

3. WYKŁAD 3: WARSTWY GRUPY WZGLĘDEM PODGRUPY. TWIERDZENIE LAGRANGE'A.

Definicja 3.1. Niech $(G, \cdot)$ będzie grupą i niech $a \in G$. Odwzorowanie $\lambda_a : G \rightarrow G$ dane wzorem

$$\lambda_a(x) = ax$$

nazywamy **przesunięciem lewostronnym o element a** , natomiast odwzorowanie $\pi_a : G \rightarrow G$ dane wzorem

$$\pi_a(x) = xa$$

nazywamy **przesunięciem prawostronnym o element a** .

Twierdzenie 3.1. Przesunięcia lewostronne i prawostronne są bijekcjami oraz

$$\lambda_a \circ \lambda_b = \lambda_{ab}, \pi_a \circ \pi_b = \pi_{ba}.$$

Dowód. Dowód przeprowadzimy dla przesunięć lewostronnych, rozumowanie dla przesunięć prawostronnych jest podobne. Dla $a, b \in G$ i ustalonego $x \in G$ mamy:

$$\lambda_a \circ \lambda_b(x) = \lambda_a(\lambda_b(x)) = a(bx) = (ab)x = \lambda_{ab}(x).$$

W szczególności

$$\lambda_a \circ \lambda_{a^{-1}} = \lambda_{1_G} = id_G \text{ oraz } \lambda_{a^{-1}} \circ \lambda_a = id_G,$$

a więc λ_a jest bijekcją. □

Definicja 3.2. Niech $(G, \cdot)$ będzie grupą, $H < G$ i $a \in G$. Zbiór

$$aH = \lambda_a(H) = \{ah : h \in H\}$$

nazywamy **warstwą lewostronną grupy G względem podgrupy H** (wyznaczoną przez element a). Zbiór wszystkich warstw lewostronnych oznaczamy

$$W_L(H) = \{aH : a \in G\}.$$

Zbiór

$$Ha = \pi_a(H) = \{ha : h \in H\}$$

nazywamy **warstwą prawostronną grupy G względem podgrupy H** (wyznaczoną przez element a). Zbiór wszystkich warstw prawostronnych oznaczamy

$$W_P(H) = \{Ha : a \in G\}.$$

Przykłady:

(1) Rozważmy grupę $\mathbb{Z}_6$ oraz $H = \{0, 3\} < \mathbb{Z}_6$. Wówczas:

$$\begin{array}{ll} 1 + H &= \{1, 4\}, & 4 + H &= \{4, 1\} = 1 + H, \\ 2 + H &= \{2, 5\}, & 5 + H &= \{5, 2\} = 2 + H, \\ 3 + H &= \{3, 0\} = H, & 0 + H &= \{0, 3\} = H, \end{array}$$

a więc $W_L(H) = \{H, 1 + H, 2 + H\}$.

(2) Rozważmy grupę $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$ oraz $H = \{ID_3, S_1\} < D(3)$. Wówczas:

$$\begin{array}{ll} ID_3 \circ H &= \{ID_3, S_1\}, & H \circ ID_3 &= \{ID_3, S_1\}, \\ S_1 \circ H &= \{ID_3, S_1\}, & H \circ S_1 &= \{ID_3, S_1\}, \\ S_2 \circ H &= \{S_2, O_2\} = H, & H \circ S_2 &= \{S_2, O_1\}, \end{array}$$

a więc warstwy lewostronne i warstwy prawostronne mogą się różnić.

Definicja 3.3. Niech $(G, \cdot)$ będzie grupą, $H < G$ i $a, b \in G$. Mówimy, że a przystaje lewostronnie do b według modułu H , co oznaczamy przez $a {}_H\equiv b$, jeśli

$$a^{-1}b \in H.$$

Mówimy, że a przystaje prawostronnie do b według modułu H , co oznaczamy przez $a \equiv_H b$, jeśli

$$ab^{-1} \in H.$$

Twierdzenie 3.2. Niech $(G, \cdot)$ będzie grupą, $H < G$ i $a \in G$.

- (1) Relacja ${}_H\equiv$ jest równoważnością oraz $[a]_{{}_H\equiv} = aH$.
- (2) Relacja $\equiv_H$ jest równoważnością oraz $[a]_{\equiv_H} = Ha$.

