Wykład 6
Przykłady homomorfizmów

Przykład 6.1. Dla dowolnych grup $(G_1, \cdot_1, e_1)$, $(G_2, \cdot_2, e_2)$ przekształcenie $f\colon G_1 \to G_2$ dane wzorem

$$f(x) = e_2 \text{ dla } x \in G_1$$

jest homomorfizmem grup, bo $f(a) \cdot_2 f(b) = e_2 \cdot_2 e_2 = e_2 = f(a \cdot_1 b)$ dla dowolnych $a, b \in G_1$. Nazywamy go *homomorfizmem trywialnym.*

Przykład 6.2. Niech G będzie grupą i $g \in G$. Wtedy przekształcenie $f\colon G \to G$ dane wzorem

$$f(x) = g \cdot x \cdot g^{-1} \text{ dla } x \in G$$

jest automorfizmem grupy G, gdyż $f(a{\cdot}b) = g{\cdot}(a{\cdot}b){\cdot}g^{-1} = (g{\cdot}a{\cdot}g^{-1}){\cdot}(g{\cdot}b{\cdot}g^{-1}) = f(a){\cdot}f(b)$ dla $a, b \in G$ oraz przekształcenie $h : G \longrightarrow G$ dane wzorem: $h(x) = g^{-1} \cdot x \cdot g$ dla $x \in G$ jest odwrotne do f. Taki automorfizm f nazywamy *automorfizmem wewnętrznym.*

Przykład 6.3. Niech H będzie dzielnikiem normalnym grupy G i niech $\pi\colon G \to G/H$ będzie odwzorowaniem danym wzorem

$$\pi(x) = xH \text{ dla } x \in G.$$

Wówczas dla dowolnych $a, b \in G$ mamy, że $\pi(ab) = (ab)H = (aH) \cdot (bH) = \pi(a) \cdot \pi(b)$, więc π jest homomorfizmem grup. Ponadto $G/H = \{aH = \pi(a) : a \in G\}$, więc π jest „na". Dla $a \in G$ mamy, że $a \in Ker(\pi) \Leftrightarrow \pi(a) = H \Leftrightarrow aH = H \Leftrightarrow a \in H$, więc $Ker(\pi) = H$. Taki homomorfizm π nazywamy *epimorfizmem naturalnym.*

Przy okazji zauważmy, że każdy dzielnik normalny grupy G jest jądrem pewnego homomorfizmu określonego na tej grupie. Stąd wobec Stwierdzenia 5. 18 (vi), **dzielniki normalne grupy G są to dokładnie jądra homomorfizmów określonych na grupie G.** Z twierdzenia o izomorfizmie wynika stąd zatem, że **każdy obraz homomorficzny grupy G jest izomorficzny z grupą ilorazową G/H dla pewnego $H \lhd G$.**

Stwierdzenie 6.4. *Niech $\langle a \rangle$ będzie cykliczną grupą nieskończoną i niech B będzie dowolną grupą. Wówczas dla dowolnego $b \in B$ przekształcenie $f\colon \langle a \rangle \to B$ dane wzorem*

$$f(a^k) = b^k \text{ dla wszystkich } k \in \mathbb{Z} \tag{1}$$

jest homomorfizmem grupy $\langle a \rangle$ w grupę B i $f(a) = b$. Ponadto $f(\langle a \rangle) = \langle b \rangle$ oraz jeśli $o(b) = \infty$, to f jest zanurzeniem, a jeśli $o(b) = n \in \mathbb{N}$, to f nie jest zanurzeniem i $Ker(f) = \langle a^n \rangle$.

Jeśli $g\colon \langle a\rangle \to B$ jest homomorfizmem i $b = f(a)$, to $g(a^k) = b^k$ dla każdego $k \in \mathbb{Z}$ i g jest ,,na"wtedy i tylko wtedy, gdy b jest generatorem grupy B.

W szczególności moc zbioru wszystkich homomorfizmów grupy $\langle a\rangle$ w grupę B jest równa mocy zbioru B.

