1 Binárne operácie

S operáciami ste sa stretli už na základnej škole. Teraz tieto vedomosti zovšeobecníme. Začneme s definíciou binárnej operácie.

Definícia 1. Binárna operácia *na množine A je zobrazenie množiny $A \times A$ do A.*

Čo to znamená? Ak máme operáciu $\circ$ na množine A a vyberieme ľubovolné dva prvky napr. x, y z tejto množiny, tak aj výsledok operácie $x \circ y$ musí patriť do množiny A. Napríklad klasické sčítanie je operácia na množine $\mathbb{N}$, lebo súčet dvoch prirodzených čísel je vždy prirodzené číslo. Naopak, klasické odčítanie nie je operáciou na $\mathbb{N}$, lebo napr. $2 \in \mathbb{N} \wedge 5 \in \mathbb{N}$, ale $2 - 5 \notin \mathbb{N}$. V definícii hovoríme o binárnej operácii, lebo s binárnymi operáciami budeme najviac pracovať, preto pokiaľ budeme hovoriť o binárnej operácii, tak slovo binárna môžeme vynechať. Okrem binárnych operácií, poznáme aj unárne operácie, napr. odmocninu na množine nezáporných reálnych čísel. Premyslite si, aké unárne operácie ešte poznáte. A samozrejme, vo všeobecnosti môžeme $n-$prvkom z množiny A priradiť prvok tejto množiny a v takom prípade hovoríme o $n-$árnej operácii na množine A.

Už na základnej škole ste si všímali niektoré pekné vlastnosti sčítania a násobenia, teraz si tieto pojmy zopakujeme.

Definícia 2. *Hovoríme, že binárna operácia $\circ$ na množine A je* **komutatívna**, *ak*

$$\forall x, y \in A \colon x \circ y = y \circ x.$$

Hovoríme, že binárna operácia $\circ$ na množine A je **asociatívna**, *ak*

$$\forall x, y, z \in A \colon (x \circ y) \circ z = x \circ (y \circ z).$$

Klasické sčítanie je komutatívna, asociatívna operácia na $\mathbb{N}$ a zrejme aj na $\mathbb{Z}, \mathbb{Q}$ a $\mathbb{R}$. Rovnako to platí aj pre klasické násobenie. Ale pre klasické odčítanie to neplatí (toto si vyskúšajte). Ešte si vysvetlíme dva dôležité pojmy:

Definícia 3. *Nech $\circ$ je binárna operácia na množine A. Ak existuje taký prvok $e \in A$, o ktorom platí*

$$\forall a \in A \colon a \circ e = e \circ a = a,$$

tak prvok e nazývame **neutrálnym prvkom** *operácie $\circ$.*

Definícia 4. *Nech $\circ$ je binárna operácia na množine A a nech e je neutrálny prvok tejto operácie. Ak o prvkoch $a, a' \in A$ platí*

$$a \circ a' = a' \circ a = e,$$

tak prvok a' nazývame **inverzným prvkom k prvku** *a (vzhľadom na operáciu $\circ$.)*

Zrejme klasické sčítanie má neutrálny prvok 0 (v tomto prípade nezáleží na tom, či pracujeme na množine $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ alebo na množine $\mathbb{R}$, lebo v ľubovolnej z týchto množín platí $0 + a = a + 0 = a$). K prvkom množiny $\mathbb{N}$ neexistujú inverzné (opačné) prvky vzhľadom na klasické sčítanie, iba k 0, tá si je sama sebe inverzná. Ako to bude s klasickým sčítaním a inverznými prvkami na množinách $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$? Premyslite si, ako to je s klasickým násobením a neutrálnym a inverznými prvkami postupne na množinách $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Nasledujúci príklad nám pomôže objasniť pojem operácie na nekonečných množinách.

Príklad 5. *Na množine $\mathbb{R}$ sú definované operácie:*

1. $a \circ b = a + b - 1$,
2. $a \star b = 2 \cdot a \cdot b$,
3. $a \Delta b = a + 2 \cdot b$.

Určte ich vlastnosti (operácie $+, -, \cdot$ sú klasické sčítanie, odčítanie a násobenie na $\mathbb{R}$.).

Riešenie. Postupne sa budeme venovať jednotlivým operáciám a ich vlastnostiam (komutatívnosť, asociatívnosť, neutrálny prvok, inverzné prvky).

1.
   - Operácia $\circ$ je komutatívna, lebo
   $$a \circ b = a + b - 1 = b + a - 1 = b \circ a.$$
   Využili sme komutativitu klasického sčítania.
   - Operácia $\circ$ je asociatívna, lebo
   $$(a \circ b) \circ c = (a+b-1) \circ c = (a+b-1)+c-1 = a+b+c-2 = a+(b+c-1)-1 = a \circ (b+c-1) = a \circ (b \circ c).$$
   Rada pre začiatočníkov: vyjadrite si $(a \circ b) \circ c$, upravte a potom si vyjadrite $a \circ (b \circ c)$, upravte a potom oba výrazy porovnajte.
   - Zistíme, či operácia $\circ$ má neutrálny prvok. Pre neutrálny prvok e musí platiť:
   $$a \circ e = e \circ a = a.$$
   Vzhľadom k tomu, že $\circ$ je komutatívna operácia, tak stačí uvažovať len jednu z uvedených rovností, teda budeme hľadať e tak, aby
   $$a \circ e = a \iff a + e - 1 = a \iff e = 1 \in \mathbb{R}.$$
   Operácia $\circ$ má teda neutrálny prvok $e = 1$ na množine $\mathbb{R}$.
   - Ešte zistíme, či ku každému prvku z $\mathbb{R}$ existuje vzhľadom k $\circ$ inverzný prvok. Teda budeme zisťovať, či vždy existuje a' tak, aby
   $$a \circ a' = a' \circ a = e = 1.$$
   Znovu využijeme komutativitu, teda budeme pracovať len s jednou z uvedených rovností:
   $$a \circ a' = 1 \iff a + a' - 1 = 1 \iff a + a' = 2 \iff a' = 2 - a.$$
   Vzhľadom k tomu, že pre každé reálne číslo a je aj $2 - a$ reálne číslo, tak inverzný prvok existuje ku každému prvku z $\mathbb{R}$, vzhľadom na operáciu $\circ$.

2.
   - Operácia $\star$ je komutatívna, lebo
   $$a \star b = 2 \cdot a \cdot b = 2 \cdot b \cdot a = b \star a.$$
   - Operácia $\star$ je asociatívna, lebo
   $$(a \star b) \star c = (2 \cdot a \cdot b) \star c = 2 \cdot (2 \cdot a \cdot b) \cdot c = 4 \cdot a \cdot b \cdot c = 2 \cdot a \cdot (2 \cdot b \cdot c) = a \star (2 \cdot b \cdot c) = a \star (b \star c).$$

- Zistíme, či operácia $\star$ má neutrálny prvok. Vzhľadom k tomu, že $\star$ je komutatívna operácia, tak budeme pokračovať ako v predchádzajúcom prípade, teda budeme hľadať e tak, aby
$$a \star e = a \iff 2 \cdot a \cdot e = a.$$
Pri vyjadrení e musíme myslieť na to, že a by mohlo byť aj nulové. Ak $a \neq 0$ potom
$$2 \cdot a \cdot e = a \iff e = \frac{1}{2}.$$
Ak $a = 0$ tak vlastne riešime rovnicu
$$2 \cdot 0 \cdot e = 0,$$
ktorej riešením je ľubovolné reálne číslo a teda aj $\frac{1}{2}$. Preto operácia $\star$ má neutrálny prvok $e = \frac{1}{2}$. Vždy treba skontrolovať, či je neutrálny prvok z množiny, na ktorej je operácia definovaná. Keby operácia $\star$ bola definovaná na množine celých čísel, tak by neutrálny prvok nemala.
- Ešte zistíme, či ku každému prvku z $\mathbb{R}$ existuje, vzhľadom k $\star$, inverzný prvok. Znovu využijeme komutativitu, teda budeme riešiť rovnicu:
$$a \star a' = \frac{1}{2} \iff 2 \cdot a \cdot a' = \frac{1}{2} \iff a \cdot a' = \frac{1}{4}.$$
Podobne, ako pri hľadaní neutrálneho prvku, aj teraz musíme rozlíšiť dve možnosti. Ak $a \neq 0$, tak $a' = \frac{1}{4 \cdot a}$, čo je v tomto prípade reálne číslo. Ak $a = 0$, tak dostaneme rovnicu $0 \cdot a' = \frac{1}{4}$, ktorá na množine $\mathbb{R}$ nemá riešenie. Preto inverzný prvok, vzhľadom k operácii $\star$, existuje pre všetky prvky z množiny $\mathbb{R} \setminus \{0\}$.

3. - Operácia Δ nie je komutatívna, lebo napr.
$$1\Delta 2 = 1 + 2 \cdot 2 = 5, \quad \text{ale} \quad 2\Delta 1 = 2 + 2 \cdot 1 = 4.$$
Rada pre začiatočníkov: Ako nájsť protipríklad? Niekedy pomôže metóda "pozriem a vidím", to sa teraz dalo uplatniť. Ale mohli sme si vyjadriť $a\Delta b = a + 2 \cdot b$, $b\Delta a = b + 2 \cdot a$ a potom tieto výrazy porovnať a následne hľadať také a, b, pre ktoré je $a\Delta b \neq b\Delta a$.
- Operácia $\star$ nie je asociatívna, lebo napr.
$$(1\Delta 2)\Delta 3 = (1 + 2 \cdot 2)\Delta 3 = 5\Delta 3 = 5 + 2 \cdot 3 = 11,$$
ale
$$1\Delta(2\Delta 3) = 1\Delta(2 + 2 \cdot 3) = 1\Delta 8 = 1 + 2 \cdot 8 = 17.$$
- Zistíme, či operácia Δ má neutrálny prvok. Vzhľadom k tomu, že Δ nie je komutatívna operácia, tak musíme vyšetriť obe rovnosti:
$$a\Delta e = a \quad \wedge \quad e\Delta a = a.$$
Teda
$$a\Delta e = a \iff a + 2 \cdot e = a \iff 2 \cdot e = 0 \iff e = 0.$$
Ale
$$e\Delta a = a \iff e + 2 \cdot a = a \iff e = -a.$$
V prvom prípade sme dostali jeden výsledok $e = 0$, pre ľubovolné $a \in \mathbb{R}$, ale v druhom prípade je e závislé od a, čo by znamenalo, že každý prvok by mal svoj

vlastný neutrálny prvok (ku každému prvku by existoval iný neutrálny prvok), ale keď si pozorne prečítame definíciu, tak zistíme, že neutrálny prvok musí byť spoločný pre všetky prvky množiny, na ktorej pracujeme. Preto operácia Δ nemá neutrálny prvok.

- Vzhľadom k tomu, že operácia Δ nemá neutrálny prvok, tak nemá zmysel uvažovať o inverzných prvkoch.

Na jednoduchej úlohe si teraz vysvetlíme operácie na konečných množinách.

Príklad 6. *Nájdite všetky operácie na množine* $\{0,1\}$ *a určte ich vlastnosti.*

Riešenie. Najskôr si musíme premyslieť, koľko je takýchto operácií. Je výhodné a aj prehľadné, zapisovať výsledky operácií na konečných množinách do operačných tabuliek, tzv. Cayleyho tabuliek. Prvky danej množiny zapíšeme do záhlaví tabuľky, tak, ako sme to robili pri tabuľkách relácií. Do vnútra tabuľky zapisujeme výsledky operácie takto:

$\star$	0	1
0	$0\star 0$	$0\star 1$
1	$1\star 0$	$1\star 1$

Teraz by už nemal byť problém odpovedať na otázku, koľko takýchto operácií existuje. Počet je taký, ako počet všetkých tabuliek, ak v ich vnútri sú vždy štyri hodnoty a pre každú z nich máme dve možnosti (výsledok operácie $\star$ môže byť v tejto úlohe len 0 alebo 1). Takže všetkých možností je $2^4 = 16$. My si postupne vypíšeme všetkých 16 operačných tabuliek a budeme sa venovať ich vlastnostiam. Niektoré vlastnosti sa dajú z tabuľky rýchlo vyčítať, niektoré nám dajú viac zabrať. Komutativita patrí k tým príjemnejším. Ak je operácia komutatívna, tak pre všetky prvky platí, že $a\star b = b\star a$, teda tabuľka takejto operácie je symetrická podľa diagonály prechádzajúcej znakom operácie.

$\star$	0	1
0	$0\star 0$	$0\star 1 = 1\star 0$
1	$1\star 0 = 0\star 1$	$1\star 1$

Podobne príjemné je aj hľadanie neutrálneho prvku. Z definície vieme, že ak existuje taký prvok $e \in A$, o ktorom platí

$$\forall a \in A\colon\ a\star e = e\star a = a,$$

tak e je neutrálnym prvkom danej operácie. To znamená, že v riadku, aj v stĺpci takéhoto prvku sa presne zopakuje záhlavie tabuľky. Nech je napr. v našom prípade 0 neutrálnym prvkom, potom tabuľka bude takáto:

$\star$	0	1
0	0	1
1	1	...

,

pričom $1\star 1 \in \{0,1\}$. Ak bude neutrálnym prvkom 1, potom tabuľka bude takáto:

$\star$	0	1
0	...	0
1	0	1

,

pričom $0\star 0 \in \{0,1\}$.

