

6. WYKŁAD 6: GRUPA ILORAZOWA, TWIERDZENIE O HOMOMORFIZMIE.

Definicja i Uwaga 6.1. Niech $(G, \cdot)$ będzie grupą, $H \triangleleft G$. Oznaczmy

$$G/H = W_P(H) = W_L(H)$$

i w zbiorze G/H określmy działanie

$$(aH) * (bH) = (a \cdot b)H.$$

Wówczas $(G/H, *)$ jest grupą, nazywamy ją **grupą ilorazową** grupy G względem podgrupy normalnej H .

Dowód. Pokażemy, że działanie $*$ jest poprawnie określone. Istotnie, ustalmy $aH, a'H, bH, b'H \in G/H$ i niech

$$aH = a'H \text{ oraz } bH = b'H.$$

Wówczas

$$\begin{aligned} (aH) * (bH) &= (a \cdot b)H = a(bH) = a(b'H) \\ &= a(Hb') = (aH)b' = (a'H)b' \\ &= a'(Hb') = a'(b'H) = (a' \cdot b')H \\ &= (a'H) * (b'H). \end{aligned}$$

Pokażemy, że działanie $*$ jest łączne. Istotnie, ustalmy $aH, bH, cH \in G/H$. Wówczas

$$\begin{aligned} ((aH) * (bH)) * (cH) &= ((a \cdot b)H) * (cH) = (a \cdot b) \cdot cH \\ &= a \cdot (b \cdot c)H = (aH) * ((b \cdot c)H) \\ &= (aH) * ((bH) * (cH)). \end{aligned}$$

Pokażemy, że $1_G H$ jest elementem neutralnym działania $\cdot$. Ustalmy $aH \in G/H$. Wówczas

$$\begin{aligned} (aH) * (1_G H) &= aH \\ (1_G H) * (aH) &= aH. \end{aligned}$$

Pokażemy istnienie elementu odwrotnego. Ustalmy $aH \in G/H$. Wówczas

$$\begin{aligned} (aH) * (a^{-1}H) &= 1_G H \\ (a^{-1}H) * (aH) &= 1_G H. \end{aligned}$$

□

Przykłady:

(1) Rozważmy $\mathbb{Z}$ oraz $3\mathbb{Z} \triangleleft \mathbb{Z}$. Wówczas:

$$\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}.$$

Tabela działań w grupie:

	$0 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$0 + 3\mathbb{Z}$	$0 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$1 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$0 + 3\mathbb{Z}$
$2 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$0 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$

W szczególności widzimy, że $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$.

Uwaga 6.1. Niech $(G, \cdot)$ będzie grupą, $H \triangleleft G$. Wówczas:

- (1) $|G/H| = (G : H)$,
 (2) $|G/H| = \frac{|G|}{|H|}$, o ile G jest skończona.

Twierdzenie 6.1 (uogólnione twierdzenie Lagrange'a). *Niech $(G, \cdot)$ będzie grupą, $H \triangleleft G$. Wówczas zbiory*

$$G \text{ oraz } G/H \times H$$

są równoliczne.

Dowód. Wybierzmy układ reprezentantów warstw $\{g_i H : i \in I\}$, a więc zbiór o następującej własności:

$$G/H = \{g_i H : i \in I\} \text{ oraz } |G/H| = |I|.$$

Zdefiniujmy funkcję $\kappa : G \rightarrow G/H$ wzorem

$$\kappa(g) = gH,$$

funkcję $l : G \rightarrow I$ warunkiem

$$l(g) = i \text{ wtedy i tylko wtedy, gdy } gH = g_i H,$$

oraz funkcję $\phi : G \rightarrow G/H$ wzorem

$$\phi(g) = (\kappa(g), g^{-1}g_{l(g)}).$$

Pokażemy, że ϕ jest bijekcją. W tym celu zdefiniujmy funkcję $\psi : G/H \times H \rightarrow G$ wzorem $\psi(g_i H, h) = g_i h^{-1}$. Wówczas

