

5. WYKŁAD 5: HOMOMORFIZMY GRUP, PODGRUPY NORMALNE.

Definicja 5.1. Niech G, F będą grupami.

- (1) Odwzorowanie $\phi : G \rightarrow F$ nazywamy **homomorfizmem**, jeśli

$$\forall a, b \in G [\phi(a \cdot b) = \phi(a) \cdot \phi(b)].$$

Zbiór wszystkich homomorfizmów grupy G w grupę F oznaczamy $\text{Hom}(G, F)$.

- (2) Homomorfizm $\phi : G \rightarrow F$ nazywamy **monomorfizmem**, jeśli jest różnowartościowy.
 (3) Homomorfizm $\phi : G \rightarrow F$ nazywamy **epimorfizmem**, jeśli jest surjektywny.
 (4) Homomorfizm $\phi : G \rightarrow G$ nazywamy **endomorfizmem**. Zbiór wszystkich endomorfizmów oznaczamy $\text{End}(G)$.
 (5) Izomorfizm $\phi : G \rightarrow G$ nazywamy **automorfizmem**. Zbiór wszystkich automorfizmów oznaczamy $\text{Aut}(G)$.
 (6) Jeśli $\phi : G \rightarrow F$ jest homomorfizmem, to zbiór

$$\ker \phi = \phi^{-1}(1_F) = \{a \in G : \phi(a) = 1_F\}$$

nazywamy **jądrem** homomorfizmu ϕ , zaś zbiór

$$\text{im} \phi = \phi(G) = \{b \in F : \exists a \in G [b = \phi(a)]\}$$

nazywamy **obrazem** homomorfizmu ϕ .

Uwaga 5.1. Niech G, F będą grupami, niech $\phi : G \rightarrow F$ będzie homomorfizmem. Wówczas:

- (1) $\phi(1_G) = 1_F$;
 (2) $\phi(a^{-1}) = (\phi(a))^{-1}$, dla $a \in G$;
 (3) $\phi(a^k) = (\phi(a))^k$, dla $a \in G$;
 (4) $r(\phi(a)) \mid r(a)$, dla $a \in G$;
 (5) jeśli ϕ jest izomorfizmem, to $r(\phi(a)) = r(a)$, dla $a \in G$.

Dowód. (1) Mamy:

$$\phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G)\phi(1_G),$$

skąd, po skróceniu, $\phi(1_G) = 1_F$.

- (2) Mamy:

$$1_F = \phi(1_G) = \phi(a \cdot a^{-1}) = \phi(a)\phi(a^{-1}),$$

skąd, po podzieleniu, $\phi(a^{-1}) = (\phi(a))^{-1}$.

- (3) Prosty dowód indukcyjny pozostawiamy Czytelnikowi jako nietrudne ćwiczenie.
 (4) Niech $r(a) = k$. Wówczas $a^k = 1_G$ i stąd

$$1_F = \phi(1_G) = \phi(a^k) = (\phi(a))^k.$$

Zatem $r(\phi(a)) \mid r(a)$.

- (5) Odwzorowanie $\phi : G \rightarrow F$ jest różnowartościowe i surjektywne, więc istnieje odwzorowanie odwrotne $\phi^{-1} : F \rightarrow G$. W szczególności

$$r(\phi(a)) \mid r(a) \text{ oraz } r(\phi^{-1}(\phi(a))) = r(a) \mid r(\phi(a)).$$

Zatem $r(\phi(a)) = r(a)$.

□

Twierdzenie 5.1. Niech G, F będą grupami, niech $\phi : G \rightarrow F$ będzie homomorfizmem. Wówczas:

- (1) $\ker \phi < G$ oraz $\text{im} \phi < F$;

- (2) ϕ jest monomorfizmem wtedy i tylko wtedy, gdy $\ker \phi = \{1_G\}$;
 (3) ϕ jest epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{im} \phi = F$;
 (4) ϕ jest izomorfizmem wtedy i tylko wtedy, gdy istnieje homomorfizm $\psi : F \rightarrow G$ taki, że

$$\phi \circ \psi = \operatorname{id}_F \text{ oraz } \psi \circ \phi = \operatorname{id}_G;$$

- (5) jeśli ϕ jest monomorfizmem, to dla każdej grupy H i dla każdych homomorfizmów $\psi_1, \psi_2 : H \rightarrow G$ jeśli $\phi \circ \psi_1 = \phi \circ \psi_2$, to $\psi_1 = \psi_2$;
 (6) jeśli ϕ jest epimorfizmem, to dla każdej grupy H i dla każdych homomorfizmów $\psi_1, \psi_2 : F \rightarrow H$ jeśli $\psi_1 \circ \phi = \psi_2 \circ \phi$, to $\psi_1 = \psi_2$.

