

# TEORIA GRUP

## Wstęp do Teorii Grup



# Rozdział I

## POJĘCIE GRUPY

### § 1. Przykłady wprowadzające

**1. Działania na liczbach całkowitych.** Dodawanie liczb całkowitych spełnia następujące warunki, które nazywamy aksjomatami dodawania i które dla całego dalszego ciągu wykładu będą miały nader wielkie znaczenie.

I. Każde dwie liczby można dodać (tj. dla dowolnych dwóch liczb  $a$  i  $b$  istnieje dokładnie określona liczba  $a+b$ , zwana ich sumą).

II. Postulat łączności dodawania: Dla dowolnych trzech liczb  $a, b, c$  zachodzi tożsamość

$$(a+b) + c = a + (b + c).$$

III. Wśród liczb istnieje dokładnie jedna liczba  $0$  (zero) spełniająca dla każdej liczby  $a$  związek

$$a+0=a.$$

IV. Dla każdej liczby  $a$  istnieje tzw. przeciwna do niej liczba,  $-a$ , o tej własności, że suma  $a+(-a)$  równa się zeru:

$$a + (-a) = 0.$$

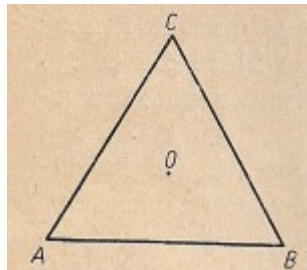
Wreszcie, zajmując nieco odrębne miejsce aksjomat

V. Postulat przemienności dodawania:

$$a + b = b + a.$$

**2. Obroty trójkąta równobocznego.** Wykażemy, że nie tylko liczby, lecz i wiele innych rzeczy można dodawać, zachowując przy tym warunki I-V.

Przykład pierwszy. Rozpatrzmy wszystkie możliwe obroty trójkąta równobocznego  $ABC$  dookoła jego środka  $O$  (rys. 1).



Będziemy przy tym utożsamiali każde dwa obroty różniące się o całkowitą ilość pełnych obrotów (tj. o wielokrotność  $360^\circ$ ) 1). Łatwo widzieć, że spośród wszystkich możliwych obrotów trójkąta tylko trzy obroty przeprowadzają trójkąt w jego pierwotne położenie, a mianowicie: obrót o  $120^\circ$ , obrót o  $240^\circ$  i tzw. obrót zerowy, pozostawiający wszystkie wierzchołki, a co za tym idzie i wszystkie boki trójkąta na miejscu. Pierwszy obrót przeprowadza wierzchołek A w wierzchołek B, wierzchołek B w wierzchołek C i wierzchołek C w wierzchołek A (mówimy, że obrót ten przesuwa wierzchołki ABC cyklicznie). Drugi obrót przesuwa A w C, B w A i C w B, tj. przesuwa cyklicznie wierzchołki w kolejności A,B,C. Teraz, zgodnie ze zdrowym rozsądkiem, wprowadzamy następujące określenie: Dodać dwa obroty, znaczy wykonać je kolejno jeden po drugim. W ten sposób obrót o  $120^\circ$  dodany do samego siebie daje obrót o  $240^\circ$ , a dodany do obrotu o  $240^\circ$  daje obrót o  $360^\circ$ , czyli obrót zerowy. Dwa obroty o  $240^\circ$  dają "obrót o  $480^\circ = 360^\circ + 120^\circ$ ", tj. obrót o  $120^\circ$ . Jeżeli obrót zerowy oznaczymy przez  $a_0$ , obrót o  $120^\circ$  przez  $a_1$ , a obrót o  $240^\circ$  przez  $a_2$ , to otrzymamy następujące związki:

$$a_0 + a_0 = a_0,$$

$$a_1 + a_0 = a_0 + a_1 = a_1,$$

$$a_2 + a_0 = a_0 + a_2 = a_2,$$

$$\begin{aligned}
a_1 + a_1 &= a_2, \\
a_1 + a_2 &= a_2 + a_1 = a_0, \\
a_2 + a_2 &= a_1.
\end{aligned}$$

Tak więc dla każdego dwóch obrotów określona jest ich suma. Czytelnik łatwo przekona się, że to dodawanie spełnia postulat łączności; oczywiście spełnia ono także postulat przemienności. Następnie, wśród rozpatrywanych przez nas obrotów istnieje obrót zerowy spełniający warunek:

$$a + a_0 = a_0 + a = a$$

dla dowolnego obrotu  $a$ . Wreszcie, każdy z trzech rozważanych obrotów ma obrót do niego przeciwny, dający w sumie z danym obrotem zero. Obrót zerowy jest oczywiście przeciwny do samego siebie:  $-a_0 = a_0$ , ponieważ  $a_0 + a_0 = a_0$ , gdy tymczasem  $-a_1 = a_2$  i  $-a_2 = a_1$  (ponieważ  $a_1 + a_2 = a_0$ ). Tak więc dodawanie obrotów trójkąta równobocznego spełnia wszystkie poprzednio wymienione postulaty dodawania. Zapiszemy jeszcze raz nasze prawa dodawania obrotów trójkąta równobocznego bardziej zwartym sposobem w postaci następującej pitagorejskiej tablicy dodawania:

	$a_0$	$a_1$	$a_2$
$a_0$	$a_0$	$a_1$	$a_2$
$a_1$	$a_1$	$a_2$	$a_0$
$a_2$	$a_2$	$a_0$	$a_1$

(I)

Sumę dwóch elementów znajdujemy w tej tablicy na przecięciu wiersza oznaczonego pierwszym elementem i kolumny oznaczonej drugim elementem. Czytelnik, który będzie wykonywał działania na rozważanych obrotach, weźmie po prostu trzy litery  $a_0$ ,  $a_1$  i  $a_2$  i będzie je dodawał posługując się wyżej wypisaną tablicą dodawania; może on przy tym zupełnie zapomnieć, co właściwie te litery oznaczają.

**3. Grupa Kleina rzędu czwartego.** Przykład drugi. Rozpatrzmy zbiór czterech liter  $a_0, a_1, a_2$  i  $a_3$ , których dodawanie określone jest za pomocą następującej tablicy:

	$a_0$	$a_1$	$a_2$	$a_3$
$a_0$	$a_0$	$a_1$	$a_2$	$a_3$
$a_1$	$a_1$	$a_0$	$a_3$	$a_2$
$a_2$	$a_2$	$a_3$	$a_0$	$a_1$
$a_3$	$a_3$	$a_2$	$a_1$	$a_0$

(II)

lub w formie rozwiniętej:

$$\begin{aligned}
a_0 + a_0 &= a_0, & a_0 + a_2 &= a_2 + a_0 = a_2, \\
a_0 + a_1 &= a_1 + a_0 = a_1, & a_0 + a_3 &= a_3 + a_0 = a_3, \\
a_1 + a_1 &= a_0, & a_2 + a_2 &= a_0, \\
a_1 + a_2 &= a_2 + a_1 = a_3, & a_2 + a_3 &= a_3 + a_2 = a_1, \\
a_1 + a_3 &= a_3 + a_1 = a_2, & a_3 + a_3 &= a_0.
\end{aligned}$$

Dodawanie jest określone dla dowolnych dwóch spośród czterech danych liter. Bezpośrednie sprawdzenie wykazuje, że to dodawanie spełnia postulaty łączności i przemienności. Litera  $a_0$  ma podstawowe własności zera; suma dwóch liter, z których jedna jest  $a_0$ , równa się drugiej literze.

W ten sposób okazało się, że w naszej „algebrze czterech liter” są spełnione postulaty I, II, III i V.

Aby się przekonać, że postulat IV jest także spełniony, wystarczy zauważyć, że założyliśmy

$$a_0 + a_0 = a_0, a_1 + a_1 = a_0, a_2 + a_2 = a_0, a_3 + a_3 = a_0,$$

tzn. że każda litera jest do siebie samej przeciwna (przy dodaniu do siebie daje zero). Rozważana „algebra czterech liter” może wydać się na pierwszy rzut oka pewnego rodzaju matematyczną zabawą, igraszką pozbawioną realnej treści. W rzeczywistości prawa tej algebry wyrażone w tablicy (II) mają zupełnie realne znaczenie, z którym się już wkrótce zapoznamy; co więcej, ta „algebra czterech liter” ma poważne znaczenie również w algebrze wyższej. Nazywa się ona grupą Kleina rzędu czwartego.

**4. Obroty kwadratu.** Przykład trzeci. Postępując analogicznie jak postępowaliśmy w przykładzie pierwszym można zbudować pewną różną od poprzedniej „algebrę czterech liter”. Rozpatrzmy kwadrat ABCD i jego obroty dookoła środka przeprowadzające ten kwadrat w pierwotne położenie. Będziemy przy tym znowu utożsamiali każde dwa obroty różniące się o wielokrotność  $360^\circ$ . W ten sposób będziemy mieli tylko cztery obroty, a mianowicie: obrót zerowy, obrót o  $90^\circ$ , obrót o  $180^\circ$  i obrót o  $270^\circ$ . Oznaczmy je odpowiednio symbolami  $a_0, a_1, a_2, a_3$ . Jeżeli przez dodawanie dwóch obrotów będziemy znowu rozumieli kolejne wykonanie ich jeden po drugim, to otrzymamy następującą tablicę dodawania, analogicznie do tablicy w przykładzie drugim:

	$a_0$	$a_1$	$a_2$	$a_3$
$a_0$	$a_0$	$a_1$	$a_2$	$a_3$
$a_1$	$a_1$	$a_2$	$a_3$	$a_0$
$a_2$	$a_2$	$a_3$	$a_0$	$a_1$
$a_3$	$a_3$	$a_0$	$a_1$	$a_2$

Dokładnie w ten sam sposób, co w tym i w pierwszym przykładzie, można rozpatrywać obroty pięciokąta foremnego i ogólnie n-kąta foremnego. Pozostawiamy czytelnikowi przeprowadzenie odpowiednich rozważań i budowę odpowiednich tablic dodawania.

## § 2. Określenie grupy

Zanim posuniemy się dalej w badaniu poszczególnych przykładów podsumujemy rozpatrzone przykłady, wprowadzając następującą podstawową definicję:

Założmy, że dany jest pewien skończony lub nieskończony zbiór  $G$ ; założmy dalej, że dla dowolnych dwóch elementów  $a$  i  $b$  zbioru  $G$  określony jest pewien trzeci element tego zbioru zwany sumą elementu  $a$  i elementu  $b$  oznaczany przez  $a+b$ . Założmy wreszcie, że ta operacja dodawania (tj. operacja pozwalająca przejść od dwóch danych elementów  $a$  i  $b$  do elementu  $a + b$ ) spełnia następujące postulaty:

I. Postulat łączności. Dla dowolnych trzech elementów  $a, b$  i  $c$  zbioru  $G$  spełniony jest związek  $(a+b) + c = a + (b + c)$ .

Warunek ten oznacza, co następuje: Oznaczmy przez  $d$  element zbioru  $G$  będący sumą elementów  $a$  i  $b$ ; tak samo oznaczmy przez  $e$  element  $b + c$  zbioru  $G$ . Wówczas  $d + c$  i  $a + e$  są jednym i tym samym elementem zbioru  $G$ .

II. Postulat istnienia elementu zerowego. Wśród elementów zbioru  $G$  istnieje pewien określony element, zwany elementem zerowym i oznaczany symbolem  $0$ , taki że

$$a+0=0+a=a$$

dla dowolnego elementu  $a$ .

III. Postulat istnienia elementu przeciwnego do dowolnego danego elementu. Dla każdego elementu  $a$  zbioru  $G$  można znaleźć taki element  $-a$  tego samego zbioru  $G$ , że

$$a + (-a) = (-a) + a = 0.$$

Zbiór  $G$  z określoną w nim operacją dodawania spełniającą wyżej przytoczone trzy postulaty nazywamy grupą; same postulaty nazywamy aksjomatami grupy. Niech w grupie  $G$  oprócz trzech

aksjomatów grupy będzie spełniony jeszcze następujący

IV. Postulat przemienności

$$a + b = b + a.$$

W tym przypadku grupę  $G$  nazywamy grupą przemianną lub abelową. Grupę nazywamy skończoną, jeżeli składa się ze skończonej ilości elementów; w przeciwnym przypadku nazywamy ją nieskończoną. Ilość elementów grupy skończonej nazywamy jej rzędem.

Zaznajomiwszy się z definicją grupy widzimy, że przykłady przytoczone w pierwszych dwóch paragrafach tego rozdziału są przykładami grup, a mianowicie poznaliśmy kolejno

1° grupę liczb całkowitych,

2° grupę obrotów trójkąta równobocznego (nazywamy ją także grupą cykliczną rzędu 3),

3° grupę Kleina rzędu 4,

4° grupę obrotów kwadratu (grupę cykliczną rzędu 4).

W końcu paragrafu pierwszego wspomniano jeszcze o grupach obrotów  $n$ -kąta foremnego (grupy cykliczne rzędu  $n$ ). Wszystkie te grupy są przemienne; z wyjątkiem grupy liczb całkowitych wszystkie one są skończone. Jeżeli chodzi o grupę liczb całkowitych, to jest ona oczywiście nieskończona.