Ak k prvku a existuje inverzný prvok a', tak potom je

$$a\star a' = a'\star a = e,$$

pričom e je neutrálny prvok. Teda ak a a a' sú k sebe inverzné, tak prvok e je ako výsledok umiestnený symetricky v tabuľke na miestach $a \star a', a' \star a$. Napr. v nasledujúcej tabuľke je 0 neutrálny prvok a 1 je sama k sebe inverzná. V tabuľke

$\star$	0	1
0	0	1
1	1	0

je neutralita prvku 0 zrejmá z prvého riadku a stĺpca, inverznosť prvku 1 k sebe samému je vyznačená červenou. Má prvok 0 inverzný prvok? Pre lepšiu názornosť to ešte ukážeme na množine $\{0, 1, 2, 3\}$. Nech prvok 2 je neutrálny a prvok 1 bude inverzný k prvku 3 a naopak. V tabuľke

$\star$	0	1	2	3
0	.	.	0	.
1	.	.	1	2
2	0	1	2	3
3	.	2	3	.

je neutralita vyznačená modrou, inverznosť červenou. Ako je to s inverzným prvkom k neutrálnemu prvku?

Ak operácia nemá neutrálny prvok, nemôže mať ani inverzné prvky. Koľko môže mať operácia neutrálnych prvkov? Koľko môže mať prvok inverzných prvkov?

Asociativita bude problematická, bude treba vyskúšať všetky možné trojice, čo v našom prípade (pri dvojprvkovej množine) je len 8 trojíc, pri viacprvkových množinách ten počet prudko rastie. Koľko je všetkých trojíc napr. pri trojprvkovej množine?

Teraz postupne prejdeme všetkých 16 možných operácií:

$\star$	0	1
0	0	0
1	0	0

Je komutatívna, asociatívna (v tomto prípade je overenie obzvášť jednoduché), nemá neutrálny prvok.

$\star$	0	1
0	1	0
1	0	0

Je komutatívna, nie je asociatívna $((0 \star 1) \star 1 \neq 0 \star (1 \star 1))$, nemá neutrálny prvok.

$\star$	0	1
0	0	1
1	0	0

Nie je komutatívna, nie je asociatívna $((1 \star 1) \star 1 \neq 1 \star (1 \star 1))$, nemá neutrálny prvok.

$\star$	0	1
0	0	0
1	1	0

Nie je komutatívna, nie je asociatívna $((1 \star 1) \star 1 \neq 1 \star (1 \star 1))$, nemá neutrálny prvok.

$\star$	0	1
0	0	0
1	0	1

Je komutatívna, asociatívna (overte a využite komutativitu), má neutrálny prvok, $e = 1$, 1 je sama sebe inverzná, 0 nemá inverzný prvok.

$\star$	0	1
0	1	1
1	0	0

Nie je komutatívna, nie je asociatívna ($(0\star0)\star0 \neq 0\star(0\star0)$), nemá neutrálny prvok.

$\star$	0	1
0	1	0
1	1	0

Nie je komutatívna, nie je asociatívna ($(0\star0)\star0 \neq 0\star(0\star0)$), nemá neutrálny prvok.

$\star$	0	1
0	1	0
1	0	1

Je komutatívna, asociatívna (overte a využite komutativitu), má neutrálny prvok, $e = 1$, 1 je sama sebe inverzná a 0 je tiež sama sebe inverzný prvok.

$\star$	0	1
0	0	1
1	1	0

Je komutatívna, asociatívna (overte a využite komutativitu), má neutrálny prvok, $e = 0$ a 0 je inverzným prvkom sama sebe, 1 je inverzným prvkom sama sebe.

$\star$	0	1
0	0	1
1	0	1

Nie je komutatívna, je asociatívna (overte a skúste nájsť v tomto prípade šikovnejšie zdôvodnenie ako skúšanie všetkých možností), nemá neutrálny prvok.

$\star$	0	1
0	0	0
1	1	1

Nie je komutatívna, je asociatívna (overte a skúste nájsť v tomto prípade šikovnejšie zdôvodnenie ako skúšanie všetkých možností), nemá neutrálny prvok.

$\star$	0	1
0	1	1
1	1	0

Je komutatívna, nie je asociatívna ($(1\star0)\star0 \neq 1\star(0\star0)$), nemá neutrálny prvok.

$\star$	0	1
0	1	1
1	0	1

Nie je komutatívna, nie je asociatívna ($(0\star0)\star0 \neq 0\star(0\star0)$), nemá neutrálny prvok.

$\star$	0	1
0	1	0
1	1	1

Nie je komutatívna, nie je asociatívna ($(0\star0)\star0 \neq 0\star(0\star0)$), nemá neutrálny prvok.

$\star$	0	1
0	0	1
1	1	1

Je komutatívna, asociatívna (overte a využite komutativitu), má neutrálny prvok, $e = 0$ a 0 je sebe aj inverzným prvkom, ale 1 inverzný prvok nemá.

$\star$	0	1
0	1	1
1	1	1

Je komutatívna, asociatívna (v tomto prípade je overenie obzvášť jednoduché), nemá neutrálny prvok.

Tento príklad bol síce zdĺhavý, ale snáď prispel k lepšiemu objasneniu operácií na konečných množinách. Teraz už asi nikoho neprekvapí nasledujúce tvrdenie.

Veta 7. *Binárna operácia (na množine A) má najviac jeden neutrálny prvok.*

Dôkaz. Tvrdenie dokážeme sporom, teda budeme predpokladať, že operácia, nazvime ju $\circ$, bude mať dva rôzne neutrálne prvky e a f. Potom

$$e = e \circ f = f \circ e,$$

lebo f je neutrálny prvok. Ale aj e je neutrálny prvok, preto

$$f = f \circ e = e \circ f.$$

Potom

$$e = e \circ f = f,$$

čo je v spore s tým, že e a f sú rôzne.

Rada pre začiatočníkov: Komu ani dôkaz nepomohol pochopiť, že neutrálny prvok môže byť len jeden, možno mu pomôže ak si skúsi vyplniť operačnú tabuľku pre napr. štvorprvkovú množinu tak, aby tam vznikli dva neutrálne prvky, síce sa mu to nepodarí vyplniť, ale jednoznačnosť neutrálneho prvku mu to objasní.

Vzhľadom k tomu, že asociativita je náročnejšia, tak jej budeme venovať zvýšenú pozornosť.

Príklad 8. *Zistite, či sú nasledujúce operácie asociatívne:*

$\star_1$	0	1	2	3
0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3

$\star_2$	0	1	2	3
0	0	1	2	3
1	0	1	2	3
2	0	1	2	3
3	0	1	2	3

$\star_3$	0	1	2	3
0	0	1	2	3
1	1	2	2	2
2	2	2	2	2
3	3	2	2	2

$\star_4$	0	1	2	3
0	0	1	2	3
1	1	0	0	0
2	2	0	0	0
3	3	0	0	0

Riešenie. Postupne sa budeme venovať jednotlivým operáciám (tabuľkám):

- Všimnime si, ako funguje operácia $\star_1$. Zrejme

  $$0 \star_1 0 = 0 \star_1 1 = 0 \star_1 2 = 0 \star_1 3 = 0,$$

  $$1 \star_1 0 = 1 \star_1 1 = 1 \star_1 2 = 1 \star_1 3 = 1,$$

  a takto by sme mohli pokračovať. Výsledkom tejto operácie je vždy prvok, ktorý je vľavo, takže keby sme aj rôznym spôsobom uzátvorkovali ľubovolný počet prvkov, výsledkom by bol prvok, ktorý bude zapísaný najviac vľavo, teda umiestnenie zátvoriek nemá na výsledok vplyv, operácia $\star_1$ je asociatívna.

- Podobne funguje aj operácia $\star_2$, výsledkom tejto operácie je vždy prvok, ktorý je vpravo, teda umiestnenie zátvoriek nemá na výsledok vplyv, operácia $\star_2$ je asociatívna.

- Operácia $\star_3$ má neutrálny prvok a ak budeme kontrolovať asociatívnosť, tak trojice, v ktorých je aspoň jeden výskyt neutrálneho prvku (jeho umiestnenie v danej trojici nie je podstatné, na ukážku uvádzame jedno z možných umiestnení) asociativitu nikdy neporušujú. Lebo (e je neutrálny prvok)

  $$(e \circ a) \circ b = a \circ b \quad \wedge \quad e \circ (a \circ b) = a \circ b.$$

  Teda sa stačí zamerať len na trojice, ktoré neutrálny prvok neobsahujú. Tie ale v prípade operácie $\star_3$ dávajú vždy výsledok 2 a preto umiestnenie zátvoriek výsledok neovplyvní, operácia $\star_3$ je asociatívna.

- Operácia $\star_4$ má tiež neutrálny prvok, preto sa stačí zamerať len na trojice, ktoré neutrálny prvok neobsahujú. V tomto prípade to síce zdanlivo vyzerá rovnako ako pri operácii $\star_3$, aj v tomto prípade sú výsledky vo zvyšku tabuľky všetky rovnaké, ale tentokrát je tým výsledkom práve neutrálny prvok 0 a vďaka tomu je napr.

  $$(1 \star_4 1) \star_4 2 = 0 \star_4 2 = 2, \text{ ale } 1 \star_4 (1 \star_4 2) = 1 \star_4 0 = 1,$$

  teda umiestnenie zátvoriek výsledok ovplyvnilo, operácia $\star_4$ nie je asociatívna.

Príklad 9. *Premyslite si (bez toho, aby ste museli skúšať všetky možnosti), prečo je operácia $\star$ asociatívna:*

$\star$	0	1	2	3
0	0	1	2	3
1	1	1	2	3
2	2	2	2	3
3	3	3	3	3

Ako sme mohli v predchádzajúcich úlohách vidieť, asociativitu nevieme tak jednoducho z tabuľky vyčítať ako napr. komutativitu. Aspoň čiastočne nám v tom pomáha nasledujúce tvrdenie.

Veta 10. *Nech $\circ$ je asociatívna operácia na množine A a nech e je neutrálny prvok tejto operácie. Potom ku každému prvku $a \in A$ existuje najviac jeden inverzný prvok.*

Dôkaz. Tvrdenie dokážeme sporom, teda budeme predpokladať, že operácia, nazvime ju $\circ$, bude asociatívna, jej neutrálny prvok označíme e a bude existovať prvok, označíme ho a, ktorý bude mať dva rôzne inverzné prvky a_1, a_2. Potom z neutrality prvku e vyplýva

$$a_1 = a_1 \circ e,$$

ďalej pre inverzný prvok a_2 platí

$$a \circ a_2 = e$$

a po dosadení a uplatnení asociatívneho zákona dostávame

$$a_1 = a_1 \circ e = a_1 \circ (a \circ a_2) = (a_1 \circ a) \circ a_2 = e \circ a_2 = a_2.$$

Čo je v spore s tým, že a_1 a a_2 sú rôzne.

Toto tvrdenie treba správne pochopiť. Je dôležité si všimnúť, že sa jedná o implikáciu a nie o ekvivalenciu. Teda, ak nejaká operácia má pre každý prvok maximálne jeden inverzný prvok, tak to ešte neznamená, že je nutne asociatívna. Naopak, stačí, ak aspoň jeden prvok má viac ako jeden inverzný prvok, asociativita je porušená. Toto sme mohli vidieť pri operácii $\star_4$. Pre lepšie pochopenie uvádzam nasledujúci príklad.

Príklad 11. *Nájdite operáciu na množine* $\{0,1,2,3\}$*, ktorá má neutrálny prvok, ku každému prvku má najviac jeden inverzný prvok a nie je asociatívna.*

Riešenie. Vzhľadom k tomu, že hľadáme operáciu na konečnej množine, budeme hľadať jej operačnú tabuľku. Najskôr vyplníme riadok a stĺpec pre neutrálny prvok. My sme zvolili $e = 0$, ale rovnako úspešní by sme boli aj pri inej voľbe.

$\star$	0	1	2	3
0	0	1	2	3
1	1	.	.	.
2	2	.	.	.
3	3	.	.	.

V ďalšom kroku budeme „kaziť“ asociativitu, ale tak, aby sme k žiadnemu prvku nevyrobili viac ako jeden inverzný prvok. Takže si vyberieme trojicu, ktorá pokazí asociativitu, napr. chceme, aby

$$(1 \star 1) \star 2 \neq 1 \star (1 \star 2).$$

Aby sme nevyrobili „veľa“ inverzných prvkov, stačí ak nebudeme 0 používať ako výsledok vo voľných políčkach tabuľky (toto si premyslite). Teraz sa budeme venovať výsledku na ľavej strane nerovnosti. Ak zvolíme napr. $(1 \star 1) = 2$, tak po dosadení zistíme, že ešte musíme určiť $2 \star 2$. Teda

$$(1 \star 1) \star 2 = 2 \star 2.$$

Môžeme zvoliť napr. $2 \star 2 = 3$, potom bude

$$(1 \star 1) \star 2 = 2 \star 2 = 3.$$

Tieto výsledky zapíšeme do tabuľky

$\star$	0	1	2	3
0	0	1	2	3
1	1	2	.	.
2	2	.	3	.
3	3	.	.	.

Mohli sme výsledok $1 \star 1$ zvoliť ľubovolný? Ako by to dopadlo, keby sme to určili takto $1 \star 1 = 1$? Teraz budeme určovať výsledky na pravej strane. Najskôr potrebujeme určiť výsledok $1 \star 2$. Tento výsledok v tabuľke ešte nemáme, dokonca ho môžeme zvoliť ľubovolne a vždy by sme ešte boli schopní asociativitu pokaziť a zároveň nevyrobiť veľa inverzných prvkov. Rozoberieme všetky možnosti:

- ak $1 \star 2 = 0$, potom pre pravú stranu máme $1 \star (1 \star 2) = 1 \star 0 = 1 \neq 3$. (asociativitu sme pokazili, a žiaden inverzný prvok sme nevyrobili, napriek tomu, že $1 \star 2 = 0$.)
- ak $1 \star 2 = 1$, potom pre pravú stranu máme $1 \star (1 \star 2) = 1 \star 1 = 2 \neq 3$. (asociativitu sme pokazili, a žiaden inverzný prvok sme nevyrobili.)
- ak $1 \star 2 = 2$, potom pre pravú stranu máme $1 \star (1 \star 2) = 1 \star 2 = 2 \neq 3$. (asociativitu sme pokazili, a žiaden inverzný prvok sme nevyrobili.)
- ak $1 \star 2 = 3$, potom pre pravú stranu máme $1 \star (1 \star 2) = 1 \star 3$. Teraz stačí dať $1 \star 3 \neq 3$ a opäť bude asociativita pokazená, a žiaden inverzný prvok nevyrobíme.