Dowód. Na mocy Stwierdzenia 3.7 każdy element grupy $\langle a\rangle$ można jednoznacznie zapisać w postaci a^k dla pewnego $k \in \mathbb{Z}$. Wobec tego f jest dobrze określone. Ponadto $f(a) = f(a^1) = b^1 = b$. Weźmy dowolne $x, y \in \langle a\rangle$. Wtedy $x = a^k$ i $y = a^l$ dla pewnych $k, l \in \mathbb{Z}$. Stąd $f(x \cdot y) = f(a^k \cdot a^l) = f(a^{k+l}) = b^{k+l}$ oraz $f(x) \cdot f(y) = b^k \cdot b^l = b^{k+l}$. Zatem $f(x \cdot y) = f(x) \cdot f(y)$ i f jest homomorfizmem. Ze wzoru (1) od razu wynika, że $f(\langle a\rangle) = \langle b\rangle$. Niech $o(b) = \infty$ i $a^k \in Ker(f)$ dla pewnego $k \in \mathbb{Z}$. Wtedy $b^k = e$ i na mocy Stwierdzenia 3.7, $k = 0$ oraz $a^k = e$. Zatem w tym przypadku $Ker(f) = \{e\}$ i na mocy Stwierdzenia 5.18 (vii), f jest zanurzeniem.

Niech teraz $o(b) = n \in \mathbb{N}$. Niech $a^k \in Ker(f)$ dla pewnego $k \in \mathbb{Z}$. Wtedy $e = f(a^k) = b^k$, skąd na mocy Stwierdzenia 3.5, $n|k$, czyli $k = nl$ dla pewnego $l \in \mathbb{Z}$ i $a^k = (a^n)^l \in \langle a^n\rangle$. Jeśli zaś $x \in \langle a^n\rangle$, to $x = (a^n)^s = a^{ns}$ dla pewnego $s \in \mathbb{Z}$, więc $f(x) = b^{ns} = (b^n)^s = e^s = e$, czyli $x \in Ker(f)$. Wobec tego w tym przypadku $Ker(f) = \langle a^n\rangle$, skąd $a^n \in Ker(f)$. Ale $a^n \neq e$, bo $o(a) = \infty$, więc $Ker(f) \neq \{e\}$ i f nie jest zanurzeniem.

Ze Stwierdzenia 5.18 (iv) mamy, że $g(a^k) = [g(a)]^k = b^k$ dla każdego $k \in \mathbb{Z}$. Ponadto wykazaliśmy wcześniej, że $g(\langle a\rangle) = \langle b\rangle$, więc g jest ,,na"wtedy i tylko wtedy, gdy b jest generatorem grupy B. □

Twierdzenie 6.5. *Jedyną z dokładnością do izomorfizmu nieskończoną grupą cykliczną jest grupa $\mathbb{Z}^+$. Każde dwie nieskończone grupy cykliczne $\langle a\rangle$ i $\langle b\rangle$ są izomorficzne. Ponadto przekształcenia $f\colon \langle a\rangle \to \langle b\rangle$ i $g\colon \langle a\rangle \to \langle b\rangle$ dane wzorami: $f(a^k) = b^k$ i $g(a^k) = b^{-k}$ dla $k \in \mathbb{Z}$ są wszystkimi różnymi izomorfizmami grupy $\langle a\rangle$ na grupę $\langle b\rangle$.*

Dowód. Niech $\langle a\rangle$ i $\langle b\rangle$ będą nieskończonymi grupami cyklicznymi. Wtedy na mocy Stwierdzenia 6.4 przekształcenie $f\colon \langle a\rangle \to \langle b\rangle$ dane wzorem $f(a^k) = b^k$ jest zanurzeniem i f jest ,,na", czyli f jest izomorfizmem. W szczególności $\mathbb{Z}^+$ jest jedyną z dokładnością do izomorfizmu nieskończoną grupą cykliczną. Ponadto $\langle b^{-1}\rangle = \langle b\rangle$, więc g jest też izomorfizmem, gdyż $(b^{-1})^k = b^{-k}$ dla dowolnego $k \in \mathbb{Z}$. Mamy też $f(a) = b \neq b^{-1} = g(a)$ na mocy Stwierdzenia 3.7, więc $f \neq g$.

