KATEDRA INFORMATIKY
PŘÍRODOVĚDECKÁ FAKULTA
UNIVERZITA PALACKÉHO

ALGEBRA

DAGMAR SKALSKÁ

VÝVOJ TOHOTO UČEBNÍHO TEXTU JE SPOLUFINANCOVÁN
EVROPSKÝM SOCIÁLNÍM FONDEM A STÁTNÍM ROZPOČTEM ČESKÉ REPUBLIKY

Olomouc 2006

Abstrakt

Tento text distančního vzdělávání seznamuje se základními pojmy algebry. Nejdříve si studující zopakuje základní pojmy z teorie množin a seznámí se s dalšími pojmy z této oblasti. V dalších kapitolách je zaveden pojem realace a jsou probírány zvláštní případy relací – zobrazení, uspořádání a ekvivalence. V šesté až osmé kapitole jsou probrány algebraické struktury s jednou a dvěma operacemi a jejich podstruktury. Poslední kapitoly se týkají vektorových prostorů.

Cílová skupina

Text je primárně určen pro posluchače prvního ročníku bakalářského studijního programu Aplikovaná informatika na Přírodovědecké fakultě Univerzity Palackého v Olomouci. Může však sloužit komukoliv se zájmem o algebru. Text předpokládá znalosti středoškolské matematiky

Obsah

Použitá označení

$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{S}$	množina všech celých sudých čísel
$\mathbb{Q}$	množina všech racionálních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{C}$	množina všech komplexních čísel
$\vee$	disjunkce (logický součet), čteme „nebo“
$\wedge$	konjunkce (logický součin), čteme „a současně“
$\Rightarrow$	implikace, čteme „jestliže, pak“
$\Leftrightarrow$	ekvivalence, čteme „právě když“
$\exists$	existenční kvantifikátor, čteme „existuje“
$\forall$	všeobecný kvantifikátor, čteme „pro všechna“

1 Základní množinové pojmy

Studijní cíle: Po prostudování kapitoly si studující připomene základní pojmy z teorie množin a seznámí se s dalšími, které bude potřebovat při studiu dalších kapitol.

Klíčová slova: Množina, množinová inkluze, sjednocení, průnik a rozdíl množin, kartézský součin a kartézská mocnina množin.

1.1 Množiny

Průvodce studiem

Se základními množinovými pojmy se na základní škole běžně a ve značném rozsahu pracuje. Připomeneme si proto pouze základní fakta, která budeme potřebovat pro další výklad.

Množina je pojem, který slouží k modelování souboru objektů, který je jednoznačně určen tím, které prvky (objekty) do něj patří. Je zvykem množiny označovat velkými písmeny a jejich prvky malými písmeny.

Symbol $x \in A$ čteme obvykle „x je prvkem množiny A“ nebo „x patří do množiny A“ nebo „x leží v množině A“. Symbol $x \notin A$ čteme obvykle „prvek x nepatří do množiny A“.
Množiny můžeme popisovat různým způsobem

- výčtem prvků
$$M_1 = \{2, 5, 7, 8, 11, 25, 67\}$$
- pomocí pevně dohodnutých symbolů
- jako obor pravdivosti určité výrokové funkce
$$M_2 = \{x | x \in \mathbb{Z}, -3 \leq x < 5\}$$
$$M_3 = \{x | x \in \mathbb{N}, 5 < x < 6\}$$

Zřejmně platí $M_2 = \{-3, -2, -1, 0, 1, 2, 3, 4\}$ a $M_3 = \emptyset$, kde symbol $\emptyset$ značí *prázdnou množinu* , tj. množinu, která neobsahuje žádný prvek.

Množina, která se skládá jen z konečného počtu prvků se nazývá *konečná množina*, každá jiná množina se nazývá *nekonečná množina*. Prázdnou množinu $\emptyset$ považujeme za konečnou množinu a říkáme, že počet prvků prázdné množiny je nula.

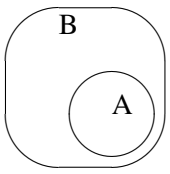
Řekneme, že množina A je *podmnožinou* množiny B právě tehdy, když každý prvek množiny A patří do množiny B. Zapisujeme potom $A \subseteq B$ (nebo také $B \supseteq A$). Jestliže $A \subseteq B$ a $A \neq B$, potom říkáme, že A je *vlastní podmnožina* B a zapisujeme $A \subset B$ (nebo také $B \supset A$). Vztahy $\subseteq$, $\subset$, $\supseteq$, $\supset$ mezi množinami se nazývají *množinové inkluze* . Množinovou inkluzi $A \subseteq B$ obvykle dokazujeme přímo pomocí definice, vezmeme libovolný prvek $x \in A$ a dokážeme, že $x \in B$. Jestliže množina A není podmnožinou množiny B, zapisujeme $A \not\subseteq B$. Chceme-li vztah $A \not\subseteq B$ dokázat, dokazujeme, že existuje prvek $x \in A$ takový, že $x \notin B$.

Jedním z nejčastěji prováděných důkazů v matematice je *důkaz rovnosti množin* , např. A = B, který obvykle provádíme pomocí tvrzení

dokážeme nejdříve inkluzi $A \subseteq B$ a potom inkluzi $B \subseteq A$

$$A = B \text{ právě tehdy, když } (A \subseteq B) \text{ a současně } (B \subseteq A).$$

Pro ilustraci základních množinových pojmů a práci s nimi se na střední škole často používají tzv. *Vennovy diagramy* . Následující obrázek ukazuje Vennův diagram pro dvě množiny A a B, pro které platí $A \subset B$.



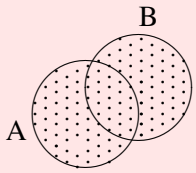
systém množin

Často se setkáváme v matematice s množinami, jejichž prvky jsou zase množiny. Pro takovou množinu používáme názvu *systém množin* . Pokud A je libovolná množina, pak všechny podmnožiny množiny A tvoří systém množin, který nazýváme *systém všech podmnožin množiny* A a označujeme symbolem 2^A. Je-li množina A konečná o n prvcích, $|A| = n$, množina 2^A je rovněž konečná a má 2^n prvků, $|2^A| = 2^n$. Je-li množina A nekonečná, množina 2^A je rovněž nekonečná. Pokud je množina A prázdná, je množina 2^A rovněž prázdná.

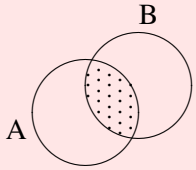
Příklad 1.1. $A = \{x, y, z\}$
$2^A = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$
$|A| = 3, |2^A| = 2^3 = 8$

Průvodce studiem

Již ze základní školy známe definici sjednocení dvou množin a průniku dvou množin.
Sjednocením $A \cup B$ množin A a B rozumíme množinu všech prvků, které patří buď do množiny A nebo do množiny B.



Průnikem $A \cap B$ množin A a B rozumíme množinu všech prvků, které patří současně do množiny A i do množiny B.



Tuto definici si nyní rozšíříme na větší počet množin.

Definice 1.2. Nechť $I \neq \emptyset$ je libovolná (tzv. indexová) množina. Nechť A_i je množina pro každé $i \in I$. Pak
sjednocení množin A_i, $i \in I$ je množina

$$\bigcup_{i \in I} A_i = \{x | \exists i_0 \in I : x \in A_{i_0}\},$$

sjednocení A_i je množina všech prvků, které patří aspoň do jedné z množin A_i

průnik množin A_i, $i \in I$ je množina

$$\bigcap_{i \in I} A_i = \{x | \forall i \in I : x \in A_i\}.$$

průnik A_i je množina všech prvků, které patří současně do všech množin A_i

Definice zahrnuje sjednocení a průnik konečného i nekonečného počtu množin. Záleží na indexové množině I. Sjednocení a průnik konečného počtu množin $A_1, A_2, ..., A_n$ zapisujeme často symboly

$$A_1 \cup A_2 \cup ... \cup A_n \text{ a } A_1 \cap A_2 \cap ... \cap A_n.$$

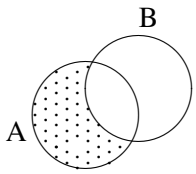
Jsou-li A a B dvě libovolné množiny, pak řekneme, že množiny A a B jsou *disjunktní* , je-li $A \cap B = \emptyset$. Řekneme, že A a B jsou *incidentní*, jestliže $A \cap B \neq \emptyset$.

Definice 1.3. Nechť A, B jsou množiny. *Rozdíl množin* A, B (v tomto pořadí) je množina

$$A - B = \{x | x \in A \text{ a současně } x \notin B\}$$

A-B je množina všech prvků, které patří do A a nepatří do B

Je-li navíc $B \subseteq A$, pak množina $A - B$ se nazývá *komplement* množiny B v množině A a označuje symbolem B'_A nebo stručně B'.



Pro sjednocení, průnik a rozdíl množin lze odvodit celou řadu tvrzení. V následující větě uvedeme pouze ta základní

Věta 1.4. *Nechť A, B, C jsou libovolné množiny, pak platí*

1. $A \cup B = B \cup A$ — *komutativní zákony*
2. $A \cap B = B \cap A$
3. $(A \cup B) \cup C = A \cup (B \cup C)$ — *asociativní zákony*
4. $(A \cap B) \cap C = A \cap (B \cap C)$
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ — *distributivní zákony*
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
7. $A - (B \cup C) = (A - B) \cap (A - C)$ — *de Morganova pravidla*
8. $A - (B \cap C) = (A - B) \cup (A - C)$

Důkaz. Dokážeme tvrzení 7. Ostatní tvrzení se dokazují stejně. Nejdříve dokážeme inkluzi

$$A - (B \cup C) \subseteq (A - B) \cap (A - C)$$

Vezmeme libovolný prvek x z množiny $A - (B \cup C)$. Podle definice rozdílu mnžin $x \in A$ a současně $x \notin B \cup C$. Podle definice sjednocení množin $x \notin B$ nebo $x \notin C$. Z předchozího vyplývá, že $x \in A$ a současně $x \notin B$, tedy podle definice rozdílu množin $x \in A - B$. Současně platí $x \in A$ a současně $x \notin C$. Opět podle definice rozdílu množin $x \in A - C$. Dospěli jsme tedy k tomu, že $x \in (A - B)$ a současně $x \in (A - C)$, tedy podle definice průniku množin $x \in (A - B) \cap (A - C)$
Nyní dokážeme inkluzi

$$(A - B) \cap (A - C) \subseteq A - (B \cup C)$$

Vezmeme libovolný prvek $x \in (A - B) \cap (A - C)$. Z definice průniku množin plyne, že $x \in A - B$ a současně $x \in A - C$. Podle definice rozdílu množin dostaneme, že $x \in A$ a současně $x \notin B$ a $x \notin C$. Podle definice sjednocení množin $x \notin B \cup C$. Použijeme opět definici rozdílu množin a dostaneme $x \in A - (B \cup C)$.
Dokázali jsme tedy, že současně platí obě inkluze $A - (B \cup C) \subseteq (A - B) \cap (A - C)$ a $(A - B) \cap (A - C) \subseteq A - (B \cup C)$, platí tedy rovnost množin

$$A - (B \cup C) = (A - B) \cap (A - C)$$

. □

1.2 Kartézský součin

Průvodce studiem

V dalších kapitolách se budeme často setkávat se zápisy tvaru $\mathbb{R}^2$, $\mathbb{Q}^3$ a podobně, proto na závěr této kapitoli definujeme pojem kartézský součin množin a kartézská mocnina množiny. Nejdříve si však musíme zavést pojem uspořádaná dvojice.

uspořádaná dvojice

Definice 1.5. Ke každým dvěma prvkům množiny M lze přiřadit nový prvek (x, y), který nazýváme *uspořádanou dvojicí* tak, že dva prvky $(x, y), (x', y')$ jsou si rovny právě tehdy, když $x = x'$ a $y = y'$. Prvek x nazýváme 1. složkou a prvek y 2. složkou uspořádané dvojice (x, y).

kartézský součin

Definice 1.6. Nechť A, B jsou libovolné množiny. Pak množina

$$A \times B = \{(x, y)|x \in A, y \in B\}$$

se nazývá *kartézský součin množin* A, B (v tomto pořadí).

Z definice kartézského součinu je zřejmé, že množiny $A \times B$ a $B \times A$ jsou obecně různé. Pokud je některá z množin A, B prázdná, kartézský součin je opět prázdná množina

$$A \times \emptyset = \emptyset \times B = \emptyset.$$

Příklad 1.7. $A = \{a, b, c, d\}, B = \{x, y\}$
$A \times B = \{(a, x), (a, y), (b, x), (b, y), (c, x), (c, y), (d, x), (d, y)\}$
$B \times A = \{(x, a), (x, b), (x, c), (x, d), (y, a), (y, b), (y, c), (y, d)\}$
$|A| = 4, |B| = 2, |A \times B| = |B \times A| = 8$

I obecně platí, když $|A| = n$ a $|B| = m$, potom $|A \times B| = n.m$.

Poznámka 1.8. Název kartézský součin pochází z geometrické interpretace. Když $X = Y = \mathbb{R}$, potom $X \times Y$ můžeme interpretovat jako všechny body roviny a čísla x, y jsou souřadnice bodu (x, y) roviny.

Podobně zavádíme kartézský součin n množin $A_1, A_2, ..., A_n, (n \geq 2)$ jako množinu uspořádaných n-tic

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n)|a_i \in A_i, i = 1, 2, ..., n\}.$$

Je-li $A_1 = A_2 = ... = A_n = A$, značíme kartézský součin $A \times A \times ... \times A$ symbolem A^n a nazýváme jej n-tá *kartézská mocnina* množiny A.

kartézská mocnina

Příklad 1.9. $\mathbb{R}^3 = \{(x, y, z)|x, y, z \in \mathbb{R}\}$ je množina všech uspořádaných trojic reálných čísel.

Shrnutí

Množiny můžeme popisovat různým způsobem, můžeme je znázornit graficky.
Systém množin je množina, jejíž prvky jsou opět množiny.
Kartézský součin dvou množin je množina všech uspořádaných dvojic prvků těchto množin.
n-tá kartézská mocnina množiny A je množina všech uspořádaných n-tic prvků množiny A.

Pojmy k zapamatování

- konečná a nekonečná množina
- inkluze množin
- systém množin
- sjednocení, průnik a rozdíl množin
- kartézský součin množin
- kartézská mocnina množiny

Kontrolní otázky

1. *Vysvětlete, co rozumíte pod pojmem množinová inkluze.*
2. *Vysvětlete, kdy jsou dvě množiny incidentní a kdy disjunktní.*
3. *Vysvětlete pojem kartézský součin dvou množin.*
4. *Lze najít nekonečnou množinu A a konečnou množinu B tak, že A - B = $\emptyset$?*
5. *Nechť A = $\{0,1,2\}$. Určete, které z následujících výroků jsou pravdivé a které nepravdivé*
   (a) $0 \subseteq A$,
   (b) $0 \in A$,
   (c) $\emptyset \subseteq A$,
   (d) $\emptyset \in A$,
   (e) $\{\emptyset\} \subseteq A$.

Cvičení

1. určete všechny prvky množin
   (a) $\{n \in \mathbb{N} \,|2n - 1 < 18\}$
   (b) $\{n \in \mathbb{N} \,|4 < 3n - 1 < 25\}$
2. Množina $A = \{a, b, c, d\}$, určete množinu 2^A
3. Množina $A = \{a, b, c, d\}$, nalezněte všechny prvky X množiny 2^A, pro které platí $X \cap \{c, d\} = \{d\}$.
4. Nechť $A = \{1, 3, 5\}$, $B = \{2, 4, 6\}$. Popište množiny
   (a) $A \times B$,
   (b) $B \times A$,
   (c) $B \times B$,
   (d) $B \times 2^B$.
5. Nechť A, B, C jsou libovolné množiny. Zjistěte, zda platí vztahy
   (a) $A \cap B = A - (A - B)$,
   (b) $A - (B - C) = (A - B) - C$.

Úkoly k textu

1. Udejte příklad konečné množiny M, jejíž prvky jsou nekonečné množiny.
2. Udejte příklad nekonečné množiny M, její prvky jsou konečné množiny.
3. Udejte příklad množin A, B tak, aby množina $A \times 2^B$ měla 12 prvků.
4. Udejte příklad dvou různých množin A, B tak, že $A - B \subseteq B - A$.
5. Udejte příklad dvou různých množin A, B tak, aby $A \times B$ měla právě 32 podmnožin.

Řešení

1. a) {1,2,3,4,5,6,7,8,9}, b) {2,3,4,5,6,7,8 }
2. $2^A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\}, \{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}, \{a,b,c,d\}\}$
3. existují 4 řešení $X_1 = \{a,d\}, X_2 = \{b,d\}, X_3 = \{a,b,d\}, X_4 = \{d\}$
4. (a) $A \times B = \{(1,2),(1,4),(1,6),(3,2),(3,4),(3,6),(5,2),(5,4),(5,6)\}$
   (b) $B \times A = \{(2,1),(2,3),(2,5),(4,1),(4,3),(4,5),(6,1),(6,3),(6,5)\}$
   (c) $B \times B$ = {(2,2), (2,4), (2,6), (4,2), (4,4), (4,6), (6,2), (6,4), (6,6)}
   (d) $2^B = \{\emptyset, \{2\}, \{4\}, \{6\}, \{2,4\}, \{2,6\}, \{4,6\}, \{2,4,6\}\}$
   $B \times 2^B = \{(2,\emptyset),(2,\{2\}),(2,\{4\}),(2,\{6\}),(2,\{2,4\}),(2,\{2,6\}),$
   $(2,\{4,6\}),(2,\{2,4,6\}),(4,\emptyset),(4,\{2\}),(4,\{4\}),(4,\{6\}),(4,\{2,4\}),$
   $(4,\{2,6\}),(4,\{4,6\}),(4,\{2,4,6\}),(6,\emptyset),(6,\{2\}),(6,\{4\}),(6,\{6\}),$
   $(6,\{2,4\}),(6,\{2,6\}),(6,\{4,6\}),(6,\{2,4,6\})\}$
5. a) ano , b) ne

2 Relace

Studijní cíle: Studující se seznámí s pojmy relace mezi množinami a relace na množině. V dalších kapitolách budou studovány speciální případy těchto relací.

Klíčová slova: relace mezi množinami, skládání relací, relace na množině, reflexivní, symetrické, antisymetrické, tranzitivní a úplné relace

Průvodce studiem

Pojem relace je matematickým protějškem běžně používaného pojmu vztah. Různé objekty jsou nebo nejsou v různých vztazích.

2.1 Relace mezi množinami

Definice 2.1. Nechť A, B jsou libovolné množiny. Pak libovolná podmnožina ϱ kartézského součinu $A \times B$ se nazývá *relace mezi množinami* A a B. Je-li $(x, y) \in \varrho$, říkáme, že prvek x je v relaci ϱ s prvkem y a zapisujeme $x \varrho y$. Jestliže je naopak $(x, y) \notin \varrho$, pak říkáme, že prvek x není v relaci ϱ s prvkem y a zapisujeme $x \bar{\varrho} y$.

Průvodce studiem

Jedná se tedy o vztahy mezi prvky dvou různých množin.

Příklad 2.2.

1. Když $A = \{a, b, c, d\}, B = \{x, y\}$, potom

$$\varrho_1 = \{(a, x), (a, y), (c, x), (d, y)\}$$

$$\varrho_2 = \{(a, x), (b, x), (c, y)\}$$

jsou relace mezi množinami A a B.

2. Prázdná množina $\emptyset$ je rovněž podmnožinou $A \times B$, je tedy rovněž relací mezi množinami A a B a nazývá se *prázdná relace.*

relace mezi $\emptyset$ a A je prázdná relace

3. Také celý kartézský součin $A \times B$ je podmnožinou sama sebe, je tedy také relací mezi množinami A a B a nazývá se *univerzální relace.*

Průvodce studiem

Definovat relaci ϱ mezi A a B znamená určit jednoznačně všechny uspořádané dvojice z $A \times B$, které patří do ϱ.

Definice 2.3. Nechť ϱ je relace mezi množinami A a B, nechť σ je relace mezi množinami B a C. Pak relace mezi množinami A a C

skládání relací

$$\sigma \circ \varrho = \{(x, y) \in A \times C | \text{ existuje } b \in B \text{ takové, že } (x, b) \in \varrho \text{ a současně } (b, y) \in \sigma\}$$

se nazývá *složená relace* z relací ϱ a σ.

Příklad 2.4. Jsou dány množiny $A = \{a, b, c, d\}, B = \{x, y\}, C = \{k, l, m, n, o\}$ a relace mezi nimi

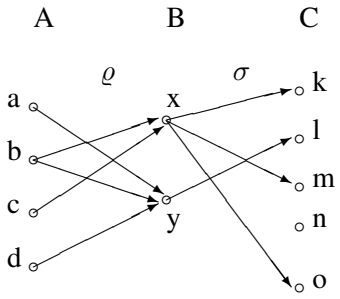
$$\varrho = \{(a, y), (b, x), (b, y), (c, x), (d, y)\},$$
$$\sigma = \{(x, k), (x, m), (x, o), (y, l)\}.$$

Složená relace je potom

$$\sigma \circ \varrho = \{(a, l), (b, k), (b, m), (b, o), (b, l), (c, k), (c, m), (c, o), (d, l)\}.$$

Poznámka 2.5. Pro větší názornost si můžeme relace mezi množinami znázorňovat graficky, zejména jsou-li množiny konečné. Když je ϱ relací mezi množinami A a B, prvky obou množin znázorníme jako body v rovině a bod $r \in A$ spojíme orientovanou šipkou s bodem $s \in B$ právě tehdy, když $(r, s) \in \varrho$. Pomocí těchto grafů můžeme schematicky znázornit i pojem skládání relací. Je zřejmé, že při relaci $\sigma \circ \varrho$ vede orientovaná šipka z bodu $r \in A$ do bodu $t \in C$ právě tehdy, když lze šipku složit ze šipky, která patří do relace ϱ a šipky patřící do relace σ.

Grafické znázornění příkladu 2.4:



Je zřejmé, že skládání relací není komutativní.

Věta 2.6. *Nechť ϱ je relace mezi A a B, σ relace mezi B a C a τ relace mezi C a D. Pak platí* *skládání relací je asociativní*

$$\tau \circ (\sigma \circ \varrho) = (\tau \circ \sigma) \circ \varrho.$$

Důkaz. Je zřejmé, že relace $\tau \circ (\sigma \circ \varrho), (\tau \circ \sigma) \circ \varrho$ jsou relace mezi množinami A a D. Jejich rovnost dokážeme jako množinovou rovnost. Dokazujeme

$$\tau \circ (\sigma \circ \varrho) \subseteq (\tau \circ \sigma) \circ \varrho.$$

Vezmeme libovolné $(x, y) \in \tau \circ (\sigma \circ \varrho)$. Potom existuje $c \in C$ tak, že $(x, c) \in \sigma \circ \varrho$ a současně $(c, y) \in \tau$. Podle definice skládání relací existuje $b \in B$ tak, že $(x, b) \in \varrho$ a současně $(b, c) \in \sigma$ a současně $(c, y) \in \tau$. Opět podle definice skládání relací $(x, b) \in \varrho$ a současně $(b, y) \in \tau \circ \sigma$. Znovu použijeme definici skládání relací a dostaneme $(x, y) \in (\tau \circ \sigma) \circ \varrho$
Inkluze $(\tau \circ \sigma) \circ \varrho \subseteq \tau \circ (\sigma \circ \varrho)$ se dokazuje stejně. □

Definice 2.7. Nechť ϱ je relace mezi množinami A a B. Relace ϱ^{-1} mezi množinami B a A definovaná vztahem *inverzní relace*

$$\varrho^{-1} = \{(u, v) \in B \times A | (v, u) \in \varrho\}$$

se nazývá *relace inverzní* k relaci ϱ.

Věta 2.8. *Nechť ϱ je relace mezi A a B, σ je relace mezi B a C. Pak platí*

1. $(\varrho^{-1})^{-1} = \varrho$,
2. $(\sigma \circ \varrho)^{-1} = \varrho^{-1} \circ \sigma^{-1}$.

Důkaz. 1. Tvrzení je zřejmé z definice inverzní relace.

2. Zřejmě $(\sigma \circ \varrho)^{-1}$ i $\varrho^{-1} \circ \sigma^{-1}$ jsou relace mezi C a A, jejich rovnost dokazujeme opět jako množinovou rovnost.

