3 Algebraické štruktúry

3.1 Grupy

Riešené príklady:

Príklad 3.1.1 Zistite, či množina $\mathbb{Z}$ spolu s binárnou operáciou $\diamondsuit$ tvoria grupu, ak $a \diamondsuit b = a + b + 7$.
Riešenie:
Chceme ukázať, že $(\mathbb{Z}, \diamondsuit)$ je grupa. Podľa definície musíme ukázať, že platia nasledujúce vlastnosti:

- množina $\mathbb{Z}$ je **uzavretá** vzhľadom na binárnu operáciu $\diamondsuit$,
- platí **asociatívny zákon**,
- množina $\mathbb{Z}$ obsahuje **neutrálny prvok** vzhľadom na operáciu $\diamondsuit$,
- ku každému prvku z množiny $\mathbb{Z}$ existuje **inverzný prvok** vzhľadom na operáciu $\diamondsuit$.

Uzavretosť: Nech $a, b \in \mathbb{Z}$ a $a \diamondsuit b = a + b + 7$. Platí: $(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \Rightarrow (a + b \in \mathbb{Z})$. $(a + b \in \mathbb{Z} \wedge 7 \in \mathbb{Z}) \Rightarrow (a + b + 7 \in \mathbb{Z}) \Rightarrow a \diamondsuit b \in \mathbb{Z}$. Prvky a, b boli zvolené ľubovoľne z množiny $\mathbb{Z}$, preto množina $\mathbb{Z}$ je vzhľadom na binárnu operáciu $\diamondsuit$ uzavretá.
Asociatívnosť: Nech $a, b, c, \in \mathbb{Z}$.

$$(a \diamondsuit b) \diamondsuit c = (a \diamondsuit b) + c + 7 = (a + b + 7) + c + 7 = a + b + c + 14$$
$$a \diamondsuit (b \diamondsuit c) = a \diamondsuit (b + c + 7) = a + (b + c + 7) + 7 = a + b + c + 14.$$

Ukázali sme, že platí rovnosť: $a \diamondsuit (b \diamondsuit c) = a + b + c + 14 = (a \diamondsuit b) \diamondsuit c$. preto platí:

$$(\forall a, b, c \in \mathbb{Z}) : ((a \diamondsuit b) \diamondsuit c = a \diamondsuit (b \diamondsuit c)).$$

Odtiaľ dostávame, že pre množinu $\mathbb{Z}$ platí asociatívny zákon vzhľadom na binárnu operáciu $\diamondsuit$.
Neutrálny prvok: Chceme nájsť taký prvok ε, aby pre všetky prvky z množiny $\mathbb{Z}$ platila nasledujúca rovnosť:

$$a \diamondsuit \varepsilon = \varepsilon \diamondsuit a = a.$$

Vezmime si ľubovoľný prvok $a \in \mathbb{Z}$. K tomuto prvku a hľadáme prvok $\varepsilon \in \mathbb{Z}$ tak, aby platila rovnosť $a \diamondsuit \varepsilon = \varepsilon \diamondsuit a = a$. Z rovnosti $a \diamondsuit \varepsilon = a + \varepsilon + 7 = a$

dostávame, že ak za ε zvolime -7, tak je splnená vyššie uvedená rovnosť. Overme, či takto zvolené ε spĺňa podmienky neutrálneho prvku v grupe.

$$[(a\diamondsuit\varepsilon = a + (-7) + 7 = a) \wedge (\varepsilon\diamondsuit a = (-7) + a + 7 = a)] \Rightarrow$$

$$\Rightarrow (\exists\varepsilon \in \mathbb{Z})(\forall a \in \mathbb{Z}) : (a\diamondsuit\varepsilon = \varepsilon\diamondsuit a = a).$$

Neutrálnym prvkom je $\varepsilon = -7$.
Inverzný prvok: Ku každému prvku a z množiny $\mathbb{Z}$ hľadáme taký prvok a' z množiny $\mathbb{Z}$, aby platila nasledujúca rovnosť: $a\diamondsuit a' = \varepsilon$ $a'\diamondsuit a$. Vezmime si ľubovoľný prvok $a \in \mathbb{Z}$ Nájdine k takto vybranému prvku inverzný prvok a', ak taký v množine $\mathbb{Z}$ existuje. Pre inverzný prvok musí platiť:

$$\begin{aligned} a\diamondsuit a' &= \varepsilon \\ a + a' + 7 &= \varepsilon \quad \wedge \quad \varepsilon = -7 \\ a + a' + 7 &= -7 \\ a + a' &= -14 \\ a' &= -a - 14. \end{aligned}$$

Stačí už len ukázať, že takto vytvorený prvok k ľubovoľnému prvku z množiny $\mathbb{Z}$ je naozaj inverzným prvkom. Spočítajme:

$$a\diamondsuit a' = a + a' + 7 = a + (-a - 14) + 7 = a - a - 14 + 7 = -7 = \varepsilon$$
$$a'\diamondsuit a = a' + a + 7 = (-a - 14) + a + 7 = -a + a - 14 + 7 = -7 = \varepsilon$$

Uvedeným postupom sme našli ku každému prvku z množiny $\mathbb{Z}$ inverzný prvok, a teda sú splnené všetky 4 vlastnosti z definície grupy, preto množina $\mathbb{Z}$ s binárnou operáciou $\diamondsuit$ je grupa. $\surd$

Príklad 3.1.2 Zistite, či množina $\mathbb{Z}$ spolu s binárnou operáciou ✠ tvoria grupu, ak a ✠ $b = (a + b)^2$.
Riešenie:
Ak chceme ukázať, že $(\mathbb{Z}, ✠)$ je grupa, tak podľa definície musíme ukázať, že množina $\mathbb{Z}$ je **uzavretá** vzhľadom na binárnu operáciu ✠, platí **asociatívnosť**, obsahuje **neutrálny prvok** vzhľadom na operáciu ✠ a ku každému prvku z množiny $\mathbb{Z}$ existuje **inverzný prvok** vzhľadom na operáciu ✠. Ak by sme chceli ukázať, že $(\mathbb{Z}, ✠)$ nie je grupa, tak stačí ukázať, že jedna z vyššie uvedených vlastností nie je splnená. Overme asociatívnosť: Nech $a, b, c, \in \mathbb{Z}$: $(a$ ✠ $b)$ ✠ $c = ((a$ ✠ $b) + c)^2$ $((a + b)^2 + c)^2 = (a + b)^4 + 2(a + b)^2c + c^2$. Ak

ukážeme, že výraz $a \maltese (b \maltese c)$ sa rovná výrazu $(a+b)^4 + 2(a+b)^2c + c^2$, tak sme ukázali platnosť asociatívneho zákona. Platí: $a \maltese (b \maltese c) = a \maltese (b+c)^2$ $= (a + (b+c)^2)^2$ $a^2 + 2a(b+c)^2 + (b+c)^4$, z toho potom vyplýva, že

$$(a \maltese b) \maltese c \neq a \maltese (b \maltese c)$$

preto neplatí asociatívny zákon na množine $\mathbb{Z}$ vzhľadom na binárnu operáciu $\maltese$, a preto množina $\mathbb{Z}$ spolu s binárnu operáciu $\maltese$ netvorí grupu. $\surd$

Príklad 3.1.3 Zistite, či množina $\mathbb{Z}$ spolu s binárnou operáciou $\square$ tvoria grupu, ak $a \square b = a + b + a^b$.
Riešenie:
Podľa definície je $(\mathbb{Z}, \square)$ grupou, ak množina celých čísel $\mathbb{Z}$ spĺňať **uzavretosť**, **asociatívnosť**, obsahuje **neutrálny prvok** vzhľadom na binárnu operáciu $\square$ a ku každému prvku z množiny $\mathbb{Z}$ existuje **inverzný prvok** vzhľadom na operáciu $\square$.
Uzavretosť: Pre $a, b \in \mathbb{Z}$: $a \square b = a + b + a^b$.

$$\big[[(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \Rightarrow (a+b) \in \mathbb{Z}] \wedge a^b \notin \mathbb{Z}\big]^1 \Rightarrow$$
$$(a + b + a^b) \notin \mathbb{Z} \Rightarrow$$
$$(a \square b) \notin \mathbb{Z}.$$

Keďže sme našli také prvky a, b z množiny $\mathbb{Z}$, pre ktoré nie je splnená uzavretosť množiny $\mathbb{Z}$, preto množina $\mathbb{Z}$ nie je vzhľadom na binárnu operáciu $\square$ uzavretá, z čoho vyplýva, že $(\mathbb{Z},\ \square)$ netvorí grupu. $\surd$

Príklad 3.1.4 Zistite, či množina $A = \{\bigstar,\ \circledast,\ \circledcirc,\ \blacklozenge\}$ spolu s binárnou operáciou $\centerdot$ tvoria grupu, ak binárna operácia $\boxdot$ je daná Cayleyho tabuľkou:

$\boxdot$	$\bigstar$	$\circledast$	$\circledcirc$	$\blacklozenge$
$\bigstar$	$\blacklozenge$	$\circledcirc$	$\circledast$	$\bigstar$
$\circledast$	$\bigstar$	$\circledcirc$	$\circledast$	$\blacklozenge$
$\circledcirc$	$\blacklozenge$	$\circledast$	$\circledcirc$	$\bigstar$
$\blacklozenge$	$\circledast$	$\bigstar$	$\blacklozenge$	$\circledcirc$

Riešenie:
Chceme ukázať, že $(A, \boxdot)$ je grupa. Podľa definície musí byť množina A **uzavretá** vzhľadom na binárnu operáciu $\boxdot$, musí platiť **asociatívnosť**, obsahovať **neutrálny prvok** vzhľadom na operáciu $\boxdot$ a ku každému prvku z

množiny A musí existovať **inverzný prvok** vzhľadom na operáciu $\boxdot$.
Nájdime neutrálny prvok množiny A vzhľadom na binárnu operáciu $\boxdot$. Máme nájsť taký prvok $\varepsilon \in A$, pre ktorý platí:

$\forall a \in A$: $a \boxdot \varepsilon = \varepsilon \boxdot a = a$.

