SLEZSKÁ UNIVERZITA V OPAVĚ
Matematický ústav v Opavě
Na Rybníčku 1, 746 01 Opava, tel. (553) 684 611
DENNÍ STUDIUM

ALGEBRA

Téma 4: Grupy, okruhy a pole

Základní pojmy

unární operace, binární operace, asociativita, komutativita, distributivita;

grupa, neutrální prvek, inverzní prvek, inverzní operace; komutativní (Abelova) grupa, aditivní grupa, multiplikativní grupa; podgrupa; homomorfismus grup, jádro a obraz homomorfismu, izomorfismus grup; triviální grupa, číselné grupy, maticové grupy, cyklické grupy, symetrické grupy;

okruh, komutativní okruh, asociativní okruh, nulový prvek okruhu, jednotkový prvek okruhu, dělitelé nuly, invertibilní prvek; podokruh; homomorfismus a izomorfismus okruhů, triviální okruh, číselné okruhy, okruh polynomů, okruh zbytkových tříd modulo n, okruh funkcí;

pole (těleso), charakteristika pole, podpole; číselná pole;

Základní úlohy

Vyšetřit vlastnosti dané operace, rozhodnout, zda množina s danými operacemi je grupa, okruh, pole; rozhodnout, zda podmnožina grupy (okruhu, pole) je podgrupa (podokruh, podpole), rozhodnout, zda dané zobrazení je homomorfismus (izomorfismus), určit jádro a obraz homomorfismu, určit charakteristiku pole.

Základní vzorce

asociativní zákon: $a \circ (b \circ c) = (a \circ b) \circ c$

komutativní zákon: $a \circ b = b \circ a$

distributivní zákony:

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

b) $(a + b) \circ c = a \circ c + b \circ c$.

Kontrolní otázky

1. Definujte grupu.
2. Buď G grupa. Je $\{e\}$ podgrupou G? Je G podgrupou G?
3. Je množina $\mathbb{R}$ s operací sčítání reálných čísel grupa? Je $\mathbb{R}$ s operací násobení reálných čísel grupa?
4. Je dělení binární operace na množině $\mathbb{R}$?
5. Je sčítání binární operace na množině sudých čísel?
6. Je sčítání binární operace na množině lichých čísel?
7. Na množině $\mathbb{R}$ zaveďte strukturu
   (a) grupy,
   (b) okruhu,
   (c) pole.

8. Vyjmenujte některé podgrupy aditivní grupy reálných čísel $(\mathbb{R}, +)$.
9. Lze zavést strukturu okruhu na jednoprvkové množině? Lze zavést na jednoprvkové množině strukturu okruhu s jednotkou?
10. Uveďte příklady okruhů, které nejsou poli.
11. Uveďte příklady polí.
12. Jakou charakteristiku má pole $\mathbb{Q}$?
13. Uveďte příklady podokruhů okruhu $\mathbb{R}$.
14. Je-li $f : G \to G'$ izomorfismus grup, určete podgrupy $\mathrm{Ker}\, f \subset G$ a $\mathrm{Im}\, f \subset G'$.
15. Uveďte příklad okruhu na dvouprvkové množině.

Příklady

1. Rozhodněte, která z uvedených dvojic (množina, operace) má strukturu grupy, případně Abelovské grupy: ($+$ značí sčítání, $\cdot$ násobení)
   $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$, $(\mathbb{R}^+, \cdot)$,
   $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$,
   (matice $m/n, +$), (matice $n/n, \cdot$), (regulární čtvercové matice,$\cdot$).
2. Dokažte, že množina všech sudých čísel s operací sčítání je izomorfní s aditivní grupou celých čísel.
3. Dokažte, že grupy $(\mathbb{R}^+, \cdot)$ a $(\mathbb{R}, +)$ jsou izomorfní.
4. Uvažujme tyto grupy: $(\mathbb{Z}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^+, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$. Vyberte všechny dvojice A, G tak, aby platilo, že A je podgrupou G.
5. Dokažte, že je-li $f : G \to G'$ homomorfismus grup a $e(e')$ je jednotka grupy $G(G')$, pak $f(e) = e'$.
6. Dokažte, že průnikem dvou podgrup grupy G je podgrupa grupy G. Platí analogické tvrzení pro konečný systém podgrup? A pro libovolný systém podgrup? Dokažte.
7. *Cyklické podgrupy*. Buď G grupa, $a \in G$. Nechť $n \in \mathbb{N}$. *n-tou mocninou prvku a* nazýváme prvek

   $$\underbrace{a \cdot a \cdots a}_{n} \quad \text{a označujeme} \quad a^n.$$

   (Dohoda: $a^0 = e$; je-li G aditivní grupa, nazýváme a^n *n-násobkem prvku a* a píšeme na.)
   Zápornou mocninu prvku a definujeme vztahem

   $$\underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n} = (a^{-1})^n; \quad \text{značíme ji} \quad a^{-n}.$$

