Homomorfizmy grup, podgrupy normalne.

Definicja:

Niech G, F będą grupami.

1. Odwzorowanie $\phi : G \to F$ nazywamy **homomorfizmem**, jeśli
$$\forall a, b \in G[\phi(a \cdot b) = f(a) \cdot f(b)].$$
Zbiór wszystkich homomorfizmów grupy G w grupę F oznaczamy $Hom(G, F)$.
2. Homomorfizm $\phi : G \to F$ nazywamy **monomorfizmem,** jeśli jest różnowartościowy.
3. Homomorfizm $\phi : G \to F$ nazywamy **epimorfizmem,** jeśli jest surjektywny.

4. Homomorfizm $\phi : G \to G$ nazywamy **endomorfizmem.** Zbiór wszystkich endomorfizmów oznaczamy $End(G)$.
5. Izomorfizm $\phi : G \to G$ nazywamy **automorfizmem.** Zbiór wszystkich automorfizmów oznaczamy $Aut(G)$.
6. Jeśli $\phi : G \to F$ jest homomorfizmem, to zbiór

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

nazywamy **jądrem** homomorfizmu ϕ, zaś zbiór

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

nazywamy **obrazem** homomorfizmu ϕ.

Uwaga

Niech G, F będą grupami, niech $\phi : G \to F$ 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. $r(\phi(a))|r(a)$, *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, $\phi(1_G) = 1_G$.
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 $r(\phi(a))|r(a)$.

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

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

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

Twierdzenie:

Niech G, F będą grupami, niech $\phi : G \to F$ będzie homomorfizmem. Wówczas:

1. $\ker \phi < G$ oraz $\operatorname{im} \phi < F$;
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 $\psi : F \to G$ taki, że

$$\phi \circ \psi = id_F \text{ oraz } \psi \circ \phi = id_G;$$

5. jeśli ϕ jest monomorfizmem, to dla każdej grupy H i dla każdych homomorfizmów $\psi_1, \psi_2 : H \to G$

$$\text{jeśli } \phi \circ \psi_1 = \phi \circ \psi_2, \text{ to } \psi_1 = \psi_2;$$

6. jeśli ϕ jest epimorfizmem, to dla każdej grupy H i dla każdych homomorfizmów $\psi_1, \psi_2 : F \to H$

$$\text{jeśli } \psi_1 \circ \phi = \psi_2 \circ \phi, \text{ to } \psi_1 = \psi_2.$$

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 $\psi : F \to G$ 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 $\phi \circ \psi = id_F$ oraz $\psi \circ \phi = id_G$ 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 $\psi : F \to G$ taki, że

$$\phi \circ \psi = id_F \text{ oraz } \psi \circ \phi = id_G.$$

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

5. Załóżmy, że ϕ jest monomorfizmem. Ustalmy grupę H, homomorfizmy $\psi_1, \psi_2 : H \to G$ 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 $\psi_1, \psi_2 : F \to H$ 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. $\phi : \mathbb{R}^* \to \mathbb{R}^*_+$, $\phi(x) = x^2$ jest homomorfizmem.
2. $\phi : \mathbb{Z} \to \mathbb{Z}$, $\phi(x) = 2x$ jest homomorfizmem.
3. $\phi : \mathbb{R}^*_+ \to \mathbb{R}$, $\phi(x) = \log x$ jest homomorfizmem.
4. $\phi : GL(n, F) \to F$, $\phi(A) = \det A$ jest homomorfizmem.
5. $\phi : G \to G$, $\phi(x) = 1_G$ jest homomorfizmem, nazywamy go **homomorfizmem trywialnym**.
6. $\phi : G \to G$, $\phi(x) = x$ jest automorfizmem.
7. $\phi : \mathbb{C} \to \mathbb{C}$, $\phi(z) = \overline{z}$ jest automorfizmem.
8. $\phi : \mathbb{R}^* \to \mathbb{R}^*$, $\phi(x) = x^{-1}$ jest automorfizmem.

9. $i_a : G \to G$, $a \in G$, $i_a(x) = axa^{-1}$ 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

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

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

Niech G, F *będą grupami,* $H < G$, $K < F$, *niech* $\phi : G \to F$ *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

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

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

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

□

Definicja

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 $H \lhd G$.

Uwaga

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.

Jedyna nietrywialna 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 $H \cap aH = \varnothing = H \cap Ha$, a zatem $aH = G \backslash H = Ha$. $\square$

Twierdzenie

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

1. $H \lhd G$,
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): $H \lhd G \Leftrightarrow \forall a \in G(aH = Ha) \Leftrightarrow \forall a \in G(aHa^{-1} = H)$.
(2) $\Rightarrow$ (3): Oczywiste.
(3) $\Rightarrow$ (4): Załóżmy, że $\forall a \in GaHa^{-1} \subset H$. Pokażemy, że $\forall a \in GaHa^{-1} \supset H$. 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 $\forall b \in GbH = Hb$, lub równoważnie $\forall b \in GbHb^{-1} = H$. 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.