### § 3. Elementarne twierdzenia o grupach

**1. Dodawanie dowolnej, skończonej ilości elementów grupy. Pierwsze prawo otwierania nawiasów.** Postulat łączności ma w teorii grup i, co za tym idzie, w całej algebrze bardzo wielkie znaczenie: pozwala on określić sumę nie tylko dwóch, ale i trzech i w ogóle dowolnej skończonej ilości elementów grupy i posługiwać się przy rozpatrywaniu tych sum zwykłymi prawami otwierania nawiasów. W istocie, niech będą dane trzy elementy  $a$ ,  $b$  i  $c$ . Dotychczas jeszcze nie wiemy, co to znaczy dodać te trzy elementy: przecież aksjomaty grupy mówią tylko o sumach dwóch składników i wyrażenia postaci  $a + b + c$  jeszcze nie są określone. Jednakże postulat łączności mówi, że dodając dwa elementy  $a$  i  $b + c$  albo dwa elementy  $a + b$  i  $c$  otrzymamy jako sumę jeden i ten sam element. Jest, więc rzeczą naturalną, że właśnie ten element, będący sumą dwóch elementów  $a$  oraz  $b + c$ , a także sumą dwóch elementów  $a + b$  oraz  $c$ , określimy jako sumę elementów  $a$ ,  $b$ ,  $c$  (w tym porządku jak napisaliśmy) i oznaczmy po prostu przez  $a + b + c$ . W ten sposób na równość

$$a + b + c = (a + b) + c = a + (b + c)$$

należy patrzeć jako na określenie wyrażenia  $a + b + c$ , sumy trzech elementów  $a$ ,  $b$ ,  $c$ .

Dokładnie tak samo można określić sumę czterech elementów  $a$ ,  $b$ ,  $c$ ,  $d$ , np. jako  $a + (b + c + d)$ .

Udowodnimy, że przy tym

$$a + (b + c + d) = (a + b) + (c + d) = (a + b + c) + d.$$

Na podstawie tego, co powiedzieliśmy poprzednio, mamy przede wszystkim

$$a + (b + c + d) = a + b + (c + d).$$

Ale dla trzech elementów  $a$ ,  $b$ ,  $c + d$  mamy

$$a + b + (c + d) = (a + b) + (c + d).$$

Z drugiej strony dla trzech elementów  $a + b$ ,  $c$ ,  $d$  mamy

$$(a + b) + (c + d) = (a + b) + c + d = (a + b + c) + d,$$

czego należało dowieść.

Niechaj symbol  $a_k + \dots + a_r$ , gdzie  $r > k$ , oznacza sumą kolejnych wyrazów ciągu  $a_0, a_1, \dots$  zaczynając od wyrazu ze wskaźnikiem  $k$  kończąc na wyrazie ze wskaźnikiem  $r$ ; na przykład dla  $r = k + 2$  symbol ten oznacza  $a_k + a_{k+1} + a_{k+2}$ . W przypadku gdy  $r = k + 1$ , symbol  $a_k + \dots + a_r$  redukuje się do sumy  $a_k + a_{k+1}$ . Ponadto umawiamy się, że dla  $r = k$  symbol ten oznacza  $a_k$ , a dla  $r < k$  symbol ten nie ma sensu.

Wyrażenie  $a_1 + \dots + a_n$  można określić metodą indukcji zupełnej w sposób następujący:

1° Przyjmujemy, że dla  $n = 0$  wyrażenie to oznacza  $a_0$ .

2° Jeżeli mamy już określone wyrażenie  $a_0 + \dots + a_n$  dla  $n$  równego pewnej liczbie  $r$ , to wyrażenie  $a_0 + \dots + a_n$  dla  $n=r+1$  określamy za pomocą wzoru

$$a_0 + \dots + a_{r+1} = (a_0 + \dots + a_r) + a_{r+1}.$$

Twierdzenie. Jeżeli  $n$  jest dowolną liczbą naturalną to dla dowolnej liczby naturalnej  $m \leq n$  zachodzi tożsamość

$$(1) \quad a_0 + \dots + a_n = (a_0 + \dots + a_{m-1}) + (a_m + \dots + a_n).$$

Dowód. Dowód przeprowadzimy metodą indukcji zupełnej. Dla  $n = 1$  mamy po stronie lewej wzoru (1) wyrażenie  $a_0 + a_1$ , a prawa strona ma sens jedynie w przypadku, gdy  $m = 1$ , i wówczas po prawej stronie mamy również  $a_0 + a_1$ .

Założmy teraz, że twierdzenie jest prawdziwe dla pewnego  $n = k$  i dla każdego  $m$  spełniającego warunek  $m \leq k$ ; znaczy to, że zakładamy prawdziwość wzoru

$$(2) \quad a_0 + \dots + a_k = (a_0 + \dots + a_{m-1}) + (a_m + \dots + a_k),$$

gdzie  $m \leq k$ . Udowodnimy prawdziwość twierdzenia dla  $n = k+1$  i dla każdego  $m$  spełniającego warunek  $m \leq k+1$ . Dodając do obu stron wzoru (2) wyraz  $a_{k+1}$  otrzymamy

$$(a_0 + \dots + a_k) + a_{k+1} = (a_0 + \dots + a_{m-1}) + (a_m + \dots + a_k) + a_{k+1},$$

skąd

$$a_0 + \dots + a_{k+1} = (a_0 + \dots + a_{m-1}) + (a_m + \dots + a_k) + a_{k+1},$$

czyli

$$(3) \quad a_0 + \dots + a_{k+1} = (a_0 + \dots + a_{m-1}) + (a_m + \dots + a_{k+1}).$$

(4)

W ten sposób z założenia prawdziwości wzoru (1) dla pewnego  $n = k$  i każdego  $m$  spełniającego warunek  $m \leq k$  wyprowadziliśmy prawdziwość wzoru (1) dla  $n=k+1$  i  $m \leq k$ . Dla zakończeniu dowodu trzeba jeszcze wykazać prawdziwość wzoru (3) dla  $m=k+1$ , czego można dokonać przez bezpośrednie sprawdzenie. Twierdzenie zostało udowodnione.

**2. Moment zerowy grupy.** Postulat istnienia elementu zerowego mówi: W grupie istnieje pewien element  $0$  taki, że dla dowolnego elementu  $a$  grupy spełniony jest warunek

$$(1) \quad a + 0 = 0 + a = a.$$

Postulat ten wcale nie mówi, że w danej grupie nie może być innego elementu  $0'$ , różnego od  $0$ , o tej samej własności

$$a + 0' = 0' + a = a$$

dla dowolnego  $a$ .

Nieistnienie takiego elementu  $0'$  wynika z następującego silniejszego twierdzenia, które nazywane jest niekiedy twierdzeniem o jednoznaczności elementu zerowego:

**TWIERDZENIE.** Jeżeli dla jakiegoś określonego elementu  $a$  grupy  $G$  można znaleźć element  $0$  spełniający jeden z warunków

$$a + 0_a = a \text{ lub } 0_a + a = a,$$

to  $0_a$ , gdzie  $0$  jest elementem zerowym grupy  $G$ .

Dowód. Załóżmy najpierw, że  $a + 0_a = a$ . Zauważmy przede wszystkim, że dla dowolnego elementu  $b$  mamy

$$b + 0_a = (b + 0) + 0_a = b + 0 + 0_a,$$

co po podstawieniu  $(-a) + a$  w miejsce  $0$  daje

$$b + 0_a = b + (-a) + a + 0_a = b + (-a) + (a + 0_a) = b + (-a) + a = b.$$

Dokładnie w ten sam sposób otrzymujemy

$$0_a + b = (0 + 0_a) + b = (-a) + a + 0_a + b = (-a) + (a + 0_a) + b = (-a) + a + b = b.$$

Tak więc dla dowolnego  $b$  zachodzą równości

$$b + 0_a = 0_a + b = b.$$

Podstawmy w szczególności  $b = 0$ . Otrzymamy

$$(2) \quad 0 + 0_a = 0_a.$$

Ale z drugiej strony, na mocy określenia elementu zerowego, mamy

$$(3) \quad 0 + 0_a = 0_a.$$

Z równości (2) i (3) wynika, że

$$0_a = 0,$$

czego należało dowieść.

Zupełnie w ten sam sposób można wyprowadzić tożsamość  $0_a = 0$  z założenia  $0_a + a = a$ .

**3. Element przeciwny.** Postulat istnienia elementu przeciwnego do danego elementu grupy mówi: Dla każdego elementu  $a$  grupy  $G$  istnieje dokładnie określony element  $-a$  taki, że

$$(-a) + a = a + (-a) = 0.$$

I tu znowu stwierdzimy tylko istnienie elementu  $-a$  nie stwierdzając jednak wcale jego jednoznaczności. Udowodnimy jednoznaczność tego elementu, tj. udowodnimy następujące Twierdzenie. Jeżeli dla danego elementu  $a$  grupy  $G$  istnieje w tej grupie element  $a'$  spełniający jeden z warunków

$$a + a' = 0 \text{ lub } a' + a = 0,$$

to zawsze  $a' = -a$ , gdzie  $-a$  oznacza element przeciwny do elementu  $a$ .

Dowód. Niech

$$a + a' = 0.$$

Skąd wynika, że

$$(-a) + (a + a') = (-a) + 0 = -a,$$

to znaczy

$$[(-a) + a] + a' = -a,$$

czyli

$$0 + a' = -a,$$

skąd

$$a' = -a.$$

W zupełnie taki sam sposób można wyprowadzić tożsamość  $a' = -a$  z założenia  $a' + a = 0$ .

Tak więc dla danego  $a$  istnieje dokładnie jeden element  $x$  spełniający równość  $a + x = 0$  lub  $x + a = 0$ , a mianowicie element  $x = -a$ .

Weźmy teraz pod uwagę element  $-a$ . Element  $a$  spełnia warunek

$$(-a) + a = 0,$$

tzn. jest on dla elementu  $-a$  tym właśnie elementem przeciwnym  $x = -(-a)$ , o którym dopiero co była mowa, tak więc

$$-(-a) = a.$$

-

**4. Odejmowanie. Drugie prawidło otwierania nawiasów.** Niech dane będą dwa elementy  $a$  i  $b$  grupy  $G$ . Do każdego z elementów  $a$  i  $b$  istnieje element przeciwny, a mianowicie odpowiednio  $-a$  i  $-b$ . Sumę elementu  $b$  i elementu  $-a$  nazywamy różnicą między elementem  $b$  (odjemną) i elementem  $a$  (odjemnikiem) i oznaczamy przez  $b - a$

$$(1) \quad b + (-a) = b - a.$$

W ten sposób ostatnia równość jest określeniem różnicy  $b - a$ , tj. określeniem odejmowania (jako działania, określającego różnicę elementów  $b$  i  $a$ ). Na mocy określenia elementu  $-a$  i postulatu łączności dodawania mamy

$$(2) \quad (b - a) + a = [b + (-a)] + a = b + [(-a) + a] = b,$$

tzn. odjemna jest równa sumie różnicy i odjemnika. Innymi słowy,  $b - a$  jest pierwiastkiem równania

$$(3) \quad x + a = b.$$

Ten pierwiastek jest jedyny, jeżeli bowiem  $c$  jest pierwiastkiem równania (3), to  $c + a = b$ , co znaczy, że

$$c + a + (-a) = b + (-a),$$

skąd

$$c = b + (-a) = b - a. \text{ Tak samo równanie}$$

$$(4) \quad a + x = b$$

ma jedyny pierwiastek  $-a + b$ .

UWAGA. Czasami pierwiastek równania (3), tj. element  $b - a = b + (-a)$ , nazywamy różnicą prawostronną, a pierwiastek równania (4), tj. element  $-a + b$  różnicą lewostronną elementów  $b$  i  $a$ . W grupach abelowych różnice te są oczywiście identyczne.

Wniosek. Jeżeli  $a + b = a + c$ , a także jeżeli  $b + a = c + a$ , to  $b = c$ .

Dla odejmowania podstawowe znaczenie ma własność elementu przeciwnego do sumy elementów grupy wyrażona wzorem

$$-(a + b) = -b - a.$$

W istocie, element  $-(a + b)$  jest jedynym elementem grupy, spełniającym warunek

$$(5) \quad a + b + x = 0,$$

ale

$$a + b + [(-b) + (-a)] = a + [b + (-b)] + (-a) = a + 0 + (-a) = a + (-a) = 0.$$

Tak więc właśnie element  $x = (-b) + (-a)$  spełnia warunek (5), czyli istotnie  $-(a + b) = (-b) + (-a)$ , co można napisać w postaci  $-(a + b) = -b - a$ .

Metodą indukcji zupełnej otrzymujemy bez trudu ogólny wynik

$$-(a_1 + \dots + a_n) = -a_n - a_{n-1} - \dots - a_1,$$

gdzie prawa część oznacza element

$$(-a_n) + (-a_{n-1}) + \dots + (-a_1)$$

Stąd na mocy określenia odejmowania wynika

$$c - (a + b) = c - b - a$$

i w ogólności

$$(6) \quad c - (a_1 + \dots + a_{n-1} + a_n) = c - a_n - a_{n-1} - \dots - a_1.$$

W grupach abelowych porządek czynników nie odgrywa żadnej roli i możemy napisać

$$(6') \quad c-(a_1+ \dots +a_{n-1} + a_n) = c - a_1 - \dots -a_{n-1} - a_n.$$

We wzorze (1) ustępu 1 zawarte są zwykłe prawidła elementarnej algebry dotyczące otwierania nawiasów przy dodawaniu i odejmowaniu.