□

Průvodce studiem

V dalším se budeme zabývat speciálním, ale v praxi často požívaným případem relací, případem, kdy $A, B \neq \emptyset$ a $A = B$.

2.2 Relace na množině

Definice 2.9. Nechť M je neprázdná množina. Pak libovolná podmnožina ϱ kartézského součinu $M \times M$ se nazývá *relace na množině* M . Množinu M s relací ϱ označujeme (M, ϱ) a říkáme, že (M, ϱ) je *množina s relací* .
Pro $x, y \in M$ budeme místo $(x, y) \in \varrho$ psát $x \varrho y$ a místo $(x, y) \notin \varrho$ píšeme $x \bar{\varrho} y$.

Průvodce studiem

Jedná se ovztahy mezi prvky jedné množiny.
Definovat relaci ϱ na množině M znamená určit jednoznačně všechny uspořádané dvojice z $M \times M$, které patří do ϱ.

Příklad 2.10. 1. Prázdná relace $\varrho_1 = \emptyset$ je relací na množině M. *prázdná relace*

2. Univerzální relace $\varrho_2 = M \times M$ je relací na množině M. *univerzální relace*

3. $\iota = \{(m, m) | m \in M\}$ je relací na M. Nazýváme ji *relace rovnosti* a je charakterizována tím, že každý prvek je v relaci právě sám se sebou. *relace rovnosti*

4. Jestliže $M = \{a, b, c, d\}$, potom

$$\varrho_3 = \{(a, a), (a, b), (b, c), (c, b), (d, b), (d, c), (d, d)\}$$

je relací na množině M.

5. Nechť $M = \mathbb{N}$ je množina všech přirozených čísel, potom *relace uspořádání čísel podle velikosti*

$$\varrho_4 = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x - y \text{ je nezáporné číslo } \}$$

je relace na množině $\mathbb{N}$; je zřejmé, že $x \varrho y$ právě tehdy, když $x \leq y$ (při uspořádání čísel podle velikosti).

6. Nechť $M = 2^A$, kde A je libovolná množina, potom $M \neq \emptyset$ a množina *relace inkluze*

$$\{(X, Y) | X, Y \in 2^A \text{ a současně } X \subseteq Y\}$$

je relace na 2^A , kterou nazýváme *relace inkluze* a označujeme obvykle symbolem $\subseteq$.

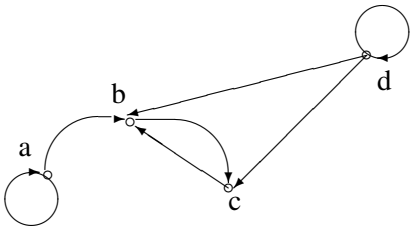
7. Nechť $M = \mathbb{N}$ je množina všech přirozených čísel, potom množina *relace dělitelnosti*

$$\{(a,b)|a,b \in \mathbb{N} \text{ a současně } a \text{ dělí } b\}$$

je relace na $\mathbb{N}$, kterou nazýváme *relace dělitelnosti* a obvykle označujeme symbolem $|$.

Relace na množině můžeme graficky znázornit. Je-li $(M, \varrho\ )$ množina s relací, pak prvky množiny M znázorníme jako body v rovině a z bodu x uděláme orientovanou šipku do bodu y právě tehdy, když $x \varrho y$. Je možné, že šipka začíná i končí ve stejném bodě. Taková šipka se nazývá smyčka. Takto vzniklý obrázek se nazývá *uzlový graf relace* ϱ .

Graf relace ϱ_3 z našeho příkladu : *uzlový graf relace*



Výhodné je rovněž vyjádření relace ϱ na množině M pomocí tabulky, kterou sestrojíme takto: do záhlaví řádků a sloupců vypíšeme prvky množiny M, do průsečíků řádku x a sloupce y zapíšeme 1, je-li $x \varrho y$ a 0, je-li $x \bar{\varrho} y$.

Tabulka relace ϱ_3 z našeho příkladu : *tabulka relace*

ϱ	**a**	**b**	**c**	**d**
a	1	1	0	0
b	0	0	1	0
c	0	1	0	0
d	0	1	1	1

Později uvidíme, že některé speciální relace je výhodné znázorňovat i jiným způsobem. Nyní si nejprve popíšeme základní speciální typy relací na množině.

Definice 2.11. Nechť (M, ϱ) je množina s relací. Řekneme, že relace je :

1. *reflexivní*, jestliže pro všechna $x \in M$ platí $x \varrho x$,
2. *symetrická*, jestliže pro všechna $x, y \in M$, pro která platí $x \varrho y$ platí i $y \varrho x$,
3. *antisymetrická*, jestliže pro všechna $x, y \in M$, pro která platí současně $x \varrho y$ a $y \varrho x$, platí $x = y$,
4. *tranzitivní*, jestliže pro všechna $x, y, z \in M$, pro která platí současně $x \varrho y$ a $y \varrho z$, platí $x \varrho z$,
5. *úplná*, jestliže pro všechna $x, y \in M$ platí $x \varrho y$ nebo $y \varrho x$.

Ukážeme si, jak se jednotlivé typy relací poznají z uzlového grafu a z tabulky:

1. reflexivní
   (a) každý bod je opatřen smyčkou
   (b) v hlavní diagonále tabulky jsou jedničky
2. symetrická

   (a) mezi dvěma různými body jsou buď dvě nebo žádná šipka
   (b) tabulka je symetrická podle hlavní diagonály

3. antisymetrická
   (a) mezi dvěma různými body je buď jedna nebo žádná šipka
   (b) dvě různá políčka symetrická podle hlavní diagonály neobsahují dvě jedničky

4. tranzitivní
   nedá se tak jednoduše určit

5. úplná
   (a) každé dva body jsou spojeny šipkou a každý bod je opatřen smyčkou
   (b) v hlavní diagonále jsou jedničky a dvě různá políčka symetrická podle hlavní diagonály obsahují aspoň jednu jedničku

Příklad 2.12.
1. Prázdná relace je symetrická, antisymetrická a tranzitivní, není reflexivní a úplná.
2. Univerzální relace je reflexivní, symetrická, tranzitivní a úplná, není antisymetrická.
3. Relace rovnosti ι je reflexivní, symetrická, antisymetrická a tranzitivní, není úplná.
4. Relace ϱ_3 nemá žádnou z uvedených vlastností.
5. Relace ϱ_4 je reflexivní, antisymetrická, tranzitivní a úplná, není symetrická.
6. Relace inkluze je reflexivní, antisymetrická a tranzitivní, není symetrická a úplná.
7. Relace dělitelnosti je reflexivní, antisymetrická a tranzitivní, není symetrická a úplná.

Shrnutí

Relace mezi množinami A, B je podmnožina kartézského součinu $A \times B$.
Relace na množině M je podmnožina kartézského součinu $M \times M$.
Relace na množině můžeme znázornit graficky nebo tabulkou.
Relace na množině může být reflexivní, symetrická, antisymetrická, tranzitivní, úplná nebo nemusí mít žádnou z těchto vlastností.

Pojmy k zapamatování

- relace na množině
- složená relace
- relace mezi množinami
- reflexivní, symetrická, antisymetrická, tranzitivní a úplná relace

Kontrolní otázky

1. *Vysvětlete pojem skládání relací a znázorněte graficky.*
2. *Vysvětlete vlastnosti relace na množině na uzlovém grafu relace.*
3. *Vysvětlete vlastnosti relace na množině na tabulce relace.*
4. *Je možné, aby relace na množině byla úplná a nebyla reflexivní?*
5. *Existuje relace na množině M, která je zároveň symetrická a antisymetrická?*

Cvičení

1. Nechť ϱ je relace mezi množinami $\mathbb{Z}$ a $\mathbb{N}$ definovaná

$$\varrho = \{(a, b)|b = a^2 \vee b = a + 1, \forall a \in \mathbb{Z}\}$$

   σ je relace mezi množinami $\mathbb{N}$ a $\mathbb{Z}$ definovaná

$$\sigma = \{(c, c^2 + 1)|\forall c \in \mathbb{N}\}.$$

   Popište relaci $\sigma \circ \varrho$ a relaci $\varrho \circ \sigma$.
2. Nechť $A = \{x, y, z\}$ a $B = \{a, b\}$. Kolik je relací mezi množinami A a B, na množině A a na množině B. Vypište všechny relace na množině B.
3. Je dána relace ϱ na množině $M = \{p, q, r\}$

$$\varrho = \{(p, p), (p, q), (q, q), (p, r), (r, p), (r, q), (r, r)\}.$$

   Je tato relace reflexivní, symetrická, antisymetrická, tranzitivní a úplná?
4. Na množině $\mathbb{N}$ je dána relace ϱ vztahem
$$x \varrho y \Leftrightarrow x.y \text{ je liché číslo pro } \forall x, y \in \mathbb{N}.$$
   Rozhodněte, zda relace ϱ je reflexivní, symetrická, antisymetrická, tranzitivní a úplná.
5. Je dána relace σ na množině $\mathbb{Z}$ vztahem

$$x \sigma y \Leftrightarrow x^2 = y \qquad \forall x, y \in \mathbb{Z}.$$

   Rozhodněte, zda relace σ je reflexivní, symetrická, antisymetrická, tranzitivní a úplná.

Úkoly k textu

1. Udejte příklad relace mezi množinami A = {2, 3, 4} a B = {1, 5, 6}.
2. Udejte příklad relace na množině $M = \{u, v, w\}$, která není reflexivní a je symetrická.
3. Kolik je relací mezi množinami $P = \{p, q\}$ a 2^P ? Udejte příklad takové relace.
4. Kolik je relací na množině $P \times P$, kde $P = \{p, q\}$. Udejte příklad takové relace.
5. Udejte příklad dvou relací ϱ a σ mezi množinami $A = \{a, b, c, d\}$ a $B = \{1, 2, 3\}$. Potom popište množinově i graficky relace ϱ^{-1} a σ^{-1}.

Řešení

1.
$$\sigma \circ \varrho = \{(a, x)|x = a^4 + 1 \vee x = a^2 + 2.a + 2, \forall a \in \mathbb{Z}\}$$
$$\varrho \circ \sigma = \{(c, y)|y = (c^2 + 1)^2 \vee y = c^2 + 2, \forall c \in \mathbb{N}\}$$
2. relací mezi množinami A a B je 64
   relací na množině A je 512
   relací na množině B je 16, jsou to relace:
   $\varrho_1 = \emptyset$, $\varrho_2 = B \times B$ = {(a,a), (a,b), (b,a), (b,b)}, ϱ_3 = {(a,a)}, ϱ_4 = {(a,b)}, ϱ_5 = {(b,a)}, ϱ_6 = {(b,b)}, ϱ_7 = {(a,a), (a,b)}, ϱ_8 = {(a,a), (b,a)}, ϱ_9 = {(a,a), (b,b)}, ϱ_{10} = {(a,b), (b,a)}, ϱ_{11} = {(a,b), (b,b)}, ϱ_{12} = {(b,a), (b,b)}, ϱ_{13} = {(a,a), (a,b), (b,a)}, ϱ_{14} = {(a,a), (a,b), (b,b)}, ϱ_{15} = {(a,a), (b,a), (b,b) }, ϱ_{16} = {(a,b), (b,a), (b,b)}
3. relace je reflexivní, tranzitivní a úplná, není symetrická a antisymetrická
4. reflexivní, symetrická a tranzitivní
5. nemá žádnou z uvedených vlastností

3 Zobrazení

Studijní cíle: Při studiu kapitoly se studující seznámí s pojmy zobrazení, injektivní, surjektivní a bijektivní zobrazení.

Klíčová slova: zobrazení množiny do množiny, definiční obor a obor hodnot, vzor prvku a obraz prvku, injektivní, surjektivní a bijektivní zobrazení, složené zobrazení, inverzní zobrazení

Průvodce studiem

Pojem zobrazení je vlastně matematický ekvivalent pojmu přiřazení. Objektům jedné množiny jsou jednoznačně přiřazovány objekty druhé množiny.

Definice 3.1. Nechť A, B jsou libovolné neprázdné množiny, nechť f je relace mezi množinami A a B, která má vlastnost :

$$\text{ke každému } x \in A \text{ existuje jediné } y \in B \text{ tak, že } (x, y) \in f.$$

Pak uspořádanou trojici (A, B, f) nazýváme *zobrazení množiny* A *do množiny* B.

Poznámka 3.2. Nechť (A, B, f) je zobrazení množiny A do množiny B. Místo (A, B, f) budeme psát $f : A \to B$ a budeme mluvit o zobrazení f množiny A do množiny B. Množinu A budeme nazývat *definičním oborem* zobrazení f a množinu B *oborem hodnot* zobrazení f.

Místo $(x, y) \in f$ budeme psát $f(x) = y$, prvek y budeme nazývat *obraz prvku* x (při zobrazení f) a prvek x budeme nazývat *vzor prvku* y (při zobrazení f).

Průvodce studiem

Zobrazení je speciální případ relace mezi množinami A a B, kdy každý prvek $x \in A$ má právě jeden obraz $y \in B$.

Příklad 3.3. Jsou dány množiny $A = \{a, b, c, d, e\}, B = \{u, v, w\}$ a relace mezi nimi

$$\varrho_1 = \{(a, u), (c, v), (d, w), (e, u)\}$$

ϱ_1 není zobrazení $A \to B$,nebot' $b \in A$ nemá žádný obraz

$$\varrho_2 = \{(a, u), (a, w), (b, v), (c, u), (d, v), (e, v)\}$$

ϱ_2 není zobrazení $A \to B$ nebot' $a \in A$ má dva obrazy

$$\varrho_3 = \{(a, u), (b, u), (c, u), (d, w), (e, w)\}$$

ϱ_3 je zobrazení $A \to B$

Zobrazení ϱ_3 můžeme zapsat

$$\varrho_3(a) = u, \varrho_3(b) = u, \varrho_3(c) = u, \varrho_3(d) = w, \varrho_3(e) = w.$$

Poznámka 3.4. Z předchozího je zřejmé, že pro zadání zobrazení je nutné zadat :

- definiční obor A
- obor hodnot B
- předpis f, který každému prvku z A přiřazuje jediný prvek z B

Předpis f je možno zadat různými způsoby:

Příklad 3.5. 1. $A = \mathbb{Z}, B = \mathbb{S}, f(x) = 2.x$ pro $\forall x \in \mathbb{Z}$

2. $A = \mathbb{N}, B = \mathbb{Z}$

$$g(x) = \begin{cases} x - 3, & 1 \leq x \leq 12 \\ 15, & x = 13 \\ x + 3, & x > 13 \end{cases}$$

Poznámka 3.6. Z definice vyplývá, že dvě zobrazení $f : A \to B$, $g : C \to D$ se rovnají , jestliže

1. $A = C$
2. $B = D$
3. $f(x) = g(x)$ pro $\forall x \in A$

Příklad 3.7. Zobrazení

1. $A_1 = \mathbb{R}$, $B_1 = \mathbb{R}$, $f_1 = \sin x$ pro $\forall x \in A_1$
2. $A_2 = \mathbb{R}$, $B_2 =< -1, 1 >$, $f_2 = \sin x$ pro $\forall x \in A_2$
3. $A_3 =< -\frac{\pi}{2}, \frac{\pi}{2} >$, $B_3 =< -1, 1 >$, $f_3 = \sin x$ pro $\forall x \in A_3$

jsou různá zobrazení, i když předpisy jsou stejné.

Průvodce studiem

1. jestliže $A \subseteq \mathbb{R}$ a $B \subseteq \mathbb{R}$, pak zobrazení $f : A \to B$ se obvykle nazývá (reálná) funkce (jedné reálné proměnné)
2. jestliže $A \subseteq \mathbb{N}$ a $B \subseteq \mathbb{R}$, pak zobrazení $f : A \to B$ se nazývá posloupnost

Poznámka 3.8. *Systém všech zobrazení množiny A do množiny B* označujeme symbolem B^A; je tedy

množina všech zobrazení $A \to B$

$$B^A = \{f | f : A \to B\}.$$

Jestliže množina A má n prvků a množina B s prvků, potom množina B^A má s^n prvků.

Definice 3.9. Nechť $f : A \to B$ je zobrazení. Pak zobrazení f se nazývá :

1. *injektivní (prosté)*, jestliže každý prvek z množiny B má při zobrazení f nejvýše jeden vzor,
2. *surjektivní (zobrazení na)*, jestliže každý prvek z množiny B má při zobrazení f aspoň jeden vzor,

3. *bijektivní (vzájemně jednoznačné)*, jestliže každý prvek z množiny B má při zobrazení f právě jeden vzor.

bijektivní zobrazení je injektivní i surjektivní zároveň

Poznámka 3.10. O každém z uvedených typů zobrazení je nutné mít přesnou představu. Je nutné vědět, jak se dokazuje, zda dané zobrazení je či není injektivní nebo surjektivní.
Nechť je $f : A \to B$ zobrazení a chceme dokázat, že

- f je injektivní,
  pak pro libovolné dva prvky $a_1, a_2 \in A$, které jsou různé, tj. $a_1 \neq a_2$, dokážeme, že $f(a_1) \neq f(a_2)$.
  Někdy je výhodnější dokazování ekvivalentním způsobem, tj. vezmeme dva prvky

  $$a_1, a_2 \in A, \text{pro které platí} f(a_1) = f(a_2)$$

  a dokážeme, že $a_1 = a_2$
- f není injektivní,
  pak musíme najít konkrétní dva prvky $a_1, a_2 \in A$ takové, že $a_1 \neq a_2$ a $f(a_1) = f(a_2)$.
- f je surjektivní,
  vezmeme libovolný prvek $b \in B$ a najdeme k němu vzor, tj. prvek $a \in A$ takový, že $f(a) = b$.
- f není surjektivní,
  pak musíme v B najít konkrétní prvek, který při zobrazení f nemá žádný vzor

Příklad 3.11. 1. Podíváme se na zobrazení z předcházejících příkladů

- zobrazení ϱ_3 z př. 3.3 není injektivní ani surjektivní — *u,w má více vzorů, v nemá žádný vzor*
- zobrazení f z př. 3.5 je bijektivní
- zobrazení g z př. 3.5 je injektivní, ale není surjektivní — *např.10 nemá žádný vzor*
- zobrazení f_1 z př. 3.7 není injektivní ani surjektivní
- zobrazení f_2 z př. 3.7 není injektivní, ale je surjektivní — *např.0.5 má nekonečně mnoho vzorů, 2 nemá žádný vzor*
- zobrazení f_3 z př. 3.7 je bijektivní

2. Nechť A je libovolná neprázdná množina. Zobrazení $id_A : A \to A$ definované vztahem $id_A(x) = x$ se nazývá *identické zobrazení* (identita) na množině A. Identita je zřejmě bijektivní zobrazení.

inverzní zobrazení

Definice 3.12. Nechť $f : A \to B$ je bijektivní zobrazení. Definujme zobrazení $f^{-1} : B \to A$ takto: pro libovolné $b \in B$ položíme $f^{-1}(b) = a$, kde $a \in A$ je vzor prvku b v zobrazení f, $f(a) = b$. Zobrazení f^{-1} se nazývá *inverzní zobrazení* k zobrazení f.

Průvodce studiem

Inverzní zobrazení je definované pouze pro bijektivní zobrazení f a každému obrazu zobrazení f přiřazuje jedinný vzor v tomto zobrazení.

Příklad 3.13. Podíváme se na zobrazení z předcházejícího příkladu

1. Zobrazení $f : \mathbb{Z} \to \mathbb{S}$ definované vztahem $f(x) = 2.x$ pro $\forall x \in \mathbb{Z}$ je bijektivní, inverzní zobrazení $f^{-1} : \mathbb{S} \to \mathbb{Z}$ je definováno vztahem $f^{-1}(s) = \frac{s}{2}$ pro $\forall s \in \mathbb{S}$.
2. Zobrazení $f_3 :< -\frac{\pi}{2}, \frac{\pi}{2} > \to < -1, 1 >$ definované vztahem $f_3(x) = \sin x$ je bijektivní, inverzní zobrazení $f_3^{-1} :< -1, 1 > \to < -\frac{\pi}{2}, \frac{\pi}{2} >$ je definováno vztahem
$$f_3^{-1}(y) = \arcsin y.$$
3. Identické zobrazení $id_A : A \to A$ je bijektivní. Pro inverzní zobrazení $id_A^{-1} : A \to A$ zřejmně platí $id_A^{-1} = id_A$.

identické zobrazení je inverzní samo k sobě

Věta 3.14. *Nechť $f : A \to B$ je bijektivní zobrazení. Pak platí*

1. *$f^{-1} : B \to A$ je bijektivní zobrazení,*
2. *$(f^{-1})^{-1} = f$.*

inverzní zobrazení k inverznímu je původní zobrazení

Důkaz. 1. Plyne přímo z definic inverzního a bijektivního zobrazení.

2. Zřejmě $(f^{-1})^{-1} : A \to B$ a podle předpokladu je $f : A \to B$. Jsou si tedy rovny definiční obory a obory hodnot a stačí dokázat rovnost předpisů:
Vezmeme libovolný prvek $x \in A$ a nechť $f(x) = y \in B$. Potom $f^{-1}(y) = x$. Odtud dostaneme $(f^{-1})^{-1}(x) = y = f(x)$.

□

skládání zobrazení

Definice 3.15. Nechť $f : A \to B$ a $g : B \to C$ jsou zobrazení. Zobrazení $g \circ f : A \to C$ definované vztahem

$$(g \circ f)(x) = g(f(x)) \text{ pro } \forall x \in A$$

se nazývá *složené zobrazení* ze zobrazení f a g.

Věta 3.16. *Nechť $f : A \to B$, $g : B \to C$ a $h : C \to D$ jsou zobrazení. Pak platí*

skládání zobrazení je asociativní

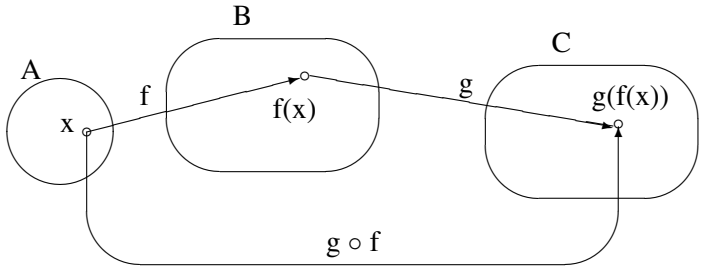
$$h \circ (g \circ f) = (h \circ g) \circ f$$

Důkaz. $h \circ (g \circ f) : A \to D$ a $(h \circ g) \circ f : A \to D$, stačí tedy dokázat rovnost předpisů:
pro libovolné $x \in A$ je $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$ □

Průvodce studiem

Z definice skládání zobrazení je zřejmé, že skládání zobrazení je vlastně skládání relací. Dále je zřejmé, že o skládání zobrazení mluvíme pouze v případě, kdy definiční obor druhého zobrazení je roven oboru hodnot prvního zobrazení.

Následující obrázek skládání zobrazení schematicky zachycuje.



Shrnutí

Zobrazení je speciální typ relace mezi množinami.
Při zadávání zobrazení je nutno zadat definiční obor, obor hodnot a předpis, který každému vzoru přiřadí jediný obraz.
Zobrazení může být injektivní, surjektivní nebo bijektivní.
Inverzní zobrazení zobrazení f je definované pro bijektivní zobrazení a každému obrazu přiřazuje jedinný vzor zobrazení f.
Zobrazení můžeme skládat.

