Wykład 5
Grupa ilorazowa, iloczyn prosty, homomorfizm

1 Grupa ilorazowa

Niech H będzie dzielnikiem normalnym grupy G. Oznaczmy przez G/H zbiór wszystkich warstw lewostronnych grupy G względem podgrupy H. Tak więc

$$G/H = \{gH : g \in G\} \tag{1}$$

oraz $|G/H| = (G : H)$. Ponadto, gdy grupa G jest skończona, to na mocy twierdzenia Lagrange'a $|G/H| = \frac{|G|}{|H|}$.

W zbiorze G/H wprowadzamy działanie $\circ$ przyjmując, że dla dowolnych $a, b \in G$:

$$(aH) \circ (bH) = (a \cdot b)H. \tag{2}$$

Uzasadnimy, że określenie działania $\circ$ jest poprawne, czyli, że nie zależy od wyboru reprezentantów warstw. Niech zatem $a, b, c, d \in G$ będą takie, że $aH = bH$ oraz $cH = dH$. Wtedy $a^{-1}b \in H$ oraz $c^{-1}d \in H$. Zatem $(ac)^{-1}(bd) = c^{-1}a^{-1}bd = (c^{-1}d)[d^{-1}(a^{-1}b)d] \in H$, gdyż $H \lhd G$. Zatem $(ac)H = (bd)H$.

Teraz uzasadnimy, że działanie $\circ$ jest łączne. W tym celu weźmy dowolne $a, b, c \in G$ i obliczmy:

$(aH) \circ [(bH) \circ (cH)] = (aH) \circ ((b \cdot c)H) = (a \cdot (b \cdot c))H = ((ab)c)H = [(ab)H] \circ (cH) = [(aH) \circ (bH)] \circ (cH)$.

Sprawdzimy, że warstwa $eH = H$ jest elementem neutralnym działania $\circ$. Dla dowolnego $a \in G$ mamy, że $(aH) \circ H = (aH) \circ (eH) = (a \cdot e)H = aH = (e \cdot a)H = (eH) \circ (aH) = H \circ (aH)$. Ponadto $(aH) \circ (a^{-1}H) = (a \cdot a^{-1})H = eH = H$ oraz $(a^{-1}H) \circ (aH) = (a^{-1} \cdot a)H = eH = H$. Zatem warstwą odwrotną do warstwy (aH) jest warstwa $a^{-1}H$, czyli

$$(aH)^{-1} = a^{-1}H \text{ dla każdego } a \in G. \tag{3}$$

W ten sposób udowodniliśmy, że system algebraiczny $(G/H, \circ, H)$ jest grupą. Nazywamy ją *grupą ilorazową* względem dzielnika normalnego H. Jeżeli grupa G jest abelowa, to grupa ilorazowa G/H też jest abelowa, gdyż $(aH) \circ (bH) = abH = baH = (bH) \circ (aH)$ dla dowolnych $a, b \in G$.

Wszędzie dalej działanie $\circ$ w grupie ilorazowej G/H będzie oznaczane tym samym symbolem, co działanie w grupie G.

Przykład 5.1. Zbudujemy tabelkę grupy ilorazowej $D_4/\{e, O_2\}$. Niech $\{e, O_2\} = H$. Wtedy:

$$D_4/H = \{\{e, O_2\}, \{S_1, S_2\}, \{S_3, S_4\}, \{O_1, O_3\}\}.$$

Ponadto, H jest elementem neutralnym grupy ilorazowej D_4/H, $S_1H = \{S_1, S_2\}$, $S_3H = \{S_3, S_4\}$, $O_1H = \{O_1, O_3\}$. Grupa ilorazowa D_4/H ma 4 elementy, więc jest abelowa. Ponadto z tabelki grupy D_4 mamy, że $g^2 \in H$ dla każdego $g \in D_4$, więc $(gH)^2 = H$ dla każdego $g \in D_4$ i grupa D_4/H nie jest cykliczna. Dalej, $\{S_1, S_2\} \circ \{S_3, S_4\} = (S_1H) \circ (S_3H) = (S_1 \circ S_3)H = O_3H = \{O_1, O_3\}$, $\{S_1, S_2\} \circ \{O_1, O_3\} = (S_1H) \circ (O_1H) = (S_1 \circ O_1)H = S_4H = \{S_3, S_4\}$, $\{S_3, S_4\} \circ \{O_1,)_3\} = (S_3H) \circ (O_3H) = (S_3 \circ O_3)H = S_2H = \{S_1, S_2\}$. Zatem tabelka grupy D_4/H wygląda tak:

$\circ$	$\{e, O_2\}$	$\{S_1, S_2\}$	$\{S_3, S_4\}$	$\{O_1, O_3\}$
$\{e, O_2\}$	$\{e, O_2\}$	$\{S_1, S_2\}$	$\{S_3, S_4\}$	$\{O_1, O_3\}$
$\{S_1, S_2\}$	$\{S_1, S_2\}$	$\{e, O_2\}$	$\{O_1, O_3\}$	$\{S_3, S_4\}$
$\{S_3, S_4\}$	$\{S_3, S_4\}$	$\{O_1, O_3\}$	$\{e, O_2\}$	$\{S_1, S_2\}$
$\{O_1, O_3\}$	$\{O_1, O_3\}$	$\{S_3, S_4\}$	$\{S_1, S_2\}$	$\{e, O_2\}$

Stwierdzenie 5.2. *Niech H będzie dzielnikiem normalnym grupy G. Wówczas dla każdego $a \in G$ i dla dowolnego $k \in \mathbb{Z}$ zachodzi wzór:*

$$(gH)^k = g^kH. \tag{4}$$

Dowód. Dla $k = 1$ mamy, że $(gH)^1 = gH$ i $g^1H = gH$, więc wzór (4) wówczas zachodzi. Załóżmy, że wzór (4) zachodzi dla pewnego $k \in \mathbb{N}$. Wtedy wzór ten zachodzi też dla liczby $k + 1$, bo na mocy założenia indukcyjnego i definicji mnożenia warstw $(gH)^{k+1} = (gH)^k \cdot (gH) = (g^kH) \cdot (gH) = (g^k \cdot g)H = g^{k+1}H$. Wobec tego na mocy zasady indukcji wzór (4) zachodzi dla każdego naturalnego k.

Jeśli $k = -l$, gdzie $l \in \mathbb{N}$, to ze wzoru na warstwę odwrotną i z pierwszej części rozwiązania, $(gH)^k = [(gH)^{-1}]^l = [g^{-1}H]^l = (g^{-1})^lH = g^{-l}H = g^kH$. W końcu, $(gH)^0 = H = eH = g^0H$, więc wzór (4) zachodzi dla dowolnego całkowitego k. □

Stwierdzenie 5.3. *Niech H będzie dzielnikiem normalnym grupy G i $a \in G$. Warstwa aH ma w grupie ilorazowej G/H skończony rząd wtedy i tylko wtedy, gdy $a^n \in H$ dla pewnego $n \in \mathbb{N}$. Ponadto $o(aH) = m \in \mathbb{N}$ wtedy i tylko wtedy, gdy $a^m \in H$ oraz $a^k \notin H$ dla wszystkich liczb naturalnych $k < m$.*

Dowód. Załóżmy, że $o(aH) = m \in \mathbb{N}$. Wtedy $(aH)^m = H$ i na mocy Stwierdzenia 5.2, $a^mH = H$, skąd $a^m \in H$. Na odwrót, niech $a^n \in H$ dla pewnego $n \in \mathbb{N}$. Wtedy $a^nH = H$, a więc na mocy Stwierdzenia 5.2, $(aH)^n = H$ i stąd $o(aH) < \infty$. Zatem warstwa aH ma w grupie ilorazowej G/H skończony rząd wtedy i tylko wtedy, gdy $a^n \in H$ dla pewnego $n \in \mathbb{N}$.

Niech teraz $o(aH) = m \in \mathbb{N}$. Wówczas z definicji rzędu elementu grupy, $(aH)^m = H$ i dla każdej liczby naturalnej $k < m$ jest $(aH)^k \neq H$. Zatem na mocy Stwierdzenia 5.2, $a^m H = H$ i $a^k H \neq H$, skąd $a^m \in H$ i $a^k \notin H$. $\square$

Przykład 5.4. Pokażemy, że grupa $\mathbb{Z}_{16}^*/\langle 7\rangle$ jest cykliczna, a grupa $\mathbb{Z}_{20}^*/\langle 9\rangle$ nie jest cykliczna.

Zauważmy, że $\mathbb{Z}_{16}^* = \{1,3,5,7,9,11,13,15\}$ oraz w tej grupie $7^2 = 7 \cdot_{16} 7 = [49]_{16} = 1$, więc $\langle 7\rangle = \{1,7\}$. Zatem $|\mathbb{Z}_{16}^*| = 8$ i $|\langle 7\rangle| = 2$, skąd $|\mathbb{Z}_{16}^*/\langle 7\rangle| = \frac{8}{2} = 4$. Ale dla $H = \langle 7\rangle$ mamy, że $3^2 = 9 \notin H$, więc $(3H)^2 \neq H$. Zatem $o(3H) > 2$, skąd $o(3H) = 4$ i grupa $\mathbb{Z}_{16}^*/\langle 7\rangle$ jest cykliczna.

