

Hierarchia algebraických štruktúr $(M, \circ)$

O operácia $\rightarrow$ grupoid
 A + asociatívna $\rightarrow$ pologrupa
 E + neutr. prvok $\rightarrow$ monoid
 I + inv. prvky $\rightarrow$ grupa
 K + komutatívna $\rightarrow$ komut. grupa

Príklady + čiastočné riešenia

1. Určte pozíciu danej alg. štruktúry v hierarchii. Ak to jej veľkosť umožňuje, uveďte príslušnú Cayleyho tabuľku.

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

O, A, ~~E, I, K~~ pologrupa

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

O, A, ~~E, I, K~~ pologrupa

c) $(\mathbb{Z}_7 \setminus \{0\}, \circ)$, kde $x \circ y = 2xy \pmod{7}$ (skúste aj $3xy$, $kxy+m$ pre rozličné k, m)

$\circ$	1	2	3	4	5	6
1	2	4	6	1	3	5
2	4	1	5	2	6	3
3	6	5	4	3	2	1
4	1	2	3	4	5	6
5	3	6	2	5	1	4
6	5	3	1	6	4	2

O, A, $e=4$,

I: $1-2, 3-3, 4-4, 5-6$

K

S predpisom $kxy+m \pmod{7}$:

Lahko sa presvedčíme, že pokiaľ k nie je nulové, tak s nenulovým m budeme vždy dostávať v tabuľke aj nuly. Takže možnosti sú dve:

Buď $k=0$ a $m=1,2,\dots,6$ (vyššie hodnoty nemá zmysel skúmať). Potom ide o pologrupu.

Alebo $k=1,2,3,4,5,6$ (vyššie hodnoty nemá zmysel skúmať) a potom musí byť $m=0$, teda predpis bude $kxy \bmod 7$.

Operácia je evidentne **komutatívna**.

Asociatívnosť – funguje:

$$\begin{array}{llll} \text{L:} & k(kxy)z & = & k^2xyz \quad \bmod 7 \\ \text{P:} & kx(kyz) & = & k^2xyz \quad \bmod 7 \end{array}$$

Neutrálny prvok:

Má platiť $kex = x \bmod 7$ pre všetky x , teda musí byť $ke = 1 \bmod 7$. Z toho dostávame pre doteraz nepreskúmané k :

$$\begin{array}{ll} k=3 & \rightarrow e=5 \\ k=4 & \rightarrow e=2 \\ k=5 & \rightarrow e=3 \\ k=6 & \rightarrow e=6 \end{array}$$

Inverzné prvky:

Má platiť $kxx^{-1} = e \bmod 7$ pre všetky x .

$$k=3, e=5$$

$$3xx^{-1} = 5 \bmod 7 \quad \rightarrow \quad xx^{-1} = 4 \bmod 7 \quad (\text{prečo? overte!})$$

dvojice navzájom inverzných prvkov: 1 – 4, 2 – 2, 3 – 6, 5 – 5

$$k=4 \rightarrow e=2$$

$$4xx^{-1} = 2 \bmod 7 \quad \rightarrow \quad xx^{-1} = 4 \bmod 7 \quad (\text{prečo? overte!})$$

dvojice navzájom inverzných prvkov: 1 – 4, 2 – 2, 3 – 6, 5 – 5

$$k=5 \rightarrow e=3$$

$$5xx^{-1} = 3 \bmod 7 \quad \rightarrow \quad xx^{-1} = 2 \bmod 7 \quad (\text{prečo? overte!})$$

dvojice navzájom inverzných prvkov: 1 – 2, 3 – 3, 4 – 4, 5 – 6

$$k=6 \rightarrow e=6$$

$$6xx^{-1} = 6 \bmod 7 \quad \rightarrow \quad xx^{-1} = 1 \bmod 7 \quad (\text{prečo? overte!})$$

dvojice navzájom inverzných prvkov: 1 – 1, 2 – 4, 3 – 5, 6 – 6

Záver

Pre $m=0$ a ľubovoľné $k=1,2,\dots,6$ ide o **komutatívnu grupu**.