   Dokažte, že $(a^{-1})^n = (a^n)^{-1}$.
   Dokažte: pro $\forall m, n$: $a^n \cdot a^m = a^m \cdot a^n = a^{n+m}$, $(a^n)^m = a^{nm}$.
   Označme $\{a\}$ podmnožinu grupy G tvořenou všemi mocninami prvku a. Dokažte, že $\{a\}$ je podgrupa grupy G—nazývá se *cyklická podgrupa* grupy G *vytvořená prvkem a*. Je tato podgrupa abelovská?
   Grupa G se nazývá *cyklická*, jestliže existuje $a \in G$ tak, že $G = \{a\}$. Ukažte, že $(\mathbb{Z}, +)$ je nekonečná cyklická grupa. Dokažte, že všechny nekonečné cyklické grupy jsou navzájem izomorfní.
   (Návod: Zkoumejte izomorfismus s cyklickou grupou $(\mathbb{Z}, +)$.)
8. Prvek a grupy G se nazývá *prvek řádu n*, jestliže $a^n = e$. Nechť v grupě G existuje právě jeden prvek x řádu 2. Pak pro $\forall a \in G$ platí $ax = xa$. Dokažte.

9. *Symetrické grupy*. Dokažte, že množina všech permutací množiny $\{1, 2, \dots, n\}$ s operací skládání permutací je grupa. Nazývá se *symetrická grupa stupně* n a označuje se S_n. Je S_n abelovská? Určete parity permutací, složenou permutaci $\sigma \circ \tau$, resp. $\tau \circ \sigma$ a jejich paritu, je-li
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 3 & 4 & 2 \end{pmatrix}.$$
Popište tyto podmnožiny grupy S_4:
–všechny permutace, které zobrazují množinu $\{1, 2\}$ do množiny $\{1, 2\}$,
–všechny permutace, které zobrazují $\{1, 2\}$ buď do $\{1,2\}$ nebo do $\{3, 4\}$.
Najděte 4 různé podgrupy grupy S_4 izomorfní s S_3.
Uvažujme grupu S_4 a její podmnožinu
$$A = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \right\}.$$
Rozhodněte, zda A je podgrupa.
10. Uvažujme aditivní grupu celých čísel $(\mathbb{Z}, +)$. Dokažte, že podmnožina A všech sudých čísel je podgrupa v $(\mathbb{Z}, +)$.
11. Označme $GL(n, \mathbb{R})$ multiplikativní grupu všech regulárních matic řádu n nad $\mathbb{R}$ (nazývá se *obecná lineární grupa* řádu n nad $\mathbb{R}$). Matice $A \in GL(n, \mathbb{R})$ se nazývá *ortogonální*, jestliže $A^{-1} = A^T$. Dokažte, že množina všech ortogonálních matic řádu n je podgrupa grupy $GL(n, \mathbb{R})$; označuje se $O(n, \mathbb{R})$ a nazývá se *ortogonální grupa*. Dokažte, že pro prvky a^i_j ortogonální matice A platí
$$\textstyle\sum_{k=1}^n a^i_k a^j_k = \delta^{ij}, \qquad \sum_{k=1}^n a^k_i a^k_j = \delta_{ij}$$
(relace ortogonality). Určete determinant ortogonální matice.
12. Označme $GL(n, \mathbb{C})$ multiplikativní grupu všech regulárních matic řádu n nad $\mathbb{C}$. Matice $A \in GL(n, \mathbb{C})$ se nazývá *unitární*, jestliže platí $A^{-1} = A^{T*}$. Dokažte, že množina $U(n, \mathbb{C})$ všech unitárních matic řádu n je podgrupa grupy $GL(n, \mathbb{C})$ (*unitární grupa*). Co platí pro determinant unitární matice? Je $O(n, \mathbb{R})$ podgrupa $U(n, \mathbb{C})$?
13. Označme $SL(n, \mathbb{R})$ množinu všech matic $A \subset GL(n, \mathbb{R})$ pro které $\det A = 1$. Dokažte, že $SL(n, \mathbb{R})$ je podgrupa $GL(n, \mathbb{R})$ (*speciální lineární grupa*).
14. *Euklidova grupa transformací* $\mathbb{R}^3$. Uvažujme množinu všech transformací Euklidova prostoru $\mathbb{R}^3$ do sebe, definovaných rovnicemi
$$\vec{r}\,' = A\vec{r} + \vec{u}, \tag{$*$}$$
kde $\vec{r}$ je polohový vektor částice $\vec{r} = (x, y, z)$, $\vec{u}$ je libovolný konstantní vektor a A je ortogonální matice (tj. taková, že $AA^T = E$). Pro $A = E$ dostáváme $\vec{r}\,' = \vec{r} + \vec{u}$ a příslušné transformace nazýváme *translace*. Pro $\vec{u} = 0$ máme $\vec{r}\,' = A\vec{r}$ a transformace nazýváme *rotace*). Dokažte, že množina transformací (*) s operací skládání transformací je grupa (*Euklidova grupa* prostoru $\mathbb{R}^3$). Určete její neutrální prvek a k libovolnému prvku prvek inverzní. Je tato grupa abelovská? Stejné otázky zkoumejte pro množinu translací a pak pro množinu rotací.
15. Dokažte, že složením homomorfismu grup a izomorfismu grup vzniká homomorfismus a složením dvou izomorfismů grup vzniká izomorfismus. Co můžete říci o složení dvou homomorfismů?
16. Uveďte příklady číselných okruhů.
17. Dokažte, že pole racionálních čísel je "nejmenší" číselné pole, tj. že je celé obsaženo v každém číselném poli.
18. Rozhodněte, které z uvedených množin mají strukturu podokruhu okruhu reálných čísel:
(a) sudá čísla
(b) lichá čísla
(c) $\mathbb{Z}$
(d) $\mathbb{R} \setminus \mathbb{Q}$

