POLITECHNIKA LUBELSKA

Ernest Nieznaj

Teoria grup

Od twierdzenia Lagrange'a do algorytmu Schreiera-Simsa

MONOGRAFIE

Lublin 2021

Teoria grup

Od twierdzenia Lagrange'a do algorytmu Schreiera-Simsa

Monografie – Politechnika Lubelska

Politechnika Lubelska
Wydział Elektrotechniki i Informatyki
ul. Nadbystrzycka 38A
20-618 Lublin

Ernest Nieznaj

Teoria grup

Od twierdzenia Lagrange'a do algorytmu Schreiera-Simsa

Wydawnictwo
Politechniki Lubelskiej

Lublin 2021

Recenzent:
dr Elżbieta Ratajczyk, Politechnika Lubelska

Publication approved by the Rector of Lublin University of Technology

ISBN: 978-83-7947-495-0

Publisher: Wydawnictwo Politechniki Lubelskiej
www.biblioteka.pollub.pl/wydawnictwa
ul. Nadbystrzycka 36C, 20-618 Lublin
tel. (81) 538-46-59

The digital version is available at the Digital Library of Lublin University of Technology: www.bc.pollub.pl

Spis treści

Teoria grup. Od twierdzenia Lagrange'a do algorytmu Schreiera-Simsa

Streszczenie

Teoria grup jest dziedziną matematyki mającą szerokie zastosowania w innych naukach jak np. w fizyce, chemii, biologii czy kryptografii. Jest też interesująca sama w sobie i stanowi obszar badań matematyków i algorytmików. Szereg problemów dotyczących teorii grup skończonych to zagadnienia czysto algorytmiczne. Problemy te towarzyszyły teorii grup od samych jej początków sięgających XVIII wieku, patrz [6, 8, 12, 18].

Celem tej monografii jest wprowadzenie do jednego z takich zagadnień, jakim jest obliczenie rzędu grupy permutacji określonej przez skończony układ generatorów. W latach 70. XX wieku matematyk Charles Sims stworzył podstawy metody, która nazywana jest obecnie algorytmem Schreiera-Simsa i służy do rozwiązania tego zagadnienia. Algorytm ten oparty jest na twierdzeniu innego matematyka Otto Schreiera z jego pracy z 1927 roku, patrz np. [2, 15, 16].

W ostatnich dziesięcioleciach algorytm ten został włączony do standardowych bibliotek różnych środowisk obliczeniowych i programistycznych takich jak Mathematica. Ponieważ grupy permutacji są częścią ogólnej teorii grup, to w kilku pierwszych rozdziałach zostały przedstawione główne pojęcia i twierdzenia w niej występujące. Niektóre z nich omówione są szczegółowo np. grupy reszt modulo. Osobny rozdział poświęcony jest też samym grupom symetrycznym. Algorytm Schreiera-Simsa przedstawiony jest w rozdziale ostatnim.

Słowa kluczowe: teoria grup, grupy permutacji, algorytm Schreiera-Simsa

Theory of groups. From Lagrange's theorem to the Schreier-Sims algorithm

Abstract

Group theory is a branch of mathematics that has many applications in e.g. physics, chemistry, biology or cryptography. It is also an interesting research area for both mathematicians and computer scientists. For instance, computational group theory is a subfield of algebra dealing with analysis and implementation of algorithms about groups. It is an interdisciplinary area between mathematics and computer science. Algorithmic questions permeated group theory from its origins in the 18th century, see [6, 8, 12, 18].

The aim of this book is to introduce a reader to one of such problems. This problem is to find the order of a permutation group given by a set of its generators. In the 1970s Charles Sims created the foundations for what is today called the Schreier-Sims algorithm. It is based on Otto Schreier's theorem from his 1927 paper. This algorithm is mostly used to calculate the order of a permutation group but the membership problem can be also solved by this method. So you can answer the question whether a particular permutation belongs to the group.

In recent decades the algorithm has been implemented in many software systems like SAGE or Mathematica, see also [2, 15, 16].

Since the field of permutation groups is part of general group theory a number of topics are covered in the first three chapters. These include algebraic product of subgroups, Lagrange's theorem, the construction of a quotient group, direct and semidirect products of groups. One chapter is devoted to permutations and one is about group actions on a set.
The Schreier-Sims algorithm is discussed in the last chapter.

Keywords: group theory, permutation groups, the Schreier-Sims algorithm

Wstęp

Monografia ta ma następujący układ.

W rozdziale 1 przedstawione sa podstawowe pojęcia związane z teorią grup. Są to m.in. definicja grupy, podgrupy, rzędu elementu i iloczynu algebraicznego podgrup. Ponadto zdefiniowane są grupy reszt modulo: addytywnej $\mathbb{Z}_p$ i multiplikatywnej $\mathbb{Z}_p^*$. Omówione są też grupy przekształceń figur płaskich i wielościanów foremnych.

Rozdział 2 dotyczy homomorfizmu grup i jego własności. Wprowadzona jest również relacja sprzężenia oraz pojęć z nią zwiazanych takich jak podgrupa niezmiennicza, centrum i komutant grupy.

W rozdziale 3 udowodnione jest twierdzenia Lagrange'a i podana jest konstrukcja grupy ilorazowej. Zdefiniowany jest też iloczyn prosty i półprosty grup. Pojęcia te zilustrowane są przykładami.

Rozdział 4 poświęcony jest grupom permutacji, nazywanych też grupami symetrycznymi. Głównymi zagadnieniami są tutaj: rozkład na cykle, parzystość i nieparzystość permutacji oraz grupa alternująca. Wyprowadzone są też wzory na ilość permutacji z ustaloną liczbą punktów stałych. Centralne twierdzenia graniczne mówi, ze graniczny rozkład permutacji ze względu na liczbę zawartych w niej inwersji jest rozkładem normalnym.

W rozdziale 5 definiujemy działanie grupy na zbiorze, orbitę i stabilizator. Ponadto działanie przechodnie, k-przechodnie, bloki oraz grupy prymitywne. Udowodnione jest też twierdzenie Cauchy'ego, które stwierdza, że jesli p jest liczbą pierwszą dzielącą rząd grupy, to grupa ta zawiera podgrupę rzędu p.

W rozdziale 6 przedstawiony jest algorytm Schreier-Simsa. Za pomacą tego algorytmu można obliczyć rząd grupy zadanej przez skończony układ generatorów oraz rozwiązać problem „członkostwa", czyli tego, czy dana permutacja do takiej grupy należy.

1. Grupy I

1.1 Grupy i podgrupy

Zaczniemy od wprowadzenia oznaczeń, pojęć oraz kilku podstawowych faktów używanych w niniejszej monografii. I tak zbiór liczb naturalnych oznaczamy przez $\mathbb{N}$, a zbiór liczb całkowitych przez $\mathbb{Z}$. Zatem

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

oraz

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Zbiór liczb wymiernych, czyli liczb postaci $\frac{m}{n}$, gdzie $m \in \mathbb{Z}$ i $n \in \mathbb{N}$, oznaczany jest przez $\mathbb{Q}$, a rzeczywistych przez $\mathbb{R}$. Zbiór liczb zespolonych to $\mathbb{C}$, czyli

$$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\},$$

gdzie $i = \sqrt{-1}$. Pierwiastkiem n-tego stopnia z liczby zespolonej z nazywa się liczbę zespoloną w, dla której $w^n = z$. Każda różna od zera liczba zespolona posiada dokładnie n pierwiastków stopnia n. Pierwiastki te zapisuje się zwykle w postaci

$$\sqrt[n]{z} = \{w_0, w_1, \ldots, w_{n-1}\},$$

gdzie

$$w_k = \sqrt[n]{|z|}\left(\cos\tfrac{\theta+2k\pi}{n} + i\sin\tfrac{\theta+2k\pi}{n}\right), \quad k = 0, 1, \ldots, n-1.$$

W powyższym wzorze $|z| = \sqrt{x^2 + y^2}$, natomiast $\theta \in [0, 2\pi)$ oznacza argument liczby z. Ponadto $\sqrt[n]{|z|}$ jest arytmetycznym pierwiastkiem rzeczywistym stopnia n. Wzory te wykorzystamy w przykładzie 1.4. Dowodzimy tam, że zbiór pierwiastków n-tego stopnia z jedynki tworzy grupę cykliczną rzędu n.

Mnożenie liczb ma bardzo dobre własności z punktu widzenia tej monografii, tzn. jest przemienne i łączne, ale ma jeden minus. Tym minusem jest fakt, że zero nie jest odwracalne i w związku z tym potrzebujemy następujących oznaczeń

$$\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}, \quad \mathbb{R}^* = \mathbb{R}\backslash\{0\}, \quad \mathbb{C}^* = \mathbb{C}\backslash\{0\}.$$

Podobnie określamy

$$\mathbb{Q}_+ = \{q \in \mathbb{Q} : q > 0\}, \quad \mathbb{R}_+ = \{q \in \mathbb{R} : q > 0\}.$$

Niech X i Y będą dowolnymi zbiorami. Odwzorowaniem, przekształceniem lub funkcją $f : X \to Y$ nazywamy przyporządkowanie każdemu $x \in X$ jedynego elementu $y \in Y$. Piszemy wtedy $y = f(x)$ i mówimy, że y jest obrazem x przez f. Jeśli każdy element $y \in Y$ jest obrazem co najmniej jednego $x \in X$, to f nazywamy odwzorowaniem X **na** Y lub **surjekcją**. Jeśli dla $x_1 \neq x_2$ spełniony jest warunek $f(x_1) \neq f(x_2)$, to o f mówimy, że jest **injekcją** lub odwzorowaniem **różnowartościowym**.

Odwzorowanie f nazywamy **wzajemnie jednoznacznym** albo **bijekcją**, jeśli każdy $y \in Y$ jest obrazem dokładnie jednego $x \in X$. Bijekcja jest więc surjekcją i injekcją. Przekształcenie $f^{-1} : Y \to X$ dane wzorem $f^{-1}(y) = x$ nazywamy odwzorowaniem **odwrotnym** do f. Nie dla wszystkich f takie przekształcenie istnieje. Te, dla których istnieje nazywamy odwracalnymi. Zbiór wszystkich funkcji z X do Y oznaczamy przez Y^X.

Niech $f : X \to Y$ i $g : Y \to Z$ będą funkcjami. **Złożeniem** lub **superpozycją** f i g nazywamy odwzorowanie $f \circ g : X \to Z$ zdefiniowane wzorem

$$(f \circ g)(x) = g(f(x)). \tag{1.1}$$

Jeśli dziedziną g jest podzbiór $D_g \subset Y$, czyli $g : D_g \to Z$, to złożenie $f \circ g$ ma sens dla tych x, dla których $f(x) \in D_g$.

Używa się różniej terminologii. W tej monografi odwzorowanie, przekształceniem i funkcja są synonimami. O funkcjach mówi się zwykle, gdy mamy do czynienia ze zbiorami liczbowymi, ale i to nie jest regułą.

Iloczynem kartezjańskim zbiorów X, Y nazywamy zbiór oznaczany przez $X \times Y$ i określony następująco

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

Jest to więc zbiór par, w których kolejność elementów jest istotna. Oznacza to, że $(x_1, y_1) = (x_2, y_2)$ wtedy i tylko wtedy, gdy $x_1 = x_2$ i $y_1 = y_2$. Jeśli X, Y są skończone, to $|X \times Y| = |X| \cdot |Y|$. Symbol $|X|$ oznacza liczbę elementów X, ponadto $X^2 = X \times X$. Podobnie definiuje się $X_1 \times X_2 \times \ldots \times X_n$.

Relacją R nazywamy dowolny podzbiór iloczynu kartezjańskiego $X \times Y$. Zatem $R \subset X \times Y$ i jeśli $(x, y) \in R$, to piszemy równoważnie xRy i mówimy, że x jest w relacji z y. Gdy $X = Y$, to R nazywana jest relacją w zbiorze X. W tym przypadku $R \subset X^2$.

O relacji $R \subset X^2$ mówimy, że jest **relacją równoważności**, jeśli spełnia następujące trzy warunki

(i) jest **zwrotna**, czyli xRx, dla każdego $x \in X$,

(ii) jest **symetryczna**, czyli $xRy \Rightarrow yRx$,

(iii) jest **przechodnia**, czyli $xRy \wedge yRz \Rightarrow xRz$.

Klasą równoważności lub **klasą abstrakcji** elementu $x \in X$ nazywamy zbiór tych elementów, z którymi x jest w relacji, tzn.

$$[x] := \{y \in X : xRy\}.$$

Zbiór wszystkich klas abstrakcji oznaczamy przez $[X]$. **Zasada abstrakcji** mówi, że dla dwie klasy abstrakcji są albo równe albo nie mają elementów wspólnych, czyli

$$[x_1] = [x_2] \quad \text{lub} \quad [x_1] \cap [x_2] = \emptyset,$$

dla dowolnych $x_1, x_2 \in X$. Oznacza to, że X można zapisać jako sumę wszystkich klas równoważności

$$X = \bigcup_{x \in X} [x].$$

Rozpatrzmy przykład. Niech X będzie zbiorem wszystkich ludzi na Ziemi. Zdefiniujmy R_1 następująco: Osoba 1 jest w relacji z Osobą 2, jeśli oboje urodzili się w tym samym miesiącu. Zatem np. Osoba 1 urodzona 9 stycznia 1940 roku jest w relacji z Osobą 2 urodzoną 25 stycznia 1988 roku. Widać, że relacja ta jest relacją równoważności i dzieli wszystkich ludzi na 12 klas abstrakcji. Klasy te to osoby urodzone w styczniu, w lutym i tak aż do grudnia.

Działaniem lub **operacją binarną** w zbiorze X nazywamy dowolne odwzorowanie z $X \times X$ w X. Działania oznacza się przeważnie symbolami typu $\circ$, $\diamond$, $\oplus$, $\otimes$ i ogólnie można je określić na dwa sposoby. Pierwszy sposób to podanie wzoru, np. $a \circ b = ab + 1$ dla $a, b \in \mathbb{R}$. Drugi sposób dotyczy sytuacji, gdy X jest zbiorem skończonym. Wtedy też można podać wzór, ale gdy X ma niewiele elementów, to działanie można określić za pomocą tabeli. W przypadku grup tabele takie nazywane są **tablicami Cayleya.** Nazwa ta pochodzi od A. Cayleya, który wprowadził je w 1854 roku.

Jeśli X ma n elementów, to liczba wszystkich możliwych działań na X, czyli funkcji z $X \times X$ w X wynosi n^{n^2}, tzn.

$$|X^{X \times X}| = n^{n^2}, \quad n \geq 2.$$

Wynika to z faktu, że każdej parze elementów z X można przyporządkować dowolny element tego zbioru. Zatem dla $n = 2$ istnieje $2^4 = 16$ działań, dla $n = 3$ mamy $3^9 = 19683$, a dla $n = 4$ istnieje 4294967296 operacji binarnych. W tabeli 1.1 podane zostały trzy takie działania dla $n = 3$.

Tabela 1.1 Trzy spośród 19 683 możliwych do określenia operacji dwuargumentowych w zbiorze $\{a, b, c\}$. Działanie w środkowej tabeli nie jest łączne.

$\circ$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\circ$	a	b	c
a	a	a	b
b	b	c	a
c	b	c	c

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Na przykład, przyporządkowanie wektorom $\vec{u}$, $\vec{v}$ z przestrzeni $\mathbb{R}^3$ ich iloczynu wektorowego $\vec{u} \times \vec{v}$ jest działaniem w zbiorze wektorów, splot jest działaniem w zbiorze funkcji, a iloczyn macierzy jest działaniem w zbiorze macierzy. Są to działania binarne. Natomiast iloczyn mieszany wektorów nie jest działaniem binarnym, ponieważ potrzebne są trzy wektory. Podobnie obliczanie pochodnej lub całki nie jest działaniem binarnym. Potrzebna jest tutaj tylko jedna funkcja. Silnia, którą za chwilę zdefiniujemy, też działaniem binarnym nie jest. Jest to działanie unarne lub jednoargumentowe.

Zatem **silnia** zdefiniowana jest nastepująco

$$n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1, \quad n \in \mathbb{N},$$

oraz przyjmujemy, że $0! = 1$. Podstawowa własność, to $n! = (n-1)! \cdot n$. Silnia rośnie dość szybko. Dobrym przybliżeniem dla dużych n jest przybliżenie Stirlinga

$$n! \approx \sqrt{2\pi n} e^{-n} n^n,$$

z którego wynika, że silnia jest w nieskończoności istotnie słabsza od n^n, czyli $n!/n^n$ dąży do zera, gdy $n \to +\infty$. Silnia ma pewną ciekawą własność. Jeśli $n \geq 2$, to w poniższym ciągu

$$n! + 2, n! + 3, n! + 4, \ldots, n! + n$$

wszystkie liczby są złożone. Pierwsza liczba dzieli się przez 2, druga przez 3, a ostatnia przez n. Ciąg ten składa się z $n - 1$ liczb. Zawsze więc istnieje dowolnie długi (ale skończony) ciąg kolejnych liczb naturalnych złożonych.

Grupą nazywamy parę $(G, \circ)$, gdzie G jest niepustym zbiorem, natomiast $\circ : G \times G \to G$ jest działaniem spełniającym trzy warunki

(i) działanie jest **łączne**, tzn. dla wszystkich $a, b, c \in G$ zachodzi równość

$$(a \circ b) \circ c = a \circ (b \circ c), \tag{1.2}$$

(ii) w zbiorze G istnieje **element neutralny** e tego działania, czyli dla każdego a mamy

$$a \circ e = e \circ a = a,$$

(iii) dla każdego $a \in G$ istnieje **element odwrotny** a^{-1}, dla którego

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Spośród działań podanych w tabeli 1.1 środkowe nie jest łączne. Mamy na przykład $(a \circ b) \circ c = b$, natomiast $a \circ (b \circ c) = a$. Pozostałe dwa działania spełniają warunek (1.2)

Z warunku (ii) wynika, że w grupie istnieje dokładnie jeden element neutralny. Gdyby istniał drugi e', to musiałaby zachodzić równość

$$e = e \circ e' = e'.$$

Z (iii) wynika natomiast, że a^{-1} wyznaczony jest jednoznacznie. Załóżmy przeciwnie, że istnieją co najmniej dwa elementy odwrotne do a. Oznaczmy dwa z nich przez a_1^{-1}, a_2^{-1}. Wówczas mielibyśmy

$$a_2^{-1} = e \circ a_2^{-1} = (a_1^{-1} \circ a) \circ a_2^{-1} = a_1^{-1} \circ (a \circ a_2^{-1}) = a_1^{-1} \circ e = a_1^{-1}.$$

Ponieważ operacja $\circ$ jest binarna, to w jednym kroku możemy pomnożyć tylko dwa sąsiednie elementy. Jeśli mamy np. iloczyn $a \circ b \circ c \circ d$, to można obliczyć go na kilka sposobów. Warunek (1.2) zapewnia jednak, że wynik ten nie zależy od kolejności „wymnażania". Mianowicie, dla tych czterech elementów mamy

$$(a \circ b) \circ c \circ d = a \circ (b \circ c) \circ d = a \circ b \circ (c \circ d).$$

Pokażemy, że jest to prawdą w ogólnym przypadku.

Twierdzenie 1.1 *Jeśli działanie $\circ$ jest łączne, to iloczyn $a_1 \circ a_2 \circ \ldots \circ a_n$ nie zależy od kolejności mnożenia elementów.*

Dowód. Aby udowodnić, że końcowy wynik nie zależy od kolejności „wymnażania" elementów najlepiej jest określić ten iloczyn rekurencyjnie. Dla $k \geq 2$ zdefiniujmy

$$\prod_{i=1}^{k} a_i = (\prod_{i=1}^{k-1} a_i) \circ a_k. \tag{1.3}$$

Zatem $a_1 \circ a_2 \circ a_3 := (a_1 \circ a_2) \circ a_3$ oraz np.

$$a_1 \circ a_2 \circ a_3 \circ a_4 := ((a_1 \circ a_2) \circ a_3) \circ a_4.$$

Udowodnimy indukcyjnie, ż dla dowolnych $k, l \in \mathbb{N}$ zachodzi równość

$$(\prod_{i=1}^{k} a_i) \circ (\prod_{j=1}^{l} a_{k+j}) = \prod_{i=1}^{k+l} a_i. \tag{1.4}$$

Dowód indukcyjny przeprowadzimy względem l. Zakładając, że powyższy wzór jest prawdziwy pokażemy, że prawdziwy jest też dla $l+1$. Korzystając z definicji rekurencyjnej i łączności mamy

$$\begin{aligned}(\prod_{i=1}^{k} a_i) \circ (\prod_{j=1}^{l+1} a_{k+j}) &= (\prod_{i=1}^{k} a_i) \circ (\prod_{j=1}^{l} a_{k+j}) \circ a_{k+l+1} \\ &= (\prod_{i=1}^{k} a_i \circ \prod_{j=1}^{l} a_{k+j}) \circ a_{k+l+1} = (\prod_{i=1}^{k+l} a_i) \circ a_{k+l+1}\end{aligned}$$

Na podstawie (1.3) ostatni iloczyn wynosi $\prod_{i=1}^{k+l+1} a_i$ i tym samym wzór (1.4) został udowodniony. Z (1.4) wynika następnie, że gdziekolwiek w iloczynie $a_1 \circ \ldots \circ a_n$ wstawimy nawiasy, to wynik będzie zawsze taki sam. □

Dodajmy, że o ile iloczyn nie zależy od kolejności mnożenia, to często zależy od kolejności elementów, tzn. ogólnie $a \circ b \neq b \circ a$.

Dla $a \in G$ określamy $a^0 := e$ i dowolną potęgę naturalną

$$a^n := \underbrace{a \circ a \circ \ldots \circ a}_{n-razy}, \quad n \geq 1.$$

Z twierdzenia 1.1 otrzymujemy wzory

$$a^m \circ a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad m, n \geq 1.$$

Działania $m + n$ i mn, to zwykłe dodawanie i mnożenie w zbiorze liczb naturalnych. Potęgi ujemne definiujemy następująco

$$a^{-n} := (a^{-1})^n, \quad n \geq 1.$$

Z definicji tej i twierdzenia 1.1 wynika poniższe twierdzenie.

Twierdzenie 1.2 *Dla dowolnych $m, n \in \mathbb{Z}$ prawdziwe są wzory*

$$a^m \circ a^n = a^{m+n}, \quad a^m \circ a^n = a^n \circ a^m, \quad (a^m)^n = a^{mn}. \tag{1.5}$$

Z powyższych równości wynika na przykład, że $(a^{-1})^n = (a^n)^{-1}$. Mianowicie, z ostatniego wzoru w (1.5) mamy $(a^n)^{-1} = a^{-n}$, natomiast a^{-n} z definicji równa się $(a^{-1})^n$.

Grupę, w której liczba elementów jest skończona nazywamy **grupą skończoną**. Wówczas liczbę jej elementów nazywamy **rzędem** grupy i oznaczamy przez $|G|$. W przeciwnym razie piszemy $|G| = \infty$. Istnieją grupy o skończonej jak i nieskończonej liczbie elementów.

W grupach zachodzi prawo skracania, tzn. można „dzielić" obie strony przez dowolny element i wynika to z faktu, że każdy element jest odwracalny. Innymi słowy, równość $a = b$ jest równoważna równości $a \circ c = b \circ c$, gdzie c jest dowolne. Oto twierdzenie.

Twierdzenie 1.3 *Niech $(G, \circ)$ będzie grupą. Wówczas dla dowolnych elementów $a, b, c \in G$ spełnione są warunki*

(i) $(a \circ b = a \circ c) \Rightarrow b = c, \quad (b \circ a = c \circ a) \Rightarrow b = c,$

(ii) $(a^{-1})^{-1} = a, \quad (a \circ b)^{-1} = b^{-1} \circ a^{-1}.$

Dowód. Dówód pierwszej implikacji w (i). Jeśli $a \circ b = a \circ c$, to

$$b = (a^{-1} \circ a) \circ b = a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) = c.$$

Podobnie jest z drugą implikacją. Jeśli $b \circ a = c \circ a$, to mamy

$$b = b \circ (a \circ a^{-1}) = (b \circ a) \circ a^{-1} = (c \circ a) \circ a^{-1} = c.$$

Przechodzimy do dowodu (ii). Ponieważ $a^{-1} \circ a = e$ oraz

$$a^{-1} \circ (a^{-1})^{-1} = e,$$

to zgodnie z definicją elementu odwrotnego $(a^{-1})^{-1} = a$. Ponadto

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ a^{-1} = e,$$

zatem $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$. □

Jeśli $b = c$, to oczywiście $a \circ b = a \circ c$ i jak już powiedzieliśmy, z powyższego twierdzenia wynika, że w dowolnej grupie zachodzi równoważność

$$a \circ b = a \circ c \quad \Leftrightarrow \quad b = c.$$

Rozważmy równanie $a^2 = a$. Mnożąc tą równość stronami przez a^{-1} dostajemy $a = e$. Z drugiej strony $e^2 = e$, więc jedynym elementem grupy spełniającym warunek $a^2 = a$ jest element neutralny.

Załóżmy teraz, że $a \circ b = e$. Wtedy $b = a^{-1}$ i mnożąc obie strony tej równości prawostronnie przez a otrzymamy $b \circ a = e$. I odwrotnie, z równości $b \circ a = e$ dostaniemy $a \circ b = e$. Innymi słowy

$$\boxed{a \circ b = e \quad \Leftrightarrow \quad b \circ a = e.} \tag{1.6}$$

Rozumując podobnie, otrzymamy

$$\boxed{a^2 = e \quad \Leftrightarrow \quad a^{-1} = a.}$$

Równanie $a^2 = e$ może mieć w grupie wiele rozwiązań, np. w grupie $(\mathbb{R}^*, \cdot)$ mamy $(-1)^2 = (1)^2 = 1$. Natomiast w grupie z przykładu 1.2, gdzie działaniem jest różnica symetryczna, każdy element ma tą własność. W grupie tej każdy element jest więc odwrotny do siebie samego.

Udowodnimy teraz, że dla każdego $n \geq 2$ i dowolnych $a_1, \ldots, a_n \in G$ zachodzi wzór

$$\boxed{(a_1 a_2 \ldots a_{n-1} a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}.} \tag{1.7}$$

Korzystamy z indukcji. Dla $n = 2$ wzór jest prawdziwy na podstawie twierdzenia 1.3. Załóżmy teraz, że (1.7) zachodzi dla ustalonego $n \geq 3$. Pokażemy, że jest on prawdziwy także dla $n + 1$. Mamy kolejno

$$\begin{aligned}(a_1 \ldots a_n a_{n+1})^{-1} &= [(a_1 \ldots a_n) a_{n+1}]^{-1} = a_{n+1}^{-1} (a_1 \ldots a_n)^{-1} \\ &= a_{n+1}^{-1} a_n^{-1} \ldots a_1^{-1}.\end{aligned}$$

Ostatecznie wzór (1.7) jest prawdziwy dla każdej liczby naturalnej $n \geq 2$.

Działanie $\circ$ nazywamy działaniem **przemiennym**, jeśli spełniony jest warunek

$$\boxed{a \circ b = b \circ a, \quad \text{dla wszystkich } \ a, b \in G.}$$

Grupę $(G, \circ)$ nazywamy **przemienną** lub **abelową**, jeśli działanie $\circ$ jest przemienne. W takiej grupie mamy oczywiście $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$ oraz ogólnie

$$(a_1 a_2 \ldots a_{n-1} a_n)^{-1} = a_1^{-1} a_2^{-1} \ldots a_{n-1}^{-1} a_n^{-1},$$

przy czym w tym iloczynie można zmieniać kolejność elementów w dowolny spsoób. Działania w grupach przemiennych oznacza się w literaturze zwykle przez $+$, natomiast elementy odwrotne nazywa się przeciwnymi.

Ponieważ dodawanie i mnożenie liczb rzeczywistych i zespolonych jest łączne i przemienne, to $(\mathbb{C},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{Z},+)$ są grupami przemiennymi, w których element odwrotny do a to $-a$ nazywany w tym przypadku przeciwnym. Elementem neutralnym w tych grupach jest oczywiście zero. Podobnie $(\mathbb{C}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}_+,\cdot)$, $(\mathbb{Q}_+,\cdot)$ są przemienne z elementem neutralnym 1 i odwrotnym do a równym $1/a$.

Dla $a,b\in\mathbb{R}$ zdefiniujmy $a\circ b=ab+a+b$. Tak określone działanie jest łączne. Za jednej strony mamy

$$(a\circ b)\circ c=(ab+a+b)c+ab+a+b+c$$

oraz

$$a\circ(b\circ c)=a(bc+b+c)+a+bc+b+c,$$

i obie te wartości są równe. Elementem neutralnym tego działania jest zero, tzn. $a\circ 0=a$, natomiast odwrotny obliczamy z równania $ab+a+b=0$. Wynika stąd, że $b=-a/(a+1)$, zatem -1 nie jest odwracalny. W rezultacie $\mathbb{R}\backslash\{-1\}$ jest grupą przemienną. Rozpatrzymy teraz dwa bardziej złożone przykłady.

Przykład 1.1 W zbiorze $\mathbb{R}^*$ definiujemy działanie

$$a\circ b=\begin{cases} ab, & a>0\\ a/b, & a<0.\end{cases} \tag{1.8}$$

Pokażemy, że $(\mathbb{R}^*,\circ)$ jest grupą nieprzemienną. Zauważmy najpierw, że elementem neutralnym tego działania jest $e=1$, natomiast a^{-1} dane jest wzorem

$$a^{-1}=\begin{cases} 1/a, & a>0\\ a, & a<0.\end{cases}$$

Udowodnimy łączność. Formalnie musimy pokazać, że spełniony jest warunek (1.2) w ośmiu przypadkach, ponieważ działanie to zależy od znaku pierwszej liczby. Rozbijemy to na dwa podprzypadki. Jeśli $a>0$, to z jednej strony

$$(a\circ b)\circ c=(ab)\circ c=\begin{cases} abc, & ab>0\\ (ab)/c, & ab<0\end{cases}=\begin{cases} abc, & b>0\\ (ab)/c, & b<0,\end{cases}$$

i z drugiej mamy

$$a\circ(b\circ c)=a(b\circ c)=\begin{cases} abc, & b>0\\ (ab)/c, & b<0.\end{cases}$$

Jeśli $a < 0$, to

$$(a \circ b) \circ c = (a/b) \circ c = \begin{cases} (ac)/b, & a/b > 0 \\ a/(bc), & a/b < 0 \end{cases} = \begin{cases} (ac)/b, & b < 0 \\ a/(bc), & b > 0 \end{cases}$$

oraz

$$a \circ (b \circ c) = a/(b \circ c) = \begin{cases} a/(bc), & b > 0 \\ (ac)/b, & b < 0. \end{cases}$$

Tym samym warunek (1.2) jest spełniony i rozważany zbiór jest grupą. Zauważmy na koniec, że $\mathbb{R}_+$ jest podgrupą abelową tej grupy. □

Przykład 1.2 Niech X będzie dowolnym zbiorem, skończonym lub nieskończonym. **Różnica symetryczna** zbiorów zdefiniowana jest następujaco

$$\boxed{A \triangle B := (A \setminus B) \cup (B \setminus A), \quad A, B \subset X.}$$

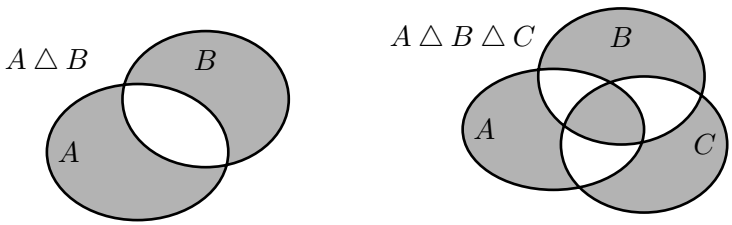
Bezpośrednio z definicji wynikają wzory

$$A \triangle \emptyset = A, \quad A \triangle A = \emptyset, \quad A \triangle B = B \triangle A. \tag{1.9}$$

Udowodnimy, że różnica symetryczna jest działaniem łacznym, tzn. dla dowolnych $A, B, C \subset X$ zachodzi równość

$$(A \triangle B) \triangle C = A \triangle (B \triangle C). \tag{1.10}$$

Odnotujmy, że zwykła różnica nie jest łączna, mamy bowiem $(A \setminus A) \setminus A = \emptyset$, natomiast $A \setminus (A \setminus A) = A$. W kwestii oznaczeń, dopełnienie zbioru A oznacza-



Rys. 1.1 Różnica symetryczna zbiorów.

my przez A^c, tzn. $A^c := X \setminus A$. Mamy więc $A \cup A^c = X$, $A \cap A^c = \emptyset$, $(A^c)^c = A$ oraz $A \setminus B = A \cap B^c$. Prawa de Morgana mówią, że $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$. Prawa rozdzielności to $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Przechodzimy do dowodu (1.10).

W pierwszym kroku zauważmy, że

$$A \triangle B = (A \cap B^c) \cup (B \cap A^c) = (A \cup B) \cap (A^c \cap B^c),$$

gdzie ostatnia równość wynika z praw rozdzielności. Następnie z praw de Morgana mamy $(A \triangle B)^c = (A^c \cup B) \cap (A \cup B^c)$ i po dalszych przekształceniach otrzymamy

$$\begin{aligned}(A \triangle B) \triangle C =& (A \cup B \cup C) \cap (A \cup B^c \cup C^c) \\ & \cap (A^c \cup B \cup C^c) \cap (A^c \cup B^c \cup C).\end{aligned}$$

Ponieważ suma i iloczyn zbiorów są działaniami łącznymi, zatem

$$\begin{aligned}(B \cup C \cup A) \cap (B^c \cup C^c \cup A) \cap (B \cup C^c \cup A^c) \cap (B^c \cup C \cup A^c) \\ = (B \triangle C) \triangle A = A \triangle (B \triangle C).\end{aligned}$$

Powyższa równość kończy dowód (1.10). Tym samym pokazaliśmy, że $(2^X, \triangle)$ jest grupą przemienną, gdzie 2^X jest rodziną wszystkich podzbiorów zbioru X. Elementem neutralnym w tej grupie jest zbiór pusty a zbiorem odwrotnym do A jest A. □

Jeśli $|X| = n$, to rodzina 2^X składa się z 2^n podzbiorów, wliczając w to zbiór pusty i X. Wynika to na przykład ze wzoru $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. Symbol Newtona $\binom{n}{k}$ zdefiniowany jest jako $\frac{n!}{k!(n-k)!}$ i liczba ta jest liczbą podzbiorów k-elementowych X. Własność $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ zapewnia, że $\binom{n}{k}$ jest liczbą naturalną dla dowolnego $n \geq k$.

Jeśli $X = \{a, b\}$, to grupa $(2^X, \triangle)$ nazywana jest **grupą czwórkową** Kleina i ma postać

$$2^X = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}. \tag{1.11}$$

Grupę tą oznacza się zwykle przez V_4. Istnieje wiele grup, których tabela działania wygląda podobnie do tabeli 1.2. Wszystkie te grupy są izomorficzne. Intuicyjnie oznacza to, że ich elementy zachowują się „tak samo". Izomorfizm grup zostanie zdefiniowany w rozdziale 2.

Jeśli grupa jest skończona, to podnosząc ustalony element do kolejnych potęg w końcu dostaniemy element neutralny. W przeciwnym razie zbiór G byłby nieskończony. W grupie o nieskończonej liczbie elementów może też tak być, ale nie zawsze. Definiujemy więc **rząd elementu** następująco

$$\boxed{rz(a) := \min\{n \geq 1 : a^n = e\}.} \tag{1.12}$$

Tabela 1.2 Tabela Cayleya grupy czwórkowej $2^{\{a,b\}}$.

$\triangle$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a,b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\emptyset$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\emptyset$

Jeśli nie ma takiego n, że $a^n = e$, to piszemy $rz(a) = \infty$. Zauważmy, że jeśli dla pewnego m zachodzi równość $a^m = e$, to możemy tylko wywnioskować, że $rz(a) \leq m$. Rząd e równa się oczywiście 1.

Twierdzenie 1.4 *Dla dowolnych $a, b \in G$ zachodzą równości*

$$rz(a) = rz(a^{-1}), \quad rz(ab) = rz(ba). \tag{1.13}$$

Dowód. Zaczniemy od dowodu pierwszego wzoru. Przyjmijmy na razie, że $rz(a) = n_1 < \infty$. Wówczas $(a^{-1})^{n_1} = (a^{n_1})^{-1} = e^{-1} = e$ i stąd

$$rz(a^{-1}) \leq n_1 = rz(a).$$

Niech $rz(a^{-1}) = n_2$. Wówczas mamy

$$a^{n_2} = (a^{-1})^{-n_2} = [(a^{-1})^{n_2}]^{-1} = e,$$

czyli $rz(a) \leq rz(a^{-1})$ i ostatecznie $rz(a) = rz(a^{-1})$.

Niech teraz $rz(a) = \infty$. Pokażemy, że wtedy również $rz(a^{-1}) = \infty$. Aby to wykazać załóżmy przeciwnie, że $rz(a^{-1}) = n_3 < \infty$. W takim razie $a^{n_3}(a^{-1})^{n_3} = e$, stąd $a^{n_3} = e$ i w rezultacie $rz(a) < \infty$. Innymi słowy, sytuacja, w której $rz(a) = \infty$ i $rz(a^{-1}) < \infty$ jest niemożliwa.

Przechodzimy do dowodu drugiego wzoru. Niech $rz(ab) = n < \infty$. Wtedy z równości $(ab)^{n-1} = b^{-1}a^{-1}$, która wynika z $(ab)^n = e$, mamy

$$(ba)^n = b(ab)^{n-1}a = bb^{-1}a^{-1}a = e,$$

zatem $rz(ba) \leq rz(ab)$. Wynika stąd, że również $rz(ab) \leq rz(ba)$. To kończy dowód drugiej równości w (1.13) dla skończonych rzędów. Jeśli $rz(ab) = \infty$, to podobnie jak wcześniej wnioskujemy, że $rz(ba) = \infty$. □

Przykład 1.3 Dla grupy z przykładu 1.1, w której jedynka jest elementem neutralnym mamy

$$a^2 = a \circ a = \begin{cases} a^2, & a > 0 \\ 1, & a < 0. \end{cases}$$

Wynika stąd, że

$$rz(a) = \begin{cases} \infty, & a > 0, a \neq 1, \\ 1, & a = 1, \\ 2, & a < 0. \end{cases}$$

W szczególności $rz(-2) = rz(-3) = 2$, ale $rz(2/3) = \infty$. Taka sytuacja nie może się zdarzyć w grupach abelowych, patrz twierdzenie 1.5. □

Twierdzenie 1.5 *Jeśli G jest grupą przemienną to*

$$(a \circ b)^n = a^n \circ b^n, \quad \forall\, n \geq 1. \tag{1.14}$$

W rezultacie, jeśli $rz(a) < \infty$ i $rz(b) < \infty$, to $rz(a \circ b) < \infty$.

Dowód. Dla $n = 1$ wzór ten jest tożsamością. Załóżmy teraz, że powyższy wzór jest prawdziwy dla pewnego $n \geq 2$. W takim razie mamy

$$\begin{aligned}(a \circ b)^{n+1} &= (a \circ b)^n \circ (a \circ b) = a^n \circ b^n \circ a \circ b \\ &= a^n \circ a \circ b^n \circ b = a^{n+1} \circ b^{n+1},\end{aligned}$$

a to dowodzi prawdziwości (1.14) dla każdego $n \in \mathbb{N}$.

Niech teraz $rz(a) = n_1$, $rz(b) = n_2$. Wtedy

$$(a \circ b)^{n_1 n_2} = a^{n_1 n_2} \circ b^{n_1 n_2} = e.$$

Oznacza to, że $rz(a \circ b) \leq n_1 n_2$. □

Niepusty podzbiór $H \subset G$ nazywamy **podgrupą** grupy $(G, \circ)$, jeśli para $(H, \circ)$ tworzy grupę. Oznacza to, że H jest „zamknięty" w tym sensie, że działanie nie wyprowadza elementów poza ten zbiór. Innyi słowy, jeśli a i b należą do H, to również $a \circ b \in H$ i $a^{-1} \in H$. Łączność w H jest spełniona, gdyż spełniona jest w całej grupie. Na przykład

$$H_1 = (G, \circ), \quad H_2 = (\{e\}, \circ)$$

są zawsze podgrupami i nazywane się **podgrupami niewłaściwymi**. Wszystkie inne to **podgrupy właściwe**. Dana grupa może nie zawierać żadnej podgrupy właściwej. Z drugiej strony, jeśli liczba elementów w grupie skończonej spełnia pewne warunki, to podgrupy właściwe zawsze istnieją, mówi o tym np. twierdzenie Cachy'ego. Z kolei w każdej grupie nieskończonej istnieje nieskończenie wiele podgrup właściwych, patrz przykład 1.5.

Twierdzenie 1.6 *Niech $(G, \circ)$ będzie grupą. Niepusty podzbiór $H \subset G$ jest podgrupą grupy G wtedy i tylko wtedy, gdy spełniony jest warunek*

$$a, b \in H \;\Rightarrow\; a \circ b^{-1} \in H. \tag{1.15}$$

Dowód. Jeśli H jest podgrupą grupy G, to warunek (1.15) jest spełniony na podstawie definicji. Udowodnimy teraz, że zachodzi implikacja w drugą stronę, tzn. że jeśli podzbiór H spełnia warunek (1.15), to jest podgrupą.

Niech $a \in H$. Wówczas $a \circ a^{-1} = e$, zatem $e \in H$. Ponieważ $e \circ a^{-1} = a^{-1}$, więc $a^{-1} \in H$. Wynika stąd, że jeśli $a, b \in H$, to

$$a \circ b = a \circ (b^{-1})^{-1} \in H$$

Zatem H jest „zamknięty" ze względu na działanie $\circ$, mnożąc dowolne jego elementy nie wyjdziemy poza H. Oznacza to, że H jest podgrupą. □

Twierdzenie 1.7 *Jeśli $\mathcal{H}$ jest niepustą rodziną podgrup grupy G, to iloczyn $\bigcap_{H\in\mathcal{H}} H$ jest także podgrupą grupy G.*

Dowód. Po pierwsze łatwo widać, że $e \in \bigcap_{H\in\mathcal{H}} H$, ponieważ element neutralny należy do każdej podgrupy. Następnie, jeśli $a, b \in \bigcap_{H\in\mathcal{H}} H$, to znowu $a, b \in H$, dla każdego H z rodziny $\mathcal{H}$. Stąd na podstawie twierdzenia 1.6 mamy $a \circ b^{-1} \in H$, dla każdego $H \in \mathcal{H}$. Zatem $a \circ b^{-1} \in \bigcap_{H\in\mathcal{H}} H$ i przecięcie to jest podgrupą. □

Twierdzenie 1.7 pozwala na zdefiniowanie najmniejszej grupy zawierającej dany zbiór elementów. Niech A będzie podzbiorem grupy G. Najmniejszą podgrupę grupy G zawierającą zbiór A nazywamy **podgrupą generowaną przez** A i oznaczamy przez $\langle A\rangle$. Zatem

$$\langle A\rangle := \bigcap_{H\in\mathcal{H}_A} H,$$

gdzie $\mathcal{H}_A$ jest rodziną podgrup G zawierających A. Rodzina ta, niezależnie od zbioru A, zawiera zawsze przynajmniej jeden element, ponieważ $G \in \mathcal{H}_A$. W najlepszym przypadku otrzymamy więc $\langle A\rangle = G$. Jeśli podzbiór A jest już podgrupą, to oczywiście $\langle A\rangle = A$. Jeśli $A = \{a_1, \ldots, a_n\}$, to używamy oznaczenia $\langle A\rangle = \langle a_1, \ldots, a_n\rangle$.