Niech $h\colon \langle a\rangle \to \langle b\rangle$ będzie izomorfizmem. Wtedy na mocy Stwierdzenia 6.4 dla $c = h(a)$ jest $h(\langle a\rangle) = \langle c\rangle$ oraz $h(a^k) = c^k$ dla $k \in \mathbb{Z}$. Ale h jest ,,na", więc c jest generatorem grupy $\langle b\rangle$ i na mocy Stwierdzenia 3.7, $c = b$ lub $c = b^{-1}$, skąd $h = f$ lub $h = g$. □

Stwierdzenie 6.6. *Niech $\langle a\rangle$ będzie grupą cykliczną rzędu $n \in \mathbb{N}$ i niech B będzie dowolną grupą. Wówczas dla dowolnego $b \in B$ takiego, że $o(b)|n$ przekształcenie $f\colon \langle a\rangle \to B$ dane wzorem*

$$f(a^k) = b^k \text{ dla wszystkich } k \in \mathbb{Z} \tag{2}$$

jest homomorfizmem grupy $\langle a\rangle$ w grupę B i $f(a) = b$. Ponadto $f(\langle a\rangle) = \langle b\rangle$ oraz jeśli

$o(b) = n$, to f jest zanurzeniem, a jeśli $o(b) \neq n$, to f nie jest zanurzeniem i $Ker(f) = \langle a^{o(b)} \rangle$.

Jeśli $g\colon \langle a \rangle \to B$ jest homomorfizmem i $b = g(a)$, to $g(a^k) = b^k$ dla każdego $k \in \mathbb{Z}$, $o(b)|n$ i g jest ,,na"wtedy i tylko wtedy, gdy b jest generatorem grupy B.

Dowód. Z Uwagi 3.4 mamy, że $o(a) = n$, więc $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ na mocy Stwierdzenia 2.16. Niech $b \in B$ będzie takie, że $o(b)|n$. Wtedy dla dowolnych $k, l \in \mathbb{Z}$ takich, że $a^k = a^l$ jest $a^{k-l} = e$, więc na mocy Stwierdzenia 3.5, $n|k-l$, skąd $o(b)|k-l$. Zatem $e = b^{k-l}$, skąd $b^k = b^l$, czyli $f(a^k) = f(b^l)$. Wobec tego f jest dobrze określone. Ponadto $f(a) = f(a^1) = b^1 = b$. Weźmy dowolne $x, y \in \langle a \rangle$. Wtedy $x = a^k$ i $y = a^l$ dla pewnych $k, l \in \mathbb{Z}$. Stąd $f(x \cdot y) = f(a^k \cdot a^l) = f(a^{k+l}) = b^{k+l}$ oraz $f(x) \cdot f(y) = b^k \cdot b^l = b^{k+l}$. Zatem $f(x \cdot y) = f(x) \cdot f(y)$ i f jest homomorfizmem. Ze wzoru (2) od razu wynika, że $f(\langle a \rangle) = \langle b \rangle$. Niech $o(b) = n$ i $a^k \in Ker(f)$ dla pewnego $k \in \mathbb{Z}$. Wtedy $b^k = e$ i na mocy Stwierdzenia 3.5, $n|k$, skąd $a^k = e$. Zatem w tym przypadku $Ker(f) = \{e\}$ i na mocy Stwierdzenia 5.18 (vii), f jest zanurzeniem. Niech teraz $o(b) \neq n$. Wtedy $o(b) < n$. Niech $a^k \in Ker(f)$ dla pewnego $k \in \mathbb{Z}$. Wtedy $e = f(a^k) = b^k$, skąd na mocy Stwierdzenia 3.5, $o(b)|k$, czyli $k = o(b)l$ dla pewnego $l \in \mathbb{Z}$ i $a^k = (a^{o(b)})^l \in \langle a^{o(b)} \rangle$. Jeśli zaś $x \in \langle a^{o(b)} \rangle$, to $x = (a^{o(b)})^s = a^{o(b)s}$ dla pewnego $s \in \mathbb{Z}$, więc $f(x) = b^{o(b)s} = (b^{o(b)})^s = e^s = e$, czyli $x \in Ker(f)$. Wobec tego w tym przypadku $Ker(f) = \langle a^{o(b)} \rangle$, skąd $a^{o(b)} \in Ker(f)$. Ale $a^{o(b)} \neq e$, bo $o(b) < n$, więc $Ker(f) \neq \{e\}$ i f nie jest zanurzeniem.

