4 Cvičení 4: Homomorfismy a další vlastnosti grup

Teorie: Nyní se budeme zabývat zobrazeními mezi grupami. Budeme navíc požadovat, aby toto zobrazení zachovávalo danou operaci. Je proto důležité rozumět pojmům jako injektivní zobrazení, surjektivní zobrazení a umět obě vlastnosti dokazovat.

Definice 16. Nechť $(G, *)$, $(H, \odot)$ jsou grupy. Řekneme, že zobrazení $\varphi : G \to H$ je homomorfismus, jestliže pro všechna $a, b \in G$ platí, že

$$\varphi(a * b) = \varphi(a) \odot \varphi(b).$$

Je-li navíc toto zobrazení injektivní, mluvíme o injektivním homomorfismu (neboli o vnoření). Je-li surjektivní, říkáme danému zobrazení surjektivní homomorfismus. Jedná-li se o bijektivní homomorfismus, potom mluvíme o izomorfismu grup, nebo též říkáme, že dané grupy jsou izomorfní.

Definice 17. Nechť $(G, *)$, $(H, \odot)$ jsou grupy, $\varphi : G \to H$ homomorfismus. Potom množinu $\operatorname{Ker} \varphi = \{g \in G \mid \varphi(g) = e_H\}$ nazýváme jádro homomorfismu φ.

Jádro homomorfismu je podgrupa grupy G (ověřte si) a má důležitou vlastnost:

Věta 10. *Nechť $(G, *)$, $(H, \odot)$ jsou grupy, $\varphi : G \to H$ homomorfismus. Potom φ je injektivní (vnoření) právě tehdy, když* $\operatorname{Ker} \varphi = \{e_G\}$.

Definice 18. Nechť $(G, *)$, $(H, \odot)$ jsou grupy, $\varphi : G \to H$ homomorfismus. Potom množinu $\operatorname{Im} \varphi = \{h \in H \mid \exists g \in G : \varphi(g) = h\}$ nazýváme obraz homomorfismu φ.

Obraz homomorfismu je podgrupa grupy H (opět si prosím ověřte) a má také důležitou vlastnost:

Věta 11. *Nechť $(G, *)$, $(H, \odot)$ jsou grupy, $\varphi : G \to H$ homomorfismus. Potom φ je surjektivní právě tehdy, když* $\operatorname{Im} \varphi = H$.

Na závěr povídání o algebraických strukturách s jednou operací si uveďme ještě několik důležitých pojmů a vlastností.

Definice 19. Řekneme, že je grupa cyklická, jestliže je generovaná nějakým svým prvkem.

Definice 20. Počet prvků konečné grupy budeme nazývat řád dané grupy.

Definice 21. Nechť G je grupa, $a \in G$. Potom nejmenší přirozené číslo n takové, že $a^n = e_G$, nazýváme řád prvku a v grupě G. Pokud takové přirozené číslo neexistuje, říkáme, že daný prvek je řádu nekonečno.

Pro řád prvku a grupy platí řada zajímavých tvrzení. My si uveďme jen dvě:

Věta 12. *Řád libovolného prvku konečné grupy dělí řád celé grupy.*

Věta 13. *Řád libovolné podgrupy dané konečné grupy dělí řád celé grupy.*

Příklad 54. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi(([a]_4, [b]_3)) = [a - b]_{12}$
2. $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi(([a]_4, [b]_3)) = [6a + 4b]_{12}$
3. $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi(([a]_4, [b]_3)) = [0]_{12}$

Výsledek.

1. Není zobrazení
2. Je homomorfismus, který není ani injektivní ani surjektivní
3. Je homomorfismus, který není ani injektivní ani surjektivní

Příklad 55. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*$, $\varphi\left(\frac{p}{q}\right) = \frac{q}{p}$
2. $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*$, $\varphi\left(\frac{p}{q}\right) = \frac{p^2}{q^2}$
3. $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*$, $\varphi\left(\frac{p}{q}\right) = \frac{p^2+q^2}{pq}$

Výsledek.

