

1. Algebrické štruktúry s jednou operáciou

V predchádzajúcich kapitolách sme sa oboznámili s pojmom binárnej operácie na množine, jej vlastnosťami (komutatívnosť, asociatívnosť), s neutrálnym prvkom a s inverznými prvkami.

Teraz sa sústredíme na nejakú množinu, na ktorej budeme mať binárnu operáciu. Podľa toho, aké bude mať vlastnosti, či bude mať neutrálny prvok a inverzné prvky, budeme hovoriť o grupoide, pologrupe, monoide či grupe.

Najprv si vždy uvedieme definíciu nového pojmu a potom si uvedieme príklady na tento pojem.

Nech je daná neprázdna množina G , na ktorej je definovaná binárna operácia $*$. Potom dvojicu $(G, *)$ nazývame grupoid.

Ak $G = N$ je množina prirodzených čísel, potom na nej máme definované operácie sčítania a násobenia. Teda dvojice $(N, +)$ a $(N, \cdot)$ sú grupoidy. Nakoľko rozdielom a podielom dvoch prirodzených čísel nemusí byť vždy prirodzené číslo, dvojice $(N, -)$ a $(N, :)$ nie sú grupoidy.

Ak $G = Z$ je množina celých čísel, potom na nej máme definované operácie sčítania, odčítania, násobenia aj delenia. Teda dvojice $(Z, +)$, $(Z, \cdot)$, $(Z, -)$ a $(Z, :)$ sú grupoidy.

Ak $G = Q$ je množina racionálnych čísel, potom na nej máme definované operácie sčítania, odčítania, násobenia aj delenia. Teda dvojice $(Q, +)$, $(Q, \cdot)$, $(Q, -)$ a $(Q, :)$ sú grupoidy.

Ak $G = R$ je množina reálnych čísel, potom na nej máme definované operácie sčítania, odčítania, násobenia aj delenia. Teda dvojice $(R, +)$, $(R, \cdot)$, $(R, -)$ a $(R, :)$ sú grupoidy.

Grupoid $(G, *)$, v ktorom je operácia $*$ asociatívna, nazývame pologrupa.

Ak $G = N$ je množina prirodzených čísel, potom na nej máme definované operácie sčítania a násobenia, ktoré sú asociatívne. Teda dvojice $(N, +)$ a $(N, \cdot)$ sú pologrupy.

Ak $G = Z$ je množina celých čísel, potom na nej máme definované operácie sčítania, odčítania, násobenia aj delenia. Asociatívne sú však iba sčítanie a násobenie. Teda dvojice $(Z, +)$ a $(Z, \cdot)$ sú pologrupy, zatiaľ čo $(Z, -)$ a $(Z, :)$ nie sú pologrupy.

Podobne je to aj s racionálnymi a reálnymi číslami. Ak $G = Q$ je množina racionálnych čísel, potom dvojice $(Q, +)$, $(Q, \cdot)$, $(R, +)$ a $(R, \cdot)$ sú pologrupy a $(Q, -)$, $(Q, :)$, $(R, -)$ a $(R, :)$ nie sú pologrupy.

Pologrupu $(G,*)$, ktorá má neutrálny prvok e vzhľadom na operáciu $*$, nazývame monoid.

Už vieme, že neutrálnym prvkom vzhľadom na operáciu násobenia je číslo 1, ktoré patrí do množiny prirodzených, celých, racionálnych i reálnych čísel. Preto $(N, \cdot)$, $(Z, \cdot)$, $(Q, \cdot)$ a $(R, \cdot)$ sú monoidy.

Taktiež už vieme, že neutrálnym prvkom vzhľadom na operáciu sčítania je číslo 0, ktoré patrí do množiny celých, racionálnych i reálnych čísel, avšak nepatrí do množiny prirodzených čísel. Preto $(N, +)$ nie je monoid, zatiaľ čo $(Z, +)$, $(Q, +)$ a $(R, +)$ sú monoidy.

Monoid $(G,*)$, v ktorom má každý prvok x množiny G inverzný prvok x^{-1} vzhľadom na operáciu $*$, nazývame grupa.

Už vieme, že inverzným prvkom k číslu x vzhľadom na operáciu sčítania je číslo $-x$. Ak x bolo celé číslo, potom aj $-x$ je celé číslo (podobne racionálne i reálne). Preto $(Z, +)$, $(Q, +)$ a $(R, +)$ sú grupy.

Taktiež už vieme, že inverzným prvkom k číslu x vzhľadom na operáciu násobenia je číslo $\frac{1}{x}$. Avšak nula nemá inverzný prvok vzhľadom na násobenie. Preto $(Z, \cdot)$, $(Q, \cdot)$ a $(R, \cdot)$ nie sú grupy.

Čo ak číslo 0 vylúčime? Ak x je celé číslo, potom číslo $\frac{1}{x}$ nemusí byť celé. Preto $(Z - \{0\}, \cdot)$ nie je grupa. Podobne, ak x je prirodzené číslo, potom číslo $\frac{1}{x}$ nemusí byť prirodzené. Preto $(N, \cdot)$ nie je grupa. Naopak, ak x je racionálne či reálne číslo, potom aj číslo $\frac{1}{x}$ je racionálne či reálne. Preto $(Q - \{0\}, \cdot)$ a $(R - \{0\}, \cdot)$ sú grupy.

Grupa $(G,*)$, v ktorej je operácia $*$ komutatívna, sa nazýva komutatívna grupa alebo aj Abelova grupa.

Už sme si povedali, že $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} - \{0\}, \cdot)$ a $(\mathbb{R} - \{0\}, \cdot)$ sú grupy.

Pretože sčítanie aj násobenie je komutatívne, všetky tieto grupy sú komutatívne, resp. Abelove.

Čo teda platí v prípade, že $(G,*)$ je grupa?

1. G je neprázdna množina,
2. $*$ je binárna operácia na G , teda ak a, b sú z množiny G , potom aj $a*b$ je z množiny G ,
3. operácia $*$ je asociatívna,
4. množina G obsahuje neutrálny prvok e vzhľadom na operáciu $*$,
5. každý prvok množiny G má inverzný prvok vzhľadom na operáciu $*$, ktorý tiež patrí do množiny G .

Ak je $(G,*)$ Abelova grupa, potom navyše platí

6. operácia $*$ je komutatívna.

V tabuľke si zhrnieme získané poznatky.

	grupoid	pologrupa	monoid	grupa	Abelova grupa
$(\mathbb{N}, +)$	áno	áno	nie	nie	nie
$(\mathbb{Z}, +)$	áno	áno	áno	áno	áno
$(\mathbb{Q}, +)$	áno	áno	áno	áno	áno
$(\mathbb{R}, +)$	áno	áno	áno	áno	áno
$(\mathbb{N}, \cdot)$	áno	áno	áno	nie	nie
$(\mathbb{Z}, \cdot)$	áno	áno	áno	nie	nie
$(\mathbb{Q}, \cdot)$	áno	áno	áno	nie	nie
$(\mathbb{R}, \cdot)$	áno	áno	áno	nie	nie
$(\mathbb{Z} - \{0\}, \cdot)$	áno	áno	áno	nie	nie
$(\mathbb{Q} - \{0\}, \cdot)$	áno	áno	áno	áno	áno
$(\mathbb{R} - \{0\}, \cdot)$	áno	áno	áno	áno	áno

Úloha:

Daná je množina párnych prirodzených čísel $G = \{2, 4, 6, 8, 10, 12, \dots\}$ a operácia sčítania.

Rozhodnite, či dvojica $(G, +)$ je grupoid, pologrupa, monoid, grupa.

Riešenie:

Pretože súčtom dvoch párnych prirodzených čísel je opäť párne prirodzené číslo, je operácia $+$ binárnou operáciou na množine G . Preto $(G, +)$ je grupoid.

Nakoľko operácia sčítania je asociatívna, je $(G, +)$ pologrupa.

Neutrálnym prvkom operácie $+$ je nula a tá nepatrí do množiny G . Preto $(G, +)$ nie je monoid, a teda ani grupa.

Úloha:

Daná je množina nepárnych prirodzených čísel $G = \{1, 3, 5, 7, 9, 11, \dots\}$ a operácia sčítania.

Rozhodnite, či dvojica $(G, +)$ je grupoid, pologrupa, monoid, grupa.

Riešenie:

Pretože súčtom dvoch nepárnych prirodzených čísel nie je nepárne prirodzené číslo, operácia $+$ nie je binárnou operáciou na množine G . Preto $(G, +)$ nie je grupoid, teda ani pologrupa, monoid či grupa.

