

Algebra a diskrétna matematika  
Prehľad z 11. týždňa  
Algebraické štruktúry s jednou binárnou operáciou

**Binárna operácia**  $\varphi$  na množine  $M$  je zobrazenie  $\varphi : M \times M \rightarrow M$ .

Poznámka: Binárna operácia je vždy *uzavretá*;  $\forall x, y \in M : \varphi(x, y) \in M$ .

Neprázdna množina  $M$  spolu s jednou alebo viacerými binárnymi operáciami tvorí **algebraickú štruktúru**.

### Grupoid

Nech  $M$  je neprázdna množina a  $*$  binárna operácia na  $M$ . Potom dvojicu  $(M, *)$  nazývame **grupoid**.

Ak  $M$  je konečná, jedná sa o *konečný grupoid*; inak *nekonečný*.

**Rád** grupoidu je veľkosť množiny  $M$ ; označujeme ho  $|M|$ .

V prípade, že je operácia  $*$  komutatívna, tak hovoríme, že grupoid je **komutatívny**, alebo **abelovský**.

### Pologrupa

**Pologrupa** je grupoid  $(M, *)$ , v ktorom je binárna operácia  $*$  asociatívna.

Príklad 1: Rozhodnite, či sú nasledujúce štruktúry pologrupy.

- a)  $(\mathbb{N}, +)$
- b)  $(\mathbb{N}, \cdot)$
- c)  $(\mathbb{Z}, -)$
- d)  $(\mathbb{Q}, +)$
- e)  $(\mathbb{Q}, \cdot)$
- f)  $(\mathbb{R} - \{0\}, \cdot)$
- g)  $(\mathbb{R} - \{0\}, /)$
- h)  $(\mathbb{C}, +)$

Odpoveď: a) áno, b) áno, c) nie d) áno e) áno, f) áno, g) nie, h) áno

Príklad 2:

a) Štruktúra  $(\mathbb{N}, *)$ , kde  $\forall m, n \in \mathbb{N} : m * n = \max\{m, n\}$ , je abelovská pologrupa.

b) Príklad nekomutatívnej pologrupy je štruktúra  $(M_X, \circ)$ , kde  $M_X$  je množina všetkých funkcií  $f : X \rightarrow X$  a operácia  $\circ$  je skladanie funkcií.

Príklad 3:

Nech množina  $M = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, n \in \mathbb{N} \right\}$  a operácia  $*$  je násobenie matíc.

Dvojica  $(M, *)$  je komutatívna pologrupa, pretože násobenie matíc je asociatívna operácia a navyše pre tento typ matíc platí aj komutativita.

## Monoid

Nech  $(M, *)$  je pologrupa.

Prvok  $e \in M$  sa nazýva **neutrálny** (jednotkový), ak

$$\forall x \in M : x * e = e * x = x$$

Pologrupa  $(M, *)$ , ktorá má neutrálny prvok, sa nazýva **monoid**.

Príklad 4: Overte, či sa jedná o monoidy.

a)  $(\mathbb{N}, +)$

b)  $(\mathbb{N}, \cdot)$

c)  $(2^{\mathbb{N}}, \cup)$

d)  $(2^{\mathbb{N}}, \cap)$

Odpoveď: a) nie, b) áno, c) áno, d) áno

Príklad 5: Zistite, či sú nasledujúce štruktúry monoidy a overte ich komutativitu.

a)  $(\{0, 1, 2, 3\}, *)$ , kde  $m * n = \max\{m + n, 3\}$

b)  $(\{0, 1, 2, 3\}, *)$ , kde  $m * n = \min\{m + n, 3\}$

c)  $(M, \cdot)$ , kde  $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z} \right\}$

Odpoveď: a) nie je algebraická štruktúra, b) komutatívny monoid c) nie je monoid

**Tvrdenie 1:** Ak v monoide existujú neutrálne prvky  $e_1$  a  $e_2$ , potom  $e_1 = e_2$ .

Dôkaz:

Predkladajme, že monoid  $(M, *)$  má dva neutrálne prvky  $e_1, e_2$ .

