ALGEBRA

Binárne operácie a polia

doc. RNDr. Štefan Peško, CSc.

Katedra matematických metód a operačnej analýzy, FRI ŽU

16. septembra 2015

Zobrazenia

Zobrazením z množiny X do množiny Y rozumieme ľubovoľný predpis, ktorý každému prvku x množiny X priradí jednoznačne určený prvok y množiny Y. Zápis $f : X \to Y$ označuje, že f je zobrazenie z X do Y. Ten jednoznačne určený prvok $y \in Y$, ktorý zobrazenie priradí prvku $x \in X$ budeme značiť $f(x)$.

Dve zobrazenia $f, g : X \to Y$ sa rovnajú, ak pre každé $x \in X$ platí $f(x) = g(x)$.

Príklad 1.1

Majme množiny $A = \{a, b, c, d, e\}, M = \{1, 2, 3, 4, 5\}$ a zobrazenia $f, g : A \to M$, kde

$$f(a) = 1, f(b) = 2, f(c) = 3, f(d) = 2, f(e) = 3,$$

$$g(a) = 1, g(b) = 2, g(c) = 5, g(d) = 4, g(e) = 3.$$

Zobrazenia f a g sa nerovnajú, lebo existuje prvok $c \in A$ pre ktorý $f(c) \neq g(c)$.

Zobrazenia

Zobrazenie $f : X \to Y$ sa nazýva

- prosté, ak rôznym prvkom $x_1.x_2 \in X$ priraďuje rôzne prvky $f(x_1), f(x_2) \in Y$ t.j. ak platí

$$(\forall x_1, x_2 \in X)(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)).$$

- na, ak na každý prvok množiny Y sa zobrazí nejaký prvok množiny X t.j. ak

$$(\forall y \in Y)(\exists x \in X)(y = f(x)).$$

- bijekcia, ak f je zároveň prosté a na.
- identické ak $Y = X$ a $(\forall x)(f(x) = x)$.

Príklad 1.1 – pokračovanie

Zobrazenia f nie je prosté ani nie je na. Zobrazenie g je bijekcia.

Binárne operácie

Nech je X neprázdna množina. Potom zobrazenie $\circ : X \times X \to X$ nazývame binárnou operáciou na množine X.
Výsledok priradený binárnou operáciou $\circ$ usporiadanej dvojici $(a, b) \in X \times X$ budeme označovať $a \circ b \in X$.

Príklad 1.2

Na množine celých kladných čísel $\{1,2,3,\dots\}$ môžeme definovať binárne operácie $\circ, \bullet, \oplus$ vzťahmi

$$a \circ b = a + b - 1, a \bullet b = a^b, a \oplus b = max\{a, b\}.$$

Keď má množina X malý počet prvkov, potom binárnu operáciu $\circ$ na nej môžeme definovat pomocou Cayleyho tabuľky – do záhlavia (zvisle i vodorovne) dáme prvky X a na ich priesečníky výsledky operácie.

Nech sú X, Y, Z neprázdne množiny. Potom zobrazenie $\clubsuit : X \times Y \to Z$ nazývame binárnou operáciou na množinách X, Y s hodnotami v množine Z. Pre $(a, b) \in X \times Y$ je $a \clubsuit b \in Z$.

Príklad 1.3

Operáciu $\square$ na množine $X = \{a, b, c\}$ definujeme pomocou Cayleyho tabuľky takto

$\square$	a	b	c
a	c	b	a
b	b	c	a
c	a	a	c

Binárna operácia $\circ$ na množine X sa nazýva

- asociatívna, ak pre všetky $x, y, z \in X$ platí

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

- komutatívna, ak pre všetky $x, y \in X$ platí

$$x \circ y = y \circ x.$$

Príklad 1.3 – pokračovanie

Zo symetrie Cayleyho tabuľky okolo hlavnej diagonály ľahko usúdime, že operácia $\square$ je komutatívna. No nie je asociatívna, lebo

$$b = a\square(a\square b) \neq (a\square a)\square b = a.$$

Prvok $e \in X$ sa nazýva neutrálny prvok binárnej operácie $\circ$ na množine X ak pre všetky $x \in X$ platí

$$x \circ e = e \circ x = x.$$

Ak má binárna operácia $\circ$ na množine X neutrálny prvok e a k danému prvku $x \in X$ existuje prvok $y \in Y$ tak, že

$$x \circ y = y \circ x = e,$$

hovoríme, že y je inverzný prvok k prvku x.