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 $H \lhd D(3)$, 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 $H \not\lhd D(3)$, 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 $Inn(G) \lhd Aut(G)$.

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 $Inn(G) \lhd Aut(G)$, 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

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

□

Twierdzenie

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

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

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 $\phi(h) = k \in K \lhd F$. 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 $SL(n, F) \lhd GL(n, F)$, ponieważ $SL(n, F) = \ker \phi$, gdzie $\phi : GL(n, F) \to F^*$ dane jest wzorem $\phi(A) = \det A$.

Grupa ilorazowa, twierdzenie o homomorfizmie.

Definicja i uwaga

Niech $(G, \cdot)$ *będzie grupą,* $H \lhd G$*. 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 $3\mathbb{Z} \lhd \mathbb{Z}$. Wówczas:

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

Tabelka 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

Niech $(G, \cdot)$ *będzie grupą,* $H \lhd G$*. Wówczas:*

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

Twierdzenie (uogólnione twierdzenie Lagrange'a)

Niech $(G, \cdot)$ *będzie grupą,* $H \lhd G$*. Wówczas zbiory*

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

są równoliczne.

Dowód:

Wybierzmy układ reprezentantów warstw $\{g_iH : i \in I\}$, a więc zbiór o następującej własności:

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

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

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

funkcję $l : G \to I$ warunkiem

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

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

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

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

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

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

Niech $(G, \cdot)$ *będzie grupą,* $H \lhd G$*. Wówczas odwzorowanie* $\kappa : G \to G/H$ *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

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

Dowód.

($\Leftarrow$): wynika z Twierdzenia 0.3 (1).

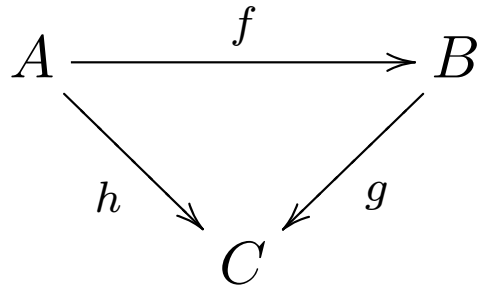
($\Rightarrow$): załóżmy, że $H \lhd G$. Rozważmy epimorfizm kanoniczny $\kappa : G \to G/H$. Wówczas $H = \ker \kappa$. $\square$

Definicja

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:

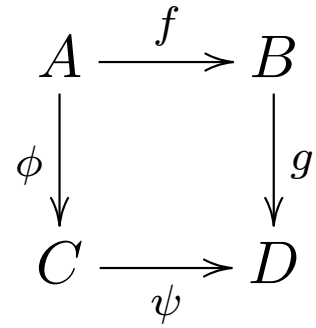
2. To, że diagram:



jest przemienny, oznacza

$$h = g \circ f.$$

3. To, że diagram:



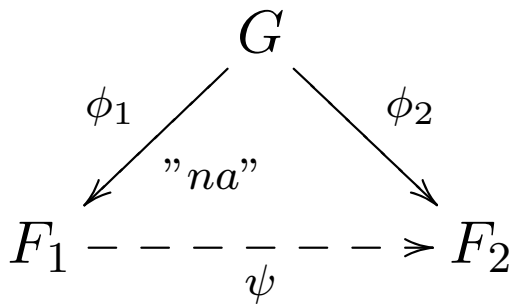
jest przemienny, oznacza

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

Twierdzenie (o homomorfizmie)

Niech G, F_1, F_2 *będą grupami* $\phi_1 : G \to F_1$ *homomorfizmem surjektywnym,* $\phi_2 : G \to F_2$ *homomorfizmem.*

1. *Jeśli istnieje homomorfizm* $\psi : F_1 \to F_2$ *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* $\psi : F_1 \to F_2$ *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. Zdefiniujmy odwzorowanie $\psi : F_1 \to F_2$. 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 $\psi, \psi' : F_1 \to F_2$ 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 kategoryjnym, więc $\psi = \psi'$.

To, że $\operatorname{im}\psi = \operatorname{im}\phi_2$ 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

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

Wniosek

Niech G, F_1, F_2 *będą grupami,* $\phi_1 : G \to F_1$ *homomorfizmem surjektywnym,* $\phi_2 : G \to F_2$ *homomorfizmem. Niech ponadto* $\ker \phi_1 \subset \ker \phi_2$. *Wówczas istnieje dokładnie jeden homomorfizm* $\psi : F_1 \to F_2$ *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 $\operatorname{im}\psi = \operatorname{im}\phi_2$, więc jeśli $\operatorname{im}\phi_2 = F_2$, to ψ jest epimorfizmem.
2. Ponieważ $\ker\psi = \phi_1(\ker\phi_2)$, więc jeśli $\ker\phi_1 = \ker\phi_2$, to

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

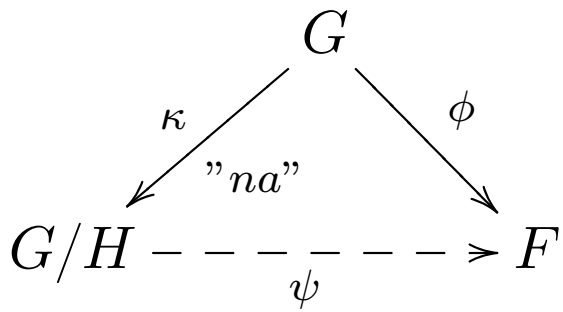
3. Wynika wprost z (1) i (2).