Pojmy k zapamatování

- zobrazení
- vzor a obraz
- definiční obor a obor hodnot
- injektivní, surjektivní a bijektivní zobrazení
- inverzní zobrazení
- složené zobrazení

Kontrolní otázky

1. *Je funkce jedné reálné proměnné zobrazení?*
2. *Je bijektivní zobrazení f injektivní?*
3. *Můžeme k zobrazení, které je surjektivní, ale není injektivní najít inverzní zobrazení?*
4. *Existuje injektivní zobrazení* $f : A \times A \to 2^A$*, je-li* $A = \{a, b, c\}$*?*

Cvičení

1. Rozhodněte, zda předpis $f(x) = \frac{2x^2+10}{x^2+1}$ je zobrazením
   (a) množiny $\mathbb{Z}$ do množiny $\mathbb{Z}$,
   (b) množiny$\mathbb{Z}$ do množiny $\mathbb{Q}$.
2. Rozhodněte, zda předpis $f(x) = \frac{3x^2+x}{x^2-4}$ je zobrazením množiny $\mathbb{Z}$ do množiny $\mathbb{Q}$.
3. Rozhodněte, zda zobrazení $f : \mathbb{N} \to \mathbb{N}$, kde
$$f(x) = \begin{cases} x+1 & x \leq 6 \\ x-1 & x > 6 \end{cases}$$
   je injektivní a surjektivní.
4. Zadejte výčtem prvků množinu A^B a množinu B^A, je-li $A = \{a, b, c\}$, $B = \{x, y\}$
5. Rozhodněte, zda zobrazení $f : \mathbb{Z} \to \mathbb{Z}$
$$f(x) = \begin{cases} 2.x-2 & x \in \mathbb{S} \\ 2.x-1 & x \notin \mathbb{S} \end{cases}$$
   je injektivní a surjektivní.
6. Rozhodněte, zda zobrazení $f : \mathbb{N} \to \mathbb{N}$
$$f(x) = \begin{cases} \frac{n+1}{2} & \text{pro } n \text{ liché} \\ \frac{n}{2} & \text{pro } n \text{ sudé} \end{cases}$$
   je surjekce, injekce nebo bijekce.

Úkoly k textu

1. Udejte příklad zobrazení $f : \mathbb{Z} \to \mathbb{N}$, které je injektivní a není surjektivní.
2. Udejte příklad zobrazení $f : \mathbb{Z} \to \mathbb{N}$, které je surjektivní a není injektivní.
3. Udejte příklad surjektivního zobrazení $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$.
4. Udejte příklad injektivního zobrazení $f : A \times A \to 2^A$, je-li $A = \{a, b\}$

Řešení

1. (a) ne
   (b) ano
2. ne
3. není injektivní ani surjektivní
4. $$B^A = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$$
   $$f_1(a) = x, f_1(b) = x, f_1(c) = x \qquad f_2(a) = x, f_2(b) = x, f_2(c) = y$$
   $$f_3(a) = x, f_3(b) = y, f_3(c) = x \qquad f_4(a) = y, f_4(b) = x, f_4(c) = x$$
   $$f_5(a) = y, f_5(b) = y, f_5(c) = x \qquad f_6(a) = y, f_6(b) = x, f_6(c) = y$$
   $$f_7(a) = x, f_7(b) = y, f_7(c) = y \qquad f_8(a) = y, f_8(b) = y, f_8(c) = y$$
   $$A^B = \{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9\}$$
   $$g_1(x) = a, g_1(y) = a \qquad g_2(x) = b, g_2(y) = b \qquad g_3(x) = c, g_3(y) = c$$
   $$g_4(x) = a, g_4(y) = b \qquad g_5(x) = a, g_5(y) = c \qquad g_6(x) = b, g_6(y) = c$$
   $$g_7(x) = b, g_7(y) = a \qquad g_8(x) = c, g_8(y) = a \qquad g_9(x) = c, g_9(y) = b$$
5. je injektivní, není surjektivní
6. surjekce

4 Uspořádané množiny

Studijní cíle: V této kapitole budeme studovat relaci uspořádání jako relaci na množině, která splňuje některé z dříve definovaných vlastností.

Klíčová slova: uspořádání, uspořádaná množina, lineární uspořádání, řetězec, minimální, nejmenší, maximální a největší prvek

Průvodce studiem

Jedním ze speciálních případů relace na množině je uspořádání. Zvláštním případem této relace je porovnávání čísel podle velikosti. Uvědomme si, že porovnávání čísel podle velikosti je pouze jedna z mnoha aplikací této relace. I v informatice je pojem uspořádání důležitým pojmem – třídící algoritmy, algoritmy vyhledávání.

Definice 4.1. Nechť (M, ϱ) je množina s relací, která je reflexivní, antisymetrická a tranzitivní. Pak relace ϱ se nazývá *uspořádání* a (M, ϱ) se nazývá *uspořádaná množina*.
Je-li navíc relace ϱ úplná, nazývá se *lineární uspořádání* a (M, ϱ) se nazývá *lineárně uspořádaná množina* nebo *řetězec*.

Poznámka 4.2.
1. Relaci uspořádání budeme v dalším označovat symbolem $\leq$ („ menší nebo rovno“).
2. Místo $x \leq y$ budeme podle potřeby psát $y \geq x$.
3. Pro $x \leq y$ a současně $x \neq y$ budeme používat stručné označení $x < y$ („ x je menší než y “).

Příklad 4.3.
1. $A \subseteq A$. *reflexivní*
2. Když $A \subseteq B$ a současně $B \subseteq A$ potom $A = B$. *antisymetrická*
3. $A \subseteq B$ a současně $B \subseteq C$, potom $A \subseteq C$ *tranzitivní*

Relace inkluze $\subseteq$ na množině 2^A je tedy relací uspořádání, (2^A, $\subseteq$) je uspořádaná množina.

Příklad 4.4. $x, y, z \in \mathbb{N}$.

1. $x|x$
2. Když $x|y$ a současně $y|x$, potom $x = y$. *reflexivní*
3. Když $x|y$ a současně $y|z$, potom $x|z$ *antisymetrická tranzitivní*

Relace dělitelnosti | na množině přirozených čísel $\mathbb{N}$ je relací uspořádání, $(\mathbb{N}, |)$ je uspořádaná množina.

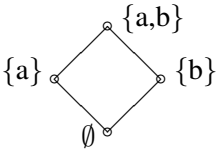
Příklad 4.5. Relace dělitelnosti | na množině celých čísel $\mathbb{Z}$ není relací uspořádání, protože není antisymetrická. ($\mathbb{Z}$, |) není uspořádaná množina. *např.* $3|-3 \wedge -3|3$, *ale* $-3 \neq 3$

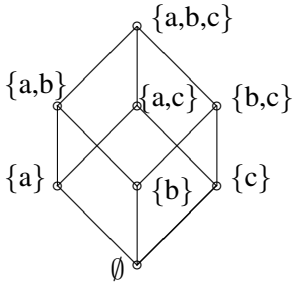
Příklad 4.6. Na množině $\mathbb{N}$ definujeme relaci $\leq$ jako relaci uspořádání čísel podle velikosti. Potom relace $\leq$ je lineární uspořádání a $(\mathbb{N}, \leq)$ je lineárně uspořádaná množina. Podobně jsou lineárně uspořádané množiny $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$. $x \leq y$ *právě když y-x je nezáporné číslo*

Poznámka 4.7. Uspořádanou množinu $(M, \leq)$ můžeme graficky znázornit pomocí tzv. *hasseovských diagramů*. Prvky množiny M znázorníme jako body v rovině tak, aby v případě, že je $x < y$, ležel bod x níže než bod y. Dva body $x, y \in M$ spojíme úsečkou právě tehdy, když $x < y$ a neexistuje $w \in M$ tak, že $x < w < y$.

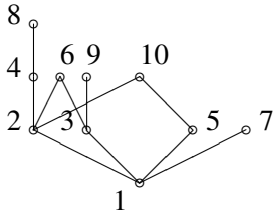
Poznamenejme, že uvedená konstrukce nedefinuje jednoznačně tvar hasseovského diagramu. Na druhé straně, jestliže známe hasseovský diagram uspořádané množiny $(M, \leq)$, pak z něj můžeme relaci $\leq$ jednoznačně určit. Můžeme tedy zadávat uspořádanou množinu hasseovským diagramem.

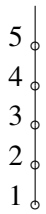
Příklad 4.8. Na následujícím obrázku je hasseovský diagram uspořádané množiny $(2^A, \subseteq)$ pro množiny $A = \{a, b\}$ a $A = \{a, b, c\}$.





Příklad 4.9. Na obrázku jsou části hasseovských diagramů uspořádaných množin $(\mathbb{N}, |)$ a $(\mathbb{N}, \leq)$.





Definice 4.10. V uspořádané množině $(M, \leq)$ se prvek $m \in M$ nazývá :

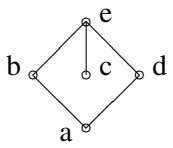
1. *nejmenší*, jestliže pro všechna $x \in M$ platí $m \leq x$
2. *největší*, jestliže pro všechna $x \in M$ platí $x \leq m$
3. *minimální*, jestliže neexistuje prvek $x \in M$ s vlastností $x < m$
4. *maximální*, jestliže neexistuje prvek $x \in M$ s vlastností $m < x$

Dva prvky $x, y \in M$ se nazývají *srovnatelné*, jestliže $x \leq y$ nebo $y \leq x$. V opačném případě se prvky $x,\ y$ nazývají *nesrovnatelné*.

Průvodce studiem

Prvek množiny je minimálním prvkem, pokud v množině neexistuje žádný prvek menší než tento prvek. Prvek množiny je maximální prvek, pokud v množině neexistuje žádný prvek větší než tento prvek. Minimální prvek nemusí být nejmenším prvkem, stejně jako maximální prvek nemusí být největším prvkem.

Příklad 4.11. $(M, \leq)$ je uspořádaná množina zadaná hasseovským diagramem



Potom nejmenší prvek neexistuje, největším prvkem je e, minimálními prvky jsou $a,\ c$, maximální je prvek e. Nesrovnatelné jsou dvojice prvků $a,\ c$, resp. $b,\ c$, resp. $d,\ c$, resp. $b,\ d$. Všechny ostatní dvojice prvků jsou srovnatelné.

Poznámka 4.12. Pokud o nějakém prvku $m \in M$ ověřujeme, že je minimálním prvkem uspořádané množiny $(M, \leq)$, pak je technicky nejvýhodnější postupovat tak, že dokazujeme implikaci:

$$x \in M \wedge x \leq m \Rightarrow x = m$$

Analogicky, pokud dokazujeme, že $m \in M$ je maximální prvek uspořádané množiny $(M, \leq)$, dokazujeme implikaci:

$$x \in M \wedge m \leq x \Rightarrow x = m$$

Věta 4.13. *Nechť $(M, \leq)$ je uspořádaná množina, pak platí:*

1. *V $(M, \leq)$ existuje nejvýše jeden nejmenší prvek a nejvýše jeden největší prvek.*
2. *Je-li $m \in M$ nejmenší (největší) prvek, pak m je také minimální (maximální) prvek a žádné další minimální (maximální) prvky v uspořádané množině $(M, \leq)$ neexistují.*
3. *$(M, \leq)$ je lineárně uspořádaná právě tehdy, když každé dva prvky množiny M jsou srovnatelné.*

Důkaz. 1. Dokazujeme sporem.
Předpokládáme, že m, m' jsou dva nejmenší prvky v $(M, \leq)$. $m \leq m'$ (protože m je nejmenší) a současně $m' \leq m$ (protože m' je nejmenší). Z antisymetrie relace $\leq$ plyne $m = m'$.
Stejně dokážeme pro největší prvek.

2. Nechť $m \in M$ je nejmenší v $(M, \leq)$ a nechť $x \in M$ je prvek, pro který platí $x \leq m$. Protože m je nejmenší prvek, musí platit $m \leq x$. Odtud z antisymetrie relace $\leq$ plyne $m = x$. Prvek m je tedy současně minimálním prvkem.
Zbývá dokázat, že žádný další minimální prvek neexistuje; dokazujeme sporem:
Nechť m' je další minimální prvek v $(M, \leq)$. Protože m je nejmenším prvkem, platí $m \leq m'$ a současně platí $m' < m$ (m' je minimální). Odtud z antisymetrie relace $\leq$ plyne $m = m'$.
Stejně dokážeme pro největší prvek.

3. Plyne ihned z definice lineárního uspořádání a definice srovnatelných prvků.

□

Shrnutí

Uspořádání je relace na množině, která je reflexivní, antisymetrická a tranzitivní.
Lineární uspořádání je relace uspořádání, která je úplná.
Hasseovské diagramy jsou grafickým znázorněním uspořádaných množin.

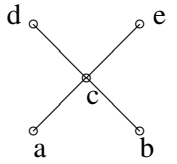
Pojmy k zapamatování

- uspořádaná množina
- řetězec
- hasseovský diagram
- nejmenší a minimální prvek
- největší a maximální prvek

Kontrolní otázky

1. *Který prvek je nejmenší a který největší v uspořádané množině $(2^A, \subseteq)$?*
2. *Jsou v uspořádané množině $(2^A, \subseteq)$ některé dva prvky nesrovnatelné?*
3. *Vysvětli rozdíl mezi minimálním a nejmenším prvkem uspořádané množiny.*
4. *Vysvětli rozdíl mezi maximálním a největším prvkem uspořádané množiny.*
5. *Je možné, aby konečná uspořádaná množina měla tři minimální prvky a žádný maximální prvek?*

Cvičení

1. Na množině $M = \{a, b, c, d\}$ je dána relace
$$\varrho_1 = \{(a,a), (b,b), (c,c), (d,d), (a,d), (a,b), (a,c), (d,b), (d,c)\}.$$
Dokažte, že ϱ_1 je relací uspořádání a nakreslete hasseovský diagram uspořádané množiny (M, ϱ_1).
2. Uspořádaná množina (M, ϱ_2), kde $M = \{a, b, c, d, e\}$, je zadána hasseovským diagramem


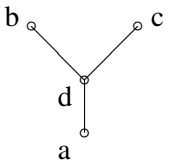
Popište relaci ϱ_2 výčtem prvků.
3. Na množině $M = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ je definována relace ϱ_3 takto:
$$x \varrho_3 y \Leftrightarrow \exists \text{ přirozené číslo } n \text{ tak, že } x = n.y.$$
Dokažte, že ϱ_3 je relací uspořádání a sestrojte hasseovský diagram uspořádané množiny (M, ϱ_3).
4. Určete nejmenší, největší, minimální a maximální prvky relací ϱ_1, ϱ_2, ϱ_3 z předchozích příkladů.
5. Rozhodněte, zda $((\mathbb{N}, \varrho)$, kde relace ϱ je definovaná vztahem
$$x \varrho y \Leftrightarrow \text{počet cifer čísla } x \text{ je větší nebo roven počtu cifer čísla } y$$
je uspořádaná množina.

Úkoly k textu

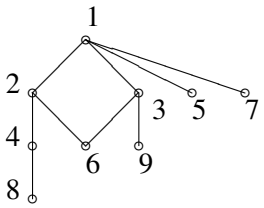
1. Nakreslete hasseovský diagram čtyřprvkové uspořádané množiny, která má dva maximální prvky a nemá nejmenší prvek.
2. Nakreslete hasseovský diagram čtyřprvkové uspořádané množiny, ve které každý prvek je současně maximálním prvkem i minimálním prvkem.
3. Uveďte příklad uspořádané množiny (M, ϱ), která obsahuje právě dva nesrovnatelné prvky a nemá přitom žádný maximální prvek ani žádný minimální prvek.
4. Uveďte příklad množiny A tak, aby uspořádaná množína $(2^A, \subseteq)$ byla lineárně uspořádaná.

Řešení

1. ϱ_1 :



2. $\varrho_2 = \{(a,a),(b,b),(c,c),(d,d),(e,e),(a,c),(a,e),(a,d),(b,c),(b,d),(b,e),(c,d),(c,e)\}$
3. ϱ_3 :



4. ϱ_1 : minimální a nejmenší a, maximální b,c, největší nemá
   ϱ_2 : minimální a,b, maximální d,e, nejmenší a největší nemá
   ϱ_3 : minimální 6,8,9, nejmenší nemá, maximální a největší 1
5. ne

5 Ekvivalence a rozklady

Studijní cíle: V této části se studující seznámí s pojmy ekvivalence a rozklad na množině a pozná, jak tyto pojmy spolu souvisí.

Klíčová slova: ekvivalence na množině, rozklad na množině, třídy rozkladu, ekvivalence příslušná rozkladu, rozklad příslušný ekvivalenci

Průvodce studiem

Dalším zvláštním případem relace na množině je ekvivalence. Ekvivalence je relace, která nám umožňuje ztotožnit prvky množiny, které mají některou vlastnost společnou. Tím nám umožňuje rozložit danou množinu na tzv. třídy, což jsou podmnožiny dané množiny, které obsahují vzájemně ekvivalentní prvky, tedy prvky se stejnou vlastností.

Definice 5.1. Nechť (M, ϱ) je množina s relací, která je reflexivní, symetrická a tranzitivní. Pak relace ϱ se nazývá *ekvivalence* na množině M.

Relaci ekvivalence obvykle značíme $\sim$.

Příklad 5.2. Následující relace

1. relace $\iota = \{(m, m) | m \in M\}$ rovnosti na množině M,
2. univerzální relace $M \times M$,
3. relace rovnoběžnosti přímek,
4. relace stejnolehlosti a podobnosti trojúhelníků

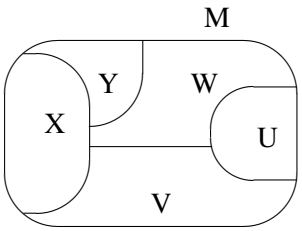
jsou relace ekvivalence.

Definice 5.3. Nechť M je libovolná neprázdná množina. Pak *rozklad na množině* M je systém $\mathcal{M}$ neprázdných podmnožin množiny M, který splňuje podmínky:

1. Pro každé $X, Y \in \mathcal{M}$ platí, pokud $X \cap Y \neq \emptyset$, potom $X = Y$
2. $\bigcup_{X_i \in \mathcal{M}} X_i = M$

Potom prvky systému $\mathcal{M}$ se nazývají *třídy rozkladu* $\mathcal{M}$.

Pojem rozkladu na množině si můžeme přiblížit na obrázku, na kterém máme schematicky znázorněn rozklad $\mathcal{M} = \{U, V, W, X, Y\}$ množiny M na pět tříd U, V, W, X, Y.



Průvodce studiem

Z obrázku a z definice je vidět, že rozklad na množině je systém množin, které nejsou prázdné, žádné dvě nemají žádný společný prvek (nepřekrývají se) a dohromady dají celou množinu (nezůstane žádné místečko prázdné).

Poznámka 5.4. Pokud dokazujeme, že $\mathcal{M}$ je rozklad na M, musíme dokázat, že :

1. Každá třída rozkladu $\mathcal{M}$ je neprázdnou podmnožinou množiny M.
2. Dvě různé třídy rozkladu $\mathcal{M}$ jsou disjunktní.
3. Sjednocení všech tříd rozkladu $\mathcal{M}$ je rovno množině M.

Příklad 5.5. Rozklad na množině celých čísel
$\mathcal{M} = \{\{x \in \mathbb{Z} |\ x < -10\}, \{x \in \mathbb{Z} |\ -10 \leq x \leq -5\}, \{-4, -3, -2, -1, 0\},$
$\{x \in \mathbb{Z} |\ x > 0 \wedge x \in S\}, \{x \in \mathbb{Z} |\ x > 0 \wedge x \notin S\}\}$.
má pět tříd, tři nekonečné a dvě konečné

Příklad 5.6. Rozklad na množině celých čísel $\mathcal{M} = \{\{x\} |\ x \in \mathbb{Z}\}$ má nekonečně mnoho tříd, každá třída obsahuje jedinný prvek

Příklad 5.7. Na množině reálných čísel označíme symbolem I_k interval $< k, k+1)$,
tzn. $I_k = \{x \in \mathbb{R} |\ k \leq x < k+1\}$. Potom $\mathcal{M} = \{I_k |\ k \in \mathbb{Z}\}$ je rozklad na množině reálných čísel, který má nekonečně mnoho tříd a každá třída má nekonečně mnoho prvků.
každý interval je zleva uzavřený a zprava otevřený

Průvodce studiem

Mezi ekvivalencemi na množině M a rozklady na množině M je úzká souvislost, jak ukazují následující věty.

Věta 5.8. *Nechť $\sim$ je relace ekvivalence na množině M. Pro $a \in M$ položme*

$$X_a = \{x \in M |\ x \sim a\}.$$

množina prvků ekvivalentních s prvkem a

Potom systém množin

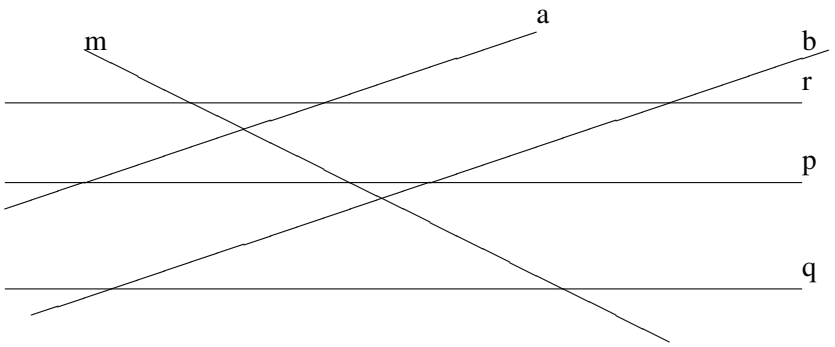
$$\{X |\quad \exists a \in M \text{ tak, že } X = X_a\}.$$

v jedné třídě jsou prvky spolu ekvivalentní

je rozklad na množině M, který označujeme $M/\sim$ a nazýváme rozklad příslušný ekvivalenci $\sim$.

Důkaz. Dokazujeme přesně podle definice rozkladu na množině. Je zřejmé, že $M/\sim$ je systém neprázdných podmnožin $(a \in X_a)$ a že $\bigcup X_a (a \in M) = M$. Stačí dokázat, že je splněna vlastnost 1 z definice rozkladu. Nechť $X_a, X_b \in M/\sim$ a nechť $X_a \cap X_b \neq \emptyset$, to znamená, že existuje prvek $w \in X_a \cap X_b$. Dokážeme, že potom $X_a = X_b$. Dokážeme implikaci $X_a \subseteq X_b$. Implikace $X_b \subseteq X_a$ se dokáže stejně:
Vezmeme libovolné $x \in X_a$. Platí tedy $x \sim a$ a současně $w \in X_a \cap X_b$. Tedy současně platí $x \sim a, w \sim b, w \sim a$. Použitím tranzitivnosti relace $\sim$ dostaneme $x \sim b$ a tedy $x \in X_b$. $\square$

Příklad 5.9. Na množině přímek $M = \{a, b, m, p, q, r\}$ je dána relace $\sim$ rovnoběžnosti přímek



přímky,které jsou rovnoběžné,jsou v jedné třídě

Rozklad příslušný této ekvivalenci je

$$M/\sim = \{\{a, b\}, \{m\}, \{p, q, r\}\}.$$

Příklad 5.10. Na množině $M = \{a, b, c, d, e\}$ je dána relace
$\varrho = \{(a, a), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b), (b, b), (c, c), (d, d), (d, e),$
$(e, d), (e, e)\}$ *ukažte,že se jedná o ekvivalenci*
Rozklad příslušný této ekvivalenci je

$$M/\varrho = \{\{a, b, c\}, \{d, e\}\}.$$

Příklad 5.11. Rozklad příslušný relaci rovnosti ι na množině M má tvar

$$M/\iota = \{\{m\} |\ m \in M\}$$

Rozklad příslušný univerzální relaci $M \times M$ na množině M má tvar

$$M/M \times M = \{M\}$$

Věta 5.12. *Necht' $\mathcal{M}$ je rozklad na množině M. Pro $a, b \in M$ položme* *prvky z jedné třídy jsou ekvivalentní*

$$a \sim_{\mathcal{M}} b \text{ právě tehdy, když existuje třída } X \in \mathcal{M} \text{ tak, že } a, b \in X.$$

Pak $\sim_{\mathcal{M}}$ je relací ekvivalence na M, kterou budeme nazývat ekvivalence příslušná rozkladu $\mathcal{M}$.

Důkaz. Dokazujeme přesně podle definice ekvivalence. Relace $\sim_{\mathcal{M}}$ je zřejmě reflexivní a symetrická. Musíme dokázat, že je rovněž tranzitivní:
Vezmeme libovolné $a, b, c \in M$. Předpokládáme, že platí $a \sim_{\mathcal{M}} b$ a současně $b \sim_{\mathcal{M}} c$. Existují tedy třídy $X, Y \in \mathcal{M}$ takové, že $a, b \in X, b, c \in Y$. Odtud dostaneme, že $b \in X \cap Y$. Podle definice rozkladu to znamená, že $X = Y$ a tedy $a, c \in X$. Odtud plyne $a \sim_{\mathcal{M}} c$. Tím je dokázáno, že relace $\sim_{\mathcal{M}}$je tranzitivní. □

Příklad 5.13. Na množině $M = \{a, b, c, d, e, f\}$ je dán rozklad

$$\mathcal{M} = \{\{a, b, d\}, \{c, e\}, \{f\}\}.$$

Určete relaci ekvivalence příslušnou tomuto rozkladu. *ekvivalence příslušná danému rozkladu*
Řešení $\sim_{\mathcal{M}} = \{(a, a), (a, b), (b, a), (a, d), (d, a), (b, d), (d, b), (b, b), (d, d), (c, c), (e, e), (c, e),$
$(e, c), (f, f)\}$

Příklad 5.14. 1. Když M je libovolná neprázdná množina a rozklad na M má tvar

$$\mathcal{M} = \{\{m\} |\ m \in M\}.$$

Potom ekvivalence příslušná tomuto rozkladu je zřejmě relace rovnosti ι na množině M.