Vidíme, že úloha má viac riešení, jedno z nich je v tabuľke:

$\star$	0	1	2	3
0	0	1	2	3
1	1	2	1	3
2	2	3	3	3
3	3	3	3	3

Čiernou farbou je vyznačený riadok a stĺpec neutrálneho prvku, červenou sme vyznačili výsledky ľavej strany, modrou výsledky pravej strany a zelené výsledky už môžu byť takmer ľubovolné. Premyslite si, aké môžu, resp. nemôžu byť tie zelené výsledky, aby sme úlohu splnili.

Veľmi pekným riešením tejto úlohy je nasledujúca operácia na množine $\{0, 1, 2, 3\}$.

$\star$	0	1	2	3
0	0	1	2	3
1	1	0	3	3
2	2	3	0	3
3	3	3	3	0

Neutrálny prvok je 0, každý prvok je sám sebe inverzný a operácia nie je asociatívna, lebo napr. $2\star(3\star3) \neq (2\star3)\star3$. Navyše, toto riešenie sa dá zovšeobecniť pre n– prvkovú množinu nasledovne. Najmenší prvok bude neutrálny, každý prvok bude sám sebe inverzný (teda na diagonále bude v každom políčku neutrálny prvok) a zvyšok tabuľky vyplníme najväčším prvkom.

2 Algebry s jednou operáciou

2.1 Grupoidy a podgrupoidy

V tejto kapitole sa budeme venovať rôznym matematickým štruktúram s jednou operáciou, všeobecne sa nazývajú algebry. Prvou z nich budú grupoidy.

Definícia 12. *Usporiadanú dvojicu $(G, \circ)$, kde G je neprázdna množina a $\circ$ je binárna operácia na množine G, nazývame* **grupoidom.** *Množinu G nazývame nosičom a operáciu $\circ$ operáciou grupoidu.*

Grupoid je teda štruktúra s jednou operáciou, napr. $\circ$, pričom od danej operácie neočakávame žiadne špeciálne vlastnosti, okrem uzavretosti na svojom nosiči G, teda

$$\forall a, b \in G \colon a \circ b \in G.$$

Napríklad $(\mathbb{N}, +)$ je grupoid, ale $(\mathbb{N}, -)$ nie je grupoid. Pokiaľ existuje taká podmnožina nosiča G, že operácia $\circ$ je na nej uzavretá, dostaneme podštruktúru grupoidu G.

Definícia 13. *Hovoríme, že grupoid $(H, \circ)$ je* **podgrupoidom** *grupoidu $(G, \circ)$, ak platí:*

- $H \subseteq G$,
- $\forall a, b \in H \colon a \circ b \in H$.

Poznámka 14. *Zrejme H je neprázdna množina, lebo $(H, \circ)$ musí byť grupoid. Ďalej, každý grupoid je svojim podgrupoidom.*

Na ozrejmenie tohto pojmu nám poslúži jednoduchá úloha.

Príklad 15. *Nech $M = \{0, 1, 2\}$. Určte tabuľkou operáciu $\circ$ tak, aby grupoid $(M, \circ)$ mal*

- *práve 1 podgrupoid,*
- *práve 2 podgrupoidy,*
- *práve 3 podgrupoidy.*

Riešenie. Postupne vyriešime jednotlivé podúlohy.

- **Práve 1 podgrupoid**
  Zrejme sa jedná o prípad, keď jediným podgrupoidom bude práve $(M, \circ)$. Teda musíme „pokaziť“ všetky jednoprvkové a dvojprvkové podgrupoidy. To znamená, že $0 \circ 0 \neq 0, 1 \circ 1 \neq 1, 2 \circ 2 \neq 2$. Týmto sme zabránili jednoprvkovým podgrupoidom. Podobne musíme zabrániť aj dvojprvkovým. Napr. ak nechceme aby $(\{0, 1\}, \circ)$ bol podgrupoid, tak aspoň jeden z výsledov $0 \circ 0, 0 \circ 1, 1 \circ 0, 1 \circ 1$ musí nadobudnúť hodnotu 2. Koľko môže byť všetkých dvojprvkových podgrupoidov? Okrem $(\{0, 1\}, \circ)$ sú ešte dva: $(\{0, 2\}, \circ)$ a $(\{1, 2\}, \circ)$. Aj tieto dva potrebujeme „pokaziť“. Prvý z nich pokazíme napr. tak, že bude $0 \star 2 = 1 \notin \{0, 2\}$. V druhom prípade stačí napr. $2 \star 2 = 0 \notin \{1, 2\}$. Potom jeden z možných grupoidov je:

$\circ$	0	1	2
0	1	0	1
1	0	2	1
2	1	1	0

Vo všeobenosti, ak chceme skonštruovať grupoid s jediným podgrupoidom, tak stačí vhodne vyplniť diagonálu. Vhodne v tomto prípade znamená, že do prvého riadku na diagonále dáme druhý prvok (poradie prvkov máme určné záhlavím), do druhého riadku na diagonálu dáme tretí prvok, teda do n. riadku dáme $(n+1)$. prvok a do posledného riadku dáme na diagonálu prvý prvok.

- **Práve 2 podgrupoidy**
  Zrejme okrem podgrupoidu $(M, \circ)$, musí mať aj nejaký ďalší podgrupoid. Napr. $(\{0\}, \circ)$. Teda všetky ostatné jednoprvkové a dvojprvkové podgrupoidy musíme „pokaziť“. Potom jedna z možností je:

$\circ$	0	1	2
0	0	1	2
1	0	2	0
2	2	2	1

- **Práve 3 podgrupoidy**
  Okrem podgrupoidu $(M, \circ)$, musí mať ďalšie dva. Tu ale nemôžeme vybrať ľubovolné dva podgrupoidy. Ak by sme zvolili napr. $(\{1,2\}, \circ)$ a $(\{0,2\}, \circ)$, tak zistíme, že to nie je možné zariadiť. Totiž, v takomto prípade by sme museli „pokaziť“ všetky jednoprvkové podgrupoidy a aby sme nestratili podgrupoid $(\{1,2\}, \circ)$, museli by sme položiť $1 \circ 1 = 2$ a $2 \circ 2 = 1$. Týmto sme však už „pokazili“ podgrupoid $(\{0,2\}, \circ)$. Premyslite si to. Aby nám nevznikali takéto problémy, je najjednoduchšie voliť jednoprvkové podgrupoidy. Vyskúšajte si to. Ďalšia vhodná voľba môžu byť podgrupoidy $(\{1,2\}, \circ)$ a $(\{1\}, \circ)$. V tomto prípade je riešením napr.:

$\circ$	0	1	2
0	1	2	2
1	2	1	2
2	0	2	1

2.2 Grupy

Pri grupoidoch sme od operácie požadovali len uzavretosť, teraz sa budeme venovať algebrám, ktorých operácie majú rôzne pekné vlastnosti.

Definícia 16. *Usporiadanú dvojicu $(G, \circ)$, kde G je neprázdna množina a $\circ$ je asociatívna operácia na množine G, nazývame* **pologrupou.** *Množinu G nazývame nosičom a operáciu $\circ$ operáciou pologrupy.*

Príklad 17. *Príkladom pologrupy je $\big((0,1),\cdot\big)$, pričom $\cdot$ je klasické násobenie. Treba si uvedomiť, že ak $x, y \in (0,1)$, tak aj súčin $x \cdot y \in (0,1)$ a klasické násobenie je asociatívna (aj komutatívna) operácia, teda spĺňa všetky požiadavky z predchádzajúcej definície, je to pologrupa, dokonca komutatína pologrupa. Dopadlo by to rovnako aj v prípade $\big((0,1),+\big)$? Odpoveď je záporná, totiž $\big((0,1),+\big)$ nie je ani grupoid.*

Definícia 18. *Pologrupa s neutrálnym prvkom sa nazýva* **monoid**.

Príklad 19. *Ak v predchádzajúcom príklade trochu zmeníme nosič, tak dostaneme monoid. Zrejme $\big((0,1\rangle,\cdot\big)$ je grupoid (teda operácia $\cdot$ je na danom nosiči uzavretá), navyše operácia $\cdot$ je asociatívna a 1 je jej neutrálnym prvkom. Teda naozaj je $\big((0,1\rangle,\cdot\big)$ monoid, dokonca komutatívny monoid. Ktoré prvky z $(0,1\rangle$ majú inverzné prvky, vzhľadom na operáciu $\cdot$?*

Definícia 20. *Monoid, v ktorom ku každému prvku existuje inverzný prvok, sa nazýva* **grupa**. *Grupa s komutatívnou operáciou sa nazýva* **komutatívna** *alebo* **Abelova grupa**.

Poznámka 21. *Zrejme $\big((0,1\rangle,\cdot\big)$, z predchádzajúceho príkladu, nie je grupa, lebo napr. $\frac{1}{2}$ nemá inverzný prvok.*

Poznámka 22. *Premyslite si, aké vlastnosti má algebra $(\langle 0,1\rangle,\cdot)$.*

Príklad 23. *Nech $A = \mathbb{Z}$ a operácia $\circ$ je daná takto: $a \circ b = a + b - 2$. Zistite, či $(A, \circ)$ je grupa.*

Riešenie. Musíme dokázať, že operácia $\circ$ je uzavretá na A, je asociatívna, má neutrálny prvok a ku každému celému číslu existuje inverzný prvok.

- Uzavretosť: Ak $a, b \in \mathbb{Z}$, potom aj $a \circ b = a + b - 2 \in \mathbb{Z}$, teda $\circ$ je uzavretá na $\mathbb{Z}$.
- Asociatívnosť: Nech $a, b, c \in A$, potom:

$$(a \circ b) \circ c = (a + b - 2) \circ c = (a + b - 2) + c - 2 = a + b + c - 4,$$

$$a(\circ b \circ c) = a \circ (b + c - 2) = a + (b + c - 2) - 2 = a + b + c - 4.$$

  Teda $(a \circ b) \circ c = a(\circ b \circ c)$
- Neutrálny prvok: Má platiť $a \circ e = e \circ a = a$, teda

$$a \circ e = a + e - 2 = a \Rightarrow e = 2 \wedge 2 \in \mathbb{Z},$$

$$e \circ a = e + a - 2 = a \Rightarrow e = 2 \wedge 2 \in \mathbb{Z}.$$

  V oboch prípadoch nám vyšiel ten istý neutrálny prvok, teda operácia má neutrálny prvok $e = 2$.

- Inverzné prvky: Nech $a \in A$, potom má platiť $a \circ a' = a' \circ a = e$, teda

$$a \circ a' = 2 \Rightarrow a + a' - 2 = 2 \Rightarrow a' = 4 - a \in \mathbb{Z},$$

a rovnako to dopadne aj v druhom prípade:

$$a' \circ a = 2 \Rightarrow a' + a - 2 = 2 \Rightarrow a' = 4 - a \in \mathbb{Z}.$$

Teda $(A, \circ)$ je grupa. Dokonca je Abelova (komutatívna). Komutatívnosť sme neoverovali a dokonca sme ju ani nevyužili pri hľadaní neutrálneho prvku, či inverzných prvkov. Môžete skúsiť tento dôkaz vylepšiť aplikáciou komutativity. Inšpirovať sa môžete v príklade 5. v časti 1.

Príklad 24. *Pre pekný príklad na konečnú grupu sa vrátime k reláciám ekvivalencie. Ak je na množine $\mathbb{Z}$ daná relácia $\equiv$ nasledovne:*

$$a \equiv b \iff 3|(a-b),$$

tak už vieme, že $\equiv$ je relácia ekvivalencie na $\mathbb{Z}$ a faktorová množina je $\mathbb{Z}/_{\equiv} = \{\overline{0}, \overline{1}, \overline{2}\}$. Túto množinu značíme $\mathbb{Z}_3$ a nazývame ju množina zvyškových tried po delení tromi. Na tejto množine zavedieme operáciu $\oplus_3$ takto:

$\oplus_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Ako vlastne počítame? Ak chceme napr. určiť $1 \oplus_3 1$, tak vykonáme klasické sčítanie a teda dostaneme $1 + 1 = 2$, keďže 2 dáva po delení tromi zvyšok dva, zapíšeme to do príslušného políčka tabuľky. Ďalej napr. $2 \oplus_3 2 = 1$, lebo $2 + 2 = 4$ a 4 dáva po delení tromi zvyšok 1. Z tabuľky vidíme, že $\oplus$ je uzavretá na svojom nosiči, ďalej 0 je neutrálny prvok a ku každému prvku existuje inverzný prvok. Asociativita vyplýva z asociativity klasického sčítania. Veľmi podobne by sme mohli zaviesť operáciu $\odot_3$.