Vieme, že v každej grupe sa náchádza práve jeden neutrálny prvok a navyše množina A je konečná a obsahuje len 4 prvky, a preto môžme overiť neutralitu každého prvku množiny A samostatne. Nech $\varepsilon = \bigstar$, potom druhý riadok aj druhý stĺpec v Cayleyho tabuľke musí byť zhodný so vzorom (t.j. prvým stĺpcom a prvým riadkom). Ľahko vidieť, že $\varepsilon \boxdot \blacklozenge = \bigstar \neq \blacklozenge$. Podobnou úvahou zistíme, že ani pre $\varepsilon = \circledast$, $\varepsilon = \circledcirc$ a $\varepsilon = \blacklozenge$ nie je splnená podmienka neutrálneho prvku, preto množina A neobsahuje vzhľadom na binárnu operáciu $\boxdot$ neutrálny prvok. Z vyššie uvedených tvrdení vyplýva, že $(A, \boxdot)$ nie je grupa. $\surd$

Príklad 3.1.5 Zistite, či množina $\mathbb{Z} - \{0\}$ spolu s binárnou operáciou $\triangle$ tvoria grupu, ak $a \triangle b = ab$.
Riešenie:
Úlohou je rozhodnúť, či $(\mathbb{Z} - \{0\}, \triangle)$ je grupa. Z definície vyplýva, že musia byť splnené nasledujúce vlastnosti:

- množina $\mathbb{Z} - \{0\}$ je **uzavretá** vzhľadom na binárnu operáciu $\triangle$,
- platí **asociatívny zákon**,
- množina $\mathbb{Z} - \{0\}$ obsahuje **neutrálny prvok** vzhľadom na operáciu $\triangle$
- ku každému prvku z množiny $\mathbb{Z} - \{0\}$ musí existovať **inverzný prvok** vzhľadom na operáciu $\triangle$.

Uzavretosť: Nech $a, b \in \mathbb{Z} - \{0\}$: $a \triangle b = ab$. Ak $a \in \mathbb{Z} - \{0\}$ a $b \in \mathbb{Z} - \{0\}$, potom $ab \in \mathbb{Z} - \{0\}$ (súčin je nenulový, lebo $a \neq 0$ aj $b \neq 0$, a teda aj $ab \neq 0$). Z toho potom dostávame, že $a \triangle b \in \mathbb{Z} - \{0\}$, pre ľubovoľné prvky a, b z množiny $\mathbb{Z} - \{0\}$. Tým sme ukázali, že množina $\mathbb{Z} - \{0\}$ je vzhľadom na binárnu operáciu $\triangle$ uzavretá.
Asociatívnosť: Pre $a, b, c, \in \mathbb{Z} - \{0\}$ platí:

$$(a \triangle b) \triangle c = (a \triangle b)c = (ab)c = abc$$
$$a \triangle (b \triangle c) = a \triangle (bc)\ a(bc) = abc$$

Z uvedených rovností vyplýva: $\forall a, b, c \in \mathbb{Z} - \{0\}$: $(a \triangle b) \triangle c = a \triangle (b \triangle c)$, preto pre množinu $\mathbb{Z} - \{0\}$ platí asociatívny zákon vzhľadom na binárnu operáciu $\triangle$.

Neutrálny prvok: Chceme nájsť taký prvok ε, aby pre všetky prvky z množiny $\mathbb{Z}-\{0\}$ platila nasledujúca rovnosť: $a \triangle \varepsilon \; \varepsilon \triangle a = a$. Vezmime si ľubovoľný prvok $a \in \mathbb{Z}-\{0\}$. K tomuto prvku a hľadáme prvok $\varepsilon \in \mathbb{Z}-\{0\}$ tak, aby platila rovnosť $a \triangle \varepsilon = a\varepsilon = a$. Ak $\varepsilon = 1$, tak je splnená vyššie uvedená rovnosť. Overme, či takto zvolené ε spĺňa podmienky neutrálneho prvku. Pre ľubovoľné a z množiny $\mathbb{Z}-\{0\}$ platí: $a \triangle \varepsilon = a.1 = a, \quad \varepsilon \triangle a = 1.a = a$. Teda $(\exists \varepsilon \in \mathbb{Z}-\{0\})(\forall\, a \in \mathbb{Z}-\{0\})$: $a \triangle \varepsilon = \varepsilon \triangle a = a$. Neutrálnym prvkom je $\varepsilon = 1$.
Inverzný prvok: Ku každému prvku a z množiny $\mathbb{Z}-\{0\}$ hľadáme taký prvok a' z množiny $\mathbb{Z}-\{0\}$, aby platila nasledujúca rovnosť: $a \triangle a' \; \varepsilon = a' \triangle a$. Vezmime si ľubovoľný prvok $a \in \mathbb{Z}-\{0\}$ Nájdine k takto vybranému prvku inverzný prvok a', ak taký v množine $\mathbb{Z}-\{0\}$ existuje. Pre inverzný prvok musí platiť:

$$\begin{aligned} a \triangle a' &= \varepsilon \\ aa' &= \varepsilon \;\wedge\; \varepsilon = 1 \\ aa' &= 1 \\ a' &= \frac{1}{a}, \qquad \text{kde} \quad a \neq 0 \end{aligned}$$

Ukážeme, že takto vytvorený prvok k ľubovoľnému prvku z množiny $\mathbb{Z}-\{0\}$ nemusí byť prvkom z mnnožiny $\mathbb{Z}-\{0\}$. Nech $a = 2$. Potom platí:

$$\begin{aligned} a \triangle a' &= \varepsilon \\ aa' &= \varepsilon = 1 \\ a' &= \frac{1}{2} \end{aligned}$$

$\frac{1}{2} \notin \mathbb{Z}-\{0\}$, teda $(\nexists\, a' \in \mathbb{Z}-\{0\})\; (\forall a \in \mathbb{Z}-\{0\})$: $a \triangle a' = \varepsilon = 1$. Ukázali sme, že v množine $\mathbb{Z}-\{0\}$ neexistuje ku každému prvku inverzný prvok, preto množina $\mathbb{Z}-\{0\}$ s binárnou operáciou $\triangle$ nie je grupa. $\mathbb{R}$ $\surd$

Príklad 3.1.6 Pomocou Cayleyho tabuľky popíšte grupu transformácií generovanú symetriami štvorca.
Riešenie:
Vieme, že ak S je množina všetkých bodov v rovine, ktoré tvoria štvorec, tak permutácia $\pi : \; S \;\mapsto\; S$ sa nazýva **symetria** štvorca S, ak zachováva vzdialenosti. Inverzná funkcia π^{-1} je tiež symetriou štvorca, súčin dvoch symetrií množiny S je tiež symetria množiny S a identická funkcia $id : \; S \;\mapsto\; S$ je tiež

symetria. Z toho vyplýva, že množina všetkých symetrií štvorca S vzhľadom na skladanie symetrií je grupa (grupa symetrií štvorca).

Nech S je množina všetkých bodov v rovine na obvode štvorca $ABCD$. Každá symetria štvorca je určená tým, ako preskupíme vrcholy $ABCD$. Popíšme jednotlivé symetrie:

R_1 = otočenie o 90° proti smeru hodinových ručičiek,
R_2 = otočenie o 180°,
R_3 = otočenie o 270° a
R_4 = otočenie o 360° čo je vlastne identita id,
D_1 = osovo súmerné preklopenie štvorca S podľa priamky, ktorá prechádza stredmi strán AB a CD,
D_2 = osovo súmerné preklopenie štvorca S podľa priamky, ktorá prechádza stredmi strán AD a BC,
D_3 = osovo súmerné preklopenie štvorca S podľa priamky, ktorá prechádza bodmi A a C,
D_4 = osovo súmerné preklopenie štvorca S podľa priamky, ktorá prechádza bodmi B a D.

Štvorec S má poradie vrcholov $ABCD$. Zistime, ako sa zmení poradie týchto bodov po aplikovaní jednotlivých symetrií.

$$\begin{aligned}
R_1 &: ABCD \longrightarrow DABC \\
R_2 &: ABCD \longrightarrow CDAB \\
R_3 &: ABCD \longrightarrow BCDA \\
R_4 &: ABCD \longrightarrow ABCD \\
D_1 &: ABCD \longrightarrow BADC \\
D_2 &: ABCD \longrightarrow DCBA \\
D_3 &: ABCD \longrightarrow ADCB \\
D_4 &: ABCD \longrightarrow CBAD
\end{aligned}$$

Vypočítajme, čomu sa rovnajú súčiny (skladanie zobrazení) týchto symetrií. Súčin $R_1 \circ R_1$ znamená, že štvorec $ABCD$ otočíme podľa R_1 o 90° a dostaneme štvorec $DABC$, tento znovu otočíme podľa R_1 o 90° a dostaneme štvorec $CDAB$, čo zodpovedá otočeniu R_2. Môžme písať, že $R_1 \circ R_1 = R_2$. Podobne vypočítame aj $R_1 \circ R_2$, štvorec $ABCD$ najprv otočíme podľa R_2 o 180°, dostanem štvorec $CDAB$ a ten ešte otočíme podľa R_1 o 90° a dostaneme šrvorec $BCDA$, čo zodpovedá použitiu R_4. Týmto postupom spočítame

všetky súčiny otočení. Pozrime sa teraz na súčin $R_1 \circ D_1$. Najprv musíme štvorec $ABCD$ preklopiť podľa D_1 a dostaneme $BADC$ a ten ešte otočíme podľa R_1 o 90° a dostávame štvorec $CBAD$, čo zodpovedá symetrii D_4. Pri výpočte jednotlivých súčinov zistíme, že súčiny otočení je komutatívna operácia, ale súčiny so symetriami D_i už komutatívne nie sú. Platí, že $D_i \circ D_i$ id pre $i = 1, 2, 3, 4$, Všetky tieto výsledky môžme zhrnúť do prehľadnej Cayleyho tabuľky:

$\circ$	R_1	R_2	R_3	R_4	D_1	D_2	D_3	D_4
R_1	R_2	R_3	R_4	R_1	D_4	D_3	D_1	D_2
R_2	R_3	R_4	R_1	R_2	D_2	D_1	D_4	D_3
R_3	R_4	R_1	R_2	R_3	D_3	D_4	D_2	D_1
R_4	R_1	R_2	R_3	R_4	D_1	D_2	D_3	D_4
D_1	D_3	D_2	D_4	D_1	R_4	R_2	R_1	R_3
D_2	D_4	D_1	D_3	D_2	R_2	R_4	R_3	R_1
D_3	D_2	D_4	D_1	D_3	R_3	R_1	R_4	R_2
D_4	D_1	D_3	D_2	D_4	R_1	R_3	R_2	R_4

Táto tabuka je Cayleyho tabuľka grupy transformácií, ktorá je generovaná symetriami štvorca. $\surd$

Poznámka 3.1.1 *Vo všeobecnosti vieme, že každý rovnostranný n-uholník má práve 2n symetrií, n rotácií a n osovo súmerných preklopení. Všetky symetrie pravidelného n-uholníka tvoria grupu s 2n prvkami. Každej symetrii takéhoto rovnostranného n-uholníka prislúcha zodpovedajúca permutácia vrcholov tohto n-uholníka.*

3.2 Cyklické grupy

Riešené príklady:

Príklad 3.2.1 Nájdite rády všetkých prvkov v grupe $(\mathbb{Z}_{10};\ \oplus)$, kde $\oplus$ je binárna operácia sčítania zvyškových tried.
Riešenie:
Množina $\mathbb{Z}_{10}$ je množina zvyškových tried $\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{7},\ \overline{8},\ \overline{9}\}$. Ku každému prvku z tejto množiny vytvoríme ich mocniny (od prvej, až po tú, kde nenastane rovnosť s neutrálnym prvkom) vzhľadom na binárnu operáciu $\oplus$.

$\overline{0}^1 = \overline{0}$,
rád$(\overline{0}) = 1$.

$\overline{1}^1 = \overline{1}$,
$\overline{1}^2 = \overline{1} \oplus \overline{1} = \overline{2}$,
$\overline{1}^3 = \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{3}$,
$\overline{1}^4 = \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{4}$,
$\overline{1}^5 = \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{5}$,
$\overline{1}^6 = \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{6}$,
$\overline{1}^7 = \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{7}$,
$\overline{1}^8 = \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{8}$,
$\overline{1}^9 = \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{9}$,
$\overline{1}^{10} = \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{0}$,
rád$(\overline{1}) = 10$.

$\overline{2}^1 = \overline{2}$, $\overline{2}^2 = \overline{2} \oplus \overline{2} = \overline{4}$, $\overline{2}^3 = \overline{4} \oplus \overline{2} = \overline{6}$, $\overline{2}^4 = \overline{6} \oplus \overline{2} = \overline{8}$,
$\overline{2}^5 = \overline{8} \oplus \overline{2} = \overline{0}$,
rád$(\overline{2}) = 5$.

$\overline{3}^1 = \overline{3}$, $\overline{3}^2 = \overline{3} \oplus \overline{3} = \overline{6}$, $\overline{3}^3 = \overline{6} \oplus \overline{3} = \overline{9}$, $\overline{3}^4 = \overline{9} \oplus \overline{3} = \overline{2}$,
$\overline{3}^5 = \overline{2} \oplus \overline{3} = \overline{5}$, $\overline{3}^6 = \overline{5} \oplus \overline{3} = \overline{8}$, $\overline{3}^7 = \overline{8} \oplus \overline{3} = \overline{1}$, $\overline{3}^8 = \overline{1} \oplus \overline{3} = \overline{4}$,
$\overline{3}^9 = \overline{4} \oplus \overline{3} = \overline{7}$, $\overline{3}^{10} = \overline{7} \oplus \overline{3} = \overline{0}$,
rád$(\overline{3}) = 10$.

$\overline{4}^1 = \overline{4}$, $\overline{4}^2 = \overline{4} \oplus \overline{4} = \overline{8}$, $\overline{4}^3 = \overline{8} \oplus \overline{4} = \overline{2}$, $\overline{4}^4 = \overline{2} \oplus \overline{4} = \overline{6}$, $\overline{4}^5 = \overline{6} \oplus \overline{4} = \overline{0}$,
rád$(\overline{4}) = 5$.

$\overline{5}^1 = \overline{5}$, $\overline{5}^2 = \overline{5} \oplus \overline{5} = \overline{0}$,
rád$(\overline{5}) = 2$.

Podobným spôsobom ukážeme, rády ostatných prvkov množiny $\mathbb{Z}_{10}$. Rád$(\overline{6})$ = 5, rád$(\overline{7})$ 10, rád$(\overline{8}) = 5$, rád$(\overline{9}) = 10$. √

Príklad 3.2.2 Zistite, či $(\mathbb{Z}_7 - \{\overline{0}\};\ \otimes)$ je cyklická grupa.
Riešenie:
Chceme zistiť, či $(\mathbb{Z}_7 - \{\overline{0}\};\ \otimes)$ je cyklická grupa. Podľa definície musí v množine $\mathbb{Z}_7 - \{\overline{0}\}$ existovať aspoň jeden taký prvok, ktorý je jej generátorom. Nejaký prvok g je generátorom množiny $\mathbb{Z}_7 - \{\overline{0}\}$, ak ku každému prvku $a \in \mathbb{Z}_7 - \{\overline{0}\}$ existuje $n \in \mathbb{N}$ také, že $g^n = a$. Postupne overme prvky $a \in \mathbb{Z}_7 - \{\overline{0}\} = \{\overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6}\}$. Prvok $\overline{1}$ nemôže byť generátorom, lebo pre všetky $n \in \mathbb{N}$ platí, že $\overline{1}^n\overline{1}$. Pozrime sa, aké prvky generuje prvok $\overline{2}$. $\overline{2}^1 = \overline{2}$, $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{1}$, $\overline{2}^4 = \overline{2}$, $\overline{2}^5 = \overline{4}$, $\overline{2}^6 = \overline{1}$..., ľahko je vidieť, že prvok $\overline{2}$ generuje len prvky $\{\overline{1},\ \overline{2},\ \overline{4}\}$. Prvok $\overline{3}$ generuje tieto prvky: $\overline{3}^1 = \overline{3}$, $\overline{3}^2 = \overline{2}$, $\overline{3}^3 = \overline{6}$, $\overline{3}^4 = \overline{4}$, $\overline{3}^5 = \overline{5}$, $\overline{3}^6 = \overline{1}$. Prvok $\overline{3}$ generuje prvky $\{\overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6}\}$ a teda je generátorom množiny $\mathbb{Z}_7 - \{\overline{0}\}$. V množine $\mathbb{Z}_7 - \{\overline{0}\}$ sme našli generátor, preto $(\mathbb{Z}_7 - \{\overline{0}\};\ \otimes)$ je cyklická grupa. √

Príklad 3.2.3 Rozhodnite, či grupa $(\mathbb{Z}_5 - \{\overline{0}\};\ \otimes)$ je izomorfná s grupou $(K_4;\ \cdot)$.
Riešenie:
Ak chceme ukázať, že tieto grupy sú izomorfné, tak musíme nájsť také bijektívne zobrazenie $\varphi : \mathbb{Z}_5 - \{\overline{0}\} \longrightarrow K_4$, že pre každú dvojicu prvkov $a, b \in \mathbb{Z}_5 - \{\overline{0}\}$ platí rovnosť $\varphi(a \otimes b) = \varphi(a) \cdot \varphi(b)$. Pomôckou pri určení zobrazenia nám môžu byť Cayleyho tabuľky daných grúp a fakt, že izomorfné grupy musia mať rovnaké všetky vlastnosti. Pozrime sa na Cayleyho tabuľky grúp $(\mathbb{Z}_5 - \{\overline{0}\};\ \otimes)$ a $(K_4;\ \cdot)$.

$\otimes$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Ľahko zistíme, že obe grupy sú cyklické. Grupa $(\mathbb{Z}_5 - \{\overline{0}\};\ \otimes)$ má generátor $\overline{2}$ a grupa $(K_4,\ \cdot)$ má generátor i. Počet prvkov v oboch množinách je rovnaký. Neutrálnym prvkom grupy $(\mathbb{Z}_5 - \{\overline{0}\};\ \otimes)$ je $\overline{1}$ a grupy $(K_4,\ \cdot)$ je 1. Tiež je dobré poznať rády prvkov v grupe. Rád$(\overline{1}) = 1$, rád$(\overline{2}) = 4$, rád$(\overline{3}) = 4$, rád$(\overline{4}) = 2$, rád$(1) = 1$, rád$(-1) = 2$, rád$(i) = 4$, rád$(-i) = 4$. Ak máme dostatok informácii o každej grupe, potom pri definovaní izomorfizmu stačí dodržiavať jednoduché pravidlá. Neutrálny prvok sa má zobraziť na neutrálny prvok, prvok s rovnakým rádom, by sa mal zobraziť na prvok s rovnakým rádom a pri cyklických grupách by mal byť aj rovnaký počet generátorov. Definujme zobrazenie φ nasledovne:

$$\begin{aligned}\varphi(\overline{1}) &= 1\\ \varphi(\overline{2}) &= i\\ \varphi(\overline{3}) &= -i\\ \varphi(\overline{4}) &= -1\end{aligned}$$

Ešte overíme, že takto definované zobrazenie φ je naozaj izomorfizmom daných grúp.