Úloha:

Daná je množina párnych prirodzených čísel $G = \{2, 4, 6, 8, 10, 12, \dots\}$ a operácia násobenia.

Rozhodnite, či dvojica $(G, \cdot)$ je grupoid, pologrupa, monoid, grupa.

Riešenie:

Pretože súčinom dvoch párnych prirodzených čísel je opäť párne prirodzené číslo, je operácia $\cdot$ binárnou operáciou na množine G . Preto $(G, \cdot)$ je grupoid.

Nakoľko operácia násobenia je asociatívna, je $(G, \cdot)$ pologrupa.

Neutrálnym prvkom operácie násobenia je číslo 1 a to nepatrí do množiny G . Preto $(G, \cdot)$ nie je monoid, a teda ani grupa.

Úloha:

Daná je množina nepárnych prirodzených čísel $G = \{1, 3, 5, 7, 9, 11, \dots\}$ a operácia násobenia.

Rozhodnite, či dvojica $(G, \cdot)$ je grupoid, pologrupa, monoid, grupa.

Riešenie:

Pretože súčinom dvoch nepárnych prirodzených čísel je opäť nepárne prirodzené číslo, je operácia $\cdot$ binárnou operáciou na množine G . Preto $(G, \cdot)$ je grupoid.

Nakoľko operácia násobenia je asociatívna, je $(G, \cdot)$ pologrupa.

Neutrálным prvkom operácie násobenia je číslo 1 a to patrí do množiny G . Preto $(G, \cdot)$ je monoid.

Pretože okrem čísla 1 žiadne iné číslo z množiny G nemá inverzný prvok v množine G vzhľadom na násobenie, $(G, \cdot)$ nie je grupa.

Úloha:

Daná je binárna operácia $\circ$ na množine $A = \{0, 1, 2, 3, 4\}$ pomocou Cayleho tabuľky.

$\circ$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Rozhodnite, či $(A, \circ)$ je grupoid, pologrupa, monoid, grupa, Abelova grupa. Prezradíme, že operácia $\circ$ je na množine A asociatívna.

Riešenie:

Pretože vo výsledkovej časti Cayleho tabuľky sú iba prvky množiny A , je $(A, \circ)$ grupoid.

Pretože operácia $\circ$ je na množine A asociatívna, je $(A, \circ)$ pologrupa. Pretože neutrálным prvkom je 1, je $(A, \circ)$ monoid. Pretože 0 nemá inverzný prvok, $(A, \circ)$ nie je grupa.

Úloha:

Daná je binárna operácia $\circ$ na množine $A = \{1, 2, 3, 4\}$ pomocou Cayleho tabuľky.

$\circ$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Rozhodnite, či $(A, \circ)$ je grupoid, pologrupa, monoid, grupa, Abelova grupa. Prezradíme, že operácia $\circ$ je na množine A asociatívna

Riešenie:

Pretože vo výsledkovej časti Cayleho tabuľky sú iba prvky množiny A , je $(A, \circ)$ grupoid.

Pretože operácia $\circ$ je na množine A asociatívna, je $(A, \circ)$ pologrupa. Pretože neutrálnym prvkom je 1, je $(A, \circ)$ monoid. Pretože 1 má inverzný prvok 1, 2 má inverzný prvok 3, 3 má

inverzný prvok 2, 4 má inverzný prvok 4 a operácia je komutatívna, je $(A, \circ)$ Abelova grupa.

Úloha:

Daná je binárna operácia $\circ$ na množine $A = \{0, 1, 2, 3\}$ pomocou Cayleho tabuľky.

$\circ$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Rozhodnite, či $(A, \circ)$ je grupoid, pologrupa, monoid, grupa, Abelova grupa. Prezradíme, že operácia $\circ$ je na množine A asociatívna

Riešenie:

Pretože vo výsledkovej časti Cayleho tabuľky sú iba prvky množiny A , je $(A, \circ)$ grupoid.

Pretože operácia $\circ$ je na množine A asociatívna, je $(A, \circ)$ pologrupa. Pretože neutrálnym prvkom je 1, je $(A, \circ)$ monoid. Pretože 0 ani 2 nemajú inverzný prvok, $(A, \circ)$ nie je grupa.

Úloha:

Daná je binárna operácia $\circ$ pomocou Cayleho tabuľky a množina $A = \{1, 2, 3\}$.

$\circ$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Rozhodnite, či $(A, \circ)$ je grupoid, pologrupa, monoid, grupa, Abelova grupa.

Riešenie:

Pretože vo výsledkovej časti Cayleho tabuľky je aj prvok 0, ktorý nepatrí do množiny A , $(A, \circ)$ nie je grupoid. Teda nemôže byť ani pologrupa, ani monoid, ani grupa.

Úloha:

Daná je binárna operácia $\circ$ na množine $A = \{0, 1, 2, 3\}$ pomocou Cayleho tabuľky.

$\circ$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Rozhodnite, či $(A, \circ)$ je grupoid, pologrupa, monoid, grupa, Abelova grupa. Prezradíme, že operácia $\circ$ je na množine A asociatívna

Riešenie:

Pretože vo výsledkovej časti Cayleho tabuľky sú iba prvky množiny A , je $(A, \circ)$ grupoid.

Pretože operácia $\circ$ je na množine A asociatívna, je $(A, \circ)$ pologrupa. Pretože neutrálnym prvkom je 0, je $(A, \circ)$ monoid. Pretože 0 má inverzný prvok 0, 1 má inverzný prvok 3, 2 má inverzný prvok 2, 3 má inverzný prvok 1 a operácia je komutatívna, je $(A, \circ)$ Abelova grupa.

Nasledujúce dve vety nám ukážu dôležité vlastnosti, ktoré majú grupy. Po každej vete si ukážeme jej aplikáciu na známych príkladoch. Ako prvé si predstavíme zákony o krátení.

Nech $(G, *)$ je grupa. Potom pre všetky prvky a, b, c z množiny G platí:

1. ak $a * c = b * c$, potom $a = b$, (pravidlo o krátení sprava)

2. ak $a * b = a * c$, potom $a = c$. (pravidlo o krátení zľava)

Pri sčítaní nám zákon o krátení hovorí asi toľko, že k oboj stranám rovnice môžeme pričítať a od oboj strán rovnice môžeme odčítať to isté číslo.

Teda:

- ak $a + 3 = b + 3$, potom $a = b$,
- ak $7x + 11 = 13y + 11$, potom $7x = 13y$,
- ak $7x + 11 = 13y + 15$, potom $7x = 13y + 4$,
- ak $a = b + 3$, potom $a - 5 = b - 2$.

Pri násobení nám zákon o krátení hovorí asi toľko, že obe strany rovnice môžeme vynásobiť tým istým nenulovým číslom alebo ich týmto číslom vydeliť.

Teda:

- ak $3 \cdot a = 3 \cdot b$, potom $a = b$,
- ak $11 \cdot a = 22 \cdot b$, potom $a = 2b$,
- ak $7 \cdot x + 7 = 14 \cdot y$, potom $x + 1 = 2 \cdot y$,
- ak $x = y + 3$, potom $3 \cdot x = 3 \cdot y + 9$,
- ak $a = 4 \cdot b + 5$, potom $4 \cdot a = 16 \cdot b + 20$.

Samozrejme, zákony o krátení neplatia iba pre sčítanie a násobenie, ale v ľubovoľnej grupe.

Teraz si ukážeme, že ak $(A, *)$ nie je grupa, ale iba pologrupa, tak zákon o krátení platiť nemusí.

Nech je daná binárna operácia $\circ$ na množine $A = \{0, 1, 2, 3\}$ pomocou Cayleho tabuľky.

$\circ$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(A, \circ)$ je pologrupa. Neutrálnym prvkom je 1. Pretože 0 ani 2 nemajú inverzný prvok, $(A, \circ)$ nie je grupa.

Všimnime si, že $2 \circ 1 = 2, 2 \circ 3 = 2$, teda $2 \circ 1 = 2 \circ 3$, ale $1 \neq 3$, teda zákon o krátení zľava neplatí. Podobne $1 \circ 2 = 2, 3 \circ 2 = 2$, teda $1 \circ 2 = 3 \circ 2$, ale $1 \neq 3$, teda zákon o krátení sprava

neplatí. Teda v monoide $(A, \circ)$ by sme rovnicu $2 \circ x = 2 \circ 3$ nemohli upraviť na $x = 3$, lebo jej riešením je aj $x = 1$.