$$\begin{aligned} \phi \circ \psi(g_i H, h) &= \phi(g_i h^{-1}) = (g_i h^{-1} H, (g_i h^{-1})^{-1} g_i) \\ &= (g_i H, h g_i^{-1} g_i) = (g_i H, h) \end{aligned}$$

oraz

$$\begin{aligned} \psi \circ \phi(g) &= \psi(gH, g^{-1}g_{l(g)}) = \psi(l(g)H, g^{-1}g_{l(g)}) \\ &= g_{l(g)}(g^{-1}g_{l(g)})^{-1} = g_{l(g)}g_{l(g)}^{-1}g = g. \end{aligned}$$

□

Definicja i Uwaga 6.2. *Niech $(G, \cdot)$ będzie grupą, $H \triangleleft G$. Wówczas odwzorowanie $\kappa : G \rightarrow G/H$ dane wzorem*

$$\kappa(g) = gH$$

*jest epimorfizmem oraz $\ker \kappa = H$. Nazywamy go **epimorfizmem kanonicznym**.*

Dowód. Pokażemy, że κ jest homomorfizmem. W tym celu ustalmy $a, b \in G$. Wówczas

$$\kappa(ab) = (ab)H = (aH)(bH) = \kappa(a)\kappa(b).$$

Ponieważ, dla dowolnego $aH \in G/H$, $aH = \kappa(a)$, więc κ jest surjekcją i pozostaje sprawdzić, że $\ker \kappa = H$. Istotnie:

$$a \in \ker \kappa \Leftrightarrow \kappa(a) = 1_G H \Leftrightarrow aH = 1_G H \Leftrightarrow a \in H.$$

□

Wniosek 6.1. *Niech $(G, \cdot)$ będzie grupą, $H < G$. Wówczas $H \triangleleft G$ wtedy i tylko wtedy, gdy H jest jądrem pewnego homomorfizmu.*

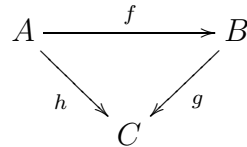
Dowód. ($\Leftarrow$): wynika z Twierdzenia 5.4 (1).

($\Rightarrow$): załóżmy, że $H \triangleleft G$. Rozważmy epimorfizm kanoniczny $\kappa : G \rightarrow G/H$. Wówczas $H = \ker \kappa$. □

Definicja 6.1. Diagram składający się ze strzałek między różnymi obiektami nazywamy **diagramem przemiennym**, gdy w każdym przypadku można przejść od jednego obiektu do drugiego za pomocą dwóch różnych ciągów strzałek.

Przykłady:

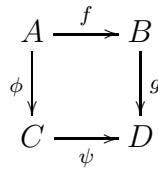
(2) To, że diagram:



jest przemienny, oznacza

$$h = g \circ f.$$

(3) To, że diagram:



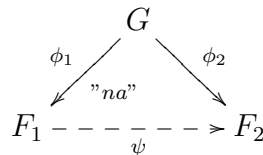
jest przemienny, oznacza

$$g \circ f = \psi \circ \phi.$$

Twierdzenie 6.2 (o homomorfizmie). Niech G, F_1, F_2 będą grupami $\phi_1 : G \rightarrow F_1$ homomorfizmem surjektywnym, $\phi_2 : G \rightarrow F_2$ homomorfizmem.

- (1) Jeśli istnieje homomorfizm $\psi : F_1 \rightarrow F_2$ taki, że $\psi \circ \phi_1 = \phi_2$, to $\ker \phi_1 \subset \ker \phi_2$.
- (2) Jeśli $\ker \phi_1 \subset \ker \phi_2$, to istnieje dokładnie jeden homomorfizm $\psi : F_1 \rightarrow F_2$ taki, że $\psi \circ \phi_1 = \phi_2$. Ponadto wówczas $\operatorname{im} \psi = \operatorname{im} \phi_2$ oraz $\ker \psi = \phi_1(\ker \phi_2)$.