2. Nechť $\mathcal{M} = \{ M \}$ tj. rozklad množiny M, který má jedinou třídu. Pak ekvivalence příslušná tomuto rozkladu je zřejmě univerzální relace $M \times M$.

Průvodce studiem

Jak vidíme z druhého a třetího příkladu, mezi ekvivalencemi na množině M a rozklady na množině M je velmi úzká souvislost. Když vyjdeme z jisté ekvivalence na množině M, utvoříme rozklad na M příslušný této ekvivalenci a potom vytvoříme ekvivalenci na M příslušnou tomuto rozkladu, dostaneme původní ekvivalenci, od které jsme vyšli. Podobně, když začneme s rozkladem, dojdeme přes ekvivalenci příslušnou k němu opět k původnímu rozkladu. Následující věta přesně popisuje situaci

Ekvivalence příslušná rozkladu $M/\sim$ je rovna původní ekvivalenci
Rozklad příslušný ekvivalenci $\sim_{\mathcal{M}}$ je roven původnímu rozkladu

Věta 5.15. *Nechť M je neprázdná množina. Pak platí*

1. *Je-li $\sim$ ekvivalence na M, pak $\sim_{M/\sim} = \sim$.*
2. *Je-li $\mathcal{M}$ rozklad na M, pak $M/\sim_{\mathcal{M}} = \mathcal{M}$.*

Důkaz. Obě tvrzení se opět dokazují jako množinové rovnosti, tz. dokážeme

$$\sim_{M/\sim} \subseteq \sim \text{ a současně } \sim \subseteq \sim_{M/\sim}$$

a

$$M/\sim_{\mathcal{M}} \subseteq \mathcal{M} \text{ a současně } \mathcal{M} \subseteq M/\sim_{\mathcal{M}}.$$

□

Shrnutí

Ekvivalence je relace na množině, která je reflexivní, symetrická a tranzitivní.
Rozklad na množině je systém množin, které jsou neprázdné, po dvou disjunktní a jejich sjednocením je celá množina.
K dané ekvivalenci přísluší rozklad na množině.
Danému rozkladu přísluší ekvivalence na množině.

Pojmy k zapamatování

- rozklad na množině
- ekvivalence na množině
- rozklad příslušný ekvivalenci
- ekvivalence příslušná rozkladu

Kontrolní otázky

1. *Vysvětlete, co je to rozklad na množině.*
2. *Jak souvisí pojem rozklad na množině s pojmem ekvivalence na množině?*
3. *Když vyjdeme z pevného rozkladu na dané množině, najdeme k němu ekvivalenci na dané množině a k ní vytvoříme příslušný rozklad, dostaneme původní rozklad na dané množině?*
4. *Lze najít rozklad na množině $\mathbb{R}$, který má konečně mnoho tříd, přičemž každá třída obsahuje konečně mnoho prvků?*

Cvičení

1. Na množině $M = \{p, q, r, s, t\}$ je definovaná relace

$$\varrho = \{(p,p), (q,q), (r,r), (s,s), (t,t), (p,q), (q,p), (p,s), (s,p), (q,s), (s,q)\}.$$

   Rozhodněte, zda ϱ je relací ekvivalence na množině M a pokud tomu tak je, sestrojte rozklad M/ϱ.

2. Na množině $M = \{u, v, w, x, y, z\}$ je dán rozklad

$$\mathcal{R} = \{\{u, y, z\}, \{v, w\}, \{x\}\}.$$

   Určete relaci $\sim_{\mathcal{R}}$

3. Vypište všechny rozklady, které lze vytvořit na množině $M = \{a, b, c, d\}$

4. Na množině $\mathbb{R}$ je definovaná relace

$$\varrho = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x - y \in \mathbb{Z}\}.$$

   Rozhodněte,zda ϱ je relací ekvivalence na $\mathbb{R}$.

5. Na množině M = {1, 3, 7, 10, 12, 16, 19, 21, 25, 28, 30} definujeme relaci ϱ takto:

$$x \varrho y \Leftrightarrow \text{čísla } x, y \text{ mají stejný součet cifer.}$$

   Dokažte, že ϱ je relací ekvivalence na M a sestrojte rozklad M/ϱ.

Úkoly k textu

1. Udejte příklad relace ϱ na množině $\mathbb{Z}$, která je současně ekvivalencí i uspořádáním.
2. Udejte příklad relace ϱ na množině $\mathbb{N}$, která je reflexivní a tranzitivní, ale není ekvivalencí ani uspořádáním.
3. Udejte příklad rozkladu na $\mathbb{N}$, který má nekonečně mnoho tříd, přičemž každá třída obsahuje nekonečně mnoho prvků.
4. Uveďte příklad ekvivalence ϱ na množině $\mathbb{R}$ tak, aby rozklad $\mathbb{R}/\varrho$ měl právě 3 třídy.

Řešení

1. ano, $\{\{p, q, s\}, \{r\}, \{t\}\}$
2. $\sim_{\mathcal{R}} = \{(u,u), (v,v), (w,w), (x,x), (y,y), (z,z), (u,y), (u,z), (y,u), (z,u)$
   $(y,z), (z,y), (v,w), (w,v)\}$
3. $\varrho_1 = \{\{a\}, \{b\}, \{c\}, \{d\}\}$ $\varrho_2 = \{\{a,b\}, \{c\}, \{d\}\}$, $\varrho_3 = \{\{a,c\}, \{b\}, \{d\}\}$
   $\varrho_4 = \{\{a,d\}, \{b\}, \{c\}\}$ $\varrho_5 = \{\{b,c\}, \{a\}\{d\}\}$ $\varrho_6 = \{\{b,d\}, \{a\}, \{c\}\}$
   $\varrho_7 = \{\{c,d\}, \{a\}, \{b\}\}$ $\varrho_8 = \{\{a,b\}, \{c,d\}\}$ $\varrho_9 = \{\{a,c\}, \{b,d\}\}$
   $\varrho_{10} = \{\{a,d\}, \{b,c\}\}$ $\varrho_{11} = \{\{a,b,c\}, \{d\}\}$ $\varrho_{12} = \{\{a,c,d\}, \{b\}\}$
   $\varrho_{13} = \{\{a,b,d\}, \{c\}\}$ $\varrho_{14} = \{\{b,c,d\}, \{a\}\}$ $\varrho_{15} = \{\{a,b,c,d\}\}$
4. ano
5. {{1, 10}, {3, 12, 21, 30}, {7, 16, 25}, {19, 28}}

6 Algebraické struktury s jednou operací

Studijní cíle: V této kapitole se studující seznámí s jistými speciálními typy zobrazení, které se nazývají operace a s množinami s těmito operacemi – grupoidy.

Klíčová slova: operace na množině, grupoid, pologrupa, grupa, celočíselná mocnina prvku, celočíselný násobek prvku

6.1 Grupoidy

Definice 6.1. Nechť G je neprázdná množina. Pak libovolné zobrazení $G \times G \to G$ se nazývá *operace na množině* G. Je-li v tomto zobrazení uspořádané dvojici $(a, b) \in G \times G$ přiřazen prvek $c \in G$, pak budeme obvykle psát $a.b = c$ a hovořit o operaci .. Množina G spolu s operací . se nazývá *grupoid* a označuje se symbolem $(G, .)$.

Průvodce studiem

Pojem operace vznikl zobecněním pojmů známých ze základní školy – sčítání, násobení, odečítání a dělení čísel. Víme, že vždy libovolné uspořádané dvojici čísel z jisté číselné množiny je přiřazeno přesně dané číslo z téže číselné množiny.

Poznámka 6.2. Operace je zvláštním případem zobrazení, ale nepoužívá se symboliky pro zobrazení. Používáme speciálních symbolů :

multiplikativní symbolika .

- $a.b = c$ a mluvíme o operaci tečka nebo o operaci násobení
- $a + b = c$ a mluvíme o operaci plus nebo o operaci sečítání

aditivní symbolika +

Někdy používáme i jiných symbolů $\circ, *, \star, \triangle, \heartsuit$ a podobně.

Příklad 6.3.

1. Pokud operace + je operace sčítání čísel, $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, jsou grupoidy.
2. Pokud operace . je operace násobení čísel, $(\mathbb{N}, .)$, $(\mathbb{Z}, .)$, $(\mathbb{Q}, .)$, $(\mathbb{R}, .)$, $(\mathbb{C}, .)$ jsou grupoidy.
3. Pokud operace - je operace odečítání čísel, $(\mathbb{N}, -)$ není grupoid a $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$, $(\mathbb{C}, -)$ jsou grupoidy.
4. Pokud operace / je operace dělení čísel $(\mathbb{N}, /)$, $(\mathbb{Z}, /)$, $(\mathbb{Q}, /)$, $(\mathbb{R}, /)$, $(\mathbb{C}, /)$ nejsou grupoidy.
5. pokud A je neprázdná množina, $(2^A, \cup)$, $(2^A, \cap)$, $(2^A, -)$ jsou grupoidy.

Průvodce studiem

Z definice je zřejmé, že grupoid je uspořádaná dvojice $(G, .)$, která se skládá z množiny a operace. Rovnost dvou grupoidů tedy znamená rovnost nosných množin a současně rovnost operací.

Příklad 6.4.

1. $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ jsou různé grupoidy.

liší se nosné množiny

2. $(\mathbb{Z}, +)$, $(\mathbb{Z}, .)$ jsou různé grupoidy.

liší se operace

Definice 6.5. Nechť $(G, .)$ je grupoid. Jestliže platí

1. $a.(b.c) = (a.b).c$ pro každou trojici prvků $a, b, c \in G$, pak operace . se nazývá *asociativní operace* a $(G, .)$ se nazývá *asociativní grupoid* nebo *pologrupa*.
2. $a.b = b.a$ pro každou dvojici prvků $a, b \in G$, pak operace . se nazývá *komutativní operace* a $(G, .)$ se nazývá *komutativní grupoid*.

operace sčítání a násobení čísel jsou komutativní a asociativní

Příklad 6.6.
1. $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{N}, .)$, $(\mathbb{Z}, .)$, $(\mathbb{Q}, .)$, $(\mathbb{R}, .)$, $(\mathbb{C}, .)$ jsou komutativní pologrupy.
2. $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$, $(\mathbb{C}, -)$ nejsou ani komutativní ani asociativní grupoidy.
3. Nechť A je neprázdná množina, $(2^A, \cap)$, $(2^A, \cup)$ jsou komutativní pologrupy.
4. Nechť A je neprázdná množina, $(2^A, -)$ není ani komutativní ani asociativní.

operace odečítání čísel není komutativní ani asociativní

průnik a sjednocení množin jsou komutativní a asociativní operace

Průvodce studiem

Asociativní zákon můžeme zobecnit pro více činitelů.

Věta 6.7. *Nechť (G, .) je pologrupa, nechť $a_1, a_2, ..., a_n \in G$ $(n \geq 2)$. Potom součin prvků $a_1, a_2, ..., a_n$ (v tomto pořadí) nezávisí na jejich uzávorkování.*

rozdíl množin není ani komutativní ani asociativní operace

Důkaz. Dokazujeme matematickou indukcí. □

Definice 6.8. Nechť $(G, .)$ je grupoid. Prvek $e \in G$ se nazývá *neutrální prvek grupoidu* $(G, .)$, jestliže platí

neutrální prvek

$$a.e = a \text{ a současně } e.a = a \text{ pro všechna } a \in G.$$

Věta 6.9. *V grupoidu existuje nejvýše jeden neutrální prvek.*

Důkaz. Dokazujeme sporem. Nechť $(G, .)$ je grupoid a $e, e' \in G$ jsou jeho neutrální prvky, potom platí:

$e.e' = e'$ (e je neutrální) a současně $e.e' = e$ (e' je neutrální). Odtud plyne $e' = e$.

□

Příklad 6.10.
1. Grupoidy $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ mají neutrální prvek 0, grupoid $(\mathbb{N}, +)$ nemá žádný neutrální prvek.
2. Grupoidy $(\mathbb{N}, .)$, $(\mathbb{Z}, .)$, $(\mathbb{Q}, .)$, $(\mathbb{R}, .)$, $(\mathbb{C}, .)$ mají neutrální prvek 1.
3. Grupoidy $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$, $(\mathbb{C}, -)$ nemají žádný neutrální prvek.
4. Pokud A je neprázdná množina, grupoid $(2^A, \cup)$ má neutrální prvek $\emptyset$, grupoid $(2^A, \cap)$ má neutrální prvek A, grupoid $(2^A, -)$ nemá žádný neutrální prvek.

Průvodce studiem

V dalším budeme mluvit v případě grupoidu $(G, .)$ (multiplikativní symbolika) o „jedničce“ grupoidu a v případě grupoidu $(G, +)$ (aditivní symbolika) o „nule“ grupoidu.

Definice 6.11. Nechť $(G, .)$ je grupoid s jedničkou e, nechť $a \in G$. Potom prvek $x \in G$, pro který platí

inverzní prvek

$$a.x = e \text{ a současně } x.a = e$$

se nazývá *inverzní prvek k prvku* a v grupoidu $(G, .)$.

Poznámka 6.12. Když používáme aditivní symboliku, tzn. $(G, +)$ s nulou o, potom místo o inverzním prvku k prvku a mluvíme o *opačném prvku k prvku* a. Je to tedy takový prvek x, pro který platí

$$a + x = o \text{ a současně } x + a = o.$$

Věta 6.13. *V pologrupě s jedničkou ke každému prvku existuje nejvýše jeden inverzní prvek.*

Důkaz. Dokazujeme opět sporem. Nechť $(G, .)$ je pologrupa s jedničkou e, nechť $a \in G$ a nechť $x, y \in G$ jsou dva inverzní prvky k prvku a. Podle definice je

$$a.x = e, \quad x.a = e, \quad a.y = e, \quad y.a = e.$$

Odtud dostaneme

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

□

Průvodce studiem

V multiplikativní symbolice inverzní prvek k prvku a označujeme a^{-1}, v aditivní symbolice opačný prvek k prvku a označujeme $-a$.

inverzní prvek k neutrálnímu prvku je neutrální prvek

Věta 6.14. *Nechť (G, .) je pologrupa s jedničkou e. Nechť $a, b \in G$ mají v (G, .) inverzní prvky a^{-1}, b^{-1}. Pak platí*

1. $e^{-1} = e$,
2. $(a^{-1})^{-1} = a$,
3. $(a.b)^{-1} = b^{-1}.a^{-1}$.

inverzní prvek k inverznímu prvku je prvek původní

inverzní prvek k součinu prvků je součin inverzních prvků v opačném pořadí

Důkaz.

1. Plyne přímo z definice inverzního prvku.
2. Plyne přímo z definice inverzního prvku.
3. Rozepsáním dostáváme

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

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

Prvek $b^{-1}.a^{-1}$ je tedy inverzním prvkem k prvku $a.b$, čili

$$(a.b)^{-1} = b^{-1}.a^{-1}$$

□

Průvodce studiem

Operace na množině jako předpis, který přiřazuje každé uspořádané dvojici prvků z G jediný prvek z G, může být zadán různým způsobem. Jedním z těchto způsobů je Cayleyho tabulka, ve které do svislého i vodorovného záhlaví jsou zapsány prvky množiny G. Výsledek operace je potom prvek v políčku tabulky, ve kterém se příslušný řádek a sloupec protínají.

Příklad 6.15. Je dána množina $G = \{a, b, c, d, e\}$ a operace $\star$ tabulkou

$\star$	**a**	**b**	**c**	**d**	**e**
a	a	c	c	a	d
b	c	b	d	b	a
c	c	d	a	c	b
d	a	b	c	d	e
e	d	a	b	e	c

Je $(G, \star)$ grupoid? Pokud ano, zjistěte, zda je asociativní a komutativní, zda má neutrální prvek a zda mají prvky z G inverzní prvky.
Řešení: Z tabulky je zřejmé, že výsledky operace mezi prvky z G jsou opět prvky z G, $(G, \star)$ je tedy grupoid. Tabulka je symetrická podle hlavní diagonály, grupoid je komutativní. Sice platí

$$(a \star b) \star c = c \star c = a \text{ a současně } a \star (b \star c) = a \star d = a,$$

ale

$$(a \star b) \star e = c \star e = b \text{ a současně } a \star (b \star e) = a \star a = a.$$

$(G, \star)$ tedy není asociativní. Z tabulky je zřejmé, že prvek d je jedničkou grupoidu $(G, \star)$.

$$a \star e = e \star a = d \qquad b \star c = c \star b = d.$$

Platí tedy

$$a^{-1} = e, \qquad b^{-1} = c, \qquad c^{-1} = b, \qquad e^{-1} = a.$$

6.2 Grupy

Průvodce studiem

Snažíme se zobecnit naše zkušenosti s počítáním s čísly. Je tedy zřejme, že budeme pracovat s grupoidy, které jsou asociativní, mají neutrální prvek a ke každému prvku existuje prvek inverzní.

Definice 6.16. Nechť $(G, .)$ je pologrupa s jedničkou, ve které ke každému prvku existuje inverzní prvek. Pak $(G, .)$ se nazývá *grupa*. Je-li navíc operace . komutativní, pak se grupa $(G, .)$ nazývá *abelovská grupa* .

Příklad 6.17.
1. $(\mathbb{N}, +)$ není grupa, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou abelovské grupy.
2. $(\mathbb{N}, .)$, $(\mathbb{Z}, .)$ nejsou grupy.
3. $(\mathbb{Q}, .)$, $(\mathbb{R}, .)$, $(\mathbb{C}, .)$ nejsou grupy. *nula nemá inverzní prvek*

4. ($\mathbb{Q}$-{0}, .), ($\mathbb{R}$-{0}, .), ($\mathbb{C}$-{0}, .) jsou abelovské grupy.

5. $(2^A, \cup)$, $(2^A, \cap)$, $(2^A, -)$ nejsou grupy.

6. $(G, \star)$ je sice grupoid s jedničkou d, ve kterém každý prvek má inverzní prvek, ale není asociativní. Takže $(G, \star)$ není grupa.

Definice 6.18. Nechť $(G, .)$ je grupoid. Řekneme, že

1. V $(G, .)$ platí *zákony o dělení*, jestliže pro každé $a, b \in G$ platí:

$$\text{existuje } x \in G \text{ tak, že a.x = b,}$$
$$\text{existuje } y \in G \text{ tak, že y.a = b.}$$

2. V $(G, .)$ platí *zákony o krácení*, jestliže pro libovolné $a, b, x \in G$ platí:

$$\text{když } a.x = b.x, \text{ potom } a = b,$$

$$\text{když } x.a = x.b \text{ potom } a = b.$$

Věta 6.19. *Nechť (G, .) je pologrupa. Pak platí:*

$$(G, .) \textit{ je grupa právě tehdy, když v } (G, .) \textit{ platí zákony o dělení.}$$

Důkaz. Věta má tvar ekvivalence. Abychom ji dokázali, musíme dokázat obě implikace „⇒“ i „⇐“.
„⇒“ Předpokládáme, že $(G, .)$ je grupa a dokážeme, že platí zákony o dělení. Stačí položit $x = a^{-1}.b, y = b.a^{-1}$. Pak

$$a.x = a.(a^{-1}.b) = b,$$
$$y.a = (b.a^{-1}).a = b.$$

„⇐“ Předpokládáme, že v pologrupě $(G, .)$ platí zákony o dělení a dokážeme, že $(G, .)$ je grupa. Musíme dokázat, že v $(G, .)$ existuje neutrální prvek a ke každému prvku existuje prvek inverzní. □

Věta 6.20. *Nechť (G, .) je grupa. Pak v (G, .) platí zákony o krácení.*

Důkaz. Nechť (G, .) je grupa a nechť $a, b, x \in G$ tak, že $x.a = x.b$. Vynásobíme rovnost zleva prvkem x^{-1} a dostaneme $x^{-1}.(x.a) = x^{-1}.(x.b)$ a odtud $a = b$. Stejně dokážeme i druhý vztah. □

6.3 Celočíselná mocnina

Definice 6.21. Nechť $(G, .)$ je grupa, nechť $a \in G$. Pak *celočíselná mocnina prvku* a je definována takto :

$$a^n = \begin{cases} \underbrace{a.a.....a}_{n\,krát} & n > 0 \\ e & n = 0 \\ \underbrace{a^{-1}.a^{-1}.....a^{-1}}_{n\,krát} & n < 0 \end{cases}.$$

Věta 6.22. *Nechť $(G, .)$ je grupa, nechť $a \in G$ a nechť m, n jsou libovolná celá čísla. Pak platí:*

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

2. $(a^m)^n = a^{m.n}$.

Důkaz.

- Když ($m > 0$ a současně $n > 0$) nebo ($m = 0, n$ libovolné) nebo ($n = 0, m$ libovolné), pak obě tvrzení plynou přímo z definice.
- Pokud $m < 0$ a současně $n < 0$, pak
  1. $g^m.g^n = (\underbrace{g^{-1}.g^{-1}.....g^{-1}}_{-m\,krát}).(\underbrace{g^{-1}.g^{-1}.....g^{-1}}_{-n\,krát}) = (\underbrace{g^{-1}.g^{-1}.....g^{-1}}_{(-m-n)\,krát}) = g^{m+n}$,
  2. $(g^m)^n = (((g^{-m})^{-1})^{-n})^{-1} = (((g^{-m})^{-n})^{-1})^{-1} = (g^{-m})^{-n} = g^{m.n}$.
- Případy ($m < 0$ a současně $n > 0$) a ($m > 0$ a současně $n < 0$) se dokážou podobně jako předchozí případ.

□

Poznámka 6.23. Použijeme-li aditivního zápisu operace, potom místo názvu celočíselná mocnina prvku a použijeme název *celočíselný násobek prvku* a. Ten je definován:

$$n.a = \begin{cases} \underbrace{a + a + ... + a}_{n\,krát} & n > 0 \\ o & n = 0 \\ \underbrace{(-a) + (-a) + ... + (-a)}_{n\,krát} & n < 0 \end{cases}.$$

Tvrzení věty 6.22 pak mají formální tvar :

1. $m.a + n.a = (m + n).a$
2. $n.(m.a) = (n.m).a$

Poznámka 6.24. Zde je zapotřebí si dát pozor na použité symboly, protože jeden symbol lze použít ve dvou významech (+ znamená jednak operaci v dané grupě a jednak sečítání celých čísel, . znamená jednak celočíselný násobek a jednak násobení celých čísel).

Průvodce studiem

Musíme si uvědomit, že náš výklad byl pouze stručným úvodem k problematice grup. Teorie grup je v současné době jedna z nejrozsáhlejších disciplin algebry.

Shrnutí

Operace na množině G je zobrazení, které každé uspořádáné dvojici prvků z G přiřadí prvek z G.
Grupoid je množina s operací.
Pologrupa je asociativní grupoid.
Grupa je pologrupa s jedničkou, ve které ke každému prvku existuje prvek inverzní.

Pojmy k zapamatování

- operace na množině
- grupoid
- pologrupa
- grupa
- celočíselná mocnina prvku
- celočíselný násobek prvku

Kontrolní otázky

1. *Vysvětli pojem grupoid.*
2. *Vysvětli pojem grupa.*
3. *Co rozumíte pod pojmem celočíselná mocnina prvku?*
4. *Platí ve známých grupách ($\mathbb{Z}$, +), ($\mathbb{Q}$, +), ($\mathbb{R}$, +),($\mathbb{C}$, +), ($\mathbb{Q}$-{0}, .), ($\mathbb{R}$-{0}, .), ($\mathbb{C}$-{0}, .) zákony o dělení a o krácení?*
5. *Je možné najít pologrupu s jedničkou, ve které k některému prvku existují dva prvky inverzní?*
6. *Je možné, aby v pologrupě, ve které platí zákony o dělení, neplatily zákony o krácení?*

Cvičení

1. Jsou ($\mathbb{S}$, +), ($\mathbb{S}$, -), ($\mathbb{S}$, .), ($\mathbb{S}$, /) grupoidy ? Pokud ano, jsou to grupy ?
2. Na množině $G = \{a, b, c, d, e\}$ je dána operace $\star$ tabulkou. Rozhodněte, zda je grupoid $(G, \star)$ komutanivní, asociativní a zda má neutrální prvek.