Teraz si uvedieme tvrdenie o počte riešení lineárnej rovnice.

Nech $(G, *)$ je grupa. Nech a, b sú ľubovoľné prvky z množiny G . Potom existujú jednoznačne určené prvky x_0 a y_0 z množiny G také, že:

1. x_0 je riešenie rovnice $a * x = b$,

2. y_0 je riešenie rovnice $y * a = b$.

Už na základnej škole sme si zvykli, že rovnice typu $\square + x = \square$ a $x + \square = \square$, kde do štvorčiek môžeme vložiť ľubovoľné dve čísla (rovnaké alebo rôzne), majú vždy jedno riešenie. Riešili sme ich takto:

$$5 + x = 11$$

$$x = 11 - 5$$

$$x = 6$$

$$11 + x = 4$$

$$x = 4 - 11$$

$$x = -7$$

$$x + 9 = 3$$

$$x = 3 - 9$$

$$x = -6$$

Podobne sme si zvykli, že rovnice typu $\square \cdot x = \square$ a $x \cdot \square = \square$, kde do štvorčiek môžeme vložiť ľubovoľné dve čísla (rovnaké alebo rôzne, do prvého štvorčeka však rôzne od nuly), majú vždy jedno riešenie. Riešili sme ich takto:

$$5 \cdot x = 15$$

$$x = 15 : 5$$

$$x = 3$$

$$11 \cdot x = 132$$

$$x = 132 : 11$$

$$x = 12$$

$$x \cdot 9 = -3$$

$$x = (-3) : 9$$

$$x = -\frac{1}{3}$$

Takto sme tieto rovnice mohli riešiť preto, lebo množina reálnych čísel tvorí spolu s operáciou sčítania grupu. Podobne, množina nenulových reálnych čísel tvorí spolu s operáciou násobenia grupu. Preto sme do prvého štvorčeka v rovniciach s násobením nemohli vložiť nulu.

A ako je to s násobením celých čísel?

Keď násobíme dve kladné čísla, máme na to množstvo vhodných modelov. Predstavme si, že mamička má 3 deti a každému dá vreckové 5 Eur. Na to potrebuje 15 Eur. Zrejme $3 \cdot 5 = 15$.

Čo ak násobíme kladné číslo so záporným? Predstavme si záporné číslo ako dlžobu. Ak si od 3 veriteľov požičiame po 150 Eur, budeme mať dlh 450 Eur. Zrejme $3 \cdot (-150) = (-450)$.

Modely pre násobenie dvoch záporných čísel však už také prirodzené nie sú. Vidíme však, že je užitočné, aby číselná množina tvorila spolu s operáciou násobenia grupu. V nej musia platiť zákony o krátení.

Koľko teda má byť $(-2) \cdot (-3)$?

Ak by to bolo -6 , potom by neplatil zákon o krátení, lebo $(-2) \cdot (-3) = -6$, ale aj $2 \cdot (-3) = -6$.

Podľa zákona o krátení by muselo platiť, že $2 = -2$, a to neplatí.

Aby množina nenulových celých čísel bola grupou, musí teda platiť, že $(-2) \cdot (-3) = 6$.

Podobne možno zdôvodniť aj to, že $2 - (-3) = 2 + 3$.

2. Algebrické štruktúry s dvoma operáciami

V predchádzajúcej kapitole sme sa oboznámili s algebrickými štruktúrami s jednou operáciou. Vysvetlili sme si, čo znamenajú pojmy grupoid, pologrupa, momoid, grupa.

V tejto kapitole sa budeme venovať dvom binárnym operáciám definovaným na tej istej množine. Vysvetlíme si pojmy polookruh, okruh, teleso, pole a obor integrity.

Nakoľko teória algebrických štruktúr s dvoma operáciami je veľmi bohatá, ale pomerne náročná, obmedzíme naše úvahy a vysvetlenia najmä na číselné množiny a na operácie sčítania a násobenia.

Najprv si vždy uvedieme definíciu nového pojmu a potom si uvedieme príklady na tento pojem.

Ak chcete, aby sa vám definície zdali zrozumiteľnejšie, predstavujte si pod množinou G množinu reálnych čísel, pod operáciou $\oplus$ sčítanie a pod operáciou $\otimes$ násobenie.

Nech je daná neprázdna množina G , na ktorej sú definované dve binárne operácie $\oplus$ a $\otimes$. Potom trojicu $(G, \oplus, \otimes)$ nazývame polookruh, ak platí:

- 1. $(G, \oplus)$ je komutatívna pologrupa,**
- 2. $(G, \otimes)$ je pologrupa,**
- 3. operácia $\otimes$ je distributívna vzhľadom na operáciu $\oplus$.**

Polookruh je teda taká neprázdna množina, na ktorej sú definované dve binárne operácie. Navyiac, prvá z operácií musí byť komutatívna, obe musia byť asociatívne a druhá z operácií musí byť distributívna vzhľadom na prvú.

Teraz obmedzíme naše úvahy na množiny prirodzených, celých, racionálnych a reálnych čísel. Budeme uvažovať operácie sčítania a násobenia. Obe tieto operácie sú komutatívne a asociatívne. Navyiac, násobenie je distributívne vzhľadom na sčítanie.

Už vieme, že $(N,+)$ je pologrupa. Taktiež vieme, že $(N,\cdot)$ je pologrupa. Preto $(N,+,\cdot)$ je polookruh.

Podobne platí, že $(Z,+,\cdot)$, $(Q,+,\cdot)$ a $(R,+,\cdot)$ sú polookruhy.

Nech je daná neprázdna množina G , na ktorej sú definované dve binárne operácie $\oplus$ a $\otimes$. Potom trojicu $(G,\oplus,\otimes)$ nazývame okruh, ak platí:

- 1. $(G,\oplus)$ je komutatívna grupa,**
- 2. $(G,\otimes)$ je pologrupa,**
- 3. operácia $\otimes$ je distributívna vzhľadom na operáciu $\oplus$.**

V čom je teda rozdiel medzi polookruhom a okruhom?

V polookruhu je $(G,+)$ komutatívna pologrupa, zatiaľ čo v okruhu je to komutatívna grupa.

Už vieme, že $(N,+)$ je pologrupa, ale nie je grupa. Preto polookruh $(N,+,\cdot)$ nie je okruh.

Taktiež už vieme, že $(Z,+)$, $(Q,+)$ a $(R,+)$ sú komutatívne (Abelove) grupy. Preto polookruhy $(Z,+,\cdot)$, $(Q,+,\cdot)$ a $(R,+,\cdot)$ sú okruhy.

Teraz si predstavíme niekoľko pojmov súvisiacich s okruhmi.

Nech $(G,\oplus,\otimes)$ je okruh. Potom:

1. Grupu $(G, \oplus)$ nazývame aditívna grupa okruhu.
2. Pologrupu $(G, \otimes)$ nazývame multiplikatívna pologrupa okruhu.
3. Neutrálny prvok grupy $(G, \oplus)$ voláme nulový prvok okruhu a označujeme ho 0 .
4. Ak má pologrupa $(G, \otimes)$ jednotkový prvok, potom ho voláme jednotkovým prvkom okruhu a označujeme ho 1 . Okruh $(G, \oplus, \otimes)$ potom nazývame okruh s jednotkovým prvkom.

5. Ak je operácia $\cdot$ komutatívna, potom okruh $(G, \oplus, \otimes)$ nazývame komutatívny okruh.
6. Inverzný prvok k prvku a vzhľadom na operáciu $\oplus$ označujeme $-a$.

Okruhy $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ sú teda komutatívne okruhy s jednotkovým prvkom.

Teraz si uvedieme dve tvrdenia, ktoré platia v ľubovoľnom okruhu a ilustrujeme si ich v okruhu $(\mathbb{R}, +, \cdot)$. Prvé sa bude týkať násobenia nulou, druhé násobenia kladných a záporných čísel.

Nech $(G, \oplus, \otimes)$ je okruh. Nech 0 je neutrálny prvok grupy $(G, \oplus)$. Potom pre každý prvok a z množiny G platí $0 \otimes a = 0$ a $a \otimes 0 = 0$.

Toto tvrdenie nám teda hovorí, že ak je jedným z operandov druhej operácie (multiplikatívnej) v okruhu nulový prvok prvej operácie (aditívnej), výsledkom je vždy nulový prvok.

V okruhu reálnych čísel s operáciami sčítania a násobenia to potom znamená, že ak akékoľvek reálne číslo násobíme nulou, výsledkom je vždy nula.