Inaczej: diagram



jest przemienny.

Dowód. (1) Ustalmy $a \in \ker \phi_1$, a więc niech $\phi_1(a) = 1_{F_1}$. Wówczas

$$\phi_2(a) = \psi \circ \phi_1(a) = \psi(\phi_1(a)) = \psi(1_{F_1}) = 1_{F_2},$$

to znaczy $a \in \ker \phi_2$.

- (2) Zdefiniujemy odwzorowanie $\psi : F_1 \rightarrow F_2$. Ustalmy $b \in F_1$. Wówczas $b = \phi_1(a)$, dla pewnego $a \in G$. Przyjmujemy

$$\psi(b) = \phi_2(a).$$

Pokażemy, że ψ jest poprawnie określone. Ustalmy $b \in F_1$. Niech $b = \phi_1(a_1) = \phi_1(a_2)$, dla pewnych $a_1, a_2 \in G$. Wówczas $\phi_1(a_1)(\phi_1(a_2))^{-1} = \phi_1(a_1 a_2^{-1}) = 1_{F_1}$, czyli $a_1 a_2^{-1} \in \ker \phi_1$. Stąd $a_1 a_2^{-1} \in \ker \phi_2$, zatem $\phi_2(a_1 a_2^{-1}) = \phi_2(a_1)(\phi_2(a_2))^{-1} = 1_{F_2}$. Wówczas $\phi_2(a_1) = \phi_2(a_2)$.

Pokażemy, że ψ jest homomorfizmem. Ustalmy $b_1, b_2 \in F_1$. Niech $b_1 = \phi_1(a_1)$, $b_2 = \phi_1(a_2)$, dla pewnych $a_1, a_2 \in G$. Wówczas:

$$\begin{aligned}\psi(b_1 b_2) &= \psi(\phi_1(a_1) \phi_1(a_2)) = \psi(\phi_1(a_1 a_2)) = \phi_2(a_1 a_2) \\ &= \phi_2(a_1) \phi_2(a_2) = \psi(\phi_1(a_1)) \psi(\phi_1(a_2)) = \psi(b_1) \psi(b_2).\end{aligned}$$

Pokażemy, że ψ jest wyznaczony jednoznacznie. Niech $\psi, \psi' : F_1 \rightarrow F_2$ będą takimi homomorfizmami, że

$$\psi \circ \phi_1 = \phi_2 \text{ oraz } \psi' \circ \phi_1 = \phi_2.$$

Ponieważ ϕ_1 jest epimorfizmem, a więc epimorfizmem kategorijskim, więc $\psi = \psi'$.

To, że $\text{im} \psi = \text{im} \phi_2$ wynika z określenia ψ , pozostaje więc pokazać, że $\ker \psi = \phi_1(\ker \phi_2)$. Ustalmy $b \in \ker \psi \subset F_1$. Niech $b = \phi_1(a)$, dla pewnego $a \in G$. Wówczas

$$\begin{aligned}b \in \ker \psi &\Leftrightarrow \psi(b) = 1_{F_2} \Leftrightarrow \psi(\phi_1(a)) = 1_{F_2} \\ &\Leftrightarrow \phi_2(a) = 1_{F_2} \Leftrightarrow a \in \ker \phi_2 \\ &\Leftrightarrow b \in \phi_1(\ker \phi_2).\end{aligned}$$

□

Wniosek 6.2. Niech G, F_1, F_2 będą grupami, $\phi_1 : G \rightarrow F_1$ homomorfizmem surjektywnym, $\phi_2 : G \rightarrow F_2$ homomorfizmem. Niech ponadto $\ker \phi_1 \subset \ker \phi_2$. Wówczas istnieje dokładnie jeden homomorfizm $\psi : F_1 \rightarrow F_2$ taki, że $\psi \circ \phi_1 = \phi_2$ oraz:

- (1) jeśli ϕ_2 jest surjektywny, to ψ jest surjektywny;
- (2) jeśli $\ker \phi_1 = \ker \phi_2$, to ψ jest różnowartościowy;
- (3) jeśli ϕ_2 jest surjektywny i $\ker \phi_1 = \ker \phi_2$, to ψ jest izomorfizmem.