$\odot_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Teda znovu násobíme klasicky a ako výsledok berieme zvyšok po delení tromi. Zrejme $(\mathbb{Z}_3, \odot_3)$ je grupoid. Vzhľadom k tomu, že vychádzame z klasického násobenia, tak je $\odot_3$ asociatívna operácia, teda $(\mathbb{Z}_3, \odot_3)$ je pologrupa. Z tabuľky vieme ďalej zistiť, že 1 je neutrálny prvok. Teda $(\mathbb{Z}_3, \odot_3)$ je monoid, ale keďže k 0 neexistuje inverzný prvok, tak to nie je grupa. Keby sme však nosič upravili na $\mathbb{Z}_3 \setminus \{0\}$, tak by sme grupu dostali. Keby sme pracovali na $\mathbb{Z}_4$, tak pre operáciu $\oplus_4$ by sme dostali rovnaký výsledok, ako pri $\mathbb{Z}_3$. Ako to bude s operáciou $\odot_4$? Pomôžeme si tabuľkou.

$\odot_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Znovu sme dostali komutatívny monoid, ale v tomto prípade nedostaneme grupu, ak budeme ako nový nosič uvažovať $\mathbb{Z}_4 \setminus \{0\}$. Prečo to pri $\mathbb{Z}_3$ fungovalo a pri $\mathbb{Z}_4$ už nefunguje? Problém je v

tom, že 3 je prvočíslo a teda mimo "nulového"riadku a stĺpca sa 0 ako výsledok nevyskytuje, po vynechaní nulového riadku a stĺpca, dostaneme grupoid (s dobrými vlastnosťami).

Zhrnutie. *Nech $n \in \mathbb{N}$, potom $(\mathbb{Z}_n, \oplus)$ je komutatívna grupa. Nech p je prvočíslo, potom $(\mathbb{Z}_p \setminus \{0\}, \odot)$ je komutatívna grupa.*

Príklad 25. *Pekným príkladom nekomutatívnej grupy, je grupa permutácií trojprvkovej množiny s operáciou skladania. Najskôr si musíme určiť nosič tejto štruktúry. Teda si vypíšeme všetky permutácie trojprvkovej množiny, napr. $\{1,2,3\}$:*

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Na jednotlivé permutácie sa môžeme dívať ako na zobrazenia, napr. $f_1 = \{[1,1],[2,2],[3,3]\}, f_2 = \{[1,1],[2,3],[3,2]\} \dots f_6 = \{[1,3],[2,2],[3,1]\}$. Potom nosič tejto algebry je $\{f_1, f_2, \dots, f_6\}$. Permutácie budeme skladať tak, ako zvyčajne skladáme zobrazenia. Ako skladáme? Napr. $f_2 \circ f_4$ dostaneme takto: V zobrazení f_4 je obraz 1 číslo 2 a číslo 2 v zobrazení f_2 má obraz číslo 3. Teda obraz čísla 1 v zobrazení $f_2 \circ f_4$ je číslo 3. Podobne dostaneme obraz čísla 2: obraz 2 v f_4 je číslo 3 a číslo 3 má v f_2 obraz číslo 2, teda $(f_2 \circ f_4)(2) = 2$. Teraz už ani nemusíme zisťovať obraz čísla 3, ten je už určený jednoznačne a je to $(f_2 \circ f_4)(3) = 1$. Teraz vyplníme operačnú tabuľku.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

Zrejme $(\{f_1, f_2, \dots, f_6\}, \circ)$ je grupoid (z tabuľky vidíme uzavretosť), f_1 je neutrálny prvok, ku každému prvku existuje inverzný prvok. Ako je to s asociatívnosťou? Nie, nebudeme skúšať všetky možné trojice. Využijeme to, čo sme sa naučili pri reláciách, odkiaľ vieme, že skladanie relácií je asociatívne a že každé zobrazenie je relácia. Teda $(\{f_1, f_2, \dots, f_6\}, \circ)$ je nekomutatívna grupa.

Možno ste si už všimli v operačných tabuľkách, že grupy sú podobné ako sudoku, v každom riadku a stĺpci sa každý prvok vyskytuje práve raz. V grupách totiž platí zákon o krátení (pravý aj ľavý).

Veta 26. *Nech $(G, \circ)$ je grupa. Potom pre ľubolné $a, b, c \in G$ platí*

$$a \circ c = b \circ c \quad \Rightarrow \quad a = b$$

a

$$c \circ a = c \circ b \quad \Rightarrow \quad a = b.$$

Premyslite si, ktoré vlastnosti grupy sú nutné, aby zákon o krátení (pravý aj ľavý) platil.

2.3 Podgrupy

Podobne ako sme pri grupoidoch skúmali ich podgrupoidy, tak sa budeme venovať aj podštruktúram grúp.

Definícia 27. *Ak H je podgrupoid grupy G grupou, nazývame ho* **podgrupou** *grupy G.*

Poznámka 28. *Predchádzajúcu definíciu treba chápať tak, že operácia grupy G je uzavretá na množine H a pre každý prvok z množiny H platí, že do H patrí aj jeho inverzný prvok (vzhľadom na operáciu grupy G).*

Na ozrejmenie problematiky uvádzame niekoľko úloh na podgrupy konečných grúp.

Príklad 29. *Nájdite všetky podgrupy grupy $(\mathbb{Z}_4, \oplus_4)$:*

$\oplus_4$	*0*	*1*	*2*	*3*
0	*0*	*1*	*2*	*3*
1	*1*	*2*	*3*	*0*
2	*2*	*3*	*0*	*1*
3	*3*	*0*	*1*	*2*

Riešenie. Využijeme poznatky o podgrupoidoch, zrejme grupa $(\mathbb{Z}_4, \oplus_4)$ má tieto podgrupoidy: $(\{0\}, \oplus_4), (\{0, 2\}, \oplus_4), (\{0, 1, 2, 3\}, \oplus_4)$. Posledný z nich je určite grupa, lebo je totožný so $(\mathbb{Z}_4, \oplus_4)$. Ďalej, $(\{0\}, \oplus_4)$ je tiež grupa, lebo má jediný prvok, ktorý je neutrálny a zároveň sám sebe inverzný. Podgrupoid $(\{0, 2\}, \oplus_4)$ je tiež grupa, prvok 0 je neutrálny a prvok 2 je sám sebe inverzný, asociatívnosť nie je treba overovať (prečo?). Teda všetky tri podgrupoidy sú podgrupami.

Príklad 30. *Nájdite všetky podgrupy grupy $(\mathbb{Z}_3, \oplus_3)$:*

$\oplus_3$	*0*	*1*	*2*
0	*0*	*1*	*2*
1	*1*	*2*	*0*
2	*2*	*0*	*1*

Riešenie. Grupa $(\mathbb{Z}_3, \oplus_3)$ má tieto podgrupoidy: $(\{0\}, \oplus_3), (\{0, 1, 2\}, \oplus_3)$. Všetky tieto podgrupoidy sú podgrupami (zdôvodnenie je podobné ako v predchádzajúcom príklade).

Príklad 31. *Nájdite všetky podgrupy grupy permutácií trojprvkovej množiny.*

Riešenie. Táto grupa má tieto podgrupoidy:

$$(\{f_1\}, \circ), (\{f_1, f_2\}, \circ), (\{f_1, f_3\}, \circ), (\{f_1, f_6\}, \circ), (\{f_1, f_4, f_5\}, \circ), (\{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ).$$

Všetky tieto podgrupoidy sú podgrupami. Možno si pozorný čitateľ už všimol, že v našich úlohách majú vždy podgrupy taký počet prvkov, ktorý je deliteľom počtu prvkov grupy. Toto nie je náhoda a funguje to pre ľubovolné grupy a ich podgrupy.

Veta 32. *(Lagrangeova veta) Počet prvkov podgrupy je deliteľom počtu prvkov grupy.*

Poznámka 33. *Ako môžeme takúto informáciu využiť? Napríklad, ak máme trinásťprvkovú grupu, tak vieme, že jej podgrupy sú len jednoprvkové a trinásťprvkové, teda iné podgrupoidy nemusíme skúmať.*

Doteraz sme sa venovali len podgrupám konečných grúp. Ako hľadať podgrupy grupy s nekonečným nosičom nám ukazuje nasledujúce tvrdenie. Toto tvrdenie samozrejme platí aj pre konečné grupy.

Veta 34. *Nech H je neprázdna podmnožina množiny G. $(H, \circ)$ je podgrupou grupy $(G, \circ)$ vtedy a len vtedy, keď platí:*

$$\forall a, b \in H \colon a \circ b^{-1} \in H,$$

pričom b^{-1} je inverzný prvok k prvku b.

Príklad 35. *Daná je grupa $(\mathbb{Z}, +)$ a množina $H = \{3 \cdot x; x \in \mathbb{Z}\}$. Dokážte, že $(H, +)$ je podgrupa grupy $(\mathbb{Z}, +)$.*

Riešenie. Stačí dokázať, že pre ľubovoľné $a, b \in H$ je

$$a + b^{-1} \in H.$$

Nech $a, b \in H$. Potom

$$\exists p, q \in \mathbb{Z} \colon a = 3p, b = 3q, b^{-1} = -3q.$$

Vypočítame

$$a + b^{-1} = 3p + (-3q) = 3(p - q).$$

Zrejme $p - q \in \mathbb{Z}$ a preto $3(p - q) \in H$, teda $(H, +)$ je podgrupou $(\mathbb{Z}, +)$.

Pomocou podgrupy vieme nasledujúcim spôsobom urobiť rozklad nosiča grupy.

Definícia 36. *(Rozklady podľa podgrupy:)*

- **Ľavý rozklad** *grupy G podľa podgrupy H je množina*

  $$\{aH \colon a \in G\},$$

  kde množiny $aH = \{a \cdot h \colon h \in H\}$ sa nazývajú **ľavé triedy** *rozkladu.*

- **Pravý rozklad** *grupy G podľa podgrupy H je množina*

  $$\{Ha \colon a \in G\}$$

  kde množiny $Ha = \{h \cdot a \colon h \in H\}$ sa nazývajú **pravé triedy** *rozkladu.*

Príklad 37. *Určte ľavý a pravý rozklad grupy $(\mathbb{Z}_4, \oplus_4)$ podľa podgrupy $(\{0, 2\}, \oplus_4)$.*

Riešenie. Budeme postupovať podľa definície, teda triedy ľavého rozkladu sú

$$0 \oplus_4 \{0, 2\} = \{0 \oplus_4 0, 0 \oplus_4 2\} = \{0, 2\},$$

$$1 \oplus_4 \{0, 2\} = \{1 \oplus_4 0, 1 \oplus_4 2\} = \{1, 3\},$$

$$2 \oplus_4 \{0, 2\} = \{2 \oplus_4 0, 2 \oplus_4 2\} = \{2, 0\},$$

$$3 \oplus_4 \{0, 2\} = \{3 \oplus_4 0, 3 \oplus_4 2\} = \{3, 1\}.$$

Podobne určíme aj triedy pravého rozkladu

$$\{0, 2\} \oplus_4 0 = \{0 \oplus_4 0, 2 \oplus_4 0\} = \{0, 2\},$$

$$\{0,2\} \oplus_4 1 = \{0 \oplus_4 1, 2 \oplus_4 1\} = \{1,3\},$$
$$\{0,2\} \oplus_4 2 = \{0 \oplus_4 2, 2 \oplus_4 2\} = \{2,0\},$$
$$\{0,2\} \oplus_4 3 = \{0 \oplus_4 3, 2 \oplus_4 3\} = \{3,1\}.$$

A teda ľavý aj pravý rozklad je $\{\{0,2\},\{1,3\}\}$. Vo všeobecnosti sa tieto rozklady rovnať nemusia, čo uvidíme v ďalšom príklade. Najskôr sa však pozrieme, čo nám takéto rozklady o podgrupe prezradia.

Definícia 38. *Podgrupa $(H,\circ)$ grupy $(G,\circ)$ sa nazýva* **normálna podgrupa,** *ak pre ľubovolné $a \in G, h \in H$ platí: $a \circ h \circ a^{-1} \in H$.*

To, či je podgrupa normálna, vieme zistiť aj pomocou ľavého a pravého rozkladu podľa danej podgrupy.

Veta 39. *Ak je ľavý a pravý rozklad grupy G podľa podgrupy H rovnaký, tak H je normálna podgrupa.*

Poznámka. Každá podgrupa komutatívnej grupy je normálna. Podgrupy nekomutatívnych grúp nemusia byť normálne.

Príklad 40. *Ukážte, že podgrupa $(\{f_1,f_2\},\circ)$ grupy všetkých permutácií trojprvkovej množiny nie je normálna.*

Riešenie.