Príklad 1.4

Nech je daná množina $M = \{e, a, b, c\}$ a na nej binárna operácia $*$ daná tabuľkou:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	e	e
b	b	e	c	a
c	c	e	a	a

Vidíme, že e je neutrány prvok a a je inverzný prvok k prvkom b, c.

Základné číselné obory

Základné číselné obory budeme označovať takto:

- $\mathbb{N}$ – množina všetkých prirodzených čísel, $(0 \in \mathbb{N})$,
- $\mathbb{Z}$ – množina všetkých celých čísel,
- $\mathbb{Q}$ – množina všetkých racionálnych čísel,
- $\mathbb{R}$ – množina všetkých reálnych čísel,
- $\mathbb{C}$ – množina všetkých komplexných čísel, ($i \in \mathbb{C} - \mathbb{R}$ je imaginárna jednotka).

Na každej z uvedených množín môžeme definovať dve binárne operácie, sčítania $+$ a násobenia $\cdot$, ktoré sú na týchto množinách asociatívne a komutatívne. Naviac je násobenie (z oboch strán) distributívne vzhľadom na sčítanie t.j. pre všetky prvky x, y, z z príslušnej množiny platí

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Cvičenie 1.1

1. Vypočítajte:
   a) $(-2+5i)\cdot(3+2i)/(3-4i)$,
   b) $((-2-5i)^2\cdot(-3+2i))^{-1}$.
2. Pre komplexné číslo $x=a+bi$, kde $a,b\in\mathbb{R}$ nazývame $a=Re(x)$ a $b=Im(x)$ jeho reálnou a imaginárnou časťou. Odvoďte vzorce:
   a) $Re(x+y)=Re(x)+Re(y)$,
   b) $Im(x+y)=Im(x)+Im(y)$,
   c) $Re(xy)=Re(x)Re(y)-Im(x)Im(y)$,
   d) $Im(xy)=Re(x)Im(y)+Im(x)Re(y)$.
3. Absolútna hodnota komplexné číslo $x=a+bi$ je definovaná ako $|x|=\sqrt{a^2+b^2}$. Zobrazte komplexné čísla zo zadania 1. v Gaussovej rovine a vypočítajte ich absolútne hodnoty.
4. Komplexne združené číslo k číslu $x=a+bi$ je číslo $\overline{x}=a-bi$. Overte nasledujúce vzťahy:
   a) $Re(x)=Re(\overline{x})=\frac{1}{2}(x+\overline{x}), Im(x)=-Im(\overline{x})=\frac{1}{2i}(x-\overline{x})$,
   b) $\overline{\overline{x}}=x, \overline{x+y}=\overline{x}+\overline{y}, |x|=|\overline{x}|, |x|^2=x\overline{x}$,
   c) $\overline{xy}=\overline{x}\,\overline{y}, |xy|=|x||y|, |x+y|\leq|x|+|y|$.

Cvičenie 1.1 (pokračovanie)

5. Upravte operáciu $*$ z príkladu 1.4 s čo najmenej zmenami tak, aby operácia nemala neutrálny prvok.
6. Definujte pre operáciu násobenia $*$ na podmnožine $M = \{1, -1, i, -i\}$ komplexných čísel Cayleyho tabuľku. Nájdite v nej neutrálny prvok a všetky inverzné prvky.
7. Overte komutatívnosť a asociatívnosť binárnych operácií $+, *$ na množine $\mathbb{Q}$.

Test 1 (ukážkový)

Skup. A: Binárna operácia $+$ na množine A sa nazýva asociatívna, ak ..... Uveďte príklad asociatívnej operácie $+$ na trojprvkovej množine A.

Skup. B: Binárna operácia $*$ na množine B sa nazýva komutatívna, ak ..... Uveďte príklad operácie $*$ na trojprvkovej množiny B, ktorá nie je komutatívna.