**5. Uwagi dotyczące aksjomatyki grup.** Dotychczas nie stawialiśmy przed sobą zadania znalezienia najmniejszej ilości postulatów, wystarczających do określenia pojęcia grupy. Istotnie, żądaliśmy początkowo, żeby element zerowy spełniał warunki

$$a+0=0+a=a$$

i żeby element  $-a$  przeciwny do danego elementu  $a$  spełniał warunki

$$a + (-a) = (-a) + a = 0.$$

Tymczasem jednak na podstawie twierdzeń udowodnionych w ustępach 2 i 3 tego paragrafu wystarczyłoby żądać spełniania któregośkolwiek z warunków: bądź  $a + 0 = a$ , bądź  $0 + a = a$ , a także któregośkolwiek z warunków: bądź  $a + (-a) = 0$ , bądź  $(-a) + a = 0$ .

Wreszcie zaznaczamy jeszcze, że w określeniu grupy (§ 2) postulaty II i III, tj. postulat istnienia elementu zerowego i postulat istnienia elementu przeciwnego, można by zastąpić jednym postulatem następującym:

Postulat nieograniczonej możliwości odejmowania: Dla dowolnych, dwóch elementów  $a$  i  $b$  można znaleźć elementy  $x$  i  $y$  takie, że  $a+x=b$  i  $y+a=b$ .

Polecamy czytelnikowi przeprowadzenie dowodu.

## Rozdział II

### GRUPY PERMUTACJI

#### § 1. Określenie grupy permutacji

Jeśli trzech ludzi: Paweł, Jan i Piotr, siedzi na ławce, założmy, od strony lewej ku prawej, to można ich przesadzić na sześć różnych sposobów, a mianowicie (licząc cały czas od strony lewej ku prawej):

1° Paweł, Jan, Piotr,

2° Paweł, Piotr, Jan,

3° Jan, Paweł, Piotr,

4° Jan, Piotr, Paweł,

5° Piotr, Paweł, Jan,

6° Piotr, Jan, Paweł.

Przejście od pewnego dowolnego uporządkowania, jakim oni siedzą, do dowolnego innego uporządkowania nazywamy permutacją. Permutację zapisujemy w następujący sposób:

$$\begin{pmatrix} \text{Paweł, Jan, Piotr} \\ \text{Jan, Piotr, Paweł} \end{pmatrix}$$

oznacza to, że Jan siadł na miejscu Pawła, Piotr – na miejscu Jana, a Paweł na miejscu Piotra.

W tym sensie można mówić o permutacjach dowolnych przedmiotów. Ponieważ przy tym rodzaj przestawianych przedmiotów nie ma znaczenia, więc przedmioty te oznaczamy zazwyczaj liczbami i mówimy o permutacjach liczb. Tak więc dla trzech liczb 1, 2, 3 otrzymujemy sześć permutacji

$$\begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}$$

Każda permutacja polega na tym, że na miejsce liczby stojącej w górnym wierszu stawiamy liczbę podpisaną pod nią w dolnym wierszu. Pierwsza permutacja:

$$\begin{pmatrix} 123 \\ 123 \end{pmatrix}$$

nazywa się permutacją tożsamościową, pozostawia ona każdą liczbę na swoim miejscu.

Dругa permutacja

$$\begin{pmatrix} 123 \\ 132 \end{pmatrix}$$

polega na tym, że liczba 1 zostaje na swoim miejscu, liczba 3 wchodzi na miejsce liczby 2, a liczba 2 - na miejsce liczby 3 itd. Ogólna postać permutacji z  $n$  liczb 1, 2, ...,  $n$  jest następująca:

$$\begin{pmatrix} 12\dots n \\ i_1 i_2 \dots i_n \end{pmatrix}$$

Tutaj  $i_1, i_2, \dots, i_n$  są tymi samymi liczbami 1, 2, ...,  $n$ , tylko napisanymi w innym na ogół porządku, np.

$$\begin{pmatrix} 12345 \\ 31452 \end{pmatrix}$$

Tu oczywiście  $n = 5$ ,  $i_1 = 3$ ,  $i_2 = 1$ ,  $i_3 = 4$ ,  $i_4 = 5$ ,  $i_5 = 2$ . Jak wiadomo, z  $n$  liczb można otrzymać  $n!$  permutacji. Powróćmy do permutacji z trzech liczb. Dodanie dwóch permutacji oznacza ich kolejne wykonanie. W rezultacie otrzymamy znowu permutację, zwaną sumą dwóch danych permutacji. Dodajmy na przykład permutacje

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix} + \begin{pmatrix} 123 \\ 321 \end{pmatrix}$$

Pierwsza permutacja zamienia jedynekę na dwójkę, a druga pozostawia dwójkę bez zmiany; tak więc po kolejnym przeprowadzeniu obu permutacji jedynka przejdzie na dwójkę. Dokładnie tak samo rozumując przekonamy się, że po przeprowadzeniu kolejno obu permutacji dwójka przejdzie na miejsce trójki, a trójka zostanie przeprowadzona na miejsce jedynki. Dlatego

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix} + \begin{pmatrix} 123 \\ 321 \end{pmatrix} = \begin{pmatrix} 123 \\ 231 \end{pmatrix}$$

Dokładnie w taki sam sposób można dodać dowolne dwie permutacje. Aby w dogodny sposób zapisać rezultaty tych wszystkich dodawań wprowadzimy następujące oznaczenia:

$$P_0 = \begin{pmatrix} 123 \\ 123 \end{pmatrix} P_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} P_3 = \begin{pmatrix} 123 \\ 231 \end{pmatrix}$$

$$P_4 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} P_5 = \begin{pmatrix} 123 \\ 321 \end{pmatrix}$$

$P_0$  nazywamy permutacją tożsamościową.

Aby znaleźć sumę dwóch permutacji, na przykład  $P_2 + P_4$ , należy wziąć wiersz, w którego nagłówku (pierwszy składnik) znajduje się pierwsza permutacja (w naszym przypadku  $P_2$ ), i kolumnę, w nagłówku której (drugi składnik) znajduje się druga permutacja (w naszym przypadku  $P_4$ ). Na przecięciu wybranego Wiersza i wybranej kolumny będzie znajdowała się szukana suma  $P_2 + P_4 = P_1$ . Przeprowadzimy ten rachunek szczegółowo. Mamy

$$P_2 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} \quad \text{i} \quad P_4 = \begin{pmatrix} 123 \\ 312 \end{pmatrix}.$$

i za pomocą takich samych rozważań, jak w przypadku równości (1) otrzymamy

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix} + \begin{pmatrix} 123 \\ 312 \end{pmatrix} = \begin{pmatrix} 123 \\ 132 \end{pmatrix}$$

tj. istotnie  $P_2 + P_4 = P_1$ . Otrzymujemy następującą tablicę dodawania:

Pier- wszy składnik	Drugi składnik					
	$P_0$	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$
$P_0$	$P_0$	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$
$P_1$	$P_5$	$P_0$	$P_3$	$P_2$	$P_5$	$P_4$
$P_2$	$P_2$	$P_4$	$P_0$	$P_5$	$P_1$	$P_3$
$P_3$	$P_3$	$P_5$	$P_1$	$P_4$	$P_0$	$P_2$
$P_4$	$P_4$	$P_2$	$P_5$	$P_0$	$P_3$	$P_1$
$P_5$	$P_5$	$P_3$	$P_4$	$P_1$	$P_2$	$P_0$

Polecamy czytelnikowi sprawdzić tym samym sposobem całą tę tablicę dodawania. Przez bezpośrednie sprawdzenie (a także za pomocą prostych rozważań) można się przekonać, że nasze dodawanie spełnia postulat łączności. Rolę elementu zerowego (zera) odgrywa oczywiście permutacja tożsamościowa:

$$P_0 = \begin{pmatrix} 123 \\ 123 \end{pmatrix}$$

Wreszcie dla każdej permutacji i istnieje przeciwna do niej, dająca w sumie z nią permutację tożsamościową; permutacja przeciwna do danej stawia wszystkie liczby, przestawione przez daną permutację, na ich poprzednie miejsce. Tak na przykład

$$-\begin{pmatrix} 123 \\ 231 \end{pmatrix} = \begin{pmatrix} 123 \\ 312 \end{pmatrix}$$

Aby od razu znaleźć w naszej tablicy permutację przeciwną do danej, należy w wierszu oznaczonym z lewej strony daną permutacją znaleźć element  $P_0$ ; w nagłówku kolumny, do której należy ten element, stoi właśnie permutacja przeciwna do danej. Mamy, jak łatwo się przekonać,

$$\begin{array}{lll} -P_0 = P_0, & -P_2 = P_2, & -P_4 = P_3, \\ -P_1 = P_1, & -P_3 = P_4, & -P_5 = P_5 \end{array}$$

Tak więc dodawanie permutacji spełnia wszystkie aksjomaty grupy; zbiór wszystkich permutacji z trzech elementów tworzy grupę. Grupę tę oznaczamy przez  $S_3$ . (Grupa  $S_3$  jest skończona, jej rząd wynosi 6. Nie jest ona grupą abelową. Istotnie, mamy na przykład

$$P_2 + P_3 = P_5, \quad P_3 + P_2 = P_1.$$

## § 2. Pojęcie podgrupy, wyjaśnione na przykładzie grup permutacji

**1. Przykład i określenie.** Jest naturalnym pytaniem, czy można otrzymać grupę, biorąc nie wszystkie, a tylko niektóre spośród naszych permutacji (z tychże trzech liczb) i pozostawiając oczywiście te same prawa dodawania. Łatwo się przekonać, że odpowiedź na to pytanie jest twierdząca. W istocie, rozpatrzmy na przykład parę elementów  $P_0$  i  $P_1$ . Nasza tablica dodawania daje nam bezpośrednio

$$\begin{array}{ll} P_0 + P_0 = P_0, & P_0 + P_1 = P_1, \\ P_1 + P_0 = P_1 & P_1 + P_1 = P_0. \end{array}$$

Widzimy, że wszystkie aksjomaty grupy są spełnione (w szczególności  $-P_0 = P_0$  i  $-P_1 = P_1$ ), to znaczy, że elementy  $P_0$  i  $P_1$ , tworzą grupę będącą częścią grupy wszystkich permutacji z trzech liczb. Dokładnie w ten sam sposób przekonamy się z kolei, że pary elementów  $P_0$  i  $P_2$  oraz  $P_0$  i  $P_5$  także tworzą grupę. Para  $P_0$  i  $P_3$  (a także para  $P_0$  i  $P_4$ ) nie tworzy grupy, ponieważ  $P_3 + P_3 = P_4$  (tj. element  $P_3$  dodany do samego siebie daje w wyniku element nie należący do naszej pary). Te proste rozważania uprawniają nas do wprowadzenia następującej ogólnej definicji:

Jeśli dana jest dowolna grupa  $G$  i jeżeli zbiór  $H$  składający się z pewnych elementów grupy  $G$  tworzy grupę (o tej samej operacji dodawania co w grupie  $G$ ), to grupa  $H$  nazywa się podgrupą grupy  $G$ .

W ten sposób każda z par elementów  $(P_0, P_1)$ ,  $(P_0, P_2)$ ,  $(P_0, P_5)$  jest podgrupą rzędu 2 grupy  $S_3$ . Innym podgrup rzędu 2 grupa  $S_3$  nie zawiera; z określenia podgrupy wynika, że każda podgrupa  $H$  grupy  $G$  zawiera element zerowy grupy  $G$ , to znaczy, że każda podgrupa rzędu 2 grupy  $S_3$  ma postać  $(P_0, P_i)$ , gdzie  $i$  jest jedną z liczb 1, 2, 3, 4, 5; ale widzieliśmy, że  $i$  nie może równać się ani 3, ani 4, wobec czego pozostają tylko rozpatrzone już podgrupy  $(P_0, P_1)$ ,  $(P_0, P_2)$ ,  $(P_0, P_5)$ . W grupie  $S_3$  istnieje także podgrupa, składająca się z trzech elementów (podgrupa rzędu 3). Jest to podgrupa  $(P_0, P_3, P_4)$ . Niech czytelnik sam przekona się, że jest to jedyna podgrupa rzędu 3 zawarta w  $S_3$ . Podgrup rzędu 4 i 5 w grupie  $S_3$  w ogóle nie ma. Tak więc podgrupami grupy  $S_3$  są:

1° trzy podgrupy rzędu 2, mianowicie  $(P_0, P_1)$ ,  $(P_0, P_2)$ ,  $(P_0, P_5)$ ;

2° jedna podgrupa rzędu 3, mianowicie  $(P_0, P_3, P_4)$ .

W ten sam sposób, w jaki zbadaliśmy grupę  $S_3$ , można byłoby zbadać grupę  $S_4$ , składającą się ze wszystkich permutacji z czterech liczb.