1. Je izomorfismus
2. Je homomorfismus, který není surjektivní ani injektivní.
3. Není homomorfismus

Příklad 56. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z}_4 \to \mathbb{C}^*$, $\varphi([a]_4) = i^a$
2. $\varphi : \mathbb{Z}_5 \to \mathbb{C}^*$, $\varphi([a]_4) = i^a$
3. $\varphi : \mathbb{Z}_4 \to \mathbb{C}^*$, $\varphi([a]_4) = (-i)^a$
4. $\varphi : \mathbb{Z} \to \mathbb{C}^*$, $\varphi(a) = i^a$

Výsledek.

1. Je homomorfismus, který není injektivní ani surjektivní.
2. Není zobrazení.
3. Je homomorfismus, který není injektivní ani surjektivní.
4. Je homomorfismus, který není ani injektivní ani surjektivní.

Příklad 57. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathcal{GL}_2(\mathbb{R}) \to \mathbb{R}^*$, $\varphi(A) = |A|$
2. $\varphi : \mathcal{GL}_2(\mathbb{R}) \to \mathbb{R}^*$, $\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a^2 + b^2$.
3. $\varphi : \mathcal{GL}_2(\mathbb{R}) \to \mathbb{R}^*$, $\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ac + bd$.

Výsledek.

1. Je surjektivní homomorfismus, který není injektivní.
2. Není homomorfismus.
3. Není homomorfismus.

Příklad 58. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z} \to \mathbb{Z}_3$, $\varphi(a) = [a]_3$
2. $\varphi : \mathbb{Z} \to \mathbb{Z}_3$, $\varphi(a) = [|a|]_3$
3. $\varphi : \mathbb{Z} \to \mathbb{Z}_2$, $\varphi(a) = [a]_2$

4. $\varphi : \mathbb{Z} \to \mathbb{Z}_2$, $\varphi(a) = [|a|]_2$

Výsledek.

1. Je surjektivní homomorfismus, který není injektivní.
2. Není homomorfismus.
3. Je surjektivní homomorfismus, který není injektivní.
4. Je surjektivní homomorfismus, který není injektivní.

Příklad 59. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z}_3 \to \mathbb{A}_4$, $\varphi([a]_3) = (1,2,4) \circ (1,3,2)^a \circ (1,4,2)$
2. $\varphi : \mathbb{Z}_3 \to \mathbb{A}_4$, $\varphi([a]_3) = (1,2) \circ (1,3,2)^a$

Výsledek.

1. Je homomorfismus.
2. Není homomorfismus.

Příklad 60. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{C} \to \mathbb{R}$, $\varphi(a + bi) = a + b$
2. $\varphi : \mathbb{C} \to \mathbb{R}$, $\varphi(a + bi) = a$
3. $\varphi : \mathbb{C}^* \to \mathbb{R}^*$, $\varphi(a + bi) = a^2 + b^2$
4. $\varphi : \mathbb{C}^* \to \mathbb{R}^*$, $\varphi(c) = 2|c|$
5. $\varphi : \mathbb{C}^* \to \mathbb{R}^*$, $\varphi(c) = |c|^3$
6. $\varphi : \mathbb{C}^* \to \mathbb{R}^*$, $\varphi(c) = 1/|c|$

Výsledek.

1. Není homomorfismus.
2. Je surjektivní homomorfismus.
3. Je surjektivní homomorfismus.
4. Je surjektivní homomorfismus.
5. Je surjektivní homomorfismus.
6. Je surjektivní homomorfismus.

Příklad 61. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = 2a$
2. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = a + 1$
3. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = 3|a|$
4. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = 1$

Výsledek.

1. Je injektivní homomorfismus.
2. Není homomorfismus.
3. Není homomorfismus.
4. Není homomorfismus.

Příklad 62. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}^*$, $\varphi((a, b, c)) = 2^a 3^b 12^c$
2. $\varphi : \mathbb{Z}_3^* \times \mathbb{Z}_5 \to \mathbb{Z}_5$, $\varphi((a, b)) = b^a$
3. $\varphi : \mathbb{Z}_2 \times \mathbb{Z} \to \mathbb{Z}$, $\varphi(([a]_2, b)) = b$

Výsledek.