Ze Stwierdzenia 5.18 mamy, że $g(a^k) = [g(a)]^k = b^k$ dla każdego $k \in \mathbb{Z}$ i $o(b)|n$. Ponadto wykazaliśmy wcześniej, że $g(\langle a \rangle) = \langle b \rangle$, więc g jest ,,na"wtedy i tylko wtedy, gdy b jest generatorem grupy B. □

Twierdzenie 6.7. *Niech $n \in \mathbb{N}$. Jedyną z dokładnością do izomorfizmu grupą cykliczną rzędu n jest grupa $\mathbb{Z}_n^+$. Każde dwie grupy cykliczne $\langle a \rangle$ i $\langle b \rangle$ rzędu n są izomorficzne. Ponadto przekształcenia $f_s\colon \langle a \rangle \to \langle b \rangle$ dane wzorami: $f_s(a^k) = b^{sk}$ dla $k \in \mathbb{Z}$ oraz $s \in \{1, 2, \ldots, n\}$ takich, że $(s, n) = 1$ są wszystkimi różnymi izomorfizmami grupy $\langle a \rangle$ na grupę $\langle b \rangle$. W szczególności istnieje dokładnie $\varphi(n)$ różnych izomorfizmów grupy $\langle a \rangle$ na grupę $\langle b \rangle$.*

Dowód. Niech $\langle a \rangle$ i $\langle b \rangle$ będą grupami cyklicznymi rzędu n i niech $s \in \{1, 2, \ldots, n\}$ będzie takie, że $(s, n) = 1$. Wtedy na mocy Wniosku 3.11, b^s jest generatorem grupy $\langle b \rangle$, więc $o(b^s) = n$. Zatem ze Stwierdzenia 6.6 przekształcenie $f_s\colon \langle a \rangle \to \langle b \rangle$ dane wzorem $f_s(a^k) = b^{sk}$ dla $k \in \mathbb{Z}$ jest zanurzeniem i f_s jest ,,na", czyli f_s jest izomorfizmem. W szczególności $\mathbb{Z}_n^+$ jest jedyną z dokładnością do izomorfizmu grupą cykliczną rzędu n. Niech $s, r \in \{1, 2, \ldots, n\}$ i $(s, n) = (r, n) = 1$ oraz $f_s = f_r$. Wtedy $f_s(a) = f_r(a)$, skąd $b^s = b^r$ i na mocy Stwierdzenia 2.16, $s = r$.

Niech $h\colon \langle a \rangle \to \langle b \rangle$ będzie izomorfizmem. Wtedy na mocy Stwierdzenia 6.6 dla $c = h(a)$ jest $h(\langle a \rangle) = \langle c \rangle$ oraz $h(a^k) = c^k$ dla $k \in \mathbb{Z}$. Ale h jest ,,na", więc c jest generatorem grupy $\langle b \rangle$ i na mocy Wniosku 3.11, $c = b^s$ dla pewnego $s \in \{1, 2, \ldots, n\}$ takiego, że $(s, n) = 1$. Zatem $h(a^k) = (b^s)^k = b^{sk}$ dla $k \in \mathbb{Z}$. Wobec tego $h = f_s$. □

Stwierdzenie 6.8. *Niech $m, n \in \mathbb{N}$. Istnieje dokładnie (n, m) wszystkich homomorfizmów grupy cyklicznej $\langle a \rangle$ rzędu n w grupę cykliczną $\langle b \rangle$ rzędu m i są one postaci:*

$$f_j(a^k) = b^{j \cdot \frac{m}{(n,m)} \cdot k} \text{ dla } k \in \mathbb{Z} \text{ oraz } j = 0, 1, \ldots, (n, m) - 1. \tag{3}$$

Ponadto $Ker(f_j) = \left\langle a^{\frac{(n,m)}{(j,(n,m))}} \right\rangle$ dla $j = 0, 1, \ldots, (n, m) - 1$.

Dowód. Oznaczmy $A = \langle a \rangle$ i $B = \langle b \rangle$. Wówczas na mocy Stwierdzenia 6.6 każdy homomorfizm $f: A \to B$ jest jednoznacznie wyznaczony przez element $c = f(a)$, przy czym $f(a^k) = c^k$ dla $k \in \mathbb{Z}$ i $o(c)|n$. Ponadto z twierdzenia Lagrange'a $o(c)|m$, więc z teorii liczb mamy, że $o(c)|(n, m)$. Z Uwagi 3.16 w grupie B istnieje dokładnie jedna podgrupa C rzędu (n, m). Dalej, z Uwagi 3.4, $o(x) = |\langle x \rangle|$ dla każdego $x \in B$. Ponadto z Twierdzenia 3.9, $o\left(b^{\frac{m}{(n,m)}}\right) = (n, m)$, więc $C = \left\langle b^{\frac{m}{(n,m)}} \right\rangle$. Ale $o(c)||C|$ i w C istnieje dokładnie jedna podgrupa rzędu $o(c)$, więc $c \in C$. W ten sposób wykazaliśmy, że jeśli $f: A \to B$ jest homomorfizmem, to $f(a) \in \langle b^{\frac{m}{(n,m)}} \rangle$. Na odwrót, jeśli $c \in \langle b^{\frac{m}{(n,m)}} \rangle$, to $o(c)|(n, m)$, więc ze Stwierdzenia 6.6 przekształcenie $f: A \to B$ dane wzorem $f(a^k) = c^k$ dla $k \in \mathbb{Z}$ jest homomorfizmem i $f(a) = c$. Wynika stąd, że istnieje dokładnie (n, m) wszystkich homomorfizmów grupy A w grupę B i wszystkie one są postaci

