opracował Maciej Grzesiak

Grupy

1. Określenie i przykłady grup

Definicja 1. Zbiór G z określonym na nim działaniem dwuargumentowym $\circ$ nazywamy *grupą*, gdy:

G1. $\forall_{x,y,z\in G}\ \ (x\circ y)\circ z = x\circ(y\circ z)$;

G2. $\exists_{e\in G}\ \ \forall_{x\in G}\ \ e\circ x = x\circ e = x$;

G3. $\forall_{x\in G}\ \ \exists_{x^{-1}\in G}\ \ x\circ x^{-1} = x^{-1}\circ x = e$.

Ponieważ działanie jest łączne, więc $(ab)c = a(bc)$ można pisać po prostu jako abc. Z tego samego powodu iloczyn $a_1a_2\ldots a_n$ można pisać bez nawiasów (ale nie można zmieniać kolejności). Jeśli $a_1 = a_2 = \ldots = a_n$, to taki iloczyn nazywamy $n-$tą potęgą i oznaczamy a^n. Określamy ponadto $a^0 = e$, $a^{-n} = (a^n)^{-1}$ lub $a^{-n} = (a^{-1})^n$.
Ćwiczenie. Wykazać, że dla $a \in G$, $m, n \in \mathbb{Z}$ $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

Jeśli $a^n = e$ dla pewnego $n > 0$, to najmniejszą z liczb o tej własności nazywamy *rzędem elementu* a i oznaczamy $|a|$. Jeśli $a^n \neq e$ dla każdego $n > 0$, to $|a| = \infty$.
Jeśli grupa ma skończoną liczbę elementów, to nazywamy ją *grupą skończoną*. Liczbę elementów grupy nazywamy *rzędem grupy*; oznaczenie: $|G|$.
Ćwiczenie. Jeśli $a^n = e$, to n dzieli się przez $|a|$.

Jeżeli G spełnia oprócz G1—G3 jeszcze:

G4. $\forall_{x,y\in G}\ \ x\circ y = y\circ x$,

to nazywamy ją *grupą abelową*.
Tradycyjnie działanie w grupie abelowej oznaczamy $+$ i stosujemy następującą terminologię:

$\cdot$	$+$
mnożenie	dodawanie
iloczyn	suma
jedynka	zero
odwrotny	przeciwny
potęga	krotność
e lub 1	0
a^{-1}	$-a$
a^n	na

Przykłady.

1. Zbiór elementów dowolnego ciała rozpatrywany z dodawaniem tworzy grupę abelową, np. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

2. Zbiór elementów niezerowych dowolnego ciała rozpatrywany z mnożeniem tworzy grupę abelową, np. $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$.

3. Zbiór $\mathbb{Z}$ z dodawaniem tworzy grupę abelową.

4. Zbiór $\mathbb{Z}_n$ reszt z dzielenia przez n z działaniem dodawania modulo n tworzy grupę abelową. Jest to grupa skończona rzędu n.

5. $\mathbb{Q}_p = \{\frac{m}{p^n} | m, n \in \mathbb{Z}\}$, gdzie p jest liczbą pierwszą, jest addytywną grupą abelową.

6. Zbiór $\mathbb{C}_n$ pierwiastków stopnia n z 1 jest grupą multiplikatywną skończoną rzędu n.

Przypomnienie. Pierwiastkami stopnia n z 1 są liczby

$$\varepsilon_k = \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n}, \qquad k = 0, 1, \ldots, n-1.$$

Można je zapisać w postaci wykładniczej:

$$\varepsilon_k = \mathrm{e}^{\mathrm{i}\,\frac{2k\pi}{n}}, \qquad k = 0, 1, \ldots, n-1$$

7. Niech Ω będzie zbiorem, a $S(\Omega)$ niech oznacza zbiór odwzorowań odwracalnych $\Omega \longrightarrow \Omega$. Zbiór $S(\Omega)$ z działaniem składania tworzy grupę.

8. W szczególności, gdy $\Omega = \{1, 2, \ldots, n\}$,to $S(\Omega)$ jest grupą permutacji n -elementowych. Nazywamy ją *grupą symetryczną* i oznaczamy S_n. Grupa S_n jest skończona; $|S_n| = n!$. Dla $n > 2$ grupy S_n są nieabelowe.

9. Niech $\mathbb{K}$ będzie dowolnym ciałem. Zbiór macierzy nieosobliwych o wyrazach z $\mathbb{K}$ z działaniem mnożenia macierzy jest grupą. Oznaczamy ją $\mathbf{GL}(n, K)$ lub $\mathbf{GL}_n(K)$ i nazywamy *pełną grupą liniową*. Jedynką tej grupy jest macierz jednostkowa; elementem odwrotnym do macierzy $\mathbf{A}$ jest macierz odwrotna $\mathbf{A}^{-1}$.
W $\mathbf{GL}_n(K)$ można rozpatrywać następujące podzbiory:
a) $\mathbf{SL}_n(K) = \{\mathbf{A} \in \mathbf{GL}_n(K) : \det \mathbf{A} = 1\}$;
b) $\mathbf{D}_n(K) = \{\mathbf{A} \in \mathbf{GL}_n(K) : \mathbf{A}$ jest diagonalna$\}$;
c) $\mathbf{T}_n(K) = \{\mathbf{A} \in \mathbf{GL}_n(K) : \mathbf{A}$ jest górnotrójkątna$\}$;
d) $\mathbf{UT}_n(K) = \{\mathbf{A} \in \mathbf{T}_n(K) : \mathbf{A}$ ma jedynki na przekątnej $\}$.
Wszystkie te podzbiory sa podgrupami, i noszą nazwy: *specjalna grupa liniowa, grupa diagonalna, grupa trójkątna, grupa unitrójkątna.*
Uwaga. Rozpatruje się również struktury uboższe (tzn. mające mniej aksjomatów) od grupy.

Definicja 2. Zbiór G z określonym na nim działaniem dwuargumentowym $\circ$ nazywamy *półgrupą*, gdy działanie to jest łączne, tj.

$$\forall_{x,y,z\in G} \;\; (x \circ y) \circ z = x \circ (y \circ z).$$

Pojęcie półgrupy okazało się bardzo użyteczne, np. w teorii automatów.

2. Podgrupy

Jeśli podzbiór H grupy G jest zamknięty ze względu na mnożenie (tj. $a, b \in H \Rightarrow ab \in H$), to ograniczenie operacji mnożenia do H jest działaniem na H. Jeżeli względem tego działania H jest grupą, to mówimy, że H *jest podgrupą* G i oznaczamy $H \leqslant G$. Jeśli $H \leqslant G$ i $H \neq G$, to piszemy $H < G$.

Lemat 1. *Następujące warunki są równoważne:*
a) $H \leqslant G$;
b) $\forall_{a,b\in H} \;\; ab^{-1} \in H$;
c) $\forall_{a,b\in H} \;\; ab \in H \wedge a^{-1} \in H$.

Warunki te można zapisać inaczej stosując pojęcie *iloczynu kompleksowego* podzbiorów grupy G:

$$AB \stackrel{\text{def}}{=} \{ab : a \in A, b \in B\}$$

i przyjmując:

$$A^{-1} \stackrel{\text{def}}{=} \{a^{-1} : \; a \in A\}$$

dla $A \subseteq G$ i $B \subseteq G$.

Lemat 2. *Następujące warunki są równoważne:*
a) $H < G$;
b) $HH \subseteq H \;\; \wedge \;\; H^{-1} \subseteq H$.

Przykłady. 1. $\mathbb{Z} < \mathbb{Q}_p < \mathbb{Q} < \mathbb{R} < \mathbb{C}$. Zauważmy, że $\mathbb{Z} = \bigcap \mathbb{Q}_p$. 2. $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$.

3. $\mathbb{C}_p < \mathbb{C}_{p^2} < \ldots < \mathbb{C}_{p^\infty}$. Ponadto $\mathbb{C}_{p^\infty} = \bigcup \mathbb{C}_{p^n}$. 4. Dla $n \geqslant 2$: $\mathbf{SL}_n(K) < \mathbf{GL}_n(K)$,

$\mathbf{D}_n(K) < \mathbf{T}_n(K)$,

$$\mathbf{UT}_n(K) \ < \ \mathbf{T}_n(K) \ < \ \mathbf{GL}_n(K).$$

3. Iloczyny proste grup

Niech G, H będą dowolnymi grupami. Wtedy w zbiorze $G \times H$ można określić działanie wzorem:

$$(g, h) \circ (g', h') = (gg', hh')$$

dla dowolnych $(g, g'), (h, h')$ ze zbioru $G \times H$. Zbiór $G \times H$ z tym działaniem tworzy grupę, której elementem neutralnym jest (e_G, e_H). Nazywamy ją *iloczynem prostym* grup G i H. Zbiory $G' = \{(g, e_H) : \ g \in G\}$ i $H' = \{(e_G, h) : \ h \in H\}$ są podgrupami grupy $G \times H$. Są one izomorficzne [1] odpowiednio z G i H.
U w a g a. W przypadku grup abelowych mówimy raczej: *suma prosta* grup.