$\star$	**a**	**b**	**c**	**d**	**e**
a	a	d	a	d	a
b	d	b	c	a	b
c	a	c	b	a	c
d	d	a	a	c	d
e	a	b	c	d	e

3. Je ($\mathbb{Z}$,$\circ$), kde operace $\circ$ je definovaná vztahem $x \circ y = x + y + 3$, grupa ?
4. Doplňte tabulku operace $\circ$ na množině $G = \{x, y, z\}$ tak, aby $(G, \circ)$ byl komutativní grupoid s jedničkou.

$\circ$	**x**	**y**	**z**
x	z	y	x
y	.	.	y
z	.	.	.

5. Na množině $G = \{a, b, c\}$ je dána operace $\star$ tabulkou:

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

   Vyšetřete, zda je grupoid $(G, \star)$ komutativní grupou.
6. Je dán komutativní grupoid $(G, \circ)$, kde $G = \{a+b.i |\ a, b \in \mathbb{Z}\}$, $\circ$ je sčítání komplexních čísel. Rozhodněte, zda $(G, \circ)$ je komutativní grupou.

Úkoly k textu

1. Uveďte příklad grupoidu $(G, \circ)$, $G = \{x, y, z\}$. Kolik takových grupoidů existuje ?
2. Uveďte příklad konečné pologrupy, která nemá neutrální prvek.
3. Udejte příklad grupoidu $(G, .)$ tak, že tento grupoid má jedničku, ale není pologrupou.
4. Udejte příklad grupoidu $(G, .)$ tak, že v tomto grupoidu neplatí zákony o dělení.

Řešení

1. ($\mathbb{S}$, +) je grupa, ($\mathbb{S}$, -),($\mathbb{S}$, .) jsou grupoidy a nejsou grupy, ($\mathbb{S}$, /) není grupoid.
2. Operace $\star$ je komutativní, není asociativní, $(G, \star)$ má jedničku e.

3. Ano, jednička je číslo - 3, k prvku x je inverzní prvek $(-\ x\ -\ 6)$.
4. Úloha má tři řešení

$\circ$	**x**	**y**	**z**
x	z	y	x
y	y	z	y
z	x	y	z

$\circ$	**x**	**y**	**z**
x	z	y	x
y	y	x	y
z	x	y	z

$\circ$	**x**	**y**	**z**
x	z	y	x
y	y	y	y
z	x	y	z

5. ano
6. Ano, neutrální prvek je 0, prvek opačný k prvku $a + b.i$ je prvek $-a - b.i$.

7 Podstruktury struktur s jednou operací

Studijní cíle: Při studiu této kapitoly se studující dozví, co je to podgrupoid a podgrupa.

Klíčová slova: množina uzavřená vzhledem k operaci, podgrupoid, podgrupa, netriviální a triviální podgrupa

Definice 7.1. Nechť $(G, .)$ je grupoid a nechť H je neprázdná podmnožina množiny G. Řekneme, že množina H *je uzavřená vzhledem k operaci* ., jestiže pro libovolnou dvojici prvků $a, b \in H$ platí $a.b \in H$.

Definice 7.2. Nechť $(G, .)$ je grupoid, nechť neprázdná podmnožina $H \subseteq G$ je uzavřená vzhledem k operaci .. Pak grupoid $(H, .)$ se nazývá *podgrupoid grupoidu* $(G, .)$.

Průvodce studiem

Podgrupoid grupoidu je neprázdná podmnožina grupoidu, která je opět grupoidem se stejnou operací.

Příklad 7.3.

1. grupoid $(\mathbb{N}, +)$ je podgrupoidem grupoidu $(\mathbb{Z}, +)$
2. grupoid $(G, \star)$ je dán tabulkou

$\star$	**a**	**b**	**c**	**d**	**e**
a	a	c	c	a	d
b	c	b	d	b	a
c	c	d	a	c	b
d	a	b	c	d	e
e	d	a	b	e	c

Určete všechny jeho podgrupoidy.
Řešení: $(\{a\}, \star)$, $(\{b\}, \star)$, $(\{d\}, \star)$, $(\{a, c\}, \star)$, $(\{a, d\}, \star)$, $(\{b, d\}, \star)$, $(\{a, c, d\}, \star)$, $(\{a, b, c, d\}, \star)$, $(\{a, b, c, d, e\}, \star)$

Věta 7.4. *Nechť (H, .) je podgrupoid grupoidu (G, .). Pak platí*

1. *Když grupoid $(G, .)$ je asociativní je i grupoid $(H, .)$ asociativní.*
2. *Když je grupoid $(G, .)$ komutativní je i grupoid $(H, .)$ komutativní.*
3. *Jestliže prvek e je jednička v grupoidu $(G, .)$ a současně $e \in H$, potom prvek e je jedničkou i v grupoidu $(H, .)$.*

Důkaz. Všechna tvrzení plynou ihned z definice. □

Poznámka 7.5. Žádnou implikaci v předchozí větě nelze obrátit.

Příklad 7.6. $(\{a, c\}, \star)$ je asociativní, ale z předcházející kapitoly víme, že $(G, \star)$ asociativní není.

podgrupa má neutrální prvek a ke každému prvku existuje inverzní prvek

Definice 7.7. Nechť $(G, .)$ je grupa, nechť $(H, .)$ je podgrupoid v $(G, .)$, který je sám grupou. Pak $(H, .)$ se nazývá *podgrupa grupy* $(G, .)$.

Věta 7.8. *Nechť (H, .) je podgrupa grupy (G, .). Pak platí :*

1. *jednička podgrupy (H, .) je totožná s jedničkou grupy (G, .)*

2. *inverzní prvek k prvku $h \in H$ v podgrupě (H, .) je totožný s inverzním prvkem k prvku h v grupě (G, .)*

Důkaz. 1. Předpokládáme, že prvek e_H je jednička v $(H, .)$ a prvek e_G je jednička v $(G, .)$. Podle definice neutrálního prvku platí

$$e_H.e_H = e_H \text{ a současně } e_H.e_G = e_H. \text{ Odtud plyne } e_H.e_H = e_H.e_G.$$

Použitím zákona o krácení dostaneme $e_H = e_G$.

2. Nechť x značí inverzní prvek k prvku h v podgrupoidu $(H, .)$ a y značí inverzní prvek k prvku h v grupoidu $(G, .)$, potom podle definice inverzního prvku platí

$$h.x = e_H = e_G \text{ a současně } h.y = e_G. \text{ Odtud plyne } h.x = h.y$$

a použitím zákona o krácení dostaneme $x = y$.

□

Průvodce studiem

Podgrupa je tedy podgrupoid, který má neutrální prvek a ve kterém ke každému prvku existuje inverzní prvek.

Poznámka 7.9. Protože nemusíme rozlišovat inverzní prvek k $h \in H$ v podgrupě a v celé grupě, budeme jej v obou případech označovat h^{-1}.

Poznámka 7.10. Je-li $(G, .)$ libovolná grupa, pak $(\{e\}, .)$ a $(G, .)$ jsou vždy podgrupy grupy $(G, .)$ a nazývají se *triviální podgrupy* grupy $(G, .)$. Ostatní podgrupy (pokud existují) se nazývají *netriviální podgrupy* grupy $(G, .)$

Příklad 7.11. 1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou podgrupy grupy $(\mathbb{C}, +)$.
$(\mathbb{N}, +)$ je podgrupoid grupy $(\mathbb{C}, +)$.

2. $(\mathbb{R}\text{-}\{0\}, .)$, $(\mathbb{Q}\text{-}\{0\}, .)$, $(\mathbb{C}\text{-}\{0\}, .)$ jsou podgrupy grupy $(\mathbb{C}\text{-}\{0\}, .)$.
$(\mathbb{Z}\text{-}\{0\}, .)$ je podgrupoid grupy $(\mathbb{C}\text{-}\{0\}, .)$.

Průvodce studiem

V grupě, která má nekonečně mnoho prvků, mohou existovat jak podgrupy, které mají nekonečně mnoho prvků, tak podgrupy, které mají libovolný konečný počet prvků.

Věta 7.12. *Nechť (G, .) je grupa, nechť H je neprázdná podmnožina v G. Pak následující výroky jsou ekvivalentní*

1. *$(H, .)$ je podgrupa v grupě $(G, .)$*

2. *Pro libovolné prvky $a, b \in H$ platí $a.b \in H$ a současně $a^{-1} \in H$*

3. *Pro libovolné prvky $a, b \in H$ platí $a.b^{-1} \in H$*

4. *Pro libovolné prvky $a, b \in H$ platí $a^{-1}.b \in H$*

Důkaz. „1. $\Rightarrow$ 2.“ plyne z definice podgrupy
„2. $\Rightarrow$ 3.“ zřejmé
„3. $\Rightarrow$ 4.“ Předpokládáme, že platí tvrzení 3. a nechť $a, b \in H$ jsou libovolné, potom podle tvrzení 3. je

$$a.a^{-1} = e \in H, e.a^{-1} = a^{-1} \in H, e.b^{-1} = b^{-1} \in H$$

a opět podle tvrzení 3. je $a^{-1}.b = a^{-1}.(b^{-1})^{-1} \in H$
„4. $\Rightarrow$ 1.“ Předpokládáme, že platí tvrzení 4. a nechť $a, b \in H$ jsou libovolné, potom podle tvrzení 4. je

$$a^{-1}.a = e \in H, a^{-1}.e = a^{-1} \in H, a.b = (a^{-1})^{-1}.b \in H$$

$(H, .)$ je tedy podgrupoid v $(G, .)$, který je asociativní (podle věty 7.4), má jedničku a ke každému prvku má prvek inverzní, je tedy podgrupou grupy $(G, .)$. □

Poznámka 7.13. Předchozí větu používáme k technickému ověření toho, zda v konkrétním případě $(H, .)$ je podgrupou $(G, .)$.

Příklad 7.14. Nechť $(G, .)$ je abelovská grupa a nechť

$$H = \{x \in G | x.x = x\}$$

Dokažte, že $(H, .)$ je podgrupa grupy $(G, .)$.
Řešení: Vezmeme libovolné dva prvky $a, b \in H$ a ukážeme, že $a.b^{-1} \in H$. Protože $(G, .)$ je abelovská grupa, platí v ní komutativní a asociativní zákony. Ty budou platit rovněž v $(H, .)$

Tvrzení dokážeme podle bodu 3 věty 7.12

$$(a.b^{-1}).(a.b^{-1}) = (a.b^{-1}).(b^{-1}.a) = a.(b^{-1}.b^{-1}).a = a.b^{-1}.a = (a.a).b^{-1} = a.b^{-1}$$

Shrnutí

Množina uzavřená vzhledem k operaci je množina, ve které výsledek operace mezi prvky této množiny je opět prvkem této množiny.
Podgrupoid je neprázdná podmnožina grupoidu, která je uzavřená vzhledem k dané operaci.
Podgrupa je podgrupoid, který je grupou.

Pojmy k zapamatování

- množina uzavřená vzhledem k operaci
- podgrupoid
- podgrupa

Kontrolní otázky

1. *Jak vysvětlíte pojem podgrupoid ?*
2. *Má každá grupa nějakou podgrupu ?*
3. *Vysvětlete, jak ověříte, že podmnožina s operací je podgrupou dané grupy.*
4. *Grupa (G, .) je abelovská. Je její podgrupa (H, .) rovněž abelovská?*

Cvičení

1. Je dán grupoid (ℕ, +) a podmnožina $H \subseteq \mathbb{N}$. Rozhodněte, zda $(H, +)$ je podgupoidem grupoidu (ℕ, +), je-li
   (a) H = ℕ - {1, 3, 5}
   (b) H = ℕ - {1, 3, 4}
2. Na množině $G = \{a, b, c, d, e\}$ je dána operace $\circ$ tabulkou

$\circ$	**a**	**b**	**c**	**d**	**e**
a	b	c	c	a	a
b	c	b	a	d	b
c	c	a	b	b	c
d	a	d	b	d	d
e	a	b	c	d	e

V grupoidu $(G, \circ)$ nalezněte všechny podgrupoidy.

3. Je dána grupa ($\mathbb{Q}$, +) a neprázdná podmnožina $H \subseteq \mathbb{Q}$

$$H = \{\frac{a}{2^k} | a \in \mathbb{Z}, k \in \mathbb{N}\}$$

Je $(H, +)$ podgrupou grupy ($\mathbb{Q}$, +) ?

4. Nechť $(G, .)$ je komutativní grupa. Označme $H = \{a \in G | a.a = e\}$. Je $(H, .)$ podgrupou grupy $(G, .)$?

Úkoly k textu

1. Uveďte příklad grupoidu $(G, .)$ s jedničkou e a jeho podgrupoidu $(H, .)$, který
   (a) nemá jedničku
   (b) má jedničku různou od e
2. Uveďte příklad dvou disjunktních podgrup v grupě ($\mathbb{N}$, .)

Řešení

1. a) ano , b) ne
2. ({b},○), ({d}, ○), ({e}, ○), ({b,d},○), ({b,e}, ○), ({d,e}, ○), ({a,b,c}, ○), ({b,d,e}, ○), ({a,b,c,d},○), ({a,b,c,e}, ○), ({a,b,c,d,e}, ○)
3. ano
4. ano

8 Struktury se dvěma operacemi

Studijní cíle: V této kapitole se studující seznámí s algebraickými strukturami se dvěma operacemi – okruhem, oborem integrity a tělesem.

Klíčová slova: okruh, dělitelé nuly, obor integrity, těleso

8.1 Okruh

Definice 8.1. Nechť R je množina se dvěma operacemi + a . taková, že platí

1. $(R, +)$ je komutativní grupa,
2. $(R, .)$ je pologrupa,
3. pro $\forall a, b, c \in R$ platí tak zvané *distributivní zákony*

distributivní zákon pro násobení zprava
distributivní zákon pro násobení zleva

$$(a + b).c = a.c + b.c$$

$$a.(b + c) = a.b + a.c.$$

Pak R s operacemi + a . se nazývá *okruh* a označuje se $(R, +, .)$.

Průvodce studiem

Zavedený pojem je zřejmě zobecněním běžných struktur se dvěma operacemi, které známe ze střední školy. Proto také zavádíme značení, které je stejné jako u známých číselných množin se dvěma operacemi

1. operaci + budeme nazývat sčítání a operaci . násobení
2. neutrální (nulový) prvek grupy $(R, +)$ se nazývá nula okruhu $(R, +, .)$ a označuje se symbolem 0
3. opačný prvek k prvku a v okruhu (R, +, .) označujeme $-a$
4. místo $a + (-b)$ píšeme $a - b$

Příklad 8.2. Pokud + znamená sečítání čísel, . násobení čísel, potom ($\mathbb{Z}$, +, .), ($\mathbb{S}$, +, .), ($\mathbb{Q}$, +, .), ($\mathbb{R}$, +, .), ($\mathbb{C}$, +, .) jsou okruhy.

Příklad 8.3. Je $(\mathbb{Q}, \oplus, \circ)$, kde operace $\oplus$ a $\circ$ jsou definované vztahy $x \oplus y = x + y$, $x \circ y = y$, okruh?
Řešení:

1. $(\mathbb{Q}, \oplus)$ je abelovská grupa, protože se jedná o sčítání racionálních čísel.

$(\mathbb{Q}, \oplus)$ je abelovská grupa

2. $(\mathbb{Q}, \circ)$ je grupoid, protože výsledek operace $\circ$ je opět racionální číslo. Ověříme platnost asociativních zákonů:

$$(x \circ y) \circ z = y \circ z = z \qquad x \circ (y \circ z) = y \circ z = z$$

$(\mathbb{Q}, \circ)$ je pologrupa

3. Zbývá ověřit platnost distributivních zákonů:

$$(x \oplus y) \circ z = z \text{ a současně } (x \circ z) \oplus (y \circ z) = z \oplus z = z + z$$

Neplatí distributivní zákon

Dostali jsme

$$(x \oplus y) \circ z \neq (x \circ z) \oplus (y \circ z)$$

$(\mathbb{Q}, \oplus, \circ)$ není okruh

Příklad 8.4. Na množině $\mathbb{R} \times \mathbb{R}$ definujeme operace

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

$\mathbb{R} \times \mathbb{R}$ je uzavřená vzhledem k operaci sčítání a násobení

pro libovolné $a, b, c, d \in \mathbb{R}$ je ($\mathbb{R} \times \mathbb{R}$, +) grupoid, který je asociativní a komutativní a má nulový prvek (0, 0), prvek $(-a, -b)$ je opačný k prvku (a, b).
($\mathbb{R} \times \mathbb{R}$, +) je tedy abelovská grupa.
($\mathbb{R} \times \mathbb{R}$, .) je asociativní grupoid.
Platnost distributivních zákonů plyne z platnosti distributivních zákonů pro čísla.
($\mathbb{R} \times \mathbb{R}$, +, .) je tedy okruh.

sčítání a násobení čísel je asociativní a komutativní

Příklad 8.5. Uvažujeme množinu $R0 = \{(r, 0)|r \in \mathbb{R}\}$, kde operace + a . jsou definované stejně jako v $\mathbb{R} \times \mathbb{R}$.

$(r_1, 0) + (r_2, 0) = (r_1 + r_2, 0)$

$(R0, +)$ je grupoid, který je asociativní a komutativní.
(0, 0) je nula v $(R0, +)$ a $(-r, 0)$ je prvek opačný k $(r, 0)$.
$(R0, +)$ je tedy abelovská grupa.
$(R0, .)$ je grupoid, který je asociativní.

$(r_1, 0).(r_2, 0) = (r_1.r_2, 0)$

Platnost distributivních zákonů plyne z platnosti distributivních zákonů pro čísla.
$(R0, +, .)$ je tedy okruh.

Věta 8.6 (pravidla pro „počítání“ v okruhu). *Necht'$(R, +, .)$ je okruh, $a, b, c \in R$ libovolné. Potom platí*

1. $a.(b - c) = a.b - a.c \qquad (a - b).c = a.c - b.c$
2. $a.0 = 0.a = 0$
3. $a.(-b) = (-a).b = -(a.b)$
4. $(-a).(-b) = a.b$

Důkaz. 1.

$$a.(b-c) = a.(b-c)+a.c-a.c = a.((b+(-c))+c)-a.c = a.(b+(-c+c))-a.c = a.b-a.c,$$

druhý vztah se dokáže podobně.

2. $a.0 + a.0 = a.(0 + 0) = a.0 = a.0 + 0$, použitím zákona o krácení v $(R, +)$ dostaneme $a.0 = 0$, stejně dokážeme $0.a = 0$.
3. Užitím 1.a 2. dostaneme $a.(-b) = a.(0 - b) = a.0 - a.b = 0 - a.b = -a.b$, podobně dokážeme $(-a).b = -(a.b)$.
4. Užitím 3. dostaneme $(-a).(-b) = -((-a).b) = -(-a.b) = a.b$.

□

Průvodce studiem

Pravidla pro počítání z předcházející věty nám opět připomínají známá pravidla pro počítání s čísly.

Definice 8.7. Nechť $(R, +, .)$ je okruh. Je-li operace . komutativní, pak okruh $(R, +, .)$ se nazývá *komutativní okruh* . Jestliže pologrupa $(R, .)$ má jedničku, pak tato se nazývá *jedničkou okruhu* $(R, +, .)$ a označuje se symbolem 1. Okruh $(R, +, .)$ se pak nazývá *okruh s jedničkou* .

Příklad 8.8.
1. Okruhy ($\mathbb{Z}$, +, .), ($\mathbb{Q}$, +, .), ($\mathbb{R}$, +, .), ($\mathbb{C}$, +, .) jsou komutativní okruhy s jedničkou 1.
2. Okruh ($\mathbb{S}$, +, .) je komutativní okruh bez jedničky.
3. Okruh ($\mathbb{R} \times \mathbb{R}$, +, .) je komutativní okruh s jedničkou (1, 1).
4. Okruh $(R0, +, .)$ je komutativní okruh s jedničkou (1, 0).

Definice 8.9. Nechť $(R, +, .)$ je okruh a nechť pro nějaká $a, b \in R$ platí

součin nenulových prvků je nula

$$a \neq 0 \text{ a současně } b \neq 0 \text{ a současně } a.b = 0.$$

Pak prvky a, b se nazývají *dělitelé nuly*.

Průvodce studiem

Již ze základní školy víme, že ve známých číselných množinách dělitelé nuly neexistují. Pokud je součin dvou čísel nula, je aspoň jedno z těchto čísel nula.

8.2 Obor integrity a těleso

Definice 8.10. Netriviální komutativní okruh s jedničkou, který nemá dělitele nuly, se nazývá *obor integrity* .

Příklad 8.11.
1. ($\mathbb{Z}$, +, .), ($\mathbb{Q}$, +, .), ($\mathbb{R}$, +, .), ($\mathbb{C}$, +, .) jsou obory integrity.
2. ($\mathbb{S}$, +, .) není obor integrity. *nemá jedničku*
3. ($\mathbb{R} \times \mathbb{R}$, +, .) není obor integrity – je sice komutativní okruh s jedničkou, ale *má dělitele nuly*

$$(0, 1) \neq (0, 0) \text{ a současně } (1, 0) \neq (0, 0) \text{ a současně } (0, 1).(1, 0) = (0, 0).$$

4. $(R0, +, .)$ je obor integrity. *je to komutativní okruh s jedničkou, který nemá dělitel nuly*

Definice 8.12. Komutativní okruh $(R, +, .)$ s vlastností $(R - \{0\}, .)$ je grupa, se nazývá *těleso*.

Průvodce studiem

Těleso je tedy komutativní okruh, který má jedničku a ve kterém ke každému nenulovému prvku existuje prvek inverzní.

Poznámka 8.13. Z definice vyplývá několik faktů :

1. Každé těleso musí obsahovat aspoň dva různé prvky, jinak by byla $R - \{0\}$ prázdná množina a $(R - \{0\}, .)$ by nebyla grupa. Tyto dva prvky jsou tedy nula a jednička.

2. Ke každému nenulovému prvku existuje vzhledem k operaci . jediný inverzní prvek.

3. Těleso nemá žádné dělitele nuly (množina nenulových prvků je uzavřená vzhledem k operaci násobení, tedy součin nenulových prvků je opět nenulový prvek). Odtud plyne, že každé těleso je oborem integrity. To však neplatí naopak. ($\mathbb{Z}$, +, .) je oborem integrity, ale není tělesem, protože ($\mathbb{Z}$ -$\{0\}$, .) není grupa.

Příklad 8.14. 1. ($\mathbb{Q}$, +, .), ($\mathbb{R}$, +, .), ($\mathbb{C}$, +, .) jsou tělesa.

2. ($\mathbb{R}$ $\times \mathbb{R}$, +, .) není těleso.

3. $(R0, +, .)$ je těleso.

Průvodce studiem

Musíme si uvědomit, co mají obory integrity a tělěsa společné a v čem se liší. V oboru integrity, na rozdíl od tělesa, nemusí ke každému nenulovému prvku existovat inverzní prvek, tedy zde obecně neexistují operace dělení. Na druhé straně obor integrity a těleso mají tu společnou vlastnost, že v nich neexistují dělitelé nuly (tedy je v nich možno při násobení krátit nenulovými prvky).

Shrnutí

Okruh je množina se dvěma operacemi, která je pro operaci sčítání abelovskou grupou, operaci násobení pologrupou a obě operace splňují distributivní zákony.
Dělitelé nuly jsou dva nenulové prvky, jejichž součin je nula.
Obor integrity je komutativní okruh s jedničkou bez dělitelů nuly.
Těleso je komutativní okruh s jedničkou, ve kterém ke každému nenulovému prvku existuje prvek inverzní.

Pojmy k zapamatování

- okruh
- dělitelé nuly
- obor integrity
- těleso

Kontrolní otázky

1. *Je každý obor integrity okruhem ?*
2. *Je každý obor integrity tělesem ?*
3. *Je každé těleso oborem integrity ?*
4. *Může existovat jednoprvkové těleso ?*

Cvičení

1. Je dána množina $\mathbb{Z}$ s operacemi $\oplus, \circ$, které jsou definovány

$$x \oplus y = x + y - 3 \qquad x \circ y = 3.$$

Ukažte, že ($\mathbb{Z}$, $\oplus, \circ$) je okruh a určete
   (a) který prvek je nulou tohoto okruhu,
   (b) který prvek je opačný k prvku x,
   (c) zda je okruh komutativní,

(d) zda má okruh jedničku,

(e) zda má okruh dělitele nuly.