(e) $\{a + b\sqrt{2}, \quad a, b \in \mathbb{Q}\}$
(f) $\{a + b\sqrt[3]{2}, \quad a, b \in \mathbb{Q}\}$
(g) $\{a + bi, \quad a, b \in \mathbb{Q}\}$
Které z nich mají strukturu pole?

19. Dokažte, že množina všech polynomů s komplexními koeficienty s operacemi sčítání a násobení polynomů je okruh. Má tento okruh jednotku? Má dělitele nuly? Je polem?

20. *Okruh zbytkových tříd modulo n.* Uvažujme okruh celých čísel $(\mathbb{Z}, +, \cdot)$. Zvolme $n \in \mathbb{N}$, $n \neq 1$ pevně. Řekneme, že čísla $z_1, z_2 \in \mathbb{Z}$ jsou *ekvivalentní*, jestliže jejich zbytky při dělení číslem n jsou si rovny. Prověřte, že takto definovaná relace je ekvivalence na množině $\mathbb{Z}$. Zřejmě tato ekvivalence definuje rozklad množiny $\mathbb{Z}$ na n disjunktních tříd $\mathbb{Z}_0, \mathbb{Z}_1, \dots \mathbb{Z}_{n-1}$, kde $\mathbb{Z}_i$ je třída ekvivalence obsahující všechna celá čísla, jejichž zbytek po dělení číslem n je roven i. Vypište rozklad množiny $\mathbb{Z}$ pro případy
(a) $n = 2$
(b) $n = 3$
(c) $n = 5$
Označme $O(n)$ množinu $\{\mathbb{Z}_0, \dots, \mathbb{Z}_{n-1}\}$ a definujme operace $+$ a $\cdot$ na $O(n)$ takto: Nechť $z_1, z_2 \in \mathbb{Z}$, $z_1 \in \mathbb{Z}_i$, $z_2 \in \mathbb{Z}_j$. Pak platí $z_1 = p_1 n + i$, $z_2 = p_2 n + j$, tedy
$$z_1 + z_2 = (p_1 + p_2)n + (i + j)$$
$$z_1 \cdot z_2 = (p_1 p_2 n + p_1 j + p_2 i)n + ij,$$
což znamená, že součet (součin) libovolných dvou prvků z třídy $\mathbb{Z}_i$ a $\mathbb{Z}_j$ padne do *téže* třídy $\mathbb{Z}_k$, kde k je zbytek při dělení čísla $i + j$ číslem n (resp. $\mathbb{Z}_l$, kde l je zbytek při dělení čísla $i \cdot j$ číslem n).
Klademe: $\mathbb{Z}_i + \mathbb{Z}_j = \mathbb{Z}_k$, $\mathbb{Z}_i \cdot \mathbb{Z}_j = \mathbb{Z}_l$, kde k, l jsou stejné jako výše. Dokažte, že množina $O(n)$ s takto definovanými operacemi sčítání a násobení je komutativní a asociativní okruh s jednotkou (určete jednotku tohoto okruhu!); nazývá se *okruh zbytkových tříd modulo n*. Určete nulový prvek a inverzní prvek k $\mathbb{Z}_i$ vzhledem ke sčítání. Dokažte, že pro $n = 2$ je $O(n)$ pole. Vyšetřete, zda jsou poli okruhy $O(3)$, $O(4)$, $O(5)$.

