2 Cvičení 2: Základy teorie grup

Teorie: V tomto cvičení se budeme zabývat základními algebraickými strukturami. Na úvod několik základních pojmů:

Definice 7. Nechť G je libovolná neprázdná množina. Binární operací na množině G rozumíme libovolné zobrazení $\circledast : G \times G \to G$.

Dohodněme se, že místo $\circledast(a, b)$ budeme psát $a \circledast b$.

Definice 8. Řekneme, že je operace $\circledast$ komutativní na množině G, jestliže pro libovolné $a, b \in G$ platí $a \circledast b = b \circledast a$.

Nyní se dostáváme k sérii definic základních algebraických struktur jako je grupoid, pologrupa, monoid a grupa.

Definice 9. Libovolnou neprázdnou množinu s operací na této množině nazýváme grupoid.

Například tedy $(\mathbb{N}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Z}_5, +)$, $(\mathbb{C}, \cdot)$ jsou grupoidy. Naopak $(\mathbb{N}, -)$, $(\mathbb{N}, :)$ grupoidy nejsou.

Definice 10. Grupoid $(G, \circledast)$ nazýváme pologrupa, jestliže pro libovolné $a, b, c \in G$ platí, že $a \circledast (b \circledast c) = (a \circledast b) \circledast c$.

Například tedy $(\mathbb{N}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Z}_5, +)$, $(\mathbb{C}, \cdot)$ jsou pologrupy, ale $(\mathbb{N}, -)$, $(\mathbb{Z}, -)$ pologrupy nejsou.

Definice 11. Nechť $(G, \circledast)$ je pologrupa. Řekneme, že prvek $e \in G$ je neutrální prvek v pologrupě G, jestliže pro libovolné $a \in G$ platí

$$\begin{aligned} a \circledast e &= a \\ e \circledast a &= a \end{aligned}$$

Například $1 + 0i$ je neutrálním prvkem v pologrupě $(\mathbb{C}, \cdot)$, 0 je neutrálním prvkem v pologrupě $(\mathbb{Z}, +)$, $[0]_5$ je neutrálním prvkem v pologrupě $(\mathbb{Z}_5, +)$.

Pro počet neutrálních prvků v dané pologrupě platí následující tvrzení:

Věta 8. *V libovolné pologrupě existuje nejvýše jeden neutrální prvek.*

Definice 12. Pologrupu s neutrálním prvkem nazýváme monoid.

Definice 13. Nechť je dána pologrupa $(G, \circledast)$ s neutrálním prvkem e. Řekneme, že prvek $b \in G$ je inverzní (opačný) k prvku $a \in G$, jestliže platí:

$$\begin{aligned} a \circledast b &= e \\ b \circledast a &= e \end{aligned}$$

Definice 14. Monoid, ve kterém ke každému prvku existuje prvek inverzní, nazýváme grupa.

Například $(\mathbb{Z}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Z}_7, +)$ jsou grupy. Oproti tomu $(\mathbb{R}, \cdot)$, $(\mathbb{Z}, \cdot)$ grupy nejsou.

Dále se můžeme podívat na podmnožiny grup. Pokud je sama podmnožina grupou, říkáme, že tvoří podgrupu dané grupy. Některé vlastnosti zdědí každá podmnožina (asociativitu, komutativitu), proto nemusíme pro podgrupy dokazovat všechny podmínky grupy.

Věta 9. *Nechť $(G, *)$ je grupa a nechť $\emptyset \neq H \subseteq G$. Potom H je podgrupa grupy G, jestliže platí*

1. *pro všechny $a, b \in H$ platí, že $a + b \in H$*
2. *pro všechny $a \in H$ platí, že $a^{-1} \in H$*

Příklad 21. Uveďte příklad:

1. Konečné komutativní grupy
2. Konečné nekomutativní grupy
3. Nekonečné komutativní grupy
4. Nekonečné nekomutativní grupy
5. Konečné komutativní pologrupy, která nebude monoidem.
6. Pětiprvkové komutativní grupy
7. Nekonečného monoidu, který nebude grupou

Řešení.

