

2. WYKŁAD 2: WARSTWY GRUPY WZGLĘDEM PODGRUPY. TWIERDZENIE LAGRANGE'A. RZĄD ELEMENTU GRUPY. GRUPY CYKLICZNE.

2.1. Warstwy grupy względem podgrupy. Twierdzenie Lagrange'a.

Definicja 2.1. 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 2.1. 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 2.2. 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 2.3. 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 $a \equiv_H b$, 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 2.2. Niech $(G, \cdot)$ będzie grupą, $H < G$ i $a \in G$.

- (1) Relacja $\equiv_H$ jest równoważnością oraz $[a]_{\equiv_H} = aH$.
- (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 $g \equiv_H g$ i tym samym relacja $\equiv_H$ jest zwrotna. Jeżeli ustalimy $g, h \in G$ takie, że $g \equiv_H h$, czyli $g^{-1}h \in H$, to wówczas $h^{-1}g = (g^{-1}h)^{-1} \in H$, czyli $h \equiv_H g$ i relacja $\equiv_H$ jest symetryczna. Podobnie, jeżeli ustalimy $g, h, k \in G$ takie, że $g \equiv_H h$ i $h \equiv_H k$, czyli takie, że $g^{-1}h \in H$ i $h^{-1}k \in H$, to wówczas $g^{-1}k = g^{-1}h \underbrace{h^{-1}k}_{\in H} \in H$, czyli $g \equiv_H k$ i

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

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

□

Wniosek 2.1. 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 2.2. 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 2.3. 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 2.4. 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 2.4 (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 2.3. 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

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

2.2. Rząd elementu grupy. Grupy cykliczne.

Definicja 2.5. Niech $(G, \cdot)$ będzie grupą, $a \in G$. Podgrupę $\langle a \rangle$ nazywamy **podgrupą cykliczną generowaną przez element a** . Mówimy, że grupa G jest **cykliczna**, gdy istnieje element $g \in G$ taki, że $G = \langle g \rangle$. Element g nazywamy **generatorem** grupy G .

Przykłady:

- (1) Niech $G = \mathbb{Z}$. Wtedy $\langle 1 \rangle = \mathbb{Z}$.
- (2) Niech $G = \mathbb{Z}_n$. Wtedy $\langle 1 \rangle = \mathbb{Z}_n$.

Twierdzenie 2.5. Jeśli rząd grupy G jest liczbą pierwszą, to G jest cykliczna i nie zawiera podgrup właściwych.

Dowód. Rozważmy grupę $(G, \cdot)$ i niech $|G| = p$, $p \in \mathbb{P}$. Pokażemy, że G jest cykliczna. Ustalmy $1_G \neq a \in G$. Wówczas $\langle a \rangle < G$ oraz $\langle a \rangle \neq \{1\}$. Wobec twierdzenia Lagrange'a, $|\langle a \rangle| \mid p$. Zatem $|\langle a \rangle| = p$, czyli $\langle a \rangle = G$.

Pokażemy, że G nie zawiera podgrup właściwych. Ustalmy $H < G$. Z twierdzenia Lagrange'a wynika, że $|H| \mid p$. Zatem $|H| = 1$ lub $|H| = p$, czyli $H = \{1\}$ lub $H = G$. $\square$

Uwaga 2.1. Jeśli G jest grupą cykliczną, to rząd G nie musi być liczbą pierwszą – na przykład rozważmy $\mathbb{Z}_6$.

Definicja 2.6. Niech $(G, \cdot)$ będzie grupą, $a \in G$. **Rzędem elementu a** nazywamy rząd podgrupy cyklicznej generowanej przez a i oznaczamy $r(a)$.

Przykłady:

- (3) Rozważmy grupę $\mathbb{R}^*$. Wówczas:
 - $\langle -1 \rangle = \{-1, 1\}$, więc $r(-1) = 2$;
 - $\langle 2 \rangle = \{2^k : k \in \mathbb{Z}\}$, więc $r(2) = \infty$.
- (4) Rozważmy grupę $\mathbb{Z}_6$. Wówczas:
 - $\langle 2 \rangle = \{0, 2, 4\}$, więc $r(2) = 3$;
 - $\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$, więc $r(1) = 6$.
- (5) Rozważmy grupę $\mathbb{Z}$. Wówczas:
 - $\langle 1 \rangle = \mathbb{Z}$, więc $r(1) = \infty$.
- (6) Rozważmy grupę $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$. Wówczas:
 - $\langle S_1 \rangle = \{I, S_1\}$, więc $r(S_1) = 2$.