4. Zbiory generujące

Jasne jest, że przekrój dowolnego zbioru podgrup danej grupy jest także podgrupą.
Niech M — dowolny podzbiór grupy G. Przekrój (M) wszystkich podgrup grupy G zawierających M nazywamy *podgrupą generowaną przez* M, a zbiór M *zbiorem generatorów* dla (M). Grupę mającą skończony zbiór generatorów nazywamy *skończenie generowaną*.

Twierdzenie 1. *Jeśli M jest podzbiorem grupy G, to*

$$(M) = \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_m^{\varepsilon_m} : \ a_i \in M, \varepsilon_i = \pm 1, m = 1, 2, \ldots\}.$$

D o w ó d. Oznaczmy prawą część przez H. Ponieważ (M) zawiera wszystkie $a_i \in M$, więc $(M) \supseteq H$. Z drugiej strony, jeśli $x, y \in H$, to $xy^{-1} \in H$, więc H jest podgrupą, oczywiście zawierającą M. Stąd $H \supseteq (M)$ i w końcu $H = (M)$. ■
Przykłady. Uwaga: jeśli zbiór M określony jest w postaci $M = \{\ldots : \ \ldots\}$, to będziemy pisać $(\ldots : \ \ldots)$ zamiast $(\{\ldots : \ \ldots\})$.

1. $\mathbb{Z} = (1)$.

2. $\mathbb{Z}_n = (1 (\mathrm{mod} n))$.

3. $\mathbb{Q} = (\frac{1}{n} : \ n = 1, 2, \ldots)$.

4. $\mathbb{Q}^* = (-1, 2, 3, 5, 7, 11, \ldots)$.

5. $\mathbb{C}_n = (\varepsilon_n), \varepsilon_n = \cos \frac{2\pi}{n} + \mathrm{i} \sin \frac{2\pi}{n} = \mathrm{e}^{\mathrm{i} \frac{2\pi}{n}}$.

6. $\mathbb{C}_{p^\infty} = (\varepsilon_{p^m} : \ m = 1, 2, \ldots)$.

5. Funkcja Eulera

Definicja 3. Funkcję φ Eulera przyporządkowuje każdej liczbie naturalnej liczbę liczb względnie z nią pierwszych nie większych od niej samej.

Przykład. Początkowe wartości funkcji Eulera:

[1] Definicja izomorfizmu w podrozdziale 7

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Funkcja Eulera odgrywa dużą rolę w teorii liczb. Ma też istotne zastosowania w kryptografii w badaniach nad złożonością szyfrów.

Własności funkcji φ.

1. Dla dowolnej liczby pierwszej p i $k \in \mathbb{N}$ jest $\varphi(p^k) = p^k - p^{k-1}$; w szczególności $\varphi(p) = p-1$.
2. Jeżeli liczby całkowite m, n są względnie pierwsze, to $\varphi(mn) = \varphi(m)\varphi(n)$.
3. Jeżeli n nie ma wielokrotnych dzielników pierwszych, tj. $n = p_1 p_2 \dots p_k$ gdzie liczby p_i są pierwsze i parami różne ($i = 1, \dots, k$), to
$$\varphi(n) = (p_1 - 1)(p_2 - 1)\dots(p_k - 1).$$
4. Dla dowolnej liczby całkowitej n zachodzi: $\sum_{m|n} \varphi(m) = n$ (sumowanie przebiega wszystkie dzielniki liczby n).
5. Jeżeli $n = \prod_{i=1}^{k} p_i^{k_i}$ jest rozkładem liczby n na czynniki pierwsze to
$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{k_i})$$

Z tych własności wynika też wzór

$$\varphi(n) = n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right)\dots\left(1 - \tfrac{1}{p_k}\right),$$

gdzie $p_1, p_2, \dots, p_k$ są wszystkimi czynnikami pierwszymi liczby n liczonymi bez powtórzeń.

Ostatni wzór można wyprowadzić bezpośrednio z zasady włączania-wyłączania.

Twierdzenie 2. (zasada włączania-wyłączania) *Niech $|S|$ oznacza liczbę elementów zbioru S. Jeżeli $A_1, A_2, \dots, A_r$ są zbiorami skończonymi, to*

$$\begin{aligned} |\textstyle\bigcup_{i=1}^{r} A_i| &= \textstyle\sum_{i=1}^{r} |A_i| - \sum_{\substack{i,j=1 \\ i\neq j}}^{r} |A_i \cap A_j| + \\ &+ \textstyle\sum_{\substack{i,j,k=1 \\ i\neq j, i\neq k, j\neq k}}^{r} |A_i \cap A_j \cap A_k| + \dots + (-1)^{r-1} |A_1 \cap A_2 \cap \dots \cap A_r|. \end{aligned}$$

Załóżmy, że liczba n ma następujący rozkład na czynniki pierwsze:

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}.$$

i niech A_i będzie zbiorem wszystkich liczb $m \in \{1, 2, \dots, n\}$ takich, że p_i dzieli m. Można wykazać, że

$$|A_i| = \frac{n}{p_i},\ |A_i \cap A_j| = \frac{n}{p_i p_j} \text{ dla } i \neq j,$$

$$|A_i \cap A_j \cap A_k| = \frac{n}{p_i p_j p_k} \text{ dla różnych } i, j, k,$$

itd. Ponieważ $\varphi(n) = n - |\bigcup_{i=1}^{r} A_i|$, więc stosując zasadę włączania-wyłączania i powyższe równości otrzymujemy:

$$\begin{aligned} \varphi(n) &= n - \textstyle\sum \frac{n}{p_i} + \sum \frac{n}{p_i p_j} - \sum \frac{n}{p_i p_j p_k} + \dots = \\ &= n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right)\dots\left(1 - \tfrac{1}{p_k}\right) \end{aligned}$$

6. Podgrupy cykliczne

Podgrupa (a) generowana przez jeden element a nazywa się *cykliczną*. Z twierdzenia o podgrupie generowanej przez zbiór wynika, że

$$(a) = \{a^n :\ n = 0, \pm 1, \pm 2, \dots\}.$$

Dwa pierwsze przykłady wyżej pokazują, że $\mathbb{Z}$ i $\mathbb{Z}_n$ są grupami cyklicznymi.

Twierdzenie 3. *(i) Każda podgrupa grupy cyklicznej jest cykliczna;*

(ii) Niech (a) będzie grupą cykliczną rzędu n. Element a^k generuje podgrupę rzędu $\frac{n}{\mathrm{nwd}(k,n)}$;

(iii) Niech (a) będzie grupą cykliczną rzędu n a l – dodatnim dzielnikiem liczby n. Wtedy (a) zawiera $\varphi(l)$ elementów rzędu l;

(iv) Grupa cykliczna rzędu n zawiera $\varphi(n)$ generatorów. Generatorami są te i tylko te elementy a^r dla których $\mathrm{nwd}(r,n)=1$.

Dowód (i) (dla grupy skończonej). Niech (a) będzie cykliczną grupą rzędu n, $H \neq \{e\}$ jej podgrupą. Niech m będzie najmniejszą liczbą całkowitą o własności:

$$a^m \in H, \;\; 0 < m < n.$$

Oczywiście $(a^m) \subseteq H$. Wykażemy, że naprawdę $(a^m) = H$. Weźmy dowolny element z H; musi on mieć postać $a^k, 0 \leqslant k < n$. Podzielmy k przez m: $k = mq + r, 0 \leqslant r < m$. Wtedy

$$a^r = a^k (a^m)^{-q} \in H.$$

Ze sposobu wyboru liczby m wynika, że $r = 0$, a więc $a^k \in (a^m)$. Dla grupy nieskończonej dowód jest analogiczny.
Dowód (iii). Niech $n = dl$. Na mocy (ii) $|a^k| = l$ wtedy, i tylko wtedy, gdy $\mathrm{nwd}(k,n) = d$. Zatem liczba elementów rzędu l jest liczbą tych $k \leqslant n$, że $\mathrm{nwd}(k,n) = d$. Ale gdy $k = dh$, to $\mathrm{nwd}(k,n) = d \Leftrightarrow \mathrm{nwd}(dh, dl) = d \Leftrightarrow \mathrm{nwd}(h,l) = 1$. ■
Przykład. Rozważmy grupę $\mathbb{C}_n$ pierwiastków stopnia n z 1, generowaną przez $\varepsilon_1 = \mathrm{e}^{\mathrm{i}\,\frac{2\pi}{n}}$. Przykładowo weźmy $n = 12$; wtedy generatorem jest liczba $\mathrm{e}^{\mathrm{i}\,\frac{\pi}{6}}$. Grupa ma 12 elementów:

$$\mathbb{C}_{12} = \{\mathrm{e}^{\mathrm{i}\,k\pi/6} : \; k = 0, 1, 2, \ldots, 11\}.$$

Dzielnikami 12 są 1, 2, 3, 4, 6, 12.
W tabeli niżej podane są te dzielniki l, wartości $\varphi(l)$, i elementy rzędu l (czyli generatory podgrupy rzędu l).

