Algebraické štruktúry s jednou binárnou operáciou

Algebra a diskrétna matematika

Prednáška č. 10

Binárna operácia

Binárna operácia je "dvojčlenná" operácia, ktorá každej usporiadanej dvojici prvkov z nejakej množiny priraďuje jediný tretí prvok z tej istej množiny; t. j.
binárna operácia φ na množine M je zobrazenie $\varphi : M \times M \to M$.

Z faktu, že φ je zobrazenie vyplýva, že

- každá binárna operácia je *uzavretá*; t. j. $\forall x, y \in M : \varphi(x, y) \in M$,
- výsledok operácie je definovaný pre *každú* usporiadanú dvojicu z $M \times M$, t. j. $\forall x, y \in M \ \exists z \in M : \varphi(x, y) = z$.

Známe príklady:
Číselné operácie: sčítanie, odčítanie, násobenie, max, min.

Množinové operácie: prienik, zjednotenie, rozdiel.

Označenie: Ak sa nejedná o známe operácie, najčastejšie používané označenie binárnej operácie je $*$, $\circ, \oplus$ alebo $\otimes$; píšeme $x * y, x \circ y$ atď.

Vlastnosti binárnych operácií

Nech $*$ je binárna operácia na množine M. Hovoríme, že operácia $*$ je

- **komutatívna**, ak $\forall x, y \in M : x * y = y * x$
- **asociatívna**, ak $\forall x, y, z \in M : (x * y) * z = x * (y * z)$

Nech $*, \circ$ sú dve binárne operácie na M. Hovoríme, že

- operácia $*$ je **zľava distributívna** vzhľadom na operáciu $\circ$, ak $\forall x, y, z \in M : x * (y \circ z) = (x * y) \circ (x * z)$,
- operácia $*$ je **sprava distributívna** vzhľadom na operáciu $\circ$, ak $\forall x, y, z \in M : (x \circ y) * z = (x * z) \circ (y * z)$,
- operácia $*$ je **distributívna** vzhľadom na operáciu $\circ$, ak je vzhľadom na $\circ$ distributívna zľava aj sprava.

Príklad

Príklad: Na množine reálnych čísel overte komutativitu a asociativitu daných operácií.

a) $a * b = \sqrt[3]{a} - \sqrt[3]{b}$

b) $a * b = |a + b|$

c) $a * b = ab + a + b$

c). $ab + a + b = ba + b + a$ $\quad \forall a, b \in R$ áno

asoc. ĽS: $a * (bc + b + c) = abc + ab + ac + a + bc + b + c$

PS: $(ab + a + b) * c = abc + ac + bc + ab + a + b + c$

áno

a). komut. $\forall a, b \in R$: $a * b = b * a$

$\sqrt[3]{a} - \sqrt[3]{b} \overset{?}{=} \sqrt[3]{b} - \sqrt[3]{a}$ $\quad$ nie $\rightarrow$ $a = 8$, $b = 27$: $\sqrt[3]{8} - \sqrt[3]{27} = 2 - 3 = -1$, $\sqrt[3]{27} - \sqrt[3]{8} = 3 - 2 = 1$

asoc. $\forall a, b, c \in R$ $\quad a * (b * c) = (a * b) * c$ $\quad a = 8$, $b = 27$, $c = 1$

$\sqrt[3]{a} - (\sqrt[3]{b} - \sqrt[3]{c}) \overset{?}{=} (\sqrt[3]{a} - \sqrt[3]{b}) - \sqrt[3]{c}$

$2 - (3 - 1) = 0 \neq (2 - 3) - 1 = -2$ $\quad$ nie

b). $\forall a, b \in R$: $|a + b| = |b + a|$ $\quad$ áno $\quad a = -100$, $b = 1$, $c = 1$

$\forall a, b, c \in R$ $\quad |a + |b + c|| \overset{?}{=} ||a + b| + c|$

$|-100 + |1 + 1|| = 98 \neq ||-100 + 1| + 1| = 99 + 1 = 100$ $\quad$ nie

Algebraické štruktúra, grupoid

Algebraická šruktúra

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

Rozoznávame veľa rôznych algebraických štruktúr podľa toho, aké vlastnosti spĺňajú ich binárne relácie.

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.

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

Pologrupa

Pologrupa

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

Príklad: Rozhodnite, či sú nasledujúce štruktúry pologrupy, prípadne grupoidy.

a) $(\mathbb{N}, +)$ áno

b) $(\mathbb{N}, \cdot)$ áno

c) $(\mathbb{N}, -)$ nie $\to$ nie je štruktúra, operácia nie je uzavretá

d) $(\mathbb{Z}, -)$ grupoid

e) $(\mathbb{Q}, \cdot)$ áno

f) $(\mathbb{Q}, /)$ nie, nedelíme 0 $\to$ nie je def. pre 0

g) $(\mathbb{R} - \{0\}, /)$ grupoid (delenie nie je asoc.)

h) $(\mathbb{C}, +)$ áno

Príklad

Overte, že nasledujúca štruktúra je pologrupa a zistite, či je abelovská.
$(\mathbb{N}, *)$, kde $\forall m, n \in \mathbb{N} : m * n = \max\{m, n\}$

1, uzavretosť ?