Uwaga 2.2. Niech $(G, \cdot)$ będzie grupą, $a \in G$. Wówczas:

- (1) $r(a) = 1$ wtedy i tylko wtedy, gdy $a = 1_G$;
- (2) $r(a) = r(a^{-1})$;
- (3) jeśli G jest skończona, to

$$r(a) < \infty \text{ oraz } r(a) \mid |G|.$$

Dowód. (1) Oczywiście.

- (2) Wystarczy zauważyć, że $\langle a \rangle = \langle a^{-1} \rangle$.

- (3) Rząd elementu a jest skończony, ponieważ $r(a) = |\langle a \rangle|$ oraz $\langle a \rangle \subset G$, więc $|\langle a \rangle| < \infty$. Dalej, rząd elementu a dzieli rząd grupy G , ponieważ $r(a) = |\langle a \rangle|$ i na mocy twierdzenia Lagrange'a $|\langle a \rangle| \mid |G|$. $\square$

Twierdzenie 2.6. *Niech $(G, \cdot)$ będzie grupą, $a \in G$.*

- (1) *Jeśli nie istnieje $n \in \mathbb{N}$ takie, że $a^n = 1_G$, to $r(a) = \infty$.*
 (2) *Jeśli istnieje $n \in \mathbb{N}$ takie, że $a^n = 1_G$, to*

$$r(a) = \min\{n \in \mathbb{N} : a^n = 1_G\}.$$

Dowód. (1) Zgodnie z definicją, $r(a) = |\langle a \rangle|$ oraz $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$. Pokażemy, że jeśli $i \neq j$, to $a^i \neq a^j$. Ustalmy i, j , $i > j$ oraz przypuśćmy, że $a^i = a^j$. Wówczas $a^{i-j} = 1_G$ oraz $i - j \in \mathbb{N}$, co jest sprzeczne z założeniem o nieistnieniu $n \in \mathbb{N}$ takiego, że $a^n = 1_G$.

Tym samym $\langle a \rangle$ zawiera nieskończenie wiele parami różnych elementów, czyli $r(a) = \infty$.

- (2) Tak jak poprzednio, $r(a) = |\langle a \rangle|$ oraz $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$. Niech $k = \min\{n \in \mathbb{N} : a^n = 1_G\}$. Pokażemy, że $|\langle a \rangle| = \{1_G, a^1, a^2, \dots, a^{k-1}\}$. Inkluzja $(\supset)$ jest oczywista, a dla dowodu inkluzji $(\subset)$ ustalmy $g \in \langle a \rangle$. Wówczas $g = a^m$, dla pewnego $m \in \mathbb{Z}$. Dzieląc z resztą m przez k otrzymujemy istnieje $q, r \in \mathbb{Z}$ takich, że

$$m = kq + r \text{ oraz } 0 \leq r < k.$$

Dalej, $a^m = a^{kq+r} = (a^k)^q a^r = a^r \in \{1, a^1, a^2, \dots, a^{k-1}\}$.

Pozostaje pokazać, że zbiór $\{1, a^1, a^2, \dots, a^{k-1}\}$ zawiera k elementów. Przypuśćmy bowiem, że istnieją $i, j \in \{0, 1, \dots, k-1\}$, $i > j$, takie, że $a^i = a^j$. Wówczas $a^{i-j} = 1_G$, ale $0 < i - j < k$, co jest sprzeczne z wyborem k . $\square$

Przykłady:

- (7) Rozważmy grupę $U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$. Wówczas $r(3) = 4$.
 (8) Rozważmy grupę $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$. Wówczas $r(O_2) = 3$.

Wniosek 2.4. *Niech $(G, \cdot)$ będzie grupą.*

- (1) *Jeżeli G jest skończona i $|G| = n$, to $\forall a \in G (a^n = 1_G)$.*
 (2) *Jeżeli $a \in G$ i $r(a) = k$, to $a^k = 1_G$.*
 (3) *Jeżeli $a \in G$, $r(a) = k$ i $a^m = 1_G$, to $k \leq m$.*

Przykład:

- (9) Rozważmy grupę $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$. Wówczas $3^4 = 1$, ale $r(3) = 2$.