l	1	2	3	4	6	12
$\varphi(l)$	1	1	2	2	2	4
elem. rzędu l	1	-1	$\mathrm{e}^{\mathrm{i}\,\frac{2\pi}{3}}, \mathrm{e}^{\mathrm{i}\,\frac{4\pi}{3}}$	$\mathrm{e}^{\mathrm{i}\,\frac{\pi}{2}}, \mathrm{e}^{\mathrm{i}\,\frac{3\pi}{2}}$	$\mathrm{e}^{\mathrm{i}\,\frac{\pi}{3}}, \mathrm{e}^{\mathrm{i}\,\frac{5\pi}{3}}$	$\mathrm{e}^{\mathrm{i}\,\frac{\pi}{6}}, \mathrm{e}^{\mathrm{i}\,\frac{5\pi}{6}}, \mathrm{e}^{\mathrm{i}\,\frac{7\pi}{6}}, \mathrm{e}^{\mathrm{i}\,\frac{11\pi}{6}}$

Przykład. Jak wiadomo, mnożenie przez liczbę $\mathrm{e}^{\mathrm{i}\,\varphi}$ można interpretować jako obrót płaszczyzny zespolonej o kąt φ. Grupę $\mathbb{C}_n$ możemy więc zastąpić grupą O_n obrotów płaszczyzny, generowaną przez obrót $o_{2\pi/n}$. Poprzedni przykład "transponujemy" następująco: dla $n = 12$ generatorem grupy obrotów jest obrót o kąt $\frac{\pi}{6}$. Grupa ma 12 elementów:

$$O_{12} = \{o_{k\pi/6} : \; k = 0, 1, 2, \ldots, 11\}.$$

Dzielnikami 12 są 1, 2 ,3, 4, 6, 12.

l	1	2	3	4	6	12
$\varphi(l)$	1	1	2	2	2	4
obroty	id	o_π	$o_{2\pi/3}, o_{4\pi/3}$	$o_{\pi/2}, o_{3\pi/2}$	$o_{\pi/3}, o_{5\pi/3}$	$o_{\pi/6}, o_{5\pi/6}, o_{7\pi/6}, o_{11\pi/6}$

Twierdzenie 4. (podstawowe teorii grup abelowych) *Jeżeli G jest grupą abelową generowaną przez skończenie wiele elementów, to G jest sumą prostą grup cyklicznych.*

Wniosek 1. *Każda skończona grupa abelowa jest sumą prostą grup cyklicznych postaci C_{p^r}, gdzie p jest liczbą pierwszą, a $r \in \mathbb{N}$.*

7. Homomorfizmy

Niech G, G' będą grupami. Odwzorowanie $f : G \longrightarrow G'$ nazywamy *homomorfizmem*, gdy dla dowolnych $a, b \in G$ spełniony jest warunek:

$$f(ab) = f(a)f(b).$$

Homomorfizm różnowartościowy nazywamy *monomorfizmem*; jeżeli obrazem G jest cała G', to mówimy o *epimorfizmie*. Homomorfizm, który jest monomorfizmem i epimorfizmem nazywamy *izomorfizmem*. Jeśli $G = G'$, to homomorfizm nazywamy *endomorfizmem*; endomorfizm, który jest izomorfizmem, nazywamy *automorfizmem*.
Jeżeli istnieje izomorfizm $f : G \longrightarrow G'$, to grupy G i G' nazywamy *izomorficznymi*; piszemy wtedy $G \cong G'$.
Przykłady. 1. Odwzorowanie $\mathbb{Z} \longrightarrow \mathbb{Z}_n$ przyporządkowujące liczbie jej resztę z dzielenia przez n jest epimorfizmem. 2. $\ln : \mathbb{R}^+ \longrightarrow \mathbb{R}^*$ oraz $\exp : \mathbb{R}^* \longrightarrow \mathbb{R}^+$ są izomorfizmami. 3. $\det : \mathbb{G}L_n(K) \longrightarrow K^*$ jest epimorfizmem. 4. $f : \mathbb{Z}_n \to O_n$, $f(k) = o_{2k\pi/n}$. Z każdym

homomorfizmem grup $f : G \longrightarrow G'$ związane są dwie podgrupy: *jądro* $\ker f \subseteq G$ i *obraz* $\operatorname{im} f \subseteq G'$:

$$\ker f = \{x \in G : \ f(x) = e\};$$

$$\operatorname{im} f = \{y \in G' : \ \exists_{x \in G} \ f(x) = y\}.$$

Sprawdzimy, że są to rzeczywiście podgrupy.
Jeśli $a, b \in \ker f$, to $f(ab^{-1}) = f(a)f(b)^{-1} = ee = e$, zatem $ab^{-1} \in \ker f$.
Jeśli $c, d \in \operatorname{im} f$, to istnieją $a, b \in G$ takie, że $c = f(a)$, $d = f(b)$. Zatem $cd^{-1} = f(a)f(b)^{-1} = f(ab^{-1})$, więc $cd^{-1} \in \operatorname{im} f$.
Warto także zauważyć, że $ab^{-1} \in \ker f \Leftrightarrow f(ab^{-1}) = e \Leftrightarrow f(a) = f(b)$. Zatem jeżeli f jest monomorfizmem, to $a \in \ker f \Rightarrow ae^{-1} \in \ker f \Leftrightarrow f(a) = f(e) \Rightarrow a = e$, więc $\ker f = e$. Odwrotnie, jeśli $\ker f = \{e\}$, to $f(a) = f(b) \Leftrightarrow ab^{-1} \in \ker f \Rightarrow ab^{-1} = e \Leftrightarrow a = b$. Wykazaliśmy więc, że homomorfizm jest monomorfizmem wtedy i tylko wtedy, gdy ma jądro jednoelementowe.

8. Grupa symetryczna S_n

Zajmiemy się bardziej szczegółowo grupą S_n permutacji n-elementowych. Permutacje oznaczać będziemy małymi literami greckimi (wyjątek — permutacja tożamościowa e).
Permutację $\pi : i \mapsto \pi(i)$, $i = 1, 2, \ldots, n$ zapisuje się w dwóch rzędach:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

podając wszystkie wartości przekształcenia π:

$$\begin{array}{cccc} 1 & 2 & \ldots & n \\ \downarrow & \downarrow & \cdots & \downarrow \\ i_1 & i_2 & \ldots & i_n \end{array} .$$

Permutacje mnoży się zgodnie z prawem składania przekształceń.
Jeżeli $\sigma, \tau \in S_n$, to $(\sigma\tau)(i) = \sigma(\tau(i))$. Np. dla

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

mamy

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 2 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

Zauważmy, że

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

więc $\sigma\tau \neq \tau\sigma$. Jak wiadomo, istnieje $n!$ permutacji n-elementowych, więc $|S_n| = n!$.
Grupy permutacji stanowią uniwersalny przykład grup skończonych.

Twierdzenie 5. (Cayleya) *Każda grupa skończona jest izomorficzna z pewną grupą permutacji.*

D o w ó d. Niech G będzie grupą, $|G| = n$. Określimy odwzorowanie $\Gamma : G \to S(G)$ wzorem $\Gamma(g) = \gamma$, gdzie

$$\gamma = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix} \in S(G).$$

γ jest oczywiście permutacją. Sprawdzimy, że Γ jest izomorfizmem. Ponieważ dla $x \in G$, $\Gamma(x)(g) = xg$, więc

$$\begin{aligned} \Gamma(ab)(g) &= (ab)g = a(bg) = a(\Gamma(b)g) = \Gamma(a)\left(\Gamma(b)(g)\right) = \\ &= \left(\Gamma(a) \circ \Gamma(b)\right)(g) \end{aligned}$$

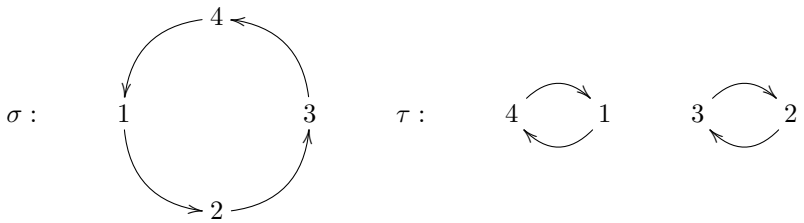
czyli $\Gamma(ab) = \Gamma(a) \circ \Gamma(b)$.
Odwzorowanie Γ jest różnowartościowe, bo jeśli $\Gamma(a) = e$, to

$$a = ae_G = \Gamma(a)(e_G) = e(e_G) = e_G,$$

więc $a = e_G$. Zatem Γ ma jądro jednoelementowe, czyli jest monomorfizmem. ■
Prawdziwe jest także poniższe twierdzenie.

Twierdzenie 6. (uogólnione twierdzenie Cayleya) *Każda grupa jest izomorficzna z grupą odwzorowań wzajemnie jednoznacznych ("permutacji nieskończonych") pewnego zbioru na siebie.*

Permutacje z S_n można rozłożyć na iloczyn prostszych permutacji. Zauważmy np., że dla powyższych σ i τ można narysować grafy:



Naturalne będzie więc nazwanie permutacji σ *cyklem* o długości 4, a permutacji τ — iloczynem dwóch *rozłącznych* cykli długości 2.
Ogólniej, mówimy, że elementy i, j są π-równoważne, jeśli $j = \pi^s(i)$ dla pewnego $s \in \mathbb{Z}$ (π^s oznacza s-krotne złożenie permutacji π). Tak zdefiniowana relacja jest relacją równoważności (sprawdzić!).
Następujące twierdzenie mówi o tym, że relacja równoważności wyznacza podział zbioru na klasy rozłączne.