Teraz $\mathbb{Z}_{20}^* = \{1,3,7,9,11,13,17,19\}$ oraz w tej grupie $9^2 = [81]_{20} = 1$, skąd $L = \langle 9\rangle = \{1,9\}$ i $|L| = 2$ oraz $|\mathbb{Z}_{20}^*| = 8$. Zatem $|\mathbb{Z}_{20}^*/\langle 9\rangle| = \frac{8}{2} = 4$. Ponadto, $1^2 = 1 \in L$, $3^2 = 9 \in L$, $7^2 = [49]_{20} = 9 \in L$, $9^2 = 1 \in L$, $11^2 = [121]_{20} = 1 \in L$, $13^2 = (-7)^2 = 7^2 = 9 \in L$, $17^2 = (-3)^2 = 9 \in L$, $19^2 = (-1)^2 = 1 \in L$, skąd $(gL)^2 = L$ dla każdego $g \in \mathbb{Z}_{20}^*$. Wobec tego grupa $\mathbb{Z}_{20}^*/\langle 9\rangle$ nie jest cykliczna.

Twierdzenie 5.5. *Dla dowolnej grupy G grupa ilorazowa G/G' jest abelowa. Ponadto, dla dzielnika normalnego H grupy G, grupa G/H jest abelowa wtedy i tylko wtedy, gdy $G' \subseteq H$.*

Dowód. Niech H będzie dzielnikiem normalnym grupy G. Wtedy dla dowolnych $a, b \in G$ mamy, że $[aH, bH] = (aH)^{-1} \cdot (bH)^{-1} \cdot (aH) \cdot (bH) = (a^{-1}H) \cdot (b^{-1}H) \cdot (abH) = (a^{-1}b^{-1}H) \cdot (abH) = a^{-1}b^{-1}abH = [a,b]H$. Zatem grupa G/H jest abelowa wtedy i tylko wtedy, gdy $[a,b] \in H$ dla dowolnych $a, b \in G$, czyli wtedy i tylko wtedy, gdy $G' \subseteq H$ na mocy definicji komutanta grupy. W szczególności mamy stąd, że grupa G/G' jest abelowa. $\square$

Przykład 5.6. Można wykazać, że istnieje grupa G rzędu 12 taka, że $|G'| = 4$. Pokażemy, że wówczas w grupie G nie istnieje podgrupa rzędu 6 (będzie to oznaczało, że nie można odwracać twierdzenia Lagrange'a!). W tym celu załóżmy, że grupa G posiada podgrupę H rzędu 6. Wtedy z twierdzenia Lagrange'a $(G : H) = \frac{|G|}{|H|} = \frac{12}{6} = 2$, więc na mocy Stwierdzenia 4.14, $H \lhd G$. Ponadto $|G/H| = 2$, więc grupa G/H jest abelowa (a nawet cykliczna). Zatem z Twierdzenia 5.5 mamy, że $G' \subseteq H$. Ale $|G'| = 4$ i $|H| = 6$ oraz 4 nie dzieli 6, więc mamy sprzeczność z twierdzeniem Lagrange'a. Zatem taka grupa G nie posiada podgrupy rzędu 6.

2 Iloczyn prosty grup

Niech $(G_1, \cdot_1, e_1)$ i $(G_2, \cdot_2, e_2)$ będą dowolnymi grupami. W zbiorze $G = G_1 \times G_2$ wprowadzamy mnożenie ,,po współrzędnych"przyjmując, że:

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2), \tag{5}$$

dla dowolnych $a_1, b_1 \in G_1$, $a_2, b_2 \in G_2$.

Niech ponadto $e = (e_1, e_2)$. Sprawdzimy, że $(G, \cdot, e)$ tworzy grupę. W tym celu weźmy dowolne $a_1, b_1, c_1 \in G_1$ oraz dowolne $a_2, b_2, c_2 \in G_2$. Wówczas:

$$(a_1, a_2) \cdot [(b_1, b_2) \cdot (c_1, c_2)] = (a_1, a_2) \cdot (b_1 \cdot_1 c_1, b_2 \cdot_2 c_2) =$$

$$= (a_1 \cdot_1 (b_1 \cdot_1 c_1), a_2 \cdot_2 (b_2 \cdot_2 c_2)) = ((a_1 \cdot_1 b_1) \cdot_1 c_1, (a_2 \cdot_2 b_2) \cdot_2 c_2) =$$