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

O, K, A (jednoduché, stačí nakresliť obrázky)

E: $E = \emptyset$ pre $(M, \cup)$
 $E = X$ pre $(M, \cap)$

I: Nie je (oba prípady)

Záver: **Monoidy.**

2. Nájdite (ak existuje) izomorfizmus $(M, \cup) \rightarrow (M, \cap)$. (Príklad nadväzuje na 1d)

$h(M) = M^c$ (komplement množiny), rovnaký predpis funguje aj opačným smerom

$(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$ (overiť podľa obrázkov)

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

Neutrálny prvok sa musí zobrazit' na neutrálny: $h(1) = 0$

V grupe $(\mathbb{Z}_5 \setminus \{0\}, * / \text{mod } 5)$ platí:	$2=2$,	$2*2=4$,	$2*2*2=3$,	$2*2*2*2=1$
V grupe $(\mathbb{Z}_4, + / \text{mod } 4)$ platí:	$1=1$,	$1+1=2$,	$1+1+1=3$,	$1+1+1+1=0$

Na základe uvedeného môžeme h definovať ďalej takto:

$h(2)=1$, $h(4)=2$, $h(3)=3$

Ubezpečte sa, že h je naozaj izomorfizmus (že je to vymyslené správne). Nájdite aj iné izomorfizmy (ten uvedený nie je jediný možný).

4. Nech $M = \{0, 1\}$. Koľko rozličných neizomorfných grupoidov $(M, \circ)$ existuje? (Využite svoje riešenie jedného z príkladov z minulého cvičenia)

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

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

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

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

Pri množine $\{0,1\}$ dvojicu izomorfných operácií zadaných tabuľkou spoznáme tak, že jednu z druhej vieme získať vzájomnou výmenou núl a jednotiek a následným preusporiadaním stĺpcov a riadkov (prečo je to tak?). Príklad:

Operácia

	0	1
0	0	0
1	0	1

Zámena 0 a 1

	1	0
1	1	1
0	1	0

Preusporiadanie

Izomorf. oper.

	0	1
0	0	1
1	1	1

Všetkých bin. operácií je 16, ale ak stotožníme izomorfné dvojice, ostane ich 10.

Operácie / Izomorfné dvojice operácií	Asoc. – pologrupy	Neutr. – monoid	Inv. – Grupa																		
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr></table> <table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>		0	1	0	0	0	1	0	0		0	1	0	1	1	1	1	1	asoc. $x \circ y = 0, \quad x \circ y = 1$	nemá e	–
	0	1																			
0	0	0																			
1	0	0																			
	0	1																			
0	1	1																			
1	1	1																			
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>1</td><td>0</td><td>1</td></tr></table> <table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>		0	1	0	0	0	1	0	1		0	1	0	0	1	1	1	1	asoc. $x \circ y = xy \ / \ x \circ y = x+y \text{ (bool.)}$	$e = 1 \ / \ 0$	0 resp. 1 nemá inv. prvok
	0	1																			
0	0	0																			
1	0	1																			
	0	1																			
0	0	1																			
1	1	1																			
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table> <table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>		0	1	0	0	0	1	1	0		0	1	0	1	0	1	1	1	nie je asoc., protipríklad 111 / 000	–	–
	0	1																			
0	0	0																			
1	1	0																			
	0	1																			
0	1	0																			
1	1	1																			
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td></tr></table> <table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr></table>		0	1	0	0	1	1	0	0		0	1	0	1	1	1	0	1	nie je asoc., protipríklad 111 / 000	–	–
	0	1																			
0	0	1																			
1	0	0																			
	0	1																			
0	1	1																			
1	0	1																			
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr></table> <table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>		0	1	0	1	0	1	0	0		0	1	0	1	1	1	1	0	nie je asoc., protipríklad 001 / 110	–	–
	0	1																			
0	1	0																			
1	0	0																			
	0	1																			
0	1	1																			
1	1	0																			
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td></tr></table>		0	1	0	1	1	1	0	0	nie je asoc., protipríklad 000	–	–									
	0	1																			
0	1	1																			
1	0	0																			
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>		0	1	0	1	0	1	1	0	nie je asoc., protipříklad 111	–	–									
	0	1																			
0	1	0																			
1	1	0																			
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>		0	1	0	0	0	1	1	1	asoc. , $x \circ y = x$	nemá e	–									
	0	1																			
0	0	0																			
1	1	1																			
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr></table>		0	1	0	0	1	1	0	1	asoc. , $x \circ y = y$	nemá e	–									
	0	1																			
0	0	1																			
1	0	1																			
<table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>1</td></tr></table> <table><tr><td></td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>		0	1	0	1	0	1	0	1		0	1	0	0	1	1	1	0	asoc. , predpis (bool.): $x \circ y = xy+x'y'$ (ekvival.) $x \circ y = xy'+x'y$ (XOR)	$e = 1 \ / \ 0$	0 – 0, 1 – 1 v oboch prípadoch
	0	1																			
0	1	0																			
1	0	1																			
	0	1																			
0	0	1																			
1	1	0																			