Twierdzenie 2.7. *Niech $(G, \cdot)$ będzie grupą, $a \in G$. Jeżeli $a^m = 1_G$, to wówczas $r(a) \mid m$.*

Dowód. Niech $r(a) = k$. Przypuśćmy, że $k \nmid m$. Dzieląc z resztą m przez k otrzymujemy istnieje liczb całkowitych $q, r \in \mathbb{Z}$ takich, że

$$m = kq + r \text{ oraz } 0 < r < k.$$

Dalej, $1_G = a^m = a^{kq+r} = (a^k)^q a^r = a^r$, co daje sprzeczność z Twierdzeniem 2.6. $\square$

Wniosek 2.5. *Niech $(G, \cdot)$ będzie grupą skończoną. Wówczas G jest cykliczna wtedy i tylko wtedy, gdy istnieje $a \in G$ taki, że $r(a) = |G|$.*

Dowód. $(\Rightarrow)$: oczywiste. $(\Leftarrow)$: niech $a \in G$ będzie taki, że $r(a) = |G|$; wówczas $|\langle a \rangle| = |G|$ oraz $\langle a \rangle < G$, czyli $\langle a \rangle = G$. $\square$

Przykłady:

(10) $\mathbb{Z}_5$ jest cykliczna, gdyż $r(1) = 5$.

(11) $U(\mathbb{Z}_8)$ nie jest cykliczna, gdyż

$$r(1) = 1, r(3) = 2, r(5) = 2 \text{ oraz } r(7) = 2.$$

(12) $\mathbb{Z}_2 \times \mathbb{Z}_2$ nie jest cykliczna, gdyż

$$r((0, 0)) = 1, r((1, 0)) = 2, r((0, 1)) = 2 \text{ oraz } r((1, 1)) = 2.$$

(13) $\mathbb{Z}_2 \times \mathbb{Z}_3$ jest cykliczna, gdyż $r((1, 2)) = 6$.

Twierdzenie 2.8. (1) *Dowolna grupa cykliczna jest abelowa.*

(2) *Podgrupa grupy cyklicznej jest cykliczna.*

Dowód. (1) Niech $G = \langle a \rangle$. Ustalmy $x, y \in G$. Wtedy $x = a^k, y = a^l$, dla pewnych $k, l \in \mathbb{Z}$. Natenczas

$$xy = a^k a^l = a^{k+l} = a^{l+k} = a^l a^k = yx.$$

(2) Niech $G = \langle a \rangle$. Ustalmy $H < G$. Możemy założyć, że $H \neq \{1_G\}$ (oczywiście podgrupa trywialna $\{1_G\}$ jest cykliczna). Ustalmy $c \in H, c \neq 1_G$. W szczególności $c = a^k$, dla pewnego $k \in \mathbb{Z}$. Możemy założyć, że $k \in \mathbb{N}$, gdyż jeśli $k < 0$, to $c^{-1} = a^{-k} \in H$. Niech $n = \min\{l \in \mathbb{N} : a^l \in H\}$.

Pokażemy, że $H = \langle a^n \rangle$. Inkluzja $(\supset)$ jest oczywista, skupmy się na dowodzie inkluzji $(\subset)$. Ustalmy $x \in H$. Wówczas $x = a^m$, dla pewnego $m \in \mathbb{Z}$. Dzieląc z resztą m przez n otrzymujemy istnieje liczb całkowitych $q, r \in \mathbb{Z}$ takich, że

$$m = nq + r \text{ oraz } 0 < r < n.$$

Dalej, $a^m = a^{nq+r} = (a^n)^q a^r$, a więc $a^r = a^m (a^n)^{-q} \in H$. Wobec wyboru n , jedyną możliwością staje się, aby $r = 0$. Wówczas $m = nq$, a stąd $x = a^m = (a^n)^q \in \langle a^n \rangle$.

□

Uwaga 2.3. Z przeprowadzonego dowodu wynika, że jeśli $(G, \cdot)$ jest grupą cykliczną, $G = \langle a \rangle$ oraz $\{1_G\} \neq H < G$, to $H = \langle a^n \rangle$, gdzie

$$n = \min\{l \in \mathbb{N} : a^l \in H\}.$$

Przykład:

(14) Rozważmy grupę $\mathbb{Z}$ oraz $H = \langle m, n \rangle < \mathbb{Z}$. H jest cykliczna oraz

$$H = \langle a^d \rangle, d = \min\{l \in \mathbb{N} : 1 \cdot l \in H\}.$$

Ponieważ $H = \{xm + yn : x, y \in \mathbb{Z}\}$, więc d jest najmniejszą z liczb naturalnych postaci $xm + yn$, a więc, wobec algorytmu Euklidesa, $d = \text{NWD}(m, n)$.