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 $\bigcap \mathscr{N} \in \mathscr{M}$.

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 $\mathscr{M} \subseteq ExpA$. Průnik prázdného podsystému systému $\mathscr{M}$ je 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 y $\mathscr{M}$, 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 Nechť $(\mathbb{R}_+, \cdot)$ 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 2.5 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 $(\mathscr{M}_{m\times n}(T); +, T, \circ)$ 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.