Twierdzenie 7. (zasada abstrakcji) *Niech X będzie zbiorem, a ρ relacją równoważności w X. Dla $x \in X$ niech $[x] = \{y \in X : \ x \sim y\}$ oznacza zbiór wszystkich elementów równoważnych z x. Wtedy dla dowolnych $x, y \in X$:*

1) $x \in [y] \Leftrightarrow x \sim y$.
2) $[x] = [y] \Leftrightarrow x \sim y$.
3) $X = \bigcup_{x \in X} [x]$.
4) $[x] \cap [y] \neq \emptyset \Leftrightarrow [x] = [y]$.

Zgodnie z zasadą abstrakcji uzyskujemy rozbicie zbioru $\Omega = \{1, 2, \ldots, n\}$

$$\Omega = \Omega_1 \cup \cdots \cup \Omega_p \tag{1}$$

na rozłączne klasy $\Omega_1, \ldots, \Omega_p$, zwane π-*orbitami*. Każdy element $i \in \Omega$ należy więc do dokładnie jednej orbity. Liczbę $l_k = |\Omega_k|$ nazywamy *długością* orbity Ω_k. Jeśli $i \in \Omega_k$, to $\Omega_k = \{i, \pi(i), \ldots, \pi^{l_k - 1}(i)\}$.
Permutację

$$\pi_k = \begin{pmatrix} i & \pi(i) & \ldots & \pi^{l_k-2}(i) & \pi^{l_k-1}(i) \\ \pi(i) & \pi^2(i) & \ldots & \pi^{l_k-1}(i) & i \end{pmatrix}$$

nazywamy *cyklem długości* l_k. Cykle będziemy zapisywać w postaci jednego wiersza:

$$\pi_k = \begin{pmatrix} i & \pi(i) & \ldots & \pi^{l_k-2}(i) & \pi^{l_k-1}(i) \end{pmatrix}.$$

Elementy te można oddzielać przecinkami lub nie.
Cykl π_k pozostawia na miejscu wszystkie elementy zbioru $\Omega \setminus \Omega_k$. Dlatego też uzasadnione jest nazywanie cykli π_s i π_t dla $s \neq t$ cyklami *rozłącznymi*.
Z rozbiciem zbioru (1) wiąże się zatem rozkład permutacji π na iloczyn

$$\pi = \pi_1 \pi_2 \cdots \pi_p, \tag{2}$$

w którym wszystkie cykle π_k są ze sobą przemienne.
W zapisie tym zwykle pomijamy cykle o długości 1, np.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} \in S_8 \tag{3}$$

można zapisać:

$$\pi = (1\,2\,3\,4\,5)(6\,7)(8) = (1\,2\,3\,4\,5)(6\,7).$$

Twierdzenie 8. *Każdą permutację $\pi \neq e$ w S_n można przedstawić w postaci iloczynu cykli rozłącznych o długości większej lub równej 2. Rozkład taki jest jednoznaczny z dokładnością do kolejności czynników.*

Rozkład na cykle pozwala na łatwe znalezienie rzędu permutacji.

Wniosek 2. *Rząd permutacji $\pi \in S_n$ jest równy najmniejszej wspólnej wielokrotności długości cykli występujących w rozkładzie (2).*

D o w ó d. Niech $\pi = \pi_1 \pi_2 \cdots \pi_p$. Ponieważ cykle są ze sobą przemienne, więc

$$\pi^s = \pi_1^s \pi_2^s \cdots \pi_p^s, \quad s = 0, 1, 2, \ldots$$

Cykle $\pi_1 \pi_2 \ldots \pi_p$ są rozłączne (działają na różnych zbiorach $\Omega_1, \ldots, \Omega_p$), więc $\pi^q = e \Leftrightarrow \pi_k^q = e \quad \forall_{k=1,2,\ldots,p}$. Zatem q jest wspólną wielokrotnością rzędów cykli π_k, czyli wspólną wielokrotnością ich długości l_k. Rzędem π jest najmniejsza taka liczba q, czyli

$$|\pi| = \mathrm{NWW}(l_1, \ldots, l_p). \blacksquare$$

Np. rząd permutacji π danej wzorem (3) wynosi 10.
Przykład. Jaki jest maksymalny rząd elementów grupy S_8?

Rozpatrując możliwe rozbicia liczby 8 na sumy:

$$8 = 2+2+2+2, 8 = 3+5, 8 = 4+4, \ldots$$

dojdziemy do wniosku, że rzędami elementów różnych od e w S_8 mogą być liczby 2,3,4,5,6,7,8,10,12,15.
Np. $\pi = (1\,2\,3\,4\,5)(6\,7\,8)$ jest rzędu 15.
Zwróćmy uwagę, że $|S_8| = 8! = 40320$.
Cykl długości 2 nazywamy *transpozycją*. Z twierdzenia 8 wynika poniższy wniosek.

Wniosek 3. *Każda permutacja $\pi \in S_n$ jest iloczynem pewnej liczby transpozycji.*

D o w ó d. Po pierwsze, $e = \tau^2$ dla dowolnej transpozycji τ. Po drugie, z twierdzenia 8 wynika, że wystarczy podać sposób rozkładu cyklu na transpozycje. Mamy np.:

$$(1\ 2\ \ldots\ l{-}1\ l) = (1\ l)(1\ l{-}1)\cdots(1\ 3)(1\ 2),$$

a ogólniej:

$$(a_1\ a_2\ \ldots\ a_{l-1}\ a_l) = (a_1\ a_l)(a_1\ a_{l-1})\cdots(a_1\ a_3)(a_1\ a_2).\square$$

Wniosek ten można wypowiedzieć inaczej:

Wniosek 4. *Transpozycje tworzą zbiór generatorów dla S_n.*

Oczywiście nie jest to minimalny zbiór generatorów, np.:

$$S_3 = (\ (1\ 2), (1\ 3), (2\ 3)\ ) = (\ (1\ 2), (1\ 3)\ ).$$

Twierdzenie 9. (o generatorach grupy S_n) *Następujące podzbiory są zbiorami generatorów grupy symetrycznej S_n:*

a) *wszystkie transpozycje elementów zbioru $\Omega = \{1, 2, \ldots, n\}$;*
b) $\{(1\ 2), (2\ 3), (3\ 4), \ldots, (n{-}1\ \ n)\}$;
c) $\{(1\ 2), (1\ 3), (1\ 4), \ldots, (1\ n)\}$;
d) $\{(1\ 2), (1\ 2\ 3 \ldots n)\}$.

D o w ó d. a) jest treścią poprzedniego wniosku.
b) Każdą transpozycję (ij), $1 \leqslant i < j \leqslant n$ można przedstawić w postaci:

$$(i\ j) = (i\ i{+}1)(i{+}1\ i{+}2)\cdots(j{-}1\ j)(j{-}2\ j{-}1)(j{-}3\ j{-}2)\cdots(i{+}1\ i{+}2)(i\ i{+}1).$$

Na mocy a) zbiór wszystkich permutacji generuje S_n, więc również zbiór transpozycji podany w b) ją generuje.
c) Teza wynika z równości $(i\ j) = (1\ i)(1\ j)(1\ i)$.
d) Niech $\alpha = (1\ \ 2)$, $\beta = (1\ \ 2 \ldots n)$. Wtedy mamy kolejno $\beta^{-1} = \beta^{n-1}$ (bo $\beta^n = e$), $(2\ 3) = \beta\alpha\beta^{-1}$, $(3\ 4) = \beta(2\ 3)\beta^{-1}$, $(4\ 5) = \beta(3\ 4)\beta^{-1}$, ..., $(n{-}1\ n) = \beta(n{-}2\ n{-}1)\beta^{-1}$. Na mocy b) zbiór $\{\alpha, \beta\}$ jest również zbiorem generatorów. ■
Warto także podkreślić, że rozkład permutacji na transpozycje nie jest jednoznaczny; więcej, różne rozkłady mogą mieć nawet różną liczbę czynników. Np. w S_4 mamy:

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 3)(1\ 3) = (1\ 3)(2\ 4)(1\ 2)(1\ 4).$$

Można jednak wykazać, że jeśli jakiś rozkład permutacji na transpozycje ma parzystą liczbę czynników, to każdy inny ma także parzystą liczbę czynników. Innymi słowy, liczba $\varepsilon_\pi = (-1)^k$, gdzie k jest liczbą transpozycji w dowolnym rozkładzie permutacji π, jest niezmiennikiem permutacji.
Dokładniej, można udowodnić kolejno poniższe lematy.

Lemat 3. *Niech $\pi \in S_n$, niech $\tau \in S_n$ będzie transpozycją. Liczby cykli występujących w rozkładach na cykle permutacji π i $\tau\pi$ różnią się o 1.*

Lemat 4. *Jeżeli permutacja tożsamościowa e jest przedstawiona w postaci iloczynu k transpozycji, np. $e = \tau_k\tau_{k-1}\cdots\tau_2\tau_1$, to liczba k jest parzysta.*

Korzystając z tych lematów można wykazać twierdzenie 10.