Grupa  $S^4$  jest rzędu  $1 \cdot 2 \cdot 3 \cdot 4 = 24$ . W ogólnym przypadku dla dowolnego  $n$  wszystkie permutacje z  $n$  liczb tworzą grupę  $S_n$  rzędu  $1 \cdot 2 \cdot 3 \cdot \dots \cdot n$ . Prawo dodawania jest we wszystkich tych grupach jednakowe: Dodać dwie permutacje z  $n$  liczb - znaczy kolejno wykonać te permutacje jedną po drugiej. Zaznaczymy wreszcie, że grupę  $S_n$  wszystkich permutacji z  $n$  elementów nazywa się często grupą symetryczną (permutacji z  $n$  elementów).

Dowolną podgrupę grupy  $S_n$  nazywamy grupą permutacji z  $n$  elementów.

**2. Warunek, aby podzbiór grupy był podgrupą.** Przy dowodzie, że pewien podzbiór  $H$  grupy  $G$  jest podgrupą, bardzo wygodnie bywa posługiwać się następującym twierdzeniem:

Podzbiór  $H$  grupy  $G$  jest wtedy i tylko wtedy podgrupą grupy  $G$ , jeżeli spełnione są następujące

warunki:

1° Suma dwóch elementów  $a$  i  $b$  zbioru  $H$  (w sensie dodawania, określonego w grupie  $G$ ) jest elementem zbioru  $H$ .

2° Element zerowy grupy  $G$  jest elementem zbioru  $H$ .

3° Dla dowolnego elementu zbioru  $H$  element przeciwny do niego także należy do  $H$ .

Dla dowodu wystarczy zauważyć, że nasze warunki wyrażają dokładnie żądanie, aby operacja dodawania określona w  $G$ , ale stosowana tylko do tych elementów grupy  $G$ , które należą jednocześnie do  $H$ , spełniała wszystkie aksjomaty grupy (łączności żądać nie trzeba: jest ona spełniona przy dodawaniu dowolnych elementów zbioru  $G$ , więc tym bardziej jest spełniona w przypadku szczególnym, gdy te elementy są zarazem elementami zbioru  $H$ ).

### § 3. Permutacje jako odwzorowania zbioru skończonego na siebie3). Permutacje parzyste i nieparzyste

1. Wprowadziliśmy pojęcie permutacji sposobem elementarnym i zarazem nieco „chałupniczym”, jak to zwykle się czyni. Jeżeli nie obawiać się ogólnomatematycznych terminów, to permutację z  $n$  elementów określamy prosto jako wzajemnie jednoznaczne odwzorowanie  $f$  zbioru danych  $n$  elementów na ten sam zbiór. Jeżeli naszymi elementami są, przypuśćmy, liczby  $1, 2, 3, \dots, n$ , to permutację

$$\begin{pmatrix} 12\dots n \\ a_1 a_2 \dots a_n \end{pmatrix}$$

określa się jako funkcję

$$a_k = f(k), \quad k=1, 2, \dots, n$$

przy czym zarówno argument, jak i wartość funkcji przebiegają zbiór liczb  $1, 2, \dots, n$ . Dla dwóch różnych wartości argumentu wartości funkcji są zawsze różne.

W szczególności permutacja jest dokładnie określona, jeżeli dla każdego  $k$  dana jest wartość  $f(k)$ , tj.  $a_k$ .

Skąd wynika, że jest rzeczą zupełnie nieistotną, w jakim porządku zapisane są liczby w górnym wierszu i ważne jest tylko, aby pod liczbą  $k$  była napisana właśnie liczba  $a_k$ . Na przykład

$$\begin{pmatrix} 12345 \\ 24351 \end{pmatrix} \text{ i } \begin{pmatrix} 34521 \\ 35142 \end{pmatrix}$$

są dwoma zapisami jednej i tej samej permutacji. Tej właściwie oczywistej uwadze można też nadać następującą postać:

Niech dana będzie permutacja

$$(1) \quad A = \begin{pmatrix} 123\dots n \\ a_1 a_2 \dots a_n \end{pmatrix}$$

Jeżeli

$$(2) \quad P = \begin{pmatrix} 123\dots n \\ p_1 p_2 \dots p_n \end{pmatrix}$$

jest dowolną permutacją z tych samych liczb  $1, 2, \dots, n$ , to permutację (1) możemy zapisać w postaci

$$\begin{pmatrix} p_1 p_2 p_3 \dots p_n \\ a_{p_1} a_{p_2} \dots a_{p_n} \end{pmatrix}$$

**2. Permutacje parzyste i nieparzyste.** Niech dana będzie permutacja

$$A = \begin{pmatrix} 123\dots n \\ a_1 a_2 \dots a_n \end{pmatrix}$$

Rozpatrzmy dowolny zbiór składający się z jakichkolwiek dwóch spośród liczb  $1, 2, \dots, n$ , przypuśćmy z liczb  $i$  i  $k$ . Taki zbiór nazywamy parą liczb, a mianowicie parą, składającą się z elementów  $i$  i  $k$ , i oznaczamy przez  $(i, k)$ .

Jak wiadomo, ilość wszystkich par, które można wybrać spośród danych  $n$  elementów, wynosi

$$\binom{n}{2} = \frac{n(n-1)}{1 \cdot 2}$$

Mówimy, że para składająca się z elementów  $i$  i  $k$  nie daje nieporządku w permutacji  $A$ , jeżeli różnice  $i - k$  oraz  $a_i - a_k$  mają ten sam znak; oznacza to, że jeżeli  $i < k$ , to musi być  $a_i < a_k$ ; jeżeli natomiast  $i > k$ , to musi być  $a_i > a_k$ . W przypadku przeciwnym mówimy, że nasza para daje w permutacji  $A$  nieporządek lub częściej: inwersję. Widzimy, że jeżeli para  $(i, k)$  daje inwersję, to mamy albo  $i < k$  i  $a_i > a_k$ , albo  $i > k$  i  $a_i < a_k$ .

Jako przykład rozpatrzmy permutacje grupy  $S_3$ .

W permutacji  $P_0 = \begin{pmatrix} 123 \\ 123 \end{pmatrix}$  nie ma ani jednej inwersji

W permutacji  $P_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix}$  jedyną inwersję tworzy para  $(2,3)$

W permutacji  $P_2 = \begin{pmatrix} 123 \\ 213 \end{pmatrix}$  jedyną inwersję tworzy para  $(1,2)$

W permutacji  $P_3 = \begin{pmatrix} 123 \\ 231 \end{pmatrix}$  istnieją dwie inwersje utworzone przez pary  $(1,3)$  i  $(2,3)$

W permutacji  $P_4 = \begin{pmatrix} 123 \\ 312 \end{pmatrix}$  istnieją dwie inwersje, utworzone przez pary  $(1,3)$  i  $(1,2)$

W permutacji  $P_5 = \begin{pmatrix} 123 \\ 321 \end{pmatrix}$  istnieją trzy inwersje utworzone przez pary  $(1,2)$ ,  $(1,3)$  i  $(2,3)$

Określenie. Permutację mającą parzystą ilość inwersji nazywamy permutacją parzystą; permutację mającą nieparzystą ilość inwersji nazywamy permutacją nieparzystą. Widzieliśmy, że w grupie  $S_3$  permutacje parzyste ( $P_0, P_3$  i  $P_4$ ) tworzą podgrupę. Naszym zadaniem będzie udowodnić, że to samo zachodzi dla dowolnej grupy  $S_n$ . Dowód, ten opiera się na pewnych wstępnych rozważaniach, do których obecnie przejdziemy.

Znakiem permutacji  $A$  będziemy nazywali liczbę  $+1$ , jeżeli permutacja  $A$  jest parzysta, a liczbę  $-1$ , jeżeli jest ona nieparzysta. Abstrahując od zwykłego użycia tego słowa nazwiemy teraz znakiem liczby wymiernej  $r$  liczbę  $+1$ , jeżeli  $r$  jest dodatnie, liczbę  $-1$ , jeżeli  $r$  jest ujemne i liczbę  $0$ , jeżeli  $r = 0$ . Znak liczby  $r$  w wyżej ustalonym sensie będziemy oznaczali przez  $\text{sgn } r$ . Przy tych oznaczeniach jest jasne, że znak permutacji  $A$  równy jest iloczynowi znaków wszystkich  $n(n-1)/2$  liczb  $(i-k)/(a_i - a_k)$ , przy czym ułamek  $(i-k)/(a_i - a_k) = (k-i)/(a_k - a_i)$  tworzymy dla każdej pary wybranej spośród liczb  $1, 2, 3, \dots, n$  tylko raz. Ta uwaga posłuży nam przy dowodzie następującego twierdzenia:

Znak sumy dwóch permutacji równa się iloczynowi znaków składników.

Niech dane będą dwie permutacje

$$A = \begin{pmatrix} 123\dots n \\ a_1 a_2 \dots a_n \end{pmatrix}, B = \begin{pmatrix} 123\dots n \\ b_1 b_2 \dots b_n \end{pmatrix}$$

Ich sumą jest oczywiście permutacja

$$(1) \quad A + B = \begin{pmatrix} 123\dots n \\ b_{a_1} b_{a_2} \dots b_{a_n} \end{pmatrix}$$

Znak A równy jest iloczynowi wszystkich znaków

$$i-k / a_i - a_k$$

Znak B równy jest iloczynowi wszystkich znaków

$$i-k / b_i - b_k$$

Ponieważ można także napisać

$$B = \begin{pmatrix} a_1 a_2 \dots a_n \\ b_{a_1} b_{a_2} \dots b_{a_n} \end{pmatrix}$$

wiec mamy:

Znak B równy jest iloczynowi wszystkich znaków  $(a_i - a_k)/(b_i - b_k)$ . Stąd natychmiast wynika:

$$\text{sgn } A * \text{sgn } B =$$

$$\begin{aligned} &= \text{iloczynowi wszystkich } \text{sgn } i-k/a_i - a_k * \text{sgn } a_i - a_k/b_{a_i} - b_{a_k} = \\ &= \text{iloczynowi wszystkich } \text{sgn } i-k/a_i - a_k * a_i - a_k/b_{a_i} - b_{a_k} = \\ &= \text{iloczynowi wszystkich } \text{sgn } i-k / b_{a_i} - b_{a_k} \end{aligned}$$

Ale ostatni iloczyn jest równy znakowi permutacji

$$\begin{pmatrix} 123\dots n \\ b_{a_1} b_{a_2} \dots b_{a_n} \end{pmatrix}$$

tj. permutacji  $A+B$ , co należało okazać.

Z udowodnionego twierdzenia bezpośrednio wynika: Suma dwóch permutacji jednakowej parzystości jest permutacją parzystą, a suma dwóch permutacji o różnej parzystości jest permutacją nieparzystą. Permutacja tożsamościowa nie zawiera ani jednej inwersji i, co za tym idzie, jest permutacją parzystą. Dalej mamy

$$A + (-A) = 0,$$

tj. suma danej permutacji  $A$  i permutacji do niej przeciwnej jest permutacją parzystą; stąd na podstawie udowodnionego wyżej twierdzenia wynika, że dowolna permutacja ma tę samą parzystość co przeciwna do niej. Tak więc suma dwóch permutacji parzystych jest permutacją parzystą, permutacja tożsamościowa jest permutacją parzystą i permutacja przeciwna do parzystej jest też parzysta. Stąd wynika, że zbiór wszystkich permutacji parzystych z  $n$  elementów jest podgrupą grupy  $S_n$  wszystkich permutacji z  $n$  elementów. Grupa permutacji parzystych z  $n$  elementów nosi nazwę naprzemiennej lub alternującej grupy permutacji z  $n$  elementów i jest oznaczona przez  $A_n$ .

Twierdzenie. Rząd grupy  $A_n$  wynosi  $n!/2$ . Innymi słowy do grupy  $A_n$  należy dokładnie połowa wszystkich permutacji z  $n$  elementów. Aby się o tym przekonać, wystarczy ustalić wzajemnie jednoznaczność między zbiorem wszystkich parzystych a zbiorem wszystkich nieparzystych permutacji z  $n$  elementów. Odpowiedniość taką ustalimy, jeżeli wybierzemy dowolną nieparzystą permutację  $P$  i każdej permutacji parzystej  $A$  przyporządkujemy odpowiednio permutację  $P + A$ . Tym sposobem:

1° Każdej permutacji parzystej będzie odpowiadała permutacja nieparzysta.

2° Dwom różnym permutacjom parzystym będą odpowiadały różne permutacje nieparzyste.

3° Każda permutacja nieparzysta  $B$  będzie przyporządkowana jednej (i tylko jednej) permutacji parzystej, a mianowicie permutacji  $-P + B$ .

W ten sposób wspomniana odpowiedniość jest odpowiednością wzajemnie jednoznacznością między zbiorem wszystkich permutacji parzystych a zbiorem wszystkich permutacji nieparzystych.

## Rozdział II

### PEWNE OGÓLNE UWAGI O GRUPACH. POJĘCIE IZOMORFIZMU

#### § 1. „Addytywna” i „mnożeniowa” terminologia w teorii grup

Częściami składowymi pojęcia grupy są:

- zbiór tych przedmiotów (liczb, permutacji, obrotów itp.), które są elementami grupy;
- określona operacja, czyli działanie, które nazwaliśmy dodawaniem, a które pozwala dla każdego dwóch  $a$  i  $b$  naszej grupy znaleźć trzeci element  $a + b$  tejże grupy.