$$= (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2) \cdot (c_1, c_2) = [(a_1, a_2) \cdot (b_1, b_2)] \cdot (c_1, c_2),$$

czyli działanie $\cdot$ jest łączne. Dalej,

$$(a_1, a_2) \cdot e = (a_1, a_2) \cdot (e_1, e_2) = (a_1 \cdot_1 e_1, a_2 \cdot e_2) = (a_1, a_2)$$

oraz

$$e \cdot (a_1, a_2) = (e_1, e_2) \cdot (a_1, a_2) = (e_1 \cdot_1 a_1, e_2 \cdot_2 a_2) = (a_1, a_2),$$

skąd wynika, że e jest elementem neutralnym działania $\cdot$. W końcu

$$(a_1, a_2) \cdot (a_1^{-1}, a_2^{-1}) = (a_1 \cdot_1 a_1^{-1}, a_2 \cdot_2 a_2^{-1}) = (e_1, e_2) = e$$

oraz

$$(a_1^{-1}, a_2^{-1}) \cdot (a_1, a_2) = (a_1^{-1} \cdot_1 a_1, a_2^{-1} \cdot_2 a_2) = (e_1, e_2) = e,$$

czyli $(G, \cdot, e)$ jest grupą oraz

$$(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1}) \text{ dla dowolnych } a_1 \in G_1, a_2 \in G_2. \tag{6}$$

Otrzymaną w ten sposób grupę oznaczamy przez $G_1 \times G_2$ i nazywamy *iloczynem prostym grup* G_1 i G_2.

Z określenia mnożenia w iloczynie prostym grup wynika od razu, że **iloczyn prosty grup abelowych jest grupą abelową**.

Stwierdzenie 5.7. *Dla dowolnych $a \in G_1$, $b \in G_2$ i dla dowolnego $k \in \mathbb{Z}$ w grupie $G_1 \times G_2$ zachodzi wzór*:

$$(a, b)^k = (a^k, b^k). \tag{7}$$

Dowód. Najpierw przez indukcję udowodnimy prawdziwość wzoru (7) dla wszystkich $k \in \mathbb{N}$. Ponieważ $(a, b)^1 = (a, b) = (a^1, b^1)$, więc wzór (7) zachodzi dla $k = 1$. Jeśli zaś wzór (7) zachodzi dla pewnego naturalnego k, to $(a, b)^{k+1} = (a, b)^k \cdot (a, b) = (a^k, b^k) \cdot (a, b) = (a^k \cdot a, b^k \cdot b) = (a^{k+1}, b^{k+1})$, na mocy założenia indukcyjnego i wzoru (5). Wobec tego na mocy zasady indukcji wzór (7) zachodzi dla każdego $k \in \mathbb{N}$.

Jeśli $k = -l$ dla pewnego $l \in \mathbb{N}$, to ze wzoru (6) i na mocy pierwszej części dowodu, $(a, b)^k = [(a, b)^{-1}]^l = (a^{-1}, b^{-1})^l = ((a^{-1})^l, (b^{-1})^l) = (a^{-l}, b^{-l}) = (a^k, b^k)$. W końcu, $(a, b)^0 = (e_1, e_2) = (a^0, b^0)$. Zatem wzór (7) zachodzi dla każdego $k \in \mathbb{Z}$. $\square$

Stwierdzenie 5.8. *Dla dowolnych $a \in G_1$, $b \in G_2$ element (a, b) grupy $G_1 \times G_2$ ma skończony rząd wtedy i tylko wtedy, gdy rzędy elementów a i b są skończone. Ponadto, jeśli $o(a) < \infty$ i $o(b) < \infty$, to rząd elementu (a, b) jest równy $[o(a), o(b)]$.*

Dowód. Załóżmy, że $o((a, b)) = n \in \mathbb{N}$. Wtedy $(a, b)^n = (e_1, e_2)$, więc na mocy wzoru (7), $(a^n, b^n) = (e_1, e_2)$. Zatem $a^n = e_1$ i $b^n = e_2$, czyli $o(a) < \infty$ i $o(b) < \infty$.