Polia

Poľom nazývame množinu $\mathbb{P}$ s dvoma význačnými prvkami, nulou 0 a jednotkou 1, a dvomi binárnymi operáciami na $\mathbb{P}$, sčítaním $+$ a násobením $\cdot$, takými, že platí

(1) $(\forall a, b \in \mathbb{P})(a + b = b + a)$,

(2) $(\forall a, b, c \in \mathbb{P})(a + (b + c) = (a + b) + c)$,

(3) $(\forall a \in \mathbb{P})(a + 0 = a)$,

(4) $(\forall a \in \mathbb{P})(\exists b \in \mathbb{P})(a + b = 0)$,

(5) $(\forall a, b, c \in \mathbb{P})(a \cdot (b + c) = a \cdot b + a \cdot c)$,

(6) $(\forall a, b \in \mathbb{P})(a \cdot b = b \cdot a)$,

(7) $(\forall a, b, c \in \mathbb{P})(a \cdot (b \cdot c) = (a \cdot b) \cdot c)$,

(8) $(\forall a \in \mathbb{P})(1 \cdot a = a)$,

(9) $(\forall a \in \mathbb{P} - \{0\})(\exists b \in \mathbb{P})(a \cdot b = 1)$,

(10) $0 \neq 1$.

Pravidlá pre počítanie

Z axióm poľa vidíme, že sčítanie a násobenie sú komutatívne (1), (6) a asociatívne (2), (7) operácie a násobenie je distributtívne vzhľadom na sčítanie (5). Ďalej 0 je neutrálny prvok sčítania (3) a 1 je neutrálny prvok násobenia (8), pričom tieto dva prvky sú rôzne (10). Z (4) resp. (9) máme pre operácie $+$ resp. $\cdot$ jednoznačne určený inverzný prvok k prvku $a \in \mathbb{P}$; nazývame ich opačný prvok $-a \in \mathbb{P}$ resp. inverzný prvok $a^{-1} \in \mathbb{P}$.

Tvrdenie 1.1

Nech $\mathbb{P}$ je pole. Potom pre ľubovoľné $n \in \mathbb{N}$ a $a, b, c, b_1, \ldots, b_n \in \mathbb{P}$ platí

(a) $a + b = a + c \Rightarrow b = c$,

(b) $(ab = ac \wedge a \neq 0) \Rightarrow b = c$,

(c) $a0 = 0$,

(d) $ab = 0 \Rightarrow (a = 0 \vee b = 0)$,

(e) $-a = (-1)a$,

(f) $a(b - c) = ab - ac$,

Konečné polia $\mathbb{Z}_n$

Pre každé kladné celé číslo n označme množinu

$$\mathbb{Z}_n = \{k \in N : k < n\} = \{0, 1, 2, \ldots, n-1\},$$

ktorú nazývame množinou zvyškových tried modulo n. Na tejto množine zavedieme dve binárne operácie $\oplus$ a $\odot$. Pre $a, b \in \mathbb{Z}_n$ kladieme

$$\begin{aligned} a \oplus b &= \text{zvyšok po delení } (a+b)/n, \\ a \odot b &= \text{zvyšok po delení } (ab)/n. \end{aligned}$$

Možno kázať, že operácie $\oplus$ a $\odot$ sú komutatívne a asociatívne a násobenie je distributávne vzhľadom na sčítanie. Ďalej 0 je neutrálny prvok sčítania a pre $n > 1$ je 1 neutrálny prvok násobenia. Navyše $\ominus a$ je opačný prvok k prvku $a \in \mathbb{Z}_n - \{0\}$; pre $a = 0$ je $\ominus 0 = 0$.

Príklad 1.5

Nech sú binárna operácia $\oplus$ a $\odot$ na množine $\mathbb{Z}_4$ definované tabuľkami:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Vidíme, že 0 je neutrány prvok sčítania a každý prvok má opačný prvok určený jednoznačne $\ominus 0 = 0, \ominus 1 = 3, \ominus 2 = 2, \ominus 3 = 1$. Jednotkovým prvkom násobenia je 1 ale inverzné prvky sú definované len pre prvky 1 a 3 pretože $1^{-1} = 1, 3^{-1} = 3$ ale pre 2 neexistuje prvok 2^{-1} taký, že $2^{-1} \odot 2 = 1$.

A tak musíme konštatovať, že $\mathbb{Z}_4$ s operáciami $\oplus$ a $\odot$ nie je pole.

