stručně na malou část počítačové grafiky, která využívá násobení matic pro transformace objektů. Geometrické transformace mají pro počítačovou grafiku značný význam. Jejich aplikací na souřadnice bodů objektu jej můžeme různě měnit. Mezi lineární transformace řadíme například: změnu měřítka, zkosení, rotaci. Nelineární jsou například: posunutí, perspektivní projekce.
Aplikaci transformace na bod P s kartézskými souřadnicemi $[x, y, z]$ získáme bod P' o souřadnicích $[x', y', z']$. Transformace objektu znamená aplikaci operace transformace na všechny jeho body, případně i na parametry, kterými je popsán.

Homogenní souřadnice

Počítačová grafika potřebuje efektivně a jednotně popsat lineární i nelineární transformace. Zavedení homogenních souřadnic pro reprezentace bodů místo kartézských souřadnic práci se všemi transformacemi značně zjednodušuje. Homogenní souřadnice tvoří základ projektivní geometrie, použité převážně při projekci trojrozměrných scén do dvourozměrné roviny. Dále se zaměříme jen na vybrané transformace v 3D prostoru.

Hlavní rozdíl oproti kartézským souřadnicím spočívá v tom, že $n+1$ souřadnic bude reprezentovat n-rozměrný bod. Konkrétně v 3D bod nemá souřadnice 3, ale 4, tedy $P = [x, y, z, w]$. První tři souřadnice jsou opět kartézské, čtvrtá vyjadřuje tzv. váhu. Je-li váha bodu nenulová, mluvíme o tzv. vlastním bodu. Jinak se jedná o bod nevlastní. Bodu se obyčejně přiřazuje váha 1 a rozdíl dvou bodů (udávající vektor) má váhu 0. Základní operací pro homogenní souřadnice $[x', y', z', w]$ je jejich převod do kartézských souřadnic $[x, y, z]$: $x := \frac{x'}{w}$, $y := \frac{y'}{w}$, $z := \frac{z'}{w}$.

Afinní transformace

Tzv. afinními transformacemi homogenních souřadnic můžeme provádět jak lineární transformace, tak i některé nelineární transformace (např. posunutí). To ale není jediná výhoda. Důležitou vlastností z implementačního hlediska je možnost transformace skládat do jedné matice a výslednou složenou transformaci aplikovat na všechny body objektu pouze jednou. Skládání transformací je realizováno násobením jejich transformačních matic, přičemž záleží na jejich pořadí. Poznamenejme, že výpočetní přínos je značný, obzvlášť, máme-li miliony bodů všech objektů.
Dále uvedeme podoby transformačních matic k jednotlivým transformacím.
Posunutí o x, y, z:

$$\begin{pmatrix} 1 & 0 & 0 & x \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & z \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Afinní transformace

Změna měřítka:

$$\begin{pmatrix} s_x & 0 & 0 & 0 \\ 0 & s_y & 0 & 0 \\ 0 & 0 & s_z & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Faktory škálování nemusí být všechny stejné a jejich význam je pro absolutní hodnotu v intervalu $(0,1)$ zmenšení/zkrácení, jsou-li větší než 1, mají efekt zvětšení/prodloužení, a jsou-li záporné, způsobí zrcadlové zobrazení. Vynulováním právě jednoho z faktorů škálování získáme tzv. ortografickou projekci na projekční rovinu tvořenou nenulovými faktory.

Afinní transformace

Zkosení podél osy x:

$$\begin{pmatrix} 1 & k_{xy} & k_{xz} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

zkosení podél osy y:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ k_{yx} & 1 & k_{yz} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

zkosení podél osy z:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ k_{zx} & k_{zy} & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Afinní transformace

Rotace okolo osy x o úhel φ:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\varphi & \sin\varphi & 0 \\ 0 & -\sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

rotace okolo osy y o úhel χ:

$$\begin{pmatrix} \cos\chi & 0 & -\sin\chi & 0 \\ 0 & 1 & 0 & 0 \\ \sin\chi & 0 & \cos\chi & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

rotace okolo osy z o úhel ψ:

$$\begin{pmatrix} \cos\psi & \sin\psi & 0 & 0 \\ -\sin\psi & \cos\psi & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$