Platí, že  $e_1 * e_2 = e_2$ , lebo  $e_1$  je neutrálny prvok.

Taktiež  $e_1 * e_2 = e_1$ , lebo  $e_2$  je neutrálny prvok.

Dostali sme, že  $e_1 = e_2$ . □

**Dôsledok:** Každý monoid má práve jeden neutrálny prvok.

## Grupa

Nech  $(M, *)$  je monoid s neutrálnym prvkom  $e$ .

Nech  $x \in M$ . Prvok  $y \in M$  sa nazýva **inverzný** k prvku  $x$ , ak platí

$$x * y = y * x = e$$

Monoid  $(M, *)$ , v ktorom ku každému prvku existuje inverzný prvok, sa nazýva **grupa**.

Príklad 6: Overte, či sa jedná o grupy.

a)  $(\mathbb{Z}, +)$

b)  $(\mathbb{Z} - \{0\}, \cdot)$

c)  $(\mathbb{Q}^+, \cdot)$

d)  $(\mathbb{R} - \{0\}, \cdot)$

Odpoveď: a) áno, b) nie, c) áno, d) áno

**Tvrdenie 2:** Ak v grupe  $(M, *)$  existujú k prvku  $x \in M$  inverzné prvky  $y_1$  a  $y_2$ , potom  $y_1 = y_2$ .

Dôkaz:

Predkladajme, že prvok  $x \in M$  má v grupe  $(M, *)$  dva inverzné prvky  $y_1, y_2 \in M$ , t. j.  $x * y_1 = y_1 * x = e$  a  $x * y_2 = y_2 * x = e$ . Potom platia nasledujúce rovnosti

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2$$

Dostali sme teda, že  $y_1 = y_2$ . □

**Dôsledok:** Každý prvok grupy má práve jeden inverzný prvok.

Inverzný prvok k prvku  $x$  označujeme  $x^{-1}$ .

Príklad 7: Množinu celých čísel si rozdelíme do dvoch množín podľa parity.

$P$  = množina všetkých celých párných čísel

$N$  = množina všetkých celých nepárnych čísel

Uvažujme množinu  $M = \{P, N\}$  s operáciou sčítania (aplikovanou medzi každou dvojicou čísel z daných množín). Dvojica  $(M, +)$  tvorí grupu. Neutrálň prvok je  $P$  a inverzný prvok k  $N$  je  $N$ .

Príklad 8: Uvažujme nasledujúce množiny

$$A = \{\dots, -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, \dots\}$$

$$B = \{\dots, -14, -11, -8, -5, -2, 1, 4, 7, 10, 13, 16, \dots\}$$

$$C = \{\dots, -13, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17, \dots\}$$

Dvojica  $(\{A, B, C\}, +)$  tvorí grupu. Jej neutrálnym prvkom je  $A$  a platí, že  $B^{-1} = C$ , teda aj  $C^{-1} = B$ .

Pre každé prirodzené číslo  $k$  označme

$$\mathbb{Z}_k = \{n \in \mathbb{Z}_0^+, n < k\} = \{0, 1, 2, \dots, k-1\}$$

Množinu  $\mathbb{Z}_k$  nazývame **množinou zvyškových tried modulo  $k$** , alebo triedami reziduí.

Definujme operáciu  $\oplus$  na množine  $\mathbb{Z}_k$  nasledovne:

$\forall a, b \in \mathbb{Z}_k : a \oplus b$  je zvyšok po delení  $(a + b) : k$ .

Operácia  $\oplus$  je na  $\mathbb{Z}_k$  asociatívna.

Neutrálny prvok vzľadom na  $\oplus$  je  $e = 0$ .

Pre každé  $a \in \mathbb{Z}_k, a \neq 0$  je inverzný prvok  $a^{-1} = k - a$ , lebo  $a \oplus a^{-1} = a \oplus (k - a) \equiv 0 \pmod{k}$ .

Dvojica  $(\mathbb{Z}_k, \oplus)$  tvorí **abelovskú grupu**.