Na odwrót, załóżmy, że $o(a) = k \in \mathbb{N}$ i $o(b) = l \in \mathbb{N}$. Oznaczmy $[k, l] = n$. Wtedy $k|n$ i $l|n$, więc $a^n = e_1$ i $b^n = e_2$, czyli na mocy wzoru (7), $(a, b)^n = (a^n, b^n) = (e_1, e_2)$, a to oznacza, że element (a, b) ma skończony rząd, przy czym $s = o((a, b)) \leq n$. Ale wtedy $(a, b)^s = (e_1, e_2)$, więc znowu ze wzoru (7), $(a^s, b^s) = (e_1, e_2)$. Zatem $a^s = e_1$ i $b^s = e_2$, skąd na mocy Stwierdzenia 3.5, $k|s$ i $l|s$. Wobec tego $[k, l]|s$, czyli $n|s$ i $n \leq s$. Ale wcześniej pokazaliśmy, że $s \leq n$, więc $s = n$, co kończy dowód naszego stwierdzenia. □

Stwierdzenie 5.9. *Niech G_1 i G_2 będą nietrywialnymi grupami. Wówczas grupa $G_1 \times G_2$ jest cykliczna wtedy i tylko wtedy, gdy grupy G_1 i G_2 są cykliczne i ich rzędy są liczbami naturalnymi względnie pierwszymi.*

Dowód. Załóżmy, że $G_1 = \langle a \rangle$, gdzie $o(a) = n \in \mathbb{N}$ i $G_2 = \langle b \rangle$, gdzie $o(b) = m \in \mathbb{N}$ oraz $(n, m) = 1$. Wtedy $|G_1 \times G_2| = nm$ i na mocy Stwierdzenia 5.8, $o((a, b)) = [n, m] = nm$, bo $(n, m) = 1$. Wobec tego (a, b) jest generatorem grupy $G_1 \times G_2$ i ta grupa jest cykliczna.

Na odwrót, załóżmy, że grupa $G_1 \times G_2$ jest cykliczna i niech (x, y) będzie jej generatorem. Ponieważ $G_1 \neq \{e_1\}$ i $G_2 \neq \{e_2\}$, więc istnieją $a \in G_1 \setminus \{e_1\}$ i $b \in G_2 \setminus \{e_2\}$. Ale (x, y) jest generatorem grupy $G_1 \times G_2$, więc $(a, e_1) = (x, y)^k$ i $(e_1, b) = (x, y)^l$ dla pewnych całkowitych k, l. Stąd i ze wzoru (7) uzyskujemy, że $a = x^k$, $e_2 = y^k$, $e_1 = x^l$ i $b = y^l$. Ponieważ $a \neq e_1$, więc $k \neq 0$. Ponieważ $b \neq e_2$, więc $l \neq 0$. Ponadto $e_2 = y^k$, więc $y^{-k} = e_2$, skąd $o(y) \in \mathbb{N}$ i podobnie $o(x) \in \mathbb{N}$. Zatem ze Stwierdzenia 5.8 generator (x, y) grupy $G_1 \times G_2$ ma skończony rząd. Wobec tego zbiór $G_1 \times G_2$ jest skończony, a zatem $|G_1| = r \in \mathbb{N}$ i $|G_2| = s \in \mathbb{N}$. Weźmy dowolne $h \in G_1$. Wtedy $(h, e_2) = (x, y)^l$ dla pewnego $l \in \mathbb{Z}$, skąd na mocy wzoru (7), $h = x^l$. Wobec tego $G_1 = \langle x \rangle$. Podobnie dowodzimy, że $G_2 = \langle y \rangle$. Ale $|G_1| = r$ i $|G_2| = s$, więc $o(x) = r$ i $o(y) = s$. Zatem ze Stwierdzenia 5.8, $o((x, y)) = [r, s]$. Ale $o((x, y)) = |G_1 \times G_2| = |G_1| \cdot |G_2| = rs$, więc $[r, s] = rs$, skąd $(r, s) = \frac{rs}{[r,s]} = 1$. □

3 Homomorfizmy grup i ich własności

Definicja 5.10. Niech $(G_1, \cdot_1, e_1)$ i $(G_2, \cdot_2, e_2)$ będą grupami. Przekształcenie $f\colon G_1 \to G_2$ takie, że

$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) \text{ dla dowolnych } a, b \in G_1 \tag{8}$$

nazywamy *homomorfizmem grupy G_1 w grupę G_2*, zaś zbiór

$$Ker(f) = \{x \in G_1 : f(x) = e_2\} \tag{9}$$

nazywamy *jądrem homomorfizmu f*. Jeżeli dodatkowo f jest różnowartościowe, to mówimy, że f jest *zanurzeniem grupy G_1 w grupę G_2*. Jeżeli zaś homomorfizm f jest bijekcją, to mówimy, że f jest *izomorfizmem grup*.