2. Je dána množina $\mathbb{Q}$ s operacemi $\oplus, \circ$, které jsou definovány

$$x \oplus y = x + y + 1 \qquad x \circ y = x + y + x.y.$$

Ukažte,že $(\mathbb{Q}, \oplus, \circ)$ je tělesem. Určete

(a) který prvek je nulou,

(b) který prvek je opačný k prvku x,

(c) který prvek je jedničkou,

(d) který prvek je inverzní k nenulovému prvku x.

3. Uvažujme podmnožinu G množiny všech komplexních čísel

$$G = \{a + b.i | a, b \in \mathbb{Z}\}.$$

Množina G se nazývá množina Gaussových celých čísel. Zjistěte, zda tato množina je

(a) oborem integrity,

(b) tělesem.

Úkoly k textu

1. Udejte příklad okruhu, který nemá dělitele nuly a přitom není oborem integrity.
2. Udejte příklad okruhu, který je oborem integrity a není tělesem.

Řešení

1. ano a) 3, b) $-x + 6$, c) ano, d) ne, e) ano
2. ano a) -1, b) $-x - 2$, c) 0, d) $y = \frac{-x}{1+x}$
3. a) ano, b) ne

9 Podstruktury struktur se dvěma operacemi

Studijní cíle: V této kapitole se studující seznámí s pojmy podokruh, podtěleso a číselné těleso.

Klíčová slova: podokruh okruhu, podokruh tělesa, podtěleso okruhu, podtěleso tělesa, číselné těleso

9.1 Podokruhy a podtělesa

Definice 9.1. Nechť $(R, +, .)$ je okruh, nechť S je neprázdná podmnožina v R, uzavřená vzhledem k operacím + a . .

Je-li $(S, +, .)$ okruh, pak jej nazýváme *podokruh okruhu* $(R, +, .)$. Je-li $(S, +, .)$ těleso, pak jej nazýváme *podtěleso okruhu* $(R, +, .)$.

V případě, že $(R, +, .)$ je těleso, hovoříme o *podokruhu tělesa* nebo o *podtělese tělesa*.

Průvodce studiem

Podokruh okruhu je tedy podmnožina okruhu, která je sama okruhem. Podtěleso okruhu je podmnožina okruhu, která je tělesem. Podokruh tělesa je podmnožina tělesa, která je okruhem a podtěleso tělesa je podmnožina tělesa, která je rovněž tělesem. Podstruktury samozřejmě musí mít stejné operace jako struktury.

Příklad 9.2.
1. ($\mathbb{S}$, +, .) je podokruh okruhu ($\mathbb{Z}$, +, .)
2. $(R0, +, .)$ je podtěleso okruhu ($\mathbb{R} \times \mathbb{R}$, +, .)
3. ($\mathbb{Z}$, +, .) je podokruh tělesa ($\mathbb{Q}$, +, .)
4. ($\mathbb{Q}$, +, .) je podtěleso tělesa ($\mathbb{R}$, +, .)

$(S, +)$ *je podgrupa grupy* $(R, +)$

$(S, .)$ *je podgrupoid grupoidu* $(R, .)$

Průvodce studiem

Je-li $(S, +, .)$ podokruh okruhu $(R, +, .)$, nulové prvky okruhů se rovnají. Pro jedničky to obecně neplatí. Některý z okruhů jedničku nemusí mít, pokud ji oba mají, mohou být jedničky různé.

Příklad 9.3. $(R0, +, .)$ je podtěleso okruhu ($\mathbb{R} \times \mathbb{R}$, +, .). $(R0, +, .)$ má jedničku (1, 0), ($\mathbb{R} \times \mathbb{R}$, +, .) má jedničku (1, 1).

v tom případě je $(S - \{0\}, .)$ *podgrupa grupy* $(R - \{0\}, .)$

Průvodce studiem

Je-li $(S, +, .)$ podtěleso tělesa $(R, +, .)$, pak musí platit $1_S = 1_R$

Následující věty nám udávají kritéria pro ověření toho, zda $(S, +, .)$ je podokruhem okruhu nebo podtělesem tělesa.

Věta 9.4. *Nechť* $(R, +, .)$ *je okruh, nechť* S *je neprázdná podmnožina množiny* R*. Potom* $(S, +, .)$ *je podokruh okruhu* $(R, +, .)$*, právě když platí*

1. *Pro každou dvojici prvků* $a, b \in S$ *je* $a - b \in S$ — $(S, +)$ *je podgrupa grupy* $(R, +)$
2. *Pro každou dvojici prvků* $a, b \in S$ *je* $a.b \in S$ — $(S, .)$ *je podgrupoid grupoidu* $(R, .)$

Důkaz. Plyne ihned z definice podokruhu. □

Věta 9.5. *Nechť* $(R, +, .)$ *je těleso, nechť* S *je alespoň dvouprvková podmnožina množiny* R. *Potom* $(S, +, .)$ *je podtělesem tělesa* $(R, +, .)$, *právě když platí*

1. *Pro každou dvojici prvků* $a, b \in S$ *je* $a - b \in S$ — $(S, +)$ *je podgrupa grupy* $(R, +)$
2. *Pro každou dvojici prvků* $a, b \in S$ *je* $a.b^{-1} \in S$ — $(S - \{0\}, .)$ *je podgrupa grupy* $(R - \{0\}, .)$

Důkaz. Plyne ihned z definice podtělesa. □

Příklad 9.6. Nechť $(R, +, .)$ je okruh. Označme

$$S = \{a \in R | \text{ pro každé } x \in R \text{ platí } a.x = x.a \ \}.$$

Dokážeme, že $(S, +, .)$ je podokruh okruhu $(R, +, .)$.
Řešení: Dokazujeme podle věty 9.4. S je podmnožina množiny R. Nula patří do S, S je tedy neprázdná množina. Pro prvky $a, b \in S$ platí $a.x = x.a$ a současně $b.x = x.b$. Platí tedy $(a - b).x = a.x - b.x = x.a - x.b = x.(a - b)$, což znamená, že $a - b \in S$. Dále platí $(a.b).x = a.(b.x) = a.(x.b) = (a.x).b = (x.a).b = x.(a.b)$, což znamená, že $a.b \in S$.
$(S, +, .)$ je tedy podokruh okruhu $(R, +, .)$.

9.2 Číselné těleso

Průvodce studiem

V předcházející kapitole jsme zavedli pojem těleso, v této kapitole pojem podtěleso. Většinou jsme pracovali s tělesy, jejichž prvky byla čísla. V následujících kapitolách budeme opět pracovat s takovými tělesy, proto si zavedeme pojem číselné těleso.

Definice 9.7. Nechť $(T, +, .)$ je podtělesem tělesa komplexních čísel ($\mathbb{C}$, +, .). Potom $(T, +, .)$ se nazývá *číselné těleso*.

Příklad 9.8. ($\mathbb{Q}$, +, .), ($\mathbb{R}$, +, .), ($\mathbb{C}$, +, .) jsou číselná tělesa.

Příklad 9.9. Označme

$$\mathbb{Q}(\sqrt{11}) = \{a + b.\sqrt{11} |\ a, b \in \mathbb{Q}\}.$$

Dokažte, že $\mathbb{Q}(\sqrt{11}, +, .)$ je číselné těleso.
Řešení: Dokážeme použitím věty 9.5 :
Množina $(\mathbb{Q}(\sqrt{11})$ zřejmě obsahuje více než jeden prvek.
Nechť $a + b.\sqrt{11}, c + d.\sqrt{11} \in \mathbb{Q}(\sqrt{11})$, to znamená $a, b, c, d \in \mathbb{Q}$.

$$(a + b.\sqrt{11}) - (c + d.\sqrt{11}) = (a - c) + (b - d).\sqrt{11} \in \mathbb{Q}(\sqrt{11}),$$

protože $a - c, b - d \in \mathbb{Q}$.

$$(a + b.\sqrt{11}).(c + d.\sqrt{11})^{-1} = \frac{a + b.\sqrt{11}}{c + d.\sqrt{11}} = \frac{(a + b.\sqrt{11})(c - d.\sqrt{11})}{(c + d.\sqrt{11})(c - d.\sqrt{11})} =$$

$$= \frac{a.c - 11.b.d}{c^2 - 11.d^2} + \frac{b.c - a.d}{c^2 - 11.d^2}.\sqrt{11} \in \mathbb{Q}(\sqrt{11}),$$

protože

$$\frac{a.c - 11.b.d}{c^2 - 11.d^2}, \frac{b.c - a.d}{c^2 - 11.d^2} \in \mathbb{Q}.$$

Věta 9.10. *Nechť $(T, +, .)$ je libovolné číselné těleso. Potom platí, že $(T, +, .)$ obsahuje těleso racionálních čísel (to znamená $T \supseteq \mathbb{Q}$).*

Důkaz. Z definice tělesa plyne, že musí existovat prvek $a \in T, a \neq 0$. Potom $\frac{a}{a} = 1 \in T$, to znamená, že těleso obsahuje prvek 1. Sečteme-li jedničku se sebou samou libovolněkrát, pak výsledek musí ležet v T. To znamená, že těleso T obsahuje množinu všech přirozených čísel $\mathbb{N}$. $a - a = 0 \in T$ a pro libovolné číslo n je $-n = 0 - n \in T$. Těleso T tedy obsahuje všechna záporná čísla. Je tedy $\mathbb{Z} \subseteq T$. V T leží i podíl libovolných dvou celých čísel s nenulovým jmenovatelem, to znamená každé racionální číslo. Odtud dostáváme $\mathbb{Q} \subseteq T$. □

Průvodce studiem

Těleso racionálních čísel je tedy nejmenší číselné těleso.

Shrnutí

Podokruh okruhu je podmnožina okruhu se stejnými operacemi, která je okruhem.
Podtěleso okruhu je podmnožina okruhu se stejnými operacemi, která je tělesem.
Podokruh tělesa je podmnožina tělesa se stejnými operacemi, která je okruhem.
Podtěleso tělesa je podmnožina tělesa se stejnými operacemi, která je tělesem.
Číselné těleso je podtěleso tělesa komplexních čísel.
Nejmenší číselné těleso je těleso racionálních čísel.

Pojmy k zapamatování

- podokruh okruhu
- podtěleso okruhu
- podokruh tělesa
- podtěleso tělesa
- číselné těleso

Kontrolní otázky

1. *Když (S, +, .) je podokruh okruhu (R, +, .), je (S,+) podgrupa grupy (R, +) ?*
2. *Je ($\mathbb{Z}$, +, .) číselné těleso ?*
3. *Jak zjistíme, že (T, +, .) je číselné těleso ?*

Cvičení

1. Množina M je dána vztahem

$$M = \{a + 7.b |\ a, b \in \mathbb{Z}\}.$$

   Je $(M, +, .)$ podokruhem okruhu ($\mathbb{Z}$, +, .) ?
2. Rozhodněte, zda $(T, +, .)$ je číselné těleso, jestliže + značí obyčejné sčítání čísel a . obyčejné násobení čísel a je-li
   (a) $T = \{a + b.\sqrt[3]{2} |\ a, b \in \mathbb{Q}\}$
   (b) $T = \{a + b.\sqrt{2} |\ a, b \in \mathbb{Q}\}$

Úkoly k textu

1. Uveďte příklad okruhu, který nemá jedničku a jeho podokruhu, který jedničku má.
2. Uveďte příklad tělesa, které není číselným tělesem.
3. Uveďte příklad číselného tělesa $(T, +, .)$ takového, že platí $\mathbb{Q} \subset T \subset \mathbb{R}$.

Řešení

1. ano
2. a) ne, b) ano

10 Vektorové prostory a jejich podprostory

Studijní cíle: Při studiu této kapitoly se studující seznámí s pojmy vektorový prostor, podprostor vektorového prostoru a podprostor generovaný množinou. S těmito pojmy budeme více pracovat v dalších kapitolách.

Klíčová slova: vektorový prostor, nulový vektor, podprostor vektorového prostoru, podprostor generovaný množinou, podprostor generovaný vektory, generátory podprostoru

10.1 Vektorové prostory

Průvodce studiem

Pojem vektoru a vektorového prostoru je jedním ze základních pojmů moderní matematiky a využívá se jej nejen v řadě disciplin ryzí matematiky, ale i v mnoha aplikacích.

Definice 10.1. Nechť $(V, +)$ je komutativní grupa, jejíž prvky nazýváme vektory, a nechť $(T, +, .)$ je číselné těleso. Nechť pro každé číslo $t \in T$ a každý vektor $u \in V$ je definován vektor $t.u \in V$ tak, že pro libovolné $t, s \in T$ a libovolné $u, v \in V$ platí:

1. $t.(u + v) = t.u + t.v$,
2. $(t + s).u = t.u + s.u$,
3. $(t.s).u = t.(s.u)$,
4. $1.u = u$.

Potom V se nazývá *vektorový prostor nad tělesem* T.

Poznámka 10.2.

- Nulový prvek z $(V, +)$ nazýváme *nulový vektor* a označujeme o.
- Opačný prvek k vektoru $u \in V$ nazýváme *opačný vektor k vektoru* u.
- Vektor $t.u$ se nazývá *součin čísla* t *s vektorem* u

Průvodce studiem

Z definice vektorového prostoru je zřejmé, že pokud chceme korektně definovat nějaký vektorový prostor, musíme

1. zadat číselné těleso T,
2. zadat množinu vektorů V,
3. zadat, jak je definováno sčítání vektorů,
4. zadat, jak je definován součin čísla z T s vektorem z V,
5. ověřit, že $(V, +)$ je komutativní grupa,
6. ověřit, že platí všechny čtyři axiomy z definice vektorového prostoru.

Poznámka 10.3. Ze střední školy víme, že vektory v rovině mohou být vyjádřeny jako uspořádaná dvojice reálných čísel – souřadnic vektorů. Podobně víme, že vektory v třírozměrném prostoru mohou být vyjádřeny jako uspořádaná trojice souřadnic vektoru. Přitom každý vektor je svými souřadnicemi plně určen. Podobně můžeme definovat vektory jakéhokoliv rozměru. Viz následující příklad.

vektorový prostor T^n

Příklad 10.4. T je libovolné číselné těleso, n je pevné přirozené číslo a nechť

$$T^n = \{(x_1, x_2, ..., x_n) | x_1, x_2, ..., x_n \in T\}$$

je množina všech uspořádaných n-tic prvků z tělesa T. Definujeme pro libovolné $u = (u_1, u_2, ..., u_n), v = (v_1, v_2, ..., v_n) \in T^n$ a $t \in T$

$$u + v = (u_1 + v_1, u_2 + v_2, ..., u_n + v_n) \qquad t.u = (t.u_1, t.u_2, ..., t.u_n)$$

kde symboly + a . na pravé straně znamenají sečítání a násobení čísel. Říkáme, že sčítání vektorů a násobení čísla vektorem je definováno po složkách. $(T^n, +)$ je zřejmě grupoid, který je asociativní a komutativní. Nulovým prvkem je vektor (0, 0, ... , 0) a opačným vektorem k vektoru $(u_1, u_2, ..., u_n)$ je vektor $(-u_1, -u_2, ..., -u_n)$. Je tedy $(T^n, +)$ komutativní grupa. $t.u \in T^n$ pro $t \in T, u \in T^n$. Snadno se ověří čtyři axiomy z definice. T^n je tedy vektorovým prostorem nad číselným tělesem T. Specielně jsou $\mathbb{R}^2, \mathbb{R}^3, \mathbb{Q}^2, \mathbb{Q}^5, \mathbb{C}^4$ vektorové prostory tohoto typu.

nulový vektorový prostor $V = \{o\}$

Příklad 10.5. T je libovolné číselné těleso a $V = \{v\}$ je libovolná jednoprvková množina. Definujeme sčítání vektorů a násobení čísla a vektoru

$$v + v = v, \qquad t.v = v \text{ pro všechna } t \in T$$

Potom zřejmě je $(V, +)$ komutativní grupa a platí všechny čtyři axiomy z definice. V je tedy vektorovým prostorem nad číselným tělesem T, nazýváme jej *nulový vektorový prostor* (nad T). Je to tedy vektorový prostor, který obsahuje jediný vektor a to vektor nulový, $v = o$.

Příklad 10.6. Uvažujeme množinu $\mathbb{Q}(\sqrt{11}) = \{a + b.\sqrt{11} | a, b \in \mathbb{Q}\}$ a číselné těleso $T = \mathbb{R}$. Z předchozí kapitoly víme, že $(\mathbb{Q}(\sqrt{11}), +)$ je komutativní grupa. Když vezmeme např. $t = \sqrt{2} \in \mathbb{R}$ a počítáme

$$\sqrt{2}.(a + b.\sqrt{11}) = (a.\sqrt{2} + b.\sqrt{2}.\sqrt{11}) \qquad a.\sqrt{2}, b.\sqrt{2} \notin \mathbb{Q}$$

a tedy $\sqrt{2}.(a + b.\sqrt{11}) \notin \mathbb{Q}(\sqrt{11})$. $\mathbb{Q}(\sqrt{11})$ tedy není vektorový prostor nad číselným tělesem $\mathbb{R}$. Snadno se přesvědčíme, že $\mathbb{Q}(\sqrt{11})$ je vektorovým prostorem nad číselným tělesem $\mathbb{Q}$.

Průvodce studiem

Množina vektorů V je vždy neprázdná. Nulový vektor ve V existuje jedinný a ke každému vektoru existuje jedinný opačný vektor. Tato tvrzení plynou z faktu, že $(V, +)$ je grupa. Musíme rozlišovat nula 0 a nulový vektor o.

Věta 10.7 (pro počítání s vektory). *Nechť V je vektorový prostor nad číselným tělesem T a nechť $t, s \in T$ a $u, v \in V$ jsou libovolné. Pak platí*

1. $t.(u - v) = t.u - t.v$,
2. $(t - s).u = t.u - s.u$,
3. $t.u = o$ *právě tehdy, když* $t = 0$ *nebo* $u = o$,

4. $t.(-u) = (-t).u = -(t.u)$.

Důkaz. Dokážeme použitím axiomů 1. – 4. z definice vektorového prostoru.

1. $t.(u - v) = t.(u + (-v)) + t.v - t.v = t.(u + (-v) + v) - t.v = t.u - t.v$.

2. $(t - s).u = (t + (-s)).u + s.u - s.u = (t + (-s) + s).u - s.u = t.u - s.u$.

3. Tvrzení má tvar ekvivalence, musíme tedy dokázat implikace

   Pokud $t.u = o$, potom $t = 0$ nebo $u = o$.

   Pokud $t = 0$ nebo $u = o$, potom $t.u = o$.

   Dokazujeme první implikaci. Předpokládáme, že $t.u = o$. Současně předpokládáme $t \neq 0$ a dokážeme, že $u = o$. Podle axiomu 4. z definice je $u = 1.u$, ale to můžeme zapsat ve tvaru
   $$(\frac{1}{t}.t).u = \frac{1}{t}.(t.u) = \frac{1}{t}.o = o.$$
   Dokazujeme druhou implikaci. Je-li $t = 0$, platí $0.u = (0 - 0).u = 0.u - 0.u = o$ podle 2.
   Je-li $u = o$, platí $t.o = t.(o - o) = t.o - t.o = o$ podle 1.

4. použijeme 1.,2.a 3.
   $t.(-u) = t.(o - u) = t.o - t.u = o - t.u = -t.u$.
   $(-t).u = (0 - t).u = 0.u - t.u = -t.u$.

□

10.2 Podprostory vektorových prostorů

Definice 10.8. Nechť V je vektorový prostor nad číselným tělesem T. Neprázdná podmnožina W množiny V se nazývá *podprostor vektorového prostoru* V, jestliže:

podprostor je uzavřený vzhledem k daným operacím sčítání vektorů a násobení vektoru číslem

1. Pro každou dvojici prvků $u, v \in W$ platí $u + v \in W$,
2. pro každý prvek $u \in W$ a číslo $t \in T$ platí $t.u \in W$.

Průvodce studiem

Každý podprostor W vektorového prostoru V musí vždy obsahovat nulový vektor

$$u \in W, 0 \in T \Rightarrow 0.u = o \in W$$

Věta 10.9. *Nechť W je podprostor vektorového prostoru V nad číselným tělesem T. Potom W je sám vektorovým prostorem nad tělesem T.*

Důkaz. Součet dvou vektorů z W a součin čísla z T s vektorem z W jsou definovány stejně jako ve V. Vezmeme libovolné prvky $u, v \in W$. Potom platí $(-1).v = -v \in W$. Dále platí $u - v = u + (-v) \in W$. $(W, +)$ je tedy podgrupou grupy $(V, +)$, která je komutativní. Tedy i grupa $(W, +)$ je komutativní. Axiomy z definice vektorového prostoru jsou ve W zřejmě splněny, protože jsou splněny v celém V. □

Poznámka 10.10. Každý vektorový prostor V je zřejmě podprostorem sám v sobě. Nulový vektorový prostor je podprostorem všech vektorových prostorů. Tyto dva podprostory se nazývají *triviální podprostory* vektorového prostoru. Všechny ostatní podprostory vektorového prostoru, pokud existují, se nazývají *netriviální podprostory* vektorového prostoru.

Příklad 10.11. Uvažujeme vektorový prostor $\mathbb{R}^3$ a množinu

$$W_1 = \{(x, 0, y) | x = y, x, y \in \mathbb{R}\}.$$

W_1 je neprázdná podmnožina R^3. Vezmeme libovolné $(x_1, 0, y_1), (x_2, 0, y_2) \in W_1$. Potom dostaneme $x_1 = y_1, x_2 = y_2$

$$(x_1, 0, y_1) + (x_2, 0, y_2) = (x_1 + x_2, 0, y_1 + y_2) \in W_1 \qquad x_1 + x_2 = y_1 + y_2$$

$$t.(x_1, 0, y_1) = (t.x_1, 0, t.y_1) \in W_1, \quad t \in \mathbb{R} \qquad t.x_1 = t.y_1$$

Podle definice je W_1 je podprostor vektorového prostoru $\mathbb{R}^3$.

Příklad 10.12. Uvažujeme opět vektorový prostor $\mathbb{R}^3$ a množinu

$$W_2 = \{(x, y, z) | x \geq 0, x, y, z \in \mathbb{R}\}.$$

W_2 je neprázdná podmnožina $\mathbb{R}^3$. Vezmeme libovolné prvky $x_1 \geq 0, x_2 \geq 0$

$$(x_1, y_1, z_1), (x_2, y_2, z_2) \in W_2.$$

Potom platí $x_1 + x_2 \geq 0$

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2) \in W_2$$

Pokud vezmeme $t < 0, t \in \mathbb{R}$ $t.x_1 < 0$ *pro* $t < 0$

$$t.(x_1, y_1, z_1) = (t.x_1, t.y_1, t.z_1) \notin W_2$$

Podle definice W_2 tedy není podprostorem vektorového prostoru $\mathbb{R}^3$.

průnik podprostorů prostoru V je opět podprostorem prostoru V

Věta 10.13. *Nechť V je vektorový prostor nad číselným tělesem T, nechť I je indexová množina a nechť pro každé $i \in I$ je W_i podprostor ve V. Potom $\bigcap_{i \in I} W_i$ je podprostor ve V.*

Důkaz. Množina $\bigcap_{i \in I} W_i$ je neprázdná, obsahuje jistě nulový vektor o. Musíme ověřit platnost podmínek 1. a 2. z definice podprostorů. Nechť $u, v \in \bigcap_{i \in I} W_i$ a $t \in T$ jsou libovolné, potom podle definice průniku množin platí $u, v \in W_i$ pro všechna $i \in I$. W_i jsou podprostory, proto $u + v \in W_i$ a $t.u \in W_i$ pro všechna $i \in I$. Opět podle definice průniku množin dostaneme $u + v \in \bigcap_{i \in I} W_i$ a $t.u \in \bigcap_{i \in I} W_i$ □

Průvodce studiem

Stručně řečeno, věta tvrdí, že průnikem libovolného počtu (konečného i nekonečného) podprostorů ve V je opět podprostor ve V.
Sjednocení podprostorů ve V nemusí být podprostorem ve V.