$$f_j(a^k) = b^{j \cdot \frac{m}{(n,m)} \cdot k} \text{ dla } k \in \mathbb{Z} \text{ oraz } j = 0, 1, \ldots, (n, m) - 1.$$

Ponadto ze Stwierdzenia 6.6, $Ker(f_j) = \langle a^{l_j} \rangle$, gdzie $l_j = o(b^{j \cdot \frac{m}{(n,m)}})$. Ale na mocy Twierdzenia 3.9, $o(b^{j \cdot \frac{m}{(n,m)}}) = \frac{(n,m)}{(j,(n,m))}$, więc $l_j = \frac{(n,m)}{(j,(n,m))}$, skąd $Ker(f_j) = \left\langle a^{\frac{(n,m)}{(j,(n,m))}} \right\rangle$. □

Przykład 6.9. Wyznaczymy wszystkie homomorfizmy grupy $A = \langle a \rangle$ cyklicznej rzędu 124 w grupę cykliczną $B = \langle b \rangle$ rzędu 168. Wypiszemy też jądro każdego z tych homomorfizmów.

Najpierw stosując algorytm Euklidesa obliczamy $(124, 168) = (124, 44) = (44, 36) = (36, 8) = (8, 4) = 4$. Następnie obliczamy $\frac{m}{(n,m)} = \frac{168}{4} = 42$. Ze Stwierdzenia 6.8 są dokładnie 4 takie homomorfizmy:

$f_0(a^k) = e$ dla każdego $k \in \mathbb{Z}$ i $Ker(f_0) = A$;
$f_1(a^k) = b^{42k}$ dla każdego $k \in \mathbb{Z}$ i $Ker(f_1) = \langle a^{\frac{4}{(1,4)}} \rangle = \langle a^4 \rangle = \{e, a^4, a^8, \ldots, a^{120}\}$,
$f_2(a^k) = b^{84k}$ dla każdego $k \in \mathbb{Z}$ i $Ker(f_2) = \langle a^{\frac{4}{(2,4)}} \rangle = \langle a^2 \rangle = \{e, a^2, a^4, \ldots, a^{122}\}$,
$f_3(a^k) = b^{126k}$ dla każdego $k \in \mathbb{Z}$ i $Ker(f_3) = \langle a^{\frac{4}{(3,4)}} \rangle = \langle a^4 \rangle = \{e, a^4, a^8, \ldots, a^{120}\}$.

Twierdzenie 6.10. *Z dokładnością do izomorfizmu istnieją dokładnie dwie grupy rzędu 4: grupa czwórkowa Kleina K i grupa cykliczna $\mathbb{Z}_4^+$.*

Dowód. Niech G będzie grupą rzędu 4. Jeśli G posiada element rzędu 4, to G jest cykliczna i z Twierdzenia 6.7, $G \cong \mathbb{Z}_4^+$. W przeciwnym przypadku ze Stwierdzenia 2.19, $G = \{e, x, y, z\}$ dla pewnych $x, y, z \in G$ takich, że $xy = yx = z$, $o(x) = o(y) = o(z) = 2$. Wobec tego tabelka grupy G ma postać:

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	z	e

Rozważmy bijekcję $f\colon K \to G$ taką, że $f(e) = e$, $f(S_a) = x$, $f(S_b) = y$ i $f(S_O) = z$. Wtedy tabelka grupy K przejdzie na tabelkę grupy G, więc f jest izomorfizmem, czyli $G \cong K$. Ponadto grupa K nie jest cykliczna, a więc K nie jest izomorficzna z grupą $\mathbb{Z}_4^+$. $\square$