Dowód. Istnienie homomorfizmu ψ wynika z twierdzenia o homomorfizmie.

- (1) Ponieważ $\text{im} \psi = \text{im} \phi_2$, więc jeśli $\text{im} \phi_2 = F_2$, to ψ jest epimorfizmem.
- (2) Ponieważ $\ker \psi = \phi_1(\ker \phi_2)$, więc jeśli $\ker \phi_1 = \ker \phi_2$, to

$$\ker \psi = \phi_1(\ker \phi_2) = \phi_1(\ker \phi_1) = \{1_{F_1}\}.$$

- (3) Wynika wprost z (1) i (2).

□

Wniosek 6.3 (twierdzenie o homomorfizmie dla grup ilorazowych). Niech G, F będą grupami, $H \triangleleft G$, $\phi : G \rightarrow F$ homomorfizmem.

- (1) Jeśli istnieje homomorfizm $\psi : G/H \rightarrow F$ taki, że $\psi \circ \kappa = \phi$ (gdzie $\kappa : G \rightarrow G/H$ oznacza epimorfizm kanoniczny), to $H \subset \ker \phi$.
- (2) Jeśli $H \subset \ker \phi$, to istnieje dokładnie jeden homomorfizm $\psi : G/H \rightarrow F$ taki, że $\psi \circ \kappa = \phi$. Ponadto wówczas $\text{im} \psi = \text{im} \phi$ oraz $\ker \psi = \kappa(\ker \phi)$.

Inaczej: diagram

$$\begin{array}{ccc} & G & \\ \kappa \swarrow & & \searrow \phi \\ G/H & \xrightarrow{\psi} & F \end{array}$$

jest przemienny.

Dowód. W twierdzeniu o homomorfizmie wystarczy wziąć $F_1 = G/H$, $F_2 = F$, $\phi_1 = \kappa$, $\phi_2 = \phi$.

□

Wniosek 6.4. Niech G, F będą grupami, $H \triangleleft G$, $\phi : G \rightarrow F$ homomorfizmem. Niech ponadto $H \subset \ker \phi$. Wówczas istnieje dokładnie jeden homomorfizm $\psi : G/H \rightarrow F$ taki, że $\psi \circ \kappa = \phi$ (gdzie $\kappa : G \rightarrow G/H$ oznacza epimorfizm kanoniczny) oraz

- (1) jeśli ϕ jest surjektywny, to ψ jest surjektywny;
- (2) jeśli $H = \ker \phi$, to ψ jest różnowartościowy;
- (3) jeśli ϕ jest surjektywny i $H = \ker \phi$, to ψ jest izomorfizmem.

Twierdzenie 6.3 (I twierdzenie Noether o izomorfizmie). Niech G, F będą grupami, $\phi : G \rightarrow F$ homomorfizmem. Wówczas

$$\operatorname{im} \phi \cong G / \ker \phi.$$

Przykłady:

- (4) Rozważmy grupy $\mathbb{R}^*$, $\{-1, 1\}$ oraz homomorfizm $\phi : \mathbb{R}^* \rightarrow \{-1, 1\}$, $\phi(x) = \operatorname{sgn}(x)$. Wówczas $\operatorname{im} \phi = \{-1, 1\}$, $\ker \phi = \mathbb{R}_+^*$, a zatem

$$\mathbb{R}^* / \mathbb{R}_+^* \cong \{-1, 1\}.$$

- (5) Rozważmy grupy $\mathbb{Z}$, $\mathbb{Z}_n$ oraz homomorfizm $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$, $\phi(x) = \text{reszta z dzielenia } x \text{ przez } n$. Wówczas $\operatorname{im} \phi = \mathbb{Z}_n$, $\ker \phi = n\mathbb{Z}$, a zatem

$$\mathbb{Z} / n\mathbb{Z} \cong \mathbb{Z}_n.$$

- (6) Rozważmy grupę G oraz homomorfizm $\phi : G \rightarrow G$, $\phi(x) = x$. Wówczas $\operatorname{im} \phi = G$, $\ker \phi = \{1_G\}$, a zatem

$$G / \{1_G\} \cong G.$$

- (7) Rozważmy grupy $GL(n, F)$, F^* oraz homomorfizm $\phi : GL(n, F) \rightarrow F^*$, $\phi(A) = \det A$. Wówczas $\operatorname{im} \phi = F^*$, $\ker \phi = SL(n, F)$, a zatem

$$GL(n, F) / SL(n, F) \cong F^*.$$

- (8) Przypomnijmy, że $\mu_n(\mathbb{C}) = \{z \in \mathbb{C}^* : z^n = 1\} < \mathbb{C}^*$. Oznaczmy ponadto:

$$\mu(\mathbb{C}) = \bigcup_{n \in \mathbb{N}} \mu_n(\mathbb{C}).$$

W szczególności łatwo sprawdzamy, że $\mu(\mathbb{C}) < \mathbb{C}^*$. Rozważmy grupy $\mathbb{Q}$, $\mu(\mathbb{C})$ oraz homomorfizm $\phi : \mathbb{Q} \rightarrow \mu(\mathbb{C})$, $\phi(\frac{m}{n}) = \cos \frac{2\pi m}{n} + i \sin \frac{2\pi m}{n}$. Wówczas $\operatorname{im} \phi = \mu(\mathbb{C})$, $\ker \phi = \mathbb{Z}$, a zatem

$$\mathbb{Q} / \mathbb{Z} \cong \mu(\mathbb{C}).$$

Twierdzenie 6.4 (II twierdzenie Noether o izomorfizmie). Niech G będzie grupą, $H < G$, $N \triangleleft G$. Wówczas

- (1) $N \cap H \triangleleft H$,
- (2) $H / N \cap H \cong HN / N$,

gdzie $HN = \{hn : h \in H, n \in N\} < G$.

Dowód. Pokażemy najpierw, że $HN < G$. Ustalmy $hn, h'n' \in HN$. Wówczas:

$$hn(h'n')^{-1} = hnn'^{-1}h'^{-1} = \underbrace{hh'^{-1}}_{\in H} \underbrace{h'nn'^{-1}}_{\substack{\in N \triangleleft G \\ \in N}} h'^{-1} \in HN.$$

Rozważmy epimorfizm kanoniczny $\kappa : G \rightarrow G/N$, a następnie jego zwężenie $\kappa|_H : H \rightarrow G/N$.

(1) Pokażemy, że $N \cap H \triangleleft H$, czyli że $N \cap H = \ker \kappa \upharpoonright_H$. W tym celu ustalmy $a \in H$. Wówczas

$$\begin{aligned} a \in \ker \kappa \upharpoonright_H &\Leftrightarrow \kappa \upharpoonright_H(a) = N \Leftrightarrow aN = N \\ &\Leftrightarrow a \in N. \end{aligned}$$

Zatem $a \in H$ i $a \in N$, więc $a \in H \cap N$.