1. Je homomorfismus.
2. Není homomorfismus.
3. Je surjekivní homomorfismus.

Příklad 63. Popište všechny homomorfismy φ

1. $\varphi : \mathbb{Z} \to \mathbb{Z}$
2. $\varphi : \mathbb{Z}_5 \to \mathbb{Z}$
3. $\varphi : \mathbb{Z} \to \mathbb{Z}_5$
4. $\varphi : \mathbb{Z}_5 \to \mathbb{Z}_5$

Příklad 64. Popište všechny homomorfismy φ

1. $\varphi : \mathbb{Z}_{15} \to \mathbb{Z}_6$
2. $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_{15}$
3. $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$
4. $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$

Příklad 65. Určete dvě různá přirozená čísla m, n tak, aby byly grupy $\mathbb{Z}_m^\times$ a $\mathbb{Z}_n^\times$ izomorfní.

Výsledek. 3,4

Příklad 66. Nechť G je komutativní grupa. Nechť $\varphi : G \to G$, $\varphi(g) = g^2$. Dokažte, že φ je homomorfismus. Uveďte příklad grup G, kdy se jedná o izomorfismus a kdy se izomorfismus nejedná.

Příklad 67. Nechť G je grupa. Nechť $\varphi : G \to G$, $\varphi(g) = g^{-1}$. Dokažte, že φ je homomorfismus právě tehdy, když je G komutativní.

Příklad 68. Dokažte, že součin cyklických grup nemusí být cyklická grupa.

Řešení. Například $\mathbb{Z}_2 \times \mathbb{Z}_2$

Příklad 69. Určete řády všech prvků v grupě $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$. vyberte generátory těchto grup.

Příklad 70. Spočítejte řád prvku

1. 60 v grupě $\mathbb{Z}_{64}$.
2. 7 v grupě $\mathbb{Z}_{17}^*$.
3. $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ v grupě $\mathcal{GL}_2(\mathbb{Z}_2)$.

Příklad 71. Nechť G je grupa. Označme $Aut(G)$ množinu všech izomorfismů $\varphi : G \to G$. Dokažte, že $Aut(G)$ tvoří grupu. Určete, kolik prvků má $Aut(\mathbb{Z}_8^\times)$, $Aut(\mathbb{Z}_8)$.

5 Cvičení 5: Okruhy a polynomy

Teorie: V tomto cvičení se podíváme na algebraické struktury se dvěma operacemi.

Definice 22. Nechť $(R, \oplus)$ je komutativní grupa a $(R, \odot)$ pologrupa s neutrálním prvkem. Nechť pro libovolné $a, b, c \in R$ platí, že

$$\begin{aligned} a \odot (b \oplus c) &= a \odot b \oplus a \odot c \\ (b \oplus c) \odot a &= b \odot a \oplus c \odot a \end{aligned}$$

Potom $(R, \oplus, \odot)$ nazýváme okruh. Je-li navíc operace $\odot$ komutativní, potom dané struktuře říkáme komutativní okruh.

Například $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_6, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ a $(Mat_2(\mathbb{R}), +, \cdot)$ tvoří okruhy.

Definice 23. Nechť $(R, \oplus, \odot)$ je okruh, $a, b \in R$. Potom prvkům a, b říkáme dělitelé nuly, pokud platí, že $a, b \neq 0$ a $a \odot b = 0$.

Definice 24. Netriviální komutativní okruh bez dělitelů nuly nazýváme obor integrity.

Například $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_7, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ tvoří obory integrity, oproti tomu $(Mat_2(\mathbb{R}), +, \cdot)$ a $(\mathbb{Z}_6, +, \cdot)$ obory integrity nejsou.

Příklad 72. Obor integrity, kde ke každému nenulovému prvku existuje prvek inverzní, se nazývá těleso.

Například $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_7, +, \cdot)$ tvoří těleso, oproti tomu $(\mathbb{Z}_6, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ tělesa nejsou.

Definice 25. Libovolnou konečnou posloupnost prvků daného okruhu nazýváme polynom.

My jsme zvyklí psát polynom ve tvaru $a_n x^n + \cdots + a_1 x + a_0$. Protože můžeme polynomy sčítat a násobit, nabízí se otázka, co za strukturu tvoří množina všech polynomů s těmito operacemi. Platí následující věta.

Věta 14.

1. *Množina všech polynomů tvoří spolu se sčítáním a násobením okruh.*
2. *Okruh polynomů nad oborem integrity je obor integrity.*
3. *Okruh polynomů nad tělesem je obor integrity.*

Definice 26. Polynom $f \in R[x]$ nazýváme ireducibilní nad R, jestliže je nekonstantní a nelze ho rozložit na součin dvou nekonstantních polynomů.