Przykład 6.11. Ze Stwierdzenia 6.7 mamy, że dla $n \in \mathbb{N}$, $f\colon \mathbb{Z}^+ \to \mathbb{Z}_n^+$ dane wzorem $f(k) = k \cdot 1$ dla $k \in \mathbb{Z}$ jest homomorfizmem grupy $\mathbb{Z}^+$ na grupę $\mathbb{Z}_n^+$ oraz $Ker(f) = \langle n \rangle$. Zatem z twierdzenia o izomorfizmie mamy

$$\mathbb{Z}_n^+ \cong \mathbb{Z}^+/\langle n \rangle.$$

Twierdzenie 6.12. *Niech $f\colon G \to A$ będzie homomorfizmem grupy skończonej G w grupę A. Wówczas $|f(G)|$ dzieli $|G|$. Jeżeli dodatkowo A jest grupą skończoną, to $|f(G)|$ dzieli $(|G|, |A|)$.*

Dowód. Z twierdzenia o izomorfizmie mamy, że $f(G) \cong G/Ker(f)$, skąd na mocy twierdzenia Lagrange'a $|f(G)| = |G/Ker(f)| = \frac{|G|}{|Ker(f)|}$, a więc $|f(G)| \mid |G|$. Jeżeli dodatkowo grupa A jest skończona, to z twierdzenia Lagrange'a i ze Stwierdzenia 5.18 (viii), $|f(G)|$ dzieli $|A|$, więc z elementarnej teorii liczb $|f(G)|$ dzieli $(|G|, |A|)$. $\square$

Wniosek 6.13. *Jeśli grupy A i B są skończone i mają względnie pierwsze rzędy, to jedynym homomorfizmem $f\colon A \to B$ jest homomorfizm trywialny.*

Dowód. Ponieważ $(|A|, |B|) = 1$, więc z Twierdzenia 6.12 mamy, że $|f(A)| = 1$. Zatem $f(A) = \{e\}$, czyli $f(a) = e$ dla każdego $a \in A$, a więc f jest homomorfizmem trywialnym. $\square$

Przykład 6.14. Pokażemy, że nie istnieje nietrywialny homomorfizm grupy D_3 w grupę $\mathbb{Z}_{15}^+$. W tym celu załóżmy, że istnieje nietrywialny homomorfizm $f\colon D_3 \to \mathbb{Z}_{15}^+$. Wtedy $|f(D_3)| > 1$ oraz z Twierdzenia 6.12, $|f(D_3) \mid |(6, 15) = 3$, więc $|f(D_3)| = 3$ oraz z twierdzenia o izomorfizmie i z twierdzenia Lagrange'a $|Ker(f)| = 2$. Ale $Ker(f) \lhd D_3$ i grupa D_3 nie posiada dzielnika normalnego rzędu 2, więc mamy sprzeczność.

Przykład 6.15. Pokażemy, że jeśli niepuste zbiory A i B są równoliczne, to grupy symetryczne $S(A)$ i $S(B)$ są izomorficzne. Rzeczywiście, niech $f\colon A \to B$ będzie bijekcją. Określamy $F\colon S(A) \to S(B)$ wzorem $F(\phi) = f \circ \phi \circ f^{-1}$ dla $\phi \in S(A)$. Wtedy ze Wstępu do matematyki mamy, że $F(\phi)$ jest bijekcją jako złożenie bijekcji, czyli $F(\phi) \in S(B)$ dla $\phi \in S(A)$. Ponadto dla dowolnych $\phi_1, \phi_2 \in S(A)$ mamy

$$F(\phi_1 \circ \phi_2) = f \circ (\phi_1 \circ \phi_2) \circ f^{-1} =$$
$$= (f \circ \phi_1 \circ f^{-1}) \circ (f \circ \phi_2 \circ f^{-1}) = F(\phi_1) \circ F(\phi_2),$$

więc F jest homomorfizmem. Ponadto $G\colon S(B) \to S(A)$ dane wzorem $G(\psi) = f^{-1} \circ \psi \circ f$ dla $\psi \in S(B)$ jest przekształceniem odwrotnym do F. Zatem F jest izomorfizmem.