1. $(\mathbb{Z}_5, +)$
2. $(\mathbb{S}_3, \circ)$
3. $(\mathbb{Z}, +)$

4. Množina všech regulárních matic spolu s násobením
5. $(\{a, b\}, \circledast)$, kde $a \circledast b = a$, $a \circledast a = a$, $b \circledast b = a$, $b \circledast a = a$.
6. $(\mathbb{Z}_5, +)$
7. $(\mathbb{Z}, \cdot)$

Příklad 22. Rozhodněte, zda daná množina $\mathbb{Z}$ tvoří spolu s operací $\heartsuit$ (komutativní) grupoid, (komutativní) pologrupu, (komutativní) monoid, (komutativní) grupu:

1. $a \heartsuit b = (a, b)$
2. $a \heartsuit b = a^b$
3. $a \heartsuit b = 2a + b$
4. $a \heartsuit b = |a|$
5. $a \heartsuit b = a + b + a \cdot b$
6. $a \heartsuit b = a + b - a \cdot b$
7. $a \heartsuit b = a + (-1)^a b$

Výsledek.

1. Daná množina s operací tvoří komutativní pologrupu, která není monoidem.
2. Daná množina s operací tvoří nekomutativní grupoid, který není pologrupou.
3. Daná množina tvoří nekomutativní grupoid, který není pologrupou.
4. Daná množina tvoří nekomutativní pologrupu, která nemá neutrální prvek.
5. Daná množina tvoří komutativní monoid, který není grupou.
6. Daná množina tvoří komutativní monoid, který není grupou.
7. Daná množina tvoří nekomutativní grupu.

Příklad 23. Rozhodněte, zda množina $G = \mathbb{R} \setminus \{0\} \times \mathbb{R}$ s operací $\triangle$ tvoří grupoid, pologrupu, pologrupu s neutrálním prvkem (monoid), grupu a zda je zadaná operace komutativní, jestliže je operace $\triangle$ definována takto: $(x, y) \triangle (u, v) = (xu, xv+y)$, pro libovolná $(x, y), (u, v) \in G$.

Výsledek. Jedná se o nekomutativní grupu.

Příklad 24. Nechť X je libovolná množina. Nechť $\mathcal{P}(X)$ značí systém všech podmnožin množiny X. Určete, zda množina $\mathcal{P}(X)$ tvoří s danou operací grupoid, pologrupu, pologrupu s neutrálním prvkem (monoid), grupu a zda je zadaná operace komutativní.

1. průnik množin
2. sjednocení množin
3. symetrický rozdíl množin

Výsledek. Je-li množina X prázdná, potom tvoří $\mathcal{P}(X)$ se všemi operacemi komutativní grupu. V ostatních případech

1. S operací průnik tvoří daná množina komutativní pologrupu s neutrálním prvkem.
2. S operací sjednocení tvoří daná množina komutativní pologrupu s neutrálním prvkem.
3. S operací symetrický rozdíl tvoří daná množina komutativní grupu.

Příklad 25. Rozhodněte, zda podmnožina G komplexních čísel tvoří spolu s operací násobení komplexních čísel grupoid, pologrupu, pologrupu s neutrálním prvkem (monoid), grupu a zda je zadaná operace komutativní.

1. $G = \{a + bi \mid a, b \in \mathbb{Z}\}$
2. $G = \{a + bi \mid a, b \in \mathbb{R}, a^2 + b^2 = 1\}$
3. $G = \{a + b \cdot \sqrt{5} \mid a, b \in \mathbb{Q}, a^2 + b^2 \neq 0\}$

Výsledek.

1. G tvoří monoid
2. G tvoří komutativní grupu
3. G tvoří komutativní grupu

Příklad 26. Dokažte, že v každé grupě o sudém počtu prvků existuje prvek, který je sám sobě inverzním a přesto to není neutrální prvek.

Řešení. Seřaďme prvky dané grupy do dvojic, přičemž ve dvojici bude vždy prvek a jeho inverze. Sám potom zůstane neutrální prvek. To je však celkem lichý počet prvků.

Příklad 27. Určete, kolika způsoby lze doplnit tabulka tak, aby $(\{a, b, c\}, \circledast)$ byl

1. grupoid
2. komutativní grupoid
3. grupoid s neutrálním prvkem
4. pologrupa s neutrálním prvkem
5. grupa

$\divideontimes$	a	b	c
a	c	b	a
b			b
c			

Výsledek.

1. 3^5
2. 9
3. 9
4. 1
5. 0

Příklad 28. Doplňte tabulku tak, aby $(\{a, b, c\}, \divideontimes)$ byla pologrupa.