Twierdzenie 10. *Jeżeli $\pi \in S_n$ jest na dwa sposoby przedstawiona w postaci iloczynu transpozycji, to albo w obu przedstawieniach liczba czynników jest parzysta, albo w obu — nieparzysta.*

D o w ó d. Niech $\pi = \tau_k\tau_{k-1}\cdots\tau_2\tau_1 = \sigma_l\sigma_{l-1}\cdots\sigma_2\sigma_1$ będą dowolnymi przedstawieniami permutacji $\pi \in S_n$ w postaci iloczynu transpozycji. Wtedy:

$$\begin{aligned} e = \pi^{-1}\pi &= (\sigma_l\sigma_{l-1}\cdots\sigma_2\sigma_1)^{-1}(\tau_k\tau_{k-1}\cdots\tau_2\tau_1) = \\ &= \sigma_1^{-1}\sigma_2^{-1}\cdots\sigma_l^{-1}\tau_k\tau_{k-1}\cdots\tau_2\tau_1 = \\ &= \sigma_1\sigma_2\cdots\sigma_l\tau_k\tau_{k-1}\cdots\tau_2\tau_1 \end{aligned}$$

jest przedstawieniem permutacji tożsamościowej w postaci iloczynu $k+l$ transpozycji. Na mocy poprzedniego lematu $k+l$ jest liczbą parzystą, więc albo k, l są obie parzyste, lub obie nieparzyste. ■

Permutację $\pi \in S_n$ nazywamy *parzystą*, gdy $\varepsilon_\pi = 1$ i *nieparzystą*, gdy $\varepsilon_\pi = -1$. Tak więc wszystkie transpozycje są permutacjami nieparzystymi. Można wykazać, że wszystkie permutacje parzyste zbioru n-elementowego ($n \geqslant 2$) tworzą podgrupę A_n grupy S_n, rzędu $\frac{n!}{2}$. Jest to tzw. *grupa alternująca*.

Definicja 4. Dwie permutacje π_1 i π_2 nazywamy *podobnymi*, jeżeli w ich rozkładach na cykle występuje tyle samo cykli tej samej długości.

Przykład. Permutacje:

$$\pi_1 = (1)(2)(3\ 4\ 5)(6\ 7\ 8\ 9\ 10)\ ,\ \ \pi_2 = (1\ 2\ 3)(4)(5\ 6\ 7\ 8\ 9)(10)$$

są podobne. Nietrudno sprawdzić, że podobieństwo jest relacją równoważności w zbiorze S_n.

Definicja 5. Mówimy, że permutacja $\pi_1 \in S_n$ jest *sprzężona* z permutacją $\pi_2 \in S_n$ *względem pewnej grupy permutacji* $G \subseteq S_n$, jeśli istnieje element π grupy G taki, że $\pi\pi_1\pi^{-1} = \pi_2$.

Łatwo wykazać, że w zbiorze G sprzężenie względem G jest relacją równoważności.
Klasy abstrakcji relacji sprzężenia (względem grupy G) w zbiorze G nazywamy *klasami elementów sprzężonych* w grupie G.

Twierdzenie 11. *Dwie permutacje $\pi_1, \pi_2 \in S_n$ są sprzężone względem S_n wtedy i tylko wtedy, gdy są podobne.*

D o w ó d. ($\Rightarrow$) Najpierw przykład: w S_4 rozważmy permutację $\pi_1 = (132)$ i sprzężoną z nią $\pi_2 = (34)\pi_1(34)$. Wtedy $\pi_2 = (142)$ jest podobna do π_1.
Ogólnie: jeśli dany jest rozkład permutacji π_1 na cykle, to rozkład π_2 otrzymujemy zastępując liczby ich obrazami przy permutacji π.
($\Leftarrow$) Znowu przykład: w S_5 rozważmy permutacje podobne $(123)(45)$ i $(143)(25)$. Określamy

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (24).$$

Wtedy $\pi(123)(45)\pi^{-1} = (143)(25)$.
Ogólnie: niech permutacje

$$\pi_1 = (a_1\ a_2\ \ldots\ a_k)(b_1\ldots\ b_l)\ldots(\ldots), \quad \pi_2 = (a_1'\ a_2'\ \ldots a_k')(b_1'\ldots\ b_l')\ldots(\ldots)$$

będą podobne. Niech

$$\pi = \begin{pmatrix} a_1 & a_2 & \ldots & a_k & b_1 & b_2 & \ldots & b_l & \ldots \\ a_1' & a_2' & \ldots' & a_k' & b_1' & b_2' & \ldots' & b_l' & \ldots \end{pmatrix} \in S_n.$$

Wtedy $\pi_2 = \pi\pi_1\pi^{-1}$. ■
W wielu zagadnieniach można utożsamiać permutacje podobne. Dlatego przydatne jest następujące pojęcie.

Definicja 6. Niech w rozkładzie permutacji $\pi \in S_n$ na cykle występuje j_k cykli o długości k, $k = 1, 2, \ldots, n$. Jednomian

$$z(\pi) = x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$$

nazywamy *typem* permutacji π.

Uwaga. Czasem typ oznacza się $z(\pi) = 1^{j_1} 2^{j_2} \cdots n^{j_n}$.

Definicja 7. *Indeksem cyklowym* grupy permutacji $G \subseteq S_n$ nazywamy wielomian:

$$Z(G) = \frac{1}{|G|} \sum_{\pi \in G} z(\pi).$$

Przykład. Niech $G = S_2 = \{e, (12)\}$. Wtedy

$$Z(S_2) = \frac{1}{2}(z(e) + z(12)) = \frac{1}{2}(x_1^2 + x_2).$$

Dla grupy S_3 mamy z kolei:

$$\begin{aligned} Z(S_3) = \frac{1}{6} \sum_{i=1}^{6} z(\pi_i) &= \frac{1}{6}(x_1^3 + x_1x_2 + x_1x_2 + x_1x_2 + x_3 + x_3) = \\ &= \frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3). \end{aligned}$$

9. Indeks cyklowy grupy dwuścianu

Definicja 8. *Grupę izometrii n-kąta foremnego ($n \geqslant 3$) nazywamy grupą dwuścianu (diedralną) i ozn. D_n.*

$|D_n| = 2n$, bo D_n składa się z n obrotów i n symetrii osiowych. Grupa ta jest generowana np. przez obrót o kąt $2\pi/n$ i jedną symetrię osiową.
Każda izometria z D_n da się opisać jako pewna permutacja wierzchołków, więc D_n można traktować jako podgrupę grupy S_n.
Np. $D_4 = \{e, (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$.

Twierdzenie 12. *1) Jeżeli $n = 2m + 1$, to*

$$Z(D_n) = \frac{1}{2n}\big(x_1^n + nx_1x_2^m + \sum_{d|n, d\neq 1} \varphi(d) x_d^{n/d}\big).$$

2) Jeżeli $n = 2m$, to

$$Z(D_n) = \frac{1}{2n}\big(x_1^n + mx_1^2x_2^{m-1} + (m+1)x_2^m + \sum_{d|n, d\neq 1,2} \varphi(d) x_d^{n/d}\big).$$

D o w ó d. Symetrie osiowe dają w D_n składniki:
$nx_1x_2^m$ dla $n = 2m + 1$,
$mx_1^2x_2^{m-1} + mx_2^m$ dla $n = 2m$.
Natomiast obroty tworzą podgrupę cykliczną. Niech g będzie generatorem — jest to cykl rzędu n, np. $g = (123 \ldots n)$. Wtedy g^k ma rząd

$$d = \frac{n}{\mathrm{nwd}(k, n)}$$

i jest iloczynem n/d cykli długości d, tj. $z(g^k) = x_d^{n/d}$. Elementów rzędu d jest tyle, ile jest takich k, że $\mathrm{nwd}(k, n) = n/d$, tj. $\varphi(d)$ (bo $\mathrm{nwd}(k, d) = 1 \Leftrightarrow \mathrm{nwd}(k \cdot \frac{n}{d}, d \cdot \frac{n}{d}) = \frac{n}{d}$). Dla $n = 2m$ istnieje jeden obrót typu x_2^m. ■
Przykład.

$$Z(D_4) = \frac{1}{8}\big(x_1^4 + 2x_1^2x_2 + 3x_2^2 + 2x_4\big).$$

10. Grupa ilorazowa

Definicja 9. *Warstwą lewostronną* grupy G względem podgrupy H wyznaczoną przez $a \in G$ nazywamy zbiór:

$$aH = \{ah : \ h \in H\}.$$

Przykłady. 1. Niech $G = \mathbb{Q}^*$, $H = \{3^n : \ n \in \mathbb{Z}\}$. Wtedy np. $5H = \{5 \cdot 3^n : \ n \in \mathbb{Z}\}$. 2. W zapisie addytywnym: niech $G = \mathbb{Z}$, $H = 3\mathbb{Z} = \{3k : \ k \in \mathbb{Z}\}$; wtedy $5+H = \{5+3k : \ k \in \mathbb{Z}\}$. 3. $G = GL_n(K)$, $H = SL_n(K)$. Dla $\mathbf{A} \in GL_n(K)$ mamy:

$$\mathbf{A}H = \{\mathbf{AB} : \ \mathbf{B} \in SL_n(K)\} = \{\mathbf{C} : \ \det \mathbf{C} = \det \mathbf{A}\}.$$

Lemat 5. *Niech $H \leqslant G$. $b \in aH \Leftrightarrow a^{-1}b \in H$.*

Lemat 6. *Relacja :*

$$a \sim b \Leftrightarrow a^{-1}b \in H$$

jest relacją równoważności w zbiorze G. Klasami abstrakcji tej relacji są warstwy G względem H.