Grupę G nazywamy **grupą cykliczną**, jeśli jest generowana przez jeden element, tzn. $G = \langle a\rangle$. Innymi słowy, w grupie cyklicznej występują potęgi tylko jednego elementu. Zbiór elementów takiej grupy może być co najwyżej przeliczalny. Można więc napisać

$$G = \langle a\rangle = \{a^n : n \in \mathbb{Z}\}.$$

Element a nazywa się wtedy **generatorem** grupy cyklicznej. Z twierdzenia 1.2 wynika, że każda grupa cykliczna jest przemienna. Możliwe są tutaj dwa przypadki: skończony i nieskończony.

Jeśli wszystkie potęgi są różne, to $|G| = \infty$. Przykładem takiej grupy jest np. zbiór potęg dwójki $\{2^n : n \in \mathbb{Z}\}$ z mnożeniem jako działaniem grupowym lub też zbiór liczb całkowitych z dodawaniem.

Druga możliwość jest taka, że pewne dwie potęgi są równe, czyli $a^k = a^l$ dla pewnych $k > l$. Wówczas $a^k a^{-l} = e$ i stąd otrzymujemy, że $a^{k-l} = e$ oraz $k - l > 0$. Pokażemy, że wtedy $G = \{e, a, a^2, \ldots, a^{n-1}\}$, gdzie

$$n = \min\{m \geq 1 : a^m = e\}.$$

Przede wszystkim zauważmy, że wszystkie elementy w G są różne. W przeciwnym razie, gdyby $a^{k_1} = a^{l_1}$ dla $k_1 > l_1$ wraz z $k_1, l_1 \in \{0, 1, \ldots, n-1\}$, to wówczas $a^{k_1 - l_1} = e$, przy czym $k_1 - l_1 < n$ i mielibyśmy sprzeczność. Następnie, jeśli m jest dowolną liczbą całkowitą, to $m = qn + r$, gdzie $q \in \mathbb{Z}$ oraz $r \in \{0, 1, \ldots, n-1\}$. Stąd mamy

$$a^m = a^{qn+r} = (a^n)^q a^r = ea^r = a^r \in G.$$

Grupę cykliczną rzędu n oznacza się zwykle przez C_n i ma ona zawsze postać

$$\boxed{C_n = \{e, a, a^2, \ldots, a^{n-1}\}.}$$

Działanie w niej określone jest następująco

$$a^k \circ a^l = \begin{cases} a^{k+l}, & k + l < n, \\ a^{k+l-n}, & k + l \geq n. \end{cases}$$

Przykład 1.4 (a) Niech $G = \mathbb{C}^*$ oraz H będzie podzbiorem składającym się liczb leżących na okręgu o promieniu 1, tzn.

$$H = \{z \in \mathbb{C}^* : |z| = 1\}.$$

Moduł liczby $z = x + iy$ dany jest wzorem

$$|z| = \sqrt{x^2 + y^2}.$$

Jeśli $|z_1| = 1$ i $|z_2| = 1$, to z własności modułu otrzymujemy

$$|z_1 z_2| = |z_1| \cdot |z_2| = 1, \quad |z_1^{-1}| = |z_1|^{-1} = 1.$$

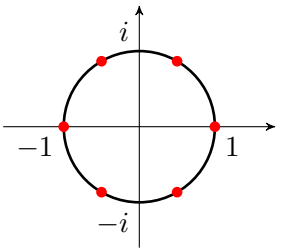
Zatem H jest podgrupą G. Dodajmy, że H jest zbiorem nieprzeliczalnym.
(b) Dla każdego $n \geq 2$ zbiór pierwiastków zespolonych z 1, czyli zbiór

$$\sqrt[n]{1} = \left\{1, z_0, z_0^2, \ldots, z_0^{n-1}\right\}, \tag{1.16}$$

gdzie $z_0 = \cos(2\pi/n) + i\sin(2\pi/n)$, jest grupą cykliczną rzędu n. Korzystając z wzoru de Moivre'a $z_0^k = \cos(2k\pi/n) + i\sin(2k\pi/n)$. Na przykład dla $n = 2$ i $n = 4$ mamy więc

$$\sqrt[2]{1} = \{1, -1\}, \quad \sqrt[4]{1} = \{1, i, -1, -i\}.$$

Jeśli $|z| \neq 1$, to zbiór pierwiastków stopnia n z z nie tworzy grupy. Mianowicie, jeśli $w_1^n = z$ i $w_2^n = z$, to $(w_1 w_2)^n \neq z$. Wynika to z tego, że w tym przypadku $|w_1|^n = |z|$ i $|w_2|^n = |z|$, natomiast $|w_1 w_2|^n = |z|^2$. □



Rys. 1.2 Zbiór punktów leżących na okręgu jednostkowym jest podgrupą $\mathbb{C}^*$.

Przykład 1.5 (a) Niezależnie od tego czy G jest grupą cykliczną, zbiór wszystkich potęg ustalonego elementu jest podgrupą G. W tym przypadku $H = \{a^n : n \in \mathbb{Z}\}$ i z twierdzenia 1.2 mamy $a^m \circ a^n = a^{m+n}$, dla dowolnych $m, n \in \mathbb{Z}$. Innymi słowy, nie wyjdziemy poza zbiór H i jak zauważyliśmy wcześniej jest on co najwyżej przeliczalny.

(b) Pokażemy, że każda grupa nieskończona ma podgrupy właściwe. Niech więc $|G| = \infty$. Możliwe są dwa przypadki. W pierwszym przypadku istnieje element $a \in G$, dla którego $rz(a) = \infty$. Wówczas na przykład podgrupa

$$\langle a^2 \rangle = \{\ldots, a^{-4}, a^{-2}, e, a^2, a^4, \ldots\}$$

jest właściwa, ponieważ nie zawiera elementu a. Gdyby zachodziła równość $a^{2n} = a$, dla pewnego $n \geq 2$, to oznaczałoby to, że rząd a jest skończony wbrew założeniu.

Drugi przypadek jest taki, że G jest torsyjna, czyli rząd każdego elementu jest skończony. Bierzemy wtedy dowolny a, dla którego $rz(a) > 1$. Podgrupa $\langle a \rangle$ jest skończona i dlatego jest właściwa. □

Niech A i B są niepustymi podzbiorami grupy G. **Iloczynem algebraicznym** lub **iloczynem kompleksowym** A i B nazywamy zbiór

$$AB := \{ab : a \in A, b \in B\}. \tag{1.17}$$

Mnożenie algebraiczne jest łączne i wynika z łączności działania grupowego. Zatem $(AB)C = A(BC)$, dla dowolnych $A, B, C \subset G$. W grupach abelowych jest ponadto działaniem przemiennym. Jeśli jeden ze zbiorów jest jednoelementowy, to zamiast $\{a\}A$ piszemy aA. Zauważmy, że $eA = Ae$, zatem zbiór $\{e\}$ jest elementem neutralnym tego działania. Jeśli przyjmiemy, że

$$A^{-1} := \{a^{-1} : a \in A\},$$

to ogólnie $AA^{-1} \neq \{e\}$. Wynika stąd, że rodzina wszystkich podzbiorów grupy G z działaniem określonym przez (1.17) nie jest grupą. Mamy jednak następującą własność

$$AG = GA = G, \quad \forall\, A \subset G. \tag{1.18}$$

Jeśli $a \in A$ i $g \in G$, to oczywiście $ag \in G$. Zatem $AG \subset G$. Z drugiej strony

$$g = a(a^{-1}g) \in AG \quad \Rightarrow \quad G \subset AG.$$

Ostatecznie $AG = G$. Podobnie dowodzi się równości $GA = G$. Zauważmy, że jeśli H jest podgrupą grupy G, to

$$H^2 = HH = H.$$

W twierdzeniu 1.7 udowodniliśmy, że zwykły iloczyn podgrup jest także podgrupą. Nie jest to ogólnie prawdą dla iloczynu algebraicznego.

Twierdzenie 1.8 *Jeśli H_1 i H_2 są podgrupami grupy G, to iloczyn algebraiczny H_1H_2 jest podgrupą grupy G wtedy i tylko wtedy, gdy*

$$H_1H_2 = H_2H_1. \tag{1.19}$$

Dowód. Dowód implikacji $\Rightarrow$. Zakładamy więc, że H_1, H_2 i H_1H_2 są podgrupami. Weźmy dowolny $h \in H_2H_1$. Wówczas $h = h_2h_1$, dla pewnych $h_2 \in H_2$, $h_1 \in H_1$. Ponieważ H_1H_2 jest podgrupą, to mamy

$$h = h_2h_1 = (h_1^{-1}h_2^{-1})^{-1} \in H_1H_2.$$

Zatem $H_2H_1 \subset H_1H_2$. Niech teraz $h' \in H_1H_2$. Wtedy $h' = h_3h_4$, dla pewnych $h_3 \in H_1$, $h_4 \in H_2$. Podobnie jak wcześniej

$$(h')^{-1} = (h_3h_4)^{-1} = h_4^{-1}h_3^{-1} \in H_2H_1.$$

Stąd $H_1H_2 \subset H_2H_1$ i w rezultacie mamy (1.19).

Dowód implikacji $\Leftarrow$. Zakładamy, że H_1, H_2 są podgrupami i zachodzi (1.19). Pokażemy, że wtedy H_1H_2 jest też podgrupą. Z łączności i założeń otrzymujemy

$$(H_1H_2)^2 = H_1(H_2H_1)H_2 = H_1(H_1H_2)H_2 = H_1^2H_2^2 = H_1H_2.$$

Wynika stąd, że jeśli $h, h' \in H_1H_2$, to również $hh' \in H_1H_2$. Ponadto

$$h^{-1} = (h_1h_2)^{-1} = h_2^{-1}h_1^{-1} \in H_2H_1 = H_1H_2,$$

gdzie $h_1 \in H_1$, $h_2 \in H_2$. Z twierdzenia 1.6 wynika więc, że H_1H_2 jest podgrupą grupy G. $\square$

Niezależnie od tego czy H_1H_2 jest podgrupą, jeśli tylko H_1 i H_2 są podgrupami skończonymi pewnej grupy, to prawdziwy jest wzór

$$|H_1H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}, \tag{1.20}$$

który udowodnimy w rozdziale 3, patrz twierdzenie 3.6. Teraz sprawdzimy powyższą tożsamość na przykładzie pierwiastków zespolonych z jedynki.

Przykład 1.6 Dla dowolnych $n, m \geq 2$ prawdą jest oczywiście

$$\sqrt[n]{1} \cdot \sqrt[m]{1} = \sqrt[m]{1} \cdot \sqrt[n]{1},$$

gdzie $\sqrt[n]{1}$ dany przez (1.16) traktujemy jak zbiór. Z twierdzenia 1.8 wynika, że $\sqrt[n]{1} \cdot \sqrt[m]{1}$ jest podgrupą $\mathbb{C}^*$. Liczbę elementów tej podgrupy można obliczyć wykorzystując wzór (1.20). Dla $n = 2$ i $m = 3$ mamy

$$\sqrt[2]{1} = \{1, -1\}, \quad \sqrt[3]{1} = \{1, -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i\}.$$

W tym przypadku $\sqrt[2]{1} \cap \sqrt[3]{1} = \{1\}$, więc $\sqrt[2]{1} \cdot \sqrt[6]{1}$ składa się z sześciu elementów i są to pierwiastki stopnia 6 z jedynki

$$\sqrt[2]{1}\sqrt[3]{1} = \{1, \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, -1, -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i, \tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i\} = \sqrt[6]{1}.$$

Dla $\sqrt[4]{1} = \{1, i, -1, -i\}$ mamy $\sqrt[4]{1} \cap \sqrt[6]{1} = \{-1, 1\}$, zatem grupa $\sqrt[4]{1} \cdot \sqrt[6]{1}$ składa się z 12 elementów

$$\begin{aligned}\sqrt[4]{1}\sqrt[6]{1} = \{&1, \tfrac{\sqrt{3}}{2} + \tfrac{1}{2}i, \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, i, -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, -\tfrac{\sqrt{3}}{2} + \tfrac{1}{2}i, -1,\\ &- \tfrac{\sqrt{3}}{2} - \tfrac{1}{2}i, -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i, -i, \tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i, \tfrac{\sqrt{3}}{2} - \tfrac{1}{2}i\} = \sqrt[12]{1}.\end{aligned}$$

Tym razem są to pierwiastki stopnia 12 z jedynki. $\square$

Grupę, w której rząd każdego elementu jest skończony nazywa się grupą **torsyjną**. W rozdziale 3 pokażemy, że każda grupa skończona jest torsyjna. Będzie to wniosek z twierdzenia Lagrange'a. Teraz podamy dwa przykłady nieskończonych grup torsyjnych.

Przykład 1.7 (a) Jeśli X jest zbiorem nieskończonym, to zbiór potęgowy 2^X jest też nieskończony i $(2^X, \triangle)$ jest grupą przemienną, patrz przykład 1.2. W tym przypadku $rz(A) = 2$, dla każdego $A \subset 2^X$ niebędącego zbiorem pustym.

(b) Wiemy już, że zbiór pierwiastków zespolonych stopnia n z jedynki jest grupą oraz, że $\sqrt[n]{1} \cdot \sqrt[m]{1}$ również jest grupą. Zbiór wszystkich pierwiastków z jedynki

$$G = \bigcup_{n=1}^{\infty} \sqrt[n]{1} = \bigcup_{n=1}^{\infty} \{z \in \mathbb{C} : z^n = 1\}$$

także jest grupą, której wszystkie elementy znajdują się na okręgu jednostkowym o środku w punkie $(0, 0)$. Jeśli bowiem $z_1, z_2 \in G$, to $z_1^{n_1} = 1$, $z_2^{n_2} = 1$, dla pewnych $n_1, n_2 \in \mathbb{N}$. Wynika stąd, że $(z_1 z_2)^{n_3} = 1$, gdzie $n_3 = \mathrm{NWW}(n_1, n_2)$. Innymi słowy, rząd każdego elementu jest skończony. Jest to więc grupa torsyjna. Dodajmy, że G jest zbiorem przeliczalnym. □

Podgrupa właściwa H nazywana jest **podgrupą maksymalną** grupy G, jeśli z faktu, że H zawiera się w innej podgrupie H' wynika, że $H' = G$. W języku matematyki musi zachodzić implikacja

$$H \subset H' \subset G \quad \Rightarrow \quad H = H'.$$

Rozważmy przykład. Zbiór liczb parzystych $2\mathbb{Z}$ jest podgrupą właściwą $\mathbb{Z}$. Jeśli $2\mathbb{Z} \subset H$ i $H \neq 2\mathbb{Z}$, to do H musi należeć przynajmniej jedna liczba nieparzysta, powiedzmy 11. Ale wtedy $11 - 10 = 1 \in H$ i stąd $H = \mathbb{Z}$, ponieważ $\langle 1, 2\mathbb{Z} \rangle = \mathbb{Z}$. Zatem $2\mathbb{Z}$ jest podgrupą maksymalną $\mathbb{Z}$. Można łatwo pokazać, że jeśli p jest liczbą pierwszą, to $p\mathbb{Z}$ też jest maksymalna. Natomiast $4\mathbb{Z}$, czyli zbiór wielokrotności 4 podgrupą maksymalną w $\mathbb{Z}$ nie jest, ponieważ $4\mathbb{Z} \subset 2\mathbb{Z}$ i oczywiście $4\mathbb{Z} \neq 2\mathbb{Z}$.

1.2 Grupy reszt $\mathbb{Z}_p$ i $\mathbb{Z}_p^*$

Niech $x \in \mathbb{R}$. Symbol $\lfloor x \rfloor$ oznacza **podłogę** lub **całość** z x, czyli największą liczbę całkowita nieprzekraczającą x. Formalna definicja wygląda tak

$$\lfloor x \rfloor := \max\{n \in \mathbb{Z} : n \leq x\}.$$

Na przykład

$$\lfloor 5.4 \rfloor = 5, \quad \lfloor -1.2 \rfloor = -2, \quad \lfloor -3 \rfloor = -3.$$

Funkcja **sufit**, oznaczana przez $\lceil x \rceil$, dana jest przez

$$\lceil x \rceil := \min\{n \in \mathbb{Z} : n \geq x\}.$$

Jest to zatem najmniejsza liczba całkowita nie większa od x. Oto przykłady

$$\lceil 5.4 \rceil = 6, \quad \lceil -1.2 \rceil = -1, \quad \lceil -3 \rceil = -3.$$

Dla tych funkcji prawdziwe są nierówności

$$x - 1 < \lfloor x \rfloor \leq x, \qquad x \leq \lceil x \rceil < x + 1, \qquad x \in \mathbb{R}.$$

Algorytm dzielenia w zbiorze liczb całkowitych zamieszczamy w poniższym twierdzeniu. Dowód oraz więcej informacji można znaleźć np. w [12].

Twierdzenie 1.9 *Niech p będzie liczbą naturalną większą od 1. Wówczas dowolną liczbę $n \in \mathbb{Z}$ można przedstawić jednoznacznie w postaci*

$$n = p \cdot q + r, \tag{1.21}$$

gdzie $q \in \mathbb{Z}$ oraz $r \in \{0, 1, \ldots, p-1\}$.

Liczbę q we wzorze (1.21) nazywa się ilorazem, natomiast r resztą z dzielenia n przez p. Liczby te można zapisać za pomocą podłogi i sufitu. Mianowicie, dla ustalonego $p \geq 2$ definiujemy funkcję $\operatorname{div} p : \mathbb{Z} \to \mathbb{Z}$ wzorem

$$n \operatorname{div} p := \left\lfloor \tfrac{n}{p} \right\rfloor. \tag{1.22}$$

Funkcja ta nazywana jest **dzieleniem całkowitym**. Oznaczmy

$$\boxed{\mathbb{Z}_p = \{0, 1, \ldots, p-1\}.}$$

Resztą modulo p nazywamy funkcję $\operatorname{mod} p : \mathbb{Z} \to \mathbb{Z}_p$ określoną wzorem

$$n \bmod p := \left(\tfrac{n}{p} - n \operatorname{div} p\right) p.$$

Wzór (1.21) można więc zapisać w postaci

$$n = (n \operatorname{div} p)p + n \bmod p. \tag{1.23}$$

Poniżej dwa przykłady

$$41 \operatorname{div} 7 = \lfloor \tfrac{41}{7} \rfloor = 5, \quad -41 \operatorname{div} 7 = \lfloor \tfrac{-41}{7} \rfloor = -6.$$

Relacja **kongruencji** lub **przystawania modulo** p w zbiorze liczb całkowitych określona jest następująco. Liczby n i m są w relacji, jeśli dają takie same reszty z dzielenia przez p. Wówczas ich różnica podzielna jest przez p. Zatem

$$\boxed{m \equiv n \,(\mathrm{mod} p) \quad \Leftrightarrow \quad m - n = k \cdot p,}$$

dla pewnego $k \in \mathbb{Z}$. Relacja ta jest relacją równoważności i dzieli zbiór $\mathbb{Z}$ na $p-1$ klas abstrakcji. Są to liczby dające resztę 1 z dzielenia przez p, liczby dające resztę 2, aż do liczb dających resztę $p-1$.

Z (1.23) wynika równość $(n \operatorname{div} p) \cdot p = n - (n \bmod p)$, zatem

$$\boxed{n \bmod p \equiv n \,(\mathrm{mod} p), \quad \forall\, n \in \mathbb{Z}.} \tag{1.24}$$

Dla $a, b \in \mathbb{Z}_p$ zdefiniujmy

$$\boxed{a +_p b := (a + b) \bmod p, \qquad a *_p b := (a \cdot b) \bmod p.} \tag{1.25}$$

Elementem neutralnym $+_p$ jest 0, tzn. $a +_p 0 = a$. Ponadto $a +_p (p - a) = 0$, dla każdego $a \in \mathbb{Z}_p$. Elementem neutralnym mnożenia $*_p$ jest natomiast 1, czyli $a *_p 1 = a$, gdzie $a \in \mathbb{Z}_p$. Własności kongruencji z następującego twierdzenia wykorzystamy do wykazania, że tak określone działania sa łączne.

Twierdzenie 1.10 *Załóżmy, że $a, b, c, d \in \mathbb{Z}$ i $p \geq 2$. Wówczas*

(i) *jeśli $a \equiv b \,(\mathrm{mod} p)$, $c \equiv d \,(\mathrm{mod} p)$, to*

$$a + c \equiv b + d \,(\mathrm{mod} p), \quad a \cdot c \equiv b \cdot d \,(\mathrm{mod} p),$$

(ii) $a \bmod p + b \bmod p \equiv a + b \,(\mathrm{mod} p)$,

(iii) $(a \bmod p) \cdot (b \bmod p) \equiv a \cdot b \,(\mathrm{mod} p)$,

(iv) $(a + b) \bmod p = (a \bmod p) +_p (b \bmod p)$,

(v) $(a \cdot b) \bmod p = (a \bmod p) *_p (b \bmod p)$.

Dowód. Dowód (i). Z założenia mamy

$$a - b = k_1 p, \quad c - d = k_2 p,$$

dla pewnych $k_1, k_2 \in \mathbb{Z}$. Dodając równości stronami otrzymujemy

$$(a + c) - (b + d) = (k_1 + k_2)p$$

i stąd wynika pierwsza tożsamość. Następnie mnożąc stronami równania mamy

$$ac - bd = (bk_2 + k_1 d + k_1 k_2 p)p.$$

co dowodzi drugiej tożsamości. Dowód (ii) i (iii). Z (1.24) mamy

$$a \bmod p \equiv a \,(\mathrm{mod} p), \quad b \bmod p \equiv b \,(\mathrm{mod} p).$$

Zatem (ii) i (iii) wynika z punktu (i).

Dowód (iv). Z definicji

$$(a \bmod p) +_p (b \bmod p) = (a \bmod p + a \bmod p) \bmod p.$$

Własność (ii) oznacza, że

$$(a \bmod p + a \bmod p) \bmod p = (a + b) \bmod p$$

i to dowodzi (iv).

Dowód (v). Z definicji

$$(a \bmod p) *_p (b \bmod p) = [(a \bmod p) \cdot (b \bmod p)](\mathrm{mod} p).$$

Własność (iii) równoważna jest

$$[(a \bmod p) \cdot (b \bmod p)](\mathrm{mod} p) = (a \cdot b)(\mathrm{mod} p)$$

i to kończy dowód (v). □

Dodawanie modulo p określone przez (1.25) można równoważnie zdefiniować w następujący sposób

$$a +_p b = \begin{cases} a + b, & a + b < p, \\ a + b - p, & a + b \geq p. \end{cases}$$

Jesteśmy gotowi do udowodnienia, że $+_p$ i $*_p$ są działaniami przemiennymi i łącznymi, ale zanim sformułujemy twierdzenie rozważmy przykład. Niech $p = 8$ i weźmy $a = 3, b = 6, c = 7$. Wówczas

$$(3 +_8 6) +_8 7 = 1 +_8 7 = 0.$$

Z drugiej strony

$$3 +_8 (6 +_8 7) = 3 +_8 5 = 0.$$

Twierdzenie 1.11 *Dla dowolnych $a, b, c \in \mathbb{Z}_p$ zachodzą równości*

(i) $a +_p b = b +_p a$, $a *_p b = b *_p a$,

(ii) $(a +_p b) +_p c = a +_p (b +_p c)$, $(a *_p b) *_p c = a *_p (b *_p c)$.

Dowód. Dowód (i) wynika z definicji (1.25) oraz faktu, że zwykłe dodawanie i mnożenie jest przemienne. Przechodzimy do dowodu (ii). Z oczywistej równości

$$[(a + b) + c] \bmod p = [a + (b + c)] \bmod p$$

oraz z punktu (iv) twierdzenia 1.10 otrzymujemy

$$\begin{aligned}[(a + b) + c] \bmod p &= [(a + b) \bmod p] +_p (c \bmod p) \\ &= [(a \bmod p) +_p (b \bmod p)] +_p (c \bmod p) \\ &= (a +_p b) +_p c.\end{aligned}$$

Podobnie mamy

$$\begin{aligned}[a + (b + c)] \bmod p &= (a \bmod p) +_p [(b + c) \bmod p)] \\ &= (a \bmod p) +_p [(b \bmod p) +_p (c \bmod p)] \\ &= a +_p (b +_p c).\end{aligned}$$

Tym samym łączności dodawania modulo p została wykazana. Podobnie dowodzi się łączności $*_p$. □

Z twierdzenia 1.10 i 1.11 wynika, że zbiór $\mathbb{Z}_p$ wraz z działaniem $+_p$ określonym przez (1.25) jest grupą przemienną. Oznacza się ją przez $(\mathbb{Z}_p, +_p)$, jednak sam zbiór $\mathbb{Z}_p$ często jest utożsamiany z samą grupą. W tabeli 1.3 podano tablicę działania w $\mathbb{Z}_6$.

Tabela 1.3 Tablica Cayleya grupy cyklicznej $\mathbb{Z}_6$.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Przechodzimy teraz do drugiego działania w (1.25). W ogólnym przypadku zbiór $\mathbb{Z}_p$ wraz z $*_p$ nie jest grupą. Mogą istnieć elementy nieodwracalne.

Rozważmy np. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Poniższe równanie

$$2a \equiv 1(\mathrm{mod}6)$$

nie ma rozwiązania w zbiorze liczb całkowitych, zatem $a = 2$ nie ma elementu odwrotnego. Równanie to równoważne jest bowiem

$$2a - 1 = 6k \quad \Leftrightarrow \quad 2a - 6k = 1,$$

gdzie $k \in \mathbb{Z}$. Brak rozwiązania wynika z tego, że różnica liczb parzystych nie może być nieparzysta. Podobnie nie są odwracalne 3 i 4. Poza jedynką odwracalna jest też piątka, która jest odwrotna do samej siebie, tzn.

$$5 \cdot 5 \equiv 1(\mathrm{mod}6).$$

Odpowiedź na pytanie, które elementy są odwracalne, a które nie zawarta jest w poniższym twierdzeniu. Dowód tego twierdzenia, oparty na algorytmie Euklidesa, można znaleźć np. w [12].

Twierdzenie 1.12 *Niech a, b, d będą ustalonymi, niezerowymi liczbami całkowitymi. Wówczas równanie*

$$ax + by = d \tag{1.26}$$

o niewiadomych x, y ma rozwiązanie w liczbach całkowitych wtedy i tylko wtedy, gdy $NWD(a, b)$ dzieli d.

W szczególnym przypadku, jeśli $\mathrm{NWD}(a, b) = 1$, to równanie (1.26) ma rozwiązanie dla każdego $d \in \mathbb{Z}$. Twierdzenie to pozwala wybrać te elementy z $\mathbb{Z}_p$, które będą odwracalne. Mianowicie, oznaczmy

$$\boxed{\mathbb{Z}_p^* := \{1 \leq k \leq p : \mathrm{NWD}(k, p) = 1\}.}$$

Jest to zbiór liczb względnie pierwszych z p. Jeśli p jest liczbą pierwszą, to oczywiście $|\mathbb{Z}_p^*| = p - 1$. Zauważmy też, że w zbiorze $\{1, 2 \ldots, p^n\}$ istnieje p^{n-1} liczb, które nie są względnie pierwsze z p^n. Są to p, $2p$, $3p$ i tak aż do $p^{n-1} \cdot p = p^n$. Zatem dla $n \geq 1$ mamy $|\mathbb{Z}_{p^n}| = p^n - p^{n-1}$.

Na przykład $\mathbb{Z}_6^* = \{1, 5\}$, $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ oraz

$$\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}.$$

Poniższe twierdzenie orzeka, że zbiór $\mathbb{Z}_p^*$ wraz z $*_p$ jest grupą przemienną. Elementem neutralnym tej grupy jest 1 i podobnie jak z $(\mathbb{Z}_p, +_p)$ grupę $(\mathbb{Z}_p^*, *_p)$ często utożsamia się z samym zbiorem $\mathbb{Z}_p^*$.

Twierdzenie 1.13 *Niech $p \geq 2$. Wówczas*

(i) *jeśli $a, b \in \mathbb{Z}_p^*$, to $a *_p b \in \mathbb{Z}_p^*$,*

(ii) *jeśli $a \in \mathbb{Z}_p^*$, to $a^{-1} = x \bmod p$, gdzie x jest rozwiązaniem równania*

$$ax + py = 1. \tag{1.27}$$

Dowód. Dowód (i). Mamy udowodnić implikację

$$\mathrm{NWD}(a, p) = 1, \quad \mathrm{NWD}(b, p) = 1 \quad \Rightarrow \quad \mathrm{NWD}(a *_p b, p) = 1.$$

Przede wszystkim zauważmy, że $a *_p b$ to reszta z dzielenia ab przez p. Zatem dla pewnego $q \in \mathbb{Z}$ mamy równość

$$ab = q \cdot p + a *_p b.$$

Załóżmy, że $a *_p b$ i p nie są względnie pierwsze. Istnieje wtedy liczba pierwsza $p_1 \geq 2$, która dzieli obie te liczby. Wynika stąd, że p_1 dzieli iloczyn ab. Jeśli p_1 dzieli a, to $\mathrm{NWD}(a, p) > 1$, ponieważ a i p mają wspólny dzielnik $p_1 \geq 2$. W drugim przypadku, jeśli p_1 dzieli b, to podobnie $\mathrm{NWD}(b, p) > 1$. Z otrzymanej sprzeczności wynika więc teza.

Dowód (ii). Istnienie rozwiązania równania (1.27) wynika z twierdzenia 1.12. Jest to szczególny przypadek równania (1.26). Mamy pokazać, że

$$a *_p (x \bmod p) = 1,$$

lub równoważnie, że

$$a(x \bmod p) = q_1 p + 1. \tag{1.28}$$

dla pewnego $q_1 \in \mathbb{Z}$. Zauważmy, że

$$x = q_2 \cdot p + x \bmod p, \quad \text{gdzie} \quad q_2 \in \mathbb{Z}.$$

Wstawiając x do równania (1.27) otrzymujemy

$$a(q_2 \cdot p + x \bmod p) + py = 1$$

lub równoważnie

$$a(x \bmod p) = -(aq_2 + y)p + 1.$$

Zatem $q_1 = -(aq_2 + y)$. To kończy dowód (1.28). □

Chociaż $\mathbb{Z}_p^*$ jest przemienna, to w ogólnym przypadku nie jest grupą cykliczną. Na przykład $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ nie jest cykliczna, ponieważ rząd

Tabela 1.4 Tablice Cayleya grupy cyklicznej $\mathbb{Z}_{10}^*$ i niecyklicznej $\mathbb{Z}_8^*$.

$*_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$*_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

każdego elementu poza jedynką wynosi 2. Jest to grupa izomorficzna z grupą czwórkową $(2^{\{a,b\}}, \triangle)$, patrz tabela 1.2. Natomiast $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ jest grupą cykliczną. Jej generatorem jest np. 3. Tablice Cayleya tych grup znajdują się w tabeli 1.4.

Przykład 1.8 Rozważmy grupę $\mathbb{Z}_{432}^*$. Ponieważ $NWD(25, 432) = 1$, więc $25 \in \mathbb{Z}_{432}^*$. Znajdziemy element do niego odwrotny. W tym celu należy znaleźć rozwiązanie równania

$$25x \equiv 1 (\mathrm{mod} 432).$$

Równanie to równoważne jest równaniu

$$25x - 432k = 1, \quad \text{gdzie } k \in \mathbb{Z}. \tag{1.29}$$

Aby rozwiązać (1.29) stosujemy najpierw algorytm Euklidesa do 432 i 25:

$$\begin{aligned} 432 &= 17 \cdot 25 + 7 \\ 25 &= 3 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1. \end{aligned}$$

Wstawiając kolejno reszty do równań od pierwszego do ostatniego otrzymamy równość

$$121 \cdot 25 - 7 \cdot 432 = 1.$$

Mamy więc rozwiązanie (1.29). Zauważmy jednak, że z tego rozwiązania można utworzyć nieskończenie wiele innych rozwiązań w następujący sposób

$$25 \cdot (121 + 432m) - 432 \cdot (7 + 25m) = 1, \quad m \in \mathbb{Z}.$$

Stąd $x = 121 + 432m$ jest ogólnym rozwiązaniem równania (1.29). W końcu z twierdzenia 1.13 mamy

$$25^{-1} = 121 \bmod 432 = 121.$$

Ponieważ $25 \cdot 121 = 3025$ oraz $3025 = 7 \cdot 432 + 1$, więc istotnie liczba ta przystaje do 1 modulo 432. □

1.3 Grupy przekształceń

Pokażemy, że składanie przekształceń jest działaniem łącznym. Niech będą dane odwzorowania

$$f : X \to Y, \quad g : Y \to Z, \quad h : Z \to W.$$

Na podstawie (1.1) mamy

$$f \circ g : X \to Z, \quad (f \circ g) \circ h : X \to W$$

oraz

$$((f \circ g) \circ h)(x) = h((f \circ g)(x)) = h(g(f(x))).$$

Podobnie

$$g \circ h : Y \to W, \quad f \circ (g \circ h) : X \to W$$

oraz

$$(f \circ (g \circ h))(x) = (g \circ h)(f(x)) = h(g(f(x))).$$

Zatem istotnie $(f \circ g) \circ h = f \circ (g \circ h)$.

Niech X będzie ustalonym zbiorem. Odwzorowanie tożsamościowe tego zbioru na siebie oznaczamy przez I, tzn.

$$I(x) = x, \quad x \in X.$$

Niech $\mathcal{G}$ będzie zbiorem składającym się z przekształceń zbioru X w siebie, czyli dla każdego $f \in \mathcal{G}$ mamy $f : X \to X$. Mówimy, że $\mathcal{G}$ jest **grupą przekształceń**, jeśli spełnione są następujące warunki

(i) $I \in \mathcal{G}$,

(ii) jeśli $f, g \in \mathcal{G}$, to $f \circ g \in \mathcal{G}$,

(iii) jeśli $f \in \mathcal{G}$, to $f^{-1} \in \mathcal{G}$.

Działaniem grupowym jest tutaj składanie przekształceń.

Grupą symetryczną lub **grupą permutacji** zbioru X nazywamy zbiór wszystkich bijekcji X w siebie i oznaczamy $Sym(X)$.

$$Sym(X) = \text{zbiór wszystkich bijekcji } f : X \to X.$$

Jeśli $|X| = n$, to $|Sym(X)| = n!$ i grupę tą oznacza się zwykle przez S_n. Grupom permutacji poświęcony jest rozdział 4.

Badanie grup przekształceń w ogólnym przypadku nie jest zbyt interesującę, ponieważ zbiory te są zbyt duże. Zwykle nakłada się pewne warunki, które przekształcenia te muszą spełniać. Na szczególną uwagę zasługują izometrie, a wśród izometrii obroty. Zaczniemy od definicji izometrii w $\mathbb{R}^n$.

Izometrią nazywamy odwzorowanie $f : \mathbb{R}^n \to \mathbb{R}^n$ spełniające warunek

$$|f(x) - f(y)| = |x - y|, \quad \text{dla wszystkich } x, y \in \mathbb{R}^n \tag{1.30}$$

gdzie $|x - y|$ jest odległością euklidesową między punktami x, y, tzn.

$$|x - y|^2 = \sum_{i=1}^{n} (x_i - y_i)^2.$$

Z (1.30) wynika, że izometrie są różnowartościowe i ciągłe. Ponadto złożenie izometrii też jest izometrią i wynika to z równości

$$|g(f(x)) - g(f(y))| = |f(x) - f(y)| = |x - y|.$$

Izometria nie musi być przekształceniem liniowym, ale jest przekształceniem afinicznym, tzn. spełnia równość

$$f(ax + by) = af(x) + bf(y),$$

dla wszystkich $x, y \in \mathbb{R}^n$ i dowolnych $a, b \in \mathbb{R}$, patrz [14]. Poniższe twierdzenie to twierdzenie 4.2 z [14]

Twierdzenie 1.14 *Każda izometria $f : \mathbb{R}^n \to \mathbb{R}^n$ jest złożeniem co najwyżej $n + 1$ symetrii płaszczyznowych.*

Symetria płaszczyznowa, o której mowa w tym twierdzeniu, oznacza symetrię względem hiperpłaszczyzny w przestrzeni $\mathbb{R}^n$. Hiperpłaszczyzna jest to zbiór punktów $\mathbb{R}^n$ spełniających równanie $\langle v, x\rangle = a$, gdzie v jest niezerowym wektorem tej przestrzeni, natomiast a jest ustaloną liczbą rzeczywistą. Wymiar tego zbioru wynosi $n - 1$. Hiperpłaszczyzną w $\mathbb{R}^2$ jest linia prosta, a w $\mathbb{R}^3$ zwykła płaszczyzna dwuwymiarowa.

Zatem każda izometria w $\mathbb{R}^2$ jest złożeniem co najwyżej trzech symetrii osiowych, czyli symetrii względem prostych. Natomiast izometria w $\mathbb{R}^3$ jest złożeniem co najwyżej czterech symetrii płaszczyznowych. Z powyższego twierdzenia wynika też, że każda izometria jest surjekcją, czyli $f(\mathbb{R}^n) = \mathbb{R}^n$.

W rezultacie f^{-1} jest również izometrią i zbiór wszystkich izometrii przestrzeni $\mathbb{R}^n$ tworzy grupę przekształceń.

Izometrią własną wielokąta lub pewnej figury płaskiej nazywamy taką izometrię płaszczyzny $\mathbb{R}^2$, która przeprowadza tą figurę na siebie. Na przykład, jeśli w wycięte z kartonu koło wbijemy w jego środek cyrkiel i następnie będziemy obracać, to po obrocie koło zawsze przejdzie na siebie. Jeśli zrobimy to samo z kartonowym kwadratem, to tylko niektóre obroty spowodują, że kwadrat przejdzie na siebie. Każda figura ma więc swoją własną grupę izometrii. Intuicja podpowiada, że im figura jest bardziej symetryczna, tym jej grupa izometrii jest większa.

Grupę izometrii własnych n-kąta foremnego na płaszczyźnie nazywamy **grupą dihedralną** i oznaczamy przez D_n

$$\boxed{D_n = \text{grupa izometrii własnych n-kąta foremnego.}}$$

Można udowodnić, patrz np. [6], że D_n jest grupą nieprzemienną rzędu $2n$. Grupa ta składa się obrotu wokół środka wielokąta o $2\pi/n$ radianów i jego potęg oraz n symetrii osiowych. Wliczając przekształcenie tożsamościowe, czyli pełny obrót, otrzymujemy

$$|D_n| = 2n, \quad n \geq 3.$$

Poniżej omówimy grupę izometrii trójkąta równobocznego i kwadratu. Działanie tych grup zaznaczone zostanie na wierzchołkach wielokątów.

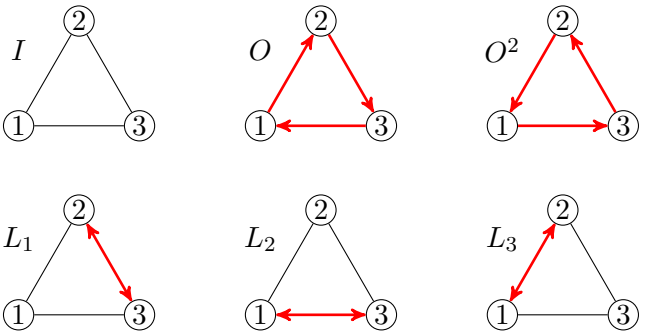
Przykład 1.9 Dla trójkąta równobocznego mamy

$$D_3 = \{I, O, O^2, L_1, L_2, L_3\},$$

gdzie O jest obrotem o 120 stopni wokół środka trójkąta, natomiast L_1, L_2, L_3 są symetriami względem symetralnych boków trójkąta, patrz rysunek 1.3. Obrót O wybrany został w kierunku zgodnym z ruchem wskazówek zegara. Jest to grupa izomorficzna z S_3, czyli grupą wszystkich permutacji zbioru trzyelementowego. Trójkąt jest jedynym wielokątem o tej własności. Równość $2n = n!$ spełniona jest tylko dla $n = 3$. Właściwe podgrupy D_3 to podgrupa obrotów $\{I, O, O^2\}$ oraz trzy podgrupy rzędu dwa: $\{I, L_1\}$, $\{I, L_2\}$, $\{I, L_3\}$. Zgodnie z twierdzeniem 1.14 obroty można zapisać jako iloczyn symetrii osiowych. Mamy więc np.

$$O = L_1 L_3, \quad O^2 = L_1 L_2.$$

Tabela działania tej grupy dana jest w zadaniu 1.9. □

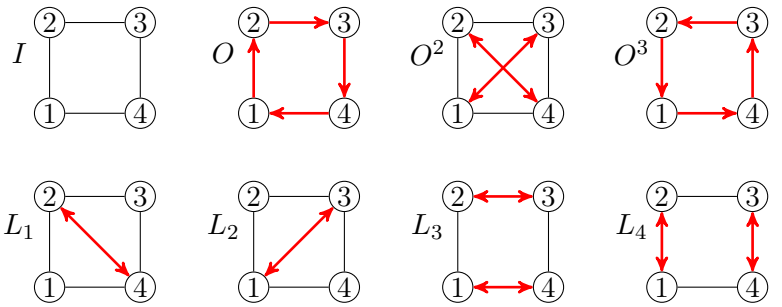


Rys. 1.3 Grupa izometrii własnych trójkąta równobocznego.

Przykład 1.10 Grupa izometrii własnych kwadratu składa się z 8 przekształceń

$$D_4 = \{I, O, O^2, O^3, L_1, L_2, L_3, L_4\},$$

gdzie O jest obrotem o 90 stopnia wokół środka kwadratu, natomiast L_1, L_2, L_3, L_4 są symetriami osiowymi, patrz rysunek 1.4. Tylko obroty są do zrealizowania w rzeczywistości. Pozostałych symetrii nie da się wykonać bez wychodzenia poza płaszczyznę. W grupie symetrii kwadratu istniej pięć pod-



Rys. 1.4 Grupa izometrii własnych kwadratu.

grup rzędu 2 i są to $\{I, O^2\}$, $\{I, L_1\}$, $\{I, L_2\}$, $\{I, L_3\}$ oraz $\{I, L_4\}$. Cechą charakterystyczną tej grupy jest to, że obrót O^2 jest przemienny z każdym elementem tej grupy, tzn.

$$XO^2 = O^2X, \quad \forall\, X \in D_4.$$

Istnieją też trzy podgrupy rzędu 4. Mamy tutaj grupę obrotów $\{I, O, O^2, O^3\}$ oraz $\{I, L_1, L_2, O^2\}$, $\{I, L_3, L_4, O^2\}$, izomorficzne z grupą czwórkową. Tabela Cayleya tej grupy dana jest w zadaniu 1.10. □

Tabela 1.5 Rzędy grup obrotów i grup symetrii wielościanów foremnych.