Teraz si dokážeme predchádzajúce tvrdenie.

Nech $(G, \oplus, \otimes)$ je okruh. Nech 0 je neutrálny prvok grupy $(G, \oplus)$. Potom pre každý prvok a z množiny G platí $0 \otimes a = 0$ a $a \otimes 0 = 0$.

Najprv si dvoma rôznymi spôsobmi vyjadríme $a \otimes a$.

$$a \otimes a = a \otimes (a + 0) = a \otimes a + a \otimes 0 \quad \dots \text{použili sme pričítanie nuly a distributívny zákon}$$

$$a \otimes a = a \otimes a + 0 \quad \dots \text{použili sme pričítanie nuly}$$

Pravé strany výrazov dáme do rovnosti a použijeme zákon o krátení v grupe.

$$a \otimes a + a \otimes 0 = a \otimes a + 0$$

$$a \otimes 0 = 0$$

Podobne sa dokáže aj vzťah $0 \otimes a = 0$.

Nech $(G, \oplus, \otimes)$ je okruh. Nech a, b sú ľubovoľné prvky z množiny G . Potom platí:

1. $-(a \otimes b) = (-a) \otimes b$

2. $-(a \otimes b) = a \otimes (-b)$

3. $(-a) \otimes (-b) = a \otimes b$

V okruhu reálnych čísel s operáciami sčítania a násobenia toto tvrdenie znamená, že ak násobíme dve záporné čísla, výsledkom je kladné číslo a ak násobíme kladné číslo so záporným, výsledok je záporný.

Najprv si dokážeme rovnosť $-(a \otimes b) = (-a) \otimes b$.

Urobíme to tak, že ukážeme, že prvok na pravej i ľavej strane je inverzný k prvku $a \otimes b$.

Pretože inverzný prvok môže byť iba jeden, rovnosť bude dokázaná.

Prvok na ľavej strane je inverzným prvkom k prvku $a \otimes b$, čo vyplýva hneď z jeho zápisu.

$$\text{Teraz počítajme } (a \otimes b) \oplus [(-a) \otimes b] = [a + (-a)] \otimes b = 0 \otimes b = 0.$$

Teda aj prvok $(-a) \otimes b$ je inverzným prvkom k prvku $a \otimes b$, z čoho vyplýva,

$$\text{že } -(a \otimes b) = (-a) \otimes b.$$

Podobne sa dokáže aj to, že $-(a \otimes b) = a \otimes (-b)$.

Teraz pomocou týchto dvoch vzťahov počítajme $(-a) \otimes (-b)$.

$$(-a) \otimes (-b) = -[a \otimes (-b)] = -[-(a \otimes b)] = a \otimes b$$

Tým je celé tvrdenie dokázané.

Teraz sa oboznámime s pojmami telesa a poľa.

Nech $(G, \oplus, \otimes)$ je okruh s jednotkovým prvkom 1, ktorý je rôzny od nulového prvku. Potom $(G, \oplus, \otimes)$ je teleso, ak každý nenulový prvok množiny G má inverzný prvok vzhľadom na operáciu $\otimes$.

V čom sa teda líši okruh a teleso?

Zatiaľ čo pri okruhu nám stačilo, aby $(G, \otimes)$ bola pologrupa, pri telese navyše vyžadujeme, aby $(G - \{0\}, \otimes)$ bola grupa.

Teleso $(G, \oplus, \otimes)$, v ktorom je operácia $\otimes$ komutatívna, nazývame pole.

V čom sa teda líši pole a teleso? V poli žiadame, aby boli komutatívne obe operácie.

Nakoľko my sa sústreďujeme najmä na množinu reálnych čísel a na nej sú operácie sčítania aj násobenia komutatívne, nebudeme sa bližšie rozdielmi medzi telesom a poľom zaoberať.

Už vieme, že $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ sú komutatívne okruhy s jednotkovým prvkom.

Rovnako vieme, že $(\mathbb{Z} - \{0\}, \cdot)$ nie je grupa, zatiaľ čo $(\mathbb{Q} - \{0\}, \cdot)$ a $(\mathbb{R} - \{0\}, \cdot)$ sú grupy.

Preto $(\mathbb{Z}, +, \cdot)$ nie je pole, zatiaľ čo $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ sú polia.

Pri násobení reálnych čísel platí, že ak chceme, aby výsledkom bola nula, potom musí byť aspoň jeden z činiteľov nulový. Je to preto, lebo reálne čísla sú oborom integrity. Tento pojem si teraz vysvetlíme.

Nech $(G, \oplus, \otimes)$ je okruh. Nech a, b sú ľubovoľné prvky množiny G rôzne od nulového prvku. Nech $a \otimes b = 0$. Potom prvky a, b nazývame netriviálne delitele nuly. Triviálnym deliteľom nuly je iba nulový prvok okruhu.

Pojem netriviálnych deliteľov nuly si nemožno vysvetliť v okruhu reálnych čísel, pretože v ňom neexistujú. V ďalšom texte však nájdeme jednu úlohu, v ktorej sa vyskytnú.

Okruh $(G, \oplus, \otimes)$, ktorý neobsahuje netriviálne delitele nuly, nazývame oborom integrity.

Pretože reálne čísla neobsahujú delitele nuly, sú oborom integrity. Podobne aj racionálne a celé čísla.

Presnejšie: Okruhy $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ sú obormi integrity.

Uvedomme si, že z definície oboru integrity vyplýva nasledujúce tvrdenie.³

Nech $(G, \oplus, \otimes)$ je oborom integrity a nech a, b sú ľubovoľné prvky množiny G rôzne od nulového prvku. Potom $a \otimes b \neq 0$.

Teda súčinom dvoch nenulových čísel je vždy nenulové číslo.

Napokon si uvedieme vzťah medzi telesom a oborom integrity, resp. medzi oborom integrity a poľom.

Každé teleso $(G, \oplus, \otimes)$ je oborom integrity.

Každé pole $(G, \oplus, \otimes)$ je oborom integrity.

Teraz si pojmy polokruh, okruh, teleso, pole a obor integrity precvičíme na úlohách.

Úloha:

Daná je množina párnych prirodzených čísel $G = \{2, 4, 6, 8, 10, 12, \dots\}$ a operácie sčítania a násobenia. Rozhodnite, či $(G, +, \cdot)$ je polokruh, okruh, obor integrity, teleso, pole.

Riešenie:

Pretože súčtom aj súčinom dvoch párnych prirodzených čísel je opäť párne prirodzené číslo, sú operácie $+$ a $\cdot$ binárnymi operáciami na množine G . Navyše vieme, že sú komutatívne, asociatívne a platí aj distributívny zákon. Preto $(G, +)$ aj $(G, \cdot)$ sú komutatívne pologrupy, z čoho vyplýva, že $(G, +, \cdot)$ je polookruh.

Neutrálnym prvkom operácie $+$ je nula a tá nepatrí do množiny G . Teda $(G, +)$ nie je komutatívna grupa. Preto $(G, +, \cdot)$ nie je okruh.

Úloha:

Daná je množina celých čísel $G = \{\dots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \dots\}$, ktoré sú násobkami čísla 3. Ďalej sú dané operácie sčítania a násobenia. Rozhodnite, či $(G, +, \cdot)$ je polokruh, okruh, obor integrity, teleso, pole.

Riešenie:

Pretože súčtom aj súčinom dvoch čísel z množiny G je opäť číslo z množiny G , sú operácie $+$ a $\cdot$ binárnymi operáciami na množine G . Navyše vieme, že sú komutatívne, asociatívne a platí aj distributívny zákon. Preto $(G, +)$ aj $(G, \cdot)$ sú komutatívne pologrupy, z čoho vyplýva, že $(G, +, \cdot)$ je polookruh.

Neutrálnym prvkom operácie $+$ je nula a tá patrí do množiny G . Inverzným prvkom k 0 je 0, k 3 je -3 , k 6 je -6 , atď. Teda $(G, +)$ je komutatívna grupa. Preto $(G, +, \cdot)$ je okruh. **po**

Pretože súčinom dvoch nenulových čísel je vždy nenulové číslo, je $(G, +, \cdot)$ obor integrity.

Neutrálnym prvkom operácie $\cdot$ je číslo 1 a to nepatrí do množiny G . Teda $(G - \{0\}, \cdot)$ nie je komutatívna grupa. Preto $(G, +, \cdot)$ nie je ani teleso, ani pole.