$$\begin{aligned}
\varphi(\overline{1}\otimes\overline{1}) &= \boldsymbol{\varphi(\overline{1})} = \mathbf{1}, & \varphi(\overline{1})\cdot\varphi(\overline{1}) &= 1\cdot 1 = \mathbf{1}\\
\varphi(\overline{1}\otimes\overline{2}) &= \boldsymbol{\varphi(\overline{2})} = \boldsymbol{i}, & \varphi(\overline{1})\cdot\varphi(\overline{2}) &= 1\cdot i = \boldsymbol{i}\\
\varphi(\overline{1}\otimes\overline{3}) &= \boldsymbol{\varphi(\overline{3})} = \boldsymbol{-i}, & \varphi(\overline{1})\cdot\varphi(\overline{3}) &= 1\cdot -i = \boldsymbol{-i}\\
\varphi(\overline{1}\otimes\overline{4}) &= \boldsymbol{\varphi(\overline{4})} = \mathbf{-1}, & \varphi(\overline{1})\cdot\varphi(\overline{4}) &= 1\cdot -1 = \mathbf{-1}\\
\varphi(\overline{2}\otimes\overline{1}) &= \boldsymbol{\varphi(\overline{2})} = \boldsymbol{i}, & \varphi(\overline{2})\cdot\varphi(\overline{1}) &= i\cdot 1 = \boldsymbol{i}\\
\varphi(\overline{2}\otimes\overline{2}) &= \boldsymbol{\varphi(\overline{4})} = \mathbf{-1}, & \varphi(\overline{2})\cdot\varphi(\overline{2}) &= i\cdot i = \mathbf{-1}\\
\varphi(\overline{2}\otimes\overline{3}) &= \boldsymbol{\varphi(\overline{1})} = \mathbf{1}, & \varphi(\overline{2})\cdot\varphi(\overline{3}) &= i\cdot -i = \mathbf{1}\\
\varphi(\overline{2}\otimes\overline{4}) &= \boldsymbol{\varphi(\overline{3})} = \boldsymbol{-i}, & \varphi(\overline{2})\cdot\varphi(\overline{4}) &= i\cdot -1 = \boldsymbol{-i}\\
\varphi(\overline{3}\otimes\overline{1}) &= \boldsymbol{\varphi(\overline{3})} = \boldsymbol{-i}, & \varphi(\overline{3})\cdot\varphi(\overline{1}) &= -i\cdot 1 = \boldsymbol{-i}\\
\varphi(\overline{3}\otimes\overline{2}) &= \boldsymbol{\varphi(\overline{1})} = \mathbf{1}, & \varphi(\overline{3})\cdot\varphi(\overline{2}) &= -i\cdot i = \mathbf{1}
\end{aligned}$$

$$\begin{array}{llll}
\varphi(\overline{3}\otimes\overline{3}) = \boldsymbol{\varphi(\overline{4})} = \boldsymbol{-1}, & \varphi(\overline{3})\cdot\varphi(\overline{3}) = -i\cdot -i = \boldsymbol{-1} \\
\varphi(\overline{3}\otimes\overline{4}) = \boldsymbol{\varphi(\overline{2})} = \boldsymbol{i}, & \varphi(\overline{3})\cdot\varphi(\overline{4}) = -i\cdot -1 = \boldsymbol{i} \\
\varphi(\overline{4}\otimes\overline{1}) = \boldsymbol{\varphi(\overline{4})} = \boldsymbol{-1}, & \varphi(\overline{4})\cdot\varphi(\overline{1}) = -1\cdot 1 = \boldsymbol{-1} \\
\varphi(\overline{4}\otimes\overline{2}) = \boldsymbol{\varphi(\overline{3})} = \boldsymbol{-i}, & \varphi(\overline{4})\cdot\varphi(\overline{2}) = -1\cdot i = \boldsymbol{-i} \\
\varphi(\overline{4}\otimes\overline{3}) = \boldsymbol{\varphi(\overline{2})} = \boldsymbol{i}, & \varphi(\overline{4})\cdot\varphi(\overline{3}) = -1\cdot -i = \boldsymbol{i} \\
\varphi(\overline{4}\otimes\overline{4}) = \boldsymbol{\varphi(\overline{1})} = \boldsymbol{1}, & \varphi(\overline{4})\cdot\varphi(\overline{4}) = -1\cdot -1 = \boldsymbol{1}
\end{array}$$

Zo zvýraznených stĺpcov je zrejmé, že takto definované zobrazenie $\varphi : \mathbb{Z}_5 - \{\overline{0}\} \longrightarrow K_4$ je izomorfizmom daných grúp, a preto grupy $(\mathbb{Z}_5 - \{\overline{0}\};\ \otimes)$ a $(K_4;\ \cdot)$ sú izomorfné. $\surd$

3.3 Podgrupy a rozklady grúp

Riešené príklady:

Príklad 3.3.1 Nájdite všetky podgrupy grupy $(\mathbb{Z}_6;\ \oplus)$.
Riešenie:
Ak chceme k nejakej grupe nájsť všetky jej podgrupy, musíme o všetkých jej podmnožinách rozhodnúť, či tvoria grupu. Pre jednoduchosť stačí len rozhodnúť, či podmnožiny sú uzavreté vzhľadom na grupovú operáciu, a či ku každému prvku existuje inverzný prvok.

Pre cyklické grupy, je to ešte jednoduchšie. Vieme, že každá podgrupa cyklickej grupy je cyklická a rád grupy je celočíselným násobkom rádu jej podgrupy. Túto vlastnosť môžme využiť na určenie podmnožín, ktoré by mohli byť podgrupou danej grupy. Jednotlivé prvky cyklickej grupy nám vygenerujú podmnožiny a o týchto množinách rozhodneme, či sú podgrupamy danej grupy. Množina $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Prvky tejto množiny generujú nasledujúce podmnožiny množiny $\mathbb{Z}_6$.[2]

$$\begin{aligned}
\langle\overline{0}\rangle &= \{\overline{0}\}\\
\langle\overline{1}\rangle &= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}\\
\langle\overline{2}\rangle &= \{\overline{0}, \overline{2}, \overline{4}\}\\
\langle\overline{3}\rangle &= \{\overline{0}, \overline{3}\}\\
\langle\overline{4}\rangle &= \{\overline{0}, \overline{2}, \overline{4}\}\\
\langle\overline{5}\rangle &= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}
\end{aligned}$$

Týmto spôsobom sme získali štyri podmnožiny $H_1\{\overline{0}\}$, $H_2 = \{\overline{0}, \overline{3}\}$, $H_3 = \{\overline{0}, \overline{2}, \overline{4}\}$ a $H_4\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Ľahko sa ukáže, že $(H_i;\ \oplus)$ pre $i = 1, 2, 3, 4$ sú podgrupami grupy $(\mathbb{Z}_6;\ \oplus)$. $\surd$

Príklad 3.3.2 Rozhodnite, či množina $H = \left\langle \binom{1234}{1324} \right\rangle$ je podgrupou grupy $(\mathsf{S}_4, \circ)$.
Riešenie:
Ak chceme ukázať, že $(H, \circ)$ je podgrupou grupy $(\mathsf{S}_3, \circ)$, tak množina H musí byť uzavretá vzhľadom na binárnu operáciu $\circ$ a ku každému prvku z množiny H musí existovať inverzný prvok v množine H. Množina $H\left\{\binom{1234}{1234}, \binom{1234}{1324}\right\}$. Uzavretosť ukážeme pomocou Caleyho tabuľky.

[2]Symbolom $\langle\rangle$ budeme označovať množinu, ktorá je generovaná prvkami, ktoré sú umiestnené v týchto zátvorkách.

$\circ$	$\binom{1234}{1234}$	$\binom{1234}{1324}$
$\binom{1234}{1234}$	$\binom{1234}{1234}$	$\binom{1234}{1324}$
$\binom{1234}{1324}$	$\binom{1234}{1324}$	$\binom{1234}{1234}$

Z tejto tabuľky je vidieť, že množina H je uzavretá vzhľadom na binárnu operáciu $\circ$ a každý prvok z množiny H je zároveň aj sám k sebe inverzným prvkom. Množina H spolu s grupovou operáciou $\circ$ tvoria podgrupu grupy $(\mathsf{S}_4, \circ)$. $\surd$

Príklad 3.3.3 Nájdite ľavý aj pravý rozklad grupy $(\mathbb{Z}_8;\ \oplus)$ podľa podgrupy $(H;\ \oplus)$ a určte index podgrupy $(H;\ \oplus)$, ak $H = \{\overline{0}, \overline{4}\}$.
Riešenie:
Pravý rozklad grupy $(\mathbb{Z}_8;\ \oplus)$ podľa podgrupy $(H;\ \oplus)$ je množina $G/H^{PR} = \{xH;\ x \in G\}$, kde $xH = \{x \oplus h;\ h \in H\}$. Ľavým rozkladom je množina $G/H^{LR} = \{Hx;\ x \in G\}$, kde $Hx = \{h \oplus x;\ h \in H\}$. Indexom podgrupy $(H;\ \oplus)$ v grupe $(\mathbb{Z}_8;\ \oplus)$ rozumieme mohutnosť množiny G/H. Spočítajme, čomu sa rovnajú množiny xH a Hx.

$$\begin{aligned}
\overline{0}H &= \{\overline{0}, \overline{4}\} & H\overline{0} &= \{\overline{0}, \overline{4}\}\\
\overline{1}H &= \{\overline{1}, \overline{5}\} & H\overline{1} &= \{\overline{1}, \overline{5}\}\\
\overline{2}H &= \{\overline{2}, \overline{6}\} & H\overline{2} &= \{\overline{2}, \overline{6}\}\\
\overline{3}H &= \{\overline{3}, \overline{7}\} & H\overline{3} &= \{\overline{3}, \overline{7}\}\\
\overline{4}H &= \{\overline{4}, \overline{0}\} & H\overline{4} &= \{\overline{4}, \overline{0}\}\\
\overline{5}H &= \{\overline{5}, \overline{1}\} & H\overline{5} &= \{\overline{5}, \overline{1}\}\\
\overline{6}H &= \{\overline{6}, \overline{2}\} & H\overline{6} &= \{\overline{6}, \overline{2}\}\\
\overline{7}H &= \{\overline{7}, \overline{3}\} & H\overline{7} &= \{\overline{7}, \overline{3}\}
\end{aligned}$$

Keďže $(\mathbb{Z}_8;\ \oplus)$ je abelovská grupa, tak ľavý a pravý rozklad sa rovná. Z vyššie uvedeného výpočtu je vidieť, že rozklad grupy $(\mathbb{Z}_8;\ \oplus)$ podľa podgrupy $(H;\ \oplus)$ je množina $G/H = \{\{\overline{0}, \overline{4}\}, \{\overline{1}, \overline{5}\}, \{\overline{2}, \overline{6}\}, \{\overline{3}, \overline{7}\}\}$. Index podgrupy $(H;\ \oplus)$ je 4. $\surd$

3.4 Okruhy, telesá a polia

Riešené príklady:

Príklad 3.4.1 Zistite, či $(A;\ +,\ \cdot)$ je okruh, ak $A = \{a + b\sqrt[3]{4};\ a, b \in \mathbb{Q}\}$.
Riešenie:
Algebraický systém $(A;\ +,\ \cdot)$ je okruhom, ak sú splnené nasleduj[úce tri vlastnosti:

1. $(A;\ +)$ je komutatívna grupa
2. $(A;\ \cdot)$ je pologrupa
3. binárna operácia $\cdot$ je distributívna vzhľadom na operáciu $+$.