Wniosek 5. *Niech $H \leqslant G$. Każdy element grupy G należy do dokładnie jednej warstwy względem H.*

Wniosek 6. (twierdzenie Lagrange'a) *. Rząd podgrupy grupy skończonej jest dzielnikiem rzędu grupy.*

D o w ó d. Niech $|G| = n$. Każdy element G należy do dokładnie jednej warstwy względem H. Ponadto każda warstwa ma tyle elementów, ile podgrupa H. Zatem:

$$n = \text{liczba warstw} \cdot \text{liczba elementów warstwy},$$

$$n = \text{liczba warstw} \cdot |H|.$$

Zatem $|H|$ jest dzielnikiem $|G|$. ■

Wniosek 7. *Jeżeli grupa G ma rząd będący liczbą pierwszą p, to jest cykliczna.*

D o w ó d. Jeżeli $a \in G$ jest rzędu n, to $\{e, a, \ldots, a^{n-1}\}$ jest podgrupą cykliczną rzędu n. Zatem $n|p$. A wiec jesli $n \neq 1$, to $n = p$, czyli $G = \{e, a, \ldots, a^{p-1}\}$. ■

Definicja 10. Zbiór warstw G względem H nazywamy *zbiorem ilorazowym* grupy G przez podgrupę H i oznaczamy G/H. Moc zbioru G/H nazywamy *indeksem podgrupy H w grupie G* ; oznaczenie $(G : H)$.

W zbiorze ilorazowym można wprowadzić działanie, ale trzeba więcej założyć o H.

Definicja 11. Podgrupę H grupy G nazywamy *podgrupą normalną lub dzielnikiem normalnym* (oznaczenie : $H \lhd G$), jeżeli spełniony jest warunek:

$$\forall_{g \in G} \ \forall_{h \in H} \ \ g^{-1}hg \in H.$$

Warunki równoważne:

$$\forall_{g \in G} \ \ gH = Hg \ ; \ \forall_{g \in G} \ \ g^{-1}Hg \subseteq H.$$

Przykłady. 1. Jeżeli G jest abelowa, to każda podgrupa jest normalna. 2. $SL_n(K)$ jest normalna w $GL_n(K)$. 3. W grupie S_3 podgrupa $H = \{e, (1\ 2)\}$ nie jest normalna, bo dla $g = (1\ 2\ 3)$, $gH = \{(1\ 2\ 3), (1\ 3)\}$, ale $Hg = \{(1\ 2\ 3), (2\ 3)\}$.

Lemat 7. *Niech $f : G \longrightarrow G'$ będzie homomorfizmem. Wtedy* $\ker f \lhd G$.

D o w ó d. Dla $g \in G$, $h \in \ker f$ mamy $f(g^{-1}hg) = f(g)^{-1}f(h)f(g) = f(g)^{-1}f(g) = e$, więc $g^{-1}hg \in \ker f$. ■

Twierdzenie 13. *Jeżeli $H \lhd G$, to działanie:*

$$aH \cdot bH = abH$$

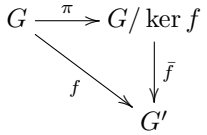
wprowadza w zbiorze ilorazowym G/H strukturę grupy, zwanej grupą ilorazową *G przez H. Warstwa $H = eH$ jest jedynką w G/H, a elementem odwrotnym do aH jest $a^{-1}H$.*

D o w ó d. Sprawdzimy, że działanie jest dobrze określone, tj.

$$(aH = a'H \ , \ bH = b'H) \implies abH = a'b'H.$$

Mamy : $a'b'H = a'(b'H) = a'(bH) = a'(Hb) = (a'H)b = (aH)b = a(Hb) = a(bH) = abH$. ■

Twierdzenie 14. (podstawowe o homomorfizmach) . *Niech $f : G \longrightarrow G'$ będzie homomorfizmem grup z jądrem $H = \ker f$. Wtedy $H \lhd G$ oraz $G/H \cong \operatorname{im} f$. Na odwrót, jeśli $H \lhd G$, to istnieje grupa G' (mianowicie G/H) i epimorfizm $\pi : G \longrightarrow G'$ o jądrze H.*



Uwaga. π nazywamy *homomorfizmem kanonicznym (naturalnym).*
D o w ó d. Wiemy już, że $H \lhd G$. Określamy odwzorowanie

$$\bar{f} : G/H \longrightarrow G' \ , \ \ \bar{f}(gH) = f(g).$$

Wykażemy, że $\bar{f}$ jest izomorfizmem. Najpierw zauważmy, że odwzorowanie $\bar{f}$ jest dobrze określone, bo jeśli $g_1H = g_2H$, to $g_1^{-1}g_2 \in H$, czyli $f(g_1^{-1}g_2) = e$, tj. $f(g_1) = f(g_2)$. Dalej, $\bar{f}$ jest homomorfizmem, bo $\bar{f}(g_1H \cdot g_2H) = \bar{f}(g_1g_2H) = f(g_1g_2) = f(g_1)f(g_2) = \bar{f}(g_1H)\bar{f}(g_2H)$. Ponadto $\bar{f}$ jest monomorfizmem, bo jeśli $\bar{f}(gH) = e$, to $f(g) = e$ czyli $g \in H$, więc $gH = H$. Oczywiście $\bar{f}(G/H) = \operatorname{im} f$, czyli obraz $\bar{f}$ jest taki sam jak obraz f. Zatem $\bar{f}$ jest szukanym izomorfizmem.
Odwrotnie, niech $H \lhd G$. Określamy $\pi : G \longrightarrow G/H$ wzorem $\pi(g) = gH$. Odwzorowanie π ma wtedy wszystkie żądane własności. ■
Niekiedy grupa jest izomorficzna z iloczynem prostym swoich podgrup. Mówi o tym poniższe twierdzenie.

Twierdzenie 15. *Niech G będzie grupą, a A i B jej dzielnikami normalnymi. Jeżeli $A \cap B = \{e\}$ i $AB = G$, to $G \cong A \times B$.*

D o w ó d. Każdy element $g \in G$ można w sposób jednoznaczny(!) przedstawić w postaci iloczynu $g = ab$, $a \in A$, $b \in B$. Określamy $f : G \longrightarrow A \times B$ wzorem $f(g) = (a, b)$. To odwzorowanie jest izomorfizmem. ■

Twierdzenie 16. *Niech $G = A \times B$. Wtedy $G/A \cong B$.*

D o w ó d. Niech $f : G \longrightarrow B$, $f(a, b) = b$. Wtedy f jest epimorfizmem z jądrem A. ■
Przykład. Rozpatrzmy odwzorowanie $|\ |$ (moduł) przyporządkowujące każdej liczbie zespo-

lonej jej wartość bezwzględną. Ponieważ $|z_1z_2| = |z_1| \cdot |z_2|$ więc jest to homomorfizm grupy multiplikatywnej $\mathbb{C}^*$ w grupę multiplikatywną $\mathbb{R}_+^*$ liczb nieujemnych. Jądrem tego homomorfizmu jest grupa $\mathbb{C}_1 = \{z \in \mathbb{C} : \ |z| = 1\}$. Grupa ilorazowa $\mathbb{C}^*/\mathbb{C}_1$ jest izomorficzna z grupą $\mathbb{R}_+^*$. Geometrycznie, elementami grupy ilorazowej są okręgi o środku w początku układu współrzędnych. Iloczynem dwu takich okręgów o promieniach r_1 i r_2 jest okrąg o promieniu r_1r_2. Grupa $\mathbb{R}_+^*$ jest także podgrupą w $\mathbb{C}^*$; łatwo zauważyć, że jest to jądro homomorfizmu $\arg : \mathbb{C}^* \longrightarrow \mathbb{R}$ ($\mathbb{R}$ — grupa addytywna). Widać, że $\mathbb{R}_+^* \cap \mathbb{C}_1 = \{1\}$ oraz $\mathbb{R}_+^*\mathbb{C}_1 = \mathbb{C}^*$. Zatem $\mathbb{C}^* \cong \mathbb{C}_1 \times \mathbb{R}_+^*$.