Tvrdenie 1.2

Množina $\mathbb{Z}_n$ s operáciami $\oplus$ a $\odot$ je pole práve vtedy, keď n je prvočíslo.

Príklad 1.6

Nech sú binárna operácia $\oplus$ a $\odot$ na množine $\mathbb{Z}_5$ definované tabuľkami:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Vidíme, že 0 je neutrány prvok sčítania a každý prvok má opačný prvok určený jednoznačne $\ominus 0 = 0, \ominus a = 5 - a, a \in \mathbb{Z}_5 - \{0\}$. Jednotkovým prvkom násobenia je 1 a inverzné prvky sú pre nenulové prvky definované jednoznačne $1^{-1} = 1, 2^{-1} = 3$, $3^{-1} = 2, 4^{-1} = 4$. Po overení axiómov zistíme, že sa jedná o pole.

Cvičenie 1.2

1. Overte pomocou axiomov poľa, že množiny $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ s operáciami $+$ a $\cdot$ sú polia.
2. Overte pravidlá pre počítanie v poliach pre $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
3. Zistite, či množina $\mathbb{Z}$ s operáciami $\oplus$ a $\otimes$ definovanými vzťahmi $a \oplus b = a + b - 1$ a $a \otimes b = a + b - a \cdot b$ je pole.
4. Overte, že množina $\mathbb{Z}_3$ s operáciami $\oplus$ a $\odot$ je pole.
5. Zistite, prečo množina $\mathbb{Z}_6$ s operáciami $\oplus$ a $\odot$ nie je pole.

Bonusový príklad 1.1

Kvaternióny (William Rowan Hamilton 1805 - 1865)

Kvaterniónmi rozumieme množinu

$$\mathbb{H} = \{q : q = a+bi+cj+dk, a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}.$$

Píšeme $q = a + bi + cj + dk \in \mathbb{H}$, kde $(a, b, c, d) \in \mathbb{R}^4$.

1. (1b) Overte komutatívnosť a asociatívnosť súčtu kvaterniónov

$$q_1 + q_2 = a_1 + a_2 + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k.$$

2. (2b) Definujte pomocou Cayleyho tabuľky operáciu násobenia $\cdot$ medzi jednotkami $M = \{-1, 1, -i, i, -j, j, -k, k\}$.
3. (3b) Overte, že súčin kvaterniónov

$$q_1 \cdot q_2 = (a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k)$$

nie je komutatívny.

Bonusový príklad 1.2

Majme množinu

$$\mathbb{M} = \{-1, 1, i, -i, j, -j, k, -k\}.$$

1. (3b) Definujte na množine $\mathbb{M}$ asociatívnu operáciu $\otimes$ pomocou Cayleyho tabuľky ak pre ľubovoľné $x \in \mathbb{M}$ platí

$$1 \otimes x = x \otimes 1 = x, -1 \otimes x = x \otimes -1 = -x,$$

$$i \otimes i = j \otimes j = k \otimes k = i \otimes j \otimes k = -1.$$

2. (1b) Zistite, či je operácia $\otimes$ na množine $\mathbb{M}$ komutatívna.
3. (1b) Nájdite, ak existuje, neutrálny prvok pre operáciu $\otimes$ na množine $\mathbb{M}$.
4. (2b) Nájdite k prvkom množiny $x \in \mathbb{M}$ inverzné prvky $x^{-1} \in \mathbb{M}$ pre operáciu $\otimes$ na množine $\mathbb{M}$.

Bonusový príklad 1.3

V poli $\mathbb{Z}_7$

1. (1b) Vyčíslite výraz $[(4 \oplus 3) \odot (4 \oplus 5)] \odot (6 \oplus 5) \oplus 2$.
2. (2b) Riešte rovnicu o jednej neznámej

$$3 \oplus (2 \odot x) \odot 5 = 4 \odot 6.$$

3. (2b) Nájdite všetky riešenia systému rovníc o troch neznámych

$$2 \odot x \oplus 5 \odot y \oplus 3 \odot z = 2$$

$$6 \odot x \oplus 4 \odot y \ominus 2 \odot z = 5.$$

4. (2b) Nájdite také riešenia systému rovníc z 3., ktoré maximalizuje cieľovú funkciu

$$F(x, y, z) = x \ominus 5 \odot y \oplus 3 \odot z \ominus 2.$$