1. Overme, či $(A;\ +)$ je komutatívna grupa t.j.

– uzavretosť množiny A vzhľadom na binárnu operáciu $+$,
– asociatívny zákon,
– existenciu neutrálneho prvku,
– existenciu inverzných prvkov,
– komutatívny zákon.

Uzavretosť: Nech $x_1, x_2 \in A$: $x_1 = a_1 + b_1\sqrt[3]{4}$ a $x_2 = a_2 + b_2\sqrt[3]{4}$, kde $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

$x_1 + x_2 = a_1 + b_1\sqrt[3]{4} + a_2 + b_2\sqrt[3]{4} = a_1 + a_2 + b_1\sqrt[3]{4} + b_2\sqrt[3]{4} =$
$= (a_1 + a_2) + (b_1 + b_2)\sqrt[3]{4} = a + b\sqrt[3]{4} = x \in A$, kde $a = a_1 + a_2$,
$b = b_1 + b_2$ a $a, b \in \mathbb{Q}$.

Keďže x_1, x_2 sme na začiatku zvolili ľubovoľné, tak množina A je uzavretá vzhľadom na binárnu operáciu $+$.
Asociatívnosť: Nech $x_1, x_2, x_3 \in A$: $x_1 = a_1 + b_1\sqrt[3]{4}$, $x_2 = a_2 + b_2\sqrt[3]{4}$ a $x_3 = a_3 + b_3\sqrt[3]{4}$, kde $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Q}$.

$x_1 + (x_2 + x_3) = a_1 + b_1\sqrt[3]{4} + (a_2 + b_2\sqrt[3]{4} + a_3 + b_3\sqrt[3]{4}) =$
$= a_1 + a_2 + a_3 + (b_1 + b_2 + b_3)\sqrt[3]{4}$
$(x_1 + x_2) + x_3 = (a_1 + b_1\sqrt[3]{4} + a_2 + b_2\sqrt[3]{4}) + a_3 + b_3\sqrt[3]{4} =$
$= a_1 + a_2 + a_3 + (b_1 + b_2 + b_3)\sqrt[3]{4}$

Z uvedených úprav je zrejmé, že $x_1 + (x_2 + x_3)$ $(x_1 + x_2) + x_3$. Teda pre ľubovoľné x_1, x_2, x_3 platí asociatívny zákon.
Neutrálny prvk: Nech $x \in A$ a $e = 0 + 0\sqrt[3]{4}$, kde $x = a + b\sqrt[3]{4}$, $a, b \in \mathbb{Q}$. Je zrejmé, že prvok e je z množiny A. Stačí ukázať, že $x + e = e + x = x$.

$$x + e = (a + b\sqrt[3]{4}) + (0 + 0\sqrt[3]{4}) = (a + 0) + (b + 0)\sqrt[3]{4} =$$
$$= a + b\sqrt[3]{4} = x$$
$$e + x = (0 + 0\sqrt[3]{4}) + (a + b\sqrt[3]{4}) = (0 + a) + (0 + b)\sqrt[3]{4} =$$
$$= a + b\sqrt[3]{4} = x$$

Ukázali sme, že e je neutrálnym prvkom množiny A vzhľadom na binárnu operáciu $+$.
Inverzný prvok: Nech $x, x' \in A$: $x = a + b\sqrt[3]{4}$ a $x' = -a - b\sqrt[3]{4}$, kde $a, b \in \mathbb{Q}$.

$$x + x' = (a + b\sqrt[3]{4}) + (-a - b\sqrt[3]{4}) = (a - a) + (b - b)\sqrt[3]{4} =$$
$$= 0 + 0\sqrt[3]{4} = e$$
$$x' + x = (-a - b\sqrt[3]{4}) + (a + b\sqrt[3]{4}) = (-a + a) + (-b + b)\sqrt[3]{4} =$$
$$= 0 + 0\sqrt[3]{4} = e$$

Ku každému prvku z množiny A existuje v množine A k nemu inverzný prvok. Zatiaľ sme ukázali, že $(A;\ +)$ je grupa.
Komutatívnosť: Nech $x_1, x_2 \in A$: $x_1 a_1 + b_1\sqrt[3]{4}$ a $x_2 = a_2 + b_2\sqrt[3]{4}$, kde $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

$$x_1 + x_2 = (a_1 + b_1\sqrt[3]{4}) + (a_2 + b_2\sqrt[3]{4}) = (a_1 + a_2) + (b_1 + b_2)\sqrt[3]{4} =$$
$$= (a_2 + a_1) + (b_2 + b_1)\sqrt[3]{4} = (a_2 + b_2\sqrt[3]{4}) + (a_1 + b_1\sqrt[3]{4}) = x_2 + x_1$$

Platí komutatívny zákon, z čoho vyplýva, že $(A;\ +)$ je komutatívna grupa.

2. Musíme ukázať, že $(A;\ \cdot)$ je pologrupa t.j. musí platiť:

– uzavretosť,
– asociatívnosť.

Uzavretosť: Nech $x_1, x_2 \in A$: $x_1 = a_1 + b_1\sqrt[3]{4}$ a $x_2 = a_2 + b_2\sqrt[3]{4}$, kde $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

$$x_1 \cdot x_2 = (a_1 + b_1\sqrt[3]{4}) \cdot (a_2 + b_2\sqrt[3]{4}) =$$
$$= a_1 \cdot a_2 + a_1 \cdot b_2\sqrt[3]{4} + b_1\sqrt[3]{4} \cdot a_2 + b_1\sqrt[3]{4} \cdot b_2\sqrt[3]{4} =$$
$$= a_1 \cdot a_2 + (a_1 \cdot b_2 + b_1 \cdot a_2 + b_1 \cdot b_2\sqrt[3]{4})\sqrt[3]{4}$$

Výraz $(a_1 \cdot b_2 + b_1 \cdot a_2 + b_1 \cdot b_2\sqrt[3]{4}) \notin \mathbb{Q}$ pre žiadne $a_i, b_i \in \mathbb{Q}$, $i = 1.\ 2$, preto $x_1 \cdot x_2 \notin A$. Množina A nie je uzavretá vzhľadom na binárnu operáciu $\cdot$, preto $(A;\ \cdot)$ nie je pologrupa, z čoho vyplýva, že $(A;\ +,\ \cdot)$ nie je okruh. $\surd$

Príklad 3.4.2 Zistite, či $(A;\ +,\ \cdot)$ je oborom integrity, ak $A = \{a + b\sqrt{5};\ a, b \in \mathbb{Q}\}$.
Riešenie:
Algebraický systém $(A;\ +,\ \cdot)$ je oborom integrity, ak je okruhom s aspoň dvoma prvkami bez netriviálnych deliteľov nuly. Najprv musíme ukázať, že algebraický systém $(A;\ +,\ \cdot)$ je okruhom t.j.

1. $(A;\ +)$ je komutatívna grupa
2. $(A;\ \cdot)$ je pologrupa
3. binárna operácia $\cdot$ je distributívna vzhľadom na operáciu $+$.

1. Overme, či $(A;\ +)$ je komutatívna grupa t.j.

– uzavretosť množiny A vzhľadom na binárnu operáciu $+$,
– asociatívny zákon,
– existenciu neutrálneho prvku,
– existenciu inverzných prvkov,
– komutatívny zákon.

Uzavretosť: Nech $x_1, x_2 \in A$: $x_1 = a_1 + b_1\sqrt{5}$ a $x_2 = a_2 + b_2\sqrt{5}$, kde $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

$$x_1 + x_2 = a_1 + b_1\sqrt{5} + a_2 + b_2\sqrt{5} = a_1 + a_2 + b_1\sqrt{5} + b_2\sqrt{5} =$$
$$= (a_1 + a_2) + (b_1 + b_2)\sqrt{5} = a + b\sqrt{5}\ x \in A,$$
kde $a = a_1 + a_2$, $b = b_1 + b_2$ a $a, b \in \mathbb{Q}$

Prvky x_1, x_2 sme na začiatku zvolili ľubovoľné, preto množina A je uzavretá vzhľadom na binárnu operáciu $+$.
Asociatívnosť: Nech $x_1, x_2, x_3 \in A$: $x_1 = a_1 + b_1\sqrt{5}$, $x_2 = a_2 + b_2\sqrt{5}$ a $x_3 = a_3 + b_3\sqrt{5}$, kde $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Q}$.

$$x_1 + (x_2 + x_3) = a_1 + b_1\sqrt{5} + (a_2 + b_2\sqrt{5} + a_3 + b_3\sqrt{5}) =$$
$$= a_1 + a_2 + a_3 + (b_1 + b_2 + b_3)\sqrt{5}$$
$$(x_1 + x_2) + x_3 = (a_1 + b_1\sqrt{5} + (a_2 + b_2\sqrt{5}) + a_3 + b_3\sqrt{5} =$$
$$= a_1 + a_2 + a_3 + (b_1 + b_2 + b_3)\sqrt{5}$$

Z vyššie prevedeného výpočtu dostávame nasledujúcu rovnosť:

$$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3.$$

Ukázali sme, že pre ľubovoľnú trojicu prvkov $x_1, x_2, x_3 \in A$ platí asociatívny zákon.