Dowód. Przeprowadzimy dowód dla warstw lewostronnych, rozumowanie dla warstw prawostronnych przebiega analogicznie. Ponieważ, dla $g \in G$ $g^{-1}g = 1 \in H$, więc $g {}_H\equiv g$ i tym samym relacja ${}_H\equiv$ jest zwrotna. Jeżeli ustalimy $g, h \in G$ takie, że $g {}_H\equiv h$, czyli $g^{-1}h \in H$, to wówczas $h^{-1}g = (g^{-1}h)^{-1} \in H$, czyli $h {}_H\equiv g$ i relacja ${}_H\equiv$ jest symetryczna. Podobnie, jeżeli ustalimy $g, h, k \in G$ takie, że $g {}_H\equiv h$ i $h {}_H\equiv k$, czyli takie, że $g^{-1}h \in H$ i $h^{-1}k \in H$, to wówczas $g^{-1}k = g^{-1}h h^{-1}k = \underbrace{g^{-1}h}_{\in H} \underbrace{h^{-1}k}_{\in H} \in H$, czyli $g {}_H\equiv k$ i

relacja ${}_H\equiv$ jest przechodnia. Tym samym pokazaliśmy, że ${}_H\equiv$ jest relacją równoważnościową na zbiorze G i pozostaje opisać jej klasy abstrakcji. W tym celu zauważmy, że

$$g \in [a]_{{}_H\equiv} \Leftrightarrow a {}_H\equiv g \Leftrightarrow a^{-1}g \in H \Leftrightarrow \exists h \in H (a^{-1}g = h) \Leftrightarrow g = ah \in aH.$$

□

Wniosek 3.1. Niech $(G, \cdot)$ będzie grupą, $H < G$ i $a, b \in G$. Wówczas:

- (1) $\forall a \in G (a \in aH)$ (symetrycznie: $\forall a \in G (a \in Ha)$).
- (2) Jeśli $aH \neq bH$, to $aH \cap bH = \emptyset$ (symetrycznie: jeśli $Ha \neq Hb$, to $Ha \cap Hb = \emptyset$).
- (3) Jeśli $aH \cap bH \neq \emptyset$, to $aH = bH$ (symetrycznie: jeśli $Ha \cap Hb \neq \emptyset$, to $Ha = Hb$).
- (4) $G = \bigcup_{a \in G} aH$ (symetrycznie: $G = \bigcup_{a \in G} Ha$).
- (5) $aH = bH$ wtedy i tylko wtedy, gdy $a^{-1}b \in H$ (symetrycznie: $Ha = Hb$ wtedy i tylko wtedy, gdy $ab^{-1} \in H$).

Wniosek 3.2. Niech $(G, \cdot)$ będzie grupą, $H < G$ i $a \in G$. Wówczas:

- (1) Każda warstwa lewostronna aH jest równoliczna ze zbiorem H .
- (2) Każda warstwa prawostronna Ha jest równoliczna ze zbiorem H .
- (3) Każda warstwa lewostronna aH jest równoliczna z warstwą prawostronną Ha .

Dowód. Równoliczność w punkcie (1) ustala bijekcja $\lambda_a : H \rightarrow aH$, równoliczność w punkcie (2) ustala bijekcja $\pi_a : H \rightarrow Ha$, a punkt (3) jest oczywistym wnioskiem z (1) i (2). □

Twierdzenie 3.3. Niech $(G, \cdot)$ będzie grupą, niech $H < G$. Wówczas zbiory $W_L(H)$ i $W_P(H)$ są równoliczne.

Dowód. Zdefiniujmy funkcję $\phi : W_L(H) \rightarrow W_P(H)$ wzorem

$$\phi(aH) = Ha^{-1}.$$

Zauważmy, że funkcja ta jest poprawnie określona, założmy bowiem, że $aH = bH$: wówczas $a^{-1}b \in H$, a stąd $a^{-1}(b^{-1})^{-1} \in H$, czyli $Ha^{-1} = Hb^{-1}$. Pozostaje sprawdzić, że ϕ istotnie jest bijekcją.