Úloha:

Daná je množina nepárnych prirodzených čísel $G = \{1, 3, 5, 7, 9, 11, \dots\}$ a operácie sčítania a násobenia. Rozhodnite, či $(G, +, \cdot)$ je polokruh, okruh, obor integrity, teleso, pole.

Riešenie:

Pretože súčtom dvoch nepárnych prirodzených čísel nie je nepárne prirodzené číslo, operácia $+$ nie je binárnou operáciou na množine G . Teda $(G, +)$ nie je pologrupa. Preto $(G, +, \cdot)$ nie je polookruh, a teda ani okruh, obor integrity, teleso, pole.

Úloha:

Dané sú binárne operácie $\oplus, \otimes$ na množine $G = \{0, 1, 2\}$ pomocou Cayleho tabuľky.

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Rozhodnite, či $(G, +, \cdot)$ je polokruh, okruh, obor integrity, teleso, pole.

Prezradíme vám, že obe operácie sú asociatívne a operácia $\otimes$ je distributívna vzhľadom na operáciu $\oplus$.

Riešenie:

Pretože vo výsledkovej časti Cayleho tabuliek sú iba prvky množiny G , sú $\oplus, \otimes$ binárnymi operáciami na množine G . Pretože sú obe komutatívne aj asociatívne, sú $(G, \oplus)$ aj $(G, \otimes)$ komutatívne pologrupy. Pretože operácia $\otimes$ je distributívna vzhľadom na operáciu $\oplus$, je $(G, +, \cdot)$ polookruh.

Neutrálnym prvkom operácie $\oplus$ je číslo 0. Inverzným prvkom k 0 je 0, k 1 je 2 a k 2 je 1. Preto $(G, \oplus)$ je komutatívna grupa. Teda $(G, +, \cdot)$ je okruh.

Pretože operácia $\otimes$ nemá netriviálne delitele nuly, je okruh $(G, +, \cdot)$ aj oborom integrity. Neutrálnym prvkom operácie $\otimes$ je číslo 1. Inverzným prvkom k 1 je 1, k 2 je 2. Preto $(G - \{0\}, \otimes)$ je komutatívna grupa. Teda $(G, +, \cdot)$ je teleso a aj pole.

Úloha:

Dané sú binárne operácie $\oplus, \otimes$ na množine $G = \{0, 1, 2, 3\}$ pomocou Cayleho tabuľky.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Rozhodnite, či $(G, +, \cdot)$ je polokruh, okruh, obor integrity, teleso, pole.

Prezradíme vám, že obe operácie sú asociatívne a operácia $\otimes$ je distributívna vzhľadom na operáciu $\oplus$.

Riešenie:

Pretože vo výsledkovej časti Cayleho tabuliek sú iba prvky množiny G , sú $\oplus, \otimes$ binárnymi operáciami na množine G . Pretože sú obe komutatívne aj asociatívne, sú $(G, \oplus)$ aj $(G, \otimes)$ komutatívne pologrupy. Pretože operácia $\otimes$ je distributívna vzhľadom na operáciu $\oplus$, je $(G, +, \cdot)$ polookruh.

Neutrálnym prvkom operácie $\oplus$ je číslo 0. Inverzným prvkom k 0 je 0, k 1 je 3, k 2 je 2 a k 3 je 1. Preto $(G, \oplus)$ je komutatívna grupa. Teda $(G, +, \cdot)$ je okruh.

Operácia $\otimes$ má netriviálneho deliteľa nuly. Je ním číslo 2, pretože $2 \otimes 2 = 0$. Preto okruh $(G, +, \cdot)$ nie je oborom integrity, teda ani telesom a ani poľom.

3. Číselné množiny ako štruktúry

V tejto časti si zhrnieme doterajšie poznatky o prirodzených, celých, racionálnych a reálnych číslach vo vzťahu k pojmom grupoid, pologrupa, monoid, grupa, polookruh, okruh, obor integrity, teleso a pole.

Taktiež sa zoznámime s určitými významnými podmnožinami množín celých a reálnych čísel a s ich vzťahom k vyššie uvedeným pojmom. Zoznámime sa aj s operáciami sčítania a násobenia modulo n .

Prirodzené čísla

Presnú definíciu množiny prirodzených čísel si vysvetlíme neskôr. Teraz sa uspokojíme s tým, že pod množinou prirodzených čísel rozumieme množinu $N = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots\}$.

Všimnime si, že nulu nepovažujeme za prirodzené číslo.

Už vieme, že operácie sčítania a násobenia sú komutatívne aj asociatívne na množine prirodzených čísel. Navyše, operácia násobenia je distributívna vzhľadom na operáciu sčítania. Preto dvojice $(N, +)$ a $(N, \cdot)$ sú pologrupy a trojica $(N, +, \cdot)$ je polookruh.

Neutrálnym prvkom vzhľadom na násobenie je číslo 1. Okrem tohto čísla žiadne iné číslo nemá inverzný prvok vzhľadom na násobenie. Preto $(N, \cdot)$ je monoid, ale nie je grupa.

Neutrálnym prvkom vzhľadom na sčítanie je číslo 0, ktoré však nepatrí do množiny N . Preto $(N, +)$ nie je monoid, a teda ani grupa. Potom $(N, +, \cdot)$ nie je okruh.

Operácie odčítania a delenia nie sú binárnymi operáciami na množine prirodzených čísel, nakoľko nemožno určiť výsledok napríklad pre $4 - 8$ alebo $4 : 8$. (výsledkom nie sú prirodzené čísla)

Celé nezáporné čísla

Pod množinou celých nezáporných čísel rozumieme zjednotenie množiny prirodzených čísel a jednoprvkovej množiny obsahujúcej číslo 0. Zvyčajne ju označujeme $N_0 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots\}$.

Už vieme, že operácie sčítania a násobenia sú komutatívne aj asociatívne na množine celých nezáporných čísel. Navyše, operácia násobenia je distributívna vzhľadom na operáciu sčítania. Preto dvojice $(N_0, +)$ a $(N_0, \cdot)$ sú pologrupy a trojica $(N_0, +, \cdot)$ je polookruh.

Neutrálnym prvkom vzhľadom na násobenie je číslo 1. Okrem tohto čísla žiadne iné číslo nemá inverzný prvok vzhľadom na násobenie. Preto $(N_0, \cdot)$ je monoid, ale nie je grupa.

Neutrálnym prvkom vzhľadom na sčítanie je číslo 0. Okrem tohto čísla žiadne iné číslo nemá inverzný prvok vzhľadom na sčítanie. Preto $(N_0, +)$ je monoid, ale nie je grupa. Potom $(N_0, +, \cdot)$ nie je okruh.

Operácie odčítania a delenia nie sú binárnymi operáciami na množine celých nezáporných čísel, nakoľko nemožno určiť výsledok napríklad pre $4 - 8$ alebo $4 : 8$. (výsledkom nie sú celé nezáporné čísla)

Celé čísla

Presnú definíciu množiny celých čísel si vysvetlíme v kurze „Celé, racionálne, reálne čísla“. Podobne to bude aj s racionálnymi číslami. Teraz sa uspokojíme s tým, že pod množinou celých čísel rozumieme množinu $Z = \{\dots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \dots\}$.

Už vieme, že operácie sčítania a násobenia sú komutatívne aj asociatívne na množine celých čísel. Navyše, operácia násobenia je distributívna vzhľadom na operáciu sčítania. Preto dvojice $(Z, +)$ a $(Z, \cdot)$ sú pologrupy a trojica $(Z, +, \cdot)$ je polookruh.

Neutrálnym prvkom vzhľadom na násobenie je číslo 1. Okrem tohto čísla a čísla -1 žiadne iné číslo nemá inverzný prvok vzhľadom na násobenie. Preto $(Z, \cdot)$ je monoid, ale nie je grupa.

Neutrálnym prvkom vzhľadom na sčítanie je číslo 0. Každé celé číslo z má vzhľadom na sčítanie inverzný prvok, ktorým je číslo $-z$. Preto $(Z, +)$ je grupa. Potom $(Z, +, \cdot)$ je okruh.

Pretože súčinom dvoch nenulových čísel je opäť nenulové číslo, je $(Z, +, \cdot)$ obor integrity.

Operácia odčítania je binárnou operáciou na množine celých čísel, pretože rozdielom dvoch celých čísel je vždy celé číslo. Operácia delenia nie je binárnou operáciou na množine celých čísel, nakoľko nemožno určiť výsledok napríklad pre $4 : 8$. (výsledkom nie je celé číslo)

Racionálne čísla

Teraz sa uspokojíme s tým, že pod množinou racionálnych čísel rozumieme množinu čísel, ktorá sa dá vyjadriť v tvare zlomku $\frac{a}{b}$, $a \in Z, b \in N$.