Zapisujeme ju jednoducho  $(\mathbb{Z}_k, +)$ .

V tejto grupe sa namiesto  $a^{-1}$  zvykne písať  $-a$ , pretože  $k - a$  je v rovnakej zvyškovej triede ako  $-a$ .

Príklad 9: Inverzné prvky v grupe  $(\mathbb{Z}_{11}, \oplus)$  sú nasledovné:

$$-1 = 10, -10 = 1$$

$$-2 = 9, -9 = 2$$

$$-3 = 8, -8 = 3$$

$$-4 = 7, -7 = 4$$

$$-5 = 6, -6 = 5$$

Príklad 10: Nájdite všetky riešenia každej z daných rovníc.

a)  $7 + x \equiv 5 \pmod{9}$

b)  $3x \equiv 4 \pmod{8}$

c)  $4x \equiv 6 \pmod{7}$

d)  $2x \equiv 3 \pmod{6}$

Odpoveď: a)  $x = 7 + 9k, k \in \mathbb{Z}$ ; b)  $x = 4 + 8k, k \in \mathbb{Z}$ , c)  $x = 5 + 7k, k \in \mathbb{Z}$

d) nemá riešenie

**Rád prvku**  $a$  grupy  $(M, *)$  je najmenšie kladné celé číslo  $n$  také, že

$$a^n = e,$$

kde  $a^n$  znamená  $n$ -krát aplikovanú operáciu  $*$  na prvok  $a$ .

Označuje sa  $|a|$ .

Ak také  $n$  neexistuje, hovoríme, že  $a$  má **nekonečný rád**.

**Príklad 11:** Určte rády daných prvkov v zodpovedajúcich grupách.

a) všetkých prvkov v  $(\mathbb{Z}_6, +)$

b) prvku  $4$  v  $(\mathbb{Z}, +)$

c) komplexnej jednotky  $i$  v  $(\mathbb{C} - \{(0, 0)\}, \cdot)$

Odpoveď: a) rád  $0$  je  $1$  (jedná sa o neutrálny prvok), rády prvkov  $1, 2, 3, 4, 5$  sú  $6, 3, 2, 3, 6$  v zodpovedajúcom poradí; b)  $\infty$ , c)  $4$

Množina **generátorov** grupy je taká podmnožina grupy, že každý prvok grupy sa dá vyjadriť ako "súčin" mocnín týchto generátorov.

**Prezentácia grupy** pomocou generátorov:  $\langle \text{generátory} \mid \text{relácie} \rangle$

**Cyklická grupa** je grupa, ktorá je generovaná jedným prvkom  $g$ , t. j. je to množina všetkých mocnín prvku  $g$ .

Zapisuje sa  $\langle g \mid g^n = e \rangle$ , skrátené  $\langle g \rangle$ .

Grupa z príkladu 7 je cyklická grupa  $(\mathbb{Z}_2, +)$  a grupa z príkladu 8 je  $(\mathbb{Z}_3, +)$ .

Príklad 12: Nájdite generátory grúp  $(\mathbb{Z}_5, +), (\mathbb{Z}_6, +), (\mathbb{Z}_5 - \{0\}, \odot), (\mathbb{Z}, +)$ .

Odpoveď:

$$(\mathbb{Z}_5, +) = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle$$

$$(\mathbb{Z}_6, +) = \langle 1 \rangle = \langle 5 \rangle$$

$$(\mathbb{Z}_5 - \{0\}, \odot) = \langle 2 \rangle$$

$$(\mathbb{Z}, +) = \langle 1 \rangle$$

Grupa symetrií pravidelného  $n$ -uholníka sa nazýva **dihedrálna grupa**.

Označuje sa  $D_n$

Jej rád je  $|D_n| = 2n$  ( $n$  osových symetrií a  $n$  otočení)

Neutrálny prvok  $e$  je identita.

Prezentácia:  $D_n = \langle r, s \mid r^n = e, s^2 = e, rs = sr^{-1} \rangle$

$r$  – rotácia o  $2\pi/n$  stupňov

$s$  – symetria podľa pevnej osi symetrie