Przykład. Niech $\varphi : \mathbb{C}^* \to \mathbb{C}^*$ będzie określone wzorem $\varphi(z) = \frac{z^3}{|z|^3}$. Sprawdzić, że φ jest homomorfizmem, wyznaczyć $\ker\varphi$ i $\operatorname{im}\varphi$, przedstawić graficznie oba zbiory i narysować warstwę $e^{\mathrm{i}\,\pi/4}\ker\varphi$.
Rozwiązanie. $\mathbb{C}^*$ jest grupą z mnożeniem. Sprawdzamy, czy φ jest homomorfizmem:

$$\varphi(z_1z_2) = \frac{(z_1z_2)^3}{|z_1z_2|^3} = \frac{z_1^3z_2^3}{|z_1|^3|z_2|^3} = \frac{z_1^3}{|z_1|^3}\cdot\frac{z_2^3}{|z_2|^3} = \varphi(z_1)\varphi(z_2).$$

Jądro tworzą rozwiązania równania $\varphi(z) = 1$, tzn.

$$\frac{z^3}{|z|^3} = 1$$

Aby je rozwiązać można np. zapisać z w postaci wykładniczej: $z = re^{\mathrm{i}\,\alpha}$. Wtedy

$$\frac{(re^{\mathrm{i}\,\alpha})^3}{|re^{\mathrm{i}\,\alpha}|^3} = 1,$$

$$e^{3\,\mathrm{i}\,\alpha} = 1$$

$$3\,\mathrm{i}\,\alpha = 2k\pi\,\mathrm{i}, \quad k \in \mathbb{Z}.$$

Zatem r jest dowolne (większe od 0), a α ma 3 wartości: 0, $2\pi/3$, $4\pi/3$:

$$\ker\varphi = \{r, re^{2\,\mathrm{i}\,\pi/3}, re^{4\,\mathrm{i}\,\pi/3} :\ r \in \mathbb{R}^+\}.$$

Geometrycznie są to 3 półproste wychodzące z początku układu, nachylone do osi rzeczywistej pod kątami 0, $2\pi/3$, $4\pi/3$.
Z kolei obraz homomorfizmu to zbiór liczb postaci $\varphi(re^{\mathrm{i}\,\alpha}) = e^{3\,\mathrm{i}\,\alpha}$, $\alpha \in \mathbb{R}$. Jest to więc okrąg jednostkowy.
Warstwa:

$$e^{\mathrm{i}\,\pi/4}\ker\varphi = \{re^{\mathrm{i}\,\pi/4}\cdot e^{2k\,\mathrm{i}\,\pi/3} :\ k = 0,1,2\} =$$
$$= \{re^{\mathrm{i}\,\pi/4}, re^{\mathrm{i}(\pi/4+2\pi/3)}, re^{\mathrm{i}(\pi/4+4\pi/3)} :\ r \in \mathbb{R}^+\}.$$

Geometrycznie są to 3 półproste wychodzące z początku układu, nachylone do osi rzeczywistej pod kątami $\frac{\pi}{4}$, $\frac{11\pi}{12}$, $\frac{19\pi}{12}$.

11. Działanie grupy na zbiorze

Definicja 12. Mówimy, że grupa G (zapisywana multiplikatywnie) *działa na zbiorze* X, jeżeli jest dane przekształcenie $G \times X \longrightarrow X$, w którym obrazem pary (g, x) jest element zbioru X, oznaczany przez gx. Zakładamy, że to przekształcenie ma następujące własności:
a) $\forall_{x\in X}\ \ ex = x$;
b) $\forall_{x\in X}\ \ \forall_{g,h\in G}\ \ (gh)x = g(hx)$.

W tym kontekście elementy grupy G nazywamy *operatorami*, a zbiór X nazywamy *G-zbiorem.* Dla $x \in X$ zbiór

$$Gx = \{gx :\ g \in G\}$$

nazywamy *G-orbitą* elementu x. Może się zdarzyć, że $Gx = \{x\}$; wtedy x nazywamy *punktem stałym* względem G.

Lemat 8. *Niech X będzie G-zbiorem. Rodzina orbit $\{Gx :\ x \in X\}$ jest podziałem zbioru X na parami rozłączne niepuste zbiory których suma jest równa X.*

D o w ó d. Wystarczy wykazać, że relacja:

$$x \sim y \iff (x, y \text{ należą do tej samej orbity})$$

jest relacją równoważności i powołać się na zasadę abstrakcji (twierdzenie 7). ■

Definicja 13. Zbiór $G_x = \{g \in G : \ gx = x\}$ nazywamy *stabilizatorem* elementu x.

Lemat 9. *G_x jest podgrupą G.*

D o w ó d. Jeśli $g, h \in G_x$, czyli $gx = hx = x$, to $g^{-1}hx = x$, więc $g^{-1}h \in G_x$. ■
Przykłady. 1. Niech G będzie grupą permutacji zbioru $\Omega = \{1, 2, \ldots, n\}$. Wtedy G działa na Ω wg wzoru $(\alpha, j) \mapsto \alpha(j)$.
W szczególności, jeśli $G = S_n$, to orbita jest tylko jedna. Stabilizatorem G_i elementu i jest wtedy grupa złożona z permutacji, w których rozkładzie na cykle występuje cykl (i). Np. gdy $G = S_6$, to $|G| = 720$ a $|G_i| = 120$ dla $i = 1, 2, \ldots, 6$.
Jeśli G jest grupa cykliczną generowaną przez π, $G = (\pi)$, to orbitami tego działania są wprowadzone wcześniej π-orbity : i, j należą do tej samej π-orbity, jeśli w rozkładzie π na cykle są elementami tego samego cyklu. Stabilizator G_i składa się wtedy z tych potęg π^k, dla których $\pi^k(i) = i$. Np. gdy $\pi = (123)(45)(6) \in S_6$ to mamy 3 orbity: $G1 = G2 = G3 = \{1, 2, 3\}$, $G4 = G5 = \{4, 5\}$, $G_6 = \{6\}$. Stabilizatory: $G_1 = G_2 = G_3 = \{e, \pi^3\}$, $G_4 = G_5 = \{e, \pi^2, \pi^4\}$, $G6 = G$. 2. Przykład poprzedni można uogólnić : każda grupa G działa na G wg wzoru $(g, x) \mapsto gx$. Wtedy orbita jest tylko jedna. Jeśli $H \leqslant G$, to H działa na G wg wzoru $(h, x) \mapsto hx$. Wtedy orbitami są warstwy prawostronne grupy G względem podgrupy H.
3. Innym działaniem G na G jest działanie poprzez automorfizmy wewnętrzne:

$$(a, g) \mapsto I_a g = aga^{-1} \quad \text{dla } a, g \in G.$$

Sprawdzimy, że jest to działanie. Mamy $I_e g = ege^{-1} = g$ oraz

$$I_{ab}g = (ab)g(ab)^{-1} = abgb^{-1}a^{-1} = aI_b ga^{-1} = I_a(I_b g),$$

a więc warunki są spełnione. Dla tego działania:

$$Gx = \{I_a x : \ a \in G\} = \{axa^{-1} : \ a \in G\}.$$

Jeżeli $x \in Z(G)$, to dla dowolnego $a \in G$ mamy $axa^{-1} = x$, więc $Gx = \{x\}$.
Elementy orbity Gx nazywamy sprzężonymi z x. W szczególności, gdy $G = S_n$, to orbitami są klasy elementów podobnych, czyli tego samego typu. Działanie, które ma tylko jedną orbitę, nazywamy *przechodnim*. Jeśli działanie jest przechodnie, to dla każdego $x \in X$, $G_x = \{e\}$.

Twierdzenie 17. (o orbitach i stabilizatorach) *Niech grupa G działa na zbiorze X. Wtedy liczność orbity Gx jest równa indeksowi stabilizatora G_x, tj.*

$$|Gx| = (G : G_x).$$

Zatem jeżeli G jest grupą skończoną, to $|Gx| = \frac{|G|}{|G_x|}$. W szczególności liczba elementów orbity jest dzielnikiem rzędu grupy.

D o w ó d. Określimy odwzorowanie $Gx \to G/G_x$ wzorem $f(y) = gG_x$ dla $y = gx$. Takie odwzorowanie jest dobrze określone, bo jeśli $y = g_1x = g_2x$, to $g_2^{-1}g_1x = x$, czyli $g_2^{-1}g_1x \in G_x$, więc $g_1G_x = g_2G_x$. Ponadto f jest surjektywne, bo g może być dowolnym elementem G. Wreszcie jeśli $g_1G_x = g_2G_x$, to $g_2^{-1}g_1x \in G_x$, czyli $g_2^{-1}g_1x = x$, więc $g_1x = g_2x$, co dowodzi, że f jest różnowartościowe. Zatem f określa równoliczność zbiorów Gx i G/G_x. ■

Twierdzenie 18. (lemat Burnside'a) *. Niech X będzie skończonym G-zbiorem. Liczba G-orbit, na które dzieli się zbiór X, jest równa*

$$\frac{1}{|G|} \sum_{g \in G} \chi(g),$$

gdzie $\chi(g)$ oznacza liczność zbioru $\{x \in X : \ gx = x\}$ punktów stałych operatora g.

D o w ó d. Utwórzmy macierz o $|X|$ wierszach i $|G|$ kolumnach następująco:

$$a_{x,g} = \begin{cases} 1 & \text{dla} \quad gx = x \\ 0 & \text{dla} \quad gx \neq x \end{cases}.$$

Obliczymy liczbę jedynek w tej macierzy dwoma sposobami. Sumując jedynki wierszami otrzymujemy $\sum_{x\in X} |G_x|$, a sumując kolumnami $\sum_{g\in G} \chi(g)$. Zatem

$$\sum_{x\in X} |G_x| = \sum_{g\in G} \chi(g).$$

czyli

$$\sum_{x\in X} \frac{|G_x|}{|G|} = \frac{1}{|G|} \sum_{g\in G} \chi(g).$$

Z twierdzenia o orbitach i stabilizatorach otrzymujemy

$$\sum_{x\in X} \frac{1}{|Gx|} = \frac{1}{|G|} \sum_{g\in G} \chi(g).$$

Zauważmy, że $\sum_{x\in Gx} \frac{1}{|Gx|} = 1$, więc $\sum_{x\in X} \frac{1}{|Gx|}$ jest liczbą orbit. ■

Przykład. Naszyjniki składają się z pięciu paciorków w trzech kolorach. Ile jest istotnie różnych naszyjników?