Už vieme, že operácie sčítania a násobenia sú komutatívne aj asociatívne na množine racionálnych čísel. Operácia násobenia je distributívna vzhľadom na operáciu sčítania. Neutrálnym prvkom vzhľadom na násobenie je číslo 1. Okrem nuly všetky čísla majú inverzný prvok vzhľadom na násobenie (získame ho „zámenou čitateľa a menovateľa“). Preto $(Q, \cdot)$ je monoid, ale nie je grupa a $(Q - \{0\}, \cdot)$ je grupa.

Neutrálnym prvkom vzhľadom na sčítanie je číslo 0. Každé racionálne číslo má vzhľadom na sčítanie inverzný prvok, ktorým získame zmenou znamienka. Preto $(Q, +)$ je grupa. Potom $(Q, +, \cdot)$ je okruh, obor integrity, teleso a aj pole.

Operácia odčítania je binárnou operáciou na množine racionálnych čísel, pretože rozdielom dvoch racionálnych čísel je vždy racionálne číslo. Operácia delenia nie je binárnou operáciou na množine racionálnych čísel, nakoľko nemožno deliť nulou. Je však binárnou operáciou na množine $Q - \{0\}$.

Reálne čísla

Množinu reálnych čísel zatiaľ budeme chápať intuitívne tak, ako sme ju chápali počas štúdia na strednej škole.

Už vieme, že operácie sčítania a násobenia sú komutatívne aj asociatívne na množine reálnych čísel. Operácia násobenia je distributívna vzhľadom na operáciu sčítania. Neutrálnym prvkom vzhľadom na násobenie je číslo 1. Okrem nuly všetky čísla r majú

inverzný prvok vzhľadom na násobenie (je to číslo $1 : r$). Preto $(R, \cdot)$ je monoid, ale nie je grupa a $(R - \{0\}, \cdot)$ je grupa.

Neutrálnym prvkom vzhľadom na sčítanie je číslo 0. Každé reálne číslo má vzhľadom na sčítanie inverzný prvok, ktorým získame zmenou znamienka. Preto $(R, +)$ je grupa. Potom $(R, +, \cdot)$ je okruh, obor integrity, teleso a aj pole.

Operácia odčítania je binárnou operáciou na množine reálnych čísel, pretože rozdielom dvoch reálnych čísel je vždy reálne číslo. Operácia delenia nie je binárnou operáciou na množine reálnych čísel, nakoľko nemožno deliť nulou. Je však binárnou operáciou na množine $R - \{0\}$.

Párne prirodzené čísla

Pod množinou párných prirodzených čísel rozumieme množinu $N_p = \{2, 4, 6, 8, 10, 12, \dots\}$.

Pretože súčtom aj súčinom dvoch párných prirodzených čísel je opäť párne prirodzené číslo, sú sčítanie aj násobenie binárnymi operáciami na množine párných prirodzených čísel. Už vieme, že operácie sčítania a násobenia sú komutatívne aj asociatívne na množine párných prirodzených čísel. Navyše, operácia násobenia je distributívna vzhľadom na operáciu sčítania. Preto dvojice $(N_p, +)$ a $(N_p, \cdot)$ sú pologrupy a trojica $(N_p, +, \cdot)$ je polookruh.

Neutrálnym prvkom vzhľadom na násobenie je číslo 1, ktoré nepatrí do množiny N_p . Preto $(N_p, \cdot)$ nie je monoid, teda ani grupa.

Neutrálnym prvkom vzhľadom na sčítanie je číslo 0, ktoré nepatrí do množiny N_p . Preto $(N_p, +)$ nie je monoid, a teda ani grupa. Potom $(N_p, +, \cdot)$ nie je okruh.

Operácie odčítania a delenia nie sú binárnymi operáciami na množine párných prirodzených čísel, nakoľko nemožno určiť výsledok napríklad pre $4 - 8$ alebo $4 : 8$. (výsledkom nie sú párne prirodzené čísla)

Nepárne prirodzené čísla

Pod množinou nepárných prirodzených čísel rozumieme množinu $N_n = \{1, 3, 5, 7, 9, 11, \dots\}$.

Pretože súčtom dvoch nepárných prirodzených čísel nie je nepárne prirodzené číslo, sčítanie nie je binárnou operáciou na množine nepárných prirodzených čísel. Preto $(N_n, +)$ nie je ani grupoid a $(N_n, +, \cdot)$ nie je ani polookruh.

Súčinom dvoch nepárných prirodzených čísel je nepárne prirodzené číslo. Preto násobenie je binárnou operáciou na množine nepárných prirodzených čísel. Už vieme, že operácia násobenia je komutatívna aj asociatívna na množine nepárných prirodzených čísel. Preto dvojica $(N_n, \cdot)$ je pologrupa.

Neutrálnym prvkom vzhľadom na násobenie je číslo 1. Žiadne iné číslo však nemá inverzný prvok vzhľadom na násobenie. Preto $(N_n, \cdot)$ je monoid, ale nie je grupa.

Operácie odčítania a delenia nie sú binárnymi operáciami na množine nepárnych prirodzených čísel, nakoľko nemožno určiť výsledok napríklad pre $3 - 7$ alebo $3 : 7$. (výsledkom nie sú nepárne prirodzené čísla)

Množina $Z_2 = \{2k : k \in \mathbb{Z}\}$

Pod množinou $Z_2 = \{2k : k \in \mathbb{Z}\}$ rozumieme množinu

$$Z_2 = \{\dots, -12, -10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, 12, \dots\}.$$

Vidíme, že súčtom aj súčinom dvoch čísel z množiny Z_2 je opäť číslo z množiny Z_2 . Preto sčítanie aj násobenie sú binárnymi operáciami na množine Z_2 . Už vieme, že operácie sčítania a násobenia sú komutatívne aj asociatívne na množine Z_2 . Navyše, operácia násobenia je distributívna vzhľadom na operáciu sčítania. Preto dvojice $(Z_2, +)$ a $(Z_2, \cdot)$ sú pologrupy a trojica $(Z_2, +, \cdot)$ je polookruh.

Neutrálnym prvkom vzhľadom na násobenie je číslo 1, ktoré nepatrí do Z_2 . Preto $(Z_2, \cdot)$ nie je monoid, a teda ani grupa.

Neutrálnym prvkom vzhľadom na sčítanie je číslo 0. Každé číslo z z množiny Z_2 má vzhľadom na sčítanie inverzný prvok, ktorým je číslo $-z$ z množiny Z_2 . Preto $(Z_2, +)$ je grupa. Potom $(Z_2, +, \cdot)$ je okruh. Pretože súčinom dvoch nenulových čísel zo Z_2 je opäť nenulové číslo zo Z_2 , je $(Z_2, +, \cdot)$ obor integrity. Nie je však teleso ani pole.

Množina $Z_n = \{n \cdot k : k \in \mathbb{Z}\}$

Pod množinou $Z_3 = \{3k : k \in \mathbb{Z}\}$ rozumieme množinu $Z_3 = \{\dots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \dots\}$.

Pod množinou $Z_4 = \{4k : k \in \mathbb{Z}\}$ rozumieme množinu $Z_4 = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$.

Pod množinou $Z_5 = \{5k : k \in \mathbb{Z}\}$ rozumieme množinu $Z_5 = \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}$.

Pod množinou $Z_n = \{n \cdot k : k \in \mathbb{Z}\}$ rozumieme množinu $Z_n = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\}$ pre ľubovoľné pevne zvolené prirodzené číslo n väčšie ako 1.

Množina Z_n má rovnaké vlastnosti ako množina Z_2 . Teda dvojice $(Z_n, +)$ a $(Z_n, \cdot)$ sú pologrupy a trojica $(Z_n, +, \cdot)$ je polookruh.

$(Z_n, \cdot)$ nie je monoid, a teda ani grupa.

$(Z_n, +)$ je grupa a $(Z_n, +, \cdot)$ je okruh a aj obor integrity. Nie je však teleso ani pole.

Iracionálne čísla

Pojem iracionálneho čísla si najprv podrobnejšie vysvetlíme.

Už na základnej škole sme sa stretli s Pytagorovou vetou. Podľa nej preponu c pravouhlého trojuholníka s odvesnami a , b vypočítame podľa vzorca $c = \sqrt{a^2 + b^2}$. (možno je nám známejší vzorec $c^2 = a^2 + b^2$)

Vezmime si pravouhlý trojuholník, ktorého obe odvesny majú dĺžku 1. Potom podľa tohto vzorca má jeho prepona dĺžku $c = \sqrt{1^2 + 1^2} = \sqrt{1+1} = \sqrt{2}$.