Dowód. (1) Pokażemy, że jądro homomorfizmu jest podgrupą. Ustalmy w tym celu elementy $a, b \in \ker \phi$. Wówczas $\phi(a) = 1_F$, $\phi(b) = 1_F$ oraz

$$\phi(ab^{-1}) = \phi(a) \cdot \phi(b^{-1}) = \phi(a) \cdot (\phi(b))^{-1} = 1_F \cdot 1_F = 1_F,$$

czyli $ab^{-1} \in \ker \phi$.

Podobnie, pokażemy, że obraz homomorfizmu jest podgrupą. Ustalmy w tym celu elementy $c, d \in \operatorname{im} \phi$. Wówczas $c = \phi(a)$, $d = \phi(b)$ dla pewnych $a, b \in G$ oraz

$$cd^{-1} = \phi(a) \cdot (\phi(b))^{-1} = \phi(a) \cdot \phi(b^{-1}) = \phi(ab^{-1}) \in \operatorname{im} \phi.$$

- (2) ($\Rightarrow$): Załóżmy, że ϕ jest monomorfizmem i ustalmy $a \in \ker \phi$. Wówczas $\phi(a) = 1_F = \phi(1_G)$ i ponieważ ϕ jest różnowartościowe, więc $a = 1_G$.

($\Leftarrow$): Załóżmy, że ϕ jest homomorfizmem, dla którego $\ker \phi = \{1_G\}$ i ustalmy $a, b \in G$ i niech $\phi(a) = \phi(b)$. Wówczas

$$1_F = \phi(a) \cdot (\phi(b))^{-1} = \phi(a) \cdot \phi(b^{-1}) = \phi(ab^{-1}),$$

czyli $ab^{-1} \in \ker \phi$, a zatem $a = b$.

- (3) jest oczywiste.
 (4) ($\Rightarrow$): Załóżmy, że ϕ jest izomorfizmem i zdefiniujmy odwzorowanie $\psi : F \rightarrow G$ wzorem

$$\psi(f) = g \text{ wtedy i tylko wtedy, gdy } \phi(g) = f.$$

Ponieważ ϕ jest epimorfizmem, więc ψ jest zdefiniowane dla każdego elementu grupy F , a ponieważ ϕ jest monomorfizmem, więc ψ jest dobrze określoną funkcją. Warunki $\phi \circ \psi = \operatorname{id}_F$ oraz $\psi \circ \phi = \operatorname{id}_G$ wynikają wprost z określenia funkcji ψ . Pozostaje sprawdzić, że ψ jest homomorfizmem. W tym celu ustalmy $f_1, f_2 \in F$. Ponieważ ϕ jest epimorfizmem, niech $f_1 = \phi(g_1)$ oraz $f_2 = \phi(g_2)$, $g_1, g_2 \in G$. Wówczas $\phi(g_1 + g_2) = \phi(g_1) + \phi(g_2) = f_1 + f_2$. Tym samym:

$$\psi(f_1 + f_2) = g_1 + g_2 = \psi(f_1) + \psi(f_2).$$

($\Leftarrow$): Załóżmy, że istnieje homomorfizm $\psi : F \rightarrow G$ taki, że

$$\phi \circ \psi = \operatorname{id}_F \text{ oraz } \psi \circ \phi = \operatorname{id}_G.$$

Pokażemy, że ϕ jest monomorfizmem. Ustalmy $g \in \ker \phi$. Wówczas $\phi(g) = 1_F$. Ponadto $g = \operatorname{id}_G(g) = \psi \circ \phi(g) = \psi(1_F) = 1_G$. Podobnie pokażemy, że ϕ jest epimorfizmem. Ustalmy $f \in F$. Wówczas $f = \operatorname{id}_F(f) = \phi \circ \psi(f) = \phi(\psi(f))$.

- (5) Załóżmy, że ϕ jest monomorfizmem. Ustalmy grupę H , homomorfizmy $\psi_1, \psi_2 : H \rightarrow G$ takie, że $\phi \circ \psi_1 = \phi \circ \psi_2$ oraz element $h \in H$. Wówczas

$$\phi(\psi_1(h)) = \phi \circ \psi_1(h) = \phi \circ \psi_2(h) = \phi(\psi_2(h))$$

i ponieważ ϕ jest injekcją, więc $\psi_1(h) = \psi_2(h)$. Wobec dowolności $h \in H$, $\psi_1 = \psi_2$.