Wielościan	Grupa obrotów	Grupa symetrii
Czworościan	12 ($\cong A_4$)	24 ($\cong S_4$)
Sześcian	24 ($\cong S_4$)	48 ($\cong S_4 \times \mathbb{Z}_2$)
Ośmiościan	24 ($\cong S_4$)	48 ($\cong S_4 \times \mathbb{Z}_2$)
Dwunastościan	60 ($\cong A_5$)	120 ($\cong A_5 \times \mathbb{Z}_2$)
Dwudziestościan	60 ($\cong A_5$)	120 ($\cong A_5 \times \mathbb{Z}_2$)

W przestrzeni $\mathbb{R}^3$ istnieje 5 wielościanów foremnych. Są to: czworościan, sześcian, ośmiościan, dwunastościan i dwudziestościan. Dla wielościanów takich zachodzi wzór Eulera

$$W + S = K + S,$$

gdzie W jest liczbą wierzchołków, S jest liczbą ścian, a K jest liczbą krawędzi wielościanu. W tabeli 1.5 podane są rzędy grup obrotów i grup symetrii tych wielościanów. W nawiasie jest też informacja o tym z jakimi grupami są one izomorficzne. Przykładowo grupa obrotów dwudziestościanu składa się z 60 obrotów i jest izomorficzna z grupą permutacji parzystych zbioru pięcioelementowego. Podobnie grupa wszystkich symetrii sześcianu jest izomorficzna z grupą $S_4 \times \mathbb{Z}_2$, czyli z iloczynem prostym S_4 i $\mathbb{Z}_2$. Iloczyn prosty grup zostanie zdefiniowany w rozdziale 3. Obliczenie rzedów grup z tabeli 1.5 można znaleźć np. w [6].

Grupę obrotów określa się też czasem jako grupę obrotów właściwcyh, czyli takich, które są możliwe do zrealizowania w przestrzeni trójwymiarowej. Natomiast grupę symetrii danej bryły określa się jako grupę obrotów niewłaściwych. Grupa symetrii danej bryły składa się więc ze „zwykłych" obrotów oraz wszystkich możliwych symetrii płaszczyznowych.

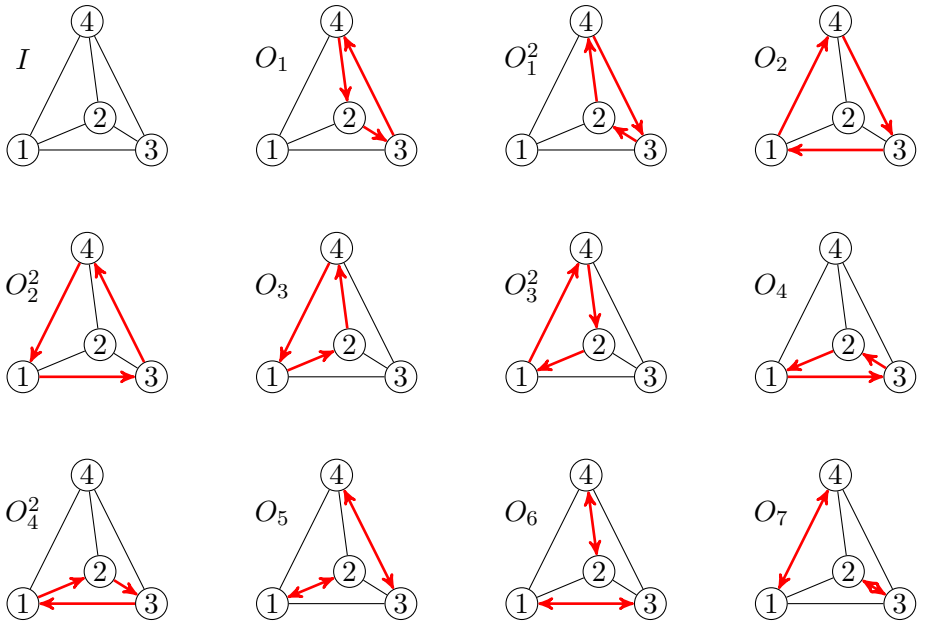
Omówimy tutaj grupę obrotów czworościanu. Podobnie jak w przypadku wielokątów płaskich w $\mathbb{R}^2$ zaznaczymy działanie tej grupy wierzchołkach czworościanu.

Przykład 1.11 Grupa obrotów czworościanu foremnego, którą oznaczymy jako A_4, składa się z 12 obrotów

$$A_4 = \{I, O_1, O_1^2, O_2, O_2^2, O_3, O_3^2, O_4, O_4^2, O_5, O_6, O_7\}.$$

Znaczenie symbolu A_4 wyjaśni się w rozdziale 4. Tak oznacza się grupę permutacji parzystych zbioru czteroelementowego. Grupa obrotów czworościanu jest po prostu izomorficzna z A_4 i widać to na jego wierzchołkach.

Do tej grupy należą: obroty O_1, O_2, O_3, O_4, wokół osi zawierających wysokości czworościanu oraz ich potęgi. Ponadto mamy 3 obroty O_5, O_6, O_7 wokół osi przechodzących przez środki przeciwległych krawędzi, patrz rysunek 1.5.



Rys. 1.5 Grupa obrotów właściwych czworościanu foremnego.

Istnieją 3 podgrupy rzędu dwa i są to $\{I, O_5\}$, $\{I, O_6\}$, $\{I, O_7\}$. Ponadto mamy 4 podgrupy rzędu 3: $\{I, O_1, O_1^2\}$, $\{I, O_2, O_2^2\}$, $\{I, O_3, O_3^2\}$, $\{I, O_4, O_4^2\}$. Istnieje też podgrupa rzędu 4 izomorficzna z grupą czwórkową $\{I, O_5, O_6, O_7\}$.

1.4 Zadania

Zadanie 1.1 Niech $G = [0, 1)$. Wykazać, że zbiór ten z działaniem

$$a \circ b := a + b - \lfloor a + b \rfloor.$$

jest grupą przemienną. □

Zadanie 1.2 Zdefiniujmy działanie

$$a \circ b := a\sqrt{b^2 + 1} + b\sqrt{a^2 + 1}, \quad a, b \in \mathbb{R}.$$

Udowodnić, że $(\mathbb{R}, \circ)$ jest grupą przemienną. □

Zadanie 1.3 Niech

$$\mathbb{Q}^*[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}\backslash\{0\}.$$

Pokazać, że $(\mathbb{Q}^*[\sqrt{2}], \cdot)$ jest grupą. □

Zadanie 1.4 Oznaczmy

$$\mathbb{Q}^*[\sqrt[3]{2}] := \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}\backslash\{0\}.$$

Pokazać, że $(\mathbb{Q}^*[\sqrt[3]{2}], \cdot)$ jest grupą. □

Zadanie 1.5 W przykładzie 1.5 wykazane zostało, że grupa nieskończona zawiera co najmniej jedną podgrupę właściwą. Udowodnić, że grupa nieskończona ma nieskończenie wiele podgrup. □

Zadanie 1.6 Niech $(G, \circ)$ będzie grupą i załóżmy, że $\varphi : G \to G'$ jest bijekcją. Określmy działanie w G' następująco

$$a' \diamond b' := \varphi(\varphi^{-1}(a') \circ \varphi^{-1}(b')), \quad a', b' \in G'.$$

Pokazać, że $(G', \diamond)$ jest grupą z elementem neutralnym równym $e' = \varphi(e)$. Element odwrotny do a' oblicza się ze wzoru

$$(a')^{-1} = \varphi((\varphi^{-1}(a'))^{-1}),$$

gdzie φ^{-1} oznacza funkcję odwrotną do φ, natomiast $(\varphi^{-1}(a'))^{-1}$ jest elementem odwrotnym do $\varphi^{-1}(a')$ w grupie $(G, \circ)$. □

Zadanie 1.7 Pokazać, że przedział $(0, 1)$ wraz z działaniem danym wzorem

$$a \circ b = \frac{ab}{2ab - a - b + 1}, \quad a, b \in (0, 1)$$

jest grupą przemienną. □

Zadanie 1.8 W zbiorze liczb naturalnych $\mathbb{N}$ określmy działanie

$$n \circ m = \begin{cases} n + m + 1 & , n, m \in 2\mathbb{N} - 1, \\ n - m + 2 & , n \in 2\mathbb{N} - 1, m \in 2\mathbb{N}, n > m - 3, \\ -n + m - 1 & , n \in 2\mathbb{N} - 1, n \in 2\mathbb{N}, n \leq m - 3, \\ n + m - 2 & , n, m \in 2\mathbb{N}, \\ -n + m + 2 & , n \in 2\mathbb{N}, m \in 2\mathbb{N} - 1, n < m + 3, \\ n - m - 1 & , n \in 2\mathbb{N}, m \in 2\mathbb{N} - 1, n \geq m + 3, \end{cases}$$

gdzie $2\mathbb{N} = \{2, 4, 6, \ldots\}$, $2\mathbb{N} - 1 = \{1, 3, 5, \ldots\}$. Udowodnić, że $(\mathbb{N}, \circ)$ jest grupą przemienną z elementem neutralnym równym 2. Element przeciwny do n to $n + 3$. □

Zadanie 1.9 Wykazać, że tablica Cayleya grupy izometrii trójkąta równobocznego D_3 ma postać

$\circ$	I	O	O^2	L_1	L_2	L_3
I	I	O	O^2	L_1	L_2	L_3
O	O	O^2	I	L_2	L_3	L_1
O^2	O^2	I	O	L_3	L_1	L_2
L_1	L_1	L_3	L_2	I	O^2	O
L_2	L_2	L_1	L_3	O	I	O^2
L_3	L_3	L_2	L_1	O^2	O	I

Zadanie 1.10 Wykazać, że tablica Cayleya grupy izometrii kwadratu D_4 ma postać

$\circ$	I	O	O^2	O^3	L_1	L_2	L_3	L_4
I	I	O	O^2	O^3	L_1	L_2	L_3	L_4
O	O	O^2	O^3	I	L_3	L_4	L_2	L_1
O^2	O^2	O^3	I	O	L_2	L_1	L_4	L_3
O^3	O^3	I	O	O^2	L_4	L_3	L_1	L_2
L_1	L_1	L_4	L_2	L_3	I	O^2	O^3	O
L_2	L_2	L_3	L_1	L_4	O^2	I	O	O^3
L_3	L_3	L_1	L_4	L_2	O	O^3	I	O^2
L_4	L_4	L_2	L_3	L_1	O^3	O	O^2	I

2. Grupy II

2.1 Homomorfizm i izomorfizm grup

Przechodzimy do ważnego pojęcia homomorfizmu grup. Pozwala ono badać związki pomiędzy różnymi grupami oraz patrzeć na nie z tego samego punktu widzenia. Innymi słowy, możemy stwierdzić czy dwie grupy mają podobne własności czy też nie. Niech więc dane będą dwie grupy: $(G_1, \circ)$ oraz $(G_2, \diamond)$. Niech ponadto e_1 oznacza element neutralny G_1, a e_2 element neutralny grupy G_2. Odwzorowanie $\varphi : G_1 \to G_2$ nazywamy **homomorfizmem** grupy G_1 w grupę G_2, jeśli zachodzi równość

$$\boxed{\varphi(a \circ b) = \varphi(a) \diamond \varphi(b), \quad \forall\, a, b \in G_1.} \tag{2.1}$$

Z definicji tej wynika, że $\varphi(e_1) = e_2$. Jeśli podstawimy $a = b = e_1$ do (2.1), to dostaniemy równość $\varphi(e_1) = \varphi^2(e_1)$. Ponieważ jedynym rozwiązaniem równania $a^2 = a$ w dowolnej grupie jest jej element neutralny, to $\varphi(e_1) = e_2$. Następnie, z równości

$$e_2 = \varphi(e_1) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$$

otrzymujemy

$$\varphi(a^{-1}) = (\varphi(a))^{-1}, \quad \forall\, a \in G_1. \tag{2.2}$$

Twierdzenie 2.1 *Jeśli φ jest homomorfizmem, to*

(i) *dla $n \geq 2$ i dowolnych $a_1, \ldots, a_n \in G_1$ zachodzi równość*

$$\varphi(a_1 a_2 \ldots a_n) = \varphi(a_1)\varphi(a_2)\ldots\varphi(a_n). \tag{2.3}$$

(ii) *dla każdego $n \in \mathbb{Z}$ mamy*

$$\varphi(a^n) = (\varphi(a))^n. \tag{2.4}$$

Dowód. Dowód (i). Korzystamy z indukcji. Dla $n = 2$ równość jest spełniona ponieważ φ jest homomorfizmem. Załóżmy, że równość (2.3) jest prawdziwa dla pewnego $n \geq 3$. Wówczas mamy

$$\varphi(a_1 \ldots a_n a_{n+1}) \overset{(2.1)}{=} \varphi(a_1 \ldots a_n)\varphi(a_{n+1}) \overset{(2.3)}{=} \varphi(a_1)\ldots\varphi(a_n)\varphi(a_{n+1}).$$

Zatem wzór (2.3) jest też prawdziwy dla $n+1$.

Dowód (ii). Jeśli $n \geq 0$, to (2.4) wynika z (2.3). W tym celu wystarczy przyjąć $a_1 = \ldots = a_n = a$. Aby otrzymać równość dla ujemnych potęg zauważmy, że

$$\varphi(a^{-n}) = \varphi((a^{-1})^n) = (\varphi(a^{-1}))^n \overset{(2.2)}{=} (\varphi(a))^{-n}.$$

Powyższa równość kończy dowód (2.4). □

Mówimy, że grupa G_2 jest **obrazem homomorficznym** grupy G_1, jeśli istnieje homomorfizm z G_1 na G_2, tzn. $\varphi(G_1) = G_2$. Homomorfizm spełniający ten warunek nazywany jest **epimorfizmem**. Homomorfizm różnowartościowy nazywany jest **monomorfizmem**. Homomorfizm grupy w siebie to **endomorfizm**, patrz rysunek 2.1.

Twierdzenie 2.2 *Niech H_1 będzie podgrupą grupy G_1, a H_2 podgrupą G_2. Jeśli $\varphi : G_1 \to G_2$ jest homomorfizmem, to*

(i) *$\varphi(H_1)$ jest podgrupą G_2,*

(ii) *$\varphi^{-1}(H_2)$ jest podgrupą G_1.*

Dowód. Dowód (i). Załóżmy, że $a, b \in \varphi(H_1)$. Wówczas dla pewnych elementów $a_1, b_1 \in H_1$ mamy $a = \varphi(a_1)$ i $b = \varphi(b_1)$ Ponieważ H_1 jest podgrupą grupy G_1, to iloczyn $a_1 b_1$ należy do H_1 i stąd $\varphi(a_1 b_1) \in \varphi(H_1)$. Następnie

$$\varphi(a_1 b_1) = \varphi(a_1)\varphi(b_1) = ab,$$

co dowodzi, że $ab \in \varphi(H_1)$. Ponadto $a_1^{-1} \in H_1$ i w rezultacie

$$a^{-1} = (\varphi(a_1))^{-1} = \varphi(a_1^{-1}) \in \varphi(H_1).$$

W końcu $\varphi(e_1) = e_2 \in \varphi(H_1)$.

Dowód (ii). Niech $a, b \in \varphi^{-1}(H_2)$. Wówczas $a = \varphi^{-1}(a_2)$, $b = \varphi^{-1}(b_2)$ dla pewnych $a_2, b_2 \in H_2$. Z równości

$$\varphi(ab) = \varphi(a)\varphi(b) = a_2 b_2$$

wynika, że $ab = \varphi^{-1}(a_2 b_2) \in \varphi^{-1}(H_2)$, gdyż $a_2 b_2 \in H_2$. Podobnie mamy

$$\varphi(a^{-1}) = (\varphi(a))^{-1} = a_2^{-1} \in H_2$$

i stąd $a^{-1} = \varphi^{-1}(a_2^{-1}) \in \varphi^{-1}(H_2)$. Oczywiście $e_1 = \varphi^{-1}(e_2)$. □

Z twierdzenia 2.2 wynika, że obraz $\varphi(G_1)$ jest podgrupą grupy G_2. Co więcej, obraz homomorficzny grupy przemiennej jest grupą przemienną. Jeśli bowiem $ab = ba$, to zgodnie z (2.1) mamy

$$\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a).$$

Może się jednak zdarzyć, że obraz grupy nieprzemiennej jest grupą przemienną. Wynika to z faktu, że homomorfizm nie musi być przekształceniem różnowartościowym. Rozważmy na przykład

$$\varphi(a) = \begin{cases} 1, & a > 0 \\ -1, & a < 0. \end{cases} \tag{2.5}$$

Powyższe odwzorowanie jest homomorfizmem pomiędzy grupą nieprzemienną $(\mathbb{R}^*, \circ)$ z przykładu 1.1, a grupą przemienną $(\{-1, 1\}, \cdot)$.

Twierdzenie 2.3 *Jeśli φ_1 jest homomorfizmem grupy G_1 w grupę G_2 i φ_2 jest homomorfizmem G_2 w grupę G_3, to złożenie $\varphi_1 \circ \varphi_2$ jest homomorfizmem pomiędzy G_1 i G_3.*

Dowód. Z założenia $\varphi_1(ab) = \varphi_1(a)\varphi_1(b)$ dla wszystkich $a, b \in G_1$ oraz $\varphi_2(cd) = \varphi_2(c)\varphi_2(d)$ dla dowolnych $c, d \in G_2$. Zatem

$$\begin{aligned}(\varphi_1 \circ \varphi_2)(ab) &= \varphi_2(\varphi_1(ab)) = \varphi_2(\varphi_1(a))\varphi_2(\varphi_1(b)) \\ &= (\varphi_1 \circ \varphi_2)(a)(\varphi_1 \circ \varphi_2)(b)\end{aligned}$$

dla dowolnych $a, b \in G_1$. Oznacza to, że $\varphi_1 \circ \varphi_2$ spełnia warunek (2.1). □

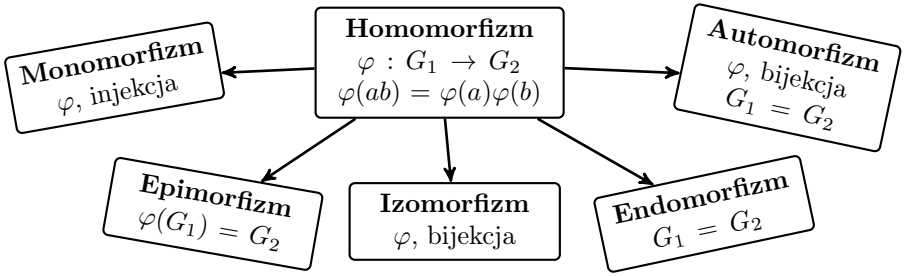
Twierdzenie 2.4 *Niech G będzie dowolną grupą. Wtedy dla każdego ustalonego $g \in G$ odwzorowania*

$$\varphi(a) = ag, \quad \psi(a) = ga, \quad a \in G \tag{2.6}$$

są bijekcjami.

Dowód. Ponieważ równania $ag = bg$, $ga = gb$ są równoważne równości $a = b$, więc oba przekształcenia są różnowartościowe. Aby wykazać, że są to surjekcje weźmy dowolny $c \in G$. Z równań $ag = c$, $ga = c$ otrzymujemy $a = cg^{-1}$ i $a = g^{-1}c$. □

Homomorfizm $\varphi : G_1 \to G_2$, który jest odwzorowaniem wzajemnie jednoznacznym nazywamy **izomorfizmem** grupy G_1 na grupę G_2. Izomorfizm grupy G na siebie nazywamy **automorfizmem**. Zauważmy, że chociaż φ



Rys. 2.1 Homomorfizm i jego różne rodzaje.

i ψ w twierdzeniu 2.4 są bijekcjami, to nie są one w ogólnym przypadku automorfizmami. Mamy bowiem $\varphi(ab) = abg$, natomiast $\varphi(a)\varphi(b) = agbg$. Podobnie $\psi(ab) = gab$ i $\psi(a)\psi(b) = gagb$.

Jeśli G_1 i G_2 są izomorficzne, to piszemy $G_1 \cong G_2$. Na przykład grupy $(\mathbb{R}, +)$ i $(\mathbb{R}_+, \cdot)$ są izomorficzne ponieważ $\varphi(x) = e^x$ jest izomorfizmem. Dla dowolnych $x_1, x_2 \in \mathbb{R}$ mamy bowiem

$$\varphi(x_1 + x_2) = e^{x_1+x_2} = e^{x_1}e^{x_2} = \varphi(x_1)\varphi(x_2).$$

Można też wziąć zamiast φ dowolną funkcję wykładniczą a^x, przy czym $a > 0$ i $a \neq 1$. Wówczas $\varphi^{-1}(x) = \log_a x$ jest izomorfizmem pomiędzy $(\mathbb{R}_+, \cdot)$ a $(\mathbb{R}, +)$.

Jeśli φ jest homomorfizmem i $rz(a) < \infty$, to również $rz(\varphi(a)) < \infty$. Jest to wniosek z (2.4). Dokładniej, jeśli $a^n = e_1$ dla pewnego $n \geq 2$, to

$$\varphi(a^n) = \varphi(e_1) = e_2 = (\varphi(a))^n.$$

Z równości tej wynika, że $rz(\varphi(a)) \leq n$. Zatem dla dowolnego homomorfizmu zachodzi nierówność

$$\boxed{rz(\varphi(a)) \leq rz(a).} \tag{2.7}$$

Homomorfizm nie zwiększa więc rzędu elementów grupy.

Twierdzenie 2.5 *Jeśli $\varphi : G_1 \to G_2$ jest izomorfizmem, to*

$$\boxed{rz(\varphi(a)) = rz(a), \quad \forall\, a \in G_1.} \tag{2.8}$$

Dowód. Z (2.7) wiadomo, że $rz(\varphi(a)) \leq rz(a)$. Udowodnimy nierówność przeciwną. Ponieważ φ^{-1} jest izomorfizmem G_2 na G_1, to z nierówności (2.7) mamy $rz(\varphi^{-1}(a)) \leq rz(a)$ i stąd

$$rz(a) = rz(\varphi^{-1}(\varphi(a))) \leq rz(\varphi(a)).$$

Ostatecznie $rz(a) = rz(\varphi(a))$. □

Twierdzenie 2.6 *Dla dowolnego ustalonego $g \in G$ przekształcenie $\varphi_g : G \to G$ określone wzorem*

$$\boxed{\varphi_g(a) = gag^{-1}, \quad a \in G,} \tag{2.9}$$

jest izomorfizmem.

Dowód. Jeśli G jest grupą przemienną, to

$$\varphi_g(a) = gag^{-1} = gg^{-1}a = a,$$

więc jest to przekształcenie tożsamościowe. W ogólnym przypadku mamy

$$\varphi_g(ab) = g(ab)g^{-1} = (gag^{-1})(gbg^{-1}) = \varphi_g(a)\varphi_g(b),$$

więc pozostaje sprawdzić, że φ_g jest bijekcją. Równość $gag^{-1} = gbg^{-1}$ równoważna jest równości $a = b$, zatem φ_g jest różnowartościowe. Niech b będzie dowolnym elementem G. Z równania $b = gag^{-1}$ dostajemy $a = g^{-1}bg$. Zatem $\varphi_g(g^{-1}bg) = b$, co oznacza, że φ_g jest surjekcją. □

Wnioskiem z powyższego twierdzenia jest fakt, że dla dowolnych $a, g \in G$ prawdziwa jest równość

$$\boxed{rz(a) = rz(gag^{-1}).} \tag{2.10}$$

Izomorfizm określony przez (2.9) nazywa się **automorfizmem wewnętrznym**. Pozostałe automorfizmy to **automorfizmy zewnętrzne**. Zbiór wszystkich automorfizmów grupy G nazywamy **grupą automorfizmów** G i oznaczamy przez $Aut(G)$.

Przykład 2.1 Ponieważ w grupie każdemu elementowi odpowiada dokładnie jeden element odwrotny, to możemy określić bijekcję $\varphi : G \to G$ wzorem

$$\varphi(a) = a^{-1}, \quad a \in G. \tag{2.11}$$

W ogólnym przypadku nie jest to jednak izomorfizm. Z jednej strony $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1}$ natomiast $\varphi(a)\varphi(b) = a^{-1}b^{-1}$. W grupie abelowej jest to oczywiście izomorfizm. Ponadto $\varphi^{-1}(a) = a^{-1}$ i oraz $\varphi(\varphi(a)) = a$. □

Homomorfizm nie musi być monomorfizmem, czyli odwzorowaniem różnowartościowym. Stopień jego nieróżnowartościowości może być różny. Rozważmy na przykład

$$\varphi(a) = sgn(a) = \begin{cases} 1, & a > 0 \\ -1, & a < 0. \end{cases}$$

Jest to homomorfizm grupy $(\mathbb{R}^*, \cdot)$ w grupę dwuelementową $\{-1, 1\}$ z mnożeniem, przy czym $\varphi^{-1}(\{1\}) = \mathbb{R}^+$. Jest on więc bardzo nieróżnowartościowy. Dobrym miernikiem tego jest pojęcie jądra.

Jądrem homomorfizmu φ działającego z G_1 w G_2 nazywamy przeciwobraz elementu neutralnego z G_2 i oznaczamy przez $Ker(\varphi)$. Zatem

$$Ker(\varphi) := \varphi^{-1}(e_2) = \{a \in G_1 : \varphi(a) = e_2\}.$$

Z twierdzenia 2.2 wynika, że jądro φ jest podgrupą grupy G_1. Im mniejsze jądro tym homomorfizm jest bardziej różnowartościowy.

Twierdzenie 2.7 *Homomorfizm $\varphi : G_1 \to G_2$ jest różnowartościowy wtedy i tylko wtedy, gdy $Ker(\varphi) = \{e_1\}$.*

Dowód. Jeśli φ jest injekcją, to równanie $\varphi(a) = e_2$ spełnia tylko e_1. Załóżmy teraz, że $Ker(\varphi) = \{e_1\}$ i $\varphi(a) = \varphi(b)$. Mnożąc obie strony ostatniej równości przez $(\varphi(b))^{-1}$ otrzymamy

$$\varphi(a)(\varphi(b))^{-1} = \varphi(ab^{-1}) = e_2.$$

Wynika stąd, że $ab^{-1} = e_1$ i w konsekwencji $a = b$. □

2.2 Sprzężenie, komutant, centrum

Niech a, b będą ustalonymi elementami grupy G. Mówimy, że a i b są **sprzężone**, jeśli $b = cac^{-1}$, dla pewnego $c \in G$. Jeśli a i b są sprzężone, to piszemy również $a \sim b$. Definicja ta w języku matematyki wygląda tak

$$\boxed{a \sim b \quad \Leftrightarrow \quad \exists\, c \in G, \quad b = cac^{-1}.} \tag{2.12}$$

Twierdzenie 2.8 *Relacja określona przez* (2.12) *jest relacją równoważności w grupie G.*

Dowód. Zauważmy, że $a = eae^{-1}$, zatem jest to relacja zwrotna. Następnie, równość $b = cac^{-1}$ jest równoważna równości $bc = ca$, a ta z kolei $a = c^{-1}bc$. Innymi słowy

$$b = cac^{-1} \quad \Rightarrow \quad a = c^{-1}bc = c^{-1}b(c^{-1})^{-1}.$$

Relacja ta jest więc symetryczna. Pozostało wykazać przechodniość. Mamy pokazać, że zachodzi implikacja $(aRb \ \wedge \ bRc) \Rightarrow aRc$. Jeśli więc $b = gag^{-1}$ oraz $c = hbh^{-1}$, to mamy

$$c = h(gag^{-1})h^{-1} = (hg)a(hg)^{-1},$$

zatem $a \sim c$ i stad $\sim$ jest relacją równoważności na G. □

Klasy abstrakcji, na które relacja ta dzieli zbiór G nazywamy **klasami elementów sprzężonych** albo **klasami sprzężoności**. W grupach przemiennych równość $b = cac^{-1}$ równoważna jest równości $b = a$. Zatem w tym przypadku klasy abstrakcji są jednoelementowe, tzn. $[a] = a$, dla każdego a i mamy trywialną równość $G = \bigcup_{a\in G}\{a\}$.

W ogólnym przypadku mamy natomiast

$$\boxed{ab \sim ba.} \tag{2.13}$$

Wynika to z równości $ba = b(ab)b^{-1}$. Podobnie mamy

$$\boxed{abc \sim cab \sim bca.} \tag{2.14}$$

Istotnie, mamy bowiem

$$cba = c(abc)c^{-1}, \quad bca = bc(abc)(bc)^{-1}.$$

Własności (2.13) i (2.14) prawdziwe są też dla iloczynu większej liczby elementów, tzn. przestawiając cyklicznie porządek elementów w iloczynie $a_1a_2 \dots a_n$ otrzymujemy elementy sprzężone

$$a_1a_2 \dots a_n \sim a_na_1a_2 \dots a_{n-1} \sim a_{n-1}a_na_1 \dots a_{n-2} \sim \dots$$

W ten sposób można skonstruować maksymalnie $n-1$ elementów sprzężonych z $a_1 \dots a_n$, jeśli będę one oczywiście różne. Z (2.10) wiemy, że rzędy elementów sprzężonych są równe, zatem

$$rz(a_1a_2 \dots a_n) = rz(a_na_1a_2 \dots a_{n-1}) = \dots$$

Twierdzenie 2.9 *Niech G będzie grupą oraz $a_1, a_2, \ldots, a_n$ jej elementami. Jeśli $a_1 a_2 \ldots a_n = e$, to każdy z ilczynów*

$$a_2 a_3 \ldots a_n a_1, \quad a_3 a_4 \ldots a_n a_1 a_2, \quad \ldots, \quad a_n a_1 a_2 \ldots a_{n-1}$$

jest też równy e, gdzie e jest elementem neutralnym G.

Dowód. Równość $ab = e$ równoważna jest równości $ba = e$, patrz (1.6). Zatem

$$a_1(a_2 \ldots a_n) = e \quad \Leftrightarrow \quad (a_2 \ldots a_{n-1} a_n) a_1 = e.$$

Postępując podobnie, czyli przestawiając cyklicznie elementy, otrzymamy wszystkie wymienione iloczyny. □

Przykład 2.2 Rozważmy grupę z przykładu 1.1. Jest to grupa nieprzemienna, w której elementem neutralnym jest 1. Wyznaczymy jej klasy sprzężoności. Jeśli $a > 0$, to ze wzoru (1.8) otrzymujemy

$$c \circ a \circ c^{-1} = \begin{cases} ca \cdot \frac{1}{c}, & c > 0 \\ \frac{c}{a} \cdot \frac{1}{c}, & c < 0, \end{cases} = \begin{cases} a, & c > 0 \\ \frac{1}{a}, & c < 0. \end{cases}$$

W tym przypadku a jest w relacji z samym sobą i z elementem do siebie odwrotnym, czyli z $1/a$. Dla $a < 0$ mamy natomiast

$$c \circ a \circ c^{-1} = \begin{cases} ca \cdot c, & c > 0 \\ \frac{c}{a} \cdot c, & c < 0, \end{cases} = \begin{cases} c^2 a, & c > 0 \\ \frac{c^2}{a}, & c < 0. \end{cases}$$

Stąd a jest w relacji z dowolnym elementem postaci $c^2 a$, dla każdego $c > 0$. Oznacza to, że dowolne dwie liczby ujemne są ze sobą w relacji i w rezultacie zbiór liczb ujemnych tworzy jedną klasę. Zatem

$$[a] = \begin{cases} \{a, \frac{1}{a}\}, & a > 0 \\ (-\infty, 0), & a < 0. \end{cases}$$

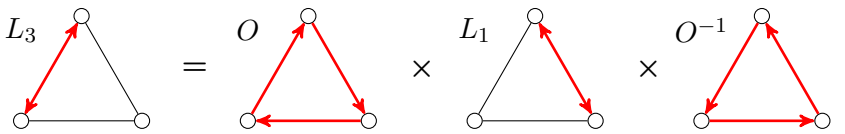
Oczywiście $[1] = \{1\}$. Podsumowując, podział $\mathbb{R}^*$ na klasy sprzężoności wygląda tak

$$\mathbb{R}^* = (-\infty, 0) \cup \bigcup_{a>0} \{a, \frac{1}{a}\}. \; \square$$

Przykład 2.3 (a) Klasy sprzężoności w grupie izometrii trójkąta równobocznego D_3 są następujące: $\{I\}$, $\{O, O^2\}$, $\{L_1, L_2, L_3\}$. Wynika to na przykład z poniższych równości

$$O^2 = L_1 O L_1^{-1}, \quad L_3 = O L_1 O^{-1}, \quad L_2 = O^2 L_1 O^{-2}.$$

Jedna z tych sytuacji przedstawiona jest na rysunku 2.2. Natomiast obrót O i symetria L_1 nie są sprzężone. Aby O i L_1 były sprzężone musi istnieć $X \in D_3$, dla którego $OX = XL_1$. Z tabeli w zadaniu 1.9 widać, że taki X nie istnieje.



Rys. 2.2 L_1 i L_3 należą do tej samej klasy sprzężoności.

(b) Istnieje pięć klas równoważności w grupie D_4 izometrii kwadratu: $\{I\}$, $\{O, O^3\}$, $\{O^2\}$, $\{L_1, L_2\}$, $\{L_3, L_4\}$. Istotnie, mamy równości

$$O^3 = L_1 O L_1^{-1}, \quad L_2 = O L_1 O^{-1}, \quad L_3 = O L_4 O^{-1}.$$

Zauważmy, że O^2 nie jest sprzężony ani z L_3 ani z L_4. Podobnie jak wcześniej warunek $O^2 = XL_3X^{-1}$ jest równoważny $O^2X = XL_3$. Z tabeli działania w tej grupie w zadaniu 1.10 wynika, że takiego X nie ma. □

Relacja sprzężenia, określona przez (2.12) przenosi się na podzbiory/podgrupy grupy G. A więc podzbiory/podgrupy H_1 i H_2 grupy G są **sprzężone**, jeśli istnieje g takie, że $H_2 = gH_1g^{-1}$. Językiem matematyki

$$H_1 \sim H_2 \quad \Leftrightarrow \quad \exists\, g \in G, \quad H_2 = gH_1g^{-1}.$$

Jest to relacja równoważności, która tym razem określona jest na rodzinie wszystkich podzbiorów/podgrup G. Ponadto, jeśli H_1, H_2 są sprzężone, to są równoliczne, tzn. $|H| = |gHg^{-1}|$.

Twierdzenie 2.10 *Niech H będzie podgrupą grupy G. Wtedy dla każdego ustalonego g podzbiór H' określony przez*

$$\boxed{H' = gHg^{-1} := \{ghg^{-1} : h \in H\}}$$

jest podgrupą grupy G izomorficzną z H.

Dowód. Niech $a, b \in H'$. Wówczas $a = gh_1g^{-1}$, $b = gh_2g^{-1}$ dla pewnych $h_1, h_2 \in H$. Ponieważ H jest podgrupą G, to $h_1h_2^{-1} \in H$. Stąd mamy

$$ab^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1} = g(h_1h_2^{-1})g^{-1} \in H'.$$

Z twierdzenia 1.6 wynika, że H' jest podgrupą grupy G, a z twierdzenia 2.6, że $\varphi_g(h) = ghg^{-1}$ jest izomorfizmem H na H'. □

Dzielnikiem normalnym, podgrupą **normalną** lub **niezmienniczą** nazywamy podgrupę H, która spełnia warunek

$$\boxed{H = gHg^{-1}, \quad \forall\, g \in G} \tag{2.15}$$

Z powyższego warunku wynika, że dla każdego $g \in G$ i dowolnego $h \in H$ istnieje $h' \in H$ spełniające

$$h = gh'g^{-1}.$$

Z równości tej wynika, że $h' = g^{-1}hg$ i wobec tego $g^{-1}hg \in H$. Ponieważ g jest dowolne, więc z (2.15) wynika, że

$$\boxed{ghg^{-1} \in H, \quad \forall\, g, h \in G.} \tag{2.16}$$

Z twierdzenia 2.6 wiadomo też, że odwzorowanie $\varphi_g(h) = ghg^{-1}$, przy ustalonym g, jest bijekcją z H na $\varphi_g(H)$. Zatem warunek (2.15) jest równoważny warunkowi (2.16). Zmieniając h, przy ustalonym g „wypełnimy" całą podgrupę H.

Powyższe dwa warunki definiujące podgrupę niezmienniczą zamienimy na jeszcze jeden równoważny każdemu z nich. W tym celu zdefiniujmy zbiory

$$gH = \{gh : h \in H\}, \quad Hg = \{hg : h \in H\},$$

które nazywane są odpowiednio **warstwą lewostronną** i **warstwą prawostronną** elementu $g \in G$ względem podgrupy H.

Twierdzenie 2.11 *Warunek* (2.15) *równoważny jest warunkowi*

$$\boxed{gH = Hg, \quad \forall\, g \in G.} \tag{2.17}$$

Dowód. Powyższy warunek oznacza, że dla dowolnego $g \in G$ i dowolnego $h \in H$ istnieje $h' \in H$ spełniające

$$gh = h'g.$$

Zatem $h' = ghg^{-1}$ i wobec tego $ghg^{-1} \in H$. Oznacza to, że zachodzi warunek (2.16), który równoważny jest warunkowi (2.15). □

Twierdzenie 2.12 *Niech $\varphi : G_1 \to G_2$ będzie homomorfizmem. Wówczas $Ker(\varphi)$ jest podgrupą niezmienniczą grupy G_1.*

Dowód. W myśl definicji (2.15) mamy udowodnić, że dla każdego $g \in G_1$ zachodzi równość

$$gH = Hg, \quad H := Ker(\varphi). \tag{2.18}$$

Aby to udowodnić pokażemy, że $gH \subset Hg$ oraz $Hg \subset gH$.

Zaczniemy od dowodu inkluzji $gH \subset Hg$. Niech h należy do H. Wówczas $gh = (ghg^{-1})g$ i wystarczy pokazać, że $ghg^{-1} \in H$, tzn. $\varphi(ghg^{-1}) = e_2$. Ciąg równości

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(h) = e_2$$

właśnie tego dowodzi. Teraz uzasadniamy zawieranie $Hg \subset gH$. Zauważmy, że $hg = g(g^{-1}hg)$ i wystarczy pokazać, że $g^{-1}hg \in H$. Mamy jednak $\varphi(g^{-1}hg) = \varphi(h) = e_2$. Dowód (2.18) i całego twierdzenia jest więc zakończony. □

Niech $a, b \in G$. **Komutatorem** a i b nazywamy element określony wzorem

$$\boxed{[a,b] := aba^{-1}b^{-1} = ab(ba)^{-1}.} \tag{2.19}$$

Czasem komutator definiuje się też tak

$$[a,b]_* := a^{-1}b^{-1}ab.$$

Związek pomiędzy tymi definicjami jest następujący

$$[a,b]_* = [a^{-1}, b^{-1}], \quad [a,b] = [a^{-1}, b^{-1}]_*.$$

Zauważmy, że $[a,a] = e$ oraz $[a,e] = [e,a] = e$, dla każdego $a \in G$.

Mówimy, że a i b **komutują**, jeśli $ab = ba$. Ponieważ równość $ab = ba$ jest równoważna równości $aba^{-1}b^{-1} = e$, więc

$$\boxed{[a,b] = e \quad \Leftrightarrow \quad ab = ba.} \tag{2.20}$$

Wynika stąd w szczególności, że $[a, a^{-1}] = e$. W rozdziale tym wprowadzimy pomocnicze oznaczenie

$$a^b := bab^{-1}.$$

Wynika stąd, że $(a^{-1})^b = (a^b)^{-1}$ i ponadto zachodzą tożsamości

$$(ab)^c = a^c b^c, \quad (a^b)^c = a^{cb}. \tag{2.21}$$

Dla dowodu sprawdzamy

$$(ab)^c = c(ab)c^{-1} = (cac^{-1})(cbc^{-1}) = a^c b^c,$$

oraz

$$(a^b)^c = c(a^b)c^{-1} = (cb)a(cb)^{-1} = a^{cb}.$$

Twierdzenie 2.13 *Dla dowolnych $a, b, c \in G$ mamy*

(i) $ab = [a, b]ba$

(ii) $[a, b]^{-1} = [b, a]$

(iii) $[[a, b], [b, a]] = e$

(iv) $[a, b]^c = [a^c, b^c]$

(v) $[a, bc] = [a, b][a, c]^b$

(vi) $[ab, c] = [b, c]^a[a, c]$.

Dowód. Dowód (i) wynika bezpośrednio z definicji komutatora. Dowód (ii)

$$[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a].$$

Punkt (iii) wynika z (ii). Dowód (iv)

$$\begin{aligned}[a^c, b^c] &= (cac^{-1})(cbc^{-1})(ca^{-1}c^{-1})(cb^{-1}c^{-1}) = caba^{-1}b^{-1}c^{-1} \\ &= c[a, b]c^{-1} = [a, b]^c.\end{aligned}$$

Dowód (v)

$$\begin{aligned}[a, bc] &= abca^{-1}c^{-1}b^{-1} = aba^{-1}b^{-1}baca^{-1}c^{-1}b^{-1} \\ &= [a, b]b[a, c]b^{-1} = [a, b][a, c]^b.\end{aligned}$$

Dowód (vi)

$$\begin{aligned}[ab, c] &= abcb^{-1}a^{-1}c^{-1} = a(bcb^{-1}c^{-1})a^{-1}(aca^{-1}c^{-1}) \\ &= [b, c]^a[a, c]. \quad \square\end{aligned}$$

Niech a_1, b_1, a_2, b_2 będą ustalonymi elementami pewnej grupy G. Chcemy odpowiedzieć na pytanie, kiedy istnieją $c, d \in G$ spełniające równość

$$[a_1, b_1][a_2, b_2] = [c, d].$$

Innymi słowy, kiedy iloczyn komutatorów jest też komutatorem. Po rozpisaniu obu stron mamy

$$a_1b_1(b_1a_1)^{-1}a_2b_2(b_2a_2)^{-1} = cdc^{-1}d^{-1}.$$

Przyjmując $c = a_1b_1$ i $d = (b_1a_1)^{-1}$ otrzymujemy

$$a_2b_2 = (a_1b_1)^{-1}, \quad (b_2a_2)^{-1} = b_1a_1.$$

Wstawiając $a_2 = (a_1b_1)^{-1}b_2^{-1}$ do drugiego równania dostajemy warunek

$$b_2(a_1b_1)b_2^{-1} = b_1a_1.$$

Warunek ten jest spełniony dla $b_2 = b_1$. Wówczas $a_2 = (b_1a_1b_1)^{-1}$.