Pokúsme sa vyjadriť číslo $\sqrt{2}$ v tvare zlomku $\frac{p}{q}$, $p \in \mathbb{Z}, q \in \mathbb{N}, (p, q) = 1$. (posledný výraz znamená, že čísla p a q sú nesúdeliteľné, teda že ich najväčším spoločným deliteľom je číslo 1)

Nech $\frac{p}{q} = \sqrt{2}$. Potom zrejme $\frac{p^2}{q^2} = 2$, z čoho vyplýva, že $p^2 = 2q^2$.

Urobme si rozklad čísla p na súčin prvočísel. Nech sa v ňom dvojka nachádza s exponentom k (k je nezáporné celé číslo). Potom v rozklade čísla p^2 na súčin prvočísel sa dvojka nachádza s exponentom $2k$.

Podobne si urobme rozklad čísla q na súčin prvočísel. Nech sa v ňom dvojka nachádza s exponentom l (l je nezáporné celé číslo). Potom v rozklade čísla q^2 na súčin prvočísel sa dvojka nachádza s exponentom $2l$ a teda v rozklade čísla $2q^2$ na súčin prvočísel sa dvojka nachádza s exponentom $2l+1$.

Vidíme, že rozklade čísla p^2 na súčin prvočísel sa dvojka nachádza s párnym exponentom a v rozklade čísla $2q^2$ na súčin prvočísel sa dvojka nachádza s nepárnym exponentom. Nakoľko vieme, že rozklad čísla na súčin prvočísel je jednoznačne určený, nemôže nastať rovnosť $p^2 = 2q^2$, z čoho vyplýva, že $\sqrt{2}$ sa nedá vyjadriť v tvare zlomku.

Vidíme teda, že číslo $\sqrt{2}$ nie je racionálne.

Podobne by sme vedeli ukázať, že racionálne nie sú ani čísla $\sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}$, $\sqrt[3]{2}, \sqrt[3]{3}, \sqrt[3]{4}, \sqrt[3]{5}$ a mnohé ďalšie.

Pri výpočte obvodu kružnice sme sa na základnej škole stretli s číslom, ktoré sme označovali π . Ani toto číslo nie je racionálne, dôkaz je však omnoho zložitejší.

Vidíme teda, že v množine reálnych čísel sa nachádza množstvo čísel, ktoré nie sú racionálne. Takéto čísla nazývame iracionálne čísla. Množinu iracionálnych čísel označíme $R - \mathbb{Q}$.

Teda iracionálnymi číslami sú napríklad:

$$\sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, -\sqrt{3}, -\sqrt{5}, -\sqrt{6}, -\sqrt{7}, -\sqrt{8},$$

$$\sqrt[3]{2}, \sqrt[3]{3}, \sqrt[3]{4}, \sqrt[3]{5}, -\sqrt[3]{2}, -\sqrt[3]{3}, -\sqrt[3]{4}, -\sqrt[3]{5},$$

$$\pi,$$

$$e, \text{ (Eulerovo číslo)}$$

$$\sin 10^\circ, \cos 10^\circ, \operatorname{tg} 10^\circ, \operatorname{cotg} 10^\circ.$$

Ako je to s operáciami sčítania, odčítania, násobenia a delenia?

Operácia sčítania nie je binárnou operáciou na množine iracionálnych čísel, pretože súčtom dvoch iracionálnych čísel nie je vždy iracionálne číslo, ako vidíme na príklade $\sqrt{2} + (-\sqrt{2}) = 0$.

Ani operácia odčítania nie je binárnou operáciou na množine iracionálnych čísel, pretože rozdielom dvoch iracionálnych čísel nie je vždy iracionálne číslo, ako vidíme na príklade $\sqrt{2} - \sqrt{2} = 0$.

Ani operácia násobenia nie je binárnou operáciou na množine iracionálnych čísel, pretože súčinom dvoch iracionálnych čísel nie je vždy iracionálne číslo, ako vidíme na príklade $\sqrt{2} \cdot \sqrt{2} = 2$.

Napokon, ani operácia delenia nie je binárnou operáciou na množine iracionálnych čísel, pretože podielom dvoch iracionálnych čísel nie je vždy iracionálne číslo, ako vidíme na príklade $\sqrt{2} : \sqrt{2} = 1$.

Teda $(R-Q, +), (R-Q, -), (R-Q, \cdot), (R-Q, :)$ nie sú ani grupoidy.

Algebraické čísla

Pojem algebraického čísla si najprv podrobnejšie vysvetlíme na konkrétnych príkladoch.

Už na základnej škole sme riešili lineárne rovnice nasledujúceho typu:

$$\begin{array}{lll} 3x + 6 = 0 & 2x - 5 = 0 & -3x + 5 = 14 \\ 3x = -6 & 2x = 5 & -3x = 9 \\ x = -2 & x = \frac{5}{2} & x = -3 \end{array}$$

Čísla a, b v rovnici $a \cdot x + b = 0$ sme nazývali koeficienty a volili sme za ne ľubovoľné racionálne čísla.

Neskôr sme riešili aj kvadratické rovnice nasledujúceho typu:

$$\begin{array}{ll} 2x^2 - 6x - 56 = 0 & 3x^2 - 6x - 5 = 0 \\ D = (-6)^2 - 4 \cdot 2 \cdot (-56) = 36 + 448 = 484 & D = (-6)^2 - 4 \cdot 3 \cdot (-5) = 36 + 60 = 96 \\ \sqrt{D} = \sqrt{484} = 22 & \sqrt{D} = \sqrt{96} \\ x_1 = \frac{-(-6) + 22}{2 \cdot 2} = \frac{28}{4} = 7 & x_1 = \frac{-(-6) + \sqrt{96}}{2 \cdot 3} = \frac{6 + \sqrt{96}}{6} \\ x_2 = \frac{-(-6) - 22}{2 \cdot 2} = \frac{-16}{4} = -4 & x_2 = \frac{-(-6) - \sqrt{96}}{2 \cdot 3} = \frac{6 - \sqrt{96}}{6} \end{array}$$

Čísla a, b, c v rovnici $a \cdot x^2 + b \cdot x + c = 0$ sme nazývali koeficienty a volili sme za ne ľubovoľné racionálne čísla.

Ak by sme si zvolili ľubovoľnú rovnicu typu

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_2 x^2 + a_1 x + a_0 = 0,$$

za koeficienty $a_n, a_{n-1}, a_{n-2}, \dots, a_2, a_1, a_0$ by sme si zvolili ľubovoľné racionálne čísla a keby sme túto rovnicu vyriešili, dostali by sme jej korene. Tieto korene by boli algebraickými číslami.

Algebraické číslo je teda také číslo, ktoré je koreňom nejakej rovnice typu $a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_2 x^2 + a_1 x + a_0 = 0$, kde $a_n, a_{n-1}, a_{n-2}, \dots, a_2, a_1, a_0$ sú racionálne čísla.

Algebrickými číslami sú napríklad:

$\sqrt{2}$ a $-\sqrt{2}$, lebo sú koreňmi rovnice $x^2 = 2$,

$\sqrt{3}$ a $-\sqrt{3}$, lebo sú koreňmi rovnice $x^2 = 3$,

$\sqrt[3]{2}$, lebo je koreňom rovnice $x^3 = 2$,

$-\sqrt[3]{2}$, lebo je koreňom rovnice $x^3 = -2$.

Existujú aj také reálne čísla, ktoré nie sú algebrické. Takéto čísla nazývame transcendentné. Sú to napríklad π , e (Eulerovo číslo), $\sin 10^\circ$, $\cos 10^\circ$, $\operatorname{tg} 10^\circ$, $\operatorname{cotg} 10^\circ$.

Dá sa dokázať, že súčtom, súčinom, rozdielom a aj podielom algebrických čísel sú algebrické čísla. Dá sa dokonca dokázať, že množina algebrických čísel spolu s operáciami sčítania a násobenia tvorí pole, ale to presahuje rámec týchto učebných textov.

Pole $(Z_2, \oplus, \odot)$

Nech Z_2 je množina obsahujúca čísla 0 a 1. Nech sú na nej dané binárne operácie $\oplus, \odot$.