- (6) Załóżmy, że ϕ jest epimorfizmem. Ustalmy grupę H , homomorfizmy $\psi_1, \psi_2 : F \rightarrow H$ takie, że $\psi_1 \circ \phi = \psi_2 \circ \phi$ oraz element $f \in F$. Ponieważ ϕ jest surjekcją, więc istnieje $g \in G$ taki, że $\phi(g) = f$. Wówczas

$$\psi_1(f) = \psi_1(\phi(g)) = \psi_1 \circ \phi(g) = \psi_2 \circ \phi(g) = \psi_2(\phi(g)) = \psi_2(f)$$

i wobec dowolności $f \in F$, $\psi_1 = \psi_2$. □

Przykłady:

- (1) $\phi : \mathbb{R}^* \rightarrow \mathbb{R}^*$, $\phi(x) = x^2$ jest homomorfizmem.
- (2) $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$, $\phi(x) = 2x$ jest homomorfizmem.
- (3) $\phi : \mathbb{R}_+^* \rightarrow \mathbb{R}$, $\phi(x) = \log x$ jest homomorfizmem.
- (4) $\phi : GL(n, F) \rightarrow F$, $\phi(A) = \det A$ jest homomorfizmem.
- (5) $\phi : G \rightarrow G$, $\phi(x) = 1_G$ jest homomorfizmem, nazywamy go **homomorfizmem trywialnym**.
- (6) $\phi : G \rightarrow G$, $\phi(x) = x$ jest automorfizmem.
- (7) $\phi : \mathbb{C} \rightarrow \mathbb{C}$, $\phi(z) = \bar{z}$ jest automorfizmem.
- (8) $\phi : \mathbb{R}^* \rightarrow \mathbb{R}^*$, $\phi(x) = x^{-1}$ jest automorfizmem.
- (9) $i_a : G \rightarrow G$, $a \in G$, $i_a(x) = axa^{-1}$ jest automorfizmem, nazywamy go **automorfizmem wewnętrznym grupy G** . Zbiór wszystkich automorfizmów wewnętrznych oznaczamy $Inn(G)$, pozostałe automorfizmy nazywamy **zewnętrznymi** a ich zbiór oznaczamy przez $Out(G)$.

Dowód. Ustalmy grupę G i element $a \in G$. Pokażemy, że i_a jest homomorfizmem; istotnie, ustalmy $x, y \in G$. Wówczas:

$$i_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = i_a(x)i_a(y).$$

Dalej, i_a jest injekcją, ponieważ

$$x \in \ker i_a \Leftrightarrow i_a(x) = 1_G \Leftrightarrow axa^{-1} = 1_G \Leftrightarrow x = a^{-1}a = 1_G.$$

i_a jest również surjekcją, gdyż

$$x = aa^{-1}xaa^{-1} = a(a^{-1}xa)a^{-1} = i_a(a^{-1}xa).$$
□

Uwaga 5.2. Niech G będzie grupą, niech $a, b \in G$. Wówczas

- (1) $i_{1_G} = id_G$,
- (2) $i_{ab} = i_a \circ i_b$,
- (3) $i_{a^{-1}} = (i_a)^{-1}$.

Dowód. (1) oczywiste.

(2) Ustalmy $x \in G$. Wówczas:

$$i_{ab}(x) = abx(ab)^{-1} = a(bxb^{-1})a^{-1} = i_a \circ i_b(x).$$

(3) Wynika wprost z (2). □

Uwaga 5.3. Niech G, F, H będą grupami. Wówczas

- (1) Jeśli $\phi \in Hom(G, F)$ i $\psi \in Hom(F, H)$, to wówczas $\psi \circ \phi \in Hom(G, H)$.
- (2) $(End(G), \circ)$ jest algebrą łączną z jedynką (ale niekoniecznie grupą).
- (3) $(Aut(G), \circ)$ jest grupą, jest to podgrupa grupy $S(G)$.

(4) Relacja $\cong$ jest równoważnością.

Twierdzenie 5.2. Niech G, F będą grupami, $H < G$, $K < F$, niech $\phi : G \rightarrow F$ będzie homomorfizmem. Wówczas:

- (1) $\phi(H) < F$,
- (2) $\phi^{-1}(K) < G$.

Dowód. (1) Ustalmy $c, d \in \phi(H)$, $c = \phi(a)$, $d = \phi(b)$, $a, b \in H$. Wówczas:

$$cd^{-1} = \phi(a)(\phi(b))^{-1} = \phi(ab^{-1}) \in \phi(H).$$

(2) analogicznie. □

Definicja 5.2. Niech G będzie grupą, niech $H, K < G$.