Wybraliśmy termin dodawanie na oznaczenie działania, które zachodzi w każdej grupie. Wybór tego czy innego terminu nie wpływa oczywiście na istotę rzeczy; W odniesieniu do każdej grupy można by mówić o mnożeniu jej elementów (a nie o ich dodawaniu), prowadzić rozważania w języku mnożeniowym, a nie w addytywnym. Dotychczas zaznajomiliśmy się z językiem addytywnym, czyli jak mówimy z addytywnym zapisem grupy. Teraz pokażemy, jak wyrażą się aksjomaty grupy w języku mnożeniowym (w mnożeniowym zapisie).

Przede wszystkim żądamy, żeby dla każdego dwóch elementów  $a$  i  $b$  naszego zbioru  $G$  był jednoznacznie określony element  $ab$  - iloczyn dwóch elementów  $a$  i  $b$ . Charakterystyczne dla grup aksjomaty przyjmą przy tym następującą postać:

I. Postulat łączności

$$(ab)c = a(bc).$$

II. Postulat istnienia elementu jednostkowego.

Wśród elementów zbioru  $G$  istnieje pewien dokładnie jeden element, zwany elementem jednostkowym, który oznaczamy przez  $e$  i nazywamy jednością grupy, taki że

$$ae = ea = a$$

dla dowolnego elementu  $a$ .

III. Warunek istnienia elementu odwrotnego do każdego danego elementu grupy.

Dla każdego danego elementu  $a$  zbioru  $G$  można znaleźć dokładnie jeden taki element  $a^{-1}$  zbioru  $G$ , że

$$aa^{-1} = a^{-1}a = e.$$

Widzimy więc, że jeżeli przemianować operację określającą daną grupę z dodawania na mnożenie, to będzie rzeczą naturalną zmienić też nazwę elementu „neutralnego” z zera na jedność i mówić o elementach odwrotnych ( $a^{-1}$ ), zamiast o elementach przeciwnych ( $-a$ ). Ta mnożeniowa terminologia jest historycznie wcześniejsza i obecnie stosowana jest przez niewątpliwą większość autorów. Najwygodniej jest w pewnych przypadkach prowadzić rozważanie dotyczące grup w addytywnym, a w innych w mnożeniowym języku. Wreszcie - jest wiele przypadków, gdy oba języki są jednakowo wygodne. Jako przykład, w którym rzeczywiście wygodniej jest posługiwać się językiem addytywnym, wskażemy grupę liczb całkowitych; operacją grupową jest tu zwykłe arytmetyczne dodawanie, elementem zerowym - zwykłe arytmetyczne zero, a pojęcie liczby

przeciwnej ma także swój zwykły arytmetyczny sens. Nie ma sensu spierać się o to, że niezgrabnie i niewygodnie byłoby zwykłe arytmetyczne dodawanie nazwać nagle mnożeniem, zero - jednością itd. Jednakże czytelnik powinien dobrze zrozumieć, że - niezależnie od wszelkich niewygód takiego przemianowania - jest ono całkiem możliwe i nie doprowadza do żadnych sprzeczności tak długo, jak długo ograniczalibyśmy się do badania grupy liczb całkowitych, tj. rozpatrywali jedną operację na liczbach całkowitych, a mianowicie arytmetyczne dodawanie.

Jeżeli równocześnie z arytmetycznym dodawaniem i rozpatrywalibyśmy i mnożenie (też w elementarnym, arytmetycznym znaczeniu), to przemianowanie, o którym była mowa, dodawania na mnożenie oczywiście zupełnie zagmatwałoby terminologię. Jako przykład grupy, dla której, przeciwnie, bardziej wygodny jest język mnożeniowy, rozpatrzmy grupę  $R$ , składającą się ze wszystkich dodatnich i ujemnych liczb wymiernych tj. ze wszystkich liczb wymiernych różnych od zera.

Jako operację grupową w grupie  $R$  przyjmujemy zwykłe arytmetyczne mnożenie. To działanie jest oczywiście łączne; zwykła jedynka spełnia w odniesieniu do naszej operacji postulat II:

$$a \cdot 1 = a \text{ dla dowolnego } a .$$

Wreszcie - dla każdego elementu zbioru  $R$  (tj. dla każdej liczby wymiernej  $a \neq 0$ ) istnieje liczba wymierna  $a^{-1} = 1/a \neq 0$ , spełniająca warunek  $aa^{-1}=1$ . Tak więc wszystkie aksjomaty grupy są spełnione; zatem wszystkie liczby wymierne różne od zera tworzą grupę ze względu na działanie zwykłego arytmetycznego mnożenia. Ponieważ  $ab = ba$ , więc grupa ta jest abelowa. Podgrupą tej grupy jest grupa wszystkich liczb wymiernych dodatnich ( $a > 0$ ). W odniesieniu do tych grup wygodniej jest posługiwać się językiem mnożeniowym. Niech czytelnik przekona się sam, że liczby wymierne ujemne nie tworzą grupy ze względu na działanie zwykłego arytmetycznego mnożenia. Wreszcie wszystkie liczby wymierne (włączając w to i liczbę zero) nie tworzą grupy ze względu na operację arytmetycznego mnożenia, ponieważ nie istnieje liczba odwrotna do zera.

Niemniej jednak ze względu na operację dodawania zbiór wszystkich liczb wymiernych tworzy, jak się o tym łatwo można przekonać, grupę  $R$ . Grupa ta zawiera jako podgrupę grupę liczb całkowitych. Aby skończyć omawianie problemów terminologicznych, zaznaczymy, że w odniesieniu do grupy permutacji nie ma poważnych podstaw do przekładania języka addytywnego nad mnożeniowy czy odwrotnie. Jednakże w języku mnożeniowym jedno z twierdzeń poprzedniego rozdziału otrzymuje bardziej symetryczną formę, a mianowicie: Znak iloczynu dwóch permutacji równa się iloczynowi ich znaków. W obecnych czasach staje się rzeczą coraz bardziej ogólnie przyjętą mówić o grupach abelowych w języku addytywnym (choć widzieliśmy dopiero co wyjątek od tej zasady na przykładzie grupy liczb wymiernych różnych od zera).

W tej książce będziemy trzymali się języka addytywnego nawet w zastosowaniu do grup nieabelowych.

## § 2. Grupy izomorficzne

Rozpatrzmy z jednej strony grupę  $R_3$  obrotów trójkąta równobocznego (rozd. 1, § 1), a z drugiej strony zawartą w grupie wszystkich permutacji z trzech cyfr podgrupę  $A_3$ , składającą się z trzech elementów  $P_0, P_3, P_4$  (rozd. II, §2). Elementy grupy  $R_3$  oznaczaliśmy przez  $a_0, a_1, a_2$ . Ustalimy teraz następującą wzajemnie jednoznaczność między elementami grupy  $R_3$  u elementami grupy  $A_3$ :

$$a_0 \leftrightarrow P_0,$$

$$a_1 \leftrightarrow P_3,$$

$$a_2 \leftrightarrow P_4.$$

Ta odpowiedniość zachowuje dodawanie w następującym sensie. Jeżeli dowolny element w lewej kolumnie może być napisany w postaci sumy dwóch elementów (oczywiście należących do tej samej lewej kolumny), na przykład  $a_0 + a_1 = a_1$  lub  $a_1 + a_1 = a_2$ , lub  $a_1 + a_2 = a_0$  i jeżeli każdy element otrzymanej równości zastąpimy przez odpowiedni element z prawej kolumny, to równość

pozostanie prawdziwa. Widzimy więc, że grupy  $R_3$  i  $A_3$ , chociaż składają się z elementów różnego gatunku (jedna grupa składa się z obrotów trójkąta, druga z permutacji cyfr), zbudowane są jednakowo; tablice dodawania tych grup różnią się tylko oznaczeniem i, co za tym idzie, przez zmianę tych oznaczeń, tj. przez przemianowanie elementów, mogą one być przekształcone jedna w drugą. Takie grupy, w których przy odpowiednim wyborze oznaczeń elementów tablice dodawania są identyczne, nazywamy grupami izomorficznymi. Zazwyczaj definicję izomorfizmu grup wypowiada się w nieco innej formie. Chodzi o to, że „przemianowanie” elementów w tablicy dodawania, o które chodziło w naszym określeniu izomorfizmu, sprowadza się w istocie do ustalenia wzajemnie jednoznacznej odpowiedniości między elementami dwóch grup. Podamy teraz określenie izomorfizmu wychodząc bezpośrednio z pojęcia odwzorowania wzajemnie jednoznacznego.

Określenie I. Niech dana będzie wzajemnie jednoznaczna odpowiedniość

$$g \leftrightarrow g'$$

między zbiorem wszystkich elementów grupy  $G$  i zbiorem wszystkich elementów grupy  $G'$ . Powiemy, że ta odpowiedniość jest odpowiednością izomorficzną (lub izomorfizmem) między tymi grupami, jeżeli spełniony jest warunek zachowania dodawania, mówiący:

Dla dowolnego związku postaci

$$g_1 + g_2 = g_3$$

między elementami jednej grupy, np.  $G$ , związek otrzymany przez zamianę elementów  $g_1, g_2, g_3$  grupy  $G$  odpowiadającymi im w grupie  $G'$  elementami  $g'_1, g'_2$  i  $g'_3$

będzie także spełniony:

$$g'_1 + g'_2 = g'_3$$

Określenie II. Dwie grupy nazywamy izomorficznymi, jeżeli można między nimi ustalić odpowiedniość izomorficzną.

Uwaga. Jeżeli żądać, żeby zawsze z warunku

$$g_1 + g_2 = g_3 \text{ (w grupie } G\text{)}$$

wynikał warunek

$$g'_1 + g'_2 = g'_3$$

dla elementów grupy  $G'$  odpowiadających elementom  $g_1, g_2, g_3$ , to zachodzi i zależność odwrotna, a mianowicie: Jeśli dla dowolnych trzech elementów  $g'_1, g'_2$  i  $g'_3$  z grupy  $G'$  zachodzi związek

$$(1) \quad g'_1 + g'_2 = g'_3$$

Istotnie, jeżeliby związek (1) nie był spełniony, to byłoby

$$g_1 + g_2 = g_4 \neq g_3$$

Na mocy wzajemnie jednoznacznej odpowiedniości między  $G$  i  $G'$  elementowi  $g_4$  grupy  $G$  odpowiada w grupie  $G'$  element  $g'_4 \neq g'_3$  i wobec naszego założenia

$$g_1 + g_2 = g_4$$

powinno wynikać

$$g'_1 + g'_2 = g'_4$$

co jest sprzeczne z tym, że

$$g'_1 + g'_2 = g'_3$$

Twierdzenie. Przy odwzorowaniu izomorficznym

$$g \leftrightarrow g'$$

grupy  $G$  na grupę  $G'$  elementowi zerowemu jednej grupy odpowiada element zerowy drugiej grupy i każdej parze wzajemnie przeciwnych elementów jednej grupy odpowiada para wzajemnie przeciwnych elementów drugiej grupy. W istocie, niech  $g_0$  będzie elementem zerowym grupy  $G$  i niech przy danym izomorfizmie między grupami  $G$  i  $G'$  odpowiada mu element  $g'$  grupy  $G'$ .

Udowodnimy, że  $g'_0$  jest elementem zerowym grupy  $G'$ . Istotnie, ponieważ  $g_0$  jest elementem zerowym grupy  $G$ , więc dla dowolnego elementu  $g$  tej grupy zachodzi

$$g + g_0 = g;$$

na mocy izomorficzności odwzorowania  $g \leftrightarrow g'$  mamy

$$g' + g'_0 = g',$$

skąd wynika, że  $g'_0$  jest elementem zerowym grupy  $G'$ . Niech  $g_1$  i  $g_2$  będzie parą elementów przeciwnych w grupie  $G$ :

$$g_1 + g_2 = g_0$$

(gdzie  $g_0$  jak poprzednio oznacza element zerowy grupy  $G$ ). Stąd

$$g'_1 + g'_2 = g'_0$$

Ponieważ  $g'_0$  jest elementem zerowym grupy  $G'$ , więc  $g'_1$  i  $g'_2$  są wzajemnie przeciwne.

### Ćwiczenia

1. Udowodnić, że grupa składająca się z dwóch elementów  $a_0$  i z tablicą dodawania

	$a_0$	$a_1$
$a_0$	$a_0$	$a_1$
$a_1$	$a_1$	$a_0$

jest izomorficzna z grupą obrotów odcinka (dookoła jego środka).

2. Udowodnić, że wszystkie grupy rzędu 2 są między sobą izomorficzne.

3. Udowodnić, że wszystkie grupy rzędu 3 są między sobą izomorficzne.

**Rozwiązanie.** Niech  $a_0, a_1, a_2$  będą elementami grupy; niech  $a_0$  będzie elementem zerowym. Wobec tego  $a_0 + a_0 = a_0$ ,  $a_0 + a_1 = a_1$ ,  $a_0 + a_2 = a_2$ . Nie może być  $a_1 + a_1 = a_1$ , ponieważ byłoby wtedy  $a_1 = a_0$ . Tak więc  $a_1 + a_1 = a_2$ .