- Zrejme $f_3^{-1} = f_3$ a teda $f_3 \circ f_2 \circ f_3^{-1} = f_3 \circ f_2 \circ f_3 = f_4 \circ f_3 = f_6 \notin \{f_1,f_2\}$, čo je v spore s tým, že by $(\{f_1,f_2\},\circ)$ mohla byť normálna podgrupa.
- To, že $(\{f_1,f_2\},\circ)$ nie je normálna grupa, sa dá ukázať aj tak, že porovnáme pravý a ľavý rozklad grupy podľa tejto podgrupy. Určíme triedy ľavého rozkladu podľa tejto podgrupy

$$f_1 \circ \{f_1,f_2\} = \{f_1 \circ f_1, f_1 \circ f_2\} = \{f_1,f_2\},$$
$$f_2 \circ \{f_1,f_2\} = \{f_2 \circ f_1, f_2 \circ f_2\} = \{f_2,f_1\},$$
$$f_3 \circ \{f_1,f_2\} = \{f_3 \circ f_1, f_3 \circ f_2\} = \{f_3,f_4\},$$
$$f_4 \circ \{f_1,f_2\} = \{f_4 \circ f_1, f_4 \circ f_2\} = \{f_4,f_3\},$$
$$f_5 \circ \{f_1,f_2\} = \{f_5 \circ f_1, f_5 \circ f_2\} = \{f_5,f_6\},$$
$$f_6 \circ \{f_1,f_2\} = \{f_6 \circ f_1, f_6 \circ f_2\} = \{f_6,f_5\}.$$

  Teda ľavý rozklad je $\{\{f_1,f_2\},\{f_3,f_4\},\{f_5,f_6\}\}$.
- A pravé triedy rozkladu dostaneme takto

$$\{f_1,f_2\} \circ f_1 = \{f_1 \circ f_1, f_2 \circ f_1\} = \{f_1,f_2\},$$
$$\{f_1,f_2\} \circ f_2 = \{f_1 \circ f_2, f_2 \circ f_2\} = \{f_2,f_1\},$$
$$\{f_1,f_2\} \circ f_3 = \{f_1 \circ f_3, f_2 \circ f_3\} = \{f_3,f_5\},$$
$$\{f_1,f_2\} \circ f_4 = \{f_1 \circ f_4, f_2 \circ f_4\} = \{f_4,f_6\},$$
$$\{f_1,f_2\} \circ f_5 = \{f_1 \circ f_5, f_2 \circ f_5\} = \{f_5,f_3\},$$
$$\{f_1,f_2\} \circ f_6 = \{f_1 \circ f_6, f_2 \circ f_6\} = \{f_6,f_4\}.$$

  Pravý rozklad je $\{\{f_1,f_2\},\{f_3,f_5\},\{f_4,f_6\}\}$, teda je iný ako ľavý, čo poukazuje na to, že sa nejedná o normálnu podgrupu.

3 Homomorfizmy

V tejto kapitole sa budeme venovať vzťahom medzi rôznymi algebraickými štruktúrami. Budeme skúmať, či sú rôzne, alebo v istom slova zmysle rovnaké. Keď si všimneme nasledujúce dve štruktúry, zadané tabuľkami

$\star$	0	1
0	0	1
1	1	0

$\circ$	a	b
a	a	b
b	b	a

tak bez dlhšieho skúmania zistíme, že stačí v prvej tabuľke 0 prepísať na a, 1 na b a z prvej štruktúry by sme dostali druhú. Teda by sme mohli vziať zobrazenie $f\colon \{0,1\} \to \{a,b\}$, pričom by platilo, že $f(0) = a, f(1) = b$. Toto zobrazenie je bijekcia (medzi nosičmi uvedených štruktúr) a jeho aplikovaním sa daná štruktúra v podstate nezmení. Samozrejme, nie vždy vieme takéto zobrazenie nájsť tak ľahko a rýchlo, niekedy sa to dokonca ani nedá.

Definícia 41. *Nech $(A,\star),(B,\circ)$ sú algebry rovnakého typu. Nech $h\colon A \to B$ je také zobrazenie, že pre ľubovolné $a,b \in A$ platí*

$$h(a \star b) = h(a) \circ h(b),$$

tak h sa nazýva **homomorfizmus** *algebry A do algebry B.*

- *Ak h je injektívny homomorfizmus, hovoríme, že h je* **monomorfizmus**.
- *Ak h je surjektívny homomorfizmus, hovoríme, že h je* **epimorfizmus**.
- *Ak h je bijektívny homomorfizmus, hovoríme, že h je* **izomorfizmus**.
- *Ak h je homomorfizmus algebry A do A, hovoríme, že h je* **endomorfizmus**.
- *Ak h je izomorfizmus A na A, hovoríme, že h je* **automorfizmus**.

V nasledujúcich úlohách sa budeme venovať izomorfizmom na algebrách s konečnými nosičmi.

Príklad 42. *Nájdite izomorfizmus (ak existuje) medzi grupoidmi danými tabuľkami:*

$\star$	*0*	*1*
0	*0*	*0*
1	*0*	*0*

$\circ$	*0*	*1*
0	*1*	*1*
1	*1*	*1*

Riešenie. V tomto prípade nájdeme izomorfizmus rýchlo, lebo operácia $\star$ priradí každej dvojici z $\{0,1\}$ hodnotu 0, naopak operácia $\circ$ priradí každej dvojici hodnotu 1. Teda $h(x) = 1 - x$ je izomorfizmus medzi nimi, lebo

$$h(a \star b) = h(0) = 1 - 0 = 1.$$

A podobne

$$h(a) \circ h(b) = (1-a) \circ (1-b) = 1.$$

Príklad 43. *Ukážte, že medzi grupoidmi danými nasledujúcimi tabuľkami*

$\star$	*0*	*1*
0	*0*	*0*
1	*1*	*0*

$\circ$	*0*	*1*
0	*1*	*0*
1	*0*	*0*

nie je možné nájsť homomorfizmus.

Riešenie. Budeme predpokladať, že taký homomorfizmus existuje. Ak by sme položili $h(0) = 0$, tak

$$h(0) \circ h(0) = 0 \circ 0 = 1 \quad \wedge \quad h(0 \star 0) = h(0) = 0,$$

teda by neplatilo

$$h(0 \star 0) = h(0) \circ h(0).$$

Ak naopak položíme $h(0) = 1$, potom

$$h(0 \star 0) = h(0) = 1 \quad \wedge \quad h(0) \circ h(0) = 1 \circ 1 = 0,$$

čo zase porušuje podmienku homomorfizmu. Žiadna ďalšia možnosť pre $h(0)$ už neexistuje, teda nemôže existovať ani homomorfizmus.

Príklad 44. *V kapitole o grupách sme zistili, že ak $n \in \mathbb{N}$, tak $(\mathbb{Z}_n, \oplus_n)$ je Abelova grupa. Rovnako, ak p je prvočíslo, tak $(\mathbb{Z}_p \setminus \{0\}, \odot_p)$ je Abelova grupa. Teda ak z množiny $\mathbb{Z}_7$ vyhodíme 0 a použijeme operáciu násobenia, dostaneme Abelovu grupu a $(\mathbb{Z}_6, \oplus_6)$ je tiež Abelova grupa.*

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\odot_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Otázka znie, či sme dostali dve naozaj rôzne šesťprvkové grupy, alebo či sa dá nájsť izomorfizmus medzi $(\mathbb{Z}_7 \setminus \{0\}, \odot_7)$ a $(\mathbb{Z}_6, \oplus_6)$.

Riešenie. Odpoveďou na túto otázku je zobrazenie $f\colon \mathbb{Z}_6 \to \mathbb{Z}_7 \setminus \{0\}$ dané takto: $f(0) = 1, f(1) = 3, f(2) = 2, f(3) = 6, f(4) = 4, f(5) = 5$. Teda $(\mathbb{Z}_7 \setminus \{0\}, \odot_7)$ a $(\mathbb{Z}_6, \oplus_6)$ sú izomorfné.

Ako hľadať zobrazenie f? Treba si uvedomiť, že neutrálny prvok z prvej množiny by sa mal zobraziť na neutrálny prvok druhej množiny (teda $f(0) = 1$) a potom si treba všimnúť inverzné prvky, aby sa zachovalo to, že obraz inverzného prvku bude inverzný prvok obrazu prvku (toto si dobre premyslite). V prvej tabuľke je okrem neutrálneho prvku len prvok 3 sám sebe inverzný, v druhej tabuľke je takýmto prvkom (okrem neutrálneho) prvok 6 (teda $f(3) = 6$). Potom napr. v prvej tabuľke sú 2 a 4 navzájom inverzné a rovnako je to aj v druhej tabuľke, teda prvá voľba padla na $f(2) = 2, f(4) = 4$, zvyšok sme dourčili opäť podľa inverzných prvkov. Voľba $f(2) = 2, f(4) = 4$, však nemusela vo všeobecnosti byť úspešná, v takom prípade by sme vyskúšali iné dvojice navzájom inverzných prvkov.

Ako skontrolujeme, že sme naozaj našli izomorfizmus? To, že f je bijekcia, je zrejmé. Ešte treba skontrolovať, či je splnená vlastnosť homomorfizmu, teda, či pre ľubovolné dvojice platí

$$f(a \oplus_6 b) = f(a) \odot_7 f(b).$$

Obe operácie sú komutatívne, navyše ak $a = 0 \vee b = 0$ (teda ak aspoň jeden z prvkov je neutrálny), tak dostaneme

$$f(0 \oplus_6 b) = f(b) \quad \wedge \quad f(0) \odot_7 f(b) = 1 \odot_7 f(b) = f(b).$$

Teda stačí skontrolovať "len" všetky dvojice zo zvyšných 5 prvkov. Iná možnosť je, že aplikujeme zobrazenie f na prvú tabuľku, teda prepíšeme v nej všetky 0 na 1, 1 na 3 atď. a potom ju

porovnáme s druhou tabuľkou, či sú totožné. Po prepísaní dostaneme

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

Táto tabuľka ešte potrebuje zásah, je potrebné popresúvať riadky a stĺpce tak, aby hodnoty v záhlaviach v riadku a stĺpci boli usporiadané vzostupne. Po presune dostaneme $\big(\mathbb{Z}_7 \setminus \{0\}, \odot_7\big)$.

Nasledujúci príklad nám priblíži homomorfizmy na nekonečných množinách.

Príklad 45. *Zrejme* $(\mathbb{R}, +), (\mathbb{R}^+, \cdot)$ *sú grupy, dokonca Abelove. Potom* $h\colon \mathbb{R} \to \mathbb{R}^+, h(x) = e^x$ *je homomorfizmus medzi nimi, lebo:*

$$h(a+b) = e^{a+b} = e^a \cdot e^b = h(a) \cdot (b).$$

Keď si uvedomíme, že h *je bijekciou* $\mathbb{R}$ *na* $\mathbb{R}^+$*, tak vidíme, že sa jedná o izomorfizmus.*

Príklad 46. *Nájdite epimorfizmus (ak existuje) medzi* $\big(\mathbb{Z}_4, \oplus_4\big)$ *a* $\big(\mathbb{Z}_2, \oplus_2\big)$.

Riešenie. Našou úlohou bude teda nájsť homomorfizmus, ktorý je surjektívny. Teda budeme hľadať zobrazenie $f\colon \{0,1,2,3\} \to \{0,1\}$ tak, aby

$$f(a \oplus_4 b) = f(a) \oplus_2 f(b),$$

pričom pre všetky prvky z $\{0,1\}$ musí existovať vzor z $\{0,1,2,3\}$.
Zrejme musí byť $f(0) = 0$ alebo $f(0) = 1$, iná možnosť nemôže nastať. Budeme sa najskôr venovať prvej možnosti ($f(0) = 0$) a pozrieme sa na $f(1)$. Tu opäť platí, že $f(1) = 0$ alebo $f(1) = 1$. Takže rozoberieme postupne obe možnosti

- Nech $f(0) = 0$ a $f(1) = 0$. Teraz pomocou vlastnosti homomorfizmu budeme určovať obrazy pre ostatné prvky $\mathbb{Z}_4$. Teda, ak f je homomorfizmus, musí platiť

  $$f(1 \oplus_4 1) = f(1) \oplus_2 f(1),$$

  po dosadení je

  $$f(1 \oplus_4 1) = f(2) \quad \wedge \quad f(1) \oplus_2 f(1) = 0 \oplus_2 0 = 0,$$

  teda

  $$f(2) = 0.$$

  Podobne dostaneme aj $f(3)$, lebo

  $$f(1 \oplus_4 2) = f(1) \oplus_2 f(2),$$

  po dosadení je

  $$f(1 \oplus_4 2) = f(3) \quad \wedge \quad f(1) \oplus_2 f(2) = 0 \oplus_2 0 = 0,$$

  teda

  $$f(3) = 0.$$

  To znamená, že sme dostali zobrazenie, ktoré nie je surjektívne a preto to nie je epimorfizmus.

- Nech $f(0) = 0$ a $f(1) = 1$. Podobne ako v predchádzajúcom prípade, musí platiť

$$f(1 \oplus_4 1) = f(1) \oplus_2 f(1),$$

po dosadení je

$$f(1 \oplus_4 1) = f(2) \quad \wedge \quad f(1) \oplus_2 f(1) = 1 \oplus_2 1 = 0,$$

teda

$$f(2) = 0.$$

Podobne dostaneme aj $f(3)$, lebo

$$f(1 \oplus_4 2) = f(1) \oplus_2 f(2),$$

po dosadení je

$$f(1 \oplus_4 2) = f(3) \quad \wedge \quad f(1) \oplus_2 f(2) = 1 \oplus_2 0 = 1,$$

teda

$$f(3) = 1.$$

Toto zobrazenie je surjektívne, ešte však musíme skontrolovať, či rovnosť

$$f(a \oplus_4 b) = f(a) \oplus_2 f(b),$$

platí pre všetky dvojice z $\{0, 1, 2, 3\}$. Teraz tých dvojíc nie je veľa, navyše operácie sú komutatívne, s neutrálnymi prvkami. Teda vyberáme dvojice len z prvkov $\{1, 2, 3\}$, čo je $3 \cdot 3 = 9$ dvojíc, vďaka komutativite stačí skontrolovať len 6 dvojíc (tri dvojice sú také, že $a = b$, pre zvyšné tri platí $a \neq b$).

Ale môžeme sa na celú úlohu pozrieť aj inak. Všimnite si, že párnym číslam zobrazenie f priradilo hodnotu 0 a nepárnym 1. Teda stačí skontrolovať len ako dopadne obraz súčtu dvoch párnych, dvoch nepárnych prvkov a potom ešte obraz súčtu dvoch prvkov s opačnou paritou. Toto si dobre premyslite.

Príklad 47. *Nájdite epimorfizmus (ak existuje) medzi* $(\mathbb{Z}_3, \oplus_3)$ *a* $(\mathbb{Z}_2, \oplus_2)$.