Môžeme teda hovoriť z kvantitatívneho hľadiska o 16 grupoidoch a z kvalitatívneho hľadiska o 10 štrukturálnych typoch grupoidov na báze danej množiny.

Asociatívnosť – pologrupy

Asociatívnosť operácií uvedených v tabuľke sa overuje pomerne jednoducho. Ak operácia nie je asociatívna, tak nie je ťažké nájsť protipríklad. Naopak, pokiaľ operácia je asociatívna, tak sa zhodou okolností aj dá vyjadriť predpisom, takže na pozitívny dôkaz netreba skúšať všetky možné trojice. V tabuľke sú uvedené protipríklady (jeden stačí, ale môžete nájsť aj ďalšie) alebo predpisy (dôkaz asociatívnosti je jednoduchý – neuvádzame).

Všetkých pologrúp je 8, typologicky je to 5 rôznych neizomorfných možností.

Neutrálny prvok – monoid

Neutrálny prvok overujeme len pre asociatívne operácie. Z 8 pologrúp sú 4 aj monoidy, kvalitatívne z 5 neizomorfných typov pologrúp sú monoidy 2.

Inverzné prvky – grupa

Iba dva zo 4 monoidov, kvalitatívne 1 z 2 typov je navyše aj grupou. Ako vidno zo symetrie tabuľky, ide o komutatívnu grupu.

Dokážte nasledujúce tvrdenia:

1. Nech $(X, \circ)$ a $(Y, \bullet)$ sú grupoidy a h je epimorfizmus z X do Y .
Ak $\circ$ je asociatívna, potom aj $\bullet$ je asociatívna.

Epimorfizmus je surjektívny, teda pre každé i, j, k z Y existujú vzory a, b, c z X .
 $(i \bullet j) \bullet k = (h(a) \bullet h(b)) \bullet h(c) = h((a \circ b) \circ c) = h(a \circ (b \circ c)) = h(a) \bullet (h(b) \bullet h(c)) = i \bullet (j \bullet k)$

2. Nech $(X, \circ)$ je monoid a e je neutrálny prvok. Ak pre všetky m z X platí $m \circ m = e$,
potom $\circ$ je komutatívna.

$$a \circ b = a \circ e \circ b = a \circ (a \circ b) \circ (a \circ b) \circ b = (a \circ a) \circ (b \circ a) \circ (b \circ b) = e \circ (b \circ a) \circ e = b \circ a$$

3. Nech operácia $\circ$ je komutatívna. Potom platí $(a \circ b)^n = a^n \circ b^n$, kde $x^n = x \circ x \circ \dots \circ x$.

$$(a \circ b)^n = a \circ b \circ a \circ b \circ a \circ b \circ \dots \circ a \circ b$$

Komutatívnosť umožňuje zamieňať poradie v ľubovoľnej dvojici susedných prvkov. To je situácia, v ktorej môžeme aplikovať napr. bubble-sort a dospieť tak k požadovanému tvaru $a^n \circ b^n$.