ϕ jest różnowartościowa, założmy bowiem, że $\phi(aH) = \phi(bH)$, czyli że $Ha^{-1} = Hb^{-1}$. Wówczas $a^{-1}(b^{-1})^{-1} \in H$, czyli $a^{-1}b \in H$, więc $aH = bH$. ϕ jest też surjektywna, ustalmy bowiem $Hb \in W_P(H)$: natenczas $Hb = H(b^{-1})^{-1} = \phi(b^{-1}H)$. □

Definicja 3.4. Niech $(G, \cdot)$ będzie grupą, niech $H < G$. Wspólną moc zbiorów $W_L(H)$ i $W_P(H)$ nazywamy **indeksem podgrupy H w grupie G** i oznaczamy $(G : H)$.

Przykłady:

- (3) Rozważmy grupę $\mathbb{Z}_6$ oraz $H = \{0, 3\} < \mathbb{Z}_6$. Wówczas $(\mathbb{Z}_6 : H) = 3$.
- (4) Rozważmy grupę $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$ oraz $H = \{ID_3, S_1\} < D(3)$. Wówczas $(D(3) : H) = 3$.
- (5) Rozważmy grupę $\mathbb{Z}$ oraz $5\mathbb{Z} < \mathbb{Z}$. Weźmy pod uwagę dwie warstwy $a + 5\mathbb{Z}$ i $b + 5\mathbb{Z}$:

$$\begin{aligned} a + 5\mathbb{Z} = b + 5\mathbb{Z} &\Leftrightarrow (-a) + b \in 5\mathbb{Z} \Leftrightarrow 5|b - a \\ &\Leftrightarrow a \equiv b \pmod{5}. \end{aligned}$$

Tym samym funkcja $\psi : W_L(5\mathbb{Z}) \rightarrow \{0, 1, 2, 3, 4\}$ dana wzorem

$$\psi(a + 5\mathbb{Z}) = \text{reszta z dzielenia } a \text{ przez } 5$$

jest różnowartościowa i surjektywna, a więc liczy warstwy. Tym samym $(\mathbb{Z} : 5\mathbb{Z}) = 5$.

- (6) Rozważmy grupę $\mathbb{R}^*$ oraz $\mathbb{R}_+^* = \{x \in \mathbb{R}^* : x > 0\}$. Weźmy pod uwagę dwie warstwy $a\mathbb{R}_+^*$ i $b\mathbb{R}_+^*$:

$$a\mathbb{R}_+^* = b\mathbb{R}_+^* \Leftrightarrow \frac{a}{b} \in \mathbb{R}_+^* \Leftrightarrow \text{sgn}a = \text{sgn}b.$$

Tym samym funkcja $\psi : W_L(\mathbb{R}_+^*) \rightarrow \{\pm 1\}$ dana wzorem

$$\psi(a\mathbb{R}_+^*) = \text{sgn}a$$

jest różnowartościowa i surjektywna, a więc liczy warstwy. Tym samym $(\mathbb{R}^* : \mathbb{R}_+^*) = 2$.

Twierdzenie 3.4 (Lagrange'a). Niech $(G, \cdot)$ będzie grupą skończoną, niech $H < G$. Wówczas

$$|G| = (G : H) \cdot |H|.$$

Dowód. Niech $(G : H) = k$ i niech $a_1H, a_2H, \dots, a_kH$ będą wszystkimi parami różnymi warstwami lewostronnymi. Wówczas

$$a_iH \cap a_jH = \emptyset, \text{ dla } i \neq j \text{ oraz } G = \bigcup_{i=1}^k a_iH,$$

a zatem

$$|G| = \sum_{i=1}^k |a_iH|$$

i ponieważ $|a_iH| = |H|$, więc

$$|G| = \sum_{i=1}^k |H| = k \cdot |H| = (G : H) \cdot |H|.$$

□

Wniosek 3.3. Niech $(G, \cdot)$ będzie grupą skończoną, niech $H < G$. Wówczas

- (1) $(G : H) = \frac{|G|}{|H|}$,
- (2) rząd podgrupy jest dzielnikiem rzędu grupy,
- (3) $(G : \{1_G\}) = |G|$ oraz $(G : G) = 1$.

Przykład:

(7) Rozważmy grupę $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$ oraz $H = \{ID_3, S_1\} < D(3)$. Wówczas

$$(D(3) : H) = \frac{|D(3)|}{|H|} = \frac{6}{3} = 2.$$