Podobnie  $a_1 + a_2 \neq a_2$  i  $a_1 + a_2 \neq a_1$ . Wobec tego  $a_1 + a_2 = a_0$ . W ten sposób rozumując otrzymamy  $a_2 + a_1 = a_0$ . Wreszcie  $a_2 + a_2 \neq a_2$  (ponieważ w przypadku przeciwnym  $a_2 = a_0$ ) i  $a_2 + a_2 \neq a_0$  (ponieważ  $a_1 + a_2 = a_0$ ). Wobec tego

$$a_2 + a_2 = a_1.$$

Tak więc w grupie rzędu 3 jest możliwa tylko jedna tablica dodawania, a mianowicie:

	$a_0$	$a_1$	$a_2$
$a_0$	$a_0$	$a_1$	$a_2$
$a_1$	$a_1$	$a_2$	$a_0$
$a_2$	$a_2$	$a_0$	$a_1$

4. Udowodnić, że każda grupa abelowa rzędu 4 jest izomorficzna bądź z grupą obrotów kwadratu, bądź z grupą Kleina czwartego rzędu (dwie ostatnie grupy nie są między sobą izomorficzne; dlaczego?).

5. Udowodnić, że grupa wszystkich liczb dodatnich (z arytmetycznym mnożeniem jako operacją grupową) jest izomorficzna z grupą wszystkich liczb (z arytmetycznym dodawaniem jako operacją grupową).

Wskazówka. Odwzorowanie izomorficzne otrzymamy przez logarytmowanie.

### § 3. Twierdzenie Cayleya

Na zakończenie tego rozdziału udowodnimy jeszcze następujące twierdzenie, odkryte przez Cayleya). Twierdzenie. Każda grupa skończona jest izomorficzna z pewną grupą permutacji.

Dowód. Niech  $G$  będzie grupą skończoną,  $n$  - jej rzędem,  $a_1, a_2, \dots, a_n$  - jej elementami, wśród których  $a_1$ , niech będzie elementem zerowym.

Napiszmy dla każdego  $i=1, 2, \dots, n$

$$a_1+a_i, a_2+a_i, \dots, a_n+a_i.$$

Wszystkie te elementy są różne i jest ich  $n$ , czyli są to te same elementy  $a_1, a_2, \dots, a_n$ , tylko zapisane w innym porządku, a mianowicie niech

$$a_1 + a_i = a_{i1}, a_2 + a_i = a_{i2}, \dots, a_n + a_i = a_{in}.$$

Tak więc elementowi  $a_i$  odpowiada permutacja

$$P_i = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 + a_i & a_2 + a_i & \dots & a_n + a_i \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i1} & a_{i2} & \dots & a_{in} \end{pmatrix}$$

lub permutacja

$$P'_i = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i1} & a_{i2} & \dots & a_{in} \end{pmatrix}$$

różniącą się od permutacji  $P_i$  tylko tym, że w permutacji  $P_i$  przestawiamy elementy grupy  $G$ , a w  $P'_i$  - wzajemnie jednoznacznie odpowiadające tym elementom ich numery.

Jeżeli  $i \neq k$ , to  $P_i \neq P_k$ , ponieważ w permutacji  $P_k$  pod elementem  $a_1$ , podpisany jest element  $a_1 + a_k = a_k$ ,  $a_k \neq a_1$ . Tak więc ustaliliśmy wzajemnie jednoznaczność między elementami  $a_1, a_2, \dots, a_n$  grupy  $G$  i permutacjami  $P_1, P_2, \dots, P_n$ .

Teraz należy udowodnić, że po pierwsze, permutacje  $P_1, P_2, \dots, P_n$  tworzą grupę ze względu na działanie zwykłego dodawania permutacji i po drugie, że grupa ta jest izomorficzna z grupą  $G$ .

Zauważmy przede wszystkim:

I. Wśród permutacji  $P_1, P_2, \dots, P_n$  istnieje permutacja tożsamościowa.

W istocie, ponieważ z założenia  $a_1$  jest elementem zerowym grupy  $G$ , permutacja

$$P_1 = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 + a_1 & a_2 + a_1 & \dots & a_n + a_1 \end{pmatrix}$$

jest permutacją tożsamościową. Udowodnimy dalej, że jeżeli  $a_h = a_i + a_k$ , to  $P_h = P_i + P_k$

Zauważmy na wstępie, że

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 + a_k & a_2 + a_k & \dots & a_n + a_k \end{pmatrix}$$

$$\begin{pmatrix} a_1 + a_i & a_2 + a_i & \dots & a_n + a_i \\ a_1 + a_i + a_k & a_2 + a_i + a_k & \dots & a_n + a_i + a_k \end{pmatrix}$$

przedstawiają jedną i tę samą permutację  $P_k$ ; w istocie, oba wzory oznaczają, że każdemu elementowi  $a$  grupy  $G$  przyporządkowany jest element  $a + a_k$  tejże grupy.

Wobec tego możemy napisać

$$P_{ii} = \begin{pmatrix} a_1 + a_i & a_2 + a_i & \dots & a_n + a_i \\ a_1 + a_i + a_k & a_2 + a_i + a_k & \dots & a_n + a_i + a_k \end{pmatrix}$$

Obecnie widzimy, że permutacja

$$P_i + P_k = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 + a_i & a_2 + a_i & \dots & a_n + a_i \end{pmatrix} + \begin{pmatrix} a_1 + a_i & a_2 + a_i & \dots & a_n + a_i \\ a_1 + a_i + a_k & a_2 + a_i + a_k & \dots & a_n + a_i + a_k \end{pmatrix}$$

na podstawie ogólnego określenia dodawania permutacji jest identyczna z permutacją

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 + a_i + a_k & a_2 + a_i + a_k & \dots & a_n + a_i + a_k \end{pmatrix}$$

Ale jeżeli  $a_i + a_k = a_n$ , to

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 + a_i + a_k & a_2 + a_i + a_k & \dots & a_n + a_i + a_k \end{pmatrix} = P_h$$

czyli

$$P_i + P_k = P_h$$

Udowodnione twierdzenie możemy sformułować następująco:

IIa. Suma dwóch elementów grupy  $G$  przyporządkowana jest sumie permutacji odpowiadających ' tym elementom.

Stąd wynika

IIb. Suma dowolnych dwóch sposobów permutacji  $P_1, P_2, \dots, P_n$  jest jedną z permutacji  $P_1, P_2, \dots, P_n$ .

Rozpatrzmy permutację  $P_i$  element  $a_i$  element  $-a_i = a_k$ . Ponieważ  $a_i + a_k = a_1$ , więc na mocy tego, co wyżej udowodniliśmy,  $P_i + P_k = P_1$ ; ale  $P_1$  jest, jak wiadomo, permutacją tożsamościową, dlatego

$$P_k = -P_i$$

Tak więc

III. Permutacja  $-P_i$  dla dowolnego  $i = 1, 2, \dots, n$  jest jedną z permutacji  $P_1, P_2, \dots, P_n$ .

Z IIb, I i III wynika, że zbiór permutacji  $P_1, P_2, \dots, P_n$  tworzy grupę ze względu na zwykłe określenie dodawania permutacji. Z IIa wynika, że grupa ta jest izomorficzna z grupą  $G$ . W ten sposób twierdzenie Cayleya jest udowodnione.

# Rozdział IV

## PODGRUPY CYKLICZNE DANEJ GRUPY

### § 1. Podgrupa generowana przez dany element grupy

Niech  $a$  będzie dowolnym elementem grupy  $G$ . Dodajmy go do samego siebie, tj. utwórzmy element  $a + a$ . Ten element oznaczmy przez  $2a$ . Podkreślamy:  $2a$  jest tylko oznaczeniem elementu  $a + a$ , przy tym nie ma oczywiście mowy o żadnym mnożeniu elementu  $a$  przez  $2$ . W ten sam sposób oznaczmy  $a + a + a$  przez  $3a$ , ogólnie

$$a + a + \dots + a = na.$$

Rozpatrzmy dalej element  $-a$  i oznaczmy kolejno

$$(-a) + (-a) \text{ przez } -2a,$$

$$(-a) + (-a) + (-a) \text{ przez } -3a,$$

.....

$$(-a) + (-a) + \dots + (-a) \text{ przez } -na.$$

Do oznaczeń tych uprawnia nas fakt, że istotnie  $na + (-na) = 0$ . Dla dowodu ostatniego twierdzenia zauważmy przede wszystkim, że w przypadku gdy  $n=1$  jest ono oczywiste (wynika z samego określenia  $-a$ ). Załóżmy, że twierdzenie to jest prawdziwe dla  $n-1$ ; przy tym założeniu udowodnimy jego prawdziwość dla  $n$ . Mamy

$$na + (-na) = [a + (n-1)a] + [-(n-1)a + (-a)] = a + \{(n-1)a + [-(n-1)a]\} + (-a).$$

Ale na mocy naszego założenia wyrażenie w nawiasie klamrowym równa się  $0$ , czyli

$$na + (-na) = a + 0 + (-a) = a + (-a) = 0,$$

czego należało dowieść.

Określiliśmy wyrażenie  $na$  dla dowolnej dodatniej i dla dowolnej ujemnej wartości  $n$ . Przyjmijmy wreszcie, że  $0a = 0$  (gdzie z lewej strony  $0$  oznacza liczbę, a z prawej element zerowy grupy  $G$ ).

Niech teraz  $p$  i  $q$  będą dowolnymi liczbami całkowitymi. Z podanego określenia wynika, że dla dowolnych całkowitych  $p$  i  $q$  zachodzi

$$pa + qa = (p+q)a.$$

Otrzymaliśmy następujący rezultat:

Zbiór  $H(a)$  tych elementów grupy  $G$ , które przy pewnym całkowitym  $n$  mogą być przedstawione w postaci  $na$ , tworzy grupę  $H(a)$  ze względu na to samo działanie dodawania, które przyjęte jest w całej grupie  $G$ .

Istotnie: 1) Suma dwóch elementów należących do  $H(a)$  jest znowu elementem  $H(a)$ ; 2) zero należy do  $H(a)$ ; 3) dla każdego elementu  $ma$  z  $H(a)$  istnieje element  $-ma$ , który także należy do  $H(a)$ .

Tak więc  $H(a)$  jest podgrupą grupy  $G$ . Podgrupa ta nazywa się podgrupą grupy  $G$  generowaną przez element  $a$ .

### § 2. Grupy cykliczne skończone i nieskończone

Określiliśmy grupę  $H(a)$  jako składającą się ze wszystkich tych elementów grupy  $G$ , które mogą być przedstawione w postaci  $ma$ . Nie zastanawialiśmy się przy tym, czy dla dwóch różnych liczb całkowitych  $m_1$  i  $m_2$  elementy  $m_1a$  i  $m_2a$  grupy  $G$  są różne, czy też może się zdarzyć, że  $m_1a = m_2a$ , chociaż  $m_1 \neq m_2$ .

Postaramy się wyjaśnić ten problem.

Przypuśćmy, że istnieją dwie różne liczby całkowite  $m_1$  i  $m_2$ , takie, że  $m_1 a = m_2 a$ . Dodając do obu stron tej równości element  $-m_1 a$  otrzymamy

$$0 = (m_2 - m_1) a.$$

Wobec tego istnieją takie liczby całkowite, że  $ma = 0$ .

Ponieważ z warunku  $ma = 0$  wynika, że  $-ma = 0$ , więc zawsze można założyć, że liczba  $m$  w równości  $ma = 0$  jest dodatnia.

Weźmy teraz najmniejszą liczbę naturalną, spełniającą warunek  $ma = 0$  i oznaczmy ją przez  $\alpha$ . Mamy

$$a \neq 0, \quad 2a \neq 0, \dots, \quad (a-1)a \neq 0, \quad \alpha a = 0$$

Udowodnimy, że elementy

$$(1) \quad 0 = 0\alpha, \quad a, \quad 2a, \dots, \quad (a-1)a$$

są wszystkie różne. W istocie, gdyby było

$$pa = qa \text{ przy } 0 \leq p < q < a - 1,$$

to otrzymalibyśmy, dodając do obu stron ostatniej równości  $pa - qa$ ,

$$(q - p)a = 0,$$

co jest sprzeczne z określeniem liczby  $a$ , ponieważ z naszych warunków wiadomo, że

$$0 < q - p \leq a - 1.$$

Tak więc elementy (1) są wszystkie różne. Udowodnimy, że wyczerpują one grupę  $H(a)$ , tj. że dla dowolnego całkowitego  $m$  mamy

$$ma = ra \text{ dla } 0 \leq r \leq \alpha - 1.$$

W tym celu podzielimy liczbę  $m$  przez liczbę  $\alpha$  (zgodnie z prawami dzielenia liczb całkowitych), a mianowicie przedstawimy ją w postaci

$$(2) \quad m = q\alpha + r,$$

gdzie  $q$  jest ilorazem, a  $r$  - resztą spełniającą warunek

$$0 \leq r < \alpha.$$

Mamy

$$ma = (q\alpha + r)a = q\alpha a + ra,$$

czyli

$$ma = ra.$$

Tak więc, jeżeli istnieją dwie takie liczby  $m_1$  i  $m_2$ , że  $m_1 a = m_2 a$ , to istnieje też taka liczba naturalna  $\alpha$ , że cała grupa  $H(a)$  składa się z  $\alpha$  wzajemnie różnych elementów (1), podczas gdy  $\alpha a = 0$ .