Poznámka 10.14. Nechť M je libovolná podmnožina vektorového prostoru V (M nemusí být podprostorem). Pak existuje alespoň jeden podprostor, který obsahuje množinu M (např. celý prostor V má tuto vlastnost). Můžeme tedy vytvořit průnik všech podprostorů, které obsahují množinu M. Tento průnik označíme $[M]$. Je tedy

$$[M] = \bigcap W_\alpha (W_\alpha \text{ je podprostor ve } V \text{ takový, že } M \subseteq W_\alpha)$$

průnik všech podprostorů prostoru V, které obsahují množinu M

a platí následující tvrzení

Věta 10.15. *Nechť M je libovolná podmnožina ve vektorovém prostoru V. Potom*

1. *$[M]$ je podprostor ve V*
2. *$[M]$ je nejmenší (vzhledem k $\subseteq$) podprostor ve V obsahující množinu M*

Důkaz. 1. Plyne přímo z předcházející věty.

2. Plyne z 1. a ze základních vlastností množinových průniků.

□

Definice 10.16. Nechť M je podmnožina ve vektorovém prostoru V a nechť $W = [M]$. Pak podprostor W se nazývá *podprostor generovaný množinou* M. Je-li specielně $M = \{u_1, u_2, ..., u_n\}$ pak W se nazývá *podprostor generovaný vektory* $u_1, u_2, ..., u_n$ a vektory $u_1, u_2, ..., u_n$ se nazývají *generátory podprostoru* W.

podprostor generovaný vektory

Poznámka 10.17. V literatuře se podprostor generovaný množinou M rovněž nazývá *lineární obal množiny* M.

Shrnutí

Vektorový prostor je komutativní grupa, jejíž prvky vynásobené číslem z daného číselného tělesa dávají opět vektory z této grupy a přitom sčítání vektorů a násobení vektoru číslem splňují 4 axiomy.
Podprostor vektorového prostoru je podmnožina vektorového prostoru, která je uzavřená vzhledem k operacím sčítání vektorů a násobení vektoru číslem.
Podprostor generovaný množinou je průnik všech podprostorů, které tuto množinu obsahují.

Pojmy k zapamatování

- vektorový prostor nad číselným tělesem
- nulový vektor
- vektor opačný k danému vektoru
- nulový vektorový prostor
- podprostor vektorového prostoru
- podprostor generovaný množinou
- podprostor generovaný vektory
- generátory podprostoru

Kontrolní otázky

1. *Jak korektně definujeme vektorový prostor?*
2. *Co musí splňovat podmnožina vektorového prostoru, aby byla podprostorem tohoto prostoru?*
3. *Obsahuje podprostor generovaný množinou M nějaký podprostor obsahující tuto množinu?*
4. *Můžeme sestrojit vektorový prostor nad číselným tělesem, který obsahuje právě 8 prvků?*

Cvičení

1. Rozhodněte, zda množina $V = \{x \in \mathbb{R} | x \geq 0\}$ s obvyklým sčítáním a násobením tvoří vektorový prostor.
2. Nechť u, v, w jsou vektory vektorového prostoru V. Zjednodušte:

$$3(2(u - 2v - w) + 3(w - v)) - 7(u - 3v - w)$$

3. Je dána množina čísel $V = \{a + b.\sqrt{3} |\ a, b \in \mathbb{Z}\}$. Sčítání vektorů definujeme jako obyčejné sčítání čísel a násobení čísla s vektorem definujeme jako obyčejné násobení čísel. Rozhodněte, zda V je vektorovým prostorem nad číselným tělesem $\mathbb{Q}$
4. Nechť V_1, V_2 jsou vektorové prostory nad číselným tělesem T. Pro libovolné $(u_1, u_2), (v_1, v_2) \in V_1 \times V_2$ a $t \in T$ definujeme

$$(u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2),$$

$$t.(u_1, u_2) = (t.u_1, t.u_2).$$

   Je $V_1 \times V_2$ vektorový prostor?
   (a) nad číselným tělesem T,
   (b) nad číselným tělesem $T \times T$.
5. Rozhodněte, zda podmnožina $W \subseteq \mathbb{R}^3$, kde

$$W = \{(3.r, -r, \sqrt{3}.r) |\ \forall r \in \mathbb{R}\},$$

   je podprostorem vektorového prostoru $\mathbb{R}^3$.
6. Rozhodněte, zda množina W = {(0,0,0,0), (1,1,1,1), (-1,-1,-1,-1)} $\subseteq \mathbb{Q}^4$ je podprostorem vektorového prostoru $\mathbb{Q}^4$.

Úkoly k textu

1. Uveďte příklad vektorového prostoru nad číselným tělesem, který obsahuje konečně mnoho prvků.
2. Uveďte příklad podmnožiny M vektorového prostoru $\mathbb{Q}^4$, která je konečná a je podprostorem v $\mathbb{Q}$.
3. Uveďte příklad podmnožiny M ve vektorovém prostoru $\mathbb{R}^4$ tak, aby $M = [M]$.
4. Popište vektorový prostor $\mathbb{C}^5$.
5. Uveďte příklad podprostoru W ve vektorovém prostoru $\mathbb{Q}^3$ tak, že

$$(1, 4, 2) \in W \wedge (1, 1, 1) \notin W$$

Řešení

1. ne, $(V, +)$ není grupa
2. $-u + 10w$
3. ne
4. a) ne, b) ano
5. ano
6. ne

11 Lineární závislost a nezávislost vektorů

Studijní cíle: Při studiu této kapitoly se studující seznámí s pojmy lineární kombinace vektorů a množina všech lineárních kombinací vektorů a pozná jaký je vztah mezi množinou všech lineárních kombinací vektorů a podprostorem generovaným těmito vektory. Pozná rovněž, co znamenají pojmy lineární závislost a nezávislost vektorů.

Klíčová slova: lineární kombinace vektorů, množina všech lineárních kombinací vektorů, lineárně závislé vektory, lineárně nezávislé vektory

Definice 11.1. Nechť V je vektorový prostor nad číselným tělesem T a nechť $u_1, u_2, ..., u_n$ je konečná posloupnost vektorů z V. Pak vektor

$$u = t_1.u_1 + t_2.u_2 + ... + t_n.u_n, \qquad \text{kde} \quad t_1, t_2, ..., t_n \in T$$

se nazývá *lineární kombinace vektorů* $u_1, u_2, ..., u_n$. *Množina všech lineárních kombinací vektorů* $u_1, u_2, ..., u_n$ se označuje $L(u_1, u_2, ..., u_n)$

$$L(u_1, u_2, ..., u_n) = \{t_1.u_1 + t_2.u_2 + ... + t_n.u_n |\ t_1, t_2, ..., t_n \in T \text{ libovolné } \}$$

Poznámka 11.2.

1. Je možné, aby se některý z vektorů vyskytoval i vícekrát. Vektory chápeme v uvedeném pořadí. $L(u_1, u_2, ..., u_n)$ znamená množinu všech lineárních kombinací vektorů $u_1, u_2, ..., u_n$. Vektorů může být i nekonečně mnoho.

   $u_i = 0.u_1 + ... + 0.u_{i-1} + 1.u_i + 0.u_{i+1} + ... + 0.u_n$
   $o = 0.u_1 + 0.u_2 + ... + 0.u_n$

2. $L(u_1, u_2, ..., u_n)$ obsahuje vždy každý z vektorů $u_1, u_2, ..., u_n$.

3. $L(u_1, u_2, ..., u_n)$ obsahuje vždy nulový vektor.

Průvodce studiem

Jaký je vztah mezi podprostorem $[u_1, u_2, ..., u_n]$ generovaným vektory $u_1, u_2, ..., u_n$ a množinou $L(u_1, u_2, ..., u_n)$ všech lineárních kombinací vektorů $u_1, u_2, ..., u_n$? Na tuto otázku nám odpoví následující věta.

Věta 11.3. *Nechť V je vektorový prostor nad číselným tělesem T a nechť $u_1, u_2, ..., u_n$ je konečná posloupnost vektorů z V. Pak platí*

1. $L(u_1, u_2, ..., u_n)$ *je podprostor ve* V.
2. $[u_1, u_2, ..., u_n] = L(u_1, u_2, ..., u_n)$,
   to znamená, že podprostor generovaný vektory $u_1, u_2, ..., u_n$ *je roven množině všech lineárních kombinací vektorů* $u_1, u_2, ..., u_n$.

Důkaz.

1. Provedeme ověřením definice podprostoru.
2. Budeme dokazovat množinovou rovnost
   $\bigcap_{i \in I} W_i (W_i$ je podprostor ve V a současně $u_1, u_2, ..., u_n \in W_i) = L(u_1, u_2, ..., u_n)$.
   „$\subseteq$“ plyne z vlastností množinového průniku, když si uvědomíme, že podle 1. části této věty $L(u_1, u_2, ..., u_n)$ je podprostor ve V a že $u_1, u_2, ..., u_n \in L(u_1, u_2, ..., u_n)$.
   „$\supseteq$“ množina na levé části inkluze je podprostor ve V, který obsahuje vektory $u_1, u_2, ..., u_n$. To znamená, že musí obsahovat rovněž jejich libovolnou lineární kombinaci.

□

Průvodce studiem

Vidíme, že podprostor generovaný vektory $u_1, u_2, ..., u_n$ a podprostor lineárních kombinací vektorů $u_1, u_2, ..., u_n$ je jedno a totéž.

podprostor generovaný vektory $v_1, v_2, ..., v_k$ je podprostorem podprostoru generovaného vektory $u_1, u_2, ..., u_n$

Věta 11.4. *Nechť V je vektorový prostor nad číselným tělesem T, nechť $u_1, u_2, ..., u_n$ je konečná posloupnost vektorů z V a nechť $v_1, v_2, ..., v_k \in L(u_1, u_2, ..., u_n)$. Pak platí:*

1. $L(v_1, v_2, ..., v_k) \subseteq L(u_1, u_2, ..., u_n)$ *neboli* $[v_1, v_2, ..., v_k] \subseteq [u_1, u_2, ..., u_n]$,
2. $[u_1, u_2, ..., u_n, v_1, v_2, ..., v_k] = [u_1, u_2, ..., u_n]$.

z generátorů můžeme vynechat vektory $v_1, v_2, ..., v_k$

Důkaz. 1. Plyne z definice podprostoru generovaného vektory $u_1, u_2, ..., u_n$ a z 2. části předchozí věty.

2. Dokazujeme opět jako množinovou rovnost.
„$\supseteq$“ plyne z definice podprostoru generovaného vektory $u_1, u_2, ..., u_n$.
„$\subseteq$“ triviálně je $u_1, u_2, ..., u_n \in L(u_1, u_2, ..., u_n)$.
Podle předpokladu je $v_1, v_2, ..., v_k \in L(u_1, u_2, ..., u_n)$.
Podle 1. části je pak

$$[u_1, u_2, ..., u_n, v_1, v_2, ..., v_k,] \subseteq [u_1, u_2, ..., u_n].$$

Dohromady platí dokazovaná rovnost.

□

Průvodce studiem

Vidíme tedy, že když přidáme ke generátorům daného podprostoru W libovolný vektor, který je jejich lineární kombinací, dostáváme opět generátory W. Když odstraníme z generátorů podprostoru W vektor, který je lineární kombinací zbývajících vektorů, dostáváme opět generátory W.

$e_1, e_2, ..., e_n$ jsou generátory vektorového prostoru T^n

Příklad 11.5. 1. Je dán vektorový prostor $T^n = [e_1, e_2, ..., e_n]$, kde

$$e_1 = (1, 0, ..., 0), e_2 = (0, 1, ..., 0), ..., e_n = (0, 0, ..., 1).$$

Libovolný vektor $u \in T^n$ můžeme vyjádřit ve tvaru

$$u = u_1.e_1 + u_2.e_2 + ... + u_n.e_n.$$

kdyby (1,2) byl generátor, např. vektor (1,3) nemůžeme určit pomocí vektoru (1,2)

2. $\mathbb{R}^2$=[(1, 0), (0, 1)]=[(1, 2), (3, 2)]=[(0, 1), (1, 1), (2, 0)]=[(-1, 1), (1, 2), (2,1), (1, -4)]. Vidíme, že vektorový prostor $\mathbb{R}^2$ můžeme generovat dvěma i více vektory, i nekonečně mnoha vektory, ale nemůžeme jej generovat jedním vektorem.

Definice 11.6. Nechť V je vektorový prostor nad číselným tělesem T a nechť $u_1, u_2, ..., u_n$ je konečná posloupnost vektorů z V. Jestliže existují čísla $t_1, t_2, ..., t_n \in T$, z nichž aspoň jedno je různé od nuly taková, že

$$t_1.u_1 + t_2.u_2 + ... + t_n.u_n = o$$

pak říkáme, že vektory $u_1, u_2, ..., u_n$ jsou *lineárně závislé*. V opačném případě říkáme, že vektory jsou *lineárně nezávislé*.

Průvodce studiem

Definici můžeme říci i jinak: Vektory jsou lineárně nezávislé, jestliže platí
$t_1.u_1 + t_2.u_2 + ... + t_n.u_n = o$ právě tehdy, když $t_1 = t_2 = ... = t_n = 0$.
Tohoto používáme k praktickému zjišťování lineární závislosti či nezávislosti vektorů. Hledáme čísla $t_1, t_2, ..., t_n$ tak, aby

$$t_1.u_1 + t_2.u_2 + ... + t_n.u_n = o.$$

Když $t_1 = t_2 = ... = t_n = 0$, jsou $u_1, u_2, ..., u_n$ lineárně nezávislé, když některé z čísel $t_1, t_2, ..., t_n$ je různé od nuly, jsou vektory $u_1, u_2, ..., u_n$ lineárně závislé.

Příklad 11.7. 1. Vektory $e_1, e_2, ..., e_n$, které generují vektorový prostor T^n, jsou lineárně nezávislé. Rozepíšeme-li rovnost

vektory $e_1, e_2, ..., e_n$ jsou lineárně nezávislé

$$t_1.e_1 + t_2.e_2 + ... + t_n.e_n = o$$

do souřadnic, dostaneme soustavu rovnic

$$\begin{aligned} t_1.1 + t_2.0 + ... + t_n.0 &= 0 \\ t_1.0 + t_2.1 + ... + t_n.0 &= 0 \\ &... \\ t_1.0 + t_2.0 + ... + t_n.1 &= 0 \end{aligned}$$

a ta má pouze nulové řešení $t_1 = t_2 = ... = t_n = 0$.
Specielně vektory $(1, 0), (0, 1)$ generující vektorový prostor $\mathbb{R}^2$ jsou lineárně nezávislé.

vektory (1,0), (0,1) jsou lineárně nezávislé

2. Rovněž vektory (1, 2), (3, 2) generující vektorový prostor $\mathbb{R}^2$ jsou lineárně nezávislé. Rozepsáním rovnosti

vektory (1,2), (3,2) jsou lineárně nezávislé

$$t_1.(1, 2) + t_2.(3, 2) = o$$

do souřadnic, dostaneme soustavu rovnic

$$\begin{aligned} 1.t_1 + 3.t_2 &= 0 \\ 2.t_1 + 2.t_2 &= 0, \end{aligned}$$

která má opět pouze nulové řešení $t_1 = t_2 = 0$.

vektory(0,1), (1,1), (2,0) jsou lineárně závislé

3. Generátory (0, 1), (1, 1), (2, 0) vektorového prostoru $\mathbb{R}^2$ jsou lineárně závislé, z rovnosti

$$t_1.(0, 1) + t_2.(1, 1) + t_3.(2, 0) = o$$

dostaneme soustavu rovnic

$$\begin{aligned} 0.t_1 + 1.t_2 + 2.t_3 &= 0 \\ 1.t_1 + 1.t_2 + 0.t_3 &= 0, \end{aligned}$$

která má nekonečně mnoho nenulových řešení.

vektory (-1,1), (1,2), (2,1), (1,-4) jsou lineárně závislé

4. Stejným způsobem můžeme ukázat, že generátory

$$(-1, 1), (1, 2), (2, 1), (1, -4)$$

vektorového prostoru $\mathbb{R}^2$ jsou lineárně závislé.

Věta 11.8. *Nechť V je vektorový prostor nad číselným tělesem T, nechť $k \geq 2$ a $u_1, u_2, ..., u_k \in V$. Pak následující výroky jsou ekvivalentní*

1. *Vektory $u_1, u_2, ..., u_k$ jsou lineárně závislé.*
2. *Existuje i ($1 \leq i \leq k$) takové, že vektor u_i je lineární kombinací zbývajících vektorů, tj. vektorů*
$$u_1, u_2, ..., u_{i-1}, u_{i+1}, ..., u_k.$$
3. *Existuje i ($1 \leq i \leq k$) takové, že*
$$[u_1, u_2, ..., u_k] = [u_1, u_2, ..., u_{i-1}, u_{i+1}, ..., u_k].$$

vektor, který je lineární kombinací zbývajících vektorů, můžeme z generátorů vynechat

Důkaz. „1. $\Rightarrow$ 2." Jestliže $u_1, u_2, ..., u_k$ jsou lineárně závislé vektory, existují čísla $t_1, t_2, ..., t_k \in T$, ze kterých je alespoň jedno nenulové tak, že

$$t_1.u_1 + t_2.u_2 + ... + t_k.u_k = o.$$

Předpokládáme např. $t_i \neq 0$, pak dostaneme

$$u_i = -\frac{t_1}{t_i}.u_1 - \frac{t_2}{t_i}.u_2 - ... - \frac{t_{i-1}}{t_i}.u_{i-1} - \frac{t_{i+1}}{t_i}.u_{i+1} - ... - \frac{t_k}{t_i}.u_k.$$

To znamená, že vektor u_i je lineární kombinací zbývajících vektorů.
„2. $\Rightarrow$ 3." Plyne z druhé části věty 11.4.
„3. $\Rightarrow$ 1." Nechť platí 3., pak

$$u_i \in [u_1, u_2, ..., u_k] = [u_1, u_2, ..., u_{i-1}, u_{i+1}, ..., u_k] = L(u_1, u_2, ..., u_{i-1}, u_{i+1}, ..., u_k).$$

To znamená

$$u_i = p_1.u_1 + p_2.u_2 + ... + p_{i-1}.u_{i-1} + p_{i+1}.u_{i+1} + ... + p_k.u_k,$$

kde $p_j \in T$. Po úpravě dostaneme

$$p_1.u_1 + p_2.u_2 + ... + p_{i-1}.u_{i-1} + (-1).u_i + p_{i+1}.u_{i+1} + ... + p_k.u_k = o.$$

Vektory $u_1, u_2, ..., u_k$ jsou tedy lineárně závislé. □

Průvodce studiem

Tvrzení 2. z předcházející věty zajišťuje pouze existenci vektoru, který lze vyjádřit jako lineární kombinaci zbývajících vektorů. Nelze obecně tvrdit, že každý z lineárně závislých vektorů $u_1, u_2, ..., u_k$ lze vyjádřit jako lineární kombinaci ostatních vektorů.

Příklad 11.9. Ve vektorovém prostoru $\mathbb{R}^2$ jsou vektory $u_1 = (1, 0), u_2 = (3, 4), u_3 = (3, 0)$ lineárně závislé, protože platí $3.u_1 + 0.u_2 - u_3 = o$. Vektor u_2 však nemůžeme vyjádřit jako lineární kombinaci vektorů u_1 a u_3.

Příklad 11.10. 1. Víme, že vektory (0, 1), (1, 1), (2, 0) jsou lineárně závislé, neboť

$$(2, 0) = -2.(0, 1) + 2.(1, 1).$$

Vektor (2, 0) můžeme vyjádřit jako lineární kombinaci zbývajících vektorů

Podobně můžeme vyjádřit

$$(1, 1) = (0, 1) + \frac{1}{2}.(2, 0), \qquad (0, 1) = (1, 1) - \frac{1}{2}.(2, 0).$$

$$[(0, 1), (1, 1), (2, 0)] = [(0, 1), (1, 1)] = [(0, 1), (2, 0)] = [(1, 1), (2, 0)].$$

2. Víme, že vektory $v_1 = (-1, 1), v_2 = (1, 2), v_3 = (2, 1), v_4 = (1, -4)$ jsou lineárně závislé. Můžeme např. vyjádřit

$$v_3 = -v_1 + v_2, \qquad v_4 = -2.v_1 - v_2.$$

$$[v_1, v_2, v_3, v_4] = [v_1, v_2] = [v_3, v_4].$$

Věta 11.11. *Nechť V je vektorový prostor nad číselným tělesem T a nechť $u_1, u_2, ..., u_k$ je konečná posloupnost vektorů z V. Pak platí:*

1. *Obsahuje-li posloupnost $u_1, u_2, ..., u_k$ nulový vektor, pak je lineárně závislá.*
2. *Obsahuje-li posloupnost $u_1, u_2, ..., u_k$ dva stejné vektory, pak je lineárně závislá.*
3. *Je-li nějaká posloupnost vybraná z posloupnosti $u_1, u_2, ..., u_k$ lineárně závislá, pak je také posloupnost $u_1, u_2, ..., u_k$ lineárně závislá.*
4. *Je-li posloupnost $u_1, u_2, ..., u_k$ lineárně nezávislá, pak každá posloupnost z ní vybraná je rovněž lineárně nezávislá.*

Důkaz. Všechna tvrzení plynou z definice lineární závislosti a předchozí věty. □

Věta 11.12 (Steinitzova věta o výměně). *Nechť V je vektorový prostor nad číselným tělesem T, $u_1, ..., u_r, v_1, ..., v_s \in V$. Nechť vektory $u_1, u_2, ..., u_r$ jsou lineárně nezávislé a nechť $u_i \in L(v_1, ..., v_s)$ pro $i = 1, 2, ..., r$. Potom platí:*

1. $r \leq s$.
2. *Při vhodném přečíslování vektorů $v_1, v_2, ..., v_s$ je*

$$L(v_1, v_2, ..., v_s) = L(u_1, u_2, ..., u_r, v_{r+1}, v_{r+2}, ..., v_s).$$

Důkaz. Najdete v literatuře, např.[HoRa03] □

Shrnutí

Vektor u je lineární kombinací vektorů $u_1, u_2, ..., u_n$, pokud jej můžeme vyjádřit jako součet číselných násobků těchto vektorů.
Množina všech lineárních kombinací vektorů $u_1, u_2, ..., u_n$ je podprostor shodný s podprostorem generovaným těmito vektory.
Vektory jsou lineárně závislé, pokud je nulový vektor jejich lineární kombinací s nenulovými násobky.

Pojmy k zapamatování

- lineární kombinace vektorů
- množina všech lineárních kombinací vektorů
- lineárně závislé vektory
- lineárně nezávislé vektory

Kontrolní otázky

1. *Co se stane, když ke generátorům $u_1, u_2, ..., u_n$ podprostoru W přidáme vektor, který je jejich lineární kombinací ?*
2. *Můžeme vyjádřit některý z vektorů $u_1, u_2, ..., u_n$ jako lineární kombinaci zbývajících vektorů, pokud jsou tyto vektory lineárně nezávislé ?*
3. *Co se stane, když v množině všech lineárních kombinací daných vektorů nahradíme některé z těchto vektorů jejich lineárními kombinacemi ?*

4. *Je možné, aby vektor $u \in \mathbb{R}^3$ generoval jiný podprostor v $\mathbb{R}^3$ než vektor $\sqrt{2}.u$?*

Cvičení

1. Zjistěte, zda vektor x je lineární kombinací vektorů $u, v, w \in \mathbb{R}^4$
   (a) $x = (1, 4, -4, 1), u = (1, 2, -1, 1), v = (2, 0, 1, 1), w = (1, 0, 2, 1)$
   (b) $x = (1, 4, -5, 2), u = (1, 3, 0, 1), v = (2, -1, 1, 0), w = (3, 1, -1, 1)$
2. Jsou dány vektory $v = (3, 1, -3), u = (1, 1, 1), w = (0, 1, 3)$ z vektorového prostoru $\mathbb{R}^3$. Rozhodněte, zda $v \in L(u, w)$.
3. Rozhodněte, zda vektory $u_1 = (1, 2, 1, 2), u_2 = (-2, 1, -2, 1), u_3 = (-1, 1, -1, 1), u_4 = (2, 0, -1, -3), u_5 = (-1, 1, 0, 2)$ generují vektorový prostor $\mathbb{R}^4$.
4. Rozhodněte, zda vektory

   $$v_1 = (2, -1, 0, -1), v_2 = (2, 1, -1, 1)$$

   a vektory

   $$w_1 = (-2, -5, 3, -5), w_2 = (2, -5, 2, -5)$$

   generují tentýž podprostor ve vektorovém prostoru $\mathbb{R}^4$.
5. Rozhodněte, zda vektory

   $$u_1 = (1, 3, -2), u_2 = (-1, 1, 2), u_3 = (1, 2, -8)$$

   vektorového prostoru $\mathbb{Q}^3$jsou lineárně závislé či lineárně nezávislé.
6. Nalezněte všechna $r \in \mathbb{R}$, pro která vektor $w = (r, -1, 2)$ leží v podprostoru $W = [u_1, u_2, u_3]$ vektorového prostoru $\mathbb{R}^3$, je-li

   $$u_1 = (1, 1, -2), u_2 = (-1, 2, 1), u_3 = (2, -1, -3).$$

7. Ve vektorovém prostoru $\mathbb{R}^3$ jsou dány vektory

   $$u = (1, 1, 1), v = (1, a, 1), w = (2, 2, a).$$

   Určete všechny hodnoty parametru $a \in \mathbb{R}$, pro které jsou tyto vektory lineárně závislé a pro které jsou lineárně nezávislé.