Twierdzenie 2.14 *Dla dowolnych $a, b \in G$ zachodzi równość*

$$[a, b][(bab)^{-1}, b] = [ab, (ba)^{-1}].$$

Dowód. Rozpisujemy lewą stronę

$$aba^{-1}b^{-1}(bab)^{-1}b(bab)b^{-1} = aba^{-1}b^{-2}a^{-1}ba$$

i prawą stronę

$$ab(ba)^{-1}(ab)^{-1}(ba) = aba^{-1}b^{-2}a^{-1}ba. \quad \square$$

Iloczyn komutatorów nie musi być komutatorem, ale mamy za to równość

$$([a_1, b_1][a_2, b_2])^c = [a_1^c, b_1^c][a_2^c, b_2^c]. \tag{2.22}$$

Dowód jest następujący

$$\begin{aligned}([a_1, b_1][a_2, b_2])^c &= c[a_1, b_1][a_2, b_2]c^{-1} = c[a_1, b_1]c^{-1}c[a_2, b_2]c^{-1} \\ &= [a_1, b_1]^c[a_2, b_2]^c = [a_1^c, b_1^c][a_2^c, b_2^c],\end{aligned}$$

gdzie ostatnia równość wynika z twierdzenia 2.13. Powyższy wzór uogólnia się do większej ilości składników

$$\left(\prod_{i=1}^{n}[a_i, b_i]\right)^c = \prod_{i=1}^{n}[a_i^c, b_i^c]. \tag{2.23}$$

Niech A, B będą podzbiorami grupy G. **Komutantem wzajemnym** A i B nazywamy podgrupę określoną następująco

$$[A, B] := \langle [a, b] : a \in A, b \in B \rangle.$$

Komutantem grupy G nazywamy podgrupę $[G, G]$. Zatem

$$[G, G] := \langle [a, b] : a, b \in G \rangle.$$

Jest to więc podgrupa generowana przez wszystkie komutatory. Ponieważ w grupie abelowej $[a, b] = \{e\}$ dla wszystkich a, b, więc w tym przypadku $[G, G] = \{e\}$. Jeśli $[G, G] = \{e\}$, to oznacza, że każdy komutator jest równy e. Z (2.20) wynika więc, że G jest przemienna.

Twierdzenie 2.15 *$[G, G]$ jest podgrupą niezmienniczą grupy G.*

Dowód. Oznaczmy $H = [G, G]$. Pokażemy, że zachodzi warunek (2.16). Każdy element H może być przedstawiony w postaci

$$h = \prod_{i=1}^{n} [a_i, b_i], \quad \text{dla pewnych} \quad a_i, b_i \in G.$$

Z własności (2.23) wynika, że

$$h^g = ghg^{-1} = \prod_{i=1}^{n} [a_i^g, b_i^g] \in H.$$

Dowód jest więc zakończony. □

Niech A będzie podzbiorem grupy G. **Centralizatorem** zbioru A nazywamy zbiór

$$C_G(A) = \{g \in G : ag = ga, \forall\, a \in A\}.$$

Podzbiór ten jest zawsze niepusty, ponieważ $e \in C_G(A)$. Pokażemy, że $C_G(A)$ jest podgrupą G. Niech $g, h \in C_G(A)$. Wówczas

$$ag = ga, \quad ah = ha, \quad \forall\, a \in A.$$

Z pierwszej równości wynika, że $g^{-1}a = ag^{-1}$, co oznacza, że $g^{-1} \in C_G(A)$. Następnie mnożąc pierwszą z równości prawostronnie przez h i drugą lewostronnie przez g otrzymujemy

$$agh = gah, \quad gah = gha.$$

Wynika stąd, że $agh = gha$, dla każdego $a \in C_G(A)$ a więc $gh \in C_G(A)$. **Centrum grupy** to centralizator całego G oznaczany przez $Z(G)$

$$\boxed{Z(G) = \{g \in G : ag = ga, \quad \forall\, a \in G\}.}$$

Wiemy już, że $Z(G)$ jest podgrupą, a jeśli odatkowo G jest przemienna, to oczywiście $Z(G) = G$.

Twierdzenie 2.16 *$Z(G)$ jest podgrupą przemienną i każda podgrupa $Z(G)$ jest podgrupą niezmienniczą grupy G.*

Dowód. Niech $g, h \in Z(G)$. Wtedy $ag = ga$, dla każdego $a \in G$. Tym razem możemy wstawić h zamiast a i stąd $hg = gh$. Zatem $Z(G)$ jest przemienna.

Niech H będzie podgrupą $Z(G)$. Mamy pokazać, że $gH = Hg$, dla każdego $g \in G$. Warstwa gH składa się elementów gh, gdzie $h \in H$. Ale h jest przemienny z każdym elementem grupy, zatem $gh = hg$ i w rezultacie $gH = Hg$. To kończy dowód. □

Przykład 2.4 Rozważmy grupę z przykładu 1.1. Jest to grupa nieprzemienna i po obliczeniach dostaniemy

$$[a, b] = \begin{cases} 1, & a > 0, b > 0, \\ a^2, & a > 0, b < 0, \\ 1/b^2, & a < 0, b > 0, \\ a^2/b^2, & a < 0, b < 0. \end{cases}$$

Zatem $[a, b] > 0$, dla wszystkich $a, b \in \mathbb{R}^*$ i stąd łatwo wyznaczyć komutant

$$[\mathbb{R}^*, \mathbb{R}^*] = (0, +\infty) = \mathbb{R}_+.$$

Natomiast centrum tej grupy to $Z(\mathbb{R}^*) = \{1\}$. Wynikają stąd poniższe wzory

$$C_{\mathbb{R}^*}(a) = \begin{cases} (0, +\infty), & a > 0, a \neq 1, \\ \mathbb{R}^*, & a = 1, \\ \{1, a\}, & a < 0. \end{cases}$$

Przykład 2.5 Załóżmy, że w pewnej grupie istnieje tylko jeden element, niech to będzie a, którego rząd wynosi 2. Pokażemy, że jest on przemienny z każdym elementem tej grupy, a więc należy on do jej centrum $Z(G)$.

Ponieważ rzędy elementów sprzężonych są równe, patrz np. (2.10), więc $(bab^{-1})^2 = e$, dla każdego $b \in G$. Z założenia jedynym nietrywialnym rozwiązaniem równania $x^2 = e$ jest a. Zatem $bab^{-1} = a$ i stąd $ab = ba$. Oznacza to, że a należy do centrum tej grupy. □

2.3 Zadania

Zadanie 2.1 Wykazać, że jeśli $b = cac^{-1}$, to $b^n = ca^n c^{-1}$, dla $n \in \mathbb{Z}$. □

Zadanie 2.2 Udowodnić równości

(i) $[a, b^{-1}] = [b^{-1}, a^{-1}]^a$,

(ii) $[a^{-1}, b] = [b, a]^{a^{-1}}$,

(iii) $[a^{-1}, b^{-1}] = [b^{-1}, a]^{a^{-1}}$. □

Zadanie 2.3 Wykazać, że

(i) $[D_3, D_3] = \{I, O, O^2\}$,

(ii) $[D_4, D_4] = \{I, O^2\}$. □

Przed następnym zadaniem pewna definicja. Komutatory wyższego rzędu definiujemy rekurencyjnie

$$[a_1, \ldots, a_n] := [[a_1, \ldots, a_{n-1}], a_n], \quad n \geq 3.$$

Analogicznie

$$[a_1, \ldots, a_n]_* := [[a_1, \ldots, a_{n-1}]_*, a_n]_*, \quad n \geq 3.$$

Dla $n = 3$ i przyjmując a, b, c zamiast a_1, a_2, a_3 otrzymujemy wzór

$$[a, b, c] = [[a, b], c] = [a, b]c[b, a]c^{-1} = [a, b][b, a]^c.$$

Wynik stąd, że

$$[a, b, c]^{-1} = [a, b]^c[b, a],$$

zatem $[a, b, c]^{-1}$ nie musi być komutatorem trzeciego rzędu. Ponadto

$$[a, b, c]_* = [[a, b]_*, c]_* = [[a^{-1}, b^{-1}]^{-1}, c^{-1}] = [b^{-1}, a^{-1}, c^{-1}].$$

Zadanie 2.4 Udowodnić następującą **tożsamość Halla**

$$[b^{-1}, a, c]^b[c^{-1}, b, a]^c[a^{-1}, c, b]^a = e.$$

Jeśli przyjmiemy $a^b = b^{-1}ab$, to powyższa równość ma postać

$$[a, b^{-1}, c]_*^b[b, c^{-1}, a]_*^c[c, a^{-1}, b]_*^a = e. \square$$

3. Grupy III

3.1 Twierdzenie Lagrange'a

Udowodnimy tutaj twierdzenie Lagrange'a, które mówi, że w przypadku grupy skończonej liczba jej elementów jest wielokrotnością rzędu dowolnej jej podgrupy. Twierdzenie to w najbardziej ogólnej formie zostało udowodnione w 1861 roku przez Jordana. Szczególne przypadki zostały wykazane wcześniej, w tym przez Lagrange'a w 1771 roku, patrz [18].

Niech H będzie podgrupą grupy G. Przypomnijmy, że zbiory

$$aH = \{ah : h \in H\}, \quad Ha = \{ha : h \in H\}$$

nazywamy warstwą lewostronną i warstwą prawostronną elementu a względem H. Są to szczególne przypadki iloczynu algebraicznego (1.17), gdzie $A = \{a\}$ i $B = H$. Ponadto $a \in aH$ i $a \in Ha$ ponieważ $e \in H$. Udowodnimy równoważność

$$\boxed{b \in aH \quad \Leftrightarrow \quad a^{-1}b \in H.} \tag{3.1}$$

Jeśli $b \in aH$, to $b = ah$ dla pewnego $h \in H$. Zatem $a^{-1}b = h$, a więc $a^{-1}b \in H$. Jeśli $a^{-1}b \in H$, to $a^{-1}b = h'$ dla pewnego $h' \in H$. Wynika stąd, że $b = ah'$, zatem $b \in aH$. Podobnie dowodzi się

$$\boxed{b \in Ha \quad \Leftrightarrow \quad ba^{-1} \in H.} \tag{3.2}$$

W grupach przemiennych zachodzi oczywiście równość $aH = Ha$, dla każdego $a \in G$. Jeśli więc $b \in aH$, to także $b \in Ha$. Na powyższe dwa warunki można też spojrzeć z innej strony. W pierwszym przypadku a i b należą do tej samej warstwy lewostronnej, a w drugim do tej samej warstwy prawostronnej. Zatem (3.1) można zapisać w postaci relacji: bRa, jeśli $a^{-1}b \in H$. Podobnie z (3.2): bRa, jeśli $ba^{-1} \in H$. Tak określone relacje są relacjami równoważności i dzielą G na rozłączne podzbiory.

Twierdzenie 3.1 *Niech H będzie podgrupą grupy G. Wówczas dla dowolnych elementów a, b tej grupy mamy*

(i) $aH = bH$ *lub* $aH \cap bH = \emptyset$,

(ii) $Ha = Hb$ *lub* $Ha \cap Hb = \emptyset$.

Dowód. Przeprowadzimy dowód dla warstw lewostronnych. Załóżmy, że $aH \cap bH \neq \emptyset$. Istnieje wtedy $c \in aH \cap bH$,zatem

$$c = ah_1, \quad c = bh_2,$$

dla pewnych $h_1, h_2 \in H$. Wynika stąd, że $a = b(h_2 h_1^{-1})$. Niech $d \in aH$. Wówczas $d = ah$ dla pewnego $h \in H$ oraz

$$d = (b(h_2 h_1^{-1}))h = b(h_2 h_1^{-1} h) \in bH.$$

Oznacza to, że $aH \subset bH$. Podobnie dowodzi się inkluzji $bH \subset aH$. Zatem jeśli przecięcie aH i bH jest niepuste, to $aH = bH$. □

Z powyższego twierdzenia wynika, że każdy element grupy należy do jednej warstwy lewostronnej i do jednej warstwy prawostronnej względem podgrupy H. Mamy bowiem $a \in aH$ i $a \in Ha$. Zatem

$$aH = bH \Leftrightarrow a^{-1}b \in H$$

oraz

$$Ha = Hb \Leftrightarrow ba^{-1} \in H.$$

Twierdzenie 3.2 *Niech H będzie podgrupą grupy G. Wówczas*

(i) *Każde dwie warstwy lewostronne względem H są równoliczne.*

(ii) *Każde dwie warstwy prawostronne względem H są równoliczne.*

(iii) *Każda warstwa lewostronna jest równoliczna z każdą warstwą prawosronną względem H.*

Dowód. Dowód (i). Niech a, b będą ustalone. Zdefiniujmy $\varphi : aH \to bH$ następująco

$$\varphi(ah) = bh, \quad h \in H.$$

Odwzorowanie φ jest różnowartościowe, ponieważ równość $bh_1 = bh_2$ równoważna jest równości $h_1 = h_2$. Ponadto φ jest surjekcją, czyli $\varphi(aH) = bH$. Dla każdego $h \in H$ istnieje bowiem $h' \in H$ spełniające $ah' = bh$. Mianowicie $h' = a^{-1}bh$. Zatem φ jest bijekcją pomiędzy aH i bH, stąd warstwy te są równoliczne.

Dowód (ii). Podobnie jak w (i) odwzorowanie $\varphi(ha) = hb$ jest bijekcją pomiędzy Ha i Hb.

Dowód (iii). Zauważmy, że $eH = H$ i $H = He$. Z (i) wynika, że każda warstwa lewostronna jest równoliczna z H a z (ii) wynika, że każda warstwa prawostronna jest równoliczna z H. Stąd wynika już teza (iii). □

Twierdzenie 3.3 *Niech H będzie podgrupą grupy G. Wówczas dla każdego elementu a tej grupy zachodzą równości*

(i) $(aH)^{-1} = Ha^{-1}$,

(ii) $(Ha)^{-1} = a^{-1}H$.

Dowód. Udowodnimy (i). Jeśli $b \in aH$, to $b = ah_1$ dla pewnego $h_1 \in H$. Stąd mamy

$$b^{-1} = h_1^{-1}a^{-1} \in Ha^{-1}.$$

Oznacza to, że $(aH)^{-1} \subset Ha^{-1}$. Następnie, jeśli $c \in Ha^{-1}$, to $c = h_2a^{-1}$ dla pewnego $h_2 \in H$. Wynika stąd, że

$$c = (ah_2^{-1})^{-1} \in (aH)^{-1}.$$

Zatem $Ha^{-1} \subset (aH)^{-1}$ i w rezultacie $(aH)^{-1} = Ha^{-1}$. □

Z ostatniego twierdzenia wynika, że zbiór warstw lewostronnych względem H jest równoliczny ze zbiorem warstw prawostronnych względem tej podgrupy. Warstwie aH możemy przyporządkować warstwę Ha^{-1}

$$aH \to Ha^{-1}.$$

Jest to odwzorowanie różnowartościowe i każda warstwa prawostronna jest obrazem pewnej warstwy lewostronnej.

Niech G będzie grupą skończoną oraz H jej podgrupą. **Indeksem podgrupy H w grupie G** nazywamy liczbę warstw lewostronnych grupy G względem H i oznaczamy przez $|G : H|$, tzn.

$$|G : H| = \text{liczba warstw lewostronnych względem } H.$$

Zauważmy, że w grupie skończonej liczba warstw prawostronnych jest równa liczbie warstw lewostronnych. Oto twierdzenie Lagrange'a.

Twierdzenie 3.4 *Niech G będzie grupą skończoną oraz H jej podgrupą. Wówczas zachodzi wzór*

$$\boxed{|G| = |H||G : H|.} \tag{3.3}$$

Dowód. Przyjmijmy $|G| = n$, gdzie $n \geq 2$. Załóżmy, że liczba warstw lewostronnych względem H wynosi r, $1 \leq r \leq n$, tzn.

$$G = a_1H \cup a_2H \cup \ldots \cup a_rH$$

dla pewnych $a_1, \ldots, a_r \in H$. Z twierdzenia 3.2 wynika, że

$$|a_i H| = |H|, \quad i = 1, 2, \ldots, r.$$

Zatem $|G| = r|H|$, co dowodzi (3.3). □

Kilka wniosków z powyższego twierdzenia. Jak już zauważyliśmy, jeśli $rz(a) = m$, to elementy $a, a^2, \ldots, a^{m-1}$ są różne i wraz z elementem neutralnym tworzą podgrupę danej grupy. Jest to podgrupa cykliczna rzędu m. Jeśli więc $|G| < \infty$, to rząd każdego $a \in G$ dzieli $|G|$.

Udowodnimy teraz implikację

$$|G| = n \quad \Rightarrow \quad \forall\, a \in G, \quad a^n = e. \tag{3.4}$$

Innymi słowy, każda grupa skończona jest torsyjna. Załóżmy, że $rz(a) = m$. W takim razie m dzieli n, czyli $n = qm$, dla pewnego $q \in \mathbb{N}$. Wówczas mamy $a^n = (a^m)^q = e$ i to kończy dowód (3.4).

Kolejny wniosek jest taki, że jeśli $|G| = n$ jest liczbą pierwszą, to G jest grupą cykliczną, czyli $G = \langle a \rangle$, dla pewnego $a \in G$. W tym celu wystarczy wziąć dowolny element $a \neq e$. Wówczas rząd a musi być równy n, czyli $G = \langle a \rangle$. W przeciwnym razie rząd a dzieliłby n wbrew założeniu.

Ostatni wniosek zapiszemy w postaci twierdzenia.

Twierdzenie 3.5 *Niech G będzie grupą skończoną, która nie zawiera żadnej podgrupy właściwej. Wtedy jej rząd $|G|$ jest liczbą pierwszą.*

Dowód. Niech $|G| = n$ i załóżmy, że $n \geq 2$. Ponieważ G nie zawiera podgrup właściwych, więc $G = \langle a \rangle$, dla pewnego $a \neq e$. W przeciwnym razie grupa $\langle a \rangle$ byłaby właściwa. Załóżmy teraz, że n nie jest liczbą pierwszą, czyli $n = qm$, gdzie $q > 1$ i $m < n$. Wówczas $(a^q)^m = e$, co oznacza, że $rz(a^q) < n$ i podgrupa generowana przez a^q byłaby właściwa. Stąd n musi być liczbą pierwszą. □

Twierdzenie 3.6 *Jeśli H_1 i H_2 są podgrupami skończonymi grupy G, to*

$$|H_1 H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}. \tag{3.5}$$

Dowód. Niech $H_3 = H_1 \cap H_2$. Wtedy H_3 jest podgrupą H_1 i H_2. W szczególności H_2 można przedstawić w postaci rozłącznych warstw względem H_3, czyli

$$H_2 = H_3 g_1 \cup H_3 g_2 \cup \ldots \cup H_3 g_r,$$

gdzie $g_i \in H_2$, dla $i = 1, \ldots, r$. Zatem H_1H_2 można zapisać jako sumę zbiorów $H_1H_3g_1, \ldots, H_1H_3g_r$. Ponieważ H_3 jest również podgrupą H_1, to $H_1H_3 = H_1$ i stąd

$$H_1H_2 = H_1g_1 \cup H_1g_2 \cup \ldots \cup H_1g_r.$$

Pokażemy, że zbiory po prawej stronie tej równości są rozłączne. Załóżmy przeciwnie, że $H_1g_i \cap H_1g_j \neq \emptyset$, dla $i \neq j$. Wówczas $hg_i = h'g_j$, dla pewnych $h, h' \in H_1$. Zatem $g_ig_j^{-1} = h^{-1}h' \in H_1$ i w rezultacie $g_ig_j^{-1} \in H_1 \cap H_2 = H_3$. Z (3.2) wynika, że $g_i \in H_3g_j$ lub równoważnie $H_3g_i = H_3g_j$. W ten sposób otrzymaliśmy sprzeczność, ponieważ warstwy $H_3g_1, \ldots, H_3g_r$ są z założenia rozłączne. Wynika stąd, że zbiory $H_1g_1, \ldots, H_1g_r$ też są rozłączne.

Następnie zauważmy, że $|H_1g_i| = |H_1|$, dla $i = 1, \ldots, r$. W takim razie $|H_1H_2| = r|H_1|$, gdzie r jest liczbą warstw prawostronnych względem H_3. Z twierdzenia 3.4 wynika, że liczba ta jest równa $|H_2|/|H_3|$. Dowód wzoru (3.5) jest więc zakończony. □

3.2 Grupy ilorazowe

Przypomnijmy, patrz definicja (2.15), że podgrupa H jest **dzielnikiem normalnym** grupy G, jeśli spełnia jeden z poniższych równoważnych warunków

(i) $H = gHg^{-1}$, dla każdego $g \in G$,

(ii) $gH = Hg$, dla każdego $g \in G$ i $h \in H$,

(iii) $ghg^{-1} \in H$, dla wszystkich $g \in G$, $h \in H$.

Ponieważ g jest dowolne, to podstawiając g^{-1} w miejsce g otrzymamy dwa kolejne równoważne warunki

(iv) $H = g^{-1}Hg$, dla każdego $g \in G$,

(v) $g^{-1}hg \in H$, dla wszystkich $g \in G$, $h \in H$.

Odnotujmy, że każda podgrupa grupy przemiennej jest jej podgrupą niezmienniczą oraz, że istnieją grupy, które takich podgrup nie mają.

Okazuje się, że zbiór warstw grupy względem jej dzielnika normalnego jest też grupą z odpowiednio określonym działaniem. Mianowicie, niech H będzie dzielnikiem normalnym G. Zdefiniujmy

$$\boxed{aH \circ bH := (ab)H, \quad a, b \in G.} \tag{3.6}$$

Pokażemy, że działanie to nie zależy od wyboru reprezentantów warstw, tzn.

$$(a' \in aH \wedge b' \in bH) \quad \Rightarrow \quad (a'b')H = (ab)H.$$

Niech $a' = ah_1$, $b' = bh_2$, gdzie $h_1, h_2 \in H$. Ponieważ H jest dzielnikiem normalnym oraz $h_1 b \in Hb$, to $h_1 b \in bH$. Stąd $h_1 b = bh_3$ dla pewnego $h_3 \in H$. Wynika stąd dalej, że

$$a'b' = a(h_1 b)h_2 = (ab)(h_3 h_2) \in (ab)H.$$

Zatem $(a'b')H = (ab)H$.

Twierdzenie 3.7 *Niech H będzie dzielnikiem normalnym grupy G. Wówczas zbiór warstw lewostronnych względem H z działaniem określonym wzorem* (3.6) *jest grupą.*

Dowód. Zgodnie z definicją mamy

$$(aH \circ bH) \circ cH = (ab)H \circ cH = (ab)cH.$$

Podobnie

$$aH \circ (bH \circ cH) = aH \circ (bc)H = a(bc)H.$$

Równość $(aH \circ bH) \circ cH = aH \circ (bH \circ cH)$ wynika więc z łączności działania w grupie G. Podgrupa H jest elementem neutralnym tego działania

$$H \circ aH = eH \circ aH = (ea)H = aH.$$

Warstwą odwrotną do aH jest warstwa $a^{-1}H$

$$aH \circ a^{-1}H = (aa^{-1})H = eH = H. \quad \square$$

Zbiór warstw względem podgrupy normalnej H z działaniem określonym wzorem (3.6) nazywamy **grupą ilorazową** grupy G względem H i oznaczamy przez G/H

$$G/H = \text{grupa ilorazowa}.$$

Jeśli G jest skończona, to z twierdzenia Lagrange'a mamy

$$|G/H| = \frac{|G|}{|H|}.$$

W tym przypadku naturalne przyporządkowanie elementowi jego warstwy nazywane jest **homomorfizmem kanonicznym**. Dokładniej, odwzorowanie $\varphi : G \to G/H$ określone wzorem $\varphi(a) = aH$ jest rzeczywiście homomorfizmem

$$\varphi(a \circ b) = (a \circ b)H = aH \circ bH = \varphi(a) \circ \varphi(b).$$

Ponieważ jest to odwzorowanie „na", to jest też nazywane epimorfizmem kanonicznym, patrz rysunek 2.1.

Na przykład, ponieważ grupa $(\mathbb{Z}_{12}, +_{12})$ jest przemienna, więc podgrupa $H = \{0, 3, 6, 9\}$ jest jej dzielnikiem normalnym, tzn. $aH = Ha$, dla każdego $a \in \mathbb{Z}_{12}$. Z twierdzenia Lagrange'a wynika, że mamy 3 warstwy lewostronne i 3 prawostronne

$$G/H = \{\{0, 3, 6, 9\}, \{1, 4, 7, 10\}, \{2, 5, 8, 11\}\} \cong \mathbb{Z}_3.$$

Przykład 3.1 Niech H będzie podgrupą grupy G taką, że

$$|G : H| = 2. \tag{3.7}$$

Pokażemy, że H jest podgrupą normalną. Z (3.7) wynika, że istnieją dwie warstwy lewostronne i dwie prawostronne. Są to H i $G\backslash H$. Dla $a \in H$ mamy

$$aH = H = Ha.$$

Jeśli natomiast $a \in G\backslash H$, to

$$aH = G\backslash H = Ha,$$

ponieważ a nie może należeć do dwóch warstw jednocześnie. □

Tabela 3.1 Tablica Cayleya grupy ilorazowej G/H izomorficznej z $\mathbb{Z}_2$.

$\circ$	H	$G\backslash H$
H	H	$G\backslash H$
$G\backslash H$	$G\backslash H$	H

$+_2$	0	1
0	0	1
1	1	0

Przykład 3.2 Rozpatrzmy dwie podgrupy grupy dihedralnej D_3

$$H_1 = \{I, O, O^2\}, \quad H_2 = \{I, L_1\}.$$

Podgrupa H_1 ma indeks 2, więc jest dzielnikiem normalnym i

$$G/H_1 = \{\{I, O, O^2\}, \{L_1, L_2, L_3\}\} \cong \mathbb{Z}_2.$$

Podgrupa H_2 nie jest podgrupą niezmienniczą, mamy np. $OH_2 = \{O, L_2\}$ oraz $H_2O = \{O, L_3\}$, zatem $OH_2 \neq H_2O$. Niezależnie od tego, zarówno zbiór warstw prawostronnych jak i lewostronnych względem H_2 tworzy podział G, patrz tabela 3.2. □

Tabela 3.2 Warstw względem H_2, która nie jest dzielnikiem normalnym D_3.

a	aH_2	H_2a
I	$\{I, L_1\}$	$\{I, L_1\}$
O	$\{O, L_2\}$	$\{O, L_3\}$
O^2	$\{O^2, L_3\}$	$\{O^2, L_2\}$
L_1	$\{I, L_1\}$	$\{I, L_1\}$
L_2	$\{O, L_2\}$	$\{O^2, L_2\}$
L_3	$\{O^2, L_3\}$	$\{O, L_3\}$

Grupa, która nie ma właściwych podgrup normalnych nazywana jest **grupą prostą**. Najprostsze przykłady grup prostych są takie, dla których $|G| = p$, gdzie p jest liczbą pierwszą. Grupy takie nie mają żadnych podgrup właściwych, więc tym bardziej nie mają podgrup normalnych.

Niech A będzie podzbiorem G. **Normalizatorem** A nazywamy zbiór

$$N_G(A) = \{g \in G : gA = Ag\}.$$

Podobnie jak w przypadku centralizatora, podzbiór ten jest zawsze niepusty, ponieważ $e \in N_G(A)$. Pokażemy, że jest podgrupą G.

Jeśli $gA = Ag$, to $g^{-1}A = Ag^{-1}$ i stąd $g^{-1} \in N_G(A)$. Jeśli dodatkowo $hA = Ah$, to z równości $hgA = hAg$ otrzymujemy $hgA = Ahg$, zatem $hg \in N_G(A)$. To pokazuje, że normalizator jest podgrupą.

Jeśli H jest podgrupą, to $H \subset N_G(H)$ ponieważ $hH = Hh$, dla każdego $h \in H$. W najlepszym więc razie $N_G(H) = G$, a w najgorszym $N_G(H) = H$.

Twierdzenie 3.8 *Niech G będzie grupą. Wówczas*

(i) *Jeśli H jest podgrupą, to H jest podgrupą normalną w $N_G(H)$*

(ii) *Jeśli A jest podzbiorem G, to liczba zbiorów z nim sprzężonych równa jest $G : N_G(A)$.*

Dowód. Dowód (i). Mamy pokazać, że $gH = Hg$, dla każdego $g \in N_G(H)$. Ale g należy do $N_G(H)$ właśnie wtedy, gdy spełnia tą równość.

Dowód (ii). Jeśli a, b należą do tej samej warstwy to $N_G(A)a = N_G(A)b$. Stąd istnieje $h \in N_G(A)$, dla którego $b = ah$. Zatem $h = a^{-1}b$ i wstawiając do równości $hA = Ah$ otrzymamy $a^{-1}bA = Aa^{-1}b$. Z tej równości wynika $bAb^{-1} = aAa^{-1}$, a to oznacza, że te zbiory są równe. Wszystkie elementy warstwy utworzą ten sam zbiór sprzężony z A.

Podobnie, jeśli $aAa^{-1} = bAb^{-1}$, to $Aa^{-1}b = a^{-1}bA$. Wynika stąd, że $a^{-1}b \in N_G(A)$, a to z (3.1) równoważne jest $b \in aN_G(A)$ i w rezultacie a i b są w jednej warstwie. Podsumowując, każdej warstwie odpowiada inny zbiór sprzężony z A. Zatem liczba różnych zbiorów sprzężonych z A równa jest liczbie warstw lewostronnych, czyli indeksowi $N_G(A)$. □

Twierdzenie 3.9 *Niech H będzie dzielnikiem normalnym grupy G. Wówczas*

(i) *Grupa $G/[G,G]$ jest przemienna,*

(ii) *Jeśli G/H jest abelowa, to $[G,G] \subset H$.*

Dowód. Dowód (i). Oznaczmy $G' = [G,G]$. Elementami grupy G/G' są warstwy. Z twierdzenia 3.3 mamy $(aG')^{-1} = G'a^{-1}$. Ponieważ G' jest również podgrupą normalną, to $G'a^{-1} = a^{-1}G'$. Komutator $[a,b]$ należy do G', zatem dla dowolnych $a, b \in G$ zachodzi równość

$$\begin{aligned}[aG', bG'] &= (aG')(bG')(aG')^{-1}(bG')^{-1} = (aba^{-1}b^{-1})G' \\ &= [a,b]G' = G'.\end{aligned}$$

Wynika stąd $(aG')(bG') = (bG')(aG')$ i G/G' jest abelowa.

Dowód (ii). Niech G/H będzie grupą przemienną. Oznacza to, że

$$(aH)(bH) = (bH)(aH), \quad \text{dla dowolnych } a, b \in G.$$

Wynika stąd dalej, że $(ab)H = (ba)H$. Mnożąc obie strony ostatniej równości przez $(a^{-1}b^{-1})H$ otrzymujemy

$$(ab)(a^{-1}b^{-1})H = [a,b]H = (ba)(a^{-1}b^{-1})H = H.$$

Równość $[a,b]H = H$ oznacza, że $[a,b] \in H$. Podgrupa H zawiera wszystkie komutatory, więc także $[G,G]$. □

Oto ciekawa wlasność centrum: jeśli G nie jest abelowa, to grupa ilorazowa $G/Z(G)$ nie jest cykliczna. Popatrzmy na twierdzenie.

Twierdzenie 3.10 *Jeżeli H jest podgrupą $Z(G)$ i grupa ilorazowa G/H jest cykliczna, to G jest grupą przemienną.*

Dowód. Niech $g \in G$ będzie taki, że

$$\begin{aligned}G/H &= \{\ldots, (gH)^{-2}, (gH)^{-1}, H, (gH)^1, (gH)^2, \ldots\} \\ &= \{\ldots, g^{-2}H, g^{-1}H, H, gH, g^2H, \ldots\}.\end{aligned}$$

Wówczas $a = g^{n_1}h_1$, $b = g^{n_2}h_2$ dla pewnych $n_1, n_2 \in \mathbb{N}$ i $h_1, h_2 \in H$. Stąd

$$\begin{aligned} ab &= g^{n_1}h_1g^{n_2}h_2 = g^{n_1}g^{n_2}h_1h_2 \\ &= g^{n_2}g^{n_1}h_2h_1 = g^{n_2}h_2g^{n_1}h_1 = ba. \end{aligned}$$

Ponieważ a i b są dowolne, więc równość $ab = ba$ zachodzi dla wszystkich elementów grupy G. Oznacza to, że G jest grupą przemienną. □

Niech $\varphi : G \to H$ będzie homomorfizmem i niech $K = Ker(\varphi)$. Jak zauważyliśmy wcześniej, patrz twierdzenie 2.12, K jest dzielnikiem normalnym grupy G, zatem odzworowanie $\kappa : G \to G/K$ określone wzorem

$$\kappa(a) = aK, \quad a \in G \tag{3.8}$$

jest homomorfizmeme „na", czyli epimorfizmem. Jądrem κ jest K, ponieważ jest to warstwa neutralna w grupie ilorazowej G/K. Poniższe twierdzenie mówi o związku pomiędzy G/K, a obrazem G przez φ i nazywane jest pierwszym twierdzeniem o izomorfizmie.

Twierdzenie 3.11 *Niech φ będzie homomorfizmem grupy G w grupę H. Wówczas istnieje izomorfizm $\varphi^* : G/Ker(\varphi) \to \varphi(G)$ spełniający $\varphi = \kappa\varphi^*$, gdzie κ dane jest wzorem (3.8).*

Dowód. Załóżmy najpierw, że $h = \varphi(a)$ i niech $K = Ker(\varphi)$. Wtedy

$$\varphi(ak) = \varphi(a)\varphi(k) = h, \quad k \in K.$$

Zatem wszystkie elementy warstwy aK przejdą na h. Jeśli ponadto $\varphi(b) = h$, to

$$\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = h^{-1}h = e_2,$$

gdzie e_2 jest elementem neutralnym H. Ale to oznacza, że $a^{-1}b \in K$ i stąd $b \in aK$. Innymi słowy, pokazaliśmy, że odwzorowanie $\varphi^* : G/K \to \varphi(G)$ dane wzorem

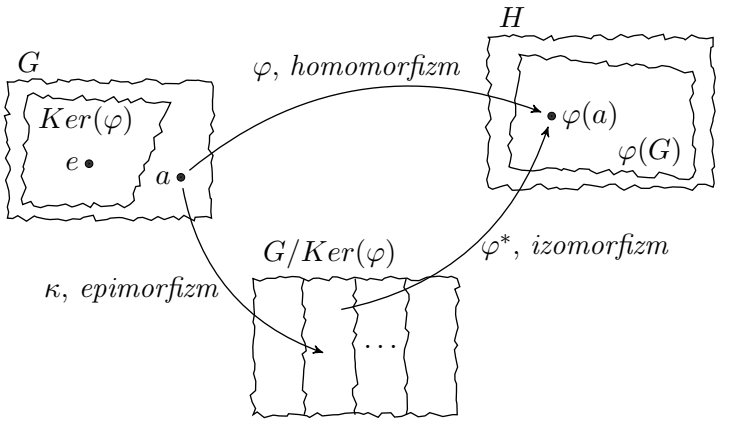
$$\varphi^*(aK) = \varphi(a), \quad a \in G,$$

jest dobrze określone, tzn. wartość φ^* na warstwie nie zależy od jej reprezentanta. Jeśli $aK = bK$, to $b^{-1}a \in K$ i stąd $\varphi^*(aK) = \varphi^*(bK)$. Podobnie dowodzi się, jeśli $\varphi(a) = \varphi(b)$, to $aK = bK$. Zatem φ^* jest bijekcją pomiędzy grupą G/K a $\varphi(G)$. Pozostaje pokazać, że φ^* jest homomorfizmem. Dla $a, b \in G$ mamy

$$\begin{aligned} \varphi^*((aK)(bK)) &= \varphi^*((ab)K) = \varphi(ab) = \varphi(a)\varphi(b) \\ &= \varphi^*(aK)\varphi^*(bK). \end{aligned}$$

Stąd φ^* jest izomorfizmem i ponadto

$$(\kappa\varphi^*)(a) = \varphi^*(\kappa(a)) = \varphi^*(aK) = \varphi(a). \square$$



Rys. 3.1 Ilustracja twierdzenia 3.11.

3.3 Iloczyn prosty i półprosty grup

Niech $(G_1, \circ)$ i $(G_2, \diamond)$ bedą dowolnymi grupami. **Iloczynem prostym** G_1 i G_2 nazywamy zbiór $G_1 \times G_2$ wraz z działaniem określonym wzorem

$$\boxed{(a_1, a_2) \otimes (b_1, b_2) := (a_1 \circ b_1, a_2 \diamond b_2),} \tag{3.9}$$

gdzie $a = (a_1, a_2), b = (b_1, b_2) \in G_1 \times G_2$. Za chwilę udowodnimy, że to działanie jest działaniem grupowym, natomiast często zamiast $(G_1 \times G_2, \otimes)$ pisze się po prostu $G_1 \times G_2$. Zauważmy, że jedynką tego działania jest $1_{G_1 \times G_2} = (1_{G_1}, 1_{G_2})$, tzn.

$$(a_1, a_2) \otimes (1_{G_1}, 1_{G_2}) = (a_1 \circ 1_{G_1}, a_2 \diamond 1_{G_2}) = (a_1, a_2),$$

gdzie 1_{G_1} to element neutralny G_1, a 1_{G_2} jest elementem neutralnym G_2.

Twierdzenie 3.12 *Niech G_1, G_2 będą grupami. Wówczas*

(i) *Iloczyn prosty jest grupą.*

(ii) *Grupa $G_1 \times G_2$ jest przemienna wtedy i tylko wtedy, gdy przemienna są G_1 i G_2,*

(iii) *Grupy $G_1 \times G_2$ i $G_2 \times G_1$ są izomorficzne.*

Dowód. Dowód (i). Łączność $\otimes$ wynika z łączności działań w poszczególnych grupach. Mianowicie, dla $a, b, c \in G_1 \times G_2$ mamy

$$\begin{aligned}(a \otimes b) \otimes c &= (a_1 b_1, a_2 b_2) \otimes (c_1, c_2) = ((a_1 b_1)c_1, (a_2 b_2)c_2) \\ &= (a_1(b_1 c_1), a_2(b_2 c_2)) = (a_1, a_2) \otimes (b_1 c_1, b_2 c_2) \\ &= (a_1, a_2) \otimes [(b_1, b_2) \otimes (c_1, c_2)] = a \otimes (b \otimes c).\end{aligned}$$

W powyższym zapisie pominięte zostały oczywiście $\circ$ i $\diamond$. Jedynką tej grupy jest $1_{G_1 \times G_2} = (1_{G_1}, 1_{G_2})$, natomiast element odwrotny do $a = (a_1, a_2)$ dany jest wzorem $a^{-1} = (a_1^{-1}, a_2^{-1})$. Dowód (ii) wynika z faktu, że równość

$$(a_1 b_1, a_2 b_2) = (b_1 a_1, b_2 a_2)$$

równoważna jest równościom $a_1 b_1 = b_1 a_1$ i $a_2 b_2 = b_2 a_2$.

Dowód (iii). Odwzorowanie

$$\varphi((a_1, a_2)) = (a_2, a_1).$$

jest izomorfizmem między $G_1 \times G_2$ a $G_2 \times G_1$. Z jednej strony jest to bijekcja, z drugiej strony mamy

$$\varphi(a \otimes b) = \varphi((a_1 b_1, a_2 b_2)) = (a_2 b_2, a_1 b_1)$$

oraz

$$\varphi(a) \otimes \varphi(b) = (a_2, a_1) \otimes (b_2, b_1) = (a_2 b_2, a_1 b_1).$$

Zatem $\varphi(a \otimes b) = \varphi(a) \otimes \varphi(b)$, dla wszystkich $a, b \in G_1 \times G_2$. $\square$

Jeśli G_1, G_2 są skończone, to $|G_1 \times G_2| = |G_1| \cdot |G_2|$. Nietrudno pokazać, że jesli H_1 jest podgrupą G_1 i H_2 podgrupą G_2, to $H_1 \times H_2$ jest podgrupą $G_1 \times G_2$. Twierdzenie odwrotne nie jest jednak prawdziwe, tzn. jeśli H jest podgrupą $G_1 \times G_2$, to wcale nie musi być podgrupą postaci $H_1 \times H_2$, gdzie H_1, H_2 są odpowiednio podgrupami G_1, G_2.

Grupa $H = G_1 \times \{e_2\}$ jest izomorficzna z G_1 i jest podgrupą niezmienniczą $G_1 \times G_2$. Mamy bowiem

$$aH = \{(a_1 h_1, a_2 h_2) : h \in H\} = \{(a_1 h_1, a_2) : h \in H\}$$

oraz

$$Ha = \{(h_1a_1, h_2a_2) : h \in H\} = \{(h_1a_1, a_2) : h \in H\}.$$

Równość $aH = Ha$ wynika z faktu, że $h_1 \in G_1$. Podobnie dowodzi się, że $\{e_1\} \times G_2$ jest też podgrupa niezmienniczą.

Przykład 3.3 (a) Rozpatrzmy $\mathbb{Z}_2 \times \mathbb{Z}_2$. W tym przypadku

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}.$$

Grupa ta składa się z 4 elementów i jest izomorficzna z grupą czwórkową V_4. Izomorfizm $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to V_4$ wygląda następująco

$$\varphi((0,0)) = 1, \quad \varphi((0,1)) = a, \quad \varphi((1,0)) = b, \quad \varphi((1,1)) = ab.$$

Przykład ten pokazuje, że iloczyn prosty grup cyklicznych nie musi być grupa cykliczną, tzn. $\mathbb{Z}_2 \times \mathbb{Z}_2$ jest izomorficzna z niecykliczną grupą V_4.

Tabela 3.3 Iloczyn prosty $\mathbb{Z}_2 \times \mathbb{Z}_2$ jest grupą izomorficzną z V_4.

$\cdot$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

(b) Niech $(\mathbb{R}^*, \circ)$ będzie grupą z przykładu 1.1. Działanie w $\mathbb{R}^* \times \mathbb{R}^*$ wygląda następująco

$$(a_1, a_2) \circ (b_1, b_2) = \begin{cases} (a_1b_1, a_2b_2), & a_1 > 0, a_2 > 0, \\ (a_1b_1, a_2/b_2), & a_1 > 0, a_2 < 0, \\ (a_1/b_1, a_2b_2), & a_1 < 0, a_2 > 0, \\ (a_1/b_1, a_2/b_2), & a_1 < 0, a_2 < 0. \end{cases}$$

Podzbiór $\mathbb{R}^* \times \mathbb{R}^*$ składający się z I i III ćwiartki jest jej podgrupą nieprzemienną, np.

$$(-2,-2) \circ (-1,-1) = (2,2), \quad (-1,-1) \circ (-2,-2) = (1/2, 1/2). \square$$

Iloczyn prosty jest jednym z narzędzi do tworzenia nowych grupy z już istniejących. Pozwala też na konstrukcję różnych (tzn. nieizomorficznych) grup o tych samych rzędach. Jeśli np. $n = 24$, to możemy utworzyć kilka grup o tym rzędzie jako iloczyn prosty grup rzędu 12 i 2, 6 i 4, 3 i 8 itd.