Twierdzenie 6.16 (Cayley'a). *Każda grupa G zanurza się w grupę symetryczną $S(G)$.*

Dowód. Niech dla $g \in G$: $l_g(x) = gx$ dla $x \in G$. Wtedy, jak wiemy l_g jest bijekcją zbioru G na siebie, więc $l_g \in S(G)$. Niech $F(g) = l_g$ dla $g \in G$. Wtedy dla $g, h, x \in G$ mamy, że $(F(gh))(x) = l_{gh}(x) = (gh)x = g(hx) = gl_h(x) = l_g(l_h(x)) = (l_g \circ l_h)(x) = (F(g) \circ F(h))(x)$, skąd $F(gh) = F(g) \circ F(h)$ i F jest homomorfizmem. Jeżeli $g \in Ker(F)$, to $l_g(x) = x$ dla $x \in G$, czyli $gx = x$ dla $x \in G$. Zatem $g = e$. Stąd ze Stwierdzenia 5.18, F jest zanurzeniem. $\square$

Z Twierdzenia Cayley'a i z Przykładu 6.15 wynika od razu następujący

Wniosek 6.17. *Każda grupa skończona rzędu n zanurza się w grupę permutacji S_n zbioru n-elementowego $\{1, 2, \ldots, n\}$.* $\square$

Przykład 6.18. Podamy ilustrację zastosowania dowodu twierdzenia Cayley'a do wyznaczenia zanurzenia grupy Kleina w grupę S_4. Z tabelki grupy Kleina odczytujemy na podstawie kolejnych jej kolumn postacie lewostronnych mnożeń l_g dla $g \in K$:

$e \mapsto \begin{pmatrix} e & S_a & S_b & S_O \\ e & S_a & S_b & S_O \end{pmatrix}$, $S_a \mapsto \begin{pmatrix} e & S_a & S_b & S_O \\ S_a & e & S_O & S_b \end{pmatrix}$, $S_b \mapsto \begin{pmatrix} e & S_a & S_b & S_O \\ S_b & S_O & e & S_a \end{pmatrix}$,

$S_O \mapsto \begin{pmatrix} e & S_a & S_b & S_O \\ S_O & S_b & S_a & e \end{pmatrix}$. Następnie wykorzystujemy bijekcję zbioru K na zbiór $\{1, 2, 3, 4\}$: $e \mapsto 1$, $S_a \mapsto 2$, $S_b \mapsto 3$, $S_O \mapsto 4$ i na mocy Przykładu 6.15 oraz tego, że złożenie zanurzeń jest zanurzeniem, otrzymujemy następujące zanurzenie grupy K w grupę S_4:

$e \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $S_a \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1,2) \circ (3,4)$,

$S_b \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1,3) \circ (2,4)$, $S_O \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1,4) \circ (3,4)$.

W szczególności mamy stąd, że $V = \{e, (1,2) \circ (3,4), (1,3) \circ (2,4), (1,4) \circ (2,3)\}$ jest podgrupą grupy S_4 i $V \cong K$.

Twierdzenie 6.19. *Wszystkimi z dokładnością do izomorfizmu grupami rzędu 6 są: $\mathbb{Z}_6^+$ i D_3.*

Dowód. Grupy $\mathbb{Z}_6^+$ i D_3 nie są izomorficzne, bo pierwsza z nich jest abelowa, a druga nie jest abelowa.

Niech G będzie grupą rzędu 6. Z Zagadki 5 z Wykładu 3 istnieje w G element a rzędu 2. Jeśli w G nie ma elementu rzędu 3, to G nie może być cykliczna, gdyż w grupie

cyklicznej rzędu 6 o generatorze u element u^2 ma rząd 3. Zatem każdy element zbioru $G \setminus \{e\}$ ma rząd 2 i $x^2 = e$ dla każdego $x \in G$. Zatem ze Stwierdzenia 2.18 grupa G jest abelowa. Istnieje zatem $v \in G \setminus \{e, a\}$ i wtedy $\{e, a, v, a \cdot v\}$ jest podgrupą rzędu 4 w grupie G, bo $a \cdot v = v \cdot a$, gdyż grupa G jest abelowa. Ale $4 \not| 6$, więc mamy sprzeczność z twierdzeniem Lagrange'a. Zatem w grupie G istnieje element b rzędu 3.

Załóżmy, że $a \cdot b = b \cdot a$. Wtedy ze Stwierdzenia 3.6, $o(a \cdot b) = 6$, więc $G = \langle a \cdot b \rangle$ i na mocy Twierdzenia 6.7, $G \cong \mathbb{Z}_6^+$.