Neutrálny prvk: Nech $x \in A$ a $e = 0+0\sqrt{5}$, kde $x = a+b\sqrt{5}$, $a, b \in \mathbb{Q}$. Čitateľ ľahko overí, že prvok e je z množiny A. Stačí ukázať, že platí rovnosť:

$$x + e = e + x = x.$$

$$x + e = (a + b\sqrt{5}) + (0 + 0\sqrt{5}) = (a + 0) + (b + 0)\sqrt{5} =$$
$$= a + b\sqrt{5} = x$$
$$e + x = (0 + 0\sqrt{5}) + (a + b\sqrt{5}) = (0 + a) + (0 + b)\sqrt{5} =$$
$$= a + b\sqrt{5} = x$$

Prvok e je neutrálnym prvkom množiny A vzhľadom na binárnu operáciu $+$.
Inverzný prvok: Nech $x \in A$: $x = a + b\sqrt{5}$, kde $a, b \in \mathbb{Q}$. Zvoľme prvok $x' \in A$ takto: $x' = -a-b\sqrt{5}$. Overíme, či takto zvolený prvok x' je inverzným prvkom k prvku x.

$$x + x' = (a + b\sqrt{5}) + (-a - b\sqrt{5}) = (a - a) + (b - b)\sqrt{5} =$$
$$= 0 + 0\sqrt{5} = e$$
$$x' + x = (-a - b\sqrt{5}) + (a + b\sqrt{5}) = (-a + a) + (-b + b)\sqrt{5} =$$
$$= 0 + 0\sqrt{5} = e$$

Vzhľadom na to, ako sme zvolili prvok x', vieme ku každému prvku z množiny A nájsť v množine A k nemu inverzný prvok. Ukázali sme, že $(A;\ +)$ je grupa.
Komutatívnosť: Nech $x_1, x_2 \in A$: $x_1a_1 + b_1\sqrt{5}$ a $x_2 = a_2 + b_2\sqrt{5}$, kde $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

$$x_1 + x_2 = (a_1 + b_1\sqrt{5}) + (a_2 + b_2\sqrt{5}) = (a_1 + a_2) + (b_{1+b_2})\sqrt{5} =$$
$$= (a_2 + a_1) + (b_2 + b_1)\sqrt{5} = (a_2 + b_2\sqrt{5}) + (a_1 + b_1\sqrt{5}) = x_2 + x_1$$

Pre ľubovoľnú dvojicu prvkov $x_1, x_2 \in A$ platí rovnosť:

$$x_1 + x_2 = x_2 + x_1,$$

teda platí komutatívny zákon, z čoho vyplýva, že $(A;\ +)$ je komutatívna grupa.

2. Ukážeme, že $(A;\ \cdot)$ je pologrupa t.j. platí:

– uzavretosť
– asociatívnosť.

Uzavretosť: Nech $x_1, x_2 \in A$: $x_1 = a_1 + b_1\sqrt{5}$ a $x_2 = a_2 + b_2\sqrt{5}$, kde $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

$$\begin{aligned}
&x_1 \cdot x_2 = (a_1 + b_1\sqrt{5}) \cdot (a_2 + b_2\sqrt{5}) = \\
&= a_1 \cdot a_2 + a_1 \cdot b_2\sqrt{5}) + b_1\sqrt{5}) \cdot a_2 + b_1\sqrt{5} \cdot b_2\sqrt{5} = \\
&= (a_1 \cdot a_2 + b_1 \cdot b_2 \cdot (\sqrt{5})^2) + (a_1 \cdot b_2 + b_1 \cdot a_2)\sqrt{5} = \\
&= (a + b\sqrt{5}), \\
&\text{kde } a = (a_1 \cdot a_2 + 5 \cdot b_1 \cdot b_2),\ b(a_1 \cdot b_2 + b_1 \cdot a_2),\ a, b \in \mathbb{Q}
\end{aligned}$$

Súčin $x_1 \cdot x_2 = (a + b\sqrt{5}) \in A$, preto $(A;\ \cdot)$ je uzavretá vzhľadom na binárnu operáciu $\cdot$.
Asociatívnosť: Nech $x_1, x_2, x_3 \in A$: $x_1 = a_1 + b_1\sqrt{5}$, $x_2 = a_2 + b_2\sqrt{5}$, $x_3 = a_3 + b_3\sqrt{5}$, kde $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Q}$.

$$\begin{aligned}
&x_1 \cdot (x_2 \cdot x_3) = (a_1 + b_1\sqrt{5}) \cdot ((a_2 + b_2\sqrt{5}) \cdot (a_3 + b_3\sqrt{5}))= \\
&= (a_1 + b_1\sqrt{5}) \cdot (a_2 \cdot a_3 + b_2 \cdot b_3(\sqrt{5})^2 + a_2 \cdot b_3\sqrt{5} + a_3 \cdot b_2\sqrt{5}) = \\
&= a_1 \cdot a_2 \cdot a_3 + a_1 \cdot b_2 \cdot b_3(\sqrt{5})^2 + a_1 \cdot a_2 \cdot b_3\sqrt{5} + a_1 \cdot a_3 \cdot b_2\sqrt{5} + \\
&a_1 \cdot a_3 \cdot b_1\sqrt{5} + b_1 \cdot b_2 \cdot b_3(\sqrt{5})^3 + a_2 \cdot b_1 \cdot b_3(\sqrt{5})^2 + a_3 \cdot b_1 \cdot b_2(\sqrt{5})^2
\end{aligned}$$

$$\begin{aligned}
&(x_1 \cdot x_2) \cdot x_3 = ((a_1 + b_1\sqrt{5}) \cdot (a_2 + b_2\sqrt{5})) \cdot (a_3 + b_3\sqrt{5}) = \\
&= (a_1 \cdot a_2 + b_1 \cdot b_2(\sqrt{5})^2 + a_1 \cdot b_2\sqrt{5} + a_2 \cdot b_1\sqrt{5}) \cdot (a_3 + b_3\sqrt{5}) = \\
&= a_1 \cdot a_2 \cdot a_3 + a_1 \cdot b_2 \cdot b_3(\sqrt{5})^2 + a_1 \cdot a_2 \cdot b_3\sqrt{5} + a_1 \cdot a_3 \cdot b_2\sqrt{5} + \\
&a_1 \cdot a_3 \cdot b_1\sqrt{5} + b_1 \cdot b_2 \cdot b_3(\sqrt{5})^3 + a_2 \cdot b_1 \cdot b_3(\sqrt{5})^2 + a_3 \cdot b_1 \cdot b_2(\sqrt{5})^2
\end{aligned}$$

Je vidieť, že platí asociatívny zákon a zároveň množina A je uzavretá vzhľadom na binárnu operáciu $\cdot$, z čoho dostávame, že $(A;\ \cdot)$ je pologrupou.

3. Musíme ešte ukázať distributívnosť vzhľadom na binárnu operáciu $+$. Nech $x_1, x_2, x_3 \in A$: $x_1 = a_1 + b_1\sqrt{5}$, $x_2 = a_2 + b_2\sqrt{5}$, $x_3 = a_3 + b_3\sqrt{5}$, kde $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Q}$.

$$\begin{aligned}
&x_1 \cdot (x_2 + x_3) = (a_1 + b_1\sqrt{5}) \cdot ((a_2 + b_2\sqrt{5}) + (a_3 + b_3\sqrt{5})) = \\
&= (a_1 \cdot a_2 + b_1 \cdot b_2(\sqrt{5})^2 + a_1 \cdot b_2\sqrt{5} + a_2 \cdot b_1\sqrt{5}) + \\
&+ (a_1 \cdot a_3 + b_1 \cdot b_3(\sqrt{5})^2 + a_1 \cdot b_3\sqrt{5} + a_3 \cdot b_1\sqrt{5}) = \\
&= (a_1 + b_1\sqrt{5}) \cdot (a_2 + b_2\sqrt{5}) + (a_1 + b_1\sqrt{5}) \cdot (a_3 + b_3\sqrt{5}) = \\
&= (x_1 \cdot x_2) + (x_1 \cdot x_3).
\end{aligned}$$

Ukázali sme, že binárna operácie $\cdot$ je distributívna vzhľadom na binárnu operáciu $+$, teda platí aj posledná vlastnosť, z čoho vyplýva, že $(A;\ +,\ \cdot)$ je okruh.

To, či okruh $(A;\ +,\ \cdot)$ je oborom integrity zistíme, až po overení, či množina A má alebo nemá netriviálne delitele nuly. Nech $x_1, x_2 \in A$: $x_1 = a_1 + b_1\sqrt{5}$, $x_2 = a_2 + b_2\sqrt{5}$, $x_1 \neq e$, $x_2 \neq e$, kde $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

$$\begin{aligned} x_1 \cdot x_2 &= e \\ (a_1 + b_1\sqrt{5}) \cdot (a_2 + b_2\sqrt{5}) &= e \\ (a_1 \cdot a_2 + b_1 \cdot b_2(\sqrt{5})^2 + a_1 \cdot b_2\sqrt{5} + a_2 \cdot b_1\sqrt{5}) &= e \\ (a_1 \cdot a_2 + 5b_1 \cdot b_2) + (a_1 \cdot b_2 + a_2 \cdot b_1)\sqrt{5} &= 0 + 0\sqrt{5} \end{aligned}$$

Z tejto rovnosti dostávame nasledujúcu sústavu dvoch rovníc s neznámymi a_1, a_2, b_1, b_2:

$$\begin{aligned} (a_1 \cdot a_2 + 5b_1 \cdot b_2) &= 0 \\ (a_1 \cdot b_2 + a_2 \cdot b_1) &= 0 \end{aligned}$$

Po vyriešenítejto sústavy a po jednoduchých úvahách s ohľadom na vyššie uvedené podmienky, čiteteľ ľahko zistí, že v množine A sa nenachádzajú netriviálne delitele nuly, preto $(A;\ +,\ \cdot)$ je oborom integrity. $\surd$

3.5 Neriešené úlohy

3.1 Zistite, či množiny spolu s danými binárnymi operáciami tvoria grupu:

a) $(\mathbb{Z};\ \square\ )\quad a\square b = a + b + ab$

b) $(\mathbb{Z};\ \nabla\ )\quad a\nabla b = a + b + 3$

c) $(\mathbb{Z};\ \heartsuit\ )\quad a\heartsuit b = a + (-1)^a b$

d) $(\mathbb{Z}_{12};\ \oplus\ )$

e) $(\mathbb{Z}_{11} - \{\overline{0}\};\ \otimes\ )$

f) $(\mathbb{Z}_n \times \mathbb{Z}_m;\ \oplus\ )$

g) $(\mathsf{S}_3,\ \circ\ )$; S_3 je množina všetkých permutácii množiny $\{1,\ 2,\ 3\}$.

