Vježbe

Lagrangeova teorema

Neka je G konačna grupa. Tada red svake njene podgrupe dijeli red grupe.

① Neka su $H_1, H_2 \leq G$ (G je konačna grupa). Ako su redovi podgrupa H_1 i H_2 uzajamno prosti brojevi, tada je $H_1 \cap H_2 = \{e\}$.

$H_1 \cap H_2 \leq H_1$ $\quad |H_1| = n$

$H_1 \cap H_2 \leq H_2$ $\quad |H_2| = m$

$|H_1 \cap H_2| = k$

L. T. $\Rightarrow k|n$ i $k|m \Rightarrow k = 1$ jer je $NZD(n,m)=1$

$\Rightarrow |H_1 \cap H_2| = 1$

$H_1 \cap H_2 = \{e\}$

Ciklična grupa

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = [a]$

$ord(a) = m \in \mathbb{N}$

$\langle a \rangle = \{a, a^2, a^3, \dots, a^{m-1}, e\}$

$|\langle a \rangle| = ord(a)$

$ord(a) = m \quad (a^m = e)$

Tvrdimo da $\langle a \rangle = \underbrace{\{e, a, \dots, a^{m-1}\}}_{H}$.

Jasno, $\boxed{H \subseteq \langle a \rangle}$ (*)

$x \in \langle a \rangle \Rightarrow x = a^n, n \in \mathbb{Z}$

$n = mq + r, \quad r \in \{0, \dots, m-1\}$.

$x = a^n = a^{mq} \cdot a^r = \underbrace{(a^m)^q}_{\sim e} \cdot a^r = e^q \cdot a^r = a^r \in H$

$\Rightarrow \boxed{\langle a \rangle \subseteq H}$ (**). Iz (*) i (**) $\Rightarrow$

$\Rightarrow \langle a \rangle = \{e, a, \dots, a^{m-1}\}$.

Svi elementi u $\{e, \dots, a^{m-1}\}$ su različiti jer $a^k = a^l \overset{k>l}{\underset{\text{bez gub.}}{\Rightarrow}} a^{k-l} = e$

$k, l \in \{0, \dots, m-1\}$ $\quad k - l < m$

$ord(a)$

↯

Primjeri.

$\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ – gen. el. su 1 i 5

$(\mathbb{Z},+)$ – generatorni elementi su 1 i -1

(2.) Svaka grupa prostog reda je ciklična.

$a \in G, a \neq e$

$H = \langle a \rangle$

$|H| = ord(a)$

$ord(a) = |H| \mid ord(G) = p$ (Lagrangeova teorema)

1° $ord(a) = |H| = 1$

2° $ord(a) = |H| = p$

1° je nemoguće jer $ord(a) > 1$

$a^1 = e$ ↯

$\Rightarrow |H| = p, |G| = p$, $H \leq G$ $\Rightarrow H = G = \langle a \rangle$

(3.) Svaka ciklična grupa je komutativna.

? $\forall x, y \in G = \langle a \rangle \quad xy = yx$

$x = a^k, y = a^l$

$xy = a^k a^l = \underbrace{(a \cdot a \cdots a)}_{k \text{ puta}} \cdot \underbrace{(a \cdot a \cdots a)}_{l \text{ puta}} =$

$= \underbrace{(a \cdot a \cdots a)}_{l \text{ puta}} \cdot \underbrace{(a \cdot a \cdots a)}_{k \text{ puta}} = a^l a^k = yx$

(4.) Dokazati da su tve grupe reda ≤ 5 komutativne.

$\overset{1}{=}$ $\{e\}$ $e \cdot e = e \cdot e$

$\overset{2,3,5}{=\!=}$ G je prostog reda $\overset{\text{Zad. 2.}}{\Longrightarrow}$ G je ciklična

$\overset{\text{Zad. 3}}{\Longrightarrow}$ G je komutativna

$\overset{4}{=}$ $G = \{e, a, b, c\}$

$|\langle a \rangle| \mid 4 \Rightarrow |\langle a \rangle| \in \{1, 2, 4\}$

$|\langle a \rangle| = \text{ord}(a) \neq 1$

1° $|\langle a \rangle| = 4 = |H|$

$H = G = \langle a \rangle$

ciklična - komutativna

2° $|\langle a \rangle| = 2$

$a^2 = e$

Analogno $b^2 = e$, $c^2 = e$.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$a \cdot b \in \{e, a, b, c\}$

$a \mid a \cdot b = e$

$a^2 b = a$

$\tilde{e}\, b = a$ // ↯

$a \mid a \cdot b = a$

$a^2 b = a^2$

$b = e$ ↯

$a \cdot b = b / b$

$ab^2 = b^2$

$a = e$ ↳

∃ Kelijeve tablice $\Rightarrow$ komutativna grupa.

⑤ Svaka podgrupa ciklične grupe je ciklična.