$\forall m, n \in N : \quad m * n = \max\{m, n\} \in N$ áno

2., Asoc.

$\forall m, n, k \in N : \quad m * (n * k) = (m * n) * k$

LS: $m * \max\{n, k\} = \max\{m, \max\{n, k\}\} = \max\{m, n, k\}$

PS: $\max\{m, n\} * k = \max\{\max\{m, n\}, k\} = \max\{m, n, k\}$

áno

3. komut.

$\forall m, n \in N : \quad m * n = n * m$

$\max\{m, n\} = \max\{n, m\}$ áno

abelovská pologrupa

Príklad

Daná je štruktúra $(M_X, \circ)$, kde M_X je množina všetkých funkcií $f : X \to X$ a operácia $\circ$ je skladanie funkcií.

Zistite, či sa jedná o pologrupu a overte komutativitu.

1., uzavretosť

$\forall f, g \in M_X :$ $f : M \to M$, $g : M \to M$ $\quad f \circ g \in M_X$ $\quad f \circ g : M \to M$? $\quad f(g(x)) \in M_X$ áno

2. Asoc.

$\forall f, g, h \in M_X :$ $f \circ (g \circ h) = (f \circ g) \circ h$

$L'S: \; f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x)))$ áno

$PS: \; (f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x)))$

POLOGRUPA

3. KOMUT.

$\forall f, g \in M_X :$ $f \circ g = g \circ f$ $\quad \underline{\text{nie}}$

$f \circ g = \sqrt{\sin x}$

$g \circ f = \sin \sqrt{x}$

$f(x) = \sqrt{x}$

$g(x) = \sin x$

Príklad

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

Ukážte, že $(M, *)$ je pologrupa. Je komutatívna (abelovská)?

1. UZAVRETOSŤ

$\forall A, B \in M: \quad A \cdot B \in M$

$\underbrace{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}}_{B} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix} \in M$ lebo $b+a \in N$

$a, b \in N$

2, ASOCIATIVITA → PLATÍ VO VŠEOBECNOSTI (VIEME Z LINEÁRNEJ ALGEBRY)

3, $\forall A, B \in M: \quad A \cdot B = B \cdot A$

$B \cdot A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix} = A \cdot B$

áno komutatívne

$\boxed{\text{komut. pologrupa}}$

Monoid

Nech $(M, *)$ je pologrupa.

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

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

Monoid

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

Príklad: Overte, či sa jedná o monoidy.

a) $(\mathbb{N}, +)$ nie, $0 \notin N$ $e = 0$

b) $(\mathbb{N}, \cdot)$ áno

c) $(2^{\mathbb{N}}, \bigcup)$ $e = \emptyset$ áno, monoid $A \cup \emptyset = A$

d) $(2^{\mathbb{N}}, \bigcap)$ $e = N$ áno, monoid $A \cap N = A$

Príklad

Určte, či je daná štruktúra monoidy a overte komutatívnosť.

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

M

1. UZAVRETÉ?

$\forall m,n \in M: \quad m*n = \min\{m+n,3\} \le 3$ $\in M?$

$\in M$ áno

$\boxed{\text{komutatívny monoid}}$

2. ASOC. $\forall m,n,k \in M: \quad m*(n*k) = (m*n)*k$

ĽS: $m*(\min\{n+k,3\}) = \min\{m+\min\{n+k,3\},3\} =$

$= \min\{m+n+k, m+3, 3\} = \min\{m+n+k,3\}$

PS: $\min\{m+n,3\}*k = \min\{\min(m+n,3)+k,3\} =$

$= \min\{m+n+k, 3+k, 3\} = \min\{m+n+k,3\}$

ĽS = PS áno

3. $e=?$ $\forall m \in M: \quad m*e = e*m = m$

$\min\{m+e,3\} = m$ $\quad e=0$ áno monoid

4. KOMUT. $\forall m,n \in M$

$m*n = n*m$

$\max\{m+n,3\} = \max\{n+m,3\}$ ✓

Príklad

Rozhodnite, o akú štruktúru sa jedná a či je abelovská.