Iloczynem prostym grup $G_1, G_2, \ldots, G_n$ nazywamy parę $(G, \otimes)$, gdzie $G = G_1 \times G_2 \times \ldots \times G_n$ oraz

$$a \otimes b := (a_1 b_1, a_2 b_2, \ldots, a_n b_n),$$

dla $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$. Podobnie jak w twierdzeniu 3.12 dowodzi się, że tak określona para jest grupą. Jej elementem neutralnym jest $1_G = (1_{G_1}, \ldots, 1_{G_n})$, a odwrotny do a to $(a_1^{-1}, \ldots, a_n^{-1})$.

Zmieniając dowolnie kolejność w iloczynie kartezjańskim $G_1 \times \ldots \times G_n$ otrzymamy w każdym przypadku grupę izomorficzną z $(G, \otimes)$. Na przykład dla $n = 3$ wszystkie grupy

$$\begin{array}{lll} G_1 \times G_2 \times G_3, & G_1 \times G_3 \times G_2, & G_2 \times G_1 \times G_3, \\ G_3 \times G_1 \times G_2, & G_2 \times G_3 \times G_1, & G_3 \times G_2 \times G_1 \end{array}$$

są izomorficzne.

Załóżmy teraz, że H_1 i H_2 są podgrupami normalnymi grupy G takimi, że $H_1 \cap H_2 = \{e\}$. Udowodnimy, że wtedy

$$ab = ba, \quad \text{dla wszystkich} \quad a \in H_1, b \in H_2. \tag{3.10}$$

Wynika stąd, że $H_1 H_2 = H_2 H_1$ i z twierdzenia 1.8 otrzymujemy, że $H_1 H_2$ jest podgupą G. Przechodzimy do dowodu ... Ponieważ H_1 jest normalna, to $bab^{-1} \in H_1$ lub równoważnie $ba^{-1}b^{-1} \in H_1$. Z normalności H_2 wynika, że $aba^{-1} \in H_2$. W takim razie

$$[a, b] = aba^{-1}b^{-1} = \underbrace{a(ba^{-1}b^{-1})}_{\in H_1} = \underbrace{(aba^{-1})b^{-1}}_{\in H_2} \in H_1 \cap H_2.$$

Jeśli więc $H_1 \cap H_2 = \{e\}$, to $[a, b] = e$, a to jest równoważne temu, że $ab = ba$, patrz (2.20). Zatem $H_1 H_2$ jest podgrupą.

Co więcej, jeśli $a_1 b_1 = a_2 b_2$, dla $a_1, a_2 \in H_1$ i $b_1, b_2 \in H_1$, to podobnie

$$\underbrace{a_2^{-1} a_1}_{\in H_1} = \underbrace{b_2 b_1^{-1}}_{\in H_2} \in H_1 \cap H_2.$$

Z równań $a_2^{-1} a_1 = e$, $b_2^{-1} b_1 = e$ otrzymujemy $a_1 = a_2$, $b_1 = b_2$.

Twierdzenie 3.13 *Jeśli H_1 i H_2 są podgrupami normalnymi grupy G takimi, że $H_1 \cap H_2 = \{e\}$ oraz $G = H_1 H_2$, to G jest izomorficzna z $H_1 \times H_2$.*

Dowód. Z dotychczasowych rozważań wynika, że każdy $g \in G$ zapisuje się jednoznacznie w postaci ab, gdzie $a \in H_1$ i $b \in H_2$. Zatem odwzorowanie $\varphi(g) = (a, b)$ jest bijekcją z G na $H_1 \times H_2$. Pozostaje sprawdzić, że jest to izomorfizm. Z równości $(a, b) = (e, e)$ wynika, że $a = e$ i $b = e$, zatem jądro φ równe jest $\{e\}$. Następnie, z przemienności mamy

$$\varphi(g_1 g_2) = \varphi(a_1 b_1 a_2 b_2) = \varphi(a_1 a_2 b_1 b_2) = (a_1 a_2, b_1 b_2)$$

oraz

$$\varphi(g_1)\varphi(g_2) = (a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Dowód jest więc zakończony. □

W przykładzie 3.3 mieliśmy do czynienia z sytuacją opisaną w powyższym twierdzeniu. Podgrupy $H_1 = \{e, a\}$ i $H_2 = \{e, b\}$ są dzielnikami normalnymi $V_4 = \{e, a, b, ab\}$, $H_1 \cap H_2 = \{e\}$ i $H_1 H_2 = V_4$. Ponadto są one izomorficzne z $\mathbb{Z}_2$, więc $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Grupa $\mathbb{Z}_{12}$ jest przemienna, a więc $H_1 = \{0, 3, 6, 9\}$ i $H_2 = \{0, 4, 8\}$ są jej dzielnikami normalnymi, $H_1 \cap H_2 = \{0\}$ oraz

$$H_1 H_2 = \{0, 4, 8, 3, 7, 11, 6, 10, 2, 9, 1, 5\} = \mathbb{Z}_{12}.$$

Zatem $\mathbb{Z}_{12}$ jest izomorficzna z $H_1 \times H_2$, a ponieważ $H_1 \cong \mathbb{Z}_4$ i $H_2 \cong \mathbb{Z}_3$, to $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$. Izomorfizm ten dany jest wzorem

$$\varphi(a) = (a \bmod 3, a \bmod 4), \quad a \in \mathbb{Z}_{12}.$$

W przypadku, gdy rzędy grup nie mają wspólnego dzielnika poza jedynką zachodzi następujące twierdzenie.

Twierdzenie 3.14 *Grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ jest cykliczna wtedy i tylko wtedy, gdy $NWD(m, n) = 1$.*

Dowód. Załóżmy, że $NWD(m, n) = 1$. Pokażemy, że wtedy $\mathbb{Z}_m \times \mathbb{Z}_n$ jest grupą cykliczną. Zgodnie z (3.9) mamy

$$(a_1, a_2) \otimes (b_1, b_2) := (a_1 +_m b_1, a_2 +_n b_2).$$

Niech rząd elementu $(1, 1)$ wynosi p. Wtedy $(1, 1)^p = (0, 0)$ i stąd

$$(p \,(\mathrm{mod} m), p \,(\mathrm{mod} n)) = (0, 0).$$

Wynika stąd, że p jest podzielne przez m i przez n. Ponieważ m i n nie mają wspólnych dzielników, więc $p = mn$. Stąd mamy

$$rz((1, 1)) = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$$

a więc $\mathbb{Z}_m \times \mathbb{Z}_n$ jest cykliczna oraz $(1,1)$ jest jej generatorem.

Implikacja w drugą stronę wygląda tak

$$\mathbb{Z}_m \times \mathbb{Z}_n \text{ cykliczna} \quad \Rightarrow \quad NWD(m,n) = 1.$$

Jest ona równoważna następującej implikacji

$$\sim NWD(m,n) = 1 \quad \Rightarrow \quad \sim \mathbb{Z}_m \times \mathbb{Z}_n \text{ cykliczna}.$$

Niech więc $NWD(m,n) = d > 1$. Oznaczmy $m_1 = m/d$, $n_1 = n/d$. Wtedy dla dowolnego $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ mamy równość

$$\begin{aligned} m_1 d n_1 \cdot (a,b) &= \Big(\frac{m}{d} d n_1 a (\mathrm{mod} m), m_1 d \frac{n}{d} b (\mathrm{mod} n)\Big) \\ &= (m n_1 a (\mathrm{mod} m), m_1 n b (\mathrm{mod} n)) = (0,0). \end{aligned}$$

Wynika stąd, że $rz((a,b)) \leq m_1 d n_1$. Zatem grupa ta nie zawiera elementu rzędu mn, a więc nie jest cykliczna. □

Niech $(G_1, \circ)$ i $(G_2, \diamond)$ będą grupami i załóżmy, że $\varphi : G_2 \to Aut(G_1)$ jest homomorfizmem. Oznacza to, że każdemu $a \in G_2$ przyporządkowany jest automorfizm φ_a grupy G_1 oraz

$$\varphi_{a \diamond b} = \varphi_a \varphi_b, \quad \text{dla wszystkich} \quad a, b \in G_2.$$

Działaniem w grupie $Aut(G_1)$ jest składanie przekształceń, które teraz zdefiniujmy w następujący sposób

$$\varphi_{a \diamond b}(g) = (\varphi_a \varphi_b)(g) := \varphi_a(\varphi_b(g)), \quad \forall\, g \in G_1. \tag{3.11}$$

Niezależnie od tego, przy ustalonym $a \in G_2$ zachodzi równość

$$\varphi_a(gh) = \varphi_a(g) \circ \varphi_a(h), \quad \text{dla dowolnych } g, h \in G_1.$$

Iloczynem półprostym G_1 i G_2 nazywamy zbiór $G_1 \times G_2$ wraz z działaniem określonym wzorem

$$\boxed{(a_1, a_2) \otimes (b_1, b_2) := (a_1 \circ \varphi_{a_2}(b_1), a_2 \diamond b_2),} \tag{3.12}$$

gdzie $a = (a_1, a_2), b = (b_1, b_2) \in G_1 \times G_2$. Pokażemy, że jest to działanie grupowe. Zaczniemy od łączności. Dla $a, b, c \in G_1 \times G_2$ z jednej strony mamy

$$(a \otimes b) \otimes c = (a_1 \varphi_{a_2}(b_1), a_2 b_2) \otimes c = (a_1 \varphi_{a_2}(b_1) \varphi_{a_2 b_2}(c_1), a_2 b_2 c_2)$$

i z drugiej

$$\begin{aligned} a \otimes (b \otimes c) &= a \otimes (b_1\varphi_{b_2}(c_1), b_2c_2) = (a_1\varphi_{a_2}(b_1\varphi_{b_2}(c_1)), a_2b_2c_2) \\ &= (a_1\varphi_{a_2}(b_1)\varphi_{a_2}(\varphi_{b_2}(c_1)), a_2b_2c_2) \end{aligned}$$

Na podstawie (3.11) oba powyższe iloczyny są równe. Element neutralny to $e = (e_1, e_2)$ a odwrotny do a dany jest wzorem

$$(a_1, a_2)^{-1} = (\varphi_{a_2^{-1}}(a_1^{-1}), a_2^{-1}).$$

Sprawdzamy

$$\begin{aligned} a \otimes a^{-1} &= (a_1, a_2) \otimes (\varphi_{a_2^{-1}}(a_1^{-1}), a_2^{-1}) = (a_1\varphi_{a_2}(\varphi_{a_2^{-1}}(a_1^{-1})), a_2a_2^{-1}) \\ &= (a_1a_1^{-1}, a_2a_2^{-1}) = (e_1, e_2). \end{aligned}$$

Iloczyn półprosty G_1 i G_2 oznacza się zwykle przez $G_1 \rtimes G_2$. Ponieważ zależy on od φ, to czasem używa się też $G_1 \rtimes_\varphi G_2$ i mówi się, że jest to **iloczyn zewnętrzny**. Wynika to stąd, że mnożymy dwie nie związane ze sobą grupy. Szczególnym przypadkiem iloczynu półprostego jest zwykły iloczyn prosty. Wystarczy w tym celu przyjąć za $\varphi_a(g) = g$, dla każdego $a \in G_2$.

Rozważmy teraz jedną grupę G i jej dwie podgrupy H_1 i H_2. Załóżmy też, że spełnione są warunki

(i) $G = H_1H_2$.

(ii) $H_1 \cap H_2 = \{e\}$.

(iii) H_1 jest podgrupą normalną G.

W takiej sytuacji G nazywana jest **iloczynem półprostym** H_1 przez H_2. Niekiedy mówi się, że jest to iloczyn **wewnętrzny**. Gdyby H_2 była też podgrupą normalną, to G byłaby izomorficzna z $H_1 \times H_2$, mówi o tym twierdzenie 3.13. Tym razem opuszcza się więc założenie o normalności H_2.

Równoważność powyższych dwóch definicji iloczynu półprostego wyjaśnia następujące twierdzenie, patrz np. [8].

Twierdzenie 3.15 *Jeśli G jest iloczynem półprostym swoich podrgup H_1 przez H_2, to istnieje homomorfizm $\varphi : H_2 \to Aut(H_1)$ taki, że G jest izomorficzna z $H_1 \rtimes_\varphi H_2$.*

W przykładzie 1.9 opisana została grupa izometrii własnych trójkąta równobocznego D_3. Niech

$$H_1 = \{I, O, O^2\} \cong \mathbb{Z}_3, \quad H_2 = \{I, L_1\} \cong \mathbb{Z}_2.$$

Podgrupa H_1 jest dzielnikiem normalnym D_3, a H_2 nie jest, patrz przykład 3.2. Ponadto $H_1 \cap H_2 = \{I\}$ oraz

$$H_1H_2 = \{I, L_1, O, L_2, O^2, L_3\} = D_3.$$

Zatem $D_3 \cong H_1 \rtimes H_2$ lub równoważnie $D_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$. Natomiast $\mathbb{Z}_3 \times \mathbb{Z}_2$ jest izomorficzna z $\mathbb{Z}_6$.

Przykład 3.4 (a) Rozważmy $\mathbb{Z}_2$ i $(\mathbb{R}, +)$ i niech $\varphi : \mathbb{Z}_2 \to Aut(\mathbb{R})$ będzie dane przez odwzorowania: $\varphi_0(g) = g$, $\varphi_1(g) = -g$. Można je zapisać jednym wzorem $\varphi_a(g) = (-1)^a g$, gdzie $a \in \mathbb{Z}_2$ i $g \in \mathbb{R}$. Zatem

$$(a_1, a_2) \otimes (b_1, b_2) = (a_1 + (-1)^{a_2} b_1, (a_2 + b_2) \bmod 2),$$

gdzie $a, b \in \mathbb{R} \times \mathbb{Z}_2$. Zauważmy, że $\mathbb{R} \rtimes \mathbb{Z}_2$ nie jest grupą przemienną, mamy np. $(1,0) \otimes (0,1) = (1,1)$, $(0,1) \otimes (1,0) = (-1,1)$.

(b) Niech $G_1 = (\mathbb{R}_+, \cdot)$, $G_2 = (\{-1,1\}, \cdot)$ oraz $\varphi_a(g) = g^a$, dla $a \in G_2$, $g \in G_1$. Nietrudno sprawdzić, że jest to homomorfizm z G_2 w grupę $Aut(G_1)$. Stąd dla $a, b \in G_1 \rtimes G_2$ mamy

$$(a_1, a_2) \otimes (b_1, b_2) = (a_1 b_1^{a_2}, a_2 b_2) = \begin{cases} (a_1 b_1, b_2), & a_2 = 1 \\ (a_1/b_1, -b_2), & a_2 = -1. \end{cases}$$

Podobnie jak w (a) jest to grupa nieprzemienna, np.

$$(2,1) \otimes (1,-1) = (2,-1) \neq (1,-1) \otimes (2,1) = (1/2,-1). \square$$

Przykład 3.5 Niech A_4 będzie grupą obrotów czworościanu foremnego omówioną w przykładzie 1.11 i rozważmy

$$H_1 = \{I, O_5, O_6, O_7\}, \quad H_2 = \{I, O_1, O_1^2\}.$$

Pierwsza podgrupa, izomorficzna z grupą V_4, jest dzielnikiem normalnym A_4, obliczone warstwy znajdują się w tabeli 3.4. Druga grupa, izomorficzna z $\mathbb{Z}_3$ nie jest podgrupą niezmienniczą, mamy np.

$$O_3H_2 = \{O_3, O_2^2, O_7\} \neq H_2O_3 = \{O_3, O_4^2, O_5\}.$$

Zatem $A_4 \cong V_4 \rtimes \mathbb{Z}_3$. $\square$

Tabela 3.4 Warstwy względem H_1, która jest dzielnikiem normalnym A_4.

a	aH_1	H_1a
I, O_5, O_6, O_7	$\{I, O_5, O_6, O_7\}$	$\{I, O_5, O_6, O_7\}$
O_1, O_2, O_3, O_4	$\{O_1, O_2, O_3, O_4\}$	$\{O_1, O_2, O_3, O_4\}$
$O_1^2, O_2^2, O_3^2, O_4^2$	$\{O_1^2, O_2^2, O_3^2, O_4^2\}$	$\{O_1^2, O_2^2, O_3^2, O_4^2\}$

3.4 Zadania

Zadanie 3.1 Niech $(G, \circ)$ będzie grupą, a H jej podgrupą o indeksie 2. Definiujemy nowe działanie

$$a \diamond b = \begin{cases} a \circ b, & a \in H \\ a \circ b^{-1}, & a \notin H. \end{cases}$$

Udowodnić, że $(G, \diamond)$ jest grupą wtedy i tylko wtedy, gdy $(G, \circ)$ jest przemienna. Następnie pokazać, że jeśli $(G, \diamond)$ jest grupą, to jest ona przemienna wtedy i tylko wtedy, gdy $a^2 = e$, dla każdego $a \in H$ i $a^2 = d$, dla $a \in G \backslash H$, gdzie d jest pewnym elementem G. □

Zadanie 3.2 Wykazać, że iloczyn prosty V_4 z $\mathbb{Z}_2$, czyli

$$V_4 \times \mathbb{Z}_2 = \{(e,0), (e,1), (a,0), (a,1), (b,0), (b,1), (ab,0), (ab,1)\}$$

jest grupą izomorficzną z grupą

$$2^{\{a,b,c\}} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\},$$

w której działaniem jest różnica symetryczna, patrz przykład 1.2. Obie te grupy są też izomorficzne z $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Zadanie 3.3 Wykazać, że $\mathbb{Z}_2 \times \mathbb{Z}_4$ nie jest izomorficzna z grupą z poprzedniego zadania. □

Zadanie 3.4 Niech D_4 będzie grupą izometrii kwadratu z przykładu 1.10 oraz $H_1 = \{I, O, O^2, O^3\}$, $H_2 = \{I, L_1\}$ jej podgrupami. Sprawdzić, że spełnione są założenia twierdzenia 3.15, zatem $D_4 \cong H_1 \rtimes H_2$.

4. Permutacje

4.1 Grupy permutacji

W rozdziale tym zajmiemy się grupami permutacji. Jak wykazaliśmy wcześniej, zbiór wszystkich bijekcji danego zbioru wraz ze składaniem przekształceń tworzy grupę nazywaną też grupą symetryczną. O ile nie będzie powiedziane inaczej, zakładamy, że

$$X = \{1, 2, \ldots, n\}, \quad n \geq 1,$$

i zamiast $Sym(X)$ piszemy S_n. Ponieważ każdą permutację można utożsamić z ciągiem n-elementowym, w którym wszystkie elementy są różne i kolejność jest istotna, więc $|S_n| = n!$ Elementy S_n będziemy oznaczali małymi greckimi literami jak np. $\alpha, \beta, \gamma, \pi, \sigma$. Zatem

$$\alpha : X \to X, \quad i \to \alpha(i), \quad i = 1, \ldots, n.$$

Dla $\alpha, \beta \in S_n$ złożenie wyznaczamy ze wzoru

$$(\alpha \circ \beta)(i) = (\alpha\beta)(i) = \beta(\alpha(i)), \quad i = 1, \ldots, n. \tag{4.1}$$

Jednym ze sposobów zapisu permutacji jest następująca postać funkcyjna

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & \ldots & n \\ \beta(1) & \beta(2) & \ldots & \beta(n) \end{pmatrix}.$$

Elementy w pierwszym wierszu to argumenty, a w drugim wartości. Na początku wykorzystamy tę formę zapisu, potem przejdziemy na wygodniejszy zapis cyklowy. Zwróćmy uwagę na to, że argumenty nie muszą być zapisane w porządku rosnącym. Można je przestawiać, ale razem z odpowiadającymi im wartościami.

Równoważna forma zapisu złożenia (4.1) wygląda więc tak

$$\alpha\beta = \begin{pmatrix} 1 & 2 & \ldots & n \\ \beta(\alpha(1)) & \beta(\alpha(2)) & \ldots & \beta(\alpha(n)) \end{pmatrix}.$$

Permutację odwrotną obliczamy tak, jak wyznacza się funkcję odwrotną, czyli zamieniami wartości funkcji z jej argumentami. Zatem

$$\alpha^{-1} = \begin{pmatrix} \alpha(1) & \alpha(2) & \ldots & \alpha(n) \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Elementy w górnym wierszu, będące teraz argumentami, porządkuje się zwykle rosnąco razem z odpowiadającymi im wartościami z dolnego wiersza. Poniżej przykład iloczynu permutacji z grupy S_6

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix}}_{\alpha} \cdot \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 2 & 4 & 6 \end{pmatrix}}_{\beta} = \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 2 & 6 \end{pmatrix}}_{\alpha\beta}$$

Sprawdzamy: $\alpha(1) = 3$, $\beta(3) = 1$, stąd $(\alpha\beta)(1) = 1$. Podobnie $\alpha(2) = 1$, $\beta(1) = 5$, stąd $(\alpha\beta)(1) = 5$, itd. Permutacje odwrotne to

$$\alpha^{-1} = \begin{pmatrix} 3 & 1 & 2 & 5 & 4 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix}.$$

oraz

$$\beta^{-1} = \begin{pmatrix} 5 & 3 & 1 & 2 & 4 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 1 & 6 \end{pmatrix}.$$

Ustalmy $\alpha \in S_n$. Element $i \in X$ jest punktem stałym α, jeśli $\alpha(i) = i$. **Zbiór punktów stałych** permutacji α oznaczamy przez $Fix(\alpha)$, tzn.

$$Fix(\alpha) := \{i \in X : \alpha(i) = i\}.$$

Zbiór ten może być pusty i mamy trywialne oszacowanie $0 \leq |Fix(\alpha)| \leq n$. Zauważmy jednak, że permutacja nie może mieć dokładnie $n-1$ punktów stałych. Pozostały element musiałby pozostać na swoim miejscu i mielibyśmy n punktów stałych. Innymi słowy, $|Fix(\alpha)| = n$ lub $|Fix(\alpha)| \leq n-2$.

Nośnikiem permutacji nazywamy zbiór wszystkich punktów X, które nie są jej punktami stałymi. Nośnik α oznaczamy przez $Act(\alpha)$. Zatem

$$Act(\alpha) := \{i \in X : \alpha(i) \neq i\}.$$

Dla dowolnego $n \geq 1$ zachodzi więc równość

$$|Fix(\alpha)| + |Act(\alpha)| = n.$$

Wynika stąd na przykład to, że $|Act(\alpha)| = 0$ lub $|Act(\alpha)| \geq 2$, ponieważ niemożliwa jest sytuacja, w której $|Fix(\alpha)| = n-1$.

Niech $i \in Act(\alpha)$ oraz $j = \alpha(i)$. Z założenia $j \neq i$, zatem $\alpha(j) \neq j$. Zachodzi więc implikacja

$$i \in Act(\alpha) \quad \Rightarrow \quad \alpha(i) \in Act(\alpha). \tag{4.2}$$

Permutacje $\alpha, \beta \in S_n$ nazywamy permutacjami **niezależnymi** lub **rozłącznymi**, jeśli spełniony jest warunek

$$Act(\alpha) \cap Act(\beta) = \emptyset.$$

Poniżej przykład takich permutacji, gdzie dodatkowo zaznaczono ich nośniki. Mamy tutaj $Act(\alpha) = \{1, 2, 4\}$, $Act(\beta) = \{3, 5, 6\}$, zatem warunek

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix}.$$

Dla tych permutacji mamy

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix} = \beta\alpha.$$

Twierdzenie 4.1 *Jeśli $\alpha, \beta \in S_n$ są niezależne, to $\alpha\beta = \beta\alpha$.*

Dowód. Oznaczmy $A = Act(\alpha)$, $B = Act(\beta)$. Wówczas $A \cap B = \emptyset$ oraz

$$X = A \cup B \cup (X \setminus (A \cup B)).$$

Jeśli $i \in A$, to z (4.2) mamy $\alpha(i) \in A$. Z założenia $i, \alpha(i) \notin B$. Zatem

$$(\alpha\beta)(i) = \beta(\alpha(i)) = \alpha(i).$$

Z drugiej strony $(\beta\alpha)(i) = \alpha(\beta(i)) = \alpha(i)$ ponieważ $i \notin Act(\beta)$.

Jeśli $i \in B$, to $\beta(i) \in B$ i stąd $i, \beta(i) \notin A$. Zatem

$$(\alpha\beta)(i) = \beta(\alpha(i)) = \beta(i).$$

Ponadto $(\beta\alpha)(i) = \alpha(\beta(i)) = \beta(i)$.

Jeśli $i \in X \setminus (A \cup B)$, to $\alpha(i) = i$ oraz $\beta(i) = i$. Stąd mamy

$$(\alpha\beta)(i) = i = (\beta\alpha)(i).$$

Dowód twierdzenia jest więc zakończony. □

Rozłączność nośników nie jest jednak warunkiem koniecznym do tego, by permutacje były przemienne. Mamy np.

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}}_{\alpha} \cdot \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}}_{\beta} = \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}}_{\alpha\beta=\beta\alpha}$$

Nośniki tych permutacji to $Act(\alpha) = \{1, 2, 3, 4\}$, $Act(\beta) = \{2, 4\}$.

Permutacja $\alpha \in S_n$ nazywana jest **permutacją cykliczną** rzędu k, **cyklem** k-wyrazowym lub k-**cyklem**, jeśli $|Act(\alpha)| = k$ i można ją zapisać w następujący cykliczny sposób

$$\alpha(i_1) = i_2, \quad \alpha(i_2) = i_3, \quad \ldots, \quad \alpha(i_{k-1}) = i_k, \quad \alpha(i_k) = i_1$$

oraz $\alpha(i) = i$ dla $i \notin \{i_1, i_2, \ldots, i_k\}$. Cykl k-wyrazowy zapisujemy w postaci

$$\alpha = (i_1, i_2, \ldots, i_k).$$

Punktów stałych permutacji, czyli 1-cykli zwykle się nie zapisuje. Zauważmy, że permutacja odwrotna do k-cyklu jest też k-cyklem oraz

$$\alpha^{-1} = (i_1, i_k, \ldots, i_2).$$

Na przykład, permutacja

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

jest 4-cyklem. Zatem $(1, 2, 3, 4)^{-1} = (1, 4, 3, 2)$. Cykle $(1, 2, 3, 4)$, $(2, 3, 4, 1)$, $(3, 4, 1, 2)$, $(4, 1, 2, 3)$ przedstawiają ta samą permutację i w związku z tym są równe, tzn.

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

Podobnie jest z dowolnym k-cyklem, tzn. cykliczne przesunięcie elementów w prawą lub lewą stronę nie zmienia tej permutacji. Zatem

$$(i_1, i_2, \ldots, i_k) = (i_2, i_3, \ldots, i_k, i_1) = \ldots$$

Transpozycją lub 2-cyklem nazywamy cykl dwuwyrazowy. W tym przypadku $\alpha = (i, j)$. Zauważmy, że $(i, j)^2 = I$ i stąd $(i, j)^{-1} = (i, j)$. Ponadto $(i, j) = (j, i)$. Transpozycja jest więc permutacją, która zamienia ze sobą dwa elementy, a pozostałe zostawia na swoich miejscach. Oto przykład transpozycji

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

Zgodnie z definicją permutacji rozłącznych, cykle $(i_1, \ldots, i_k)$ i $(j_1, \ldots, j_l)$ są rozłączne, jeśli

$$\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset.$$

Z teorii liczb wiadomo, że każdą liczbę całkowitą można rozłożyć na iloczyn liczb pierwszych, np. $12 = 2^2 \cdot 3$. Podobnie jest z permutacjami. Nie każda permutacja jest oczywiście permutacją cykliczną, ale można ją zawsze rozłożyć na iloczyn rozłącznych składowych. Składowe te będą elementarnymi cyklami, z których składa się permutacja.

Twierdzenie 4.2 *Każda permutacja $\alpha \in S_n$ jest cyklem lub można ją przedstawić jako iloczyn rozłącznych cykli.*

Dowód. Dowód indukcyjny względem n. Dla $n = 1$ istnieje tylko jedna permutacja i jest to 1-cykl, więc twierdzenie jest prawdziwe. Załóżmy teraz, że twierdzenie jest prawdziwe dla każdego $k < n$ i zdefiniujemy ciąg elementów X następująco

$$i_1 = 1, \quad i_k = \alpha(i_{k-1}), \quad k \geq 2.$$

Wynika stąd w szczególności, że $i_k = \alpha^{k-1}(1)$. Ponieważ $|X| = n$, więc jest to ciąg ograniczony. Niech

$$r = \min\{k \geq 2 : i_k = 1\}.$$

Liczba ta jest skończona, co więcej $r \leq n$. Pokażemy, że $i_k \neq i_l$ dla dowolnych $1 < k < l \leq r$. W tym celu zauważmy, że równość $i_k = i_l$ równoważna jest równości $\alpha^{k-1}(1) = \alpha^{l-1}(1)$, która z kolei równoważna jest $1 = \alpha^{l-k}(1)$. Ponieważ $l - k \leq r - 2$, więc przeczyłoby to definicji r.

Jeśli $r = n$, to α jest n-cyklem. Jeśli $r < n$, to α można zapisać jako iloczyn r-cyklu $(i_1, \ldots, i_r)$ i pewnej permutacji β zbioru $Y = X \setminus \{i_1, \ldots, i_r\}$. Ponieważ $|Y| < n$, więc z założenia indukcyjnego wynika, że β jest iloczynem rozłącznych cykli. Zatem i α można przedstawić jako iloczyn rozłącznych cykli. □

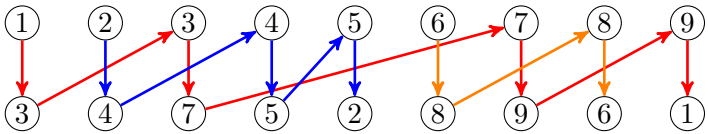
Przykład 4.1 (a) Rozważmy permutację

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 7 & 5 & 2 & 8 & 9 & 6 & 1 \end{pmatrix}.$$

Bierzemy na zmianę argumenty i wartości zaczynając od 1

$$1 \to 3 \to 7 \to 9 \to 1$$

czyli powstał 4-cykl (1,3,7,9). Następnie $2 \to 4 \to 5 \to 2$ czyli mamy 3-cykl $(2, 4, 5)$ oraz $6 \to 8 \to 6$, czyli transpozycja $(6, 8)$. Zatem α zapisujemy jako $\alpha = (1, 3, 7, 9)(2, 8, 5)(4, 6)$.



Rys. 4.1 Każdą permutację można zapisać jako iloczyn rozłącznych cykli.

(b) Permutacja

$$\beta = (1,2)(1,4)(3,4,6)(1,5,3)(4,5)$$

jest iloczynem cykli, ale nie są one rozłączne. Aby uzyskać rozkład na rozłączne cykle, należy kolejno wykonać mnożenia. Zatem

$$\begin{aligned}\beta &= (1,2,4)(3,4,6)(1,5,3)(4,5) = (1,2,6,3,4)(1,5,3)(4,5)\\ &= (1,2,6)(3,4,5)(4,5) = (1,2,6)(4,5).\end{aligned}$$

Ostatecznie $\beta = (1,2,6)(4,5)$. □

Transpozycję (i,j) nazywamy **transpozycją elementów sąsiednich**, jeśli $j = i+1$ lub równoważnie $i = j-1$. Wszystkich transpozycji w grupie S_n jest $\binom{n}{2}$, natomiast transpozycji elementów sąsiednich mamy $n-1$ i są to permutacje

$$(1,2),(2,3),\ldots,(n-1,n).$$

Zauważmy, że

$$\prod_{i=1}^{n-1}(i,i+1) = (1,n,n-1,\ldots,3,2).$$

Twierdzenie 4.3 *Prawdziwe są następujące stwierdzenia.*

(i) *Każdą permutację można zapisać jako iloczyn transpozycji.*

(ii) *Każda transpozycja jest iloczynem nieparzystej liczby transpozycji elementów sąsiednich.*

Dowód. Dowód (i) wynika z twierdzenia 4.2 oraz faktu, że dowolny cykl można przedstawić jako iloczyn transpozycji. Mianowicie, dla $k \geq 2$ zachodzi równość

$$(i_1,i_2,\ldots,i_k) = (i_1,i_2)(i_1,i_3)\ldots(i_1,i_{k-1})(i_1,i_k). \tag{4.3}$$

Po prawej stronie mamy $k-1$ transpozycji.

Dowód (ii). Jeśli $i < j$, to (i, j) można zapisać w postaci

$$(i, i+1)(i+1, i+2)\dots(j-1, j)(j-2, j-1)\dots(i+1, i+2)(i, i+1).$$

W powyższym iloczynie mamy $2(j-i)-1$ składników. Liczba ta jest zawsze nieparzysta. □

Z powyższego twierdzenia wynika, że

$$\boxed{S_n = \langle\{(i, j) : i, j \in \{1, 2, \dots, n\}\}\rangle} \tag{4.4}$$

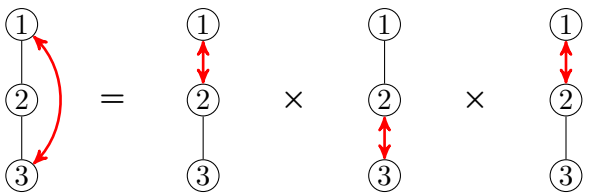
oraz

$$\boxed{S_n = \langle(1, 2), (2, 3), \dots, (n, n-1)\rangle.} \tag{4.5}$$

Mamy więc np. $(1, 3) = (1, 2)(2, 3)(1, 2)$, patrz rysunek 4.2. Podobnie transpozycję $(3, 7)$ zapisujemy jako

$$(3, 7) = (3, 4)(4, 5)(5, 6)(6, 7)(5, 6)(4, 5)(3, 4).$$

Mamy więc $2 \cdot (7-3) - 1 = 7$ transpozycji elementów sąsiednich.



Rys. 4.2 Każdą transpozycję można zapisać jako iloczyn transpozycji elementów sąsiednich.

Poniżej jeszcze jedno twierdzenie o generowaniu grupy S_n.

Twierdzenie 4.4 *Dla $n \geq 2$ mamy*

$$S_n = \langle(1, 2), (1, 3), \dots, (1, n)\rangle \tag{4.6}$$

$$S_n = \langle(1, 2, 3, \dots, n), (1, 2)\rangle. \tag{4.7}$$

Dowód. Dowód (4.6). Wystarczy pokazać, że dowolną transpozycję można zapisać jako iloczyn transpozycji postaci $(1, i)$, dla $i = 2, \dots, n$. Dla dowolnych i, j mamy równość

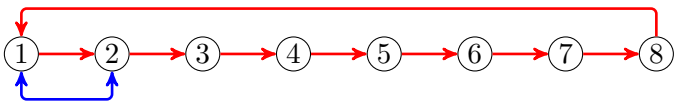
$$(i, j) = (1, i)(1, j)(1, i).$$

Z powyższej równości i z (4.4) wynika (4.6).

Dowód (4.7). Pokażemy, że za pomocą n-cyklu $(1, 2, \ldots, n)$ i transpozycji $(1, 2)$ można zapisać dowolną transpozycję elementów sąsiednich. Mianowicie, elementy i oraz $i+1$ „ustawiamy" najpierw na miejscach 1 i 2 za pomocą n-cyklu. Następnie wykonujemy transpozycję $(1, 2)$. Transpozycja ta zamieni i z $i + 1$. Po tym „wracamy" na elementy i oraz $i + 1$ przez permutację odwrotną do rozważanego n-cyklu. W ten sposób otrzymujemy transpozycję $(i, i + 1)$. Podsumowując

$$(i, i + 1) = (1, 2, \ldots, n)^{-i+1} \cdot (1, 2) \cdot (1, 2, \ldots, n)^{i-1},$$

dla $i = 2, 3, \ldots, n - 1$. Na podstawie (4.5) dowód jest zakończony. □



Rys. 4.3 Każdą permutację z grupy S_n można zapisać jako kombinację n-cyklu $(1, 2, \ldots, n)$ i transpozycji $(1, 2)$.

Zgodnie z definicją (1.12), rząd permutacji $\alpha \in S_n$ określony jest przez

$$rz(\alpha) = \min\{k \geq 1 : \alpha^k = I\}.$$

Z twierdzenia 1.4 wynika, że $rz(\alpha) = rz(\alpha^{-1})$ i $rz(\alpha\beta) = rz(\beta\alpha)$, dla dowolnych $\alpha, \beta \in S_n$. Aby obliczyć rząd danej permutacji, należy najpierw zapisać ją w postaci iloczynu rozłącznych cykli. Dla k-cyklu mamy bowiem

$$rz((i_1, i_2, \ldots, i_k)) = k.$$

Następnie, jeśli $\alpha = \prod_{i=1}^{m} \alpha_i$, gdzie $\alpha_1, \alpha_2, \ldots, \alpha_m$ są niezależnymi cyklami o długości odpowiednio $l_1, \ldots, l_m$, to

$$rz(\alpha) = \mathrm{NWW}(l_1, l_2, \ldots, l_m), \tag{4.8}$$

gdzie $\mathrm{NWW}(l_1, \ldots, l_m)$ oznacza najmniejszą wspólną wielokrotność $l_1, \ldots, l_m$. W ogólnym przypadku wartość ta nie przekracza iloczynu $l_1 \ldots l_m$ i jest równa $\prod_{i=1}^{m} l_i$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(l_i, l_j) = 1$, dla $i \neq j$. Innymi słowy, gdy każde dwie z tych liczb są względnie pierwsze.

Przykład 4.2 (a) Niech $\alpha \in S_{15}$ będzie następującą permutacją

$$\alpha = (1, 3, 4, 10, 14, 15)(2, 13, 5, 12)(6, 11)(7, 8, 9).$$

Na podstawie (4.8) mamy $rz(\alpha) = \text{NWW}(6, 4, 2, 3) = 12$.

(b) Jaki jest największy rząd permutacji z grupy S_{15}? W tym celu trzeba znaleźć największą wartość $\text{NWW}(l_1, \ldots, l_m)$ przy warunku

$$15 = l_1 + l_2 + \ldots + l_m,$$

gdzie $l_i \geq 1$ dla $i = 1, 2, \ldots, m$. Problem ten można rozwiązać eksperymentalnie. Permutacja, która składa się z jednego cyklu ma rząd co najwyżej 15. Jeśli jest iloczynem dwóch rozłącznych cykli, to największy rząd wynosi $\text{NWW}(8, 7) = 56$. Jeśli z kolei $\alpha = \alpha_1\alpha_2\alpha_3$, to maksymalny rząd uzyskamy dla $l_1 = 3$, $l_2 = 5$ $l_3 = 7$. Rząd ten wynosi $\text{NWW}(3, 5, 7) = 105$ i jest to największy rząd permutacji z S_{15}. Jedna z takich permutacji ma postać

$$(1, 2, 3)(4, 5, 6, 7, 8)(9, 10, 11, 12, 13, 14, 15).$$

Zauważmy, że rząd permutacji

$$(1, 2, 3, 4, 5)(6, 7, 8, 9, 10)(11, 12, 13, 14, 15)$$

wynosi 5. Trójka liczb $5, 5, 5$ maksymalizuje iloczyn $l_1l_2l_3$ równy w tym przypadku 125, nie maksymalizuje natomiast rzędu permutacji. □

Funkcja, która każdej liczbie naturalnej n przyporządkowuje największy rząd permutacji z S_n nazywa się **funkcją Landau** i oznaczana jest zwykle przez $g(n)$. W przykładzie 4.2 pokazaliśmy, że $g(15) = 105$. Rozkład na cykle permutacji o największym rzędzie nie musi być jednoznaczny. Na przykład $g(11) = 30$ i możliwe długości cykli to $5, 6$ lub $1, 2, 3, 5$. W 1902 roku Edmund Landau udowodnił, że

$$\lim_{n\to+\infty} \frac{\ln(g(n))}{\sqrt{n\ln(n)}} = 1.$$

Dla $n = 100$ iloraz pod granicą wynosi około 0.89. Więcej informacji na temat tej funkcji można znaleźć np. w [11]. W tabeli 4.1 podane są jej wartości do $n = 40$.

Niech dana będzie permutacja $\alpha \in S_n$, gdzie $n \geq 2$

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & j & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(i) & \ldots & \alpha(j) & \ldots & \alpha(n) \end{pmatrix}.$$

Elementy $\alpha(i), \alpha(j)$ tworzą **inwersję**, jeśli $i < j$ oraz $\alpha(i) > \alpha(j)$. Liczbę wszystkich inwersji w permutacji α oznaczamy przez $Inw(\alpha)$. Najmniejsza

Tabela 4.1 Wartości funkcja Landau do $n = 40$.

n	$g(n)$	n	$g(n)$	n	$g(n)$	n	$g(n)$
1	1	11	30	21	420	31	4620
2	2	12	60	22	420	32	5460
3	3	13	60	23	840	33	5460
4	4	14	84	24	840	34	9240
5	6	15	105	25	1260	35	9240
6	6	16	140	26	1260	36	13860
7	12	17	210	27	1540	37	13860
8	15	18	210	28	2310	38	16380
9	20	19	420	29	2520	39	16380
10	30	20	420	30	4620	40	27720

możliwa liczba inwersji wynosi zero. Jest tak dla permutacji tożsamościowej, tzn. $Inw(I) = 0$. Natomiast największa liczba inwersji wynosi $\binom{n}{2}$ dla permutacji

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & n-1 & n-2 & \dots & 2 & 1 \end{pmatrix}.$$

W tym przypadku każda para liczb tworzy inwersję, zatem

$$Inw(\gamma) = (n-1) + (n-2) + \ldots + 1 = \frac{n(n-1)}{2} = \binom{n}{2}.$$

Zauważmy, że $\gamma = (1,n)(2,n-1)\cdot\ldots$ jest iloczynem rozłącznych transpozycji. W zależności od parzystości n mamy

$$\gamma = \begin{cases} (1,2m)(2,2m-1)\ldots(m,m+1), & n = 2m, \\ (1,2m+1)(2,2m)\ldots(m,m+2), & n = 2m+1. \end{cases}$$

W obu przypadkach występuje m transpozycji. Gdy n jest liczbą nieparzystą, to γ ma jeden punkt stały. Rząd tej permutacji wynosi dwa, zatem $\gamma^{-1} = \gamma$.

Permutację $\alpha \in S_n$ nazywamy permutacją **parzystą**, jeśli liczba inwersji w niej występująca jest parzysta. Permutację nazywamy **nieparzystą**, jeśli $Inw(\alpha)$ jest nieparzysta. **Znakiem** permutacji nazywamy liczbę $(-1)^{Inw(\alpha)}$ i oznaczamy przez $Sgn(\alpha)$. Zatem

$$Sgn(\alpha) = (-1)^{Inw(\alpha)} = \begin{cases} 1, & \alpha \quad \text{parzysta} \\ -1, & \alpha \quad \text{nieparzysta.} \end{cases}$$

Permutacja tożsamościowa jest parzysta, ponieważ $Inw(I) = 0$. Pokażemy teraz, że pojedyncza transpozycja jest permutacją nieparzystą, czyli

$$\boxed{Sgn((i,j)) = -1, \quad \text{dla dowolnych} \quad i \neq j.} \tag{4.9}$$

Permutacja (i,j) w zapisie funkcyjnym bez argumentów ma postać

$$1, 2, \ldots, i-1, \boxed{j}, i+1, \ldots, j-1, \boxed{i}, j+1, \ldots, n.$$

Element j tworzy łącznie $j-i$ inwersji. Ponadto elementy od $i+1$ do $j-1$ tworzą inwersję z i. Stąd

$$Inw((i,j)) = (j-i) + (j-i-1) = 2(j-i) - 1.$$

Liczba ta jest zawsze nieparzysta i stąd wynika (4.9). Okazuje się też, że pomnożenie dowolnej permutacji przez transpozycję zmienia jej parzystość.