21. Určete charakteristiku
    (a) číselného pole,
    (b) pole $O(2)$.

22. Dokažte, že zobrazení: $\det GL(n, \mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot)$ je homomorfismus grup. Určete jeho jádro Ker(det) a obraz Im(det).

Zápočtové příklady

1. Dokažte, že množina $A \subset G$ je podgrupa $\Leftrightarrow$ když pro $\forall a, b \in A$ platí $ab^{-1} \in A$.

2. *Galileiho grupa transformací*. Dokažte, že množina transformací $\mathbb{R} \times \mathbb{R}^3 \to \mathbb{R} \times \mathbb{R}^3$ typu
$$\vec{r}\,' = \vec{r} + \vec{v}t, \quad t' = t \tag{$**$}$$
kde $\vec{v}$ je konstantní vektor, tvoří grupu s operací skládání transformací. (Transformace (**) nazýváme *Galileiho transformace*). Dokažte dále, že transformace prostoru $\mathbb{R} \times \mathbb{R}^3$ definované vztahy $\vec{r}\,' = A\vec{r} + \vec{v}t + \vec{u}$, $t' = t$ tvoří grupu (*Galileiho grupa*). Ukažte, že libovolnou transformaci z Galileiho grupy lze vyjádřit jako složení rotace, translace a Galileiho transformace. Rozhodněte, zda grupa Galileiho transformací, resp. Galileiho grupa je Abelova.

3. Dokažte, že množina spojitých reálných funkcí s operací sčítání a násobení funkcí je okruh. Rozhodněte, zda tento okruh je
    (a) komutativní,
    (b) asociativní
Má tento okruh jednotku? Má dělitele nuly?

4. Uvažujme množinu všech vektorů v $\mathbb{R}^3$ s operacemi sčítání vektorů a vektorového součinu vektorů, definovanými takto: je-li $\vec{u} = (u_1, u_2, u_3)$, $\vec{v} = (v_1, v_2, v_3)$, klademe

$$\vec{u} + \vec{v} = (u_1 + v_1, u_2 + v_2, u_3 + v_3)$$

$$\vec{u} \times \vec{v} = (u_2v_3 - u_3v_2, -u_1v_3 + v_1u_3, u_1v_2 - u_2v_1);$$

(někdy píšeme také

$$\vec{u} \times \vec{v} = \begin{vmatrix} \vec{e}_1 & \vec{e}_2 & \vec{e}_3 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix},$$

kde $\vec{e}_1, \vec{e}_2, \vec{e}_3$ jsou jednotkové vektory ve směru "souřadnicových os"). Dokažte, že $(\mathbb{R}^3, +, \times)$ je okruh. Je tento okruh komutativní? Je asociativní? Má dělitele nuly? Má jednotku?

5. Dokažte, že existuje surjektivní homomorfismus obecné lineární grupy $GL(n, \mathbb{R})$ na multiplikativní grupu reálných čísel $(\mathbb{R} \setminus \{0\}, \cdot)$.

6. Nechť $f : G \to G'$ je homomorfismus grup. Dokažte, že Ker f je podgrupa v G a Im f je podgrupa v G'.