

Algebraické štruktúry s jednou operáciou

Pojmy

Hierarchia (kategórie) algebraických štruktúr $(M, \circ)$:

$\circ$	je operácia	$\rightarrow$ grupoid
	+ asociatívna	$\rightarrow$ pologrupa
	+ neutr. prvok (obojsmerný)	$\rightarrow$ monoid
	+ inv. prvky	$\rightarrow$ grupa
	+ komutatívna	$\rightarrow$ komutatívna/abelovská grupa

Riešené príklady I

Príklad 1

Na množine $M = \{1, 2, 3\}$ je daná operácia $x \circ y = x$. Kategorizujte $(M, \circ)$.

Riešenie:

Táto operácia sa už vyskytla v neriešených príkladoch z predošlého cvičenia. Zhrnieme:

operácia ✓ asociatívna ✓ // nie je komutatívna
neutr. prvok je iba pravý, to na monoid nestačí $\Rightarrow$ pologrupa

Príklad 2

Na $M = (\mathbb{R} \setminus \{0\})^2$ je daná operácia $[a, b] \circ [c, d] = [-ac, bd]$. Kategorizujte $(M, \circ)$.

Riešenie:

operácia ✓

asociatívna ✓ lebo: $([a, b] \circ [c, d]) \circ [g, h] = [-ac, bd] \circ [g, h] = [acg, bdh]$

$$[a, b] \circ ([c, d] \circ [g, h]) = [a, b] \circ [-cg, dh] = [acg, bdh]$$

komutatívna ✓ $[a, b] \circ [c, d] = [-ac, bd] = [-ca, db] = [c, d] \circ [a, b]$

neutr. prvok ✓ $[a, b] \circ [e, f] = [a, b]$, tj. $[-ae, bf] = [a, b] \Rightarrow [e, f] = [-1, 1]$

inv. prvky ✓ zapíšeme $[a, b]^{-1}$ po zložkách ako $[a', b']$, potom musí platiť:
 $[a, b] \circ [a', b'] = [-1, 1]$, tj. $[-aa', bb'] = [-1, 1]$, odkiaľ dostaneme
 $[a, b]^{-1} = [a', b'] = [1/a, 1/b]$

$\Rightarrow$ grupa

Príklad 3

Na množine matic 2×2 (zápis ako v Matlabe¹) $M = \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}$, $x \in \mathbb{R} \setminus \{0\}$, $y \in \mathbb{R}$ je daná operácia $*$ bežného maticového násobenia. Kategorizujte $(M, *)$.

Riešenie:

operácia ✓ $\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} u & v \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} xu & xv+y \\ 0 & 1 \end{bmatrix}$ *výsledok má správny tvar*
asociatívnosť ✓ *súčin matic je asociatívny (vieme z LA)*
neutrálny prvok ✓ *pri súčine to môže byť iba jednotková matica, ktorá však v M je prítomná.*
inverzné prvky ✓ platí: $\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1/x & -y/x \\ 0 & 1 \end{bmatrix}$
– keďže x je nenulové, inverzná matica existuje a patrí do M.
 $\Rightarrow$ grupa

Príklad 4

Je dané univerzum X a množina všetkých jeho podmnožín 2^X . Kategorizujte štruktúry $(2^X, \cup)$, $(2^X, \cap)$ a $(2^X, \Delta)$.

Riešenie:

Všetko potrebné už bolo preskúmané na minulom cvičení, takže teraz stačí už len rozdať tituly.

$(2^X, \cup)$ $\cup$ je oper., asoc., kom., neutr. prvok je $\{\}$ $\rightarrow$ monoid
 $(2^X, \cap)$ $\cap$ je oper., asoc., kom., neutr. prvok je X $\rightarrow$ monoid
 $(2^X, \Delta)$ Δ je oper., asoc., kom., neutr. prvok je $\{\}$, inv. k A je $A \rightarrow$ komut. grupa

Príklad 5

Kategorizujte nasledujúce štruktúry:

- a) $(\mathbb{Z}_n, +)$ b) $(\mathbb{Z}_3, *)$ c) $(\mathbb{Z}_3 \setminus \{0\}, *)$ d) $(\mathbb{Z}_4 \setminus \{0\}, *)$
e) $(\mathbb{Z}_n \setminus \{0\}, *)$, kde n je prvočíslo

Poznámka: Množinu $\mathbb{Z}_n$ tvoria prvky $\{0, 1, 2, \dots, n-1\}$. Pridružená operácia sa vždy (aj keď to nie je výslovne uvedené) rozumie s dodatkom "modulo n ".

¹ Prepíšte si to na papier tak, ako bežne zapisujete matice napr. v LA, bude to zrozumiteľnejšie.