4. Nech $(X, \circ)$ je grupa. Ak $(x \circ x) \circ (y \circ y) = (x \circ y) \circ (x \circ y)$, potom $x \circ y = y \circ x$.
(Dokázali ste tým, že $\circ$ je za daných podmienok komutatívna?)

Tvrdenie vyplýva priamo zo zákonov o krátení. Týka sa iba prvkov x, y a nemusí platiť všeobecne, teda na komutatívnosť to nestačí.

5. Každá konečná (!) pologrupa obsahuje idempotentný prvok (tj. $x \circ x = x$, ozn. IP).

Vyberme nejaký prvok a . Pre jednoduchosť operáciu budem značiť $x \circ x = xx$.

Ak $xx = a$, IP sa našiel. Inak označím $aa=b$.

Ak $bb=b$, našiel sa IP. Ak $bb=a$, aplikujem postup U (uvedený nižšie). Inak označím $bb=c$.

Takto postupujem ďalej a nerobím si ťažkú hlavu z počtu písmen v abecede.

Všeobecne: Ak pre nejaký prvok p platí $pp=p$, našiel sa IP. Ak $pp=m$ (m je nejaký prvok, ktorý sme skúmali ešte pred p), aplikujem postup U (nižšie). Inak označím $pp=q$. Atd'.

Vzhľadom na konečný počet prvkov v pologrupe raz musí nastať situácia, že sa "minú" prvky a ak sa doteraz nenašiel IP, už ostane iba možnosť aplikovať postup U.

Postup U:

Nech pre nejaký prvok y platí $yy = s$, kde s je prvok skúmaný ešte skôr ako sme prišli ku y . Vzhľadom na spôsob „výroby“ prvkov platí $y=s^n$ kde n je nejaké prirodzené číslo. Ak dáme obe tieto skutočnosti dokopy, dostávame $s^{2n}=s$.

Položme $x=s^{2n-1}$. Platí: $xx = s^{2n-1}s^{2n-1} = s^{2n+2n-2} = s^{1+2n-2} = s^{2n-1} = x$.

Prvok x je idempotentný.

6. Každá grupa s maximálne 5 prvkami je komutatívna.

Úlohu budeme riešiť zatiaľ bez pojmov *cyklickej grupy* a *generátorov*. Riešenie bude zdĺhavejšie, ale poučné.

1 prvok

□	e
e	e

Jediný prvok musí byť neutrálny (povinne prítomný v grupe). Ako vidno z tabuľky, pri tomto počte nie je možné nebyť komutatívnou.

2 prvky

Neutrálny prvok e a ešte jeden iný – označíme ho a . Tabuľka grupy je iba jedna možná – komutatívnosť je zrejme. (Ak napr. položíme $e=0$ a $a=1$, ide o grupu $(\mathbb{Z}_2, +)$).

□	e	a
e	e	a
a	a	e

3 prvky

Neutrálny prvok e a ešte dva iné – označíme ich a, b . Tabuľka grupy sa zostaví nasledovne – prvý stĺpec a riadok s neutrálnym prvkom sú zrejme, ostatné prvky sa doplnia tak, aby v každom riadku aj stĺpci bol každý prvok práve raz (trochu pripomína sudoku). Možný výsledok je iba jeden (ak napr. $e=0$, $a=1$ a $b=2$, ide o grupu $(\mathbb{Z}_3, +)$). Komutatívnosť je zrejme.

□	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4 prvky

Neutrálny prvok e a ešte tri iné – označíme ich a, b, c . Tabuľka grupy sa zostaví nasledovne: Riadok a stĺpec pri neutrálnom prvku sú jasné. Ďalej rozlíšime dve možnosti –

1. buď $a \cdot a = b$ (možnosť $a \cdot a = c$ je izomorfná, neuvádzam) alebo **2.** $a \cdot a = e$.
(Prípady $a \cdot a = a$ je vylúčený, to by viedlo k stotožneniu $a=e$.)

1.