Operácia $\oplus$ priradí dvojici $[a, b]$ zvyšok po delení súčtu $a + b$ číslom 2 a operácia $\odot$ priradí dvojici $[a, b]$ zvyšok po delení súčinu $a \cdot b$ číslom 2.

Cayleho tabuľky operácií $\oplus, \odot$ vyzerajú takto:

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

Vidíme, že vo výsledkovej časti Cayleho tabuliek sú iba prvky množiny Z_2 . Teda $\oplus, \odot$ sú binárne operácie na množine Z_2 . Nakoľko obe tabuľky sú súmerné podľa hlavnej diagonály, sú obe operácie komutatívne.

Obe operácie sú aj asociatívne. Mohli by sme sa o tom presvedčiť overením týchto 8 rovností pre operáciu $\oplus$:

$$(0 \oplus 0) \oplus 0 = 0 \oplus (0 \oplus 0), (0 \oplus 0) \oplus 1 = 0 \oplus (0 \oplus 1), (0 \oplus 1) \oplus 0 = 0 \oplus (1 \oplus 0),$$

$$(0 \oplus 1) \oplus 1 = 0 \oplus (1 \oplus 1), (1 \oplus 0) \oplus 0 = 1 \oplus (0 \oplus 0), (1 \oplus 0) \oplus 1 = 1 \oplus (0 \oplus 1),$$

$$(1 \oplus 1) \oplus 0 = 1 \oplus (1 \oplus 0), (1 \oplus 1) \oplus 1 = 1 \oplus (1 \oplus 1) \text{ a analogických 8 rovností pre operáciu } \odot.$$

Operácia $\odot$ je distributívna vzhľadom na operáciu $\oplus$, o čom by sme sa presvedčili overením 8 rovností typu $(0 \oplus 1) \odot 1 = (0 \odot 1) \oplus (1 \odot 1)$ a 8 rovností typu $1 \odot (0 \oplus 1) = (1 \odot 0) \oplus (1 \odot 1)$.

Neutrálnym prvkom operácie $\oplus$ je 0. Inverzným prvkom k prvku 0 vzhľadom na operáciu $\oplus$ je 0 a inverzným prvkom k prvku 1 vzhľadom na operáciu $\oplus$ je 1. Preto $(Z_2, \oplus)$ je komutatívna (Abelova) grupa.

Neutrálnym prvkom operácie $\odot$ je 1. Inverzným prvkom k prvku 1 vzhľadom na operáciu $\odot$ je 1. Prvok 0 nemá inverzný prvok vzhľadom na operáciu $\odot$. Preto $(Z_2 - \{0\}, \odot)$ je komutatívna (Abelova) grupa.

Z uvedeného vyplýva, že $(Z_2, \oplus, \odot)$ je pole, a teda aj polookruh, okruh, obor integrity a teleso.

Pole $(Z_3, \oplus, \odot)$

S týmto poľom sme sa v tomto učebnom texte už stretli. Nech Z_3 je množina obsahujúca čísla 0, 1 a 2. Nech sú na nej dané binárne operácie $\oplus, \odot$. Operácia $\oplus$ priradí dvojici $[a, b]$ zvyšok po delení súčtu $a + b$ číslom 3 a operácia $\odot$ priradí dvojici $[a, b]$ zvyšok po delení súčinu $a \cdot b$ číslom 3. Cayleho tabuľky operácií $\oplus, \odot$ vyzerajú takto:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Vidíme, že vo výsledkovej časti Cayleho tabuliek sú iba prvky množiny Z_3 . Teda $\oplus, \odot$ sú binárne operácie na množine Z_3 . Nakoľko obe tabuľky sú súmerné podľa hlavnej diagonály, sú obe operácie komutatívne.

Obe operácie sú aj asociatívne. Mohli by sme sa o tom presvedčiť overením 27 rovností pre operáciu $\oplus$ typu $(1 \oplus 2) \oplus 0 = 1 \oplus (2 \oplus 0)$ a 27 rovností pre operáciu $\odot$ typu $(1 \odot 2) \odot 0 = 1 \odot (2 \odot 0)$.

Operácia $\odot$ je distributívna vzhľadom na operáciu $\oplus$, o čom by sme sa presvedčili overením 27 rovností typu $(0 \oplus 2) \odot 1 = (0 \odot 1) \oplus (2 \odot 1)$ a 27 rovností typu $1 \odot (2 \oplus 1) = (1 \odot 2) \oplus (1 \odot 1)$.

Neutrálnym prvkom operácie $\oplus$ je 0. Inverzným prvkom k prvku 0 vzhľadom na operáciu $\oplus$ je 0, k 1 je 2 a k 2 je 1. Preto $(Z_3, \oplus)$ je komutatívna (Abelova) grupa.

Neutrálnym prvkom operácie $\odot$ je 1. Inverzným prvkom k prvku 1 vzhľadom na operáciu $\odot$ je 1 a k 2 je 2. Prvok 0 nemá inverzný prvok vzhľadom na operáciu $\odot$. Preto $(Z_3 - \{0\}, \odot)$ je komutatívna (Abelova) grupa.

Z uvedeného vyplýva, že $(Z_3, \oplus, \odot)$ je pole, a teda aj polookruh, okruh, obor integrity a teleso.

Okruh $(Z_4, \oplus, \odot)$

S týmto okruhom sme sa v tomto učebnom texte už stretli. Nech Z_4 je množina obsahujúca čísla 0, 1, 2 a 3. Nech sú na nej dané binárne operácie $\oplus, \odot$. Operácia $\oplus$ priradí dvojici $[a, b]$ zvyšok po delení súčtu $a + b$ číslom 4 a operácia $\odot$ priradí dvojici $[a, b]$ zvyšok po delení súčinu $a \cdot b$ číslom 4. Cayleho tabuľky operácií $\oplus, \odot$ vyzerajú takto:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Vo výsledkovej časti Cayleho tabuliek sú iba prvky množiny Z_4 . Teda $\oplus, \odot$ sú binárne operácie na množine Z_4 . Tabuľky sú súmerné podľa hlavnej diagonály, teda obe operácie sú komutatívne.

Obe operácie sú aj asociatívne. Mohli by sme sa o tom presvedčiť overením 64 rovností pre operáciu $\oplus$ a 64 rovností pre operáciu $\odot$.

Operácia $\odot$ je distributívna vzhľadom na operáciu $\oplus$, o čom by sme sa presvedčili overením 128 rovností.

Neutrálnym prvkom operácie $\oplus$ je 0. Inverzným prvkom k prvku 0 vzhľadom na operáciu $\oplus$ je 0, k 1 je 3, k 2 je 2 a k 3 je 1. Preto $(Z_4, \oplus)$ je komutatívna (Abelova) grupa.

Neutrálnym prvkom operácie $\odot$ je 1. Vidíme, že 2 nemá inverzný prvok vzhľadom na operáciu $\odot$. Preto $(Z_4, \odot)$ je monoid a $(Z_4 - \{0\}, \odot)$ nie je grupa.

Z uvedeného vyplýva, že $(Z_4, \oplus, \odot)$ je okruh, teda aj polookruh. Nie je však oborom integrity, nakoľko má netriviálneho deliteľa (prvok 2). Rovnako nie je ani teleso a ani pole.

Okruhy $(Z_k, \oplus, \odot)$

Nech Z_k je množina obsahujúca celé čísla $0, 1, 2, \dots, k-1$. Nech sú na nej dané binárne operácie $\oplus, \odot$. Operácia $\oplus$ priradí dvojici $[a, b]$ zvyšok po delení súčtu $a + b$ číslom k a operácia $\odot$ priradí dvojici $[a, b]$ zvyšok po delení súčinu $a \cdot b$ číslom k .

Už sme sa dozvedeli, že $(Z_2, \oplus, \odot)$ a $(Z_3, \oplus, \odot)$ sú polia. Taktiež sme sa dozvedeli, že $(Z_4, \oplus, \odot)$ je okruh, avšak nie je pole a ani obor integrity.

Ako je to pre ľubovoľné celé číslo k väčšie ako 4?

Dá sa dokázať, že všetky trojice $(Z_k, \oplus, \odot)$ sú okruhy pre ľubovoľné celé číslo k väčšie ako 1. Tieto okruhy sú poliami (obormi integrity) práve vtedy, ak k je prvočíslo.

Úloha:

Zostrojte Cayleho tabuľku operácie $\odot$ v okruhu $(Z_6, \oplus, \odot)$. Ktoré čísla sú netriviálnymi deliteľmi nuly?

Riešenie:

$\odot$	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

Netriviálnymi deliteľmi nuly sú čísla 2, 3 a 4.