Riešenie:

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

operácia – súčet celých čísel je celé číslo a modulo n výsledok bezpečne zaparkuje do $\mathbb{Z}_n$
asoc., kom. – súčet je asociatívny a komutatívny, modulo n to nemá ako pokaziť
neutrálly prvok pri súčte je 0, pričom 0 patrí do $\mathbb{Z}_n$, takže je to v poriadku
inverzné prvky – pre každé x existuje $x^{-1} = n-x$ patriace do $\mathbb{Z}_n$. Lahko overíme, že platí:
$$x + (n-x) \mid \text{mod } n = n \mid \text{mod } n = 0$$

$\Rightarrow (\mathbb{Z}_n, +)$ je komutatívna grupa

b) $(\mathbb{Z}_3, *)$

operácia – súčin celých čísel je celé číslo a modulo 3 výsledok bezpečne zaparkuje do $\mathbb{Z}_3$
asoc., kom. – súčin je asociatívny a komutatívny, modulo 3 to nemá ako pokaziť
neutrálly prvok pri súčine je 1, pričom 1 patrí do $\mathbb{Z}_3$, takže je to v poriadku
 x^{-1} neexistuje pre 0 !!
 $\Rightarrow (\mathbb{Z}_3, *)$ je monoid

c) $(\mathbb{Z}_{3 \setminus \{0\}}, *)$

operácia – množinu tvoria čísla 1 a 2, ich vzájomné súčiny sú (po prípadnom mod 3) zas 1 a 2
asoc., kom. – ako vyššie
neutrálly prvok $e=1$ tu stále máme, takže v poriadku
inverzné prvky : $1^{-1} = 1, 2^{-1} = 2$ bez nuly to už je v poriadku
 $\Rightarrow (\mathbb{Z}_{3 \setminus \{0\}}, *)$ je komutatívna grupa

d) $(\mathbb{Z}_{4 \setminus \{0\}}, *)$

Príklad vyzerá na prvý pohľad podobne ako predošlý, ale netreba sa nechať "voviesť" do omylu". Tu totiž $*$ nie je ani len operácia, keďže $2*2=0$ (mimo množiny)

e) $(\mathbb{Z}_{n \setminus \{0\}}, *)$, kde n je prvočíslo

Problému, ktorý nastal v predošlom príklade, sa vyhneme tým, že n bude prvočíslo, tj. nenájdu sa dve čísla (medzi 0 až $n-1$), ktorých súčin by bol rovný $k*n$, čiže 0 pri pohľade cez "mod n ". Rovnako ako vyššie, máme operáciu, je asoci., kom., a je tu neutrálly prvok $e=1$.

S inverznými prvkami je to dramatickejšie. Najprv malá odbočka.

Je možné, aby existovali dva rôzne prvky a, b zo $\mathbb{Z}_{n \setminus \{0\}}$, kde $n > a > b$, tak aby platilo
 $a*x = b*x \text{ mod } n$?

Ak by sme ich našli, potom by muselo byť $(a-b)*x = 0 \mid \text{mod } n$.

Ak n je prvočíslo a 0 nie je prítomná v $\mathbb{Z}_{n \setminus \{0\}}$, x tú nulu nespraví - ostáva možnosť

$a-b = 0 \mid \text{mod } n$, čo vzhľadom na veľkosť a, b implikuje ich rovnosť.

Odpoveď na vyššie položenú otázku je teda NIE. Ak a, b sa nerovnajú, tak sa nerovnajú ani $ax, bx \text{ (mod } n)$.

Späť k inverzným prvkom. Číslo x môžeme násobiť n rôznymi číslami. Výsledky (je ich spolu n) vychádzajú medzi 0 až $n-1$ a musia byť navzájom rôzne! Takže aj číslo 1 musí byť medzi nimi. Tj. ku každému x existuje kamarát x^{-1} , s ktorým v súčine dajú 1.

$\Rightarrow (\mathbb{Z}_{n \setminus \{0\}}, *)$ je komutatívna grupa

Poznámka: Úvahy v predošlom príklade sa dajú zovšeobecniť k tvrdeniu, že v akejkol'vek grupe z rovnosti $a \circ x = b \circ x$ plynie $a=b$ (pravidlo o krátení). Nepochybne na niektorej prednáške o tom bola/bude reč.

Homomorfizmus

Pojmy

Homomorfizmus $h: (L, \circ) \rightarrow (M, \circ)$ je zobrazenie, ktoré "rešpektuje operácie", tj.

$$\text{pre všetky } x, y \in L \text{ platí} \quad h(x \circ y) = h(x) \circ h(y)$$

Ak je h navyše bijekcia, ide o izomorfizmus, teda zobrazenie, ktoré úplne presne skopíruje celú štruktúru $(L, \circ)$ do $(M, \circ)$. Existencia izomorfizmu medzi $(L, \circ)$ a $(M, \circ)$ dokazuje, že ide z hľadiska algebry o rovnakú štruktúru (len ich prvky a operácie sú inak označené).

Riešené príklady II

Príklad 1

Je dané zobrazenie $h: (\mathbb{R}^+, *) \rightarrow (\mathbb{R}, +)$, $h(x) = \ln(x)$. Zistite, či je h homomorfizmus.

Riešenie:

$$h(x*y) = \ln(x*y) = \ln(x) + \ln(y) = h(x) + h(y) \quad \checkmark \quad \text{izomorfizmus}$$

Príklad 2

Je dané zobrazenie $h: (\mathbb{R}^+, *) \rightarrow (\mathbb{R}^+, *)$, $h(x) = \sqrt{x}$. Zistite, či je h homomorfizmus.