Otrzymujemy następującą sytuację: Szereg

$$\dots, \quad -ma, \quad \dots, \quad -a, \quad 0, \quad a, \quad \dots, \quad ma, \quad \dots$$

jest nieskończonym powtórzeniem (w obie strony - na prawo i na lewo) swojego „odcinka” (1). W istocie,

$$(a+1)a = \alpha a + a = a,$$

$$(a+2)a = \alpha a + 2a = 2a,$$

$$\dots$$

$$(2\alpha - 1)a = \alpha a + (a-1)a = (\alpha - 1)a,$$

$$2\alpha a = 0,$$

$$(2\alpha + 1)a = a \text{ itd.}$$

Analogicznie w lewo

$$-a - \alpha a - a = (a-1)\alpha,$$

$$-2a = \alpha a - 2a = (\alpha - 2)a,$$

$$\dots$$

$$-(a-1)a = \alpha a - (a-1)a = a,$$

$$-\alpha a = 0 \text{ itd.}$$

Aby przekonać się, jaki właściwie element grupy  $H(a)$  otrzymujemy biorąc sumę

$$a+a+\dots+a=ma$$

lub

$$(-a) + (-a) + \dots + (-a) = -ma,$$

należy podzielić  $m$  (lub  $-m$ ) przez  $a$ . Otrzymana z tego dzielenia nieujemna reszta  $r$ ,  $0 \leq r \leq a - 1$  daje nam odpowiedź na nasze pytanie:

$$ma = ra.$$

Stąd także wynika, jak należy dodawać elementy grupy  $H(a)$ :

$$pa + qa = (p + q)a - ra,$$

gdzie  $r$  jest resztą z dzielenia  $p+q$  przez  $a$ .

Rozpatrzmy teraz  $\alpha$ -kąć foremny. Kąć środkowy uparty na boku naszego wielokąta wynosi

$$\varphi = 2\pi / a$$

Wielokąt pozostaje w tym samym położeniu przy obrotach o kąty:  $0$  (obrót tożsamościowy),  $\varphi$ ,  $2\varphi$ , ...,  $(a - 1)\varphi$ . Jeżeli będziemy utożsamiali każde dwa obroty różniące się od siebie o wielokrotność pełnych obrotów; to żadne inne oprócz wymienionych  $a$  obrotów nie będą pozostawiały naszego wielokąta w tym samym położeniu. Przy tym suma obrotu o kąć  $p\varphi$  i obrotu o kąć  $q\varphi$  jest obrotem o kąć  $r\varphi$ , gdzie  $r$  jest resztą z dzielenia  $p+q$  przez  $a$ .

Widzimy więc, że jeżeli obrotowi naszego wielokąta o kąć  $m\varphi$  przyporządkować element  $ma$  grupy  $H(a)$ , to utrzymamy odwzorowanie izomorficzne grupy  $H(a)$  na grupę obrotów foremnego  $\alpha$ -kąćta.

Grupy izomorficzne z grupami obrotów wielokątów foremnymi nazywają się skończonymi grupami cyklicznymi. Tak więc, jeżeli dla pewnych  $m_1$  i  $m_2$  jest  $m_1\alpha = m_2\alpha$ , to grupa  $H(a)$  jest grupą cykliczną. Tablice dodawania dla grup cyklicznych rzędu 3 i 4 wypisane były w rozdz. I, § 1 (pierwszy i trzeci przykład). Tablica dodawania dla grupy cyklicznej rzędu  $m$  ma postać:

	$a_0$	$a_1$	$a_2$	$a_3$	...	$a_{m-1}$
$a_0$	$a_0$	$a_1$	$a_2$	$a_3$	...	$a_{m-1}$
$a_1$	$a_1$	$a_2$	$a_3$	$a_4$	...	$a_0$
$a_2$	$a_2$	$a_3$	$a_4$	$a_5$	...	$a_1$
$a_3$	$a_3$	$a_4$	$a_5$	$a_6$	...	$a_2$
.	.	.	.	.	...	.
.	.	.	.	.	...	.
.	.	.	.	.	...	.
$a_{m-3}$	$a_{m-3}$	$a_{m-2}$	$a_{m-1}$	$a_0$	...	$a_{m-4}$
$a_{m-2}$	$a_{m-2}$	$a_{m-1}$	$a_0$	$a_1$	...	$a_{m-3}$
$a_{m-1}$	$a_{m-1}$	$a_0$	$a_1$	$a_2$	...	$a_{m-2}$

Ta tablica dodawania może służyć jako inne określenie grupy cyklicznej rzędu  $m$ .

Badaliśmy przypadek, gdy dla danego elementu  $a$  grupy  $G$  istnieją takie dwie liczby całkowite  $m_1$  i  $m_2$ , że  $m_1a = m_2a$ .

Rozpatrzmy teraz przypadek, kiedy takich dwóch liczb nie ma, tzn. gdy elementy

$$(3) \dots, -ma, \dots, -2a, -a, 0, a, 2a, \dots, ma, \dots$$

są wszystkie różne. Wówczas elementy (3) znajdują się we wzajemnie jednoznacznej odpowiedniości z liczbami całkowitymi: Elementowi  $ma$  odpowiada liczba całkowita  $m$  i odwrotnie.

Jeśli przy tym

$$m_1a + m_2a = m_3a,$$

to

$$m_1 + m_2 = m_3.$$

Stąd wynika, że nasza wzajemnie jednoznaczna odpowiedniość jest izomorfizmem między podgrupą  $H(a)$  i grupą wszystkich liczb całkowitych.

Grupy izomorficzne z grupą liczb całkowitych nazywają się grupami cyklicznymi nieskończonymi. Dalej, ponieważ dwie grupy  $A$  i  $B$  izomorficzne z jedną i tą samą grupą  $C$  są oczywiście też izomorficzne między sobą więc wszystkie grupy cykliczne nieskończone są między sobą izomorficzne. Z tego samego powodu izomorficzne są między sobą wszystkie skończone grupy cykliczne tego samego rzędu  $m$ .

Podsumujemy rozważanie tego paragrafu.

Twierdzenie. Każdy różny od zera element  $a$  grupy  $G$  generuje skończoną lub nieskończoną grupę cykliczną  $H(a)$ . Rząd grupy  $H(a)$  nazywa się też rzędem elementu  $a$ .

Wreszcie, możemy jeszcze określić grupy cykliczne (skończone i nieskończone) następująco:

Grupą cykliczną nazywamy każdą grupę generowaną przez jeden ze swoich elementów.

### § 3. Układ generatorów

Wróćmy na chwilę myślą do grupy cyklicznej  $H(a)$  generowanej przez element  $a$  grupy  $G$ . Mówimy generowanej przez element  $a$ , w tym sensie, że każdy element tej grupy jest sumą pewnej ilości składników, z których każdy równa się  $a$  albo  $-a$ .

Zamiast mówić, że grupa  $H(a)$  jest generowana przez element  $a$ , mówi się często, że element  $a$  jest elementem tworzącym grupy  $H(a)$ . Nie każda jednak grupa jest grupą cykliczną, nie każda grupa ma tylko jeden element tworzący; grupy niecykliczne mają nie jeden, lecz co najmniej dwa, a czasem i nieskończenie wiele elementów tworzących; pojęciu jednego elementu tworzącego odpowiada w tym przypadku pojęcie układu generatorów.

Określenie. Zbiór  $E$  elementów grupy  $G$  nazywa się układem generatorów tej grupy, jeżeli każdy element grupy  $G$  jest sumą skończonej ilości składników, z których każdy jest albo elementem zbioru  $E$ , albo jest przeciwny do pewnego elementu zbioru  $E$ .

Przykład. Rozpatrzmy płaszczyznę i pewien układ współrzędnych kartezjańskich na tej płaszczyźnie. Oznaczmy przez  $G$  zbiór tych punktów  $P = (x, y)$ , których obie współrzędne  $x$  i  $y$  są liczbami całkowitymi. Przyjmijmy następujące prawo dodawania punktów: Sumą dwóch punktów  $P_1 = (x_1, y_1)$  i  $P_2 = (x_2, y_2)$  nazywamy punkt  $P_3 = (x_3, y_3)$  o współrzędnych  $x_3 = x_1 + x_2$ ,  $y_3 = y_1 + y_2$ . Czytelnik łatwo może się przekonać, że zbiór  $G$  z tak określonym dodawaniem jest grupą abelową (patrz rozdz. I, § 2, IV) i że punkty  $(0, 1)$  i  $(1, 0)$  tworzą układ generatorów tej grupy.

Uwaga. Czytelnik obeznany z pojęciem liczby zespolonej natychmiast zrozumie, że poprzednio zbudowana grupa jest izomorficzna z grupą liczb zespolonych całkowitych (z dodawaniem jako operacją grupową). Przy tym liczbę zespoloną  $x$  i  $y$  nazywamy całkowitą, jeżeli  $x$  i  $y$  są liczbami całkowitymi.

**Ćwiczenie.** Udowodnić, że każdy układ liczb naturalnych, których największy wspólny dzielnik równa się jedności, jest układem generatorów grupy wszystkich liczb całkowitych.

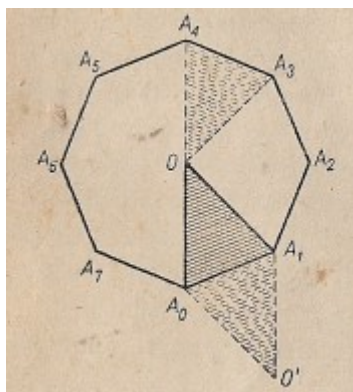
## Rozdział V

### ELEMENTARNE GRUPY RUCHÓW

#### § 1. Przykłady i określenie grup izometrii własnych figur geometrycznych

**1. Ruchy płaskie nie zmieniające danego wielokąta foremnego.** Obszerną i bardzo ważną klasą różnorodnych grup zarówno skończonych, jak i nieskończonych są grupy izometrii własnych figur

geometrycznych. Przez termin izometria własna danej figury geometrycznej  $F$  będziemy rozumieli taki ruch figury  $F$  (na płaszczyźnie lub w przestrzeni), który nie zmienia położenia figury  $F$ . Zaznajomiliśmy się już z elementarnymi grupami izometrii własnych, a mianowicie z grupami obrotów wielokątów foremnych.



Niech dany będzie na płaszczyźnie wielokąt foremny  $A_0A_1 \dots A_n$ , np. ośmiokąt foremny  $A_0A_1A_2A_3A_4A_5A_6A_7$  (wszściek wierzchołki są ponumerowane kolejno w jednym kierunku, np. w kierunku przeciwnym do ruchu wskazówek zegara). Trzeba znaleźć te ruchy wielokąta w jego płaszczyźnie, które pozostawiają go na tym samym miejscu. Przy takim ruchu każdy wierzchołek wielokąta powinien przejść na wierzchołek, każdy bok - na bok, a środek wielokąta musi pozostać bez zmiany. Niech przy pewnym określonym ruchu wierzchołek  $A_0$  przejdzie, przypuśćmy, w wierzchołek  $A_k$  (na rys.  $k = 4$ ); wówczas bok  $A_0A_1$  musi przejść bądź na bok  $A_kA_{k+1}$ , bądź na bok  $A_kA_{k-1}$ . Ale jeżeli bok  $A_0A_1$  przeszedłby na bok  $A_kA_{k-1}$ , to trójkąt  $A_0A_1O$  przeszedłby w trójkąt  $A_kA_{k-1}$

$O$ . Ten ostatni trójkąt można by, poruszając go tylko w jego płaszczyźnie, przeprowadzić w położenie  $A_0A_1O'$  będące zwierciadlanym odbiciem trójkąta  $A_0A_1O$  względem boku  $A_0A_1$ . W rezultacie okazałoby się, że trójkąt  $A_0A_1O$  przeprowadziliśmy ruchem pozostawiającym go w jego płaszczyźnie w jego zwierciadlane odbicie, co jest niemożliwe. Tak więc bok  $A_0A_1$  musi przejść w bok  $A_kA_{k+1}$ . Dokładnie w ten sam sposób przekonamy się, że bok  $A_1A_2$  przechodzi w  $A_{k+1}A_{k+2}$ , bok  $A_2A_3$  przechodzi w  $A_{k+2}A_{k+3}$  itd. Innymi słowy nasz ruch jest obrotem wielokąta w jego płaszczyźnie o kąt  $2k\pi / n$ . Tak więc: Każda izometria własna  $n$ -kąta foremnego w jego płaszczyźnie jest obrotem tego  $n$ -kąta o kąt  $2k\pi / n$ , gdzie  $k$  jest pewną liczbą całkowitą. Wobec tego takich obrotów istnieje  $n$  i obroty te jak wiemy, tworzą grupę.