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

1. UZAVRETOSŤ

$\forall A, B \in M: \quad A \cdot B \in M$

$$\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} x & y \\ z & t \end{pmatrix}}_{B} = \begin{pmatrix} \overset{\in \mathbb{Z}}{ax+bz} & \overset{\in \mathbb{Z}}{ay+tb} \\ \underset{\in \mathbb{Z}}{cx+dz} & \underset{\in \mathbb{Z}}{cy+dt} \end{pmatrix} \in M$$

áno

$a, b, c, d, x, y, z, t \in \mathbb{Z} \Rightarrow$

2. ASOC. áno

3.) $e = ?$ $\quad e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \qquad A \cdot I = A = I \cdot A$

4.) $A \cdot B = B \cdot A$

$$B \cdot A = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \overset{\neq\, ax+bz}{ax+cy} & \\ & \end{pmatrix}$$

nie

$\boxed{\text{nekomutatívny monoid}}$

Jednoznačnosť neutrálneho prvku

Tvrdenie

Ak v monoide existujú neutrálne prvky e_1 a e_2, potom $e_1 = e_2$.

Dôkaz:

Predokladajme, 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

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

Grupa

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

Príklad: Overte, či sa jedná o grupy.

a) $(\mathbb{Z}, +)$ áno $e=0$ inverz k x je $-x$

b) $(\mathbb{Z} - \{0\}, \cdot)$ nie grupa $e=1$ inverz k x je $\frac{1}{x} \notin \mathbb{Z}$
$\to$ monoid

c) $(\mathbb{Q}^+, \cdot)$ $\to$ nie lebo pre 0 nemáme inverz

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

Jednoznačnosť inverzného prvku

Tvrdenie

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

Dôkaz:

Predpokladajme, 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 $x * y_2 = y_2 * x = e$

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

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

$P =$ množina všetkých celých párnych čísel $\to 0$

$N =$ množina všetkých celých nepárnych čísel $\to 1$

zvyšky po delení 2

Uvažujme $M = \{P, N\}$. Tvorí $(M, +)$ grupu?

1. UZAVRETOSŤ

$P + N = N \qquad N + P = N \qquad \in M$

$P + P = P \qquad N + N = P$

2. ASOC. + áno

3) $e = P$

4) $P^{-1} = P$

$N^{-1} = N$

grupa

Príklad

$A = \{\dots, -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, 18, 21, 24\} = \{3k, k \in Z\}$

$B = \{\dots, -14, -11, -8, -5, -2, 1, 4, 7, 10, 13, 16, 19, 22\} = \{3k+1, k \in Z\}$

$C = \{\dots, -13, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17, \dots\} = \{3k+2, k \in Z\}$

Tvorí dvojica $(\underbrace{\{A, B, C\}}_{M}, +)$ grupu?

zvyšok po delení číslom 3

1. uzavr.

$A + B = B$ $B + B = C$
$A + C = C$ $B + C = A$ $\in M$ áno
$A + A = A$ $C + C = B$

$A \to 0$
$B \to 1$
$C \to 2$ $e = 0$

2. asoc. + áno

$0 + 0 = 0$
$0 + 1 = 1$
$1 + 2 = 0$

3.) $e = A$

4.) $A^{-1} = A$
$B^{-1} = C$
$C^{-1} = B$

áno grupa

$(Z_k, \oplus)$

Pre každé prirodzené čislo k označme

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

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

$\forall a, b \in \mathbb{Z}_k : \quad a \oplus b$ 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 $a \in \mathbb{Z}_k$ je inverzný prvok $a^{-1} = k - a$, lebo $a \oplus a^{-1} = a \oplus (k-a) \equiv 0 \pmod{k}$.

Dvojica $(Z_k, \oplus)$ tvorí **abelovskú grupu**.

Zapisujeme ju jednoducho $(Z_k, +)$.

Pre každé prirodzené čislo k označme

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

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

$\forall a, b \in \mathbb{Z}_k : \quad a \oplus b$ 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 $a \in \mathbb{Z}_k$ je inverzný prvok $a^{-1} = k - a$, lebo $a \oplus a^{-1} = a \oplus (k-a) \equiv 0 \pmod{k}$.

Dvojica $(Z_k, \oplus)$ tvorí **abelovskú grupu**.

Zapisujeme ju jednoducho $(Z_k, +)$.

Príklad

Nájdite všetky inverzné prvky v grupe $(\mathbb{Z}_{11}, \oplus)$.

$\mathbb{Z}_{11} = \{0, 1, 2, \ldots \quad 10\}$

$e = 0$

$1^{-1} = 10$

$2^{-1} = 9$

$3^{-1} = 8$

$4^{-1} = 7$

$5^{-1} = 6$

$6^{-1} = 5$

$7^{-1} = 4$

$8^{-1} = 3$

$9^{-1} = 2$

$10^{-1} = 1$

Príklad

Nájdite všetky riešenia každej z daných rovníc.

a) $7 + x = 6 \pmod 9$

$x = 8$

$\{9k + 8,\ k \in \mathbb{Z}\}$

b) $x + x + x = 5 \pmod 8$

$x = 7$

$\{8k + 7,\ k \in \mathbb{Z}\}$

c) $x + x + 9 = 3 \pmod{11}$

$x + x = 3 + 2$

$x + x = 5$

$x = 8$

$\{11k + 8,\ k \in \mathbb{Z}\}$