Riešenie:

$$h(x*y) = \sqrt{x*y} = \sqrt{x} * \sqrt{y} = h(x)*h(y) \quad \checkmark \quad \text{izomorfizmus}$$

Príklad 3

Je dané zobrazenie $h: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$, $h(x) = 2x$. Zistite, či je h homomorfizmus.

Riešenie:

$$h(x+y) = 2(x+y) = 2x + 2y = h(x) + h(y) \quad \checkmark \quad \text{homomorfizmus}$$

Príklad 4

Je dané zobrazenie $h: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_n, +)$, $h(x) = x \bmod 7$. Ukážte, že je h homomorfizmus a nájdite jeho jadro.

Riešenie:

$$h(x+y) = (x+y) \bmod 7 = (x \bmod 7 + y \bmod 7) \bmod 7 = h(x) + h(y) \quad \checkmark \quad \text{homomorfizmus}$$

Je jedno, či mod 7 aplikujeme na viackrát alebo iba raz súhrnne na konci.

Jadro (prvky, ktoré sa zobrazia na neutrálny prvok): $\text{Ker}(h) = 7\mathbb{Z}$

Príklad 5

Je dané zobrazenie $h: (\mathbb{R}, +) \rightarrow (\mathbb{C}, *)$, $h(x) = \exp(i\pi x)$. Zistite, či je h homomorfizmus.

Riešenie:

$$h(x+y) = \exp(i\pi(x+y)) = \exp(i\pi x) * \exp(i\pi y) = h(x) * h(y) \quad \checkmark \quad \text{homomorfizmus}$$

Príklad 6

Nájdite (ak existuje) izomorfizmus $(M, \cup) \rightarrow (M, \cap)$.

Riešenie:

Izomorfizmus musí o.i. zobrazit' neutrálny prvok na neutrálny. V tomto prípade prázdnu množinu na celok X . Túto vlastnosť má napr. komplement. Overme, či ide o izomorfizmus.

- injektívnosť: pre dve rôzne A, B sa nepochybne líšia aj A^c, B^c .
- surjektívnosť: Pre každé A existuje množina A^c a platí $(A^c)^c = A$. Tj. každej množine A viem nájsť vzor pri operácii komplement.
- homorfizmus: platí $(A \cup B)^c = A^c \cap B^c$ (de Morganov zákon)

Navrhnuté zobrazenie je izomorfizmus.

Neriešené príklady

1. Kategorizujte nasledujúce štruktúry.

Ak to veľkosť množiny dovoľí, uveďte aj Cayleyho tabuľku.

Ak ste vlastnosti niektorých operácií skúmali pred týždňom, stačí sa na to odvolať.

a) $(\mathbb{R}^2, \circ)$, kde $(a,b) \circ (c,d) = (a, d)$

b) $(\mathbb{R}^2, \circ)$, kde $(a,b) \circ (c,d) = (ac, ad)$

c) $(\mathbb{Z}_7 \setminus \{0\}, \circ)$, kde $x \circ y = 2xy \mid \text{mod } 7$

d) $(\mathbb{Z}_5 \setminus \{0\}, \circ)$, kde $x \circ y = 3xy \mid \text{mod } 5$

e) $(M, \cup)$, kde $M = 2^X$ (tj. potenčná množina univerza X).

f) $(M, \cap)$, kde $M = 2^X$

g) (M, Δ) , kde $M = 2^X$ a Δ je symetrická diferencia

2. Navrhните zobrazenie $h: (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, *)$ tak, aby bolo izomorfizmom.

3. Je dané zobrazenie $h: (\mathbb{R}, *) \rightarrow (\mathbb{R}, *)$, $h(x) = x^3$. Zistite, či je h homomorfizmus alebo izomorfizmus.

4. Je dané zobrazenie $h: (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$, $h(x) = 7x$. Zistite, či je h homo/izo-morfizmus.

5. Je dané zobrazenie $h: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_7, +)$, $h(x) = 2x \mid \text{mod } 7$. Ukážte, že h je homomorfizmus a nájdite jeho jadro.

6.** Nájdite (ak existuje) izomorfizmus $(\mathbb{Z}_5 \setminus \{0\}, * \mid \text{mod } 5) \rightarrow (\mathbb{Z}_4, + \mid \text{mod } 4)$.

7.* Nech $M = \{0, 1\}$.

a) Koľko rozličných neizomorfných grupoidov $(M, \circ)$ existuje? Treba ich vypísať?

b) Koľko rozličných neizomorfných pologrúp $(M, \circ)$ existuje? Vypíšte ich.

c) Koľko rozličných neizomorfných monoidov $(M, \circ)$ existuje? Vypíšte ich.

d) Koľko rozličných neizomorfných grúp $(M, \circ)$ existuje? Vypíšte ich.

e) Koľko rozličných neizomorfných komutatívnych grúp $(M, \circ)$ existuje? Vypíšte ich.