Riešenie. Budeme predpokladať, že taký epimorfizmus existuje, teda skúsime ho nájsť. Zrejme pre $f(0)$ môžu nastať len dve možnosti (podmienky sú rovnaké ako v predchádzajúcom príklade, len namiesto $\mathbb{Z}_4$ máme teraz $\mathbb{Z}_3$) $f(0) = 0$ alebo $f(0) = 1$. Najskôr sa budeme venovať prvej možnosti, nech teda $f(0) = 0$. Potom pre $f(1)$ opäť dostaneme dve možnosti a obe ich postupne vyšetríme.

- Nech $f(0) = 0$ a $f(1) = 0$. Potom, ak f je homomorfizmus, musí platiť

$$f(1 \oplus_3 1) = f(1) \oplus_2 f(1),$$

po dosadení je

$$f(1 \oplus_3 1) = f(2) \quad \wedge \quad f(1) \oplus_2 f(1) = 0 \oplus_2 0 = 0,$$

teda

$$f(2) = 0.$$

To znamená, že sme dostali zobrazenie, ktoré nie je surjektívne a preto to nie je epimorfizmus.

- Nech $f(0) = 0$ a $f(1) = 1$. Potom

  $$f(1 \oplus_3 1) = f(1) \oplus_2 f(1),$$

  po dosadení je

  $$f(1 \oplus_3 1) = f(2) \quad \wedge \quad f(1) \oplus_2 f(1) = 0 \oplus_2 0 = 0,$$

  teda

  $$f(2) = 0.$$

  Teraz sme dostali surjektívne zobrazenie a ešte musíme skontrolovať, či rovnosť

  $$f(a \oplus_3 b) = f(a) \oplus_2 f(b),$$

  platí pre všetky dvojice z $\{0, 1, 2\}$. Teda by to malo platiť aj

  $$f(2 \oplus_3 2) = f(2) \oplus_2 f(2),$$

  ale

  $$f(2 \oplus_3 2) = f(1) = 1 \quad \wedge \quad f(2) \oplus_2 f(2) = 0 \oplus_2 0 = 0.$$

  Takže f je síce surjektívne zobrazenie, ale nie je to homomorfizmus.

- Ešte nám ostala možnosť $f(0) = 1$. Pozrime sa, čo by nám táto možnosť priniesla. Pre homomorfizmus musí platiť

  $$f(0 \oplus_3 0) = f(0) \oplus_2 f(0).$$

  Pre túto možnosť dostávame

  $$f(0 \oplus_3 0) = f(0) = 1 \quad \wedge \quad f(0) \oplus_2 f(0) = 1 \oplus_2 1 = 0,$$

  teda f nie je homomorfizmus (a preto nemôže byť ani epimorfizmus) a zároveň sme už vyčerpali všetky možnosti, teda epimorfizmus medzi $(\mathbb{Z}_3, \oplus)$ a $(\mathbb{Z}_2, \oplus)$ neexistuje.

Premyslite si, pre aké $m, n \in \mathbb{N}$ existuje epimorfizmus medzi $(\mathbb{Z}_n, \oplus_n)$ a $(\mathbb{Z}_m, \oplus_m)$. Ďalej si premyslite, či vôbec malo v predchádzajúcej úlohe zmysel skúšať možnosť $f(0) = 1$.

Predpokladám, že uvedené úlohy dostatočne objasnili podstatu hľadania izomorfizmov a epimorfizmov. Konštrukcie zvyšných typov homomorfizmov, teda monomorfizmu, endomorfizmu a automorfizmu, sú veľmi podobné.

4 Kongruencie

Už na základnej škole pri zlomkoch ste sa stretli s reláciou ekvivalencie, len ste si to neuvedomili. Zlomky $\frac{1}{2}$ a $\frac{2}{4}$ sa rovnajú (samozrejme sa rovnajú aj s mnohými ďalšími) a tak by sme mohli reláciu ekvivalencie na množine $\mathbb{Z} \times \mathbb{N}^+$ definovať tak, že dve dvojice $[m, n], [m', n']$ sú v relácii, ak sa rovnajú zlomky $\frac{m}{n}, \frac{m'}{n'}$, faktorová množina by obsahovala všetky zlomky v základnom tvare. A samozrejme, ak budeme zlomky napr. sčitovať, tak výsledok sa nezmení, ak namiesto $\frac{1}{2} + \frac{3}{4}$ sčítame $\frac{3}{6} + \frac{9}{12}$, oba výsledky budú z tej istej triedy. Podobne je to aj napr. pri násobení. Presne na takomto princípe je založený aj posledný, dôležitý pojem tohto tematického celku.

Definícia 48. *Nech $(X, \circ)$ je algebra, R je ekvivalencia na X. Potom R je* **kongruencia** *na X ak platí:*

$$[a, b] \in R \wedge [c, d] \in R \Rightarrow [a \circ c, b \circ d] \in R.$$

Inými slovami, relácia kongruencie alebo kongruencia je ekvivalencia na algebre (napr. grupe), ktorá je zlúčiteľná so všetkými operáciami na tejto algebre Teda ak sú operandy na rovnakom mieste po dvoch ekvivalentné, potom musia aj výsledky operácie byť ekvivalentné.

Problematiku si objasníme na nasledujúcich príkladoch.

Príklad 49. *Zistite, či relácia $\equiv$ daná takto*

$$a \equiv b \iff 6|(a - b),$$

je kongruencia na množine $\mathbb{Z}$ vzhľadom na klasické sčítanie.

Riešenie. Zrejme $\big(\mathbb{Z}, +\big)$ je Abelova grupa a relácia $\equiv$ je ekvivalencia na množine $\mathbb{Z}$ (toto sme už riešili v predchádzajúcich kapitolách). Všimnime si rozklad množiny $\mathbb{Z}$, daný ekvivalenciou $\equiv$. Rozklad má 6 tried a dve celé čísla sú spolu v jednej triede, ak dávajú rovnaký zvyšok po delení šiestimi. Jednotlivé triedy označíme postupne $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$, pričom číslo $a \in \mathbb{Z}$ je prvkom triedy $\overline{i} \iff \exists k \in \mathbb{Z}\colon a = 6k + i$. Podľa definície kongruencie už zostáva overiť len to, či platí

$$\big[(a \equiv b) \wedge (c \equiv d)\big] \Rightarrow \big(a + c \equiv b + d\big).$$

Tvrdenie dokážeme priamo. Teda nech je splnený predpoklad

$$a \equiv b \wedge c \equiv d,$$

potom podľa definície relácie $\equiv$ platí

$$6|(a - b) \wedge 6|(c - d).$$

Potom

$$6\big|\big[(a - b) + (c - d)\big],$$

po vhodnej úprave dostaneme

$$6\big|\big[(a + c) - (b + d)\big],$$

čo je ekvivalentné s tým, že

$$a + c \equiv b + d.$$

Teda $\equiv$ je kongruencia na množine $\mathbb{Z}$ vzhľadom na klasické sčítanie.

Čo to znamená? Pokiaľ nás pri sčitovaní dvoch čísel zaujíma len aký zvyšok po delení šiestimi dáva výsledok, tak nemusíme sčitovať tie dve zadané čísla, ale len ich zvyšky po delení šiestimi.

To znamená, že zo $(\mathbb{Z}, +)$ sa presunieme do $(\mathbb{Z}_6, \oplus_6)$, čím si úlohu zjednodušíme (teda aspoň tí, ktorí neradi pracujú s veľkými číslami). Potom si vystačíme s touto tabuľkou:

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Teraz si úlohu trochu skomplikujeme.

Príklad 50. *Zistite, či relácia $\equiv$ daná takto*

$$a \equiv b \iff 6|(a-b),$$

je kongruencia na množine $\mathbb{Z}$ vzhľadom na klasické násobenie.

Riešenie. Podobne ako v predchádzajúcej úlohe treba zistiť len to, či platí

$$a \equiv b \wedge c \equiv d \Rightarrow a \cdot c \equiv b \cdot d.$$

Tvrdenie dokážeme znovu priamo. Teda nech je splnený predpoklad

$$a \equiv b \wedge c \equiv d,$$

potom podľa definície relácie $\equiv$ platí

$$6|(a-b) \wedge 6|(c-d).$$

Teraz musíme urobiť jeden umelý krok. Zrejme ak $6|(a-b) \Rightarrow 6|c \cdot (a-b)$, potom

$$6\big|\big[c \cdot (a-b) + b \cdot (c-d)\big],$$

po úprave

$$6\big|\big[c \cdot a - c \cdot b + b \cdot c - b \cdot d\big],$$

teda

$$6\big|\big[c \cdot a - b \cdot d\big],$$

čo je ekvivalentné s tým, že

$$a \cdot c \equiv b \cdot d.$$

Teda $\equiv$ je kongruencia na množine $\mathbb{Z}$ vzhľadom na klasické násobenie.

Čo to znamená v tomto prípade? V podstate to isté, čo v príklade 49., akurát pre operáciu násobenia, teda namiesto v $(\mathbb{Z}, \cdot)$ budeme počítať v $(\mathbb{Z}_6, \odot_6)$ a vystačíme si s touto tabuľkou:

$\odot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Študenti, ktorí riešili matematickú olympiádu, sa už s týmto určite stretli, a zrejme poznajú aj nasledujúcu definíciu.

Definícia 51. *Hovoríme, že dve čísla $a, b \in \mathbb{Z}$ sú kongruentné, ak ich rozdiel je deliteľný číslom m, ktoré nazývame* **modul** *$(m|(a-b))$. Formálne*

$$a \equiv b \pmod{m}.$$

Poznámka 52. *Predchádzajúce príklady môžeme preto zovšeobecniť. Zrejme v relácii $\equiv$ by sme číslo 6 mohli zameniť za ľubovolné iné prirodzené číslo m. Potom*

$$\left.\begin{array}{ll} a \equiv b & (\mathrm{mod}\ m) \\ c \equiv d & (\mathrm{mod}\ m) \end{array}\right\} \Rightarrow \quad a + c \equiv b + d \pmod{m}.$$

teda $\equiv$ je kongruencia na $(\mathbb{Z}, +)$.
Podobne aj

$$\left.\begin{array}{ll} a \equiv b & (\mathrm{mod}\ m) \\ c \equiv d & (\mathrm{mod}\ m) \end{array}\right\} \Rightarrow \quad a \cdot c \equiv b \cdot d \pmod{m}.$$

teda $\equiv$ je kongruencia aj na $(\mathbb{Z}, \cdot)$.

Využitie tejto kongruencie je najmä v teórii čísel, na ilustráciu uvádzam nasledujúci príklad.

Príklad 53. *Aké sú posledné dve číslice čísla 3^{1234}?*

Riešenie. Posledné dve cifry čísla určuje zvyšok po delení číslom 100, preto použijeme kongruenciu s modulo 100. Postupne budeme umocňovať číslo 3 a budeme hľadať takú mocninu, ktorá končí na 01. Zrejme

$$3^2 \equiv 9 \pmod{100},$$
$$3^4 \equiv 9 \cdot 9 \equiv 81 \pmod{100},$$
$$3^8 \equiv 81 \cdot 81 \equiv 61 \pmod{100},$$
$$3^{10} \equiv 61 \cdot 9 \equiv 49 \pmod{100},$$
$$3^{20} \equiv 49 \cdot 49 \equiv 1 \pmod{100}.$$

Ako nám táto informácia pomôže? Využijeme, že $1234 = 61 \cdot 20 + 14$ a teda $3^{1234} = (3^{20})^{61} \cdot 3^{14}$. Potom

$$(3^{20})^{61} \equiv 1^{61} \equiv 1 \pmod{100},$$
$$3^{1234} \equiv 3^{14} \pmod{100},$$
$$3^{14} \equiv 49 \cdot 81 \equiv 69 \pmod{100},$$

teda uvedené číslo končí dvojčíslím 69.

Poznámka 54. *Koho táto úloha zaujala, tak si môže vyhľadať Eulerovu vetu, pomocou ktorej by sme mocninu čísla 3, ktorá je kongruentná s 1 dokázali nájsť efektívnejšie.*

Vzťah medzi kongruenciami a normálnymi podgrupami vyjadrujú nasledujúce tvrdenia.

Veta 55. *Nech $(G, \circ)$ je grupa, R je kongruencia na G. Nech $1 \in G$ je neutrálny prvok v G. Potom $H = [1]_R = \{x; x \in G \wedge [x, 1] \in R\}$ je normálna podgrupa grupy G.*

Príklad 56. *Na množine permutácií množiny $\{1, 2, 3\}$ určte reláciu R tak, aby R bola kongruencia na tejto množine vzhľadom na operáciu skladania (vieme, že sa jedná o grupu, označme ju $(G, \circ)$) a potom podľa predchádzajúceho tvrdenia nájdite podgrupu grupy $(G, \circ)$ a overte, že je normálna.*

Riešenie. Toto je pomerne náročná úloha, obzvlášť pre začiatočníkov. Musíme nájsť reláciu R, ktorá bude reláciou ekvivalencie na množine $\{f_1, f_2, \ldots, f_6\}$ a zároveň bude platiť pre ľubovolné f_i, f_j, f_m, f_n

$$[f_i, f_j] \in R \wedge [f_m, f_n] \in R \Rightarrow [f_i \circ f_m, f_j \circ f_n] \in R,$$

teda R je kongruencia. Spomínanú grupu permutácií si pripomenieme operačnou tabuľkou (vyrobili sme ju príklade 25.):

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

Nie je problém vyrobiť reláciu ekvivalencie na tejto množine, stačí vyrobiť ľubovolný rozklad, napr. $\{\{f_1, f_2, f_3\}, \{f_4, f_5, f_6\}\}$. Tento rozklad má dve triedy, môžeme ich označiť takto: $\overline{f_1}, \overline{f_4}$ a teraz by sme mali skontrolovať, či táto relácia je aj kongruencia. Teda musíme zistiť, či napr. platí, že ak zoberieme ľubovolný prvok z triedy $\overline{f_1}$ a ľubovolný prvok z triedy $\overline{f_4}$ výsledok bude vždy z tej istej triedy. Vyskúšame to. Všimneme si, že napr.

$$f_1 \in \overline{f_1} \quad \wedge \quad f_4 \in \overline{f_4} \quad \wedge \quad f_1 \circ f_4 = f_4 \in \overline{f_4},$$
$$f_2 \in \overline{f_1} \quad \wedge \quad f_5 \in \overline{f_4} \quad \wedge \quad f_2 \circ f_5 = f_3 \in \overline{f_1}.$$

Toto je ale porušenie toho, čo od kongruencie požadujeme. To znamená, že uvedený rozklad neindukuje tú správnu reláciu ekvivalencie. Vyskúšame iný (snáď vhodnejší) rozklad $\{\{f_1, f_4, f_5\}\{f_2, f_3, f_6\}\}$. Rozklad má opäť len dve triedy, môžeme si ich označiť $\overline{f_1}, \overline{f_2}$. Pre lepšiu názornosť si v tabuľke vyznačíme prvky týchto tried rôznymi farbami, prvky z $\overline{f_1}$ budú vyznačené červenou, tie z $\overline{f_2}$ čiernou:

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

A teraz budeme vypĺňať tabuľku pre $(\{\overline{f_1}, \overline{f_2}\}, \circ)$, teda budeme kontrolovať, či sme už konečne dostali kongruenciu.