- (1) Elementy $x, y \in G$ nazywamy **sprzężonymi**, gdy istnieje element $a \in G$ taki, że $y = i_a(x)$. Element ten nazywamy **elementem sprzęgającym**. Elementy sprzężone oznaczamy $x \sim y$.
- (2) Podgrupy $H, K < G$ nazywamy **sprzężonymi**, gdy istnieje element $a \in G$ taki, że $H = i_a(K)$. Element ten nazywamy **elementem sprzęgającym**.

Uwaga 5.4. Niech G będzie grupą.

- (1) Relacja sprzęgania $\sim$ jest relacją równoważnościową i jako taka rozbija G na klasy równoważności. Klasy równoważności relacji $\sim$ nazywamy **klasami elementów sprzężonych** i oznaczamy

$$K(x) = \{y \in G : \exists a \in G [y = i_a(x)]\}.$$

- (2) $x \in K(x)$, dla $x \in G$.
- (3) $K(x) \neq K(y) \Rightarrow K(x) \cap K(y) = \emptyset$, dla $x, y \in G$.
- (4) $K(x) \cap K(y) \neq \emptyset \Rightarrow K(x) = K(y)$, dla $x, y \in G$.
- (5) $G = \bigcup_{x \in G} K(x)$.
- (6) Rzędy grup sprzężonych są równe.

Dowód. (2), (3), (4) i (5) są prostymi konsekwencjami (1). (6) wynika z faktu, iż pomiędzy grupami sprzężonymi potrafimy wskazać bijekcję ustanowioną przez automorfizm wewnętrzny. Pozostaje udowodnić (1). Ponieważ $x = i_{1_G}(x)$, więc $\sim$ jest zwrotna. Jest też symetryczna, gdyż:

$$x \sim y \Leftrightarrow y = axa^{-1}, a \in G \Leftrightarrow x = a^{-1}ya = i_{a^{-1}}(y), a^{-1} \in G.$$

Na koniec $\sim$ jest przechodnia, albowiem

$$x \sim y \wedge y \sim z \Leftrightarrow y = axa^{-1}, z = byb^{-1}, a, b \in G \Rightarrow z = baxa^{-1}b^{-1} = i_{ba}(x).$$

□

Definicja 5.3. Niech G będzie grupą, niech $H < G$. H nazywamy **podgrupą normalną** (lub **dzielnikiem normalnym** albo **podgrupą niezmienniczą**), jeśli

$$\forall a \in G (aH = Ha).$$

Oznaczamy $H \triangleleft G$.

Uwaga 5.5. Niech G będzie grupą.

- (1) Jeśli G jest abelowa, to każda jej podgrupa jest normalna.
- (2) Podgrupy $\{1_G\}$ i G są normalne.
- (3) Jeśli $H < G$ i $(G : H) = 2$, to H jest podgrupą normalną.

Dowód. Jedyną nietrywialną część uwagi to (3), poprzestaniemy zatem na jej dowodzie. Ustalmy $a \in G$. Jeśli $a \in H$, to wtedy $aH = H = Ha$. Jeśli $a \notin H$, to wtedy $H \neq aH$ oraz $H \neq Ha$. Ponieważ $(G : H) = 2$, więc $W_L(H) = \{aH, H\}$ oraz $W_P(H) = \{Ha, H\}$. Ponadto $G = aH \cup H = Ha \cup H$ oraz $H \cap aH = \emptyset = H \cap Ha$, a zatem $aH = G \setminus H = Ha$. $\square$

Twierdzenie 5.3. *Niech G będzie grupą, niech $H < G$. Następujące warunki są równoważne:*

- (1) $H \triangleleft G$,
- (2) $\forall a \in G(aHa^{-1} = H)$,
- (3) $\forall a \in G(aHa^{-1} \subset H)$,
- (4) $\forall a \in G(a \in H \Rightarrow K(a) \subset H)$.

Dowód. (1) $\Leftrightarrow$ (2): $H \triangleleft G \Leftrightarrow \forall a \in G(aH = Ha) \Leftrightarrow \forall a \in G(aHa^{-1} = H)$.

(2) $\Rightarrow$ (3): Oczywiste.

(3) $\Rightarrow$ (4): Załóżmy, że $\forall a \in G aHa^{-1} \subset H$. Pokażemy, że $\forall a \in G aHa^{-1} \supset H$. Ustalmy $a \in G$ oraz $x \in H$. W szczególności

$$a^{-1}x(a^{-1})^{-1} = y \in a^{-1}H(a^{-1})^{-1} \subset H,$$

zatem $x = aya^{-1} \in aHa^{-1}$.