(2) Pokażemy, że $\text{im} \kappa \upharpoonright_H = HN/N$. Ustalmy $cN \in \text{im} \kappa \upharpoonright_H$. Wówczas:

$$\begin{aligned} cN \in \text{im} \kappa \upharpoonright_H &\Leftrightarrow \exists a \in H(aN = cN) \\ &\Leftrightarrow \exists a \in H(a^{-1}c \in N) \\ &\Leftrightarrow \exists a \in H \exists b \in N(a^{-1}c = b) \\ &\Leftrightarrow \exists a \in H \exists b \in N(c = ab) \\ &\Leftrightarrow c \in HN \Leftrightarrow cN \in HN/N. \end{aligned}$$

Korzystając z I twierdzenia Noether o izomorfizmie otrzymujemy

$$H/N \cap H \cong HN/N.$$

□

Przykłady:

(9) Rozważmy grupę $\mathbb{Z}$ i jej podgrupy $12\mathbb{Z} < \mathbb{Z}$ oraz $20\mathbb{Z} \triangleleft \mathbb{Z}$. Wówczas $12\mathbb{Z} + 20\mathbb{Z} = 4\mathbb{Z}$, $12\mathbb{Z} \cap 20\mathbb{Z} = 60\mathbb{Z} \triangleleft 12\mathbb{Z}$ oraz $12\mathbb{Z}/60\mathbb{Z} \cong 4\mathbb{Z}/20\mathbb{Z}$.

Twierdzenie 6.5 (lemat o odpowiedniości między podgrupami). *Niech G, F będą grupami, $\pi : G \rightarrow F$ homomorfizmem surjektywnym i niech $N = \ker \pi$. Oznaczmy*

$$\mathcal{R} = \{H : H < G \text{ oraz } N \subset H\}, \mathcal{S} = \{K : K < F\}.$$

Wówczas odwzorowania

$$\begin{aligned} \phi : \mathcal{R} &\rightarrow \mathcal{R}, \phi(H) = \pi(H), \\ \psi : \mathcal{R} &\rightarrow \mathcal{S}, \psi(K) = \pi^{-1}(K) \end{aligned}$$

są wzajemnie odwrotne i zachowują inkluzję, indeks, normalność i grupy ilorazowe.

Dowód. Pokażemy, że $\psi \circ \phi = \text{id}_{\mathcal{R}}$. Ustalmy w tym celu $H < G$ i niech $N \subset H$. Wówczas:

$$\psi \circ \phi(H) = \psi(\pi(H)) = \pi^{-1}(\pi(H))$$

i wobec tego wystarczy sprawdzić, że $H = \pi^{-1}(\pi(H))$. Dla dowodu inkluzji ($\subset$) ustalmy $a \in H$. Wówczas $\pi(a) \in \pi(H)$ oraz

$$a \in \pi^{-1}(\pi(a)) \subset \pi^{-1}(\pi(H)).$$

Dla dowodu inkluzji ($\supset$) ustalmy $a \in \pi^{-1}(\pi(H))$. Wówczas $\pi(a) \in \pi(H)$, czyli $\pi(a) = \pi(b)$, dla pewnego $b \in H$. Wówczas:

$$1_F = (\pi(b))^{-1}\pi(a) = \pi(b^{-1}a).$$

Zatem $b^{-1}a \in \ker \pi = N \subset H$. Stąd:

$$a \in bH = H.$$

Pokażemy, że $\phi \circ \psi = \text{id}_{\mathcal{S}}$. Ustalmy w tym celu $K < F$. Wówczas:

$$\phi \circ \psi(K) = \phi(\pi^{-1}(K)) = \pi(\pi^{-1}(K)) = K \cap \text{im} \pi = K.$$

Pokażemy, że jeśli $H_1 \subset H_2$, dla $H_1, H_2 \in \mathcal{R}$, to $\phi(H_1) \subset \phi(H_2)$. Ustalmy w tym celu $H_1, H_2 < G$ i niech $N \subset H_1, H_2$. Dalej, ustalmy $c \in \phi(H_1) = \pi(H_1)$. Niech $c = \pi(a)$, dla pewnego $a \in H_1 \subset H_2$. Tym samym $c \in \pi(H_2) = \phi(H_2)$.