Ako takúto tabuľku vyplníme? Zopakujeme si definíciu kongruencie a uvedomíme si, čo znamená. Tabuľka bude mať len dva riadky a stĺpce, teda potrebujeme určiť výsledky $\overline{f_1} \circ \overline{f_1}, \overline{f_1} \circ \overline{f_2}, \overline{f_2} \circ \overline{f_1}, \overline{f_2} \circ \overline{f_2}$. Najskôr určíme $\overline{f_1} \circ \overline{f_1}$, pozrieme si v tabuľke všetky také výsledky, kde sú obe f_i, f_j z $\overline{f_1}$, to znamená, že sú vyznačené červenou farbou. Vidíme, že všetky takéto výsledky sú červené, teda sú z triedy $\overline{f_1}$, preto $\overline{f_1} \circ \overline{f_1} = \overline{f_1}$. Podobne určíme aj $\overline{f_1} \circ \overline{f_2}$, teda sa pozrieme, aké sú výsledky, ak ľavý operand je červený a pravý čierny-teda sledujeme riadky prislúchajúce k červeným a stĺpce k čiernym vstupom. Všetky takéto výsledky sú čierne, teda z triedy $\overline{f_2}$. Takto určíme aj zvyšné dva výsledky a dostaneme tabuľku

$\circ$	$\overline{f_1}$	$\overline{f_2}$
$\overline{f_1}$	$\overline{f_1}$	$\overline{f_2}$
$\overline{f_2}$	$\overline{f_2}$	$\overline{f_1}$

Vďaka tomu, že sme boli schopní túto tabuľku jednoznačne vyplniť (teda sa nestalo, že by sme pri niektorom políčku dostali červený aj čierny výsledok zároveň), máme skontrolované, že relácia daná rozkladom $\{\{f_1, f_4, f_5\}\{f_2, f_3, f_6\}\}$ je kongruencia. Teraz ešte musíme nájsť podgrupu, ktorá bude podľa vety 55. normálna. Do tejto podgrupy patria také prvky, ktoré sú v tej istej triede rozkladu ako neutrálny prvok pôvodnej grupy. Neutrálny prvok je f_1, teda podgrupa $H = \{f_1, f_4, f_5\}$ je normálna. Ak to chceme skontrolovať, musíme urobiť ľavý a pravý rozklad podľa tejto podgrupy a pre normálnu grupu sa oba rozklady rovnajú. Skontrolujte si to a premyslite si, prečo sa v tomto prípade dá dopredu očakávať pozitívny výsledok, napriek tomu, že pôvodná grupa nie je komutatívna.

Veta 57. *Nech $(G, \circ)$ je grupa, $H \subseteq G$ je jej normálna podgrupa. Potom relácia $R = \{[x, y]; x, y \in G \wedge y^{-1} \circ x \in H\}$ je kongruencia na G.*

Príklad 58. *Vyberte si ľubovolnú normálnu podgrupu grupy $(\mathbb{Z}_4, \oplus_4)$ a podľa predchádzajúceho tvrdenia nájdite reláciu R a overte, že sa jedná o kongruenciu na $\mathbb{Z}_4$.*

Riešenie. Z príkladu 29. vieme, že grupa $(\mathbb{Z}_4, \oplus_4)$ má tieto podgrupy: $(\{0\}, \oplus_4), (\{0, 2\}, \oplus_4), (\{0, 1, 2, 3\}, \oplus_4)$. Vyberieme si podgrupu $(\{0, 2\}, \oplus_4)$ a aplikujeme predchádzajúce tvrdenie. Teda treba skontrolovať, ktoré dvojice do relácie R patria a ktoré nepatria. Napr. dvojica $[0, 0] \in R$, lebo $0 \in \mathbb{Z}_4$, inverzný prvok k 0 je 0 a

$$0 \oplus_4 0 = 0 \in \{0, 2\}.$$

Podobne zistíme, že aj dvojice $[1, 1], [2, 2], [3, 3]$ patria do R. Podrobne vysvetlíme dvojicu $[1, 1]$. Zrejme $1 \in \mathbb{Z}_4$, inverzný prvok k 1 je 3 a

$$3 \oplus_4 1 = 0 \in \{0, 2\}.$$

Naopak, napr. dvojica $[0, 1] \notin R$, lebo $0, 1 \in \mathbb{Z}_4$, inverzný prvok k 1 je 3 a

$$3 \oplus_4 0 = 3 \notin \{0, 2\}.$$

Takto postupne zistíme, že $R = \{[0, 0], [1, 1], [2, 2], [3, 3], [0, 2], [2, 0], [1, 3], [3, 1]\}$. Zrejme relácia R je reláciou ekvivalencie (overte si to). Rozklad množiny $\mathbb{Z}_4$ vzhľadom k R je $\{\{0, 2\}, \{1, 3\}\}$, faktorová množina $\mathbb{Z}_4/_R = \{\overline{0}, \overline{1}\}$. Treba ešte overiť, že platí

$$[a, b] \in R \wedge [c, d] \in R \Rightarrow [a \oplus_4 c, b \oplus_4 d] \in R.$$

teda z tabuľky pre $(\mathbb{Z}_4, \oplus_4)$

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

vytvoríme tabuľku pre $(\{\overline{0}, \overline{1}\}, \oplus)$

$\oplus$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

Ako túto tabuľku vyrábame? Podobne ako v predchádzajúcom príklade. V tabuľke pre $(\mathbb{Z}_4, \oplus_4)$ sú červenou farbou vyznačené prvky z triedy $\overline{0}$, prvky z triedy $\overline{1}$ sú vyznačené čiernou farbou. Ak máme vyplniť v tabuľke pre $(\{\overline{0}, \overline{1}\}, \oplus)$ napr. výsledok $\overline{0} \oplus \overline{0}$, tak si pozrieme všetky výsledky

pre červené sčítance v tabuľke pre $(\mathbb{Z}_4, \oplus_4)$. Vo všetkých prípadoch je výsledok "červený", teda príslušné políčko vieme jednoznačne vyplniť a vpíšeme tam $\overline{0}$. Podobne postupujeme aj pri vyplňovaní zvyšných troch políčok. Keďže bol vždy výsledok jednoznačný, máme skontrolované, že R je kongruencia.

Definícia 59. *Nech $(G, \circ)$ je grupa, $H \subseteq G$ je jej normálna podgrupa. Nech relácia $R = \{[x, y]; x, y \in G \wedge y^{-1} \circ x \in H\}$ je kongruencia na G (to, že R je kongruencia už vieme z vety 57.). Potom grupa tried grupy G vzhľadom na normálnu podgrupu H sa nazýva* **faktorovou grupou** *a označuje sa G/H.*

Poznámka 60. *V príklade 58. je faktorovou grupou $\big(\{\overline{0}, \overline{1}\}, \oplus\big)$. Všimnite si, že $\big(\{\overline{0}, \overline{1}\}, \oplus\big)$ je izomorfná s grupou $\big(\mathbb{Z}_2, \oplus_2\big)$.*

Poznámka 61. *V príklade 49. sme mali faktorovú množinu $\mathbb{Z}/_{\equiv} = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Zistili sme, že relácia $\equiv$ je kongruencia vzhľadom na klasické sčítanie na $\mathbb{Z}$, teda teda $\big(\mathbb{Z}_6, \oplus_6\big)$ je faktorová grupa. K akej normálnej podgrupe podľa vety 57. bola táto kongruencia vytvorená? Všimnite si podgrupu $H = \{6 \cdot k \colon k \in \mathbb{Z}\}$. Ukážte, že je to naozaj podgrupa (návod nájdete v príklade 35.). To, že je to normálna podgrupa vyplýva z toho, že $\big(\mathbb{Z}, +\big)$ je komutatívna a prepojenie s reláciou $\equiv$ plynie z vety 57.*

5 Úlohy na precvičenie

5.1 Operácie

1. Na množine $A = \{a, b, c\}$ definujte (tabuľkou) operáciu, ktorá je

   (a) komutatívna a asociatívna,

   (b) komutatívna, ale nie je asociatívna,

   (c) asociatívna, ale nie je komutatívna,

   (d) nie je ani komutatívna, ani asociatívna.

   Výsledky: Napr.:

   a)

$\star$	a	b	c
a	c	c	c
b	c	c	c
c	c	c	c

   b)

$\star$	a	b	c
a	a	b	c
b	b	a	a
c	c	a	a

   c)

$\star$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

   d)

$\star$	a	b	c
a	a	c	c
b	b	a	c
c	c	b	c

2. Na množine $\mathbb{Z}$ sú definované operácie

   (a) $a \circ b = a + b + 1$,

   (b) $a \star b = 2a + b$,

   (c) $a \Delta b = a^3 + b^3$.

   (d) $a * b = a + b - a \cdot b$.

   Určte ich vlastnosti.

   Výsledky: a)$\circ$ je komutatívna, asociatívna, má neutrálny prvok $e = -1$, ku každému prvku z $\mathbb{Z}$ existuje inverzný prvok $-2 - a$, b) $\star$ nie je komutatívna, nie je asociatívna, nemá neutrálny prvok, teda ani inverzné prvky, c) Δ je komutatívna, nie je asociatívna, nemá neutrálny prvok, teda ani inverzné prvky, d) $*$ je komutatívna, asociatívna, má neutrálny prvok $e = 0$, inverzný prvok existuje len pre tie $a \in \mathbb{Z}$, pre ktoré je zlomok $\frac{a}{a-1}$ celé číslo.

3. V ktorých z nasledujúcich prípadov je skladanie funkcií operácia na F?

   (a) F je množina všetkých konštantných funkcií,

   (b) F je množina všetkých lineárnych funkcií,

   (c) F je množina všetkých kvadratických funkcií.

   Výsledky: a) jedná sa o operáciu, b) jedná sa o operáciu, c) nejedná sa o operáciu. Treba si dobre uvedomiť definíciu operácie a uvedomiť si, že napr. v časti a) treba zistiť, či zložením dvoch lineárnych funkcií, bude opäť funkcia lineárna.

4. Na intervale $\langle 0, 1\rangle$ definujeme operáciu $\star_1$ nasledovne: $a \star_1 b = \max\{a, b\}$. Rozhodnite o pravdivosti tvrdenia: Operácia $\star_1$ je asociatívna na $\langle 0, 1\rangle$. Svoju odpoveď zdôvodnite.

   Výsledky: Tvrdenie je pravdivé, pri zdôvodnení môžete postupovať rozobraním všetkých možností pre vstupy vzhľadom na ich klasické usporiadanie.

5. Na intervale $\langle 0, 1\rangle$ definujeme operáciu $\star_2$ nasledovne: $a \star_2 b = \min\{a, b\}$. Rozhodnite o pravdivosti tvrdenia: Operáce $\star_2$ je asociatívna na $\langle 0, 1\rangle$. Svoju odpoveď zdôvodnite.

   Výsledky: Tvrdenie je pravdivé, pri zdôvodnení môžete postupovať rozobraním všetkých možností pre vstupy vzhľadom na ich klasické usporiadanie.

6. Na množine $\mathbb{N}^+$ definujeme operáciu $\star_3$ nasledovne: $a \star_3 b = NSD\{a, b\}$. Rozhodnite o pravdivosti tvrdenia: Operácia $\star_3$ je asociatívna na $\mathbb{N}^+$. Svoju odpoveď zdôvodnite.

   Výsledky: Tvrdenie je pravdivé, pre zdôvodnenie môžete využiť asociativitu minima.

7. Na množine $\mathbb{N}^+$ definujeme operáciu $\star_4$ nasledovne: $a \star_4 b = NSN\{a, b\}$. Rozhodnite o pravdivosti tvrdenia: Operácia $\star_4$ je asociatívna na $\mathbb{N}^+$. Svoju odpoveď zdôvodnite.

   Výsledky: Tvrdenie je pravdivé, pre zdôvodnenie môžete využiť asociativitu maxima.

8. Na intervale $\langle 0, 1\rangle$ definujeme operáciu $\star_5$ nasledovne: $a \star_5 b = \frac{a.b}{2-a-b+ab}$. Rozhodnite o pravdivosti tvrdenia: Operácia $\star_5$ je asociatívna na $\langle 0, 1\rangle$. Svoju odpoveď zdôvodnite.