h) $(\mathbb{Z};\ -\ )$

i) $(\{x \in \mathbb{R}\colon\ x = 7^k,\ k \in \mathbb{Z}\ \};\ +\ )$

j) $(\{2^n\colon\ n \in \mathbb{Z}\ \};\ +\ )$

k) $(\{x \in \mathbb{R}\colon\ x = 7^k,\ k \in \mathbb{Z}\ \};\ \cdot\ )$

l) $(\{2^n\colon\ n \in \mathbb{Z}\ \};\ \cdot\ )$

m) $(\mathbb{Z};\ +\ )$

n) $(\mathbb{Z};\ \cdot\ )$

o) $(\mathbb{Q}^+;\ +\ )$

p) $(\mathbb{Z};\ \clubsuit\ )\quad a\clubsuit b = a^2 b^2$

q) $(\mathbb{Z};\ \spadesuit\ )\quad a\spadesuit b = ab + 1$

r) $(\mathbb{R}^+;\ \diamondsuit\ )\quad a\diamondsuit b = a^b$

s) $(\mathbb{R} \times \mathbb{R};\ \square\ )\quad (a, b)\square(c, d) = (a, b + d)$

t) $(\mathbb{R} - \{0\} \times \mathbb{R};\ \nabla\ )\quad (a, b)\nabla(c, d) = (ac, ad + b)$

u) $(\mathbb{Z} \times \mathbb{Z};\ \bullet\ )\quad (a, b) \bullet (c, d) = (ac, b)$

3.2 Zistite, či množina $A \subseteq \mathbb{Z}_{11}$ spolu s binárnou operáciou $\otimes$ - násobenie modulo 11, tvorí grupu:

a) $A = \{\bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9}\}$

b) $A = \{\bar{8}, \bar{7}, \bar{5}, \bar{3}, \bar{1}\}$

c) $A = \{\bar{1}, \bar{8}\}$

d) $A = \{\bar{1}, 1\bar{0}\}$

3.3 Zistite, či $(\mathsf{A}; \circ)$, je grupa, ak A $\{f_1, f_2, f_3, \ldots, f_6\}$, $f_i : \mathbb{R} - \{0, 1\} \longrightarrow \mathbb{R} - \{0, 1\}$ a f_i sú dané predpisom:
$f_1 = x, \quad f_2 = \frac{1}{x}, \quad f_3 = 1 - x, \quad f_4 = \frac{1}{1-x}, \quad f_5 = 1 - \frac{1}{x}, \quad f_6 = \frac{x}{x-1}$.

3.4 Nech $K_n = \{x \in \mathbb{C} : \quad x^n = 1, \quad n \in \mathbb{N}\}$. Zistite, či množina K_n tvorí grupu vzhľadom na operáciu sčítania alebo násobenia.

3.5 Opíšte Cayleho tabuľkou grupu transformácii generovanú symetriami:

a) rovnostranného trojuholníka

b) obdĺžnika, ktorý nie je štvorec

3.6 Nájdite rády všetkých prvkov v grupe:

a) $(\mathbb{Z}_{12};\ \oplus)$

b) $(K_8;\ \cdot)$

c) $(\mathbb{Z}_{11} - \{\bar{0}\};\ \otimes)$

d) $(\mathsf{S}_3;\ \circ)$

3.7 Nájdite rády prvkov:

a) $\bar{2}$, $\bar{3}$ v grupe $(\mathbb{Z}_8;\ \oplus)$

b) 2, 3 v grupe $(\mathbb{Z};\ \heartsuit)$, pričom $a \heartsuit b = a + (-1)^a b$

3.8 Zistite, ktoré z nasledujúcich grúp sú cyklické:

$(\mathbb{R};\ +)$ $(\mathbb{Q};\ +)$ $(K_8;\ \cdot)$ $(\mathbb{Z}_8;\ \oplus)$
$(\mathsf{S}_3;\ \circ)$ $(\mathbb{R}-\{0\};\ \cdot)$ $(\mathbb{Z}_{12};\ \oplus)$ $(\mathbb{Z}_7-\{\bar{0}\};\ \otimes)$
$(\mathbb{Z}_{11}-\{\bar{0}\};\ \otimes)$ $(\mathbb{Z}_2\times\mathbb{Z}_2;\ \oplus)$ $(\mathbb{Z}_2\times\mathbb{Z}_3;\ \oplus)$ $(\mathbb{Z}_2\times\mathbb{Z}_4;\ \oplus)$
$(\{2^n : n\in\mathbb{N}\};\ \cdot)$ $(\{x\in\mathbb{R} : x=7^k, k\in\mathbb{Z}\};\ \cdot)$

3.9 Nájdite grupu, v ktorej každý prvok okrem neutrálneho je jej generátorom.

3.10 Zistite, či zobrazenie $f : A \longrightarrow B$ je homomorfizmom resp. izomorfizmom grúp $(A;\circ)$, $(B;\bullet)$:

a) $A=\mathbb{Z}$, $B=\mathbb{Z}$, $\circ=+$, $\bullet=+$; $\quad f(x)=4x$

b) $A=\mathbb{R}-\{0\}$, $B=\mathbb{R}$, $\circ=\cdot$, $\bullet=+$; $\quad f(x)=\ln x$

c) $A=\mathbb{R}^+$, $B=\mathbb{R}^+$, $\circ=\cdot$, $\bullet=\cdot$; $\quad f(x)=\frac{1}{\sqrt{x}}$

d) $A=\mathbb{R}\times\mathbb{R}$, $B=\mathbb{R}$, $\circ=+$, $\bullet=+$; $\quad f(x,y)=x-2y$

3.11 Zistite, ktoré z nasledujúcich grúp sú izomorfné:

$(\mathbb{R};\ +)$ $(K_6;\ \cdot)$ $(K_8;\ \cdot)$ $(\mathbb{Z}_8;\ \oplus)$
$(\mathsf{S}_3;\ \circ)$ $(\mathbb{R}-\{0\};\ \cdot)$ $(\mathbb{Z}_7-\{\bar{0}\};\ \oplus)$ $(\mathbb{Z}_7-\{\bar{0}\};\ \otimes)$
$(\mathbb{Z};\ +)$ $(\mathbb{Z}_2\times\mathbb{Z}_4;\ \oplus)$

3.12 Nájdite všetky izomorfizmy $f : (K_8;\ \cdot) \longrightarrow (\mathbb{Z}_8;\ \oplus)$.

3.13 Nájdite všetky podgrupy grupy:

a) $(K_8;\ \cdot)$

b) $(\mathbb{Z}_8;\ \oplus)$

c) $(\mathsf{S}_3;\ \circ)$

3.14 Je $(H;\ \cdot)$ podgrupou grupy $(G;\ \cdot)$, ak $H = \{-1, 1\}$ a $G = \mathbb{R} - \{0\}$?

3.15 Zistite, či $(G_i;\ \cdot)$ pre $i = 1, 2, 3$ sú podgrupy grupy $(M;\ \cdot)$, ak $M = \{X \in M_n(\mathbb{R}) : \det(X) \in \mathbb{R}\}$ [3]:

a) $G_1 = \{A \in M : \det(A) > 0\}$

b) $G_2 = \{A \in M : \det(A) = 1\}$

c) $G_3 = \{A \in M : |\det(A)| = 1\}$

d) $G_4 = \{A \in M : A \text{ je diagonálna}\}$

3.16 Ktoré z nasledujúcich množín určujú podgrupy grupy $(\mathbb{C}-\{0\}, \cdot)$ resp. $(\mathbb{C}, +)$:

a) $\{a + bi : \quad a, b \in \mathbb{Z}\}$

b) $\{z \in \mathbb{C} : \quad |z| = 1\}$

c) $\{z \in \mathbb{C} : \quad |z| < 1\}$

3.17 Nájdite ľavý a pravý rozklad grupy G podľa podgrupy H:

a) $(\mathbb{Z}_{15};\ \oplus)$ a $H = \langle\overline{12}\rangle$

b) $(\mathbb{Z}_7 - \{\bar{0}\};\ \otimes)$ a $H = \langle\bar{4}\rangle$

c) $(\mathsf{S}_3;\ \circ)$ a $H = \left\langle \binom{123}{231} \right\rangle$

d) $(\mathsf{S}_3;\ \circ)$ a $H = \left\langle \binom{123}{213} \right\rangle$

e) $(\mathbb{Q} - \{0\};\ \cdot)$ a $H = \{-1, 1\}$

f) $(K_8;\ \cdot)$ a $H = \langle i\rangle$

3.18 Nájdite G/H a určte indexy podgrupy H v grupe G, ak:

a) $(\mathbb{Z}_6;\ \oplus)$ a $H = \langle\bar{4}\rangle$

b) $(\mathbb{Z};\ +)$ a $H = \langle 3\rangle$

[3] Symbol $M_n(\mathbb{R})$ označuje množinu všetkých štvorcových matíc typu $n \times n$ nas množinou reálnych čísel $\mathbb{R}$

c) $(\mathbb{Z}_{12};\ \oplus)$ a $H = \langle \bar{9} \rangle$

3.19 Zistite, či množina spolu s dvomi binárnymi operáciami $(\mathsf{A};\ +, \cdot)$ tvorí okruh, obor integrity, teleso alebo pole, ak:

a) $\mathsf{A} = \{a + b\sqrt{2} + c\sqrt[3]{2} :\ a, b, c \in \mathbb{Q}\}$

b) $\mathsf{A} = \{a + bi :\ a, b \in \mathbb{Z}\}$

c) $\mathsf{A} = \{a + bi :\ a, b \in \mathbb{Q}\}$

d) $\mathsf{A} = \{a + b\sqrt[3]{2} :\ a, b \in \mathbb{Q}\}$

e) $\mathsf{A} = \{x \in \mathbb{R} :\ x = 7^k, \quad k \in \mathbb{Z}\}$

f) A je množina párnych prirodzených čísel

g) A je množina všetkých komplexných jednotiek

h) A je množina všetkých párnych celých čísel

3.20 Zistite, či $(\mathcal{P}(A);\ \div, \cap)$, $A \neq \emptyset$ je okruh resp. pole, ak $X \div Y = (X - Y) \cup (Y - X)$.