Analogicznie pokazujemy, że jeśli $K_1 \subset K_2$, dla $K_1, K_2 \in \mathcal{S}$, to $\psi(K_1) \subset \psi(K_2)$.

Pokażemy, że jeśli $H \in \mathcal{R}$ i $(G : H) = n$, to $(F : \phi(H)) = n$. Ustalmy $H < G$ i niech $N \subset H$ oraz $(G : H) = n$. Wystarczy oczywiście pokazać, że zbiory $W_L(H)$ oraz $W_L(\phi(H))$ są równoliczne. Zdefiniujmy w tym celu odwzorowanie $\bar{\phi} : W_L(H) \rightarrow W_L(\phi(H))$ wzorem

$$\bar{\phi}(aH) = \pi(a)\phi(H)$$

oraz odwzorowanie $\bar{\psi} : W_L(\phi(H)) \rightarrow W_L(H)$ wzorem

$$\bar{\psi}(c\phi(H)) = \pi^{-1}(c\phi(H)).$$

Pokażemy, że $\bar{\psi} \circ \bar{\phi} = id_{W_L(H)}$. Ustalmy w tym celu $aH \in W_L(H)$. Pokażemy zatem, że $\bar{\psi} \circ \bar{\phi}(aH) = aH$. Dla dowodu inkluzji ($\supset$) ustalmy $ah \in aH$. Wówczas:

$$\begin{aligned} \pi(ah) &\in \pi(aH) = \pi(a)\pi(H) \\ &= \pi(a)\phi(H) = \bar{\phi}(aH), \end{aligned}$$

zatem

$$\begin{aligned} ah &\in \pi^{-1}(\pi(ah)) = \pi^{-1}(\bar{\phi}(aH)) \\ &= \pi^{-1}(\pi(a)\phi(H)) \\ &= \bar{\psi}(\pi(a)\phi(H)) = \bar{\psi} \circ \bar{\phi}(aH). \end{aligned}$$

Dla dowodu inkluzji ($\subset$) ustalmy $x \in \bar{\psi} \circ \bar{\phi}(aH)$. Wówczas:

$$\begin{aligned} \pi(x) &\in \pi(\bar{\psi} \circ \bar{\phi}(aH)) = \pi(\bar{\psi}(\pi(a)\phi(H))) \\ &= \pi(\pi^{-1}(\pi(a)\phi(H))) = \pi(\pi^{-1}(\pi(a)\pi(H))) \\ &= \pi(\pi^{-1}(\pi(aH))) \subset \pi(aH). \end{aligned}$$

Tym samym:

$$\exists h \in H(\pi(x) = \pi(ah))$$

lub równoważnie:

$$\exists h \in H(1_F = \pi(x^{-1}ah))$$

czyli $x^{-1}ah \in \ker \pi = N \subset H$. Stąd $(x^{-1}ah)^{-1} = h^{-1}a^{-1}x \in H$. Zatem $x \in ahH = aH$.

Analogicznie pokazujemy, że $\bar{\phi} \circ \bar{\psi} = id_{W_L(\phi(H))}$, co kończy dowód tej części twierdzenia. Również analogicznie pokazujemy, że jeśli $K \in \mathcal{S}$ i $(F : K) = n$, to $(G : \psi(K)) = n$.

Z Twierdzenia 5.4 (2) i (3) wynika od razu, że jeśli $H \in \mathcal{R}$ i $H \triangleleft G$, to $\phi(H) \triangleleft F$ oraz że jeśli $K \in \mathcal{S}$ i $K \triangleleft F$, to $\psi(K) \triangleleft G$.