Definicja 5.11. Powiemy, że grupa G_2 jest *obrazem homomorficznym* grupy G_1, jeżeli istnieje homomorfizm f grupy G_1 na grupę G_2.

Definicja 5.12. Powiemy, że grupa G_1 *zanurza się w grupę G_2*, jeśli istnieje zanurzenie $f: G_1 \to G_2$.

Definicja 5.13. Powiemy, że grupy G_1 i G_2 są *izomorficzne* i piszemy, $G_1 \cong G_2$, jeżeli istnieje izomorfizm $f: G_1 \to G_2$.

Definicja 5.14. *Automorfizmem grupy G* nazywamy każdy izomorfizm $f: G \to G$.

Stwierdzenie 5.15. *Złożenie homomorfizmów jest homomorfizmem, tzn. jeżeli $f: G_1 \to G_2$ i $g: G_2 \to G_3$ są homomorfizmami grup, to $g \circ f: G_1 \to G_3$ też jest homomorfizmem grup. W szczególności złożenie izomorfizmów jest izomorfizmem.*

Dowód. Rzeczywiście, dla dowolnych $a, b \in G_1$: $(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$. $\square$

Stwierdzenie 5.16. *Jeżeli $f: G_1 \to G_2$ jest izomorfizmem grup, to $f^{-1}: G_2 \to G_1$ też jest izomorfizmem grup.*

Dowód. Rzeczywiście, ponieważ f jest bijekcją, więc ze wstępu do matematyki f^{-1} istnieje, jest bijekcją oraz dla $x \in G_1$ i $y \in G_2$ mamy, że $y = f(x) \iff f^{-1}(y) = x$. Weźmy dowolne $y_1, y_2 \in G_2$. Wtedy istnieją $x_1, x_2 \in G_1$ takie, że $y_1 = f(x_1)$ i $y_2 = f(x_2)$, więc $y_1 y_2 = f(x_1)f(x_2) = f(x_1 x_2)$, skąd $f^{-1}(y_1 y_2) = x_1 x_2 = f^{-1}(y_1)f^{-1}(y_2)$. $\square$

Ze stwierdzeń 5.15 i 5.16 oraz z tego, że przekształcenie tożsamościowe grupy G w grupę G jest jej automorfizmem wynika od razu następujące

Stwierdzenie 5.17. *Dla dowolnych grup G_1, G_2, G_3:*
a) $G_1 \cong G_1$,
b) jeśli $G_1 \cong G_2$, to $G_2 \cong G_1$,
c) jeśli $G_1 \cong G_2$ i $G_2 \cong G_3$, to $G_1 \cong G_3$. $\square$

Stwierdzenie 5.18. *Niech $(G_1, \cdot_1, e_1)$ i $(G_2, \cdot_2, e_2)$ będą grupami i niech $f: G_1 \to G_2$ będzie homomorfizmem. Wówczas:*
(i) $f(e_1) = e_2$,

(ii) $f(a^{-1}) = [f(a)]^{-1}$ *dla każdego* $a \in G_1$,

(iii) $f(a_1 \cdot_1 a_2 \cdot_1 \ldots \cdot_1 a_n) = f(a_1) \cdot_2 f(a_2) \cdot_2 \ldots \cdot_2 f(a_n)$ *dla dowolnych* $a_1, \ldots, a_n \in G_1$ *oraz dla dowolnego* $n \geq 2$,

(iv) $f(a^k) = [f(a)]^k$ *dla dowolnych* $a \in G_1, k \in \mathbb{Z}$,

(v) jeżeli $a \in G_1$ *i* $o(a) \in \mathbb{N}$, *to* $o(f(a)) \in \mathbb{N}$ *oraz* $o(f(a)) \mid o(a)$,

(vi) $Ker(f) \lhd G_1$,

(vii) f *jest zanurzeniem wtedy i tylko wtedy, gdy* $Ker(f) = \{e_1\}$,

(viii) jeżeli $H \leq G_1$, *to* $f(H) = \{f(h) : h \in H\} \leq G_2$,

(ix) jeżeli $K \leq G_2$, *to* $f^{-1}(K) = \{x \in G_1 : f(x) \in K\} \leq G_1$.

Dowód. (i). Mamy, $f(e_1) = f(e_1 \cdot_1 e_1) = f(e_1) \cdot_2 f(e_1)$, skąd po skróceniu $e_2 = f(e_1)$.

(ii). Rzeczywiście, $f(a^{-1}) \cdot_2 f(a) = f(a^{-1} \cdot_1 a) = f(e_1) = e_2$ na mocy (i), więc $f(a^{-1}) = [f(a)]^{-1}$.