3.21 Zistite, či $(M;\ +, \cdot)$ je pole, ak:

a) $M = M_n(\mathbb{R})$

b) $M = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \in M_2(\mathbb{R}) \right\}$

3.22 Zistite, či dané zobrazenie f je homomorfizmom alebo izomorfizmom okruhov O_1, O_2:

a) $f : \mathbb{C} \longrightarrow \mathbb{R}, \quad f(a + bi) = a$; ak $O_1 = (\mathbb{C};\ +, \cdot)$, $O_2 = (\mathbb{R};\ +, \cdot)$

b) $f : \mathbb{R} \longrightarrow \mathbb{C}, \quad f(a) = a + 0i$; ak $O_1 = (\mathbb{R};\ +, \cdot)$, $O_2 = (\mathbb{C};\ +, \cdot)$

c) $f : \mathbb{R}^2 \longrightarrow \mathbb{R}, \quad f(a, b) = a$; ak $O_1 = (\mathbb{R}^2;\ +, \cdot)$, $O_2 = (\mathbb{R};\ +, \cdot)$

3.23 Nech je daná množina $\mathsf{A} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M_2(\mathbb{R}) \right\}$ a zobrazenie $\varphi : \mathbb{C} \longrightarrow \mathsf{A}$, $\varphi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Rozhodnite, či zobrazenie φ je homomorfizmom resp. izomorfizmom okruhov $(\mathsf{A};\ +, \cdot)$ a $(\mathbb{C};\ +, \cdot)$.

3.24 Rozhodnite, či zobrazenie $\varphi(a,b) = (b,0,a)$ je homomorfizmus resp. izomorfizmus okruhov $(\mathbb{R}^3;\ +,\cdot)$ a $(\mathbb{R}^2;\ +,\cdot)$, ak $+$ a $\cdot$ sú sčítanie a násobenie n-tíc po jednotlivých zložkách.

3.25 Rozhodnite, či zobrazenie $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ je homomorfizmom resp. izomorfizmom okruhov $(\mathbb{R}^3;\ +,\cdot)$ a $(\mathbb{R}^2;\ +,\cdot)$, ak:

a) $f : f(x,y,z) = (x,y)$

b) $f : f(x,y,z) = (y,y)$

3.6 Výsledky neriešených úloh

3.1 **a)** nie je grupa **b)** je grupa **c)** je grupa **d)** je grupa **e)** je grupa **f)** je grupa **g)** je grupa **h)** nie je grupa **i)** nie je grupa **j)** nie je grupa **k)** je grupa **l)** je grupa **m)** je grupa **n)** nie je grupa **o)** nie je grupa **p)** nie je grupa **q)** nie je grupa **r)** nie je grupa **s)** nie je grupa **t)** je grupa **u)** nie je grupa

3.2 **a)** áno **b)** nie **c)** nie **d)** áno

3.3 áno

3.4 Tvorí grupu vzhľadom na operáciu násobenia.

3.5 **a)** Ponechávame na čitateľa. **b)** Ponechávame na čitateľa.

3.6 **a)** rád$(\bar{0}) = 1$, rád$(\bar{1}) =$ rád$(\bar{5}) =$ rád$(\bar{7}) =$ rád$(\overline{11}) = 12$, rád$(\bar{2}) =$ rád$(\overline{10}) = 6$, rád$(\bar{3}) =$ rád$(\bar{9}) = 4$, rád$(\bar{4}) =$ rád$(\bar{8}) = 3$ **b)** rád$(1) = 1$, rád$(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i) = 8$, rád$(i) = 4$, rád$(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i) = 8$, rád$(-1) = 2$, rád$(-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i) = 8$, rád$(-i) = 4$, rád$(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i) = 8$ **c)** rád$(\bar{1}) = 1$, rád$(\bar{2}) =$ rád$(\bar{6}) =$ rád$(\bar{7}) =$ rád$(\bar{8}) =$rád$(\bar{9}) = 10$, rád$(\bar{3}) =$ rád$(\bar{4}) =$ rád$(\bar{5}) = 5$, rád$(\overline{10}) = 2$ **d)** rád $\binom{123}{123} = 1$, rád$\binom{123}{213} = 2$, rád$\binom{123}{132} = 2$, rád$\binom{123}{321} = 2$, rád$\binom{123}{312} = 3$, rád$\binom{123}{213} = 3$

3.7 **a)** rád$(\bar{2}) = 4$, rád$(\bar{3}) = 8$ **b)** rád$(2)\infty$, rád$(3) = 2$

3.8 Cyklické sú grupy: $(K_8;\ \cdot)$, $(\mathbb{Z}_8;\ \oplus)$, $(\mathbb{Z}_{12};\ \oplus)$, $(\mathbb{Z}_7 - \{\bar{0}\};\ \otimes)$, $(\mathbb{Z}_{11} - \{\bar{0}\};\ \otimes)$, $(\mathbb{Z}_2 \times \mathbb{Z}_3;\ \oplus)$, $(\{2^n :\ n \in \mathbb{N}\};\ \cdot)$, $(\{x \in \mathbb{R} :\ x = 7^k, k \in \mathbb{Z}\};\ \cdot)$

3.9 Napríklad grupa: $(\mathbb{Z}_7;\ \oplus)$.

3.10 **a)** homomorfizmus **b)** izomorfizmus **c)** izomorfizmus **d)** homomorfizmus

3.11 $(\mathbb{R};\ +) \cong (\mathbb{R} - \{0\};\ \cdot)$, $(K_8;\ \cdot) \cong (\mathbb{Z}_8;\ \oplus)$, $(K_6;\ \cdot) \cong (\mathbb{Z}_7 - \{\bar{0}\};\ \oplus)$,

3.12 Tabuľka vzorov a obrazov jednotlivých izomorfizmov:

vzor	a	1	$\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$	i	$-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$	-1	$-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$	-i	$\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$
obraz	$\varphi_1(a)$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
obraz	$\varphi_2(a)$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
obraz	$\varphi_3(a)$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
obraz	$\varphi_4(a)$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

3.13 **a)** K_8, $\{1\}$, $\{-1,1\}$, $\{-1,1,-i,i\}$ **b)** $\mathbb{Z}_8$, $\{\bar{0}\}$, $\{\bar{0},\bar{4}\}$, $\{\bar{0},\bar{2},\bar{4},\bar{6}\}$ **c)** S_3, $\{\binom{123}{123}\}$, $\{\binom{123}{123},\binom{123}{132}\}$, $\{\binom{123}{123},\binom{123}{321}\}$, $\{\binom{123}{123},\binom{123}{213}\}$, $\{\binom{123}{123},\binom{123}{312},\binom{123}{231}\}$

3.14 Áno.

3.15 **a)** áno **b)** áno **c)** áno **d)** áno

3.16 **a)** podgrupa grupy $(\mathbb{C};\ +)$ **b)** podgrupa grupy $(\mathbb{C}-\{0\};\ \cdot)$ **c)** podgrupa grupy $(\mathbb{C}-\{0\};\ \cdot)$

3.17 Rozklady grupy G podľa podgrupy H:

a) $\text{ĽR} = \text{PR} = \{\{\bar{0},\bar{3},\bar{6},\bar{9},\overline{12}\},\{\bar{1},\bar{4},\bar{7},\overline{10},\overline{13}\},\{\bar{2},\bar{5},\bar{8},\overline{11},\overline{14}\}\}$

b) $\text{ĽR} = \text{PR} = \{\{\bar{1},\bar{2},\bar{4}\},\{\bar{3},\bar{5},\bar{6}\}\}$

c) $\text{ĽR} = \text{PR} = \{\{\binom{123}{123},\binom{123}{231},\binom{123}{312}\},\{\binom{123}{132},\binom{123}{213},\binom{123}{321}\}\}$

d) $\text{ĽR} = \{\{\binom{123}{123},\binom{123}{213}\},\{\binom{123}{231},\binom{123}{132}\},\{\binom{123}{321},\binom{123}{312}\}\}$
$\text{PR} = \{\{\binom{123}{123},\binom{123}{213}\},\{\binom{123}{312},\binom{123}{132}\},\{\binom{123}{213},\binom{123}{321}\}\}$

e) $\text{ĽR} = \text{PR} = \{\{x,-x\} : x \in \mathbb{Q}-\{0\}\}$

f) $\text{ĽR} = \text{PR} = \{\{-1,1,i,-i\},\{\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i,\ \frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i,\ -\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i,\ -\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\}\}$

3.18 Rozklad grupy G podľa podgrupy H a index podgrupy H:

a) $G/H = \{\{\bar{0},\bar{2},\bar{4}\},\{\bar{1},\bar{3},\bar{5}\}\}$, index je 2

b) $G/H = \{\{3k :\ k \in \mathbb{Z}\},\{3k+1 :\ k \in \mathbb{Z}\},\{3k+2 :\ k \in \mathbb{Z}\}\}$, index je 3

c) $G/H = \{\{\bar{0},\bar{3},\bar{6},\bar{9}\},\{\bar{1},\bar{4},\bar{7},\overline{10}\},\{\bar{2},\bar{5},\bar{8},\overline{11}\}\}$, index je 3

3.19 **a)** nie je okruh **b)** je obor integrity **c)** je pole **d)** nie je okruh **e)** nie je okruh **f)** nie je okruh **g)** nie je okruh **h)** je obor integrity

3.20 $(\mathcal{P};\ \div,\cap)$ je okruh, ale nie je pole.

3.21 **a)** nie je pole **b)** je pole

3.22 **a)** nie je homomorfizmus **b)** je homomorfizmus, ale nie je izomorfizmus **c)** je homomorfizmus, ale nie je izomorfizmus

3.23 Zobrazenie φ je izomorfizmom.

3.24 Zobrazenie φ je homomorfizmus, ale nie je izomorfizmus.

3.25 **a)** zobrazenie f je homomorfizmus, ale nie je izomorfizmus **b)** zobrazenie f je homomorfizmus, ale nie je izomorfizmus