Twierdzenie 4.5 *Dla dowolnego $\alpha \in S_n$ i dowolnej transpozycji $\beta = (k,l)$ mamy równość*

$$Sgn(\alpha)Sgn(\alpha\beta) = Sgn(\alpha)Sgn(\beta\alpha) = -1. \tag{4.10}$$

Dowód. Rozważmy najpierw sytuację, w której $\beta = (k, k+1)$. Wówczas $\alpha(i) = k$, $\alpha(j) = k+1$, dla pewnych i, j. Stąd mamy

$$\begin{aligned}\alpha\beta &= \begin{pmatrix} 1 & \ldots & i & \ldots & j & \ldots & n \\ \alpha(1) & \ldots & k & \ldots & k+1 & \ldots & \alpha(n) \end{pmatrix} \begin{pmatrix} 1 & \ldots & k & k+1 & \ldots & n \\ 1 & \ldots & k+1 & k & \ldots & n \end{pmatrix} \\ &= \begin{pmatrix} 1 & \ldots & i & \ldots & j & \ldots & n \\ \alpha(1) & \ldots & k+1 & \ldots & k & \ldots & \alpha(n) \end{pmatrix}.\end{aligned}$$

Zatem $(\alpha\beta)(i) = k+1$ oraz $(\alpha\beta)(j) = k$. Jeśli w α pomiędzy k a $k+1$ jest x liczb mniejszych od k, to wtedy

$$Inw(\alpha\beta) = Inw(\alpha) - x + (x+1) = Inw(\alpha) + 1$$

i stąd

$$Sgn(\alpha)Sgn(\alpha\beta) = (-1)^{2Inw(\alpha)+1} = -1.$$

Dowodzi to równości (4.10) w tym przypadku. Następnie, z twierdzenia 4.3 wynika, że dowolną transpozycję (k,l) można zapisać jako iloczyn nieparzystej ilości transpozycji elementów sąsiednich. Zatem pomnożenie α przez (k,l) zmieni ilość inwersji w α o liczbę nieparzystą. To dowodzi pierwszej części wzoru (4.10).

Rozważmy teraz iloczyn $\beta\alpha$. Dla $\beta = (k, k+1)$ mamy

$$\beta\alpha = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ 1 & \dots & k+1 & k & \dots & n \end{pmatrix} \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ \alpha(1) & \dots & \alpha(k) & \alpha(k+1) & \dots & \alpha(n) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ \alpha(1) & \dots & \alpha(k+1) & \alpha(k) & \dots & \alpha(n) \end{pmatrix}.$$

Elementy $\alpha(k)$ i $\alpha(k+1)$ zostały zamienione. Zatem $Inw(\beta\alpha) = Inw(\alpha)+1$ lub $Inw(\beta\alpha) = Inw(\alpha) - 1$. W obu przypadkach $Sgn(\alpha)Sgn(\beta\alpha) = -1$.

Następnie, dowolną transpozycję (k, l) można zapisać jako iloczyn nieparzystej liczby transpozycji postaci $(k, k+1)$, więc α i $\beta\alpha$ mają zawsze inną parzystość. □

Twierdzenie 4.6 *Iloczyn parzystej (nieparzystej) liczby transpozycji jest permutacją parzystą (nieparzystą).*

Dowód. Dowód indukcyjny względem liczby transpozycji. Jeśli $k = 1$, to iloczyn składa się z jednej transpozycji, która jest permutacją nieparzystą, patrz (4.9). Załóżmy teraz, że twierdzenie jest prawdziwe dla $k - 1$, tzn.

$$\alpha = (i_1, j_1)(i_2, j_2) \dots (i_{k-1}, j_{k-1}) \quad \Rightarrow \quad Sgn(\alpha) = (-1)^{k-1}.$$

Z (4.10) mamy

$$Sgn(\alpha \cdot (i_k, j_k)) = (-1)Sgn(\alpha) = (-1)^k.$$

To kończy dowód twierdzenia. □

Z powyższego twierdzenia i z (4.3) wynika, że

$$Sgn((i_1, i_2, \dots, i_k)) = \begin{cases} 1, & k = 2m+1, \\ -1, & k = 2m. \end{cases}$$

Zatem 3-cykl jest permutacją parzystą, 4-cykl jest permutacją nieparzystą, 5-cykl jest parzystą itd.

Twierdzenie 4.7 *Dla dowolnych $\alpha, \beta \in S_n$ zachodzi równość*

$$Sgn(\alpha)Sgn(\beta) = Sgn(\alpha\beta) \tag{4.11}$$

zatem $\varphi(\alpha) = Sgn(\alpha)$ jest homomorfizmem pomiędzy S_n a $(\{-1, 1\}, \cdot)$.

Dowód. Załóżmy najpierw, że β jest transpozycją. Wtedy z (4.10) mamy $Sgn(\alpha)Sgn(\alpha\beta) = -1$. Ponieważ $Sgn(\beta) = -1$ oraz $Sgn(\alpha) = 1/Sgn(\alpha)$, to $Sgn(\alpha\beta) = Sgn(\alpha)Sgn(\beta)$. Dowodzi to (4.11) w tym przypadku.

Załóżmy teraz, że wzór (4.11) jest prawdziwy dla dowolnego α i dowolnej permutacji β będącej iloczynem co najwyżej $l-1$ transpozycji. Pokażemy, że jest on też prawdziwy, jeśli β jest iloczynem l transpozycji.

Niech $\beta = \prod_{k=1}^{l}(i_k, j_k)$. Wówczas

$$Sgn(\alpha\beta) = Sgn(\alpha \prod_{k=1}^{l-1}(i_k, j_k)(i_l, j_l)) = Sgn(\alpha \prod_{k=1}^{l-1}(i_k, j_k))Sgn((i_l, j_l))$$
$$= Sgn(\alpha)Sgn(\prod_{k=1}^{l-1}(i_k, j_k))Sgn((i_l, j_l)) = Sgn(\alpha)Sgn(\beta).$$

Ponieważ każdą permutację można przedstawić w postaci iloczynu transpozycji, więc dowód twierdzenia jest zakończony. □

Twierdzenie 4.7 stwierdza, że iloczyn dwóch permutacji parzystych jest permutacją parzystą. Podobnie iloczyn dwóch permutacji nieparzystych jest permutacją parzystą. Natomiast iloczyn permutacji parzystej i nieparzystej jest permutacją nieparzystą. Równość (4.11) przenosi się na większą liczbę permutacji, tzn. $\prod_{i=1}^{k} Sgn(\alpha_i) = Sgn(\prod_{i=1}^{k} \alpha_i)$, dla dowolnych $\alpha_1, \ldots, \alpha_k$. Wynika stąd dalej, że

$$Sgn([\alpha, \beta]) = 1, \tag{4.12}$$

dla dowolnych $\alpha, \beta \in S_n$. Innymi słowy, komutator jest zawsze permutacją parzystą. Ponieważ $Sgn(\alpha) = Sgn(\alpha^{-1})$, więc

$$Sgn([\alpha, \beta]) = Sgn(\alpha)Sgn(\beta)Sgn(\alpha^{-1})Sgn(\beta^{-1})$$
$$= (Sgn(\alpha)Sgn(\beta))^2 = 1.$$

Przykład 4.3 (a) Niech $\alpha = (1, 2, 3, 4)$, $\beta = (4, 5)$ będą elementami S_5. Wówczas

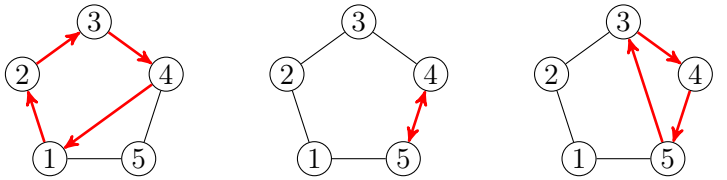
$$[\alpha, \beta] = (1, 2, 3, 4)(4, 5)(1, 4, 3, 2)(4, 5) = (3, 4, 5).$$

jest 3-cyklem, patrz rysunek 4.4.

(b) Dla $\alpha = (1, 2, 3, 4, 5)$ i $\beta = (1, 6, 7, 8, 2)$ z grupy S_8 mamy

$$[\alpha, \beta] = (1, 2, 3, 4, 5)(1, 6, 7, 8, 2)(1, 5, 4, 3, 2)(1, 2, 8, 7, 6)$$
$$= (1, 5)(2, 8).$$

Tym razem jest to podwójna transpozycja. Jest to w pewnym sensie permutacją trochę „słabsza" od 3-cyklu, patrz twierdzenie 5.6. □



Rys. 4.4 Komutator α i β jest w tym przypadku 3-cyklem.

Twierdzenie 4.8 *Liczba permutacji parzystych w S_n, gdzie $n \geq 2$, równa jest liczbie permutacji nieparzystych i w związku z tym wynosi $n!/2$.*

Dowód. Załóżmy, że w grupie S_n mamy k permutacji nieparzystych. Jedną z nich jest np. transpozycja $(1,2)$. Zdefiniujmy φ następująco

$$\varphi(\alpha) = \alpha \cdot (1,2), \quad \alpha \in S_n.$$

Ponieważ φ bijekcją, więc $\varphi(S_n) = S_n$. Ale z (4.10) wynika, że φ zmienia parzystość każdej permutacji. W S_n mamy więc jednocześnie k oraz $n! - k$ permutacji nieparzystych. Jest to możliwe tylko wtedy, gdy $k = n! - k$, czyli dla $k = n!/2$. Dowodzi to, że $k = n!/2$. □

Z twierdzenia 4.7 wynika, że $\varphi^{-1}(1)$, czyli zbiór permutacji parzystych jest podgrupą normalną S_n. Podgrupę tą nazywa się **grupą alternującą** stopnia n i oznacza zwykle przez A_n. Zatem

$$A_n = \text{grupa permutacji parzystych } X,$$

gdzie $X = \{1, 2, \ldots, n\}$. Jeśli X jest innym zbiorem n-elementowym, to grupę tą oznacza się $Alt(X)$. Z twierdzenia 4.8 wynika, że $|A_n| = n!/2$, dla $n \geq 2$. Dla $n = 3$ mamy $A_3 = \{I, (1,2,3), (1,3,2)\}$ oraz dla $n = 4$

$$\begin{aligned} A_4 = \{&I, (1,2,3), (1,3,2), (1,2,4), (1,4,2), (2,3,4), (2,4,3), \\ &(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}. \end{aligned}$$

Jest to grupa izomorficzna z grupą obrotów czworościanu foremnego opisaną w przykładzie 1.11.

Transpozycje są podstawowymi cegiełkami, z których zbudowane są wszystkie permutacje. Dla permutacji parzystych takimi cegiełkami są 3-cykle.

Twierdzenie 4.9 *Grupa permutacji parzystych jest generowana przez wszystkie 3-cykle, tzn.*

$$A_n = \langle \{(i,j,k) : i,j,k \in \{1,2,\ldots,n\}\} \rangle, \quad n \geq 3.$$

Dowód. Każdą permutację z A_n można zapisać w postaci iloczynu parzystej liczby transpozycji. Transpozycje te można połączyć w pary i wymnożyć. Możliwe wyniki dla każdej pary są następujące

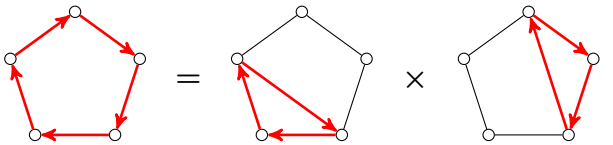
$$\begin{cases} (i,j)(i,j) = I, \\ (i,j)(i,k) = (i,j,k), \\ (i,j)(k,l) = (i,j,k)(k,i,l). \end{cases}$$

Wynika stąd, że każdy element A_n jest iloczynem 3-cykli. □

Na przykład, dla $\alpha = (1,2,3,4,5)$ mamy

$$\alpha = (1,2)(1,3)(1,4)(1,5) = (1,2,3)(1,4,5).$$

Sytuację tą przedstawiono na rysunku 4.5.



Rys. 4.5 Każdą permutację parzystą można zapisać jako iloczyn 3-cykli.

Przykład 4.4 Udowodnimy, że jeśli H jest podgrupą grupy S_n i H nie zawiera się w A_n, to dokładnie połowę elementów H stanowią permutacje parzyste. Druga połowa to permutacje nieparzyste. Dowód podobny jest do dowodu twierdzenia 4.8.

Niech $\beta \in H$ będzie jedną z permutacji nieparzystych. Z założenia istnieje przynajmniej jedna taka permutacja. Wówczas

$$\varphi(\alpha) = \alpha \cdot \beta, \quad \alpha \in H$$

jest bijekcją, która zmienia parzystość każdego elementu H. Jeśli liczba permutacji nieparzystych wynosi k, to $k = |H| - k$, tzn. $k = |H|/2$. □

Rozważmy grupę S_6. Spośród 720 elementów istnieje w niej 120 6-cykli, czyli permutacji postaci $(i_1, i_2, i_3, i_4, i_5, i_6)$. Wynika to z tego, że przy ustalonym i_1 można zmieniać porządek pozostałych elementów na 5!=120 sposobów. Jeśli chodzi o 5-cykle, to jest ich $\binom{6}{5} \cdot 4! = 144$. Najpierw wybieramy 5 liczb z sześciu, następnie z tych pięciu tworzymy 5-cykle. Podobnie liczba 4-cykli wynosi $\binom{6}{4} \cdot 3! = 90$. Liczba permutacji postaci $(i_1, i_2, i_3)(i_4, i_5)$ równa jest 120 i wynika ze wzoru $\binom{6}{3}\binom{3}{2}2!$.

Zliczymy jeszcze elementy typu $(i_1, i_2, i_3)(i_4, i_5, i_6)$. Ponieważ w obu cyklach mamy po 3 elementy, to przy wyborze tych elementów do cykli permutacje zostaną policzone dwukrotnie. Kolejność cykli rozłącznych nie jest istotna w zapisie permutacji. Zatem mamy $\binom{6}{3}\binom{3}{3}2!2!/2! = 40$ takich permutacji.

O permutacjach $\alpha, \beta \in S_n$ mówimy, że mają ten sam typ, jeśli w rozkładzie na iloczyn cykli rozłącznych mają jednakową ilość cykli tej samej długości. Na przykład permutacje $(1,2)(3,4)(5,6)$ i $(1,3)(2,4)(5,6)$ mają ten sam typ, natomiast $(1,2,3)$ i $(1,2)(3,4)$ nie mają tego samego typu.

Na podstawie definicji (2.12) permutacje α i β są sprzężone, jeśli istnieje trzecia permutacja γ, dla której $\beta = \gamma\alpha\gamma^{-1}$. Twierdzenie 2.8 mówi, że relacja sprzężenia jest relacją równoważności i w związku z tym dzieli grupę S_n na rozłączne klasy. Okazuje się, że permutacje należą do tej samej klasy, jeśli mają ten sam typ. Dowodzimy tego w poniższych twierdzeniach.

Zanim przejdziemy do twierdzeń zauważmy, że jeśli

$$\beta = \gamma_1\alpha\gamma_1^{-1} = \gamma_2\alpha\gamma_2^{-1},$$

to permutacja $\gamma_1^{-1}\gamma_2$ jest przemienna z α, tzn.

$$\alpha(\gamma_1^{-1}\gamma_2) = (\gamma_1^{-1}\gamma_2)\alpha. \tag{4.13}$$

Z równości tej wynika, że $\gamma_1^{-1}\gamma_2$ należy do centralizatora α, czyli do zbioru wszystkich permutacji, z którymi α jest przemienna.

Twierdzenie 4.10 *Niech $\alpha \in S_n$ będzie permutacją, której rozkład na iloczyn rozłącznych cykli ma postać*

$$\alpha = (\alpha_{11} \ldots \alpha_{1k_1})(\alpha_{21} \ldots \alpha_{2k_2}) \ldots (\alpha_{m1} \ldots \alpha_{mk_m}).$$

Wówczas dla dowolnej permutacji $\beta \in S_n$ mamy

$$\beta\alpha\beta^{-1} = (\beta_{11} \ldots \beta_{1k_1})(\beta_{21} \ldots \beta_{2k_2}) \ldots (\beta_{m1} \ldots \beta_{mk_m}),$$

gdzie $\beta_{ij} = \beta^{-1}(\alpha_{ij})$.

Dowód. Zapiszmy β w postaci

$$\beta = \begin{pmatrix} \beta_{11} & \ldots & \beta_{1k_1} & \beta_{21} & \ldots & \beta_{2k_2} & \ldots & \beta_{m1} & \ldots & \beta_{mk_m} \\ \alpha_{11} & \ldots & \alpha_{1k_1} & \alpha_{21} & \ldots & \alpha_{2k_2} & \ldots & \alpha_{m1} & \ldots & \alpha_{mk_m} \end{pmatrix}$$

Innymi słowy, $\beta(\beta_{ij}) = \alpha_{ij}$ lub równoważnie $\beta^{-1}(\alpha_{ij}) = \beta_{ij}$. Następnie zauważmy, że

$$\beta\alpha\beta^{-1}(\beta_{ij}) = \begin{cases} \beta_{ij+1}, & j = 1, 2, \ldots, k_i - 1, \\ \beta_{i1}, & j = k_i. \end{cases}$$

dla $i = 1, 2, \ldots, m$. $\square$

Twierdzenie 4.11 *Niech $\alpha, \beta \in S_n$ będą dowolnymi permutacjami mającymi taki sam typ rozkładu na iloczyn rozłącznych cykli, tzn.*

$$\alpha = (\alpha_{11} \dots \alpha_{1k_1})(\alpha_{21} \dots \alpha_{2k_2}) \dots (\alpha_{m1} \dots \alpha_{mk_m}).$$
$$\beta = (\beta_{11} \dots \beta_{1k_1})(\beta_{21} \dots \beta_{2k_2}) \dots (\beta_{m1} \dots \beta_{mk_m}).$$

Wówczas $\beta = \gamma\alpha\gamma^{-1}$, gdzie

$$\gamma = \begin{pmatrix} \beta_{11} & \dots & \beta_{1k_1} & \beta_{21} & \dots & \beta_{2k_2} & \dots & \beta_{m1} & \dots & \beta_{mk_m} \\ \alpha_{11} & \dots & \alpha_{1k_1} & \alpha_{21} & \dots & \alpha_{2k_2} & \dots & \alpha_{m1} & \dots & \alpha_{mk_m} \end{pmatrix}.$$

Permutacje α i β są więc sprzężone.

Dowód. Podobnie jak w dowodzie poprzedniego twierdzenia sprawdzamy

$$\gamma\alpha\gamma^{-1}(\beta_{ij}) = \begin{cases} \beta_{ij+1}, & j = 1, 2, \dots, k_i - 1, \\ \beta_{i1}, & j = k_i. \end{cases}$$

dla $i = 1, 2, \dots, m$. W ogólnym przypadku γ nie jest wynaczona jednoznacznie. Wynika to z faktu, że elementy wewnątrz danego cyklu w α lub β można cyklicznie przestawiać. □

Przykład 4.5 Rozważmy $\alpha, \beta \in S_8$

$$\alpha = (1, 4)(2, 3, 6)(5, 8, 7), \quad \beta = (2, 5)(1, 6, 7)(3, 4, 8).$$

Oto przykładowe γ, dla których $\beta = \gamma\alpha\gamma^{-1}$

$$\gamma_1 = \begin{pmatrix} 2 & 5 & 1 & 6 & 7 & 3 & 4 & 8 \\ 1 & 4 & 2 & 3 & 6 & 5 & 8 & 7 \end{pmatrix} = (1, 2)(5, 4, 8, 7, 6, 3),$$
$$\gamma_2 = \begin{pmatrix} 2 & 5 & 1 & 6 & 7 & 3 & 4 & 8 \\ 4 & 1 & 2 & 3 & 6 & 5 & 8 & 7 \end{pmatrix} = (2, 4, 8, 7, 6, 3, 5, 1),$$
$$\gamma_3 = \begin{pmatrix} 2 & 5 & 1 & 6 & 7 & 3 & 4 & 8 \\ 1 & 4 & 3 & 6 & 2 & 7 & 5 & 8 \end{pmatrix} = (4, 5)(2, 1, 3, 7).$$

4.2 Punkty stałe permutacji

Zajmiemy się tutaj wyprowadzeniem wzorów na liczbę permutacji z daną liczbą punktów stałych. W szczególnych przypadkach permutacje takie można wyznaczyć bezpośrednio. Na przykład istnieje 6 permutacji z S_4, które

mają dokładnie dwa punkty stałe. Są to

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Można następnie wyprowadzić wzory rekurencyjne. W tym problemie najlepiej jest jednak wykorzystać zasadę włączeń i wyłączeń.

Jeśli A_1, A_2 są rozłącznymi zbiorami skończonymi, to liczba elementów w $A_1 \cup A_2$ równa jest $|A_1| + |A_2|$. W ogólnym przypadku mamy

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Powyższy wzór wynika z faktu, że jeśli $a \in A_1$ i $a \in A_2$, to w sumie $|A_1|+|A_2|$ zostanie on zliczony dwa razy.

Podstawiając $A_1 \cup A_2$ w miejsce A_1 i A_3 w miejsce A_2 otrzymujemy wzór dla trzech zbiorów

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| =& |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &+ |A_1 \cap A_2 \cap A_3|. \end{aligned}$$

Postępując podobnie dostajemy wzór dla dowolnych podzbiorów $A_1, \ldots, A_n$ pewnego skończonego zbioru X

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} (-1)^{i+1} s_i, \tag{4.14}$$

gdzie

$$s_i = \sum_{J \subset X, |J|=i} |\bigcap_{j \in J} A_j|. \tag{4.15}$$

Sumowanie w s_i odbywa się po wszystkich podzbiorach i-elementowych X, zatem liczba składników w tej sumie wynosi $\binom{n}{i}$. Mamy więc np.

$$\begin{aligned} s_1 &= |A_1| + |A_2| + \ldots + |A_n|, \\ s_2 &= |A_1 \cap A_2| + \ldots + |A_{n-1} \cap A_n|. \end{aligned}$$

Wzór (4.14) można następnie udowodnić indukcyjnie, lub też w następujący sposób. Załóżmy, że $a \in \bigcup_{i=1}^{n} A_i$. Zatem a należy do co najmniej jednego ze zbiorów $A_1, \ldots, A_n$. Niech k będzie liczbą zbiorów, do których należy a. Wówczas a zostanie zliczony k razy w składniku s_1, $\binom{k}{2}$ razy w s_2, $\binom{k}{3}$ razy

w s_3 itd. Zatem po prawej stronie wzoru (4.14) element a zostanie policzony dokładnie raz. Mianowicie

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \ldots + (-1)^{k-1}\binom{k}{k}$$
$$= 1 - \sum_{i=0}^{k}(-1)^i\binom{k}{i} = 1 - (1 + (-1))^k = 1.$$

W dalszym ciągu będziemy potrzebowali następującego twierdzenia. Jest to twierdzenia 10.2 z [4].

Twierdzenie 4.12 *Niech $A_1, \ldots, A_n$ będą podzbiorami skończonego zbioru X. Wtedy liczba elementów X, które należą do dokładanie m $(1 \leq m \leq n)$ spośród tych zbiorów wynosi*

$$\sum_{i=0}^{n-m}(-1)^i\binom{m+i}{m}s_{m+i}, \tag{4.16}$$

gdzie $s_1, \ldots, s_n$ dane są wzorem (4.15).

Wracamy do grupy S_n. Dla $m = 1, 2, \ldots, n$ oznaczmy

$$A_i := \{\alpha \in S_n : \alpha(i) = i\}.$$

Do zbioru A_i należą więc te permutacje, które zostawiają i na swoim miejscu. Stąd mamy $|A_i| = (n-1)!$, $|A_{i_1} \cap A_{i_2}| = (n-2)!$ i ogólnie

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = (n-k)!,$$

gdzie $\{i_1, \ldots, i_k\}$ jest k-elementowym podzbiorem $\{1, \ldots, n\}$. Zatem w naszej sytuacji

$$s_i = \binom{n}{i}(n-i)! = \frac{n!}{i!}, \quad i = 1, 2, \ldots, n. \tag{4.17}$$

Z (4.14) otrzymujemy wzór na liczbę permutacji, które mają co najmniej jeden punkt stały

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n}(-1)^{i+1}\frac{n!}{i!} = n!\sum_{i=1}^{n}(-1)^{i+1}\frac{1}{i!}.$$

Dla $m = 0, 1, 2, \ldots, n$ oznaczmy

$$S_n(m) = \{\alpha \in S_n : |Fix(\alpha)| = m\}.$$

Stąd liczba permutacji, które nie mają ani jednego punktu stałego wynosi $n! - n! \sum_{i=1}^{n} (-1)^{i+1}/i!$ lub równoważnie

$$|S_n(0)| = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n \frac{1}{n!}\right). \tag{4.18}$$

Z rozwinięcia Taylora e^x dla $x = 0$ wynika, że dla dużych n suma w nawiasie jest w przybliżeniu równa e^{-1}. Dokładniej, mamy

$$\lim_{n \to +\infty} \frac{|S_n(0)|}{n!} = \lim_{n \to +\infty} \sum_{i=0}^{n} (-1)^i \frac{1}{i!} = e^{-1} \approx 0.367.$$

Gdybyśmy wybrali losowo jedną z permutacji zbioru n-elementowego, to szansa, że permutacja ta nie ma punktu stałego wynosi w przybliżeniu 0.367. Zatem szansa wybrania permutacji, która ma przynajmniej jeden punkt stały wynosi około 0.623.

Twierdzenie 4.13 *Niech $n \geq 1$. Wówczas*

$$|S_n(m)| = \frac{n!}{m!} \sum_{i=0}^{n-m} (-1)^i \frac{1}{i!}. \tag{4.19}$$

Dowód. Na podstawie (4.16) i (4.17) mamy

$$\sum_{i=0}^{n-m} (-1)^i \binom{m+i}{m} \frac{n!}{(m+i)!} = \frac{n!}{m!} \sum_{i=0}^{n-m} (-1)^i \frac{1}{i!}.$$

Oznacza to koniec dowodu. □

Ponieważ $|S_n(n)| = 1$ i $|S_n(n-1)| = 0$, to wzory podobne do (4.18) otrzymujemy dla $m \leq n - 2$. I tak np.

$$|S_n(1)| = n! \left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} - \ldots + (-1)^{n-1} \frac{1}{(n-1)!}\right)$$
$$|S_n(2)| = \frac{n!}{2} \left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} - \ldots + (-1)^{n-2} \frac{1}{(n-2)!}\right).$$

Dla $n = 3$ istnieją dwie permutacje, które nie mają punktów stałych i są to $(1, 2, 3)$, $(1, 3, 2)$, czyli permutacje

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Stąd i z (4.18) otrzymujemy zależność rekurencyjną

$$|S_n(0)| = n|S_{n-1}(0)| + (-1)^n, \quad n \geq 2,$$

gdzie $|S_1(0)| = 0$. Natomiast z (4.19) otrzymujemy następującą rekurencję dla permutacji, które mają dokładnie m punktów stałych

$$|S_n(m)| = \frac{n}{m}|S_{n-1}(m-1)|, \quad m = 1, 2, \ldots, n.$$

W tabeli 4.2 podane są wartości obliczone z tych rekurencji do $n = 10$.

Dla $m \geq 1$ mamy też

$$\lim_{n\to+\infty} \frac{|S_n(m)|}{n!} = \lim_{n\to+\infty} \frac{1}{m!} \sum_{i=0}^{n-m} (-1)^i \frac{1}{i!} = \frac{1}{m!} e^{-1}.$$

Zatem granicznym rozkładem $|S_n(m)|$ jest rozkład Poissona. Przypomnijmy, że zmienna losowa X ma rozkład Poissona z parametrem $\lambda > 0$, jeśli

$$P(X = m) = e^{-\lambda} \frac{\lambda^m}{m!}, \quad m = 0, 1, 2, \ldots$$

Wartość oczekiwana takiej zmiennej wynosi λ. Wariancja też jest równa λ. Jesli λ jest liczbą całkowitą, to istnieją dwie najbardziej prawdopodobne wartości i są to λ i $\lambda - 1$. Jeśli $\lambda \notin \mathbb{N}$, to modą tego rozkładu jest $\lfloor \lambda \rfloor$.

Tabela 4.2 Punkty stałe grup permutacji od S_3 do S_{10}.

m	$S_3(m)$	$S_4(m)$	$S_5(m)$	$S_6(m)$	$S_7(m)$	$S_8(m)$	$S_{10}(m)$
0	2	9	44	265	1 854	14 833	1 334 961
1	3	8	45	264	1 855	14 832	1 334 960
2	0	6	20	135	924	7420	667 485
3	1	0	10	40	315	2464	222 480
4		1	0	15	70	630	55 650
5			1	0	21	112	11 088
6				1	0	28	1 890
7					1	0	240
8						1	45
9							0
10							1

4.3 Centralne twierdzenie graniczne

Każdej permutacji $\alpha \in S_n$ można przyporządkować liczbę inwersji w niej występujących. Jak już zauważyliśmy najmniejsza liczba inwersji wynosi zero, a największa $n(n-1)/2$. W celu dokładniejszego zbadania tego, jak wygląda rozkład permutacji ze względu na liczbę inwersji wprowadzimy pewne zmienne losowe.

Zaczniemy od przestrzeń probabilistycznej $(\Omega, \mathcal{F}, P)$, którą definiujemy następująco. Za Ω przyjmujemy S_n, $\mathcal{F}$ jest rodziną wszystkich podzbiorów Ω, a miara P jest tutaj klasycznym prawdopodobieństwem, czyli

$$P(\{\alpha\}) = \frac{1}{n!}, \quad \text{dla każdego } \alpha \in S_n.$$

Miara ta rozszerza się naturalnie na wszystkie podzbiory Ω.

Mówimy, że liczba $k \in \{1, \ldots, n\}$ tworzy w danej permutacji r inwersji, jeśli poprzedza r liczb spośród $1, 2, \ldots, k-1$. W ten sposób każdej permutacji można przyporządkować liczbę inwersji utworzonych przez element k. Zdefiniujmy więc

$$X_k(\alpha) = \text{liczba inwersji utworzonych przez } k \text{ w } \alpha. \tag{4.20}$$

Wartość X_k zależy oczywiście od α. Zatem X_k jest zmienną losową określoną na S_n o wartościach w zbiorze $\{0, 1, \ldots, k-1\}$. Łączna liczba inwersji w danej permutacji jest także zmienną losową. Oznaczymy ją tym razem przez $\Sigma_n(\alpha)$ zamiast $Inw(\alpha)$. Zatem zgodnie z definicją

$$\Sigma_n = X_1 + X_2 + \ldots + X_n. \tag{4.21}$$

Ponieważ jedynka jest najmniejszą liczbą w zbiorze, więc $X_1 = 0$, niezależnie od permutacji. Na przykład, dla permutacji

$$3, 2, 1, 5, 4, 10, 9, 7, 8, 6$$

mamy $X_1 = 0$, $X_2 = 1$, $X_3 = 2$, $X_4 = 0$, $X_5 = 1$, $X_6 = 0$, $X_7 = 1$, $X_8 = 1$, $X_9 = 3$ i $X_{10} = 4$. Zatem $\Sigma_{10} = 13$.

Twierdzenie 4.14 *Zmienna losowa X_k ma rozkład jednostajny dyskretny na zbiorze $\{0, 1, \ldots, k-1\}$, czyli*

$$P(X_k = r) = \frac{1}{k}, \qquad r = 0, 1, \ldots, k-1. \tag{4.22}$$

Dowód. Zliczymy te permutacje, w których element k tworzy r inwersji.

Wybieramy najpierw r spośród $k-1$ liczb na $\binom{k-1}{r}$ sposobów. Oznaczmy te liczby przez $i_1, \ldots, i_r$. Pozostałe niewybrane to $i_{r+1}, \ldots, i_{k-1}$. Następnie wybieramy k spośród n miejsc, w których ustawiamy liczby $1, 2, \ldots, k$ następująco

$$i_{r+1}, \ldots, i_{k-1}, \boxed{k}, i_1, i_2, \ldots, i_r$$

Liczba takich wyborów wynosi $\binom{n}{k}$. Liczby po lewej stronie k można przestawiać na $r!$ sposobów, natomiast elementy po prawej stronie k przestawiamy na $(k-r-1)!$ sposobów. Liczby $k+1, k+2, \ldots, n$ ustawiamy na pozostałych miejscach na $(n-k)!$ sposobów. Zatem liczba wszystkich permutacji, w których k tworzy r inwersji wynosi

$$\binom{k-1}{r}\binom{n}{k} r!(k-r-1)!(n-k)! = \frac{n!}{k}.$$

Stąd otrzymujemy

$$P(X_k = r) = \frac{1}{n!} \cdot \frac{n!}{k} = \frac{1}{k}.$$

To kończy dowód twierdzenia. □

Z (4.22) otrzymujemy wzór na średnią

$$E(X_k) = \sum_{r=0}^{k-1} r \cdot \frac{1}{k} = \frac{1}{k} \cdot \frac{(1+k-1)(k-1)}{2} = \frac{k-1}{2}. \tag{4.23}$$

Podobnie obliczamy drugi moment

$$E(X_k^2) = \sum_{r=0}^{k-1} r^2 \cdot \frac{1}{k} = \frac{1}{k} \cdot \frac{(k-1)k(2k-1)}{6} = \frac{(k-1)(2k-1)}{6}.$$

Stąd mamy wzór na wariancję

$$D^2(X_k) = E(X_k^2) - E^2(X_k) = \frac{k^2-1}{12}, \quad k \geq 1. \tag{4.24}$$

Rozważmy $n = 8$ i zmienną X_8. Permutacje, w których 8 tworzy 7 inwersji mają postać

$$\boxed{8}, 1, 2, 3, 4, 5, 6, 7$$

Elementy, które znajdują się po prawej stronie ósemki można przestawiać w dowolny sposób. Nie ma to wpływu na wartość X_8. Innymi słowy, z informacji, że $X_8 = 7$ nie jesteśmy w stanie wywnioskować nic o wartościach

zmiennych $X_1, \ldots, X_7$. Podobnie, permutacje, w których 8 tworzy 5 inwersji mają postać

$$6, 7, \ 8\ , 1, 2, 3, 4, 5$$

Po prawej stronie ósemki mamy teraz pięć liczb, a po lewej dwie. Elementy te można znowu przestawiać dowolnie pod warunkiem, że po prawej stronie zawsze będzie pięć, a po lewej dwa. Tak jak wcześniej informacja, że $X_8 = 5$ nie ma pływu na wartości $X_1, \ldots, X_7$. Wnioskujemy stąd, że $X_1, \ldots X_7$ są niezależne od X_8. Jeśli teraz ustalimy wartość X_8 i X_7 to okaże się, że nie ma to wpływu na wartości $X_1, \ldots, X_6$, a więc te dwie grupy zmiennych losowych są niezależne. Z rozumowania tego wynika, że w ogólnym przypadku

$$P(X_1 = r_1, X_2 = r_2, \ldots, X_n = r_n) = \frac{1}{n!},$$

dla dowolnych dopuszczalnych $r_1, \ldots, r_n$, czyli dla $r_k \in \{0, 1, \ldots, k-1\}$, gdzie $k = 1, \ldots, n$. Zmienne losowe $X_1, X_2, \ldots, X_n$ są więc niezależne, ale nie mają takich samych rozkładów. Nie można więc zastosować najbardziej znanej wersji centralnego twierdzenia granicznego, w którym zakłada się równość rozkładów. Twierdzenie, które jest odpowiednie w naszej sytuacji wymaga spełnienia warunku Lindeberga (4.25). Następujące ogólne twierdzenie można znaleźć np. w [3].

Twierdzenie 4.15 *Niech $X_1, X_2, \ldots$ będzie ciągiem niezależnych zmiennych losowych o skończonych średnich $\mu_k = E(X_k)$ i wariancjach $\sigma_k^2 = D^2(X_k)$. Niech $\Sigma_n = X_1 + \ldots + X_n$, $m_n = \sum_{k=1}^n \mu_k$, $s_n^2 = \sum_{k=1}^n \sigma_k^2$ oraz dla $\varepsilon > 0$ zdefiniujmy*

$$U_k = \begin{cases} X_k - \mu_k, & |X_k - \mu_k| \le \varepsilon s_n \\ 0, & |X_k - \mu_k| > \varepsilon s_n. \end{cases}$$

Jeśli $\lim_{n\to\infty} s_n = +\infty$ oraz dla każdego $\varepsilon > 0$ spełniony jest warunek

$$\lim_{n\to+\infty} \frac{1}{s_n^2} \sum_{k=1}^n E(U_k^2) = 1, \tag{4.25}$$

to dla każdego $x \in \mathbb{R}$ mamy

$$\lim_{n\to+\infty} P\left(\frac{\Sigma_n - m_n}{s_n} \le x\right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{1}{2}t^2} dt. \ \square$$

W naszym przypadku, czyli dla zmiennych danych przez (4.20), na podstawie (4.23) mamy

$$m_n = E(\Sigma_n) = \tfrac{1}{2} \sum_{k=1}^{n} (k-1) = \tfrac{1}{4} n(n-1), \quad n \ge 1,$$

oraz z (4.24) otrzymujemy

$$s_n^2 = D^2(\Sigma_n) = \tfrac{1}{12}\sum_{k=1}^{n}(k^2-1) = \tfrac{1}{72}(2n^3+3n^2-5n).$$

Dla X_k mamy ponadto oszacowanie

$$X_k - \tfrac{1}{2}(k-1) \le \tfrac{1}{2}(k-1) \le n.$$

Ponieważ $s_n \approx C \cdot n^{3/2}$, więc dla dowolnego $\varepsilon > 0$ i dostatecznie dużego n zachodzi nierówność $X_k - \frac{1}{2}(k-1) \le \varepsilon s_n$. Zatem $U_k = X_k - \mu_k$ od pewnego k_0 i związku z tym warunek (4.25) jest spełniony. Zatem Σ_n ma asymptotyczny rozkład normalny. Dla $n = 10$ mamy $m_{10} = 22.5$, $s_{10}^2 = 31.25$ i zmienna losowa Σ_{10} przyjmuje wartości ze zbioru $\{0, 1, \ldots, 45\}$.

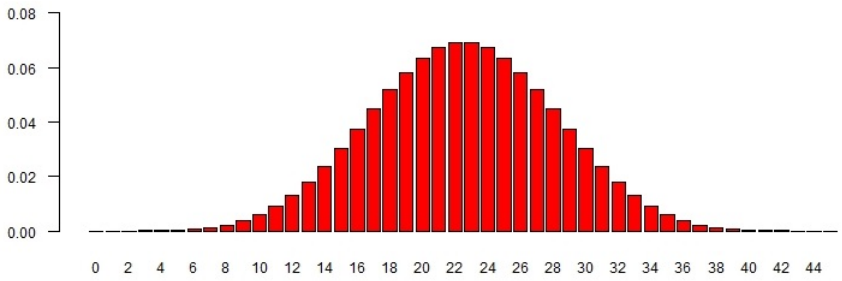
Korzystając z programu **Mathematica** i poniższej funkcji

ResourceFunction ["PermutationCountByInversions "][10]

otrzymamy listę z liczbą permutacji z daną liczbą inwersji od 0 do 45

```
{1, 9, 44, 155, 440, 1068, 2298, 4489, 8095, 13 640, 21 670,
32 683, 47 043, 64 889, 86 054, 110 010, 135 853, 162 337,
187 959, 211 089, 230 131, 243 694, 250 749, 250 749,
243 694, 230 131, 211 089, 187 959, 162 337, 135 853,
110 010, 86 054, 64 889, 47 043, 32 683, 21 670, 13 640,
8095, 4489, 2298, 1068, 440, 155, 44, 9, 1}
```

Jeśli liczby te podzielimy przez 10!, to otrzymamy rozkład prawdopodobieństwa Σ_{10}. Na rysunku 4.6 rozkład ten przedstawiony jest w postaci wykresu kolumnowego.



Rys. 4.6 Rozkład prawdopodobieństwa zmiennej losowej Σ_{10}.

5. Działanie grupy na zbiorze

5.1 Działanie, orbita, stabilizator

Niech X będzie dowolnym, niepustym zbiorem a G pewną grupą. **Działaniem grupy** G na zbiorze X nazywamy dowolny homomorfizm φ działający z G w grupę $Sym(X)$, czyli w zbiór wszystkich bijekcji zbioru X. Mówimy też równoważnie, że G **działa** na X. Permutację X odpowiadającą elementowi g oznaczamy przez φ_g. Ponieważ φ jest homomorfizmem, więc spełnione są warunki

$$\boxed{(1)\ \varphi_e = I, \qquad (2)\ \varphi_{gh} = \varphi_g \varphi_h,} \tag{5.1}$$

dla wszystkich $g, h \in G$. Tak jak w poprzednim rozdziale I oznacza permutację tożsamościową, tzn. $I(x) = x$, dla każdego $x \in X$. Jeśli $Ker(\varphi) = \{e\}$, to mówi się, że działanie φ jest **wierne**. Iloczyn $\varphi_g \varphi_h$ to złożenie odwzorowań, zatem w zgodnie z oznaczeniem (1.1) mamy

$$(\varphi_g \varphi_h)(x) = \varphi_h(\varphi_g(x)), \quad x \in X.$$

O działaniu grupy na zbiorze można też myśleć jako o funkcji dwóch zmiennych $\tilde{\varphi} : G \times X \to X$ zdefiniowanej jako $\tilde{\varphi}(g, x) := \varphi_g(x)$. Funkcja ta spełnia warunki

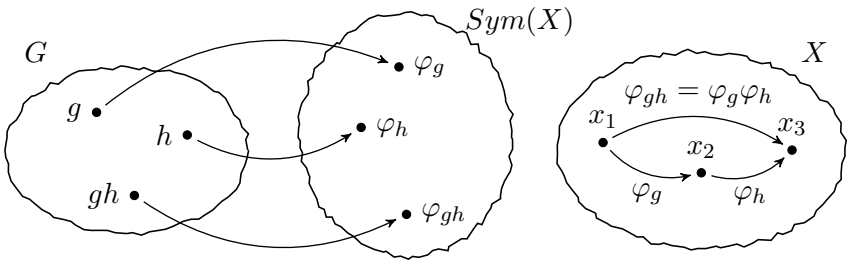
$$\tilde{\varphi}(e, x) = x, \quad \tilde{\varphi}(gh, x) = \tilde{\varphi}(h, \tilde{\varphi}(g, x)),$$

dla wszystkich i $g, h \in G$ i $x \in X$. Na rysunku 5.1 przedstawiono powyższe definicje w sposób bardziej przemawiający do wyobraźni.