Dosadím hodnotu b na pozíciu (a, a) . Ostatné hodnoty sa do tabuľky dajú doplniť jediným spôsobom. Ako vidno zo symetrie tabuľky, komutatívnosť "máme".

□	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(Ak napr. položíme $e=0$, $a=1$, $b=2$, $c=3$, ide o grupu $(\mathbb{Z}_4, +)$)

2.

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

Ostatné hodnoty do tabuľky doplníme tak, aby v každom riadku i stĺpci bolo každé písmeno práve raz. To sa dá urobiť iba dvoma spôsobmi, i) a ii):

i)

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

Táto možnosť je izomorfná s prípadom 1. (Položme $e=0$, $a=2$, $b=1$ a $c=3$ a dostaneme opäť grupu $(\mathbb{Z}_4, +)$). Komutatívnosť je viditeľná.

ii)

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

Komutatívnosť je zrejmá.

(Položme $e=00$, $a=01$, $b=10$ a $c=11$ a dostaneme grupu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$)

5 prvkov

Neutrálny prvok e a ešte štyri iné – označíme ich a , b , c , d .

Podľa vyššie uvedených pravidiel vieme zostaviť mnoho rozličných tabuliek, z ktorých však veľká časť nebude spĺňať podmienku asociatívnosti. Doteraz pre počet 4 a menej sme asociatívnosť priamo neoverovali, avšak pre každý z typov sme našli konkrétnu realizáciu, o ktorej sa vie, že ide o grupu (dokázali sme alebo viete ľahko dokázať).

V prípade 5 prvkov podmienku asociatívnosti intenzívne využijeme pri dopĺňaní hodnôt do tabuliek tak, aby sme vedeli včas vylúčiť nevhodné možnosti. Jedno z ľahko použiteľných pravidiel bude nutná podmienka asociatívnosti v tejto podobe:

ak je $\square$ asociatívna a $a^a = b$, potom $a^b = b^a$ (asociatívnosť aplikovaná na trojicu aaa).

Na začiatok opäť rozlíšime dva prípady – 1. buď $a^a = e$ alebo 2. $a^a = b$ (ďalšie možnosti $a^a = c$, $a^a = d$ sú izomorfné, neuvádzam).

1.

Riadok so vstupom a môžeme doplniť podľa pravidiel hodnotami cdb alebo dbc (iná možnosť nie je). Obe možnosti sú izomorfné (presvedčte sa!), preto uvedieme len prvú z nich:

$\square$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b				
c	c				
d	d				

Rýchly test asociatívnosti: $(a \circ a) \circ b = e \circ b = b$; $a \circ (a \circ b) = a \circ c = d$.

Nemusíme ďalej pokračovať, nie je splnená podmienka asociatívnosti. Možnosť 1, teda nevedie k žiadnej grupe.

2.

Riadok so vstupom a môžeme doplniť podľa pravidiel hodnotami i) cde, dec (obe možnosti sú izomorfné, ďalej uvedieme len prvú z nich) alebo ii) edc .

i) Keďže $a \circ a = b$, tak musí platiť $a \circ b = b \circ a$, čo jednoznačne určuje stĺpec so vstupom a .

$\square$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c			
c	c	d			
d	d	e			

Zvyšných 9 hodnôt v tabuľke potom vieme jednoznačne doplniť:

$\square$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Ak teraz položíme napr. $e=0, a=1, b=2, c=3, d=4$, dostávame komutatívnu grupu $(\mathbb{Z}_5, +)$

ii) Keďže $a \circ a = b$, tak musí platiť $a \circ b = b \circ a$, čo jednoznačne určuje stĺpec so vstupom a .

$\square$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	e	d	c
b	b	e			
c	c	d			
d	d	c			

Zvyšných 9 hodnôt v tabuľke nejde doplniť. Táto vetva nevedie ku grupe.

Záver.

Grupy s počtom prvkov najviac 5 sú všetky komutatívne. Nie je ich veľa a pre každý z nájdených typov poznáme nejaké konkrétne realizácie.

Ako je to s grupami s počtom prvkov 6, 7, ... ? Dá sa pokračovať v podobných úvahách ako doteraz?