Na koniec, w świetle udowodnionej już części twierdzenia, jest oczywiste, że jeśli $H_1, H_2 \in \mathcal{R}$ oraz $H_1 \triangleleft H_2$, to $\phi(H_2)/\phi(H_1)$ jest dobrze określoną grupą ilorazową oraz że jeśli $K_1, K_2 \in \mathcal{S}$ oraz $K_1 \triangleleft K_2$, to $\psi(K_2)/\psi(K_1)$ również jest dobrze określoną grupą ilorazową. $\square$

Wniosek 6.5 (III twierdzenie Noether o izomorfizmie). *Niech G będzie grupą, $H < G$, $N \triangleleft G$ oraz $N \subset H$. Wówczas*

- (1) $H \triangleleft G$ wtedy i tylko wtedy, gdy $H/N \triangleleft G/N$,
- (2) jeśli $H \triangleleft G$, to $G/H \cong (G/N)/(H/N)$.

Dowód. W lemacie o odpowiedniości między podgrupami wystarczy przyjąć $F = G/N$ oraz $\pi = \kappa$. $\square$

Twierdzenie 6.6 (o klasyfikacji grup cyklicznych). *Niech G będzie grupą cykliczną.*

- (1) Jeśli G jest nieskończona, to $G \cong \mathbb{Z}$.

(2) Jeśli G jest skończona i $|G| = \mathbb{Z}_n$, to $G \cong \mathbb{Z}_n$.

Dowód. Ustalmy grupę cykliczną $G = \langle a \rangle$. Zdefiniujmy odwzorowanie $\phi : \mathbb{Z} \rightarrow G$ wzorem $\phi(k) = a^k$.

Pokażemy, że ϕ jest epimorfizmem. Istotnie, ϕ jest homomorfizmem, gdyż dla ustalonych $k, l \in \mathbb{Z}$ zachodzi $\phi(k+l) = a^{k+l} = a^k a^l = \phi(k)\phi(l)$. Jest też surjekcją, gdyż dla ustalonego $b \in G$, $b = a^k$, dla pewnego $k \in \mathbb{Z}$, a zatem $b = \phi(k)$.

(1) Załóżmy, że $|G| = \infty$, a więc w szczególności $r(a) = \infty$. Pokażemy, że ϕ jest izomorfizmem. Ustalmy w tym celu $k \in \ker \phi$. Wówczas

$$k \in \ker \phi \Leftrightarrow \phi(k) = 1 \Leftrightarrow a^k = 1 \Leftrightarrow k = 0,$$

a zatem $\ker \phi = \{0\}$ i ϕ jest izomorfizmem.

(2) Załóżmy, że $|G| = n$, a więc w szczególności $r(a) = n$. Pokażemy, że $\ker \phi = n\mathbb{Z}$. Ustalmy w tym celu $k \in \ker \phi$. Wówczas

$$\begin{aligned} k \in \ker \phi &\Leftrightarrow \phi(k) = 1 \Leftrightarrow a^k = 1 \Leftrightarrow n|k \\ &\Leftrightarrow k = nt, \text{ dla pewnego } t \in \mathbb{Z}, \end{aligned}$$

a zatem $\ker \phi = n\mathbb{Z}$. Z I twierdzenia o izomorfizmie, $\mathbb{Z}/n\mathbb{Z} \cong G$ i ponieważ $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, więc $G \cong \mathbb{Z}_n$. □

Uwaga 6.2. Niech G, F będą grupami, niech G będzie cykliczna, a $\phi : G \rightarrow F$ niech będzie epimorfizmem. Wówczas F jest grupą cykliczną.

Dowód. Ustalmy grupy $G = \langle a \rangle$, F i epimorfizm $\phi : G \rightarrow F$. Pokażemy, że $F = \langle \phi(a) \rangle$. Inkluzja $(\supset)$ jest oczywista, pozostaje udowodnić inkluzję $(\subset)$. Ustalmy w tym celu $c \in F$. Wówczas $c = \phi(b)$, dla pewnego $b \in G$. Ponadto $b = a^k$, dla pewnego $k \in \mathbb{Z}$. Zatem $c = \phi(a^k) = \phi(a)^k \in \langle \phi(a) \rangle$. □