(iii). Dla $n = 2$ teza wynika z definicji homomomorfizmu, a jeżeli zachodzi ona dla pewnego naturalnego n oraz $a_1, \ldots, a_n, a_{n+1} \in G_1$, to $f(a_1 \cdot_1 \ldots \cdot_1 a_n \cdot_1 a_{n+1}) = f((a_1 \cdot_1 \ldots \cdot_1 a_n) \cdot_1 a_{n+1}) = f(a_1 \cdot_1 \ldots \cdot_1 a_n) \cdot_2 f(a_{n+1}) = f(a_1) \cdot_2 \ldots \cdot_2 f(a_n) \cdot_2 f(a_{n+1})$.

(iv). Wynika od razu z (ii) oraz z (iii).

(v). Niech $o(a) = n \in \mathbb{N}$. Wtedy $a^n = e_1$, skąd na mocy (i) oraz (iv), $e_2 = f(a^n) = [f(a)]^n$. Zatem istnieje liczba naturalna k taka, że $k = o(f(a))$ i z własności rzędu elementu grupy $k \mid n$, bo $[f(a)]^n = e_2$.

(vi). Z (i) mamy, że $e_1 \in Ker(f)$. Jeśli $x, y \in Ker(f)$, to $f(x) = f(y) = e_2$, skąd $f(x \cdot_1 y) = f(x) \cdot_2 f(y) = e_2 \cdot_2 e_2 = e_2$, czyli $x \cdot_1 y \in Ker(f)$ oraz na mocy (ii), $f(x^{-1}) = [f(x)]^{-1} = e_2^{-1} = e_2$, czyli $x^{-1} \in Ker(f)$. Zatem $Ker(f) \leq G_1$. Ponadto dla $g \in G_1, h \in Ker(f)$ na mocy (iii) oraz (ii) mamy, że $f(g \cdot_1 h \cdot_1 g^{-1}) = f(g) \cdot_2 f(h) \cdot_2 [f(g)]^{-1} = f(g) \cdot_2 e_2 \cdot_2 [f(g)]^{-1} = e_2$, skąd $g \cdot_1 h \cdot_1 g^{-1} \in Ker(f)$. Zatem $Ker(f) \lhd G_1$.

(vii). Załóżmy, że f jest zanurzeniem i niech $x \in Ker(f)$. Wtedy $f(x) = e_2 = f(e_1)$, skąd $x = e_1$. Ale $e_1 \in Ker(f)$, więc stąd $Ker(f) = \{e_1\}$. Na odwrót, załóżmy, że $Ker(f) = \{e_1\}$ i niech $a, b \in G_1$ będą takie, że $f(a) = f(b)$. Wtedy $e_2 = f(a) \cdot_2 [f(b)]^{-1} = f(a) \cdot_2 f(b^{-1}) = f(a \cdot_1 b^{-1})$, skąd $a \cdot_1 b^{-1} \in Ker(f) = \{e_1\}$, czyli $a \cdot_1 b^{-1} = e_1$. Zatem $a = b$ i f jest zanurzeniem.

$(viii)$. Z (i) mamy, że $e_2 = f(e_1) \in f(H)$, gdyż $e_1 \in H$. Niech $x, y \in f(H)$. Wtedy istnieją $a, b \in H$ takie, że $x = f(a)$ i $y = f(b)$. Zatem $a \cdot_1 b^{-1} \in H$, skąd $f(a \cdot_1 b^{-1}) \in f(H)$ oraz $x \cdot_2 y^{-1} = f(a) \cdot_2 [f(b)]^{-1} = f(a) \cdot_2 f(b^{-1}) = f(a \cdot_1 b^{-1})$, czyli $x \cdot_2 y^{-1} \in f(H)$ i $f(H) \leq G_2$.

(ix). Ponieważ $e_2 \in K$ i $e_2 = f(e_1)$, więc $e_1 \in f^{-1}(K)$. Niech $a, b \in f^{-1}(K)$. Wtedy $f(a), f(b) \in K$, skąd $f(a \cdot_1 b^{-1}) = f(a) \cdot_2 [f(b)]^{-1} \in K$, czyli $a \cdot_1 b^{-1} \in f^{-1}(K)$. Zatem $f^{-1}(K) \leq G_1$. $\square$

Jeżeli $f: G_1 \to G_2$ jest izomorfizmem grup, to $|G_1| = |G_2|$ oraz każda własność grupy G_1 definiowana za pomocą działania w tej grupie jest zachowywana przez f. Z tego powodu **w algebrze utożsamia się grupy izomorficzne**.