(1) $\Rightarrow$ (4): Załóżmy, że $\forall b \in G bH = Hb$, lub równoważnie $\forall b \in G bHb^{-1} = H$. Ustalmy $a \in H$. Pokażemy, że $K(a) = \{y \in G : \exists b \in G[y = i_b(x)]\} \subset H$. Ustalmy $x \in K(a)$, $x = bab^{-1}$, dla pewnego $b \in G$. Wówczas $x \in bHb^{-1} = H$.

(4) $\Rightarrow$ (1): Załóżmy, że dla wszystkich $a \in H$ zachodzi $K(a) \subset H$. Ustalmy $a \in G$. Pokażemy, że $aH = Ha$.

($\subset$): Ustalmy $ax \in aH$. W szczególności $x \in H$, a zatem $K(x) \subset H$. Stąd $\forall b \in G(bxb^{-1} \in H)$. W szczególności, $axa^{-1} \in H$, czyli $ax \in Ha$.

($\supset$): analogicznie. $\square$

Przykłady:

- (10) Rozważmy $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$ oraz $H = \{ID_3, O_1, O_2\} < D(3)$. Wówczas $H \triangleleft D(3)$, ponieważ $(D(3) : H) = 2$.
- (11) Rozważmy $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$ oraz $H = \{ID_3, S_1\} < D(3)$. Wówczas $H \not\triangleleft D(3)$, ponieważ $S_2 \circ H = \{S_2, O_1\}$ ale $H \circ S_2 = \{S_2, O_2\}$.
- (12) Rozważmy $Aut(G)$ oraz $Inn(G) < Aut(G)$. Wówczas $Inn(G) \triangleleft Aut(G)$.

Dowód. Pokażemy, że $Inn(G) < Aut(G)$. Ustalmy $i_a, i_b \in Inn(G)$. Wówczas

$$i_a \circ (i_b)^{-1} = i_a \circ i_{b^{-1}} = i_{ab^{-1}} \in Inn(G).$$

Pokażemy, że $Inn(G) \triangleleft Aut(G)$, czyli że $\forall \phi \in Aut(G)[\phi \circ Inn(G) \circ \phi^{-1} \subset Inn(G)]$. Ustalmy $\phi \in Aut(G)$ oraz $i_a \in Inn(G)$. Pokażemy, że $\phi \circ i_a \circ \phi^{-1} = i_{\phi(a)} \in Inn(G)$; istotnie, dla $x \in G$ otrzymujemy

$$\begin{aligned} \phi \circ i_a \circ \phi^{-1}(x) &= \phi(i_a(\phi^{-1}(x))) = \phi(a\phi^{-1}(x)a^{-1}) \\ &= \phi(a)\phi(\phi^{-1}(x))\phi(a^{-1}) \\ &= \phi(a)x\phi(a^{-1}) = i_{\phi(a)}(x). \end{aligned}$$

$\square$

Twierdzenie 5.4. *Niech G, F będą grupami, $H < G$, $K < F$, niech $\phi : G \rightarrow F$ będzie homomorfizmem. Wówczas:*

- (1) $\ker \phi \triangleleft G$,

- (2) jeśli $K \triangleleft F$, to $\phi^{-1}(K) \triangleleft G$,
 (3) jeśli $H \triangleleft G$ i ϕ jest epimorfizmem, to $\phi(H) \triangleleft F$.

Dowód. (1) Pokażemy, że $\forall a \in G [a \ker \phi a^{-1} \subset \ker \phi]$. Ustalmy $a \in G$, $h \in \ker \phi$, to znaczy $\phi(h) = 1_F$.

Mamy:

$$\phi(aha^{-1}) = \phi(a)\phi(h)\phi(a^{-1}) = \phi(a)(\phi(a))^{-1} = 1_F,$$

czyli $aha^{-1} \in \ker \phi$.

- (2) Pokażemy, że $\forall a \in G [a\phi^{-1}(K)a^{-1} \subset \phi^{-1}(K)]$. Ustalmy $a \in G$, $h \in \phi^{-1}(K)$, to znaczy $\phi(h) = k \in K \triangleleft F$. Mamy:

$$\phi(aha^{-1}) = \phi(a)\phi(h)(\phi(a))^{-1} = \phi(a)k(\phi(a))^{-1} \in K$$

czyli $aha^{-1} \in \phi^{-1}(K)$.

- (3) analogicznie.

□

Przykład:

- (13) Rozważmy $GL(n, F)$ oraz $SL(n, F) < GL(n, F)$. Wówczas $SL(n, F) \triangleleft GL(n, F)$, ponieważ $SL(n, F) = \ker \phi$, gdzie $\phi : GL(n, F) \rightarrow F^*$ dane jest wzorem $\phi(A) = \det A$.