□

Wniosek (twierdzenie o homomorfizmie dla grup ilorazowych)

Niech G, F będą grupami, $H \lhd G$, $\phi : G \to F$ homomorfizmem.

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



jest przemienny.

Dowód.

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

Wniosek

Niech G, F będą grupami, $H \lhd G$, $\phi : G \to F$ homomorfizmem. Niech ponadto $H \subset \ker \phi$. Wówczas istnieje dokładnie jeden homomorfizm $\psi : G/H \to F$ taki, że $\psi \circ \kappa = \phi$ (gdzie $\kappa : G \to G/H$ 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 (I twierdzenie Noether o izomorfizmie)

Niech G, F będą grupami, $\phi : G \to F$ homomorfizmem. Wówczas

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

Przykłady:

4. Rozważmy grupy $\mathbb{R}^*$, $\{-1,1\}$ oraz homomorfizm $\phi : \mathbb{R}^* \to \{-1,1\}$, $\phi(x) = \operatorname{sgn}(x)$. 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 $\phi : \mathbb{Z} \to \mathbb{Z}_n$, $\phi(x) =$ reszta z dzielenia x 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 $\phi : G \to G$, $\phi(x) = x$. 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 $\phi : GL(n, F) \to F^*$, $\phi(A) = \det A$. 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 $\phi : \mathbb{Q} \to \mu(\mathbb{C})$, $\phi(\frac{m}{n}) = \cos\frac{2\pi m}{n} + i\sin\frac{2\pi m}{n}$. Wówczas $\operatorname{im}\phi = \mu(\mathbb{C})$, $\ker\phi = \mathbb{Z}$, a zatem

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

Twierdzenie (II twierdzenie Noether o izomorfizmie)

Niech G *będzie grupą,* $H < G$, $N \lhd G$. *Wówczas*

1. $N \cap H \lhd H$,
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:

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

Rozważmy epimorfizm kanoniczny $\kappa : G \to G/N$, a następnie jego zwężenie $\kappa\restriction_H : H \to G/N$.

1. Pokażemy, że $N \cap H \lhd H$, czyli że $N \cap H = \ker \kappa\restriction_H$. W tym celu ustalmy $a \in H$. Wówczas

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

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

2. Pokażemy, że $\operatorname{im}\kappa\restriction_H = HN/N$. Ustalmy $cN \in \operatorname{im}\kappa\restriction_H$. Wówczas:

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

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 $20\mathbb{Z} \lhd \mathbb{Z}$. Wówczas $12\mathbb{Z} + 20\mathbb{Z} = 4\mathbb{Z}$, $12\mathbb{Z} \cap 20\mathbb{Z} = 60\mathbb{Z} \lhd 12\mathbb{Z}$ oraz $12\mathbb{Z}/60\mathbb{Z} \cong 4\mathbb{Z}/20\mathbb{Z}$.

Twierdzenie (lemat o odpowiedniości między podgrupami)

Niech G, F będą grupami, $\pi : G \to F$ 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

$$\phi : \mathcal{R} \to \mathcal{R}, \phi(H) = \pi(H),$$

$$\psi : \mathcal{R} \to \mathcal{S}, \psi(K) = \pi^{-1}(K)$$

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

Dowód:

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

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

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 $\phi \circ \psi = id_{\mathcal{S}}$. Ustalmy w tym celu $K < F$. Wówczas:

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

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 $\overline{\phi} : W_L(H) \to W_L(\phi(H))$ wzorem

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

oraz odwzorowanie $\overline{\psi} : W_L(\phi(H)) \to W_L(H)$ wzorem

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

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

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

zatem

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

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

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

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 że $\overline{\phi} \circ \overline{\psi} = id_{W_L(\phi(H))}$, 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 0.3 (2) i (3) wynika od razu, że jeśli $H \in \mathcal{R}$ i $H \lhd G$, to $\phi(H) \lhd F$ oraz że jeśli $K \in \mathcal{S}$ i $K \lhd F$, to $\psi(K) \lhd G$.

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

Wniosek (III twierdzenie Noether o izomorfizmie)

Niech G będzie grupą, $H < G$, $N \lhd G$ oraz $N \subset H$. Wówczas

1. *$H \lhd G$ wtedy i tylko wtedy, gdy $H/N \lhd G/N$,*
2. *jeśli $H \lhd G$, 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 (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 $\phi : \mathbb{Z} \to G$ 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

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

Dowód.

Ustalmy grupy $G = \langle a \rangle$, F i epimorfizm $\phi : G \to F$. 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 $c = \phi(a^k) = \phi(a)^k \in \langle \phi(a) \rangle$. $\square$