W wielu przypadkach działanie grupy powstaje w sposób naturalny. Na przykład, grupa obrotów czworościanu foremnego, opisana w przykładzie 1.11, działa na wszystkie jego elementy, tzn. na wierzchołki, krawędzie i ściany. Na rysunku 1.5 zaznaczono działanie na wierzchołki, ale równie dobrze można to zrobić z krawędziami lub ścianami. W ten sposób otrzymalibyśmy pewne podgrupy S_6 i S_4. Byłyby one izomorficzne z A_4. W każdym z tych trzech przypadków działanie jest wierne, ponieważ tylko obrót identycznościowy zostawia poszczególne elementy na swoich miejscach.

Podobnie, dowolną podgrupę S_n można traktować jak grupę działającą na zbiorze $\{1, \ldots, n\}$. Działanie tej grupy polega na tym, że punkty $1, \ldots, n$ są przesuwane w inne miejsca. Homomorfizm, o którym mowa w (5.1) ma postać $\varphi_g = g$, gdzie g jest już permutacją z S_n.

Nic nie stoi na przeszkodzie, żeby przyjąć $X = G$. Zdefiniujemy 3 naturalne działania grupy na samej sobie. Są to działania ogólne i dotyczą każdej



Rys. 5.1 Działanie grupy G na zbiorze X.

grupy. Zanim to zrobimy, zauważmy jeszcze, że jeśli G działa na X i H jest podgrupą G, to H działa również na X. Wynika to bezpośrednio z (5.1).

Pierwsze działanie to działanie przez **prawe przesunięcie**, które definiujemy wzorem

$$\boxed{\varphi_g(a) = ag, \quad a \in G.} \tag{5.2}$$

Istotnie, $\varphi_e = I$, $\varphi_{gh}(a) = a(gh)$ oraz

$$(\varphi_g\varphi_h)(a) = \varphi_h(\varphi_g(a)) = (ag)h = \varphi_{gh}(a).$$

Drugie działanie to zmodyfikowane **lewe przesunięcie**

$$\boxed{\varphi_g(a) = g^{-1}a, \quad a \in G.} \tag{5.3}$$

Podobnie jak wcześniej, $\varphi_e = I$, $\varphi_{gh}(a) = (gh)^{-1}a$ oraz

$$(\varphi_g\varphi_h)(a) = \varphi_h(g^{-1}a) = h^{-1}(g^{-1}a) = (gh)^{-1}a = \varphi_{gh}(a).$$

Trzecie działanie to działanie przez **sprzężenie**, które definiujemy następująco

$$\boxed{\varphi_g(a) = g^{-1}ag, \quad a \in G.} \tag{5.4}$$

Równość $g^{-1}ag = g^{-1}bg$ równoważna jest równości $a = b$, więc φ_g jest injekcją. Z równania $g^{-1}ag = b$ wynika, że $a = gbg^{-1}$, więc φ_g jest także surjekcją i w rezultacie $\varphi_g \in Sym(G)$. Ponieważ $\varphi_e = I$, $\varphi_{gh}(a) = (gh)^{-1}a(gh)$ oraz

$$(\varphi_g\varphi_h)(a) = h^{-1}(g^{-1}ag)h = (gh)^{-1}a(gh) = \varphi_{gh}(a),$$

więc warunki (5.1) są spełnione.

W twierdzeniu 2.6 pokazaliśmy, że odwzorowanie $\psi_g(a) = gag^{-1}$, dla ustalonego g, jest izomorfizmem grupy G w siebie. Jest to po prostu zmodyfikowana wersja (5.4). Nie jest to jednak homomorfizm w sensie podanym w (5.1). Z jednej strony mamy $\psi_{gh}(a) = ghag(gh)^{-1}$, natomiast

$$(\psi_g\psi_h)(a) = \psi_h(\psi_g(a)) = hga(hg)^{-1}.$$

Podobna sytuacja jest z lewym przesunięciem. Jeśli $\psi_g(a) = ga$, to nie jest to homomorfizm w sensie (5.1). Stąd „modyfikacja" w (5.3). Poniższe twierdzenie to twierdzenie Cayleya, które mówi, że każda skończona grupa ma swoją reprezentację w pewnej grupie permutacji.

Twierdzenie 5.1 *Jeśli $G = \{g_1, \ldots, g_n\}$ jest grupą skończoną, to jest ona izomorficzna z pewną podgrupą S_n.*

Dowód. Każdemu $g \in G$ przyporządkujmy φ_g dane wzorem (5.2). Jest to bijekcja, patrz twierdzenie 2.4, zatem $\varphi_g \in Sym(G)$. Ponadto, odwzorowanie $g \to \varphi_g$ jest homomorfizmem G w $Sym(G)$.

Oznaczmy $H = \{\varphi_g : g \in G\}$. Z twierdzenia (2.2) wynika, że H jest podgrupą $Sym(G)$. Zatem $g \to \varphi_g$ jest izomorfizmem pomiędzy G a H. Ponieważ między zbiorem $\{g_1, \ldots, g_n\}$ i $\{1, \ldots, n\}$ istnieje bijekcja, więc $Sym(G) \cong S_n$ i to kończy dowód. □

Jeśli G działa na X, to każdemu $g \in G$ przyporządkowana jest permutacja φ_g zbioru X, którą będziemy również oznaczać przez $g(x)$.

Niech $x \in X$ i załóżmy, że $G = \{g_1, g_2, \ldots, g_n\}$. **Orbitą** x nazywamy zbiór

$$G(x) := x^G = Orb(x) = \{g_1(x), g_2(x), \ldots, g_n(x)\}.$$

W tym przypadku $|Orb(x)| \leq n$, dla każdego $x \in X$. Zauważmy też, że orbita jest zawsze niepusta ponieważ $x \in Orb(x)$. Jeśli ponadto X jest zbiorem skończonym, to i liczba wszystkich orbit jest także skończona.

Orbity są w istocie klasami abstrakcji następującej relacji równoważności określonej na X

$$x_1 R x_2 \quad \Leftrightarrow \quad x_2 = g(x_1), \quad \text{dla pewnego } g \in G.$$

W związku z tym dwie orbity są albo równe albo rozłączne i zbiór ich wszystkich stanowi podział X. Jeśli $\mathcal{O}_1, \ldots, \mathcal{O}_m$ są tymi orbitami, to

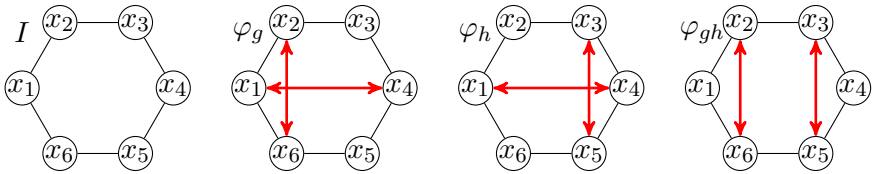
$$X = \bigcup_{i=1}^{m} \mathcal{O}_i, \quad \text{oraz} \quad \mathcal{O}_i \cap \mathcal{O}_j = \emptyset, \quad i \neq j.$$

Powyższe klasy nazywane są też **orbitami działania** G na X.

Przykład 5.1 (a) Niech $X = \{x_1, \ldots, x_6\}$ będzie zbiorem wierzchołków sześciokąta foremnego, patrz rysunek 5.2. Działanie $G = \{e, g, h, gh\}$, czyli grupy czwórkowej na X określamy następująco: $\varphi_e = I$ oraz

$$\varphi_g = (x_1, x_4)(x_2, x_6),\ \varphi_h = (x_1, x_4)(x_3, x_5),\ \varphi_{gh} = (x_1, x_5)(x_2, x_4).$$

Ponieważ jądrem φ jest e, więc jest to działanie wierne. Innymi słowy, grupę G można traktować jak podgrupę S_6 lub $Sym(X)$. Istnieją 3 orbity tego działania: $\{x_1, x_4\}$, $\{x_2, x_6\}$, $\{x_3, x_5\}$.



Rys. 5.2 Działanie grupy czwórkowej

(b) Dla G i X z punktu (a) określmy $\psi : \psi_e = I$, $\psi_g = \psi_h = (x_1, x_4)$ oraz $\psi_{gh} = \psi_g \psi_h = I$. Odwzorowanie to także jest homomorfizmem grupy G w $Sym(X)$, ale nie jest działaniem wiernym, ponieważ $Ker(\psi) = \{e, gh\}$. W tym przypadku istnieje 5 orbit: $\{x_1, x_4\}$, $\{x_2\}$, $\{x_3\}$, $\{x_5\}$, $\{x_6\}$. □

Niech $\mathcal{A}$ będzie ustalonym podzbiorem X. **Stabilizatorem punktowym** $\mathcal{A}$ w grupie G nazywamy zbiór tych elementów G, które zostawiają wszystkie punkty w $\mathcal{A}$ na swoich miejscach. Zatem

$$G_{(\mathcal{A})} := \{g \in G : g(x) = x, \text{ dla wszystkich } x \in \mathcal{A}\}.$$

Stabilizatorem łącznym zbioru $\mathcal{A}$ w grupie G nazywamy zbiór tych elementów G, które nie wyprowadzają punktów zbioru $\mathcal{A}$ z $\mathcal{A}$, tzn.

$$G_{\{\mathcal{A}\}} := \{g \in G : g(\mathcal{A}) = \mathcal{A}\}.$$

Łatwo widać, że $G_{(\mathcal{A})} \subset G_{\{\mathcal{A}\}}$. Jeśli permutacja zostawia punkty na swoich miejscach, to tym bardziej nigdzie ich nie „wyprowadza".

Dla $\mathcal{A} = \{x\}$ mamy oczywiście $G_{(x)} = G_{\{x\}}$ i w tym wypadku piszemy G_x. Aby uniknąć konfliktu oznaczeń z cyklami, jeśli $\mathcal{A} = \{x_1, \ldots, x_k\}$, to stabilizator punktowy tego zbioru oznaczamy przez $G_{x_1,\ldots,x_k}$.

Twierdzenie 5.2 *$G_{(\mathcal{A})}$ i $G_{\{\mathcal{A}\}}$ są podgrupami G oraz $G_{(A)}$ jest podgrupą normalną $G_{\{A\}}$.*

Dowód. Łatwo widać, że $e \in G_{(\mathcal{A})}$ i $e \in G_{\{\mathcal{A}\}}$. Inkluzja $G_{(\mathcal{A})} \subset G_{\{\mathcal{A}\}}$ również jest jasna. Załóżmy, że $g, h \in G_{\{\mathcal{A}\}}$. Wówczas

$$g(\mathcal{A}) = \mathcal{A},\ g^{-1}(\mathcal{A}) = \mathcal{A},\ h(\mathcal{A}) = \mathcal{A},\ h^{-1}(\mathcal{A}) = \mathcal{A}.$$

W rezultacie

$$(gh^{-1})(\mathcal{A}) = h^{-1}(g(\mathcal{A})) = \mathcal{A},$$

tzn. $gh^{-1} \in G_{\{\mathcal{A}\}}$. Z twierdzenia 1.6 wynika, że że rozważany zbiór jest podgrupą. Podobnie jeśli $g(x) = x$ i $h(x) = x$, dla $x \in \mathcal{A}$, to również $h^{-1}(g(x)) = x$, stąd $G_{(\mathcal{A})}$ też jest podgrupą.

Udowodnimy teraz, że

$$g \cdot G_{(\mathcal{A})} = G_{(\mathcal{A})} \cdot g, \quad \forall\, g \in G_{\{\mathcal{A}\}}.$$

W tym celu wystarczy pokazać, że $ghg^{-1} \in G_{(\mathcal{A})}$, dla każdego $h \in G_{(\mathcal{A})}$. Jeśli $x \in \mathcal{A}$, to mamy

$$(ghg^{-1})(x) = g^{-1}(h(g(x))) = g^{-1}(g(x)) = x.$$

Zatem $ghg^{-1} \in G_{(\mathcal{A})}$ i dowód twierdzenia jest zakończony. □

Ustalmy $x \in X$. Z twierdzenia 5.2 wynika, że stabilizator x, oznaczany także przez $Stab(x)$, czyli

$$G_x = Stab(x) = \{g \in G : g(x) = x\}$$

jest podgrupą grupy G. Rozważmy $h \notin G_x$ i powiedzmy, że $h(x) = x_1$. Wówczas warstwa prawostronna $G_x h$ składa się z elementów postaci gh, gdzie $g \in G_x$. Zauważmy, że wówczas $(gh)(x) = h(g(x)) = x_1$, więc

$$G_x h = \{g \in G : g(x) = x_1\}.$$

Zatem warstwa $G_x h$ składa się z tych permutacji, które przesuwają x na x_1. Fakt ten wykorzystamy w algorytmie Schreiera-Simsa w następnym rozdziale. Załóżmy, że $h'(x) = x_1$ i $h' \neq h$. Czy wtedy $G_x h = G_x h'$? Tak i wynika to z równoważności

$$\boxed{g_1(x) = g_2(x) \quad \Leftrightarrow \quad G_x g_1 = G_x g_2.} \tag{5.5}$$

Dla dowodu zauważmy, że równość $g_1(x) = g_2(x)$ równoważna jest równości $g_2^{-1}(g_1(x)) = x$, tzn. $g_1 g_2^{-1} \in G_x$ i stąd $g_1 \in G_x g_2$. To dowodzi (5.5).

Podobnie jest z warstwami lewostronnymi. Niech $h(x_1) = x$ i $h \notin G_x$. Wtedy

$$hG_x = \{g \in G : g(x_1) = x\},$$

czyli warstwa ta składa się z permutacji, które przesuwają x_1 na x. Jeśli ponadto $h'(x_1) = x$, to $h'G_x = hG_x$.

Teraz twierdzenie wiążące orbity ze stabilizatorami. Mamy tutaj pewną ciekawą rzecz. Jeśli dwa punkty leżą na tej samej orbicie, to ich stabilizatory są sprzężone.

Twierdzenie 5.3 *Niech G będzie grupą działającą na X i niech $|X| < \infty$. Wówczas*

(i) *Jeśli $x_2 = g(x_1)$, to $G_{x_1} = gG_{x_2}g^{-1}$.*

(ii) *Dla każdego $x \in X$ zachodzi wzór*

$$|G/G_x| = |G : G_x| = |x^G|. \tag{5.6}$$

(iii) *Jeśli G jest skończona, to*

$$|G| = |x^G| \cdot |G_x|, \quad \forall\, x \in X. \tag{5.7}$$

Dowód. Dowód (i). Załóżmy, że $x_2 = g(x_1)$ i $h \in G_{x_2}$. Wtedy $h(x_2) = x_2$ i stąd $h(g(x_1)) = g(x_1)$. Zatem $g^{-1}(h(g(x_1))) = x_1$, czyli $ghg^{-1} \in G_{x_1}$. Innymi słowy, $gG_{x_2}g^{-1} \subset G_{x_1}$.

Pokażemy teraz, że $G_{x_1} \subset gG_{x_2}g^{-1}$. Niech $h \in G_{x_1}$, tzn. $h(x_1) = x_1$. Ponieważ $g^{-1}(x_2) = x_1$, to

$$(g^{-1}hg)(x_2) = g(h(g^{-1}(x_2))) = g(h(x_1)) = g(x_1) = x_2.$$

Zatem $h' := g^{-1}hg \in G_{x_2}$ i stad $gh'g^{-1} = h$. Podsumowując, $h \in gG_{x_2}g^{-1}$.

Dowód (ii). Ustalmy $x \in X$ i załóżmy, że $Orb(x) = \{x_1, \ldots, x_k\}$. Zdefiniujmy odwzorowanie $\varphi : Orb(x) \to G/G_x$ następująco

$$\varphi(x_i) = G_x g, \quad \text{jeśli } g(x) = x_i.$$

Z (5.5) wynika, że φ jest dobrze określone i w związku z tym jest bijekcją. Zatem $|G/G_x| = k$ i stąd (5.6).

Dowód (iii). Korzystamy z twierdznia Lagrange'a. Ponieważ G_x jest podgrupą G, więc $|G| = |G/G_x| \cdot |G_x| = |x^G| \cdot |G_x|$. Tym samym dowód jest zakończony. □

Bezpośrednim wnioskiem z twierdzenia 5.3 jest

$$\boxed{Orb(x_1) = Orb(x_2) \quad \Rightarrow \quad |G_{x_1}| = |G_{x_2}|.} \tag{5.8}$$

Mianowicie, z równości $|x_1^G| \cdot |G_{x_1}| = |x_2^G| \cdot |G_{x_2}|$ i $|x_1^G| = |x_2^G|$ wynika właśnie powyższa implikacja.

Znane nam już pojęcia punktu stałego i nośnika permutacji rozszerzamy na zbiory permutacji. Niech H bedzie podzbiorem grupy G i niech G działa na X. **Nośnikiem** H nazywamy zbiór tych punktów, które pod wpływem H zostaną przesunięte, czyli

$$Act(H) := \{x \in X : g(x) \neq x, \text{ dla co najmniej jednego } g \in H\}.$$

Zbiorem punktów stałych H nazywamy zbiór tych punktów X, które pod wpływem H nie zostaną przesunięte, tzn.

$$Fix(H) := \{x \in X : g(x) = x, \text{ dla każdego } g \in H\}.$$

Twierdzenie 5.4 *Niech G będzie grupą skończoną działającą na X i niech $|X| < \infty$. Wtedy liczba orbit działania G wynosi*

$$m = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|. \tag{5.9}$$

Dowód. Niech Z będzie podzbiorem $G \times X$ określonym przez

$$Z = \{(g, x) : g(x) = x\}.$$

Następnie zauważmy, że

$$|Z| = \sum_{g \in G} Fix(g) = \sum_{x \in X} |G_x|. \tag{5.10}$$

Załóżmy, że istnieje m orbit i niech $\{x_1, \ldots, x_m\}$ będzie zbiorem reprezentantów tych orbit, tzn. $x_i \in \mathcal{O}_i$, dla $i = 1, \ldots, m$. Ponieważ $\bigcup_{i=1}^{m} \mathcal{O}_i = X$, więc z (5.8) otrzymujemy

$$\sum_{x \in X} |G_x| = \sum_{i=1}^{m} \Big(\sum_{x \in \mathcal{O}_i} |G_x| \Big) = \sum_{i=1}^{m} |x_i^G| \cdot |G_{x_i}| = \sum_{i=1}^{m} |G| = m|G|.$$

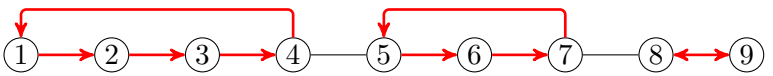
Podstawiając do (5.10) mamy $\sum_{g \in G} Fix(g) = m|G|$. □

Prawa strona wzoru (5.9) to średnia liczba punktów stałych przypadająca na element grupy. Jeśli istnieje tylko jedna orbita, to średnia ta wynosi 1. Załóżmy, że $|X| \geq 2$. Wówczas $|Fix(e)| = |X| > 1$. Jeśli średnia arytmetyczna nieujemnych liczb wynosi 1 i jedna z tych liczb jest większa od 1, to wśród nich musi istnieć taka, która jest mniejsza niż 1. Zatem w przypadku jednej orbity istnieje $g \in G$, dla którego $|Fix(g)| = 0$. Permutacja ta „przesuwa" wszystkie punkty X.

Przykład 5.2 Niech $X = \{1, 2, \ldots, 9\}$ i G będzie grupą cykliczną rzędu dwanaście określoną następująco

$$G = \langle \alpha \rangle, \quad \alpha = (1, 2, 3, 4)(5, 6, 7)(8, 9). \tag{5.11}$$

Jej działanie przedstawione jest na rysunku 5.3. Jest to ta sytuacja omawiana wcześniej, w której permutacja działa na „swoje" punkty.



Rys. 5.3 Działanie grupy danej przez (5.11)

Zauważmy, że α jest permutacją parzystą. Wynika to z faktu, że 4-cykl i transpozycja są nieparzyste oraz 3-cykl jest parzysty. Zatem wszystkie elementy G są permutacjami parzystymi. Jeśli chodzi o orbity, to mamy tutaj 3 orbity działania: $\mathcal{O}_1 = \{1, 2, 3, 4\}$, $\mathcal{O}_2 = \{5, 6, 7\}$, $\mathcal{O}_3 = \{8, 9\}$. Istotnie, dla $x_1 = 1$ mamy: $1 \to 1(I)$, $1 \to 2(\alpha)$, $1 \to 3(\alpha^2)$, $1 \to 4(\alpha^2)$, zatem $1^G = \{1, 2, 3, 4\}$. Łatwo jest wyznaczyć stabilizatory. Permutacje, które zostawiają jedynkę na miejscu to I, α^4 i α^8, zatem

$$G_1 = \{I, \alpha^4, \alpha^8\} = \{I, (5, 6, 7), (5, 7, 6)\}.$$

Ponadto $G_1 = G_2 = G_3 = G_4$. Podobnie obliczamy pozostałe stabilizatory. Wszystkie te informacje zostały zebrane w tabeli 5.1. Na koniec odnotujmy, że każdy stabilizator jest dzielnikiem normalnym grupy G, ponieważ jest ona przemienna. □

Tabela 5.1 Orbity działania i stabilizatory grupy danej przez (5.11)

X, x	Orbita, x^G	$\lvert x^G \rvert$	Stabilizator, G_x	$\lvert G_x \rvert$
1, 2, 3, 4	$\{1, 2, 3, 4\}$	4	$\{I, \alpha^2, \alpha^4\}$	3
5, 6, 7	$\{5, 6, 7\}$	3	$\{I, \alpha^3, \alpha^6, \alpha^9\}$	4
8, 9	$\{8, 9\}$	2	$\{I, \alpha^2, \alpha^4, \alpha^6, \alpha^8, \alpha^{10}\}$	6

Przykład 5.3 Niech $X = \{1, 2, 3, 4, 5\}$. Elementy tego zbioru rozmieszczamy tak jak na rysunku 5.4, przy czym taki sposob ich rozmieszczenia nie jest oczywiście istotny. Zadanie nasze polega na wyznaczeniu rzędu grupy

$$G = \langle \alpha \rangle, \quad \alpha = (1, 2, 3), \quad \beta = (1, 4, 5). \tag{5.12}$$

Zauważmy na początek, że α i β są parzyste, więc $\langle \alpha, \beta \rangle \subset A_5$. Rząd tej grupy może być równy co najwyżej 60. Pokażemy, że za pomocą α i β można otrzymać dowolny 3-cykl i w rezultacie każdą permutację parzystą zbioru pięcioelementowego. Innymi słowy, udowodnimy, że $G \cong A_5$.

Rys. 5.4 Generatory grupy (5.12)

Wszystkich 3-cykli jest $2 \cdot \binom{5}{3} = 20$, ale wystarczy pokazać jak otrzymać tylko dziesięć z nich. Zaczniemy od komutatora $[\beta, \alpha]$. Kolejno obliczamy: $\alpha^{-1} = (1, 3, 2)$, $\beta^{-1} = (1, 5, 4)$, $\beta\alpha = (1, 4, 5, 2, 3)$, $\beta^{-1}\alpha^{-1} = (1, 5, 4, 3, 2)$. Stąd mamy

$$\gamma := [\beta, \alpha] = (1, 4, 5, 2, 3) \cdot (1, 5, 4, 3, 2) = (1, 3, 5).$$

Za pomocą sprzężeń otrzymamy pozostałe 3-cykle. Zatem $\alpha\gamma\alpha^{-1} = (2, 5, 3)$, $\alpha^{-1}\gamma\alpha = (1, 5, 2)$, itd. Podsumowując, wszystkie 3-cykle wyrażone są za pomocą α i β

$$\begin{aligned}
(1,2,3) &= \alpha & (1,4,5) &= \beta \\
(1,2,4) &= [\beta^{-1}, \alpha^{-1}] & (2,3,4) &= \beta^{-1}\alpha\beta \\
(1,2,5) &= \alpha^{-1}\gamma^{-1}\alpha & (2,3,5) &= \beta\alpha\beta^{-1} \\
(1,3,4) &= \beta^{-1}\gamma^{-1}\beta & (2,4,5) &= (\alpha\beta)\gamma(\alpha\beta)^{-1} \\
(1,3,5) &= \gamma & (3,4,5) &= \alpha\beta\alpha^{-1}
\end{aligned}$$

Ponieważ $\alpha^2 = \alpha^{-1}$ i $\beta^2 = \beta^{-1}$, to każda z grup $\langle \alpha, \beta^2 \rangle$, $\langle \alpha^2, \beta^2 \rangle$, $\langle \alpha^2, \beta \rangle$ jest izomorficzna z A_5. Poza 3-cyklami w A_5 jest w $\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$ podwójnych transpozycji oraz $4! = 24$ cykle długości 5. Doliczając I mamy w sumie $20 + 15 + 24 + 1 = 60$ permutacji. □

5.2 Działanie przechodnie

Działanie grupy G na zbiorze X jest **przechodnie** lub **tranzytywne**, jeśli $x^G = X$, dla każdego $x \in X$. Innymi słowy, istnieje tylko jedna orbita. Równoważnie, dla punktów x_1, x_2 istnieje $g \in G$ takie, że $g(x_1) = x_2$.

Grupa działająca przechodnio na X jest **regularną**, jeśli $G_x = \{e\}$, dla każdego $x \in X$. Wprowadza się czasem pojęcie grupy **semi-regularnej**. Spełnia ona tylko warunek, że stabilizator każdego x składa się z jedynki bez założenia tranzytywności.

Z twierdzenia 5.3 wynika, że jeśli G jest skończona i działa tranzytywnie na X, to rodzina $\{G_x : x \in X\}$ jest klasą sprzężoności grupy G. Ponadto $|X| = |G/G_x|$ i $|G| = |X| \cdot |G_x|$, dla każdego $x \in X$.

Niech $k \in \mathbb{N}$ i niech X^k oznacza iloczyn kartezjański k kopii zbioru X. Działanie G na X przenosi się naturalnie na X^k. Mianowicie, definiujemy

$$g(\mathbf{x}) := (g(x_1), \ldots, g(x_k)),$$

gdzie $\mathbf{x} = (x_1, \ldots, x_k) \in X^k$. Oznaczmy przez $X^{(k)}$ podzbiór X^k składający się z tych ciągów, w których nie ma powtórzeń, tzn. jeśli $\mathbf{x} \in X^{(k)}$, to żadne dwa elementy spośród $x_1, \ldots, x_k$ nie są sobie równe. Jeśli X ma n elementów, to $|X^k| = n^k$ i $|X^{(k)}| = n!/(n-k)!$

Jeśli działanie G na $X^{(k)}$ jest przechodnie, to mówimy, że działanie G jest k-**przechodnie** lub k-**tranzytywne**. Intuicyjne rozumienie tego jest takie, że każdy ciąg k różnych punktów może przejść na każdy inny ciąg składający się z k punktów. Definicja ma więc sens, jeśli $k \leq |X|$. Nietrudno zauważyć, że grupa, która jest k-przechodnia jest też l-przechodnia, jeśli $l < k$.

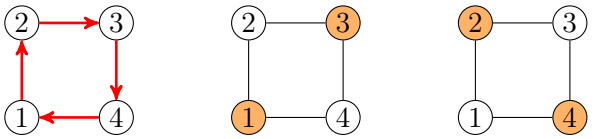
Niech $\mathcal{B}$ będzie podzbiorem X. Zdefiniujmy $\mathcal{B}^g := \{g(x) : x \in \mathcal{B}\}$. Jest to po prostu obraz $\mathcal{B}$ poprzez odwzorowanie g i może być też oznaczany jako $g(\mathcal{B})$. Niech G będzie grupą przechodnią na X.

Niepusty podzbiór $\mathcal{B} \subset X$ nazywamy **blokiem względem** G lub krótko **blokiem**, jeśli dla każdego $g \in G$ zachodzi jedna z równości

$$\mathcal{B}^g = \mathcal{B} \quad \text{lub} \quad \mathcal{B}^g \cap \mathcal{B} = \emptyset.$$

Intuicyjne rozumienie tego warunku jest takie, że elementy $\mathcal{B}$ zawsze „podróżują razem" w tym sensie, że albo razem zostają w $\mathcal{B}$ albo razem z niego wychodzą.

Zauważmy, że zarówno X jak i każdy zbiór jednoelementowy $\{x\}$ jest blokiem. Bloki te nazywane są blokami **trywialnymi**. O pozostałych blokach mówi się, że są **nietrywialne**. Blokiem **minimalnym** nazywamy blok o



Rys. 5.5 Nietrywialne bloki grupy cyklicznej $\langle(1,2,3,4)\rangle$.

najmniejszej liczbie elementów spośród wszystkich bloków o co najmniej dwóch elementach.

Niech $X = \{1,2,3,4\}$ i G będzie grupą cykliczną generowaną przez $\alpha = (1,2,3,4)$, patrz rysunek 5.5. Jest to grupa tranzytywna i istnieją dwa nietrywialne bloki: $\mathcal{B}_1 = \{1,3\}$, $\mathcal{B}_2 = \{2,4\}$. Blokiem nie jest natomiast $\{1,2\}$, ponieważ $\{1,2\}^\alpha = \{2,3\}$. Nie jest też blokiem $\{1,2,3\}$, mamy bowiem $\{1,2,3\}^\alpha = \{2,3,4\}$. W tym ostatnim przypadku jedynka i dwójka pozostały w zbiorze, natomiast 3 opuściła go i przeszła na 4.

Twierdzenie 5.5 *Niech $G = \{g_1, \ldots, g_n\}$ będzie grupą tranzytywną działającą na skończonym zbiorze X. Wówczas*

(i) *Jeśli $\mathcal{B}_1$ i $\mathcal{B}_2$ są blokami o niepustym przecięciu, to $\mathcal{B}_1 \cap \mathcal{B}_1$ też jest blokiem.*

(ii) *Jeśli $\mathcal{B}$ jest blokiem, to $\mathcal{B}^{g_i}$ także jest blokiem, dla każdego $g_i \in G$.*

(ii) *Jeśli $\mathcal{B}$ jest blokiem, to zbiory $\mathcal{B}^{g_1}, \mathcal{B}^{g_1}, \ldots, \mathcal{B}^{g_n}$ tworzą podział X.*

Dowód. Dowód (i). Niech $\mathcal{C} = \mathcal{B}_1 \cap \mathcal{B}_2$ i ustalmy $g \in G$. Mamy pokazać, że $\mathcal{C}^g = \mathcal{C}$ lub $\mathcal{C}^g \cap \mathcal{C} = \emptyset$. Przede wszystkim zauważmy, że $(\mathcal{B}_1 \cap \mathcal{B}_2)^g = \mathcal{B}_1^g \cap \mathcal{B}_2^g$, ponieważ g jest bijekcją. Zatem

$$\mathcal{C}^g = \begin{cases} \mathcal{B}_1 \cap \mathcal{B}_2, & \mathcal{B}_1^g = \mathcal{B}_1, \mathcal{B}_2^g = \mathcal{B}_2 \\ \emptyset, & \text{w pozostałych przypadkach.} \end{cases}$$

Dowód (ii). Niech $\mathcal{C} = \mathcal{B}^{g_i}$ i załóżmy, że $\mathcal{C} \cap \mathcal{C}^g \neq \emptyset$, tzn. $g_i(\mathcal{B}) \cap g(g_i(\mathcal{B})) \neq \emptyset$. Wówczas biorąc przeciwobraz części wspólnej mamy

$$\mathcal{B} \cap g_i^{-1}(g(g_i(\mathcal{B}))) \neq \emptyset \quad \Leftrightarrow \quad \mathcal{B} \cap \mathcal{B}^{g_i g g_i^{-1}} \neq \emptyset.$$

Ponieważ $\mathcal{B}$ jest blokiem, więc $\mathcal{B}^{g_i g g_i^{-1}} = \mathcal{B}$. Stąd $\mathcal{B}^{g_i} = \mathcal{B}^{g_i g}$ i w rezultacie $\mathcal{C} = \mathcal{C}^g$. Oznacza to, że $\mathcal{C}$ jest blokiem.

Dowód (iii). Z punktu (ii) wiadomo, że $\mathcal{B}^{g_i}$ i $\mathcal{B}^{g_j}$ są albo równe albo rozłączne. Wystarczy pokazać, że $\bigcup_{i=1}^n \mathcal{B}^{g_i} = X$. Niech $x_1 \in \mathcal{B}$ i $x_2 \notin \mathcal{B}$.

Wtedy istnieje g_1 takie, że $g_1(x_1) = x_2$ i jeśli $\mathcal{B} \neq \mathcal{B}^{g_1}$, to $\mathcal{B} \cap \mathcal{B}^{g_1} = \emptyset$ ponieważ $\mathcal{B}$ jest blokiem. Mamy teraz dwie możliwości.

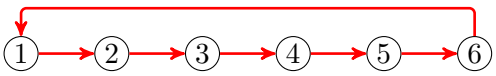
Jeśli $X = \mathcal{B} \cup \mathcal{B}^{g_1}$, to dowód jest zakończony. Jeśli $X \neq \mathcal{B} \cup \mathcal{B}^{g_1}$, to wybieramy $x_3 \notin \mathcal{B} \cup \mathcal{B}^{g_1}$. Istnieje wtedy g_2 takie, że $x_3 = g_2(x_2)$.

Wynika stąd, że $\mathcal{B}^{g_2} \neq \mathcal{B}$, $\mathcal{B}^{g_2} \neq \mathcal{B}^{g_1}$ oraz $\mathcal{B}^{g_2} \cap (\mathcal{B} \cup \mathcal{B}^{g_1}) = \emptyset$. Wtedy znowu albo X jest równy sumie bloków $\mathcal{B}$, $\mathcal{B}^{g_1}$, $\mathcal{B}^{g_2}$ albo nie jest. Ponieważ X jest skończony, to powtarzając powyższą procedurę, po skończonej liczbie kroków wyczerpiemy cały X. □

Przykład 5.4 Rozważmy bardziej złożoną sytuację niż tą przedstawioną na rysunku 5.5. Niech $X = \{1, 2, 3, 4, 5, 6\}$ i tym razem

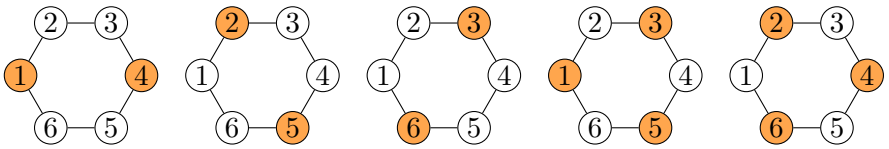
$$G = \langle \alpha \rangle, \quad \alpha = (1, 2, 3, 4, 5, 6). \tag{5.13}$$

Zatem $G \cong \mathbb{Z}_6$. Działanie G na X jest tranzytywne, istnieje tylko jedna orbita, patrz rysunek 5.6. Nie jest jednak 2-tranzytywne, np. zbiór $\{1, 2\}$ nigdy nie przejdzie na $\{1, 3\}$ bo grupa ta przesuwa wszystkie elementy zawsze o tą samą ilość miejsc. Istnieje pięć nietrywialnych bloków i są to: $\mathcal{B}_1 = \{1, 4\}$,



Rys. 5.6 Działanie G jest przechodnie, ale nie jest 2-przechodnie.

$\mathcal{B}_2 = \{2, 5\}$, $\mathcal{B}_3 = \{3, 6\}$, $\mathcal{B}_4 = \{1, 3, 5\}$ i $\mathcal{B}_5 = \{2, 4, 6\}$. Mamy bowiem $\mathcal{B}_1^G = \{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}$ i $\mathcal{B}_4^G = \{\mathcal{B}_4, \mathcal{B}_5\}$. Zbiór $\{1, 2\}$ nie jest blokiem, ponieważ $\{1, 2\}^\alpha = \{2, 3\}$. Podobnie blokiem nie jest $\{1, 2, 3\}$. Bloki minimalne to $\mathcal{B}_1$, $\mathcal{B}_2$ i $\mathcal{B}_3$. Wszystkie nietrywialne bloki zostały pokazane na rysunku 5.7. □



Rys. 5.7 Pięć nietrywialnych bloków grupy (5.13)

Niech G będzie grupą działającą tranzytywnie na X. Mówimy, że G jest **prymitywna**, jeśli nie ma nietrywialnych bloków na zbiorze X. Pokażemy, że jeśli działanie grupy jest 2-przechodnie, to jest ona prymitywna, czyli nie zawiera nietrywialnego bloku.

Załóżmy przeciwnie, że $\mathcal{B}$ jest takim blokiem. Oznacza to, że istnieją $x_1, x_2 \in \mathcal{B}$, $x_3 \notin \mathcal{B}$ oraz permutacja g taka, że $g(x_1) = x_1$ i $g(x_2) = x_3$.

W takim razie $x_1 \in \mathcal{B}$, $x_1 \in g(\mathcal{B}) = \mathcal{B}^g$ i stąd $\mathcal{B} \cap \mathcal{B}^g \neq \emptyset$, gdzie $\mathcal{B} \neq \mathcal{B}^g$. Otrzymaliśmy sprzeczność z tym, że $\mathcal{B}$ jest blokiem.

Twierdzenie 5.6 *Niech X będzie zbiorem skończonym i G będzie podgrupą prymitywną grupy $Sym(X)$. Wówczas*

(i) *Jeśli G zawiera 3-cykl, to $Alt(X) \subset G$.*

(ii) *Jeśli G zawiera 2-cykl, to $G = Sym(X)$.*

Dowód. Dowód (i). Dla $\mathcal{S} \subset X$ niech $Alt(\mathcal{S})$ oznacza podgrupę $Alt(X)$, której każda permutacja zostawia na swoich miejscach elementy $X \backslash \mathcal{S}$. Załóżmy, że $\mathcal{S}$ jest maksymalnym podzbiorem X takim, że $Alt(\mathcal{S}) \subset G$. Ponieważ grupa G zawiera 3-cykl, to $|\mathcal{S}| \geq 3$. Udowodnimy, że w istocie $\mathcal{S} = X$.

Załóżmy przeciwnie, że $\mathcal{S} \neq X$. Ponieważ G jest prymitywna, to zbiór ten nie jest blokiem i stąd istnieje $g \in G$, dla którego $\mathcal{S} \cap \mathcal{S}^g \neq \emptyset$ lub $\mathcal{S} \cap \mathcal{S}^g \neq \mathcal{S}$.

Załóżmy najpierw, że $\mathcal{S} \cap \mathcal{S}^g = \{x\}$. Ponieważ $Alt(\mathcal{S})$ jest podgrupą G oraz $g^{-1}Alt(\mathcal{S})g = Alt(\mathcal{S}^g)$, to G zawiera 3-cykle $g_1 = (x, y_1, z_1)$, $g_2 = (x, y_2, z_2)$, gdzie $y_1, z_1 \in \mathcal{S}$ i $y_2, z_2 \in \mathcal{S}^g$. Wówczas G zawiera poniższy komutator

$$g_3 = [g_2^{-1}, g_1^{-1}] = g_2^{-1} g_1^{-1} g_2 g_1 = (x, y_1, y_2),$$

gdzie $x, y_1 \in \mathcal{S}$. Gdyby $\mathcal{S} \cap \mathcal{S}^\alpha$ zawierał co najmniej dwa punkty, np. x_1, x_2, to trzeba wziąć dowolny $w \in \mathcal{S}^g \backslash \mathcal{S}$. Ponieważ $x_1, x_2, w \in \mathcal{S}^g$, to G zawiera 3-cykl (x_1, x_2, w). Niech zatem $g_3 = (x, y_1, y_2)$. Zdefiniujmy $\mathcal{S}' = S \cup \{y_2\}$. Pokażemy, że $Alt(\mathcal{S}') \subset G$.

W tym celu wystarczy pokazać, że jeśli $g \in Alt(\mathcal{S}')$ i $g(y_2) \neq y_2$, to $g \in G$. Ponieważ $x_3 = g(y_2) \in \mathcal{S}$, to istnieje permutacja $h \in Alt(\mathcal{S})$ taka, że $h(x_3) = y_1$ i wtedy $gh \cdot (x, y_1, y_2) \in Alt(\mathcal{S}')$ z punktem stałym y_2.

Stąd $gh \cdot (x, y_1, y_2)$ i $h \cdot (x, y_1, y_2)$ należą do G, a więc także $g \in G$. Zatem $Alt(\mathcal{S}')$ jest podgrupą G wbrew założeniu o maksymalności zbioru $\mathcal{S}$. Wnioskujemy, że $\mathcal{S} = X$.

Dowód (ii). Niech $|X| \geq 3$ i załóżmy, że G zawiera transpozycję (x_1, x_2). Wówczas $\mathcal{B} = \{x_1, x_2\}$ nie jest blokiem (zakładamy, że G jest prymitywna), zatem istnieje permutacja $g \in G$ taka, że zbiór $\mathcal{B} \cap \mathcal{B}^g$ ma jeden element. Można przyjąć, że $\mathcal{B}^g = \{x_1, x_3\}$, gdzie $x_3 \neq x_2$. Następnie zauważmy, że 3-cykl (x_1, x_2, x_3) należy do G, ponieważ

$$(x_1, x_2, x_3) = (x_1, x_2) \cdot (x_1, x_3) = (x_1, x_2) \cdot g^{-1} \cdot (x_1, x_2) \cdot g.$$

Z punktu (i) wynika, że $Alt(X)$ jest podgrupą G. W związku z tym podgrupa generowana przez transpozycję (x_1, x_2) i podgrupę permutacji parzystych

jest też podgrupą G. Ale $\langle (x_1, x_2), Alt(X)\rangle = Sym(X)$, ponieważ (x_1, x_2) jest permutacją nieparzystą. □

Zanim przejdziemy do twierdzenia Cauchy'ego udowodnimy pewien pomocniczy fakt. Ustalmy liczbę naturalną p większą od jednego i niech

$$\mathbf{x} = (x_1, \ldots, x_p) \in \mathbb{R}^p.$$

Załóżmy, że $r \in \mathbb{N}$. Cykliczne przesunięcie elementów $\mathbf{x}$ o r miejsc w prawo oznaczmy przez $\mathbf{x}^r$. Zatem

$$\mathbf{x}^r = (x_{p-r+1}, \ldots, x_p, x_1, \ldots, x_{p-r}).$$

Niech $\mathbf{x}^0 = \mathbf{x}$. Łatwo widać, że jeśli $r \geq p$, to $\mathbf{x}^r = \mathbf{x}^{r \bmod p}$. Oznaczmy

$$[\mathbf{x}] := \{\mathbf{x}, \mathbf{x}^1, \mathbf{x}^2, \ldots, \mathbf{x}^{p-1}\}.$$

Udowodnimy, że jeśli p jest liczbą pierwszą, to

$$|[\mathbf{x}]| = \begin{cases} 1, & \text{gdy } x_1 = x_2 = \ldots = x_p \\ p, & \text{w pozostałych przypadkach.} \end{cases} \tag{5.14}$$

Jeśli p nie jest liczbą pierwszą, to nie jest to ogólnie prawdą. Na przykład, dla $p = 4$ i ciagu $\mathbf{x} = (1, 2, 1, 2)$ mamy $\mathbf{x}^1 = (2, 1, 2, 1)$ oraz $\mathbf{x}^2 = \mathbf{x}$, $\mathbf{x}^3 = \mathbf{x}^1$. Zatem w tym przypadku $|[\mathbf{x}]| = 2 \neq 4$.