Úkoly k textu

1. Uveďte příklad vektorů z $\mathbb{R}^3$, které jsou lineárně nezávislé a generují prostor $\mathbb{R}^3$.
2. Uveďte příklad vektorů z $\mathbb{R}^3$, které jsou lineárně závislé a generují $\mathbb{R}^3$.
3. Uveďte příklad vektorů z $\mathbb{R}^3$, které jsou lineárně nezávislé a negenerují prostor $\mathbb{R}^3$.
4. Uveďte příklad vektorů z $\mathbb{R}^3$, které jsou lineárně závislé a negenerují prostor $\mathbb{R}^3$.

Řešení

1. a) ano, $x = 2u - w$ b) ne
2. ano, $v = 3u - 2w$
3. ne (např. vektor (1,1,1,2) se nedá vyjádřit jako lineární kombinace vektorů u_1, u_2, u_3, u_4, u_5)
4. ano ($w_1 = 2.v_1 - 3.v_2, w_2 = 3.v_1 - 2.v_2$)
5. lineárně nezávislé
6. r = -1
7. $a = 1 \vee a = 2$ lineárně závislé
   $a \neq 1 \wedge a \neq 2$ lineárně nezávislé

12 Báze a dimenze vektorových prostorů

Studijní cíle: V této kapitole se studující seznámí s pojmy báze a dimenze vektorového prostoru a souřadnice vektoru.

Klíčová slova: báze vektorového prostoru, dimenze vektorového prostoru, souřadnice vektoru

12.1 Báze vektorového prostoru

Definice 12.1. Nechť V je vektorový prostor nad číselným tělesem T. Konečná posloupnost vektorů $u_1, u_2, ..., u_n$ z V se nazývá *báze vektorového prostoru* V, jestliže platí :

1. vektory $u_1, u_2, ..., u_n$ jsou lineárně nezávislé,
2. vektory $u_1, u_2, ..., u_n$ generují vektorový prostor V.

$$[u_1, u_2, ..., u_n] = V.$$

Průvodce studiem

Bází vektorového prostoru jsou tedy vektory, které generují tento prostor a jsou lineárně nezávislé. Tato definice nezaručuje existenci báze a neříká nic o počtu bází ve V. To si nejdříve ukážeme na příkladech.

Příklad 12.2.

1. Vektory

$$e_1 = (1, 0, ..., 0), e_2 = (0, 1, ..., 0), ..., e_n = (0, 0, ..., 1)$$

jsou bází vektorového prostoru T^n.
Specielně vektory (1, 0), (0, 1) jsou bází vektorového prostoru $\mathbb{R}^2$.

jsou lineárně nezávislé a generují T^n

2. Vektory (1, 2), (3, 2) jsou bází vektorového prostoru $\mathbb{R}^2$.
Vektorový prostor $\mathbb{R}^2$ má nekonečně mnoho bází.

jsou lineárně nezávislé a generují $\mathbb{R}^2$

3. Vektory (0, 1), (1, 1), (2, 0) nejsou bází vektorového prostoru $\mathbb{R}^2$.

generují $\mathbb{R}^2$, ale jsou lineárně závislé

4. Vektory (-1, 1), (1, 2), (2, 1), (1, -4) rovněž nejsou bází vektorového prostoru $\mathbb{R}^2$.
5. Nulový vektorový prostor $V = \{o\}$ nemá bázi.

Věta 12.3. *Konečná posloupnost vektorů $u_1, u_2, ..., u_n$ je bází vektorového prostoru V právě tehdy, když každý vektor $w \in V$ je možno jediným způsobem vyjádřit ve tvaru*

$$w = t_1.u_1 + t_2.u_2 + ... + t_n.u_n, \qquad t_1, t_2, ..., t_n \in T.$$

Důkaz. Věta má tvar ekvivalence, musíme tedy dokázat obě implikace:
„⇒“ Předpokládáme, že $u_1, u_2, ..., u_n$ je báze vektorového prostoru V, potom existence vyjádření

$$w = t_1.u_1 + t_2.u_2 + ... + t_n.u_n, \qquad t_1, t_2, ..., t_n \in T,$$

plyne z definice báze. Dokážeme jeho jednoznačnost. Dokazujeme sporem. Předpokládáme, že existují dvě taková vyjádření

$$w = t_1.u_1 + t_2.u_2 + ... + t_n.u_n, \qquad w = r_1.u_1 + r_2.u_2 + ... + r_n.u_n, \qquad t_i, r_i \in T.$$

Potom po odečtení dostaneme

$$(t_1 - r_1).u_1 + (t_2 - r_2).u_2 + ... + (t_n - r_n).u_n = o.$$

Vektory $u_1, u_2, ..., u_n$ jsou lineárně nezávislé, pro všechna $i = 1, 2, ...n$ tedy platí $t_i - r_i = 0$. Odtud dostaneme $t_i = r_i$.
„ $\Leftarrow$“ Nechť každý vektor se dá jednoznačně vyjádřit ve tvaru

$$w = t_1.u_1 + t_2.u_2 + ... + t_n.u_n, \qquad t_1, t_2, ..., t_n \in T.$$

Musíme dokázat, že vektory $u_1, u_2, ..., u_n$ jsou bází V. Zřejmě je

$$V = L(u_1, u_2, ...u_n) = [u_1, u_2, ..., u_n].$$

Zbývá dokázat, že vektory $u_1, u_2, ..., u_n$ jsou lineárně nezávislé. Nechť tedy

$$t_1.u_1 + t_2.u_2 + ... + t_n.u_n = o.$$

Platí však také

$$0.u_1 + 0.u_2 + ... + 0.u_n = o.$$

Z jednoznačnosti vyjádření plyne, že $t_1 = t_2 = ... = t_n = 0$. To znamená, že vektory $u_1, u_2, ..., u_n$ jsou lineárně nezávislé. Dohromady dostáváme, že jsou bází V. □

Věta 12.4. *Nechť $u_1, u_2, ..., u_n$ je báze vektorového prostoru V. Pak platí:*

1. *Jestiže $v_1, v_2, ..., v_m$ je báze prostoru V, pak je $m = n$.*
2. *Jestiže vektory $w_1, w_2, ..., w_s$ generují prostor V, pak z nich lze vybrat bázi.*
3. *Každou konečnou posloupnost lineárně nezávislých vektorů z V lze doplnit na bázi.*

Důkaz. 1. Když dvakrát aplikujeme Steinitzovu větu, dostaneme $n \leq m$ a $m \leq n$ a odtud plyne $m = n$.

2. Podle předpokladu má V bázi a tedy $V \neq \{o\}$.
Nechť vektory $w_1, w_2, ..., w_s$ generují prostor V. Alespoň jeden z nich je různý od nulového vektoru a můžeme je přečíslovat tak, že $w_1, w_2, ..., w_i$ jsou lineárně nezávislé a $w_1, w_2, ..., w_i, w_j$ jsou lineárně závislé pro každé j s vlastností $i < j \leq n$. Odtud dostaneme $w_j \in L(w_1, w_2, ..., w_i)$, a tedy

$$V = L(w_1, w_2, ..., w_s) \subseteq L(w_1, w_2, ..., w_i)$$

Opačná inkluze je triviální a $V = L(w_1, w_2, ..., w_i)$ a vektory $w_1, w_2, ..., w_i$ jsou bází prostoru V

3. Nechť $w_1, w_2, ..., w_r$ jsou lineárně nezávislé vektory z V. Podle Steinitzovy věty je po vhodném přečíslování

$$V = L(u_1, u_2, ..., u_n) = L(w_1, w_2, ..., w_r, u_{r+1}, u_{r+2}, ..., u_n)$$

a odtud podle 1. a 2. části této věty dostaneme, že vektory

$$w_1, w_2, ..., w_r, u_{r+1}, u_{r+2}, ..., u_n$$

jsou bází V.

□

Průvodce studiem

První část věty nám říká, že pokud má vektorový prostor bázi, pak všechny báze se skládají ze stejného počtu vektorů. Toho použijeme v definici dimenze. Z druhé části věty je zřejmé, že z hlediska generátorů je báze „nejchudší“. Pokud některý z vektorů báze vypustíme, již vektory vektorový prostor negenerují.

Příklad 12.5. 1. (1, 0), (0, 1) a (1, 2), (3, 2) jsou dvě báze vektorového prostoru $\mathbb{R}^2$. *obě mají stejný počet vektorů 2*

2. Vektory (0, 1), (1, 1), (2, 0) generují vektorový prostor $\mathbb{R}^2$ a jsou lineárně závislé; můžeme z nich vybrat bázi např. (0, 1), (1, 1). *z generátorů můžeme vybrat bázi*

3. Vektory (-1, 1), (1, 2), (2, 1), (1, -4) generují vektorový prostor $\mathbb{R}^2$ a jsou lineárně závislé; můžeme z nich vybrat bázi např. (-1, 1), (1, 2).

4. Uvažujeme vektorový prostor $\mathbb{R}^3$. Vektory (1, 0, 0), (0, 1, 0) jsou lineárně nezávislé, ale netvoří bázi $\mathbb{R}^3$.
   Stačí přidat jeden vektor, který není jejich lineární kombinací např. (1, 1, 1) a vektory (1, 0, 0), (0, 1, 0), (1, 1, 1) tvoří bázi prostoru $\mathbb{R}^3$. *lineárně nezávislé vektory můžeme doplnit na bázi*

12.2 Dimenze vektorového prostoru

Definice 12.6. Nechť V je vektorový prostor nad číselným tělesem T. Pak

1. Je-li V nulovým vektorovým prostorem ($V = \{o\}$), říkáme , že *dimenze* V je nula a píšeme dim V = 0.

2. Existuje-li báze $u_1, u_2, ..., u_n$ prostoru V, pak říkáme, že *dimenze* V je n a píšeme dim $V = n$.

3. Je-li $V \neq \{o\}$ a nemá žádnou bázi, říkáme, že *dimenze* V je nekonečno a píšeme dim $V = \infty$.

Vektorové prostory z 1. a 2. se nazývají *konečnědimenzionální*, vektorové prostory z 3. se nazývají *nekonečnědimenzionální* .

Příklad 12.7. 1. dim T^n = n , specielně dim $\mathbb{R}^2$ = 2 a dim $\mathbb{R}^3$ = 3.

2. příkladem nekonečnědimenzionálního prostoru je prostor všech polynomů s reálnými koeficienty $\mathbb{R}[x]$.

V dalším se budeme zabývat konečnědimenzionálními vektorovými prostory.

Průvodce studiem

V praxi se často setkáváme s úlohou, že ve vektorovém prostoru, jehož dimenzi n známe, ověřujeme, zda posloupnost n vektorů tvoří jeho bázi. V tomto případě stačí ověřit pouze jednu ze dvou podmínek definice báze, jak ukazuje následující věta.

Věta 12.8. *Nechť V je vektorový prostor nad číselným tělesem T, dim $V = n$ ($n \geq 1$) a nechť $u_1, u_2, ..., u_n$ je konečná posloupnost n vektorů z V. Pak následující výroky jsou ekvivalentní*

1. *Vektory $u_1, u_2, ..., u_n$ jsou bází prostoru V.*
2. *Vektory $u_1, u_2, ..., u_n$ jsou lineárně nezávislé.*
3. *Vektory $u_1, u_2, ..., u_n$ generují prostor V.*

Důkaz. „1. $\Rightarrow$ 2." Plyne z definice báze.
„2. $\Rightarrow$ 3." Nechť vektory $u_1, u_2, ..., u_n$ jsou lineárně nezávislé. Protože dim $V = n$, tak podle bodu 3 věty 12.4 jsou vektory $u_1, u_2, ..., u_n$ bází V. Odtud plyne $u_1, u_2, ..., u_n$ generují V.
„3. $\Rightarrow$ 1." Nechť $u_1, u_2, ..., u_n$ generují V, ale dim $V = n$ a podle bodu 2 věty 12.4 vektory $u_1, u_2, ..., u_n$ jsou bází V. □

Věta 12.9. *Nechť W_1, W_2 jsou podprostory vektorového prostoru V. Potom platí:*

1. *Když $W_1 \subseteq W_2$, platí dim$W_1 \leq$ dimW_2.*
2. *Když $W_1 \subseteq W_2$ a současně dimW_1 = dimW_2, tak platí $W_1 = W_2$.*

Důkaz. Pokud $W_1 = \{o\}$ nebo $W_2 = \{o\}$, obě tvrzení zřejmě platí. Nechť $W_1 \neq \{o\}$ a současně $W_2 \neq \{o\}$ a nechť $u_1, u_2, ..., u_r$ je báze W_1 a $v_1, v_2, ..., v_s$ je báze W_2. Jestliže $W_1 \subseteq W_2$ potom $u_i \in W_2 = L(v_1, v_2, ..., v_s), i = 1, 2, ...r$, přičemž vektory $u_1, u_2, ..., u_r$ jsou lineárně nezávislé. Jsou tedy splněny předpoklady Steinitzovy věty. Potom

1. podle Steinitzovy věty je $r \leq s$, čili dim $W_1 \leq$ dim W_2.
2. Je-li dim W_1 = dim W_2 to znamená $r = s$, pak opět podle Steinitzovy věty je $L(v_1, v_2, ..., v_s) = L(u_1, u_2, ..., u_r)$, čili $W_1 = W_2$.

□

Poznámka 12.10. Z předchozí věty plyne několik důležitých výsledků :

1. Dimenze podprostoru je vždy menší nebo rovna dimenzi celého prostoru.
2. Je-li podprostor W_1 vlastní podmnožinou podprostoru $W_2 (W_1 \subset W_2)$, potom je dim $W_1 <$ dim W_2. Nemůže se tedy stát, aby dva podprostory stejné dimenze byly ostře v inkluzi.

12.3 Souřadnice vektoru

Průvodce studiem

Danou bázi $u_1, u_2, ..., u_n$ vektorového prostoru V chápeme jako uspořádanou n–tici vektorů z V. Rovnost dvou bází znamená rovnost dvou uspořádaných n–tic vektorů z V. Závisí tedy na pořadí vektorů. To se ukáže v dalším, při zavádění pojmu souřadnice vektoru.

Definice 12.11. Nechť $u_1, u_2, ..., u_n$ je báze vektorového prostoru V a nechť vektor $w \in V$ je vyjádřen ve tvaru

$$w = t_1.u_1 + t_2.u_2 + ... + t_n.u_n, \qquad t_1, t_2, ..., t_n \in T.$$

Pak číslo t_i nazýváme *i–tou souřadnicí vektoru* w v bázi $u_1, u_2, ..., u_n$ a uspořádanou n–tici $(t_1, t_2, ..., t_n)$ nazýváme *souřadnicemi vektoru* w v bázi $u_1, u_2, ..., u_n$.

Průvodce studiem

1. Pojem souřadnice vektoru je vždy vázán na nějakou pevnou bázi prostoru V. Zřejmě jeden vektor má v různých bázích obecně různé souřadnice.
2. Podle věty 12.3 má každý vektor $w \in V$ při dané bázi $u_1, u_2, ..., u_n$ souřadnice v této bázi, které jsou určeny jednoznačně a naopak ke každé uspořádané n–tici $(t_1, t_2, ..., t_n)$, $t_1, t_2, ..., t_n \in T$ existuje jediný vektor, jehož souřadnice v dané bázi jsou právě $(t_1, t_2, ..., t_n)$.
3. Souřadnice vektoru můžeme psát do řádků i do sloupců.

Příklad 12.12. Ve vektorovém prostoru $\mathbb{R}^3$ má v bázi $e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 1, 0)$ vektor w souřadnice (1, -2, 3).

1. V bázi e_2, e_3, e_1 vektor w má souřadnice (-2, 3, 1).
2. Máme určit souřadnice vektoru w v bázi $u_1 = (1, 1, 0), u_2 = (0, 1, 1), u_3 = (1, 0, 1)$
   *Řešení:*Rozepsáním rovnosti

   w=$t_1.u_1 + t_2.u_2 + t_3.u_3$

   $$(1, -2, 3) = t_1.(1, 1, 0) + t_2.(0, 1, 1) + t_3.(1, 0, 1)$$

   do souřadnic dostaneme soustavu

   $t_1 = -2, t_2 = 0, t_3 = 3$ *je řešením soustavy*

   $$\begin{aligned} t_1 + t_3 &= 1 \\ t_1 + t_2 &= -2 \\ t_2 + t_3 &= 3. \end{aligned}$$

   Vektor w má tedy v bázi u_1, u_2, u_3 souřadnice (-2, 0, 3).
3. V bázi u_3, u_1, u_2 má vektor w souřadnice (3, -2, 0).

Věta 12.13. *Necht'*$u_1, u_2, ..., u_n$ *je báze vektorového prostoru V. Necht'*$t \in T$ *a necht'vektor* $x \in V$ *má v bázi* $u_1, u_2, ..., u_n$ *souřadnice* $(x_1, x_2, ..., x_n)$ *a vektor* $y \in V$ *má v bázi* $u_1, u_2, ..., u_n$ *souřadnice* $(y_1, y_2, ..., y_n)$. *Potom*

1. *vektor* $x + y$ *má v bázi* $u_1, u_2, ..., u_n$ *souřadnice*

   souřadnice součtu vektorů jsou součet souřadnic těchto vektorů

   $$(x_1 + y_1, x_2 + y_2, ..., x_n + y_n),$$

2. *vektor* $t.x$ *má v bázi* $u_1, u_2, ..., u_n$ *souřadnice*

   souřadnice součinu čísla a vektoru jsou součin čísla a souřadnic tohoto vektoru

   $$(t.x_1, t.x_2, ..., t.x_n).$$

Důkaz. 1. Podle předpokladu je

$$x = x_1.u_1 + x_2.u_2 + ... + x_n.u_n, \qquad y = y_1.u_1 + y_2.u_2 + ... + y_n.u_n.$$

Potom po úpravě dostaneme

$$x + y = (x_1 + y_1).u_1 + (x_2 + y_2).u_2 + ... + (x_n + y_n).u_n$$

a odtud již plyne tvrzení věty.

2. Dokážeme podobně.

□

Shrnutí

Bázi vektorového prostoru tvoří vektory, které generují tento prostor a jsou lineárně nezávislé.
Pokud má vektorový prostor bázi, pak všechny jeho báze mají stejný počet vektorů.
Z generátorů vektorového prostoru můžeme vždy vybrat bázi.
Dimenze vektorového prostoru je počet vektorů jeho báze.
Každý vektor můžeme vyjádřit jako lineární kombinaci vektorů báze.
Koeficienty této lineární kombinace jsou souřadnice daného vektoru v dané bázi.

Pojmy k zapamatování

- báze vektorového prostoru
- dimenze vektorového prostoru
- souřadnice vektoru v dané bázi

Kontrolní otázky

1. *Jsou lineárně závislé vektory, které generují vektorový prostor, jeho bází?*
2. *Kolik vektorů má báze vektorového prostoru V, pro který platí dim $V = k$?*
3. *Co je i-tou souřadnicí vektoru w v bázi $u_1, u_2, ..., u_n$?*
4. *Jsou dány libovolné vektory $u, v, w \in \mathbb{Q}^2$. Jsou tyto vektory lineárně nezávislé?*
5. *Můžeme najít dvoudimenzionální podprostor W ve vektorovém prostoru $\mathbb{R}^4$ tak, že W obsahuje vektory (1,1,1,1), (0,1,0,0), (0,0,1,0)?*

Cvičení

1. Rozhodněte, zda vektory

$$u_1 = (1, 1, 2), u_2 = (-3, 4, 1), u_3 = (5, 4, 3)$$

   tvoří bázi vektorového prostoru $\mathbb{R}^3$.
2. Ve vektorovém prostoru $\mathbb{Q}^4$ nechť je zadán podprostor $W = [w_1, w_2, w_3, w_4]$

$$w_1 = (1, 2, 0, 1), w_2 = (0, 1, 2, 3), w_3 = (3, 5, -2, 0), w_4 = (3, 6, 0, 3).$$

   Z generátorů w_1, w_2, w_3, w_4 podprostoru W vyberte bázi podprostoru W.
3. Určete všechny hodnoty parametru a, pro které zadané vektory

$$v_1 = (1, 3, a), v_2 = (3, 2, 2.a), v_3 = (5, 8, a)$$

   tvoří bázi vektorového prostoru $\mathbb{R}^3$.
4. Ve vektorovém prostoru $\mathbb{R}^4$ jsou dány lineárně nezávislé vektory

$$u_1 = (1, 1, 0, 0), u_2 = (0, 1, 1, 0), u_3 = (0, 0, 1, 1), u_4 = (0, 0, 0, 1)$$

   Vyjádřete souřadnice vektoru w = (3,2,1,0)
   (a) v bázi u_1, u_2, u_3, u_4,
   (b) v bázi u_3, u_1, u_4, u_2.
5. V závislosti na parametru a určete dimenzi podprostoru $W = L(u_1, u_2, u_3)$ vektorového prostoru $\mathbb{R}^3$, je-li

$$u_1 = (1, 1, 1), u_2 = (1, a, 1), u_3 = (2, 2, a).$$

Úkoly k textu

1. Uveďte příklad vektorů z vektorového prostoru $\mathbb{R}^3$, které jsou generátory, ale nejsou bází vektorového prostoru $\mathbb{R}^3$.
2. Uveďte příklad vektorů z vektorového prostoru $\mathbb{R}^3$, které jsou lineárně nezávislé, ale nejsou bází vektorového prostoru $\mathbb{R}^3$.
3. Uveďte příklad dvoudimenzionálního podprostoru W ve vektorovém prostoru $\mathbb{R}^4$ tak, že podprostor W obsahuje vektor (1,0,0,1).

Řešení

1. ano
2. w_1, w_2
3. všechna $a \in \mathbb{R} - \{0\}$
4. a) (3,-1,2,-2) b) (2,3,-2,-1)
5. $a = 1 \vee a = 2$ dim $W = 2$
   $a \neq 1 \wedge a \neq 2$ dim $W = 3$

Reference

[Bec05] Bečvář J.: *Lineární algebra*. matfyzpress, Praha, 2005

[Bic00] Bican L.: *Lineární algebra a geometrie*. Academia, Praha, 2000

[EmKu07] Emanovský P., Kühr J.: *Cvičení z algebry pro 1.ročník I*. Universita Palackého, Olomouc, 2007

[GaTa88] Garding L.,Tambour T.: *Algebra for computer science*. Springer, New York, 1988

[Hor91] Horák P.: *Algebra a teoretická aritmetika*. Masarykova univerzita, Brno, 1991

[Hor06] Horák P.: *Cvičení z algebry a teoretické aritmetiky*. Masarykova univerzita, Brno, 2006

[HoRa03] Hort D., Rachůnek J.: *Algebra I*. Universita Palackého, Olomouc, 2003

[Chaj03] Chajda I.: *Okruhy a moduly*. Universita Palackého, Olomouc, 2003

[Chaj05] Chajda I.: *Úvod do algebry (grupoidy a grupy)*. Universita Palackého, Olomouc, 2005

[MoZa02] Motl L.,Zahradník M.: *Pěstujeme lineární algebru*. Universita Karlova, Praha, 2002

[Rach05] Rachůnek J.: *Grupy a okruhy*. Universita Palackého, Olomouc, 2005

[SzMo02] Szidarovszky F., Molnár S.: *Introduction to Matrix Theory with Applications to Business and Economics*. World Scientific, New Jersey, 2002