Twierdzenie 5.19 (o izomorfizmie). *Jeżeli $f\colon G_1 \to G_2$ jest homomorfizmem grup, to*

$$f(G_1) \cong G_1/Ker(f).$$

W szczególności, jeżeli f jest ,,na", to $G_2 \cong G_1/Ker(f)$.

Dowód. Ze Stwierdzenia 5.18 (viii), $f(G_1) \leq G_2$. Ponadto f odwzorowuje grupę G_1 na $f(G_1)$. Oznaczmy $Ker(f) = H$. Wtedy ze Stwierdzenia 5.18 (vi), $H \lhd G_1$. Niech $F : G_1/H \longrightarrow f(G_1)$ będzie dane wzorem

$$F(xH) = f(x) \text{ dla } x \in G_1.$$

Wtedy dla $x, y \in G_1$ mamy

$$F(xH) = F(yH) \iff f(x) = f(y) \iff [f(x)]^{-1} \cdot_2 f(y) = e_2 \iff$$

$$\iff f(x^{-1}) \cdot_2 f(y) = e_2 \iff f(x^{-1} \cdot_1 y) = e_2 \iff x^{-1} \cdot_1 y \in H \iff xH = yH.$$

Zatem F jest dobrze określoną funkcją różnowartościową. Ale F jest ,,na", więc F jest bijekcją. Ponadto

$$F((xH) \cdot_1 (yH)) = F((x \cdot_1 y)H) = f(x \cdot_1 y) = f(x) \cdot_2 f(y) = F(xH) \cdot_2 F(yH).$$

Zatem F jest izomorfizmem grup, czyli $f(G_1) \cong G_1/Ker(f)$. $\square$

Uwaga 5.20. Niech $(G, \cdot, e)$ będzie grupą i niech $f\colon G \to A$ będzie bijekcją zbioru G na zbiór A. W zbiorze A wprowadzamy działanie $\circ$ przy pomocy wzoru:

$$a \circ b = f(f^{-1}(a) \cdot f^{-1}(b)) \text{ dla } a, b \in A.$$

Niech $\epsilon = f(e)$. Wówczas na mocy Uwagi 1.26, $(A, \circ, \epsilon)$ jest grupą i $f^{-1}(a \circ b) = f^{-1}(a) \cdot f^{-1}(b)$ dla dowolnych $a, b \in A$ oraz f^{-1} jest bijekcją. Zatem f^{-1} jest izomorfizmem grup, czyli $A \cong G$. W szczególności wynika stąd, że jeśli G jest grupą skończoną i $f\colon G \to A$ jest bijekcją oraz w tabelce grupy G w miejsce każdego elementu $x \in G$ wstawimy element $f(x)$, to trzymamy tabelkę grupy A izomorficznej z grupą G.

Zagadka 1. Niech H będzie podgrupą grupy G. Pokazać, że jeśli H nie jest dzielnikiem normalnym grupy G, to wzór

$$(aH) \circ (bH) = (a \cdot b)H \quad \text{dla } \ a, b \in G$$

nie jest dobrze określony na zbiorze wszystkich warstw lewostronnych grupy G względem podgrupy H.

Zagadka 2. Udowodnij, że obraz homomorficzny grupy cyklicznej jest grupą cykliczną.

Zagadka 3. Udowodnij, że dla dowolnej liczby pierwszej nieparzystej p i dla dowolnego $\alpha \in \mathbb{N}$ grupy $\mathbb{Z}^*_{2p^\alpha}$ i $\mathbb{Z}^*_{p^\alpha}$ są izomorficzne.

Zagadka 4. Udowodnij, że dla dowolnego $n \in \mathbb{N}$ w grupie $\mathbb{Q}^+/\mathbb{Z}$ istnieje dokładnie jedna podgrupa rzędu n.

Zagadka 5. Udowodnij, że jeśli grupa $G/Z(G)$ jest cykliczna, to grupa G jest abelowa.

Zagadka 6. Uzasadnij, że jeśli H jest nietrywialną podgrupą grupy $\mathbb{Q}^+$, to każdy element grupy $\mathbb{Q}^+/H$ ma skończony rząd. Udowodnij też, że jeśli grupa $\mathbb{Q}^+/H$ jest skończona, to $H = \mathbb{Q}$.

Zagadka 7. Niech H będzie dzielnikiem normalnym grupy G i niech $U, W \in G/H$. Udowodnij, że wówczas w grupie ilorazowej G/H: $U \cdot W = \{a \cdot b \ : \ a \in U,\ b \in W\}$.