Przechodzimy do dowodu (5.14). Załóżmy więc, że $\mathbf{x} = \mathbf{x}^r$ dla pewnego $r \in \{1, \ldots, p-1\}$. Porównując wartości na kolejnych współrzędnych otrzymujemy

$$x_i = x_{k+i \bmod p}, \quad \text{gdzie} \quad k = p - r,$$

dla $i = 1, 2, \ldots, p$. Ponieważ $k \in \{1, 2, \ldots, p-1\}$, więc mamy ciąg równości

$$x_1 = x_{k+1 \bmod p} = x_{2k+1 \bmod p} = \ldots = x_{(p-1)k+i \bmod p}.$$

Jeśli p jest liczbą pierwszą, to wszystkie indeksy są różne. Jeśli bowiem dla pewnych l_1, l_2 zachodzi równość

$$(l_1 k + 1) \bmod p = (l_2 k + 1) \bmod p,$$

to $(l_2 - l_1)k \equiv 0 \bmod p$. W takim razie p dzieli iloczyn $(l_2 - l_1)k$, ale nie jest to możliwe, ponieważ p jest liczbą pierwszą oraz $l_2 - l_1 \leq p - 1$, $k \leq p - 1$. W związku z tym $x_1 = \ldots = x_p$.

Udowodnimy teraz twierdzenia Cauchy'ego, które pochodzi z 1845 roku. W 1959 roku McKay, patrz [10], podał elegancki dowód tego twierdzenia, liczący około 20 liniek, który tutaj zaprezentujemy.

Twierdzenie 5.7 *Jeśli G jest grupą skończoną i liczba pierwsza p dzieli $|G|$, to istnieje w niej nietrywialne rozwiązanie równania $a^p = e$.*

Dowód. Załóżmy, że $|G| = n$ i rozważmy podzbiór G^k określony jako

$$S = \{\mathbf{a} = (a_1, a_2, \ldots, a_p) : a_1 a_2 \ldots a_p = e\},$$

gdzie $a_1, \ldots, a_p \in G$. Widać, że $|S| = n^{p-1}$, ponieważ $a_1, \ldots, a_{p-1}$ mogą być dowolne i wtedy $a_p = (a_1 \ldots a_{p-1})^{-1}$. Następnie $\mathbf{a}$ i $\mathbf{a}'$ nazywamy równoważnymi, jeśli elementy $\mathbf{a}'$ powstały przez cykliczne przestawienie elementów $\mathbf{a}$. Z twierdzenia 2.9 wynika, że jest to relacja równoważnosci na S.

Z (5.14) wiadomo, że $|[\mathbf{a}]| = 1$, jeśli wszystki elementy $\mathbf{a}$ są równe lub $|[\mathbf{a}]| = p$, jeśli przynajmniej dwa są różne. Oznaczmy przez r liczbę tych ciągów z S, w których wszystkie elementy są równe. Wtedy r jest liczbą rozwiązań równania $a^p = e$. Niech s będzie liczbą różnych pozostałych klas równoważności. Wówczas $r + sp = n^{p-1}$. Jeśli p dzieli n, to dzieli też r. □

6. Algorytm Schreiera-Simsa

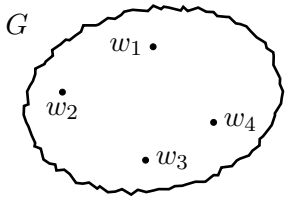
6.1 Twierdzenie Schreiera

Niech G będzie grupą skończoną działającą na X określoną w taki sposób, że podany jest zbiór jej generatorów, tzn.

$$G = \langle W \rangle, \quad \text{gdzie} \quad W = \{w_1, w_2, \ldots, w_k\}. \tag{6.1}$$

Innymi słowy, każdy element $g \in G$ można zapisać w postaci $w_{i_1} w_{i_2} \ldots w_{i_m}$, dla pewnych $w_{i_1}, \ldots, w_{i_m} \in W$. Przedstawienie takie nie musi być i zwykle nie jest jednoznaczne. Naturalnie nasuwające się pytanie jest takie: jaki jest rząd tej grupy? I ogólnie, jakie elementy z $Sym(X)$ należą do G, a jakie nie.

Jeśli $W = \{w_1\}$, to $G = \{w_1^m : m \in \mathbb{Z}\}$ jest w tym przypadku grupą cykliczną, izomorficzną z $\mathbb{Z}_n$, gdzie $n = |G|$. Poza tym, w „najlepszym"



Rys. 6.1 Zbiór generatorów grupy G.

wypadku dostaniemy oczywiście $G = Sym(X)$, a w „najgorszym" $G = \{I\}$, gdzie I jest jedynką w grupie $Sym(X)$.

Niech H będzie podgrupą grupy G. Może to być np. stabilizator pewnego $x \in X$. Dowolny element z H można oczywiście wyrazić przez iloczyn elementów z W. Takie przedstawienie jest jednak zbyt ogólne i może być mało przydatne do badania podgrupy H. Nie wszystkie elementy W muszą należeć do H, a często jest tak, że $W \cap H = \emptyset$. Powstaje więc kolejne pytanie: czy istnieje dokładniejszy sposób opisu H?

Problemy, które chcemy rozwiązać w tym rozdziale są następujące

(a) Znaleźć rząd grupy danej przez (6.1).

(b) Mając $g \in Sym(X)$ odpowiedzieć na pytanie czy $g \in G$?

(c) Mając podgrupę H znaleźć jej dokładniejszy opis w ramach zbioru W.

Zaczniemy od pewnej ogólnej definicji. Niech $\mathcal{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ będzie rodziną podzbiorów skończonego zbioru X. **Transwersalą** rodziny $\mathcal{A}$ nazywamy zbiór $T = \{t_1, \ldots, t_n\}$ składający się z różnych elementów X takich, że $t_i \in \mathcal{A}_i$, dla $i = 1, \ldots, n$. Innymi słowy, jest to „zbiór reprezentantów" tej rodziny, z którym spotkaliśmy się już wcześniej.

Jeśli zbiory $\mathcal{A}_1, \ldots, \mathcal{A}_n$ są parami rozłączne, czyli $\mathcal{A}_i \cap \mathcal{A}_j = \emptyset$, gdy $i \neq j$, to transwersala tej rodziny zawsze istnieje. Wystarczy wybrać po jednym, dowolnym elemencie z każdego zbioru.

W pozostałych przypadkach transwersala może nie istnieć. Na przykład dla zbiorów $A_1 = \{1, 2\}$, $A_2 = \{3\}$, $A_3 = \{1, 3\}$, $A_4 = \{2, 3\}$ nie istnieje. Warunki, które powinna spełniać rodzina $\mathcal{A}$, aby miała transwersalę są następujące (patrz np. twierdzenie 26.1 w [17]): *Rodzina $\mathcal{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ niepustych podzbiorów X ma transwersalę wtedy i tylko wtedy, gdy dla każdego $k = 1, 2, \ldots, n$, suma jej dowolnych k podzbiorów składa się z co najmniej k elementów.*.

Rozważmy rodzinę warstw prawostronnych G względem podgrupy H. Ponieważ warstwy są rozłączne, to istnieje transwersala T tej rodziny. Jeśli więc $T = \{t_1, \ldots, t_k\}$, to $G = \bigcup_{i=1}^{k} Ht_i$, gdzie Ht_i są tymi warstwami. Następnie zdefiniujmy

$$\overline{g} := Hg \cap T, \quad g \in G. \tag{6.2}$$

Odwzorowanie to elementowi g przyporządkowuje „reprezentanta" warstwy, do której należy. Oto twierdzenie, które rozwiązuje problem (c) i prowadzi do rozwiązania (a) i (b). Jest to twierdzenie Schreiera, patrz np. [2].

Twierdzenie 6.1 *Niech G będzie grupą skończoną i H jej podgrupą. Załóżmy, że T jest transwersalą warstw prawostronnych H w G oraz, że $1 \in T$. Jeśli W jest zbiorem generatorów grupy G, to*

$$V := \{tw(\overline{tw})^{-1} : w \in W, t \in T\} \tag{6.3}$$

jest zbiorem generatorów podgrupy H.

Dowód. Z definicji (6.2) mamy $Htw = H(\overline{tw})$, dla ustalonych t, w. Wynika stąd, że $Htw(\overline{tw})^{-1} = H$, czyli, że warstwa elementu $tw(\overline{tw})^{-1}$ jest równa podgrupie H. Zatem

$$tw(\overline{tw})^{-1} \in H, \quad \forall\, w \in W, t \in T. \tag{6.4}$$

Oznacza to, że $V \subset H$. Pokażemy teraz, że każdy element $h \in H$ można zapisać jako iloczyn elementów z V. Robimy to w następujący sposób. Ponieważ

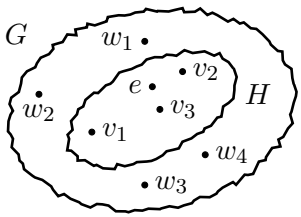
$G = \langle W \rangle$, więc w szczególności $h = \prod_{i=1}^{m} w_i$, dla pewnych $w_1, \ldots, w_m \in W$. Niech $t_0 = 1$ (z założenia $1 \in T$, gdzie 1 to element neutralny grupy oznaczany wcześniej przez e lub I). Wówczas

$$h = t_0 w_1 w_2 \ldots w_m = (t_0 w_1 t_1^{-1})(t_1 w_2 t_2^{-1}) \ldots (t_{m-1} w_m t_m^{-1}) t_m,$$

gdzie $t_i := \overline{t_{i-1} w_i} \in T$, dla $i = 1, \ldots, m$. Z (6.4) mamy $t_{i-1} w_i t_i^{-1} \in H$, zatem $\prod_{i=1}^{m} t_{i-1} w_i t_i^{-1} \in H$ i w rezultacie $t_m \in H$. Stąd $t_m \in H \cap T$. Następnie zauważmy, że H i T mogą mieć tylko jeden punkt wspólny. Zatem $t_m = 1$. To kończy dowód twierdzenia. □

Elementy zbioru (6.3) nazywa się **generatorami Schreiera** podgrupy H. Otto Schreier (1901-1929) był matematykiem austricakim. Publikował prace głównie dotyczące teorii grup. Twierdzenie to pochodzi z jego pracy z 1927 roku, w której uogólnił rezultat J.Nielsena z 1921 roku mówiący, że podgrupa skończenie generowanej grupy wolnej jest wolna. To ogólne twierdzenie nazywane jest w literaturze twierdzeniem Nielsena-Schreiera.

Twierdzenie 6.1 daje nam procedurę znajdowania generatorów podgrupy, jeśli znamy jej transwersalę warstw prawostronnych. Zauważmy, że zbiór tych



Rys. 6.2 Ilustracja twierdzenia 6.1.

generatorów składa się z $|W| \cdot |T|$ elementów i najczęściej nie jest minimalnym zbiorem generatorów podgrupy H. Zwykle daje się go mocno zredukować. Z twierdzenia Lagrange'a mamy równość $|G| = |T| \cdot |H|$ i twierdzenie 6.1 można następnie zastosować do H i jej pewnej podgrupy.

6.2 Algorytm Schreiera-Simsa

Niech $x_1 \in X$ będzie elementem nośnika pewnego $g \in W$, czyli $g(x_1) \neq x_1$. Po skończenie wielu krokach znajdziemy jego orbitę $\mathcal{O}_1 = x_1^G$. Jednocześnie z orbitą znajdujemy transwersalę T_1 warstw prawostronnych G względem stabilizatora G_{x_1} i odwzorowanie $\overline{g}$ występujące w twierdzeniu 6.1, gdzie $H = G_{x_1}$. Z twierdzenia 5.3 wynika, że $|T_1| = |\mathcal{O}_1|$. W ten sposób otrzymamy

zbiór V_1, którego elementami są generatory G_{x_1}. Następnie maksymalnie redukujemy V_1. Niech ten zredukowany zbiór będzie dalej oznaczony przez V_1 i zdefiniujmy $W_1 := V_1$, $G(1) := G_{x_1}$. Z twierdzenie Lagrange'a mamy $|G| = |\mathcal{O}_1| \cdot |G(1)|$.

Wychodzimy teraz od W_1 i $G(1)$ i znajdujemy $x_2 \in X$, który należy do nośnika pewnego elementu z W_1. Znajdujemy jego orbitę $\mathcal{O}_2 = x_2^{G(1)}$, transwersalę warstw prawostronnych T_2 grupy $G(1)$ względem stabilizatora $G(1)_{x_2}$ i odwzorowanie $\overline{g}$. Otrzymamy zbiór V_2 generujący $G(2) := G(1)_{x_2}$. Zauważmy, że $G(1)_{x_2} = G_{x_1,x_2}$ oraz $|T_2| = |\mathcal{O}_2|$. Z twierdzenia Lagrange'a $|G(1)| = |\mathcal{O}_2| \cdot |G(2)|$ i stąd $|G| = |\mathcal{O}_1| \cdot |\mathcal{O}_2| \cdot |G(2)|$.

Dalej postępujemy rekurencyjnie. Wychodzimy od $W_2 := V_2$ i $G(2)$. Znajdujemy x_3 należący do nośnika pewnego elementu z W_2.

Po skończonej liczbie kroków $d \geq 1$ otrzymamy $W_d = \{I\}$ i $G(d) = \{I\}$. W wyniku powyższej procedury dostaniemy

(i) zbiór $\mathcal{B} = \{x_1, x_2, \ldots, x_d\}$, który jest bazą X, tzn. $G_{(\mathcal{B})} = \{I\}$,

(ii) rodzinę $W_1, W_2, \ldots, W_d$, w której W_i jest zbiorem generatorów $G(i)$, gdzie
$$G(i) := G(i-1)_{x_i} = G_{x_1,\ldots,x_i}, \quad i = 1, \ldots, d,$$

(iii) orbity $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_d$, gdzie $\mathcal{O}_i = x_i^{G(i-1)}$ i stąd
$$|G| = \prod_{i=1}^{d} |\mathcal{O}_i| = |\mathcal{O}_1| \cdot |\mathcal{O}_2| \cdot \ldots \cdot |\mathcal{O}_d|. \tag{6.5}$$

(iv) rodzinę transwersal $T_1, T_2, \ldots, T_d$, gdzie T_i jest zbiorem reprezentantów warstw prawostronnych $G(i)$ względem $G(i-1)$ oraz
$$|T_i| = |\mathcal{O}_i|, \quad i = 1, 2, \ldots, d. \tag{6.6}$$

Ponieważ $|\mathcal{O}_i| \leq n$, dla każdego $i = 1, \ldots, d$, to z (6.5) wnioskujemy, że $|G| \leq n^{|\mathcal{B}|}$. Mamy więc oszacowanie $|\mathcal{B}| \geq (\log |G|)/(\log n)$.

Twierdzenie 6.2 *Każdy element $g \in G$ można przedstawić jednoznacznie w postaci*
$$g = t_d t_{d-1} \ldots t_1, \quad \textit{gdzie } t_i \in T_i. \tag{6.7}$$

Dowód. Znajdujemy $t_1 \in T_1$, dla którego $g(x_1) = t_1(x_1)$. Taki element istnieje, ponieważ g należy do pewnej warstwy prawostronnej wyznaczonej

przez podgrupę G_{x_1}, a dokładniej $t_1 = G_{x_1} g \cap T_1$. Następnie obliczamy $g_1 := g t_1^{-1}$ i zauważmy, że $(g t_1^{-1})(x_1) = t_1^{-1}(g(x_1)) = x_1$, zatem $g_1 \in G_{x_1}$.

Następnie znajdujemy $t_2 \in T_2$ spełniające $g_1(x_2) = t_2(x_2)$, obliczamy $g_2 := g_1 t_2^{-1} = g t_1^{-1} t_2^{-1}$ i podobnie jak wcześniej widać, że $g_2 \in G_{x_1,x_2}$. W ten sposób, po d krokach, dojdziemy do $t_d \in T_d$ spełniającgo $g_{d-1}(x_d) = t_d(x_d)$. Wówczas $g_d := g t_1^{-1} \dots t_d^{-1}$. Ponieważ $G_{x_1,\dots,x_d} = \{I\}$, więc $g_d = I$ i stąd otrzymujemy (6.7). □

6.3 Przykłady

Przykład 6.1 Niech elementy zbioru $X = \{1,2,3,4,5,6\}$ będą rozmieszczone tak jak na rysunku 6.3. Znajdziemy rząd następującej grupy

$$G = \langle \alpha, \beta \rangle, \quad \alpha = (1,2,3,4),\ \beta = (1,5,6,2). \tag{6.8}$$

Sam sposób rozmieszczenia punktów X nie jest istotny, ale pozwala lepiej zobrazować działanie G. Poza tym istnieje rzeczywisty model takiej sytuacji jak np. obracanie warstwy prawej i górnej w kostce Rubika lub jej pokrewnych „układankach", patrz np. [8].

Zobaczmy na początek jak działa komutator: $[\alpha, \beta] = (1,4)(2,6)$. Podwójna transpozycja to trochę słabiej niż 3-cykl, patrz twierdzenie 5.6, ale dzięki temu badanie tej grupy jest ciekawsze.

Rys. 6.3 Generatory grupy (6.8)

Zaczniemy od wyznaczenia orbity $x_1 = 1$, ponieważ np. $x_1 \in Act(\alpha)$. Wyznaczamy kolejno orbitę (w nawiasach podane są permutacje): $1 \to 1(I)$, $1 \to 2(\alpha)$, $1 \to 3(\alpha^2)$, $1 \to 4(\alpha^3)$ oraz $1 \to 5(\beta)$, $1 \to 6(\beta^2)$. Zatem

$$\mathcal{O}_1 = 1^G = \{1,2,3,4,5,6\}, \quad T_1 = \{I, \alpha, \alpha^2, \alpha^3, \beta, \beta^2\}.$$

Następnie korzystamy z twierdzenia 6.1, gdzie $H = G_1$, V oznaczamy przez V_1 i $W = \{\alpha, \beta\}$. Zbiór generatorów Schreiera G_1 składa się z 12 permutacji

$$V_1 = \Big\{ \alpha(\overline{\alpha})^{-1}, \beta(\overline{\beta})^{-1}, \alpha^2(\overline{\alpha^2})^{-1}, \alpha\beta(\overline{\alpha\beta})^{-1}, \alpha^3(\overline{\alpha^3})^{-1}, \alpha^2\beta(\overline{\alpha^2\beta})^{-1}, \\ I(\overline{I})^{-1}, \alpha^3\beta(\overline{\alpha^3\beta})^{-1}, \beta\alpha(\overline{\beta\alpha})^{-1}, \beta^2(\overline{\beta^2})^{-1}, \beta^2\alpha(\overline{\beta^2\alpha})^{-1}, \beta^3(\overline{\beta^3})^{-1} \Big\}.$$

Teraz znajdujemy reprezentantów: $\overline{\alpha} = \alpha$, $\overline{\beta} = \beta$, $\overline{\alpha^2} = \alpha^2$, $\overline{\alpha\beta} = I$ (dlatego, że $1 \to 1(\alpha\beta)$), $\overline{\alpha^3} = \alpha^3$, $\overline{\alpha^2\beta} = \alpha^2$ ($\alpha^2\beta(1) = 3 = \alpha^2(1)$), $\overline{I} = I$, $\overline{\beta^2} = \beta^2$, $\overline{\beta\alpha} = \beta$ (mamy bowiem $\beta\alpha(1) = \alpha(5) = 5 = \beta(1)$), $\overline{\beta^2\alpha} = \beta^2$ ($\beta^2\alpha(1) = \alpha(6) = 6 = \beta^2(1)$) oraz $\overline{\beta^3} = \beta^3$. Przykładowe obliczenie: $\alpha^2\beta(\overline{\alpha^2\beta})^{-1} = \alpha^2\beta(\alpha^2)^{-1} = \alpha^2\beta\alpha^2$, ponieważ $\alpha^{-2} = \alpha^2$. Redukując identyczność i powtarzające się permutacje otrzymamy

$$V_1 = \left\{\alpha\beta, \alpha^2\beta\alpha^2, \alpha^3\beta\alpha^{-3}, \beta\alpha\beta^{-1}, \beta^2\alpha\beta^2\right\}.$$

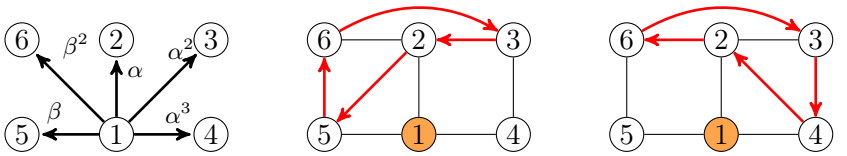
Pozostaje obliczyć iloczyny w nawiasach. Poniżej pomocnicze obliczenia.

$$\begin{array}{lll}
\alpha^2 = (1,3)(2,4) & \alpha^2\beta = (1,3,5,6,2,4) & \beta^2\alpha\beta^2 = (3,4,6,5) \\
\alpha^3 = (1,4,3,2) & \alpha^2\beta\alpha^2 = (3,5,6,4) & \alpha^3\beta = (1,4,3)(2,5,6) \\
\beta^2 = (1,6)(2,5) & \beta\alpha = (1,5,6,3,4) & \alpha^3\beta\alpha^{-3} = (2,5,6,3) \\
\beta^3 = (1,2,6,5) & \beta\alpha\beta^{-1} = (2,6,3,4) & \alpha^{-2} = \alpha^2, \alpha^{-1} = \alpha^3 \\
\alpha\beta = (2,3,4,5,6) & \beta^2\alpha = (1,6,2,5,3,4) & \beta^{-2} = \beta^2, \beta^{-1} = \beta^3
\end{array}$$

Zauważmy, że $(2,6,3,4)^2 \cdot (2,5,6,3) = (3,5,6,4)$, $(3,4,6,5)^3 = (3,5,6,4)$ oraz $(2,6,3,4) \cdot (2,5,6,3) = (2,3,4,5,6)$, więc zbiór generatorów można zredukować do dwóch permutacji. Mianowicie, $V_1 = \{(2,5,6,3), (2,6,3,4)\}$, zatem

$$G_1 = \langle \alpha_1, \beta_1 \rangle, \quad \alpha_1 = (2,5,6,3),\ \beta_1 = (2,6,3,4).$$

Generatory α_1, β_1 wyrażają się przez generatory grupy G: $\alpha_1 = \alpha^{-1}\beta\alpha$, $\beta_1 = \beta\alpha\beta^{-1}$. Na rysunku 6.4 oprócz transwersali (na czarno) zaznaczono ich działanie (na czerwono). Zatem $|G| = 6|G_1|$ i znamy generatory G_1.



Rys. 6.4 Transwersala T_1 i generatory stabilizatora G_1

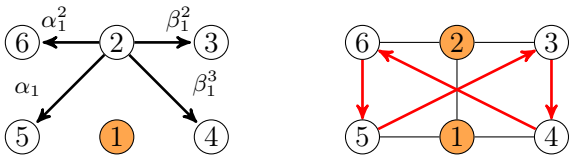
Z G_1 postępujemy tak, jak postępowaliśmy na początku z G. Wybieramy dowolną z liczb znajdujących się w nośnikach α_1, β_1, niech to będzie 2. Znajdujemy jej orbitę: $2 = 2^I$, $3 = 2^{\beta_1^2}$, $4 = 2^{\beta_1^3}$, $5 = 2^{\alpha_1}$, $6 = 2^{\alpha_1^2}$. Zatem $\mathcal{O}_2 = \{2,3,4,5,6\}$, a reprezentacja warstw prawostronnych podgrupy $G_{1,2}$

w G_1 ma postać $T_2 = \{I, \beta_1^2, \beta_1^3, \alpha_1, \alpha_1^2\}$. Przyjmując $W_1 = \{\alpha_1, \beta_1\}$, zbiór generatorów $G_{1,2}$ ma postać

$$V_2 = \Big\{ I, \alpha_1(\overline{\alpha_1})^{-1}, \beta_1(\overline{\beta_1})^{-1}, \alpha_1^2(\overline{\alpha_1^2})^{-1}, \alpha_1\beta_1(\overline{\alpha_1\beta_1})^{-1}, \alpha_1^3(\overline{\alpha_1^3})^{-1},$$
$$\alpha_1^2\beta_1(\overline{\alpha_1^2\beta_1})^{-1}, \beta_1^2\alpha_1(\overline{\beta_1^2\alpha_1})^{-1}, \beta_1^3(\overline{\beta_1^3})^{-1}, \beta_1^3\alpha_1(\overline{\beta_1^3\alpha_1})^{-1}, \beta_1^4(\overline{\beta_1^4})^{-1} \Big\}.$$

Obliczamy reprezentantów: $\overline{\alpha_1} = \alpha_1$, $\overline{\alpha_1^2} = \alpha_1^2$, $\overline{\alpha_1^3} = \beta_1^2$, ponieważ $2^{\alpha_1^3} = 3 = 2^{\beta_1^2}$, $\overline{\beta_1} = \alpha_1^2$, $\overline{\alpha_1\beta_1} = \alpha_1$, mamy bowiem $2^{\alpha_1\beta_1} = 5 = 2^{\alpha_1}$, $\overline{\alpha_1^2\beta_1} = \beta_1^2$, ponieważ $2^{\alpha_1^2\beta_1} = 3 = 2^{\beta_1^2}$, $\overline{\beta_1^3} = \beta_1^3$, $\overline{\beta_1^3\alpha_1} = \beta_1^3$, mamy $2^{\beta_1^3\alpha_1} = 4 = 2^{\beta_1^3}$ i w końcu $\overline{\beta_1^4} = \overline{I} = I$. Po wstępnej redukcji dostaniemy pięć permutacji: $\alpha_1\beta_1\alpha_1^{-1}$, $\alpha_1^3\beta_1^{-2}$, $\alpha_1^2\beta_1^{-1}$, $\beta_1^2\alpha_1$, $\beta_1^3\alpha_1\beta_1^{-3}$.

Następnie zauważmy, że $\alpha_1\beta_1\alpha_1^{-1}$, $\alpha_1^2\beta_1^{-1}$ i $\beta_1^2\alpha_1$ równe są $(3,5,6,4)$. Dwie ostatnie permutacje $\alpha_1^3\beta_1^{-2}$, $\beta_1^3\alpha_1\beta_1^{-3}$ to $(3,4,6,5)$. Wyjściowy zbiór zredukowany został do jednej permutacji: $V_2 = \{\alpha_2\}$, gdzie $\alpha_2 = (3,4,6,5)$. Generator ten, zapisany przy użyciu α i β ma postać $[\alpha^{-1}, \beta^{-1}]\alpha^2\beta^{-1}$.



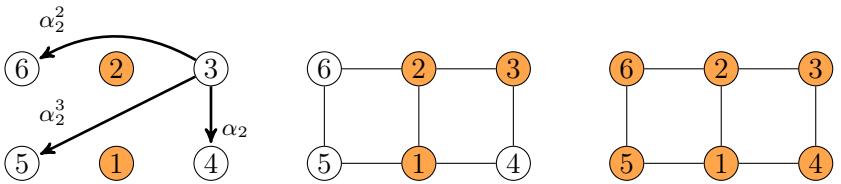
Rys. 6.5 Transwersala T_2 i generator stabilizatora $G_{1,2}$

Obliczenia pokazują ponadto, że $\alpha_2 = \beta^2\alpha\beta^2$. Podsumowując, stabilizator $G_{1,2}$ jest generowany przez permutacją cykliczną α_2 i składa się z czterech elementów, patrz rysunek 6.5.

Niech teraz $x_3 = 3$ i przyjmijmy $W_2 = \{\alpha_2\}$. Wtedy $\mathcal{O}_3 = \{3,4,5,6\}$, $T_3 = \{I, \alpha_2, \alpha_2^2, \alpha_2^3\}$ zatem zbiór generatorów $G_{1,2,3}$ składa się z czterech permutacji: I, $\alpha_2(\overline{\alpha_2})^{-1}$, $\alpha_2^2(\overline{\alpha_2^2})^{-1}$, $\alpha_2^3(\overline{\alpha_2^3})^{-1}$. W tym przypadku reprezentacje są tożsame z wyjściowymi permutacjami, zatem $V_3 = \{I\}$ i stąd $G_{1,2,3} = \{I\}$. Innymi słowy, stabilizator x_3 w grupie $G_{1,2}$ to permutacja identycznościowa.

Problem znalezienia rzędu G jest rozwiązany. Mamy bowiem $|G_{1,2,3}| = 1$, $|G_{1,2}| = 4|G_{1,2,3}| = 4$, $|G_1| = 5|G_{1,2}| = 20$ i stąd $|G| = 6|G_1| = 120$. Zatem $G \neq S_6$, czyli za pomocą α, β i ich kombinacji nie można uzyskać wszystkich permutacji zbioru sześcioelementowego. Podsumowanie tych informacji, tzn. generatory i orbity znajdują się w tabeli 6.1.

W tabeli 6.2 zamieszczone zostały transwersale T_1, T_2, T_3. Z twierdzenia 6.2 wynika, że każdą permutację należąca do $\langle\alpha, \beta\rangle$ można zapisać w sposób jednoznaczny w postaci $t_3t_2t_1$, gdzie $t_3 \in T_3$, $t_2 \in T_2$ i $t_1 \in T_1$. Informacje



Rys. 6.6 Transwersala T_3 i stabilizator $G_{1,2,3} = \{I\}$

Tabela 6.1 Podsumowanie algorytmu Schreiera-Simsa dla grupy (6.8).

Grupa	Generatory	x	Orbita	Rząd
G	$\alpha = (1,2,3,4)$ $\beta = (1,5,6,2)$	1	$\{1,2,3,4,5,6\}$	$\lvert G\rvert = 6\lvert G_1\rvert$
G_1	$\alpha_1 = (2,5,6,3)$ $\beta_1 = (2,6,3,4)$	2	$\{2,3,4,5,6\}$	$\lvert G_1\rvert = 5\lvert G_{1,2}\rvert$
$G_{1,2}$	$\alpha_2 = (3,4,6,5)$	3	$\{3,4,5,6\}$	$\lvert G_{1,2}\rvert = 4$
$G_{1,2,3}$	$\alpha_3 = I$	–	–	$\lvert G_{1,2,3}\rvert = 1$

z tej tabeli można następnie wykorzystać do stwierdzenia, czy dana permutacja należy do G. Niech $\gamma = (1,3,4)$. Czy prawdą jest, że $\gamma \in G$? Aby odpowiedzieć na to pytanie, wybierzmy dowolny element z $Act(\gamma)$, np. 1. Ponieważ $\gamma(1) = 3$, więc w T_1 znajdujemy permutację, która przeprowadza 1 na 3. Jest to $\alpha^2 = (1,3)(2,4)$. Wówczas w permutacji $\gamma\alpha^{-2}$ jedynka będzie punktem stałym: $\gamma\alpha^{-2} = (2,4,3)$. Następnie w T_2 znajdujemy element, który przesuwa 2 na 4. Jest to $\beta_1^3 = (2,4,3,6)$ i $\gamma\alpha^{-2}\beta_1^{-3} = (3,6)$. Na koniec wybieramy z T_3 tą permutację, która przesuwa 3 na 6. Okazuje się, że jest to $\alpha_2^2 = (3,6)(4,5)$ i w związku z tym: $\gamma\alpha^{-2}\beta_1^{-3}\alpha_2^{-2} = (4,5)$. Gdyby γ należała do G, to permutacja $\gamma\alpha^{-2}\beta_1^{-3}\alpha_2^{-2}$ powinna należeć do $G_{1,2,3}$, czyli powinna być równa I. Wynika to z definicji transwersal. Zatem $\gamma \notin G$ i można to zapisać w następujący sposób

$$\gamma \cdot \underbrace{(1,3)(2,4)}_{\in T_1^{-1}} \cdot \underbrace{(2,6,3,4)}_{\in T_2^{-1}} \cdot \underbrace{(3,6)(4,5)}_{\in T_3^{-1}} = (4,5) \neq I.$$

Przeprowadzając podobną procedurę dla $\eta = (1,3,4)(2,6,5)$ otrzymamy

$$\eta \cdot \underbrace{(1,3)(2,4)}_{\in T_1^{-1}} \cdot \underbrace{(2,6)(3,5)}_{\in T_2^{-1}} \cdot \underbrace{(3,6)(4,5)}_{\in T_3^{-1}} = I.$$

Wynika stąd, że $\eta \in G$ oraz $\eta = \alpha_2^2\alpha_1^2\alpha^2$, gdzie $\alpha_2^2 \in T_3$, $\alpha_1^2 \in T_2$ i $\alpha^2 \in T_1$. Uwzględniając to, że α_1 i α_2 wyrażają się przez α i β, tzn. $\alpha_1 = \alpha^{-1}\beta\alpha$, $\alpha_2 = \beta^2\alpha\beta^2$, dostajemy $\eta = \beta^2\alpha^2\beta^2\alpha^3\beta^2\alpha^3$.

Informacje zebrane w tabeli 6.2 można wykorzystać do wygenerowania losowej permutacji z rozważanej grupy. W tym celu należy wybrać losowo t_3, t_2, t_1 z odpowiednio T_3, T_2, T_1 i wymnożyć. Otrzymamy losowo wybraną permutację z tej grupy. Ponieważ wybory są niezależne, to prawdopodobieństwo otrzymania konkretnej permutacji wynosi $\frac{1}{120}$, tzn. $\frac{1}{6} \cdot \frac{1}{5} \cdot \frac{1}{4}$.

Tabela 6.2 Przykładowe transwersale dla grupy danej przez (6.8)

T_1	$=$	T_2	$=$	T_3	$=$
I	I	I	I	I	I
α	$(1,2,3,4)$	β_1^2	$(2,3)(4,6)$	α_2	$(3,4,6,5)$
α^2	$(1,3)(2,4)$	β_1^3	$(2,4,3,6)$	α_2^3	$(3,5,6,4)$
α^3	$(1,4,3,2)$	α_1	$(2,5,6,3)$	α_2^2	$(3,6)(4,5)$
β	$(1,5,6,2)$	α_1^2	$(2,6)(3,5)$		
β^2	$(1,6)(2,5)$				

Pokażemy jeszcze, że

$$\langle\alpha,\beta\rangle = \langle\alpha^2,\beta\rangle = \langle\alpha,\beta^2\rangle. \tag{6.9}$$

Zauważmy, że $\langle\alpha^2,\beta\rangle \subset \langle\alpha,\beta\rangle$. Z równosci $\alpha = \beta^2\alpha^2\beta^{-1}\alpha^2\beta^2$ wynika, że $\alpha \in \langle\alpha^2,\beta\rangle$, stąd $\langle\alpha,\beta\rangle \subset \langle\alpha^2,\beta\rangle$. To dowodzi pierwszej równości w (6.9). Druga równość wynika z faktu, że $\beta = \alpha^2\beta^2\alpha^{-1}\beta^2\alpha^2$. Jeśli chodzi o grupę $\langle\alpha^2,\beta^2\rangle$, to składa się z sześciu permutacji i jest izomorficzna z S_3, tzn.

$$\langle\alpha^2,\beta^2\rangle = \{I, \alpha^2, \beta^2, \alpha^2\beta^2, \beta^2\alpha^2, \alpha^2\beta^2\alpha^2\}.$$

Izomorfizm ten określony jest przez przypisanie α^2 i β^2 odpowiednich generatorów w S_3: $\alpha^2 \to (1,2)$, $\beta^2 \to (2,3)$. □

Przykład 6.2 Każdą permutację α należącą do grupy S_n, $n \geq 2$, można zapisać jednoznacznie w postaci $\alpha_2\alpha_3\ldots\alpha_n$, gdzie $\alpha_i \in L_i$ oraz

$$L_i = \{(1,i),(2,i),\ldots,(i-1,i),I\}, \quad i = 2,3,\ldots,n.$$

Zauważmy, że $|L_i| = i$ oraz $L_i \cap L_j = I$, dla $i \neq j$. Stosujemy algorytm Schreiera-Simsa do S_n generowanej przez wszystkie transpozycje i zbioru

$X = \{1, \ldots, n\}$. Tym razem zaczynamy od $x_1 = n$. Orbitą x_1 jest cały zbiór X, a zbiór reprezentantów T_1 składa się z transpozycji $(n, 1)$, $(n, 2)$, $\ldots$, $(n, n-1)$. Innymi słowy, $T_1 = L_n$. Następnie bierzemy $x_2 = n - 1$. Wówczas $T_2 = L_{n-1}$. Postępując podobnie, dojdziemy do $x_{n-1} = 2$ i wtedy $T_{n-1} = L_2 = \{I, (2, 1)\}$. Stabilizatorem $\{1, \ldots, n-1\}$ jest I, a to oznacza koniec procedury.

Na przykład, permutację $\alpha = (3, 5, 2, 6, 4, 1) \in S_6$ można zapisać w postaci $(2, 1)(3, 2)(4, 1)(5, 2)(6, 4)$. Transwersale dla tego przypadku podane są w tabeli 6.3. Jak już zauważyliśmy, zbiory $L_2, \ldots, L_n$ można wykorzystać do losowego wygenerowania permutacji z S_n. W tym celu losujemy α_i z L_i, dla $i = 2, \ldots, n$ i wszystkie transpozycje wymnażamy. Otrzymamy permutację, której prawdopodobieństwo wybrania p wynosiło $1/n!$ Ponieważ wybory są niezależne, więc rzeczywiście

$$p = \prod_{i=2}^{n} \frac{1}{|L_i|} = \prod_{i=2}^{n} \frac{1}{i} = \frac{1}{n!} = \frac{1}{|S_n|}.$$

Tabela 6.3 Przykładowe transwersale dla grupy S_6.

T_1	T_2	T_3	T_4	T_5
I	I	I	I	I
(6,5)	(5,4)	(4,3)	(3,2)	(2,1)
(6,4)	(5,3)	(4,2)	(3,1)	
(6,3)	(5,2)	(4,1)		
(6,2)	(5,1)			
(6,1)				

W programie **Mathematica** lub bezpośrednio na stronie internetowej **WolframAlpha** dostępnych jest szereg funkcji dotyczących obliczeń związanych z algebrą i grupami. Wracając do przykładu 6.1, generatory można zdefiniować w następujący sposób

a=Cycles[{{1, 2, 3, 4}}]; b=Cycles[{{1,5,6, 2}}];

Następnie, za pomocą poleceń

Grupa=PermutationGroup[a, b]; GroupOrder[Grupa]

„utworzymy" grupę generowaną przez te permutacje i obliczymy jej rząd, równy w tym przypadku 120. Taki też wynik zwróci funkcja **GroupOrder**.

Za pomocą **GroupElements** można uzyskać dostęp do wszystkich elementów grupy, tzn. wyświetli się lista wszystkich permutacji, które można uzyskać za pomocą **a** i **b**. Do obliczania stabilizatorów można wykorzystać np. funkcję **GroupStabilizer**. Łańcuch kolejnych stabilizatorów otrzymamy korzystając z **GroupStabilizerChain**. Zatem wpisując

GroupStabilizerChain[Grupa]

dostaniemy poniższy wynik

```
{{}->PermutationGroup[{Cycles[{{1,5,6,2}}],Cycles[{{1,2,3,4}}],
Cycles[{{2,6,3,4}}],Cycles[{{3,6},{4,5}}],Cycles[{{3,5,6,4}}]}],
{1}->PermutationGroup[{Cycles[{{2,6,3,4}}],Cycles[{{3,6},{4,5}}],
Cycles[{{3,5,6,4}}]}],{1,2}->PermutationGroup[{Cycles[{{3,6},
{4,5}}],Cycles[{{3,5,6,4}}]}],{1,2,3}->PermutationGroup[{}]}
```

czyli listę z informacją o generatorach kolejnych stabilizatorów w odniesieniu do bazy $\{1, 2, 3\}$.

6.4 Zadania

Zadanie 6.1 Niech $X = \{1, 2, 3, 4, 5, 6\}$. Znaleźć rząd następujacej grupy

$$G = \langle \alpha, \beta \rangle, \quad \alpha = (1, 4),\ \beta = (1, 2, 3)(4, 5, 6).$$

Następnie zbadać czy permutacja $(1, 2, 3, 4)$ należy do G. □

Zadanie 6.2 Wykazać, że każdą permutację $\beta \in A_n$, $n \geq 3$, można zapisać jednoznacznie w postaci $\beta_{n-2}\beta_{n-3} \ldots \beta_1$, gdzie $\beta_i \in K_i$ oraz

$$K_i = \{(i, i+1, i+2), (i, i+2, i+3), \ldots, (i, n-1, n), (i, n, i+1), I\},$$

dla $i = 1, \ldots, n-2$. Podobnie jak w przykładzie 6.2 mamy $|K_i| = n - i + 1$ i $K_i \cap K_j = I$, dla $i \neq j$. Następnie zbiory te mogą zostać wykorzystane do wygenerowania tym razem losowej permutacji parzystej z A_n. □

Bibliografia

[1] Bagiński C., *Wstęp do teorii grup*, SCRIPT, Warszawa 2012.

[2] Dixon J.D., Mortimer B., *Permutation groups*, Springer-Verlag, 1996.

[3] Feller W., *Wstęp do rachunku prawdopodobieństwa*, PWN, 1966.

[4] Flachsmeyer J., *Kombinatoryka*, PWN, Warszawa 1977.

[5] Gardiner C.F. *Algebraic structures*, Wiley, 1986.

[6] Gilbert W.J., Nicholson W.K., *Algebra współczesna z zastosowaniami*, WNT, Warszawa 2008.

[7] Hall M., *The theory of groups*, New York, 1968.

[8] Joyner D., *Adventures in group theory*, The Johns Hopkins University Press, 2008.

[9] Kostrikin A., *Wstęp do algebry*, I-III, PWN, 2004.

[10] McKay J.H. *Another proof of Cauchy's group theorem*, Am. Math. Monthly, vol. 66, No. 2, 1959.

[11] Miller W., *The maximum order of an element of a finite symmetric group*, Am. Math. Monthly, vol. 94, 1987, pp. 497–506.

[12] Ross K.A., Wright C.R.B., *Matematyka dyskretna*, PWN, 1996.

[13] Rutkowski J., *Algebra abstrakcyjna w zadaniach*, PWN, 2012.

[14] Rzymowski W., *Macierze i operatory*, UMCS, Lublin 2005.

[15] Seress A., *Permutation group algorithms*, Cambridge University Press, 2003.

[16] Sims Ch. *Computation with finitely presented groups*, Cambridge University Press, 1994.

[17] Wilson R., *Wprowadzenie do teorii grafów*, PWN, Warszawa 2004.

[18] Wussing H., *The genesis of the abstract group concept*, Dover, 1994.