   Výsledky: Tvrdenie je pravdivé, pre zdôvodnenie si vyjadrite obe možné usporiadania zátvoriek, upravte a porovnajte

9. Na intervale $\langle 0, 1)$ definujeme operáciu $\star_6$ nasledovne: $a \star_6 b = \frac{a+b-2a.b}{1-a.b}$. Rozhodnite o pravdivosti tvrdenia: Operácia $\star_6$ je asociatívna na $\langle 0, 1)$. Svoju odpoveď zdôvodnite.

   Výsledky: Tvrdenie je pravdivé, pre zdôvodnenie si vyjadrite obe možné usporiadania zátvoriek, upravte a porovnajte

10. Nájdite asociatívnu operácie na množine reálnych čísel $\star_1, \star_2, \star_3$ (rôzne!), tak, aby platilo:

$$a \star_3 b = \frac{a \star_1 b + a \star_2 b}{2}.$$

    Výsledky: napr.: $a \star_1 b = 6, a \star_2 b = 4 \Rightarrow a \star_3 b = 5$.

11. Nájdite dve rôzne asociatívne operácie $\star$ a $\circ$, obe nad $\mathbb{R}$, tak aby operácia $\oplus$ nad $\mathbb{R}$, ktorá je definovaná nasledovne

$$a \oplus b = (a \star b) - (a \circ b)$$

    a) bola asociatívna,

    b) nebola asociatívna.

    Výsledky: napr.:

    a) $a \star b = 6, a \circ b = 4 \Rightarrow a \oplus b = 2, b) a \star b = a \cdot b, a \circ b = a + b \Rightarrow a \oplus b = a \cdot b - (a + b)$.

12. * Nech $p \neq 0, g \neq 0, r$ sú pevne zvolené reálne čísla. Na množine $\mathbb{R}$ je definovaná operácia $\circ$ nasledovne:

$$a \circ b = p.a + q.b + r.$$

    Aké musia byť čísla p, q, r, ak

    - operácia $\circ$ má byť asociatívna,
    - operácia $\circ$ má byť komutatívna,
    - operácia $\circ$ má mať neutrálny prvok,
    - ku každému prvku z $\mathbb{R}$ má existovať inverzný prvok.

5.2 Algebry a podalgebry

1. Na množine $A = \{a, b, c, d\}$ definujte operáciu $\star$ tak, aby grupoid $(A, \star)$ mal

   (a) práve jeden podgrupoid,

   (b) práve dva podgrupoidy,

   (c) práve tri podgrupoidy,

   (d) práve päť podgrupoidov.

Výsledky: napr.:

a)

$\star$	a	b	c	d
a	b	c	c	d
b	b	c	c	d
c	c	b	d	d
d	d	d	d	a

b)

$\star$	a	b	c	d
a	a	c	c	d
b	d	a	c	d
c	a	b	b	d
d	a	b	c	c

c)

$\star$	a	b	c	d
a	a	c	c	d
b	b	b	d	b
c	c	a	b	b
d	d	b	b	c

d)

$\star$	a	b	c	d
a	a	c	c	b
b	b	b	d	a
c	d	d	c	a
d	d	a	b	d

a) Podgrupoid je len $(A, \star)$, b) podgrupoidy sú $(A, \star), (\{a\}, \star)$, c) podgrupoidy sú $(A, \star), (\{a\}, \star), (\{b\}, \star)$, d) podgrupoidy sú $(A, \star), (\{a\}, \star), (\{b\}, \star), (\{c\}, \star), (\{d\}, \star)$.

2. Na množine $M = \{a, b, c, d\}$ je daná operácia $\circ$ nasledovne:

$\circ$	a	b	c	d
a	c	a	c	c
b	a	b	c	d
c	c	c	b	b
d	c	d	b	b

   (a) Je $(M, \circ)$ pologrupa?

   (b) Vypíšte všetky dvojprvkové podgrupoidy $(M, \circ)$.

Výsledky: a) Nejedná sa o pologrupu, je porušená asociativita, napr. $c \circ (c \circ d) \neq (c \circ c) \circ d$. Dvojprvkové podgrupoidy sú: $(\{b, c\}, \circ), (\{b, d\}, \circ)$.

3. Na množine $A = \{a, b, c, d\}$ definujte operáciu $\star$ tak, aby $(A, \star)$

   (a) bol grupoid, ale nie asociatívny grupoid,

   (b) bol asociatívny grupoid bez neutrálneho prvku,

   (c) bol asociatívny grupoid s neutrálnym prvkom,

   (d) bola grupa.

Výsledky: napr.

a)

$\star$	a	b	c	d
a	a	c	c	d
b	b	a	c	d
c	c	b	c	d
d	d	d	d	d

b)

$\star$	a	b	c	d
a	a	b	c	d
b	a	b	c	d
c	a	b	c	d
d	a	b	c	d

c)

$\star$	a	b	c	d
a	a	b	c	d
b	b	b	b	b
c	c	b	b	b
d	d	b	b	b

d)

$\star$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

4. Na množine $\mathbb{Z}$ sú definované operácie

   (a) $a \circ b = a + b - 1$,

   (b) $a \star b = a \cdot b$,

   (c) $a \Delta b = a \cdot b - 1$.

   Zistite, v ktorých prípadoch sa jedná o grupu.

Výsledky: a) je grupa, b) nie je grupa, napr. 2 nemá inverzný prvok, c) nie je grupa, je porušená asociativita.

5. Nech $A = \{a, b, c, d, e, f\}$. Nájdite operáciu $\circ$ tak, aby $(A, \circ)$ bol grupoid, ale nie grupa, a aby aspoň jeden jeho podgrupoid bol grupou na svojom nosiči.

Výsledky: Napr.:

$\circ$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	a	a	a	a
c	c	a	a	a	a	a
d	d	a	a	a	a	a
e	e	a	a	a	a	a
f	f	a	a	a	a	a

Zrejme $(A, \circ)$ nie je grupa, nie je asociatívna, ale podgrupoid $(\{a, b\}, \circ)$ je grupa, izomorfná so $(\mathbb{Z}_2, \oplus_2)$.

6. Nech $A = \{a, b, c, d, e, f\}$. Nájdite operáciu $\circ$ tak, aby $(A, \circ)$ bol neasociatívny grupoid s neutrálnym prvkom a každý jeho prvok mal práve jeden inverzný prvok.

   Výsledky: Inšpirujte sa príkladom 11..

7. Na množine $A = \{a, b, c, d\}$ nájdite nekomutatívnu grupu, ak sa to dá. Svoju odpoveď zdôvodnite.

   Výsledky: Taká grupa neexistuje. Dôkaz skúste urobiť sporom.

8. Na množine $A = \{a, b, c, d, e, f\}$ nájdite nekomutatívnu grupu, ak sa to dá. Svoju odpoveď zdôvodnite.

   Výsledky: Taká grupa existuje, je izomorfná s grupou z príkladu 25..

9. Na množine $M = \{0, a, b, c, d, 1\}$ je daná operácia $\circ$ nasledovne:

$\circ$	0	a	b	c	d	1
0	0	0	0	0	d	1
a	0	0	0	a	d	1
b	0	0	0	b	d	1
c	0	a	b	c	d	1
d	d	d	d	d	1	1
1	1	1	1	1	1	1

   Je $(M, \circ)$ pologrupa? Svoju odpoveď zdôvodnite.

   Výsledky: Operácia je na M uzavretá, aj asociatívna, teda $(M, \circ)$ je pologrupa. Nezabudnite na zdôvodnenie asociativity.

10. Na množine $M = \{0, a, b, c, d, 1\}$ je daná operácia $\circ$ nasledovne:

$\circ$	0	a	b	c	d	1
0	0	0	b	c	0	1
a	0	0	b	c	a	1
b	b	b	b	c	b	1
c	c	c	c	1	c	1
d	0	a	b	c	d	1
1	1	1	1	1	1	1

    Je $(M, \circ)$ pologrupa? Svoju odpoveď zdôvodnite.

    Výsledky: Operácia je na M uzavretá, aj asociatívna, teda $(M, \circ)$ je pologrupa. Nezabudnite na zdôvodnenie asociativity.

11. * Nech $a_1, a_2, \cdots, a_n$ sú prvky grupy. Zapíšte inverzný prvok k prvku $a_1.a_2.\cdots.a_n$.

12. * Dokážte, že ak v grupe $(G, .)$ platí $a.b = a$, tak $b = e$.

13. * Dokážte, že v konečnej grupe s párnym (sudým) počtom prvkov existuje prvok a, pre ktorý platí: $a \neq e, a.a = e$.

14. * Dokážte, že ak $x \circ x = e$ pre každý prvok x grupy $(G, \circ)$, tak $(G, \circ)$ je komutatívna grupa.

5.3 Homomorfizmy a kongruencie

1. Na množine $A = \{a, b, c, d\}$ je tabuľkou daná operácia $\circ$ a na množine $B = \{1, 2, 3, 4\}$ operácia $\star$. Zistite, či existuje izomorfizmus medzi grupoidmi $(A, \circ)$ a $(B, \star)$. V prípadě kladnej odpovede izomorfizmus nájdite, v opačnom prípade zdôvodnite jeho neexistenciu.

$\circ$	a	b	c	d
a	a	b	a	c
b	b	d	b	c
c	a	b	c	d
d	c	c	d	a

$\star$	1	2	3	4
1	3	1	4	1
2	1	2	4	2
3	4	4	2	3
4	1	2	3	4

Výsledky: Izomorfizmus existuje: $f(a) = 2, f(b) = 1, f(c) = 4, f(d) = 3$.

2. Na množine $A = \{a, b, c, d\}$ je tabuľkou daná operácia $\circ$ a na množine $B = \{1, 2, 3, 4\}$ operácia $\star$. Zistite, či existuje izomorfizmus medzi grupoidmi $(A, \circ)$ a $(B, \star)$. V prípadě kladnej odpovede izomorfizmus nájdite, v opačnom prípade zdôvodnite jeho neexistenciu.

$\circ$	a	b	c	d
a	a	b	c	d
b	b	d	b	c
c	c	b	c	d
d	d	c	d	a

$\star$	1	2	3	4
1	3	1	4	1
2	1	2	4	3
3	4	4	2	3
4	1	3	3	4

Výsledky: Izomorfizmus neexistuje, napr. grupoid $(A, \circ)$ má neutrálny prvok, ale grupoid $(B, \star)$ nemá neutrálny prvok.

3. Nájdite epimorfizmus algebier $(\mathbb{Z}_6, \oplus_6)$ na $(\mathbb{Z}_2, \oplus_2)$, $(\mathbb{Z}_6, \oplus_6)$ na $(\mathbb{Z}_3, \oplus_3)$, $(\mathbb{Z}_6, \oplus_6)$ na $(\mathbb{Z}_5, \oplus_5)$.

Výsledky: Epimorfizmus $(\mathbb{Z}_6, \oplus_6)$ na $(\mathbb{Z}_2, \oplus_2)$ je $f(0) = f(2) = f(4) = 0, f(1) = f(3) = f(5) = 1$, epimorfizmus $(\mathbb{Z}_6, \oplus_6)$ na $(\mathbb{Z}_3, \oplus_3)$ je $f(0) = f(3) = 0, f(1) = f(4) = 1, f(2) = f(4) = 2$, epimorfizmus $(\mathbb{Z}_6, \oplus_6)$ na $(\mathbb{Z}_5, \oplus_5)$ neexistuje. Pozor, nestačí epimorfizmy nájsť, treba ukázať, že to epimorfizmy sú.

4. Na množine $A = \{a, b, c, d\}$ je daná relácia R takto

$$R = \{[a, a], [a, b], [b, a], [b, b], [c, c], [c, d], [d, c], [d, d]\}.$$

Ďalej je na množine A tabuľkou daná operácia $\circ$ takto

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Dokážte, že relácia R je kongruencia na množine A vzhľadom na operáciu $\circ$.

5. Na množine $A = \{a, b, c, d, e, f\}$ je daný rozklad $\mathcal{S}$ nasledovne:

$$\mathcal{S} = \{\{a, e\}, \{b, d\}, \{c\}, \{f\}\}.$$

- Určte reláciu ekvivalencie R, ktorá je daná rozkladom $\mathcal{S}$.
- Na množine A určte operáciu $\circ$ tak, aby R bola reláciou kongruencie na A vzhľadom k operácii $\circ$.

Výsledky: $R = \{[a, a], [b, b], [c, c], [d, d], [e, e], [f, f], [a, e], [e, a], [b, d], [d, b]\}$, operácia môže byť napr. $\forall a, b \in A; a \circ b = a$.

6. Na množine $A = \{a, b, c, d, e, f\}$ je daný rozklad $\mathcal{S}$ nasledovne:

$$\mathcal{S} = \{\{a, b, c, e\}, \{d\}, \{f\}\}.$$

   - Určte reláciu ekvivalencie R, ktorá je daná rozkladom $\mathcal{S}$.
   - Na množine A určte operáciu $\circ$ tak, aby R bola reláciou kongruencie na A vzhľadom k operácii $\circ$.

   Výsledky: $R = \{[a, a], [b, b], [c, c], [d, d], [e, e], [f, f], [a, b], [a, c], [a, e], [b, a], [b, c], [b, e], [c, a], [c, b], [c, e], [e, a], [e, b], [e, c]\}$, operácia môže byť napr. $\forall a, b \in A; a \circ b = a$.

7. * Dokážte, že $13|(2^{70} + 3^{70})$.

8. * Číslo 4444^{4444} zapísané v desiatkovej sústave má ciferný súčet A. Nech B je ciferný súčet čísla A. Nájdite ciferný súčet čísla B.