Ponieważ kolor każdego paciorka można wybrać na 3 sposoby, więc naszyjników jest $3^5 = 243$. Jednak nie wszystkie są istotnie różne. Jeśli naszyjnik traktować jako pięciokąt foremny, którego wierzchołki są pomalowane trzema ustalonymi kolorami (np. czerwony, niebieski, zielony), to istotna jest sekwencja kolorów. Należy zatem utożsamić te naszyjniki, które można otrzymać przez obrót pewnego ustalonego naszyjnika. Zatem możemy na zbiorze X wszystkich 243 naszyjników rozpatrywać działanie grupy obrotów; wtedy liczba istotnie różnych naszyjników jest liczbą orbit tego działania. Na mocy lematu Burnside'a otrzymamy:

$$\text{liczba orbit} = \frac{1}{5} \sum_{i=1}^{5} \chi(o_i),$$

gdzie o_i jest obrotem o kąt $\frac{2\pi}{5} i$ dla $i = 1, 2, \ldots, 5$. Ponieważ naszyjnik niezmienniczy przy obrocie o kąt niezerowy musi być 1-kolorowy, więc $\chi(o_i) = 3$ dla $i = 1, 2, 3, 4$; ale $\chi(o_5) = 243$. Zatem

$$\text{liczba orbit} = \frac{1}{5}(4 \cdot 3 + 243) = 51.$$

Ale zwrot "istotnie różne" można rozumieć inaczej. Można utożsamiać naszyjniki które można otrzymać przez obrót oraz te, które można otrzymać przez "przełożenie na drugą stronę", czyli przez symetrię. Matematycznym modelem będzie wtedy działanie grupy diedralnej D_5. Oprócz obrotów zawiera ona jeszcze 5 symetrii osiowych s_i, przy czym $\chi(s_i) = 3^3 = 27$ (kolory 3 wierzchołków wybieramy na 3 sposoby, ale dwa pozostałe muszą mieć taki kolor jak wierzchołek symetryczny). Zatem wtedy

$$\text{liczba orbit} = \frac{1}{10}(4 \cdot 3 + 243 + 5 \cdot 27) = 39.$$

Przykład. Ogólniej, naszyjniki składają się z n paciorków w k kolorach. Ile jest istotnie różnych naszyjników?

a) Jeśli grupą działającą jest grupa obrotów:

$$G = \{o_1, \ldots, o_n\}$$

gdzie o_n jest obrotem o kąt $\frac{2\pi}{n} i$ dla $i = 1, 2, \ldots, n$, to mamy

$$\chi(o_i) = k^{\text{nwd}(n,i)},$$

bo jeżeli $\mathrm{nwd}(n,i)=d$, to obrót o_i jest rzędu $\frac{n}{d}$, co oznacza, że tyle paciorków (co d-ty) musi być tego samego koloru.
(Przykładowo, gdy $n=8, i=6$, to $d=2$. Obrót o_6 jest obrotem o kąt $\frac{3}{2}\pi$, czyli paciorki przechodzące na siebie to 1,7,5,3 oraz 2,8,6,4. Zatem co drugi musi być tego samego koloru. Jest więc k^2 możliwości wyboru kolorów.)
Liczba orbit wynosi:

$$\frac{1}{n}\sum_{i=1}^{n} k^{\mathrm{nwd}(n,i)}.$$

Np. dla $n=6$, $k=3$ otrzymujemy 130.
b) Jeśli grupą działającą jest grupa diedralna, to dochodzą jeszcze symetrie.
W przypadku n nieparzystego oś symetrii musi przechodzić przez wierzchołek. Wtedy

$$\chi(s) = k^{\frac{n+1}{2}}$$

dla każdej symetrii s.
W przypadku n parzystego oś symetrii może przechodzić przez dwa wierzchołki (symetria s_w) lub być symetralną boku (symetria s_b). Wtedy

$$\chi(s_w) = k^{\frac{n}{2}+1}, \quad \chi(s_b) = k^{\frac{n}{2}}.$$

Zatem:
— dla n nieparzystego liczba orbit wynosi

$$\frac{1}{2n}\left(\sum_{i=1}^{n} k^{\mathrm{nwd}(n,i)} + n\cdot k^{\frac{n+1}{2}}\right) = \frac{1}{2n}\sum_{i=1}^{n} k^{\mathrm{nwd}(n,i)} + \frac{1}{2}k^{\frac{n+1}{2}};$$

— dla n parzystego liczba orbit wynosi

$$\frac{1}{2n}\left(\sum_{i=1}^{n} k^{\mathrm{nwd}(n,i)} + \frac{n}{2}\cdot k^{\frac{n}{2}+1} + \frac{n}{2}\cdot k^{\frac{n}{2}}\right) = \frac{1}{2n}\sum_{i=1}^{n} k^{\mathrm{nwd}(n,i)} + \frac{1}{4}k^{\frac{n}{2}}(k+1).$$

Np. dla $n=6$, $k=3$ otrzymujemy 92.
Uwaga. Obroty i symetrie o których mowa wyżej można interpretować jako permutacje. Jeżeli pod działaniem permutacji naszyjnik nie zmienia się, to znaczy, że paciorki odpowiadające elementom tego samego cyklu są jednakowego koloru. Zatem:
Jeżeli permutacja $\pi \in S_n$ ma r cykli (wliczając cykle długości 1), to liczba pokolorowań stałych dla π wynosi k^r (k — liczba kolorów).

Wniosek 8. *Jeżeli G jest grupą permutacji działającą na zbiorze pokolorowań, i znamy jej indeks cyklowy $Z(G)$, to liczbę różnych pokolorowań otrzymamy podstawiając w $Z(G)$ $x_1 = x_2 = \cdots = x_n = k$.*

Przykład. Jeśli $G=(\pi)$, gdzie $\pi=(12345)$, to $Z(G)=\frac{1}{5}(x_1^5+4x_5)$. Podstawiając $k=3$ otrzymamy $\frac{1}{5}(243+12)=51$.
Ogólniej, prawdziwe jest następujące twierdzenie.

Twierdzenie 19. *Niech G będzie grupą permutacji zbioru X, a $\tilde{X}$ zbiorem funkcji $X\to Y$. Dla $\sigma\in G$ określamy $\tilde{\sigma}:\tilde{X}\to\tilde{X}$ wzorem*

$$\tilde{\sigma}(f) = f\circ\sigma$$

dla $f\in\tilde{X}$. Zbiór $\tilde{G}=\{\tilde{\sigma}:\ \sigma\in G\}$ jest grupą działajacą na zbiorze $\tilde{X}$. Ponadto, jeśli n jest liczba cykli w rozkładzie permutacji σ, to

$$|\tilde{X}_\sigma| = |Y|^n.$$

D o w ó d. Wykażemy, że $\tilde{\sigma}$ jest odwzorowaniem różnowartościowym. Przypuśćmy, że dla pewnych $f, g \in \tilde{X}$ jest $\tilde{\sigma}(f) = \tilde{\sigma}(g)$, tj.

$$f(\sigma(x)) = \tilde{\sigma}(f)(x) = \tilde{\sigma}(g)(x) = g(\sigma(x))$$

dla każdego $x \in X$. Ale ponieważ σ jest permutacją, więc jej wartościami są wszystkie elementy zbioru X, a więc f i g mają równe wartości na wszystkich elementach zbioru X. Stąd $f = g$.
Zatem $\tilde{G}$ można traktować jako grupę permutacji izomorficzną z G.
Załóżmy, że σ jest permutacją zbioru X z rozkładem na cykle $\sigma = \sigma_1\sigma_2 \dots \sigma_n$. Jeżeli $f \in \tilde{X}_\sigma$, tj. $\tilde{\sigma}(f) = f$, to funkcja f musi mieć stałą wartość na każdym cyklu permutacji σ. Ponieważ jest n cykli i $|Y|$ możliwych wartości dla każdego cyklu, więc $|\tilde{X}_\sigma| = |Y|^n$.
Przykład. Niech $X = \{1, 2, \dots, 8\}$, $Y = \{a, b, c\}$. Jeśli $\sigma = (135)(26)(47)(8)$, to $|\tilde{X}_\sigma| = 3^4 = 81$.
Przykład. Na ile sposobów można pokolorować wierzchołki kwadratu używając czterech różnych kolorów?
Grupą symetrii kwadratu jest grupa diedralna D_4. Ponieważ

$$Z(D_4) = \frac{1}{8}(x_1^4 + 2x_1^2x_2 + 3x_2^2 + 2x_4),$$

więc podstawiając $x_1 = x_2 = x_3 = x_4 = 4$ otrzymujemy

$$\frac{1}{8}(4^4 + 2 \cdot 4 + 3 \cdot 4^2 + 2 \cdot 4) = 55.$$