Teraz załóżmy, że $a \cdot b \neq b \cdot a$. Ponieważ $o(b) = 3$, więc z Uwagi 3.4, $H = \langle b \rangle$ jest podgrupą rzędu 3 grupy G i $|G| = 6$, więc $(G : H) = 2$, skąd na mocy Stwierdzenia 4.14, $H \lhd G$. Dalej, ze Stwierdzenia 2.16, $H = \{e, b, b^2\}$. Ale $a^{-1} = a$, więc $a \cdot b \cdot a \in \langle b \rangle$ oraz $a \cdot b \cdot a \neq b$ i $a \cdot b \cdot a \neq e$, więc $a \cdot b \cdot a = b^2$, skąd $b \cdot a = a \cdot b^2$ i $b^2 \cdot a = a \cdot b$. Stąd wynika, że elementy: e, a, b, b^2, $a \cdot b$, $a \cdot b^2$, są parami różne, a ponieważ $|G| = 6$, więc $G = \{e, a, a \cdot b, a \cdot b^2, b, b^2\}$. Ponadto z naszych rozważań wynika, że tabelka działania $\cdot$ w grupie G wygląda następująco:

$\cdot$	e	a	$a \cdot b$	$a \cdot b^2$	b	b^2
e	e	a	$a \cdot b$	$a \cdot b^2$	b	b^2
a	a	e	b	b^2	$a \cdot b$	$a \cdot b^2$
$a \cdot b$	$a \cdot b$	b^2	e	b	$a \cdot b^2$	a
$a \cdot b^2$	$a \cdot b^2$	b	b^2	e	a	$a \cdot b$
b	b	$a \cdot b^2$	a	$a \cdot b$	b^2	e
b^2	b^2	$a \cdot b$	$a \cdot b^2$	a	e	b

Niech $f\colon D_3 \to G$ będzie bijekcją taką, że $f(e) = e$, $f(S_a) = a$, $f(S_b) = a \cdot b$, $f(S_c) = a \cdot b^2$, $f(O_1) = b$, $f(O_2) = b^2$. Wtedy tabelka grupy D_3 przejdzie na tabelkę grupy G, więc na mocy Uwagi 5.20, f jest izomorfizmem, czyli $G \cong D_3$. $\square$

Przykład 6.20. Udowodnimy, że dla dowolnego ciała K istnieje epimorfizm $f\colon GL_n(K) \to K^*$. Niech $f(A) = \det(A)$ dla $A \in GL_n(K)$. Z algebry liniowej wynika, że f jest odwzorowaniem w zbiór K^*. Natomiast z twierdzenia Cauchy'ego wynika, że f jest homomorfizmem grup. Dla dowolnego $a \in K^*$ niech X_a oznacza macierz kwadratową stopnia n, która jest diagonalna i na głównej przekątnej ma elementy $a, 1, \ldots, 1$. Wtedy $\det(X_a) = a \cdot 1 \cdot \ldots \cdot 1 = a$, więc $a = f(X_a)$. Zatem funkcja f jest "na" i f jest epimorfizmem.

Zauważmy jeszcze, że $Ker(f) = SL_n(K)$. Zatem z twierdzenia o izomorfizmie mamy, że $GL_n(K)/SL_n(K) \cong K^*$.

Zagadka 1. Udowodnij, że grupy D_4 i Q_8 nie są izomorficzne.

Zagadka 2. Udowodnij, że $UT_3(\mathbb{Z}_2) \cong D_4$.

Zagadka 3. Udowodnij, że zbiór $Aut(G)$ wszystkich automorfizmów grupy G tworzy

grupę ze względu na składanie przekształceń. Uzasadnij też, że zbiór $Inn(G)$ wszystkich automorfizmów wewnętrznych grupy G jest podgrupą grupy $Aut(G)$.

Zagadka 4. Udowodnij, że grupa D_4 zanurza się w grupę S_4.

Zagadka 5. Niech a i b będą różnymi elementami rzędu 2 w grupie G, przy czym $a \cdot b = b \cdot a$. Uzasadnij, że istnieje dokładnie jeden homomorfizm grup $f\colon Q_8 \to G$ taki, że $f(i) = a$, $f(k) = b$ i podaj obrazy pozostałych elementów grupy Q_8.

Zagadka 6. Niech X będzie niepustym zbiorem generatorów grupy G i niech f, g będą homomorfizmami określonymi na grupie G w grupę A takimi, że $f(x) = g(x)$ dla każdego $x \in X$. Udowodnij, że wówczas $f = g$.

Zagadka 7. Wyznacz wszystkie homomorfizmy grupy $\mathbb{Q}^+$ w grupę $\mathbb{Q}^*$.