$\divideontimes$	a	b	c
a	b	a	c
b			
c			

Příklad 29. Doplňte tabulku tak, aby $(\{a, b, c\}, \divideontimes)$ byla grupa.

$\divideontimes$	a	b	c
a			
b	c	a	
c			

Příklad 30. Nechť $(G, \circ)$ je grupa, nechť $a \in G$ je libovolný pevný prvek. Definujme na G operaci $\heartsuit$ následovně: $x \heartsuit y = x \circ a \circ y$ pro libovolné $x, y \in G$. Dokažte, že $(G, \heartsuit)$ tvoří grupu.

Příklad 31. Uveďte příklad:

1. Dvou disjunktních podgrup grupy $\mathbb{Z}$.
2. Dvou různých podgrup grupy $\mathbb{Z}$.

3. Grupy, která má právě jednu podgrupu.
4. Podgrupy $\mathbb{C}^*$, která má 17 prvků.
5. Čtyř různých podgrup grupy $\mathbb{Z}$, které obsahují číslo 45.

Příklad 32. Popište všechny podgrupy grupy $\mathbb{Z}_{30}$ a nakreslete, jak jsou v sobě vnořeny.

Výsledek. Je jich celkem 8.

Příklad 33. Dokažte, že $H = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ tvoří podgrupu grupy $(\mathbb{R}, +)$.

Příklad 34. Dokažte, že $H = \{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\}$ tvoří podgrupu grupy $(\mathbb{C}, +)$.

Příklad 35. Dokažte, že $H = \{c \in \mathbb{C} \mid |c| = 1\}$ tvoří podgrupu grupy $(\mathbb{C}^*, \cdot)$.

Příklad 36. Popište všechny konečné podgrupy grupy $(\mathbb{R}^*, \cdot)$

Výsledek. Dvě podgrupy: $\{1\}, \{-1, 1\}$.

Příklad 37. Dokažte, že průnikem dvou podgrup grupy G je opět podgrupa grupy G.

Příklad 38. Označme $Mat_n(T)$ množinu všech čtvercových matic řádu n s koeficienty z množiny T. Dokažte, že $G = (Mat_2(\mathbb{R}), +)$ tvoří komutativní grupu a rozhodněte, zda množina H tvoří podgrupu grupy G:

1. $H = Mat_2(\mathbb{Z})$
2. $H = Mat_2(\mathbb{N}_0)$
3. $H = \left\{ \begin{pmatrix} 0 & a \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$
4. $H = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$
5. $H = \left\{ \begin{pmatrix} b & a \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$

Výsledek.

1. Ano
2. Ne
3. Ano
4. Ne
5. Ano

Příklad 39. Označme $\mathcal{GL}_n(\mathbb{R})$ množinu všech regulárních čtvercových matic s reálnými koeficienty. Dokažte, že $G = \mathcal{GL}_2(\mathbb{R})$ tvoří grupu a rozhodněte, zda množina H tvoří podgrupu grupy G:

1. $H = \mathcal{GL}_2(\mathbb{Q})$
2. $H = \mathcal{GL}_2(\mathbb{Z})$
3. $H = \{A \in \mathcal{GL}_2(\mathbb{Z}) \mid |A| = 1\}$
4. $H = \left\{ \begin{pmatrix} 0 & a \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$
5. $H = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \mid a \in \mathbb{Z} \right\}$
6. $H = \left\{ \begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$
7. $H = \left\{ \begin{pmatrix} 0 & a \\ b & c \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$
8. $H = \left\{ \begin{pmatrix} 1 & a \\ b & c \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$

Výsledek.

1. Ano
2. Ne
3. Ano
4. Ne
5. Ano
6. Ano
7. Ne
8. Ano

Příklad 40.

1. Rozhodněte, zda množina $H = \{a \in \mathbb{R}^* \mid a^2 \in \mathbb{Q}\}$ tvoří podgrupu grupy $(\mathbb{R}^*, \cdot)$
2. Rozhodněte, zda množina $H = \{a \in \mathbb{R} \mid a^2 \in \mathbb{Q}\}$ tvoří podgrupu grupy $(\mathbb{R}, +)$

Výsledek.

1. Ano
2. Ne

Příklad 41. Nechť G je komutativní grupa. Označme $H = \{g \in G \mid g^2 = e_G\}$. Dokažte, že H tvoří podgrupu grupy G a zdůvodněte, proč je důležitá komutativita grupy G.