$G = \langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$

$H \leq G$

1° $H = \{e\} = \langle e \rangle$

2° $H \neq \{e\}$

$\Downarrow$

$\exists a^k \in H, k \in \mathbb{N}$ (also je $a^{k \overset{\in}{,} k<0}$ onda $(a^k)^{-1} = a^{-k} \in H, -k \in \mathbb{N}$)

$l = \min \{ k \in \mathbb{N} \mid a^k \in H \}$ (*), $a^l \in H$

? $H = \langle a^l \rangle$? Jasno $\langle a^l \rangle \subseteq H$

$\langle (a^l)^z \mid z \in \mathbb{Z} \rangle$

Neka je $x \in H$ proizvoljno.

$H \subseteq G \Rightarrow x \in G = \langle a \rangle$

$x = a^s \overset{?}{=} (a^l)^{?}$

Euklidov algoritam:

$s = l \cdot q + r, \quad r \in \{0, \dots, l-1\}$

$x = a^s = a^{l \cdot q + r} = a^{l \cdot q} \cdot a^r = \underbrace{(a^l)^q}_{\in H} \cdot a^r \rightarrow$ Tablguačijemo da $a^r \in H$

$\uparrow$
H

Ako je $r \in \{1, \dots, l-1\}$ onda $\lightning$ sa (*)

$\Rightarrow r = 0$

$\Downarrow$

$l \mid s$

$s = l \cdot q$

$$x = a^s = a^{l \cdot q} = (a^l)^q$$

(6.) Odrediti neizomorfne podgrupe date grupe.

a) $(\mathbb{Z}_{12}, +_{12})$

b) $(\mathbb{Z}_{15}, +_{15})$

a) $\mathbb{Z}_{12}$ - ciklična grupa

$\mathbb{Z}_{12} = \langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \dots, \bar{11}\}$

$H \leq G$

$|H| \mid |G|$

$|H| \in \{1, 2, 3, 4, 6, 12\}$

$H_1 = \{\bar{0}\} = \langle \bar{0} \rangle$

$H_2 = \{\bar{0}, \bar{6}\} = \langle \bar{6} \rangle$

$H_3 = \{\bar{0}, \bar{4}, \bar{8}\} = \langle \bar{4} \rangle = \langle \bar{8} \rangle$

$H_4 = \{\bar{3}, \bar{6}, \bar{9}, \bar{0}\} = \langle \bar{3} \rangle = \langle \bar{9} \rangle$

$H_6 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} = \langle \bar{2} \rangle = \langle \bar{10} \rangle$

$H_{12} = \mathbb{Z}_{12} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$

b) $|H| \in \{1, 3, 5, 15\}$

$H_1 = \{e\}$

$H_{15} = Z_{15} = \langle \bar{1} \rangle = \langle \bar{2} \rangle = \langle \bar{4} \rangle = \langle \bar{7} \rangle = \langle \bar{8} \rangle =$
$= \langle \bar{11} \rangle = \langle \bar{13} \rangle = \langle \bar{14} \rangle$

$H_3 = \{\bar{0}, \bar{5}, \bar{10}\} = \langle \bar{5} \rangle = \langle \bar{10} \rangle$

$H_5 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}\} = \langle \bar{3} \rangle = \langle \bar{6} \rangle = \langle \bar{9} \rangle = \langle \bar{12} \rangle$

Vježba

Direktna produkt grupa

$(G_1, \cdot)$, $(G_2, *)$

$G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$

$(G_1 \times G_2, \circledast)$

$(x_1, y_1) \circledast (x_2, y_2) = (x_1 \cdot x_2, y_1 * y_2)$

e_1 jed. u G_1, e_2 jed. u G_2

$e = (e_1, e_2)$ jed. u $G_1 \times G_2$

$(x, y)^{-1} = (x^{-1}, y^{-1})$

1. Neka je $G = G_1 \times G_2$ direktni produkt grupa G_1 i G_2 i preslikavanja

$p_1 : G_1 \times G_2 \to G_1$, $p_1(x, y) = x$

$p_2 : G_1 \times G_2 \to G_2$, $p_2(x, y) = y$

} projekcije

Dokazati da su p_1 i p_2 homomorfizmi.

$(x_1, y_1), (x_2, y_2) \in G_1 \times G_2$

$p_1((x_1, y_1) \circledast (x_2, y_2)) = p_1(x_1 \cdot x_2, y_1 * y_2) =$

$= x_1 \cdot x_2$

$p_1(x_1, y_1) = x_1$, $p_1(x_2, y_2) = x_2$

$p_1(x_1, y_1) \cdot p_1(x_2, y_2) = x_1 \cdot x_2 \Rightarrow$

$\Rightarrow p_1((x_1, y_1) \otimes (x_2, y_2)) = p_1(x_1, y_1) \cdot p_1(x_2, y_2)$

Analogno za p_2.

(2.) Dokažati da su homomorfizmi sljedeća preslikavanja:

$\left.\begin{array}{l} \mu_1 : G_1 \to G_1 \times G_2, \ \mu_1(a) = (a, e_2) \\ \mu_2 : G_2 \to G_1 \times G_2, \ \mu_2(b) = (e_1, b) \end{array}\right\}$ utapanja

$a_1, a_2 \in G_1$

$\mu_1(a_1 \cdot a_2) = (a_1 \cdot a_2, e_2) = (a_1 \cdot a_2, e_2 * e_2) =$

$= \mu_1(a_1, e_2) \otimes (a_2, e_2) = \mu_1(a_1) \otimes \mu_1(a_2) \Rightarrow$

$\Rightarrow \mu_1$ je homomorfizam, analogno za μ_2

(3.) Ako su $C_2 = \{a, a^2 = e_1\}$ i $C_3 = \{b, b^2, b^3 = e_2\}$ ciklične grupe reda 2 i 3 respektivno, naći $C_2 \times C_3$.

$C_2 \times C_3 = \{(a,b), (a,b^2), (a,e_2), (e_1,b), (e_1,b^2), (e_1,e_2)\}$

$(C_2 \times C_3, \otimes) \stackrel{?}{=} \langle (a,b) \rangle$

$(a,b)^1 = (a,b)$

$(a,b)^2 = (a,b) \otimes (a,b) = (a^2, b^2) = (e_1, b^2)$

$(a,b)^3 = (e_1, b^2) \otimes (a,b) = (a, b^3) = (a, e_2)$

$(a,b)^4 = (a, e_2) \otimes (a,b) = (a^2, b) = (e_1, b)$

$(a,b)^5 = (e_1, b) \otimes (a,b) = (a, b^2)$

$(a,b)^6 = (a, b^2) \otimes (a,b) = (a^2, b^3) = (e_1, e_2)$

$\langle (a,b) \rangle = C_2 \times C_3$

Napomena: $C_m \times C_n$ je ciklična ako i $nzd(m,n) = 1$.

(4.) Neka su A i B grupe i $A \times B$ njihov dir. pr. Dokazati da $A \times B$ sadrži podgrupe A' i B' koje su izomorfne grupama A i B respektivno.

$A' = A \times \{e_2\}$, $B' = \{e_1\} \times B$

$A' \subseteq A \times B$

$A' \overset{?}{\leq} A \times B$

$(a_1, e_2), (a_2, e_2) \in A'$

$a_1 \in A$, $a_2 \in A$

$(a_1, e_2) \otimes (a_2, e_2)^{-1} \overset{?}{\in} A'$

$(a_1, e_2) \otimes (a_2^{-1}, e_2^{-1}) = (a_1, e_2) \otimes (a_2^{-1}, e_2) = (a_1 a_2^{-1}, e_2 * e_2)$

$= (a_1 a_2^{-1}, e_2) \in A' \Rightarrow A' \leq A \times B$

$a_1 a_2^{-1} \in A$, $e_2 \in B$

$\phi : A' \to A$

$\phi(a_1, e_2) = a$

$\phi((a_1, e_2) \otimes (a_2, e_2)) = \phi(a_1 a_2, e_2) = a_1 a_2 =$

$= \phi(a_1, e) \cdot \phi(a_2, e) \Rightarrow \phi$ je homomorfizam

"na":

$a \in A$

$(a, e_2) \xrightarrow{\phi} a$

$\in A'$

"1-1":

$\phi(a, e_2) = \phi(b, e_2)$

$a \quad\quad b$

$\Downarrow \quad\quad \Downarrow$

$a = b$

$\Downarrow$

$(a, e_2) = (b, e_2)$

ϕ je izomorfizam

(5.) Neka je $G = A \times B$. Dokazati da su $A' : B'$ normalne podgrupe u $A \times B$.

$A', B' \overset{?}{\triangleleft} A \times B$

I način.

$p_2 : A \times B \to B$ je homomorfizam (zad. 1)

$\operatorname{Ker} p_2 = \{(a, b) \in A \times B \mid p_2(a, b) = e_2\} =$

$= \{(a, b) \in A \times B \mid b = e_2\} = A \times \{e_2\} = A' \Rightarrow$

Обнова т. о hom. gr. $\Rightarrow A' \triangleq A \times B$

За B' поматрати p_1.

II начин.

$A' \overset{?}{\triangleq} A \times B$

$(a, e_2) \in A'$

$(g_1, g_2) \in A \times B$

$g_1 a \in A$

$g_2 \in B$

$(g_1, g_2) \circledast (a, e_2) \circledast (g_1, g_2)^{-1} \overset{?}{\in} A'$

$\|$

$(g_1, g_2) \circledast (a, e_2) \circledast (g_1^{-1}, g_2^{-1}) = (g_1 a g_1^{-1}, g_2 e_2 g_2^{-1}) =$

$= (g_1 a g_1^{-1}, e_2) \in A'$

$\in A$