**2. Symetrie wielokąta foremnego w przestrzeni trójwymiarowej.** W poprzednich rozważaniach istotną rolę odgrywało założenie, że rozpatrujemy tylko izometrię własną wielokąta w jego płaszczyźnie. Jeżeli rozpatrywalibyśmy izometrię własną  $n$ -kąta w przestrzeni, to do wyliczonych obrotów doszłyby jeszcze „odwrócenia” wielokąta, tj. obroty o  $180^\circ$  dookoła jego osi symetrii,  $n$ -kąta foremnego ma  $n$  osi symetrii: w przypadku  $n$  parzystego osiami symetrii jest  $n/2$  prostych, łączących pary przeciwległych wierzchołków wielokąta i  $n/2$  prostych łączących środki jego przeciwległych boków. W przypadku  $n$  nieparzystego osiami symetrii są proste łączące wierzchołki ze środkami przeciwległych boków wielokąta. Dowód tego, że te  $n$  obrotów i  $n$  odwróceń  $n$ -kąta foremnego wyczerpują wszystkie izometrie własne  $n$ -kąta, tj. wszystkie jego ruchy w przestrzeni przeprowadzające go w to samo położenie, wynika z rozważań § 3 tego rozdziału. Polecamy czytelnikowi powrócić do tego problemu po przeczytaniu wymienionego paragrafu i jeszcze raz przemyśleć wszystkie problemy związane z izometriami własnymi wielokątów foremnych.

**3. Ogólne określenie grupy izometrii własnych danej figury w przestrzeni lub na płaszczyźnie.** Niech dana będzie w przestrzeni lub na płaszczyźnie figura  $F$ . Rozpatrzmy wszystkie izometrie własne tej figury, tj. wszystkie ruchy (w przestrzeni lub na płaszczyźnie), nie zmieniające położenia tej figury. Jako sumę  $g_1 + g_2$  dwóch izometrii własnych  $g_1$  i  $g_2$  określimy ruch będący rezultatem kolejnego wykonania najpierw ruchu  $g_1$  potem ruchu  $g_2$ . Oczywiście ruch  $g_1 + g_2$  jest, także izometrią własną figury  $F$ , przy założeniu, że każdy z ruchów  $g_1$  i  $g_2$  oddzielnie jest izometrią własną. Zbiór wszystkich izometrii własnych figury  $F$  z wyżej określoną operacją dodawania tworzy grupę. Istotnie, dodawanie ruchów spełnia postulat łączności, dalej, w zbiorze izometrii własnych istnieje zerowa lub „tożsamościowa” izometria własna, a mianowicie „ruch” pozostawiający w tym samym miejscu każdy punkt figury. Wreszcie dla każdej izometrii własnej  $g$  istnieje przeciwna jej izometria własna  $-g$  (przeprowadzająca każdy punkt z powrotem w położenie wyjściowe, z tego położenia jakie zajął on po izometrii własnej  $g$ ).

## §2. Grupy ruchów prostej, okręgu i płaszczyzny

Grupy izometrii własnych wielokątów foremnych są grupami skończonymi. W tym rozdziale poznamy jeszcze inne skończone grupy izometrii własnych, a mianowicie grupy izometrii własnych pewnych wielościanów. Obecnie jednak podamy kilka przykładów grup izometrii własnych, które są grupami nieskończonymi.

Pierwszy przykład to grupa izometrii własnych prostej i dowolnej, zawierającej tę prostą, płaszczyzny. Ta 1grupa składa się z ruchów polegających na ślizganiu się prostej po sobie, które nazwiemy izometriami własnymi pierwszego rodzaju, i z obrotów prostej w rozważanej płaszczyźnie o kąt  $180^\circ$  dookoła dowolnego z jej punktów; nazwiemy te obroty izometriami własnymi drugiego rodzaju.

(Grupa izometrii własnych prostej nie jest grupą abelową. Aby się o tym przekonać, wystarczy dodać dwie izometrie własne, z których jedna jest pierwszego rodzaju, a druga drugiego rodzaju; rezultat tego dodawania ulega zmianie przy zamianie porządku składników). Oczywiście wszystkie izometrie własne drugiego rodzaju można otrzymać dodając (tj. kolejno wykonując) wszystkie możliwe izometrie własne pierwszego rodzaju (ślizganie prostej po sobie) z dowolnym obrotem o  $180^\circ$  (tj. z obrotem o  $180^\circ$  dookoła jednego dowolnie ustalonego punktu tej prostej).

Ślizgania prostej po sobie stanowią podgrupę grupy wszystkich jej izometrii własnych. Te ślizgania są jedynymi ruchami posuwającymi prostą wzdłuż niej samej. Każdemu takiemu ruchowi odpowiada wzajemnie jednoznacznie pewna liczba rzeczywista wskazująca, o jaką odległość i w jakim z dwóch możliwych kierunków posunęliśmy prostą wzdłuż niej samej. Stąd łatwo wywnioskować, że grupa wszystkich poślizgów prostej jest izomorficzna z grupą liczb rzeczywistych (ze zwykłym dodawaniem jako operacją grupową).

Jako drugi przykład rozpatrzmy grupę wszystkich izometrii własnych okręgu w jego płaszczyźnie. Grupa ta składa się ze wszystkich możliwych obrotów okręgu dookoła jego środka w jego płaszczyźnie, przy czym jak zawsze utożsamiamy każde dwa obroty, różniące się o wielokrotność  $2\pi$ . W ten sposób każdemu elementowi rozważanej grupy odpowiada określony kąt  $\varphi$ . Mierząc ten kąt w mierze łukowej (radialnej) otrzymamy liczbę rzeczywistą  $x$ . Ponieważ jednak kąty różniące się o całkowitą wielokrotność  $2\pi$  przyporządkowane są temu samemu obrotowi okręgu, więc każdemu elementowi grupy obrotów odpowiada nie tylko dana liczba  $x$ , lecz i wszystkie liczby postaci  $x + 2\pi k$ , gdzie  $k$  jest dowolną liczbą całkowitą. Z drugiej strony, każdej liczbie rzeczywistej  $x$  odpowiada jeden dokładnie określony obrót okręgu, a mianowicie obrót o kąt, którego miara łukowa wynosi  $x$ . W ten sposób między obrotem okręgu a liczbami rzeczywistymi ustalona została następująca odpowiedniość: Każdej liczbie rzeczywistej  $x$  odpowiada dokładnie jeden określony obrót, mianowicie obrót o kąt  $x$ . Przy tym jednak każdemu obrotowi przyporządkowana jest nie jedna, lecz nieskończenie wiele liczb rzeczywistych, z których każde dwie różnią się o całkowitą wielokrotność  $2\pi$ .

Grupę obrotów okręgu oznacza się grecką literą  $\chi$  (kappa) od słowa *kyklos* oznaczającego okrąg.

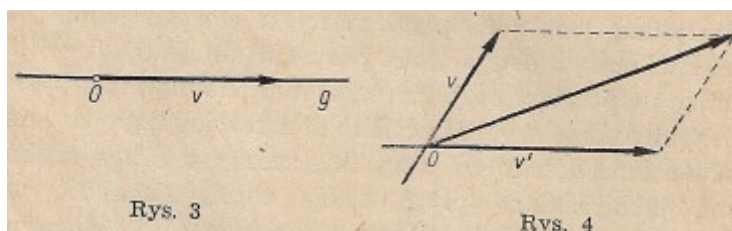
Jako trzeci przykład rozpatrzmy grupę wszystkich ruchów płaszczyzny po sobie. Najprościej rozpatrywać nic jedną, lecz dwie płaszczyzny, z których jedna jest nieruchoma, a druga może poruszać się, jak gdyby ślizgając się po pierwszej. Pierwszą nieruchomą płaszczyznę możemy sobie wyobrazić jako stół rozciągający się nieskończenie daleko we wszystkie strony, a drugą ruchomą jako szklaną płytę, także rozciągającą się we wszystkich kierunkach w nieskończoność i leżącą na tym stole. Idzie więc wobec tego o zbadanie wszystkich możliwych ruchów szklanej płyty po stole, przy których płyta ta cały czas pozostaje na tym stole.

W grupie wszystkich ruchów płaszczyzny po sobie istnieje nieskończenie wiele podgrup. Spośród nich wymienimy przede wszystkim nieskończenie wiele grup obrotów: Zbiór wszystkich obrotów płaszczyzny dookoła dowolnego ustalonego punktu tej płaszczyzny tworzy grupę i każda z tych grup jest, jak łatwo spostrzec, izomorficzna z grupą  $\chi$ ; wszystkie te grupy są wobec tego abelowe.

Obok grup obrotów w grupie wszystkich ruchów płaszczyzny po sobie istnieją podgrupy przesunięć równoległych wzdłuż różnych prostych; jeżeli dana jest prosta  $g$ , to płaszczyznę można przesuwać wzdłuż tej prostej (tak, aby prosta  $g$  a także wszystkie równoległe do niej proste ślizgały się po sobie). Te ślizgania wzdłuż prostej  $g$  możliwe są w dwóch przeciwnych kierunkach i tworzą grupę, która nazywa się grupą przesunięć równoległych płaszczyzny wzdłuż danej prostej. Grupa ta jest

oczywiście podgrupą grupy wszystkich ruchów płaszczyzny po sobie.

Każdy ruch wzdłuż prostej  $g$  można scharakteryzować długością i zwrotem pewnego odcinka  $v$ , odłożonego na



prostej  $g$  od pewnego, raz na zawsze ustalonego punktu  $O$  tej prostej. Jest to ten odcinek  $v$ , o który podczas naszego ruchu przesunął się punkt  $O$ . Stąd natychmiast wynika, że grupa przesunięć równoległych płaszczyzny wzdłuż danej prostej  $g$  jest izomorficzna z grupą wszystkich liczb rzeczywistych (ze zwykłym dodawaniem-jako operacją grupową).

Rozpatrzmy dwa ruchy  $u$  i  $v'$  płaszczyzny wzdłuż dwóch nierównoległych prostych  $g$  i  $g'$ .

Kolejne wykonanie tych dwóch ruchów doprowadza płaszczyznę do tego samego położenia, do jakiego doprowadziłoby ją przesunięcie wzdłuż przekątnej równoległoboku zbudowanego na odcinkach  $u$  i  $v'$  o długość tej przekątnej (zasada równoległoboku lub zasada dodawania wektorów). Tak więc suma dwóch dowolnych przesunięć równoległych jest przesunięciem równoległym, które nie zależy od porządku składników. Stąd wynika, że zbiór wszystkich przesunięć równoległych płaszczyzny wzdłuż wszystkich możliwych prostych tworzy grupę abelową będącą podgrupą grupy wszystkich symetrii płaszczyzny po płaszczyźnie.

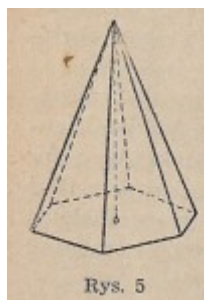
**Ćwiczenia.** 1. Udowodnić, że grupa wszystkich przesunięć równoległych płaszczyzny jest izomorficzna z grupą liczb zespolonych ze zwykłym dodawaniem jako operacją grupową.

2. Udowodnić, że zbiór wszystkich obrotów płaszczyzny w płaszczyźnie (wokół wszystkich możliwych punktów tej płaszczyzny) nie tworzy grupy.

Wszystkie dopiero co rozpatrzone grupy, mianowicie grupy symetrii prostej, okręgu i płaszczyzny mają następującą cechę szczególną: Wszystkie te grupy składają się z ruchów odpowiedniej figury po sobie. Innymi słowy, podczas każdego z tych ruchów cała figura (okrąg, prosta, płaszczyzna) pozostaje cały czas w tym samym położeniu. Taka własność nie jest zachowana przy izometriach własnych wielokątów. Tutaj końcowe położenie poruszanej figury pokrywa się z początkowym, ale położenia pośrednie, które zajmuje figura w czasie ruchu, różnią się od położenia początkowego i końcowego. Ten sam stan rzeczy będzie i przy ruchach wielościanów, do których obecnie przechodzimy.

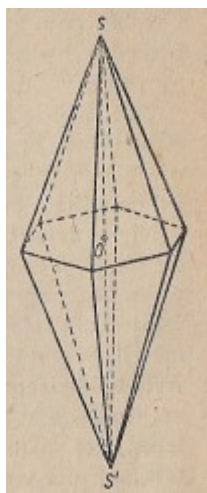
### § 3. Grupy obrotów ostrosłupa foremnego i piramidy podwójnej

**1. Ostrosłup foremny.** Grupa obrotów ostrosłupa foremnego o podstawie  $n$ -kątnej (dookoła jego osi)



jest oczywiście izomorficzna z grupą obrotów  $n$ -kąta foremnego leżącego w podstawie tego ostrosłupa; grupa ta jest zatem grupą cykliczną rzędu  $n$ . Łatwo przekonać się, że obroty ostrosłupa dookoła jego osi (o kąty  $0, 2\pi/n, \dots, (n-1)2\pi/n$ ) wyczerpują zbiór wszystkich izometrii własnych tego ostrosłupa.

**2. Piramida podwójna.** Określimy obecnie grupę izometrii własnych bryły, znanej pod nazwą foremnej piramidy podwójnej  $n$ -kątnej (rys. 6).



Bryła ta składa się z foremego ostrosłupa o podstawie n-kątnej i zwierciadlanego odbicia tego ostrosłupa względem jego podstawy. Udowodnimy, że grupa izometrii własnych piramidy podwójnej składa się z następujących elementów:

1° obrotów wokół osi piramidy (o kąty  $0, 2\pi/n, \dots, (n-1) 2\pi/n$ ;

2° tak zwanych „odwróceń” piramidy, czyli obrotów o kąt  $\pi$  dookoła jakiegokolwiek osi symetrii „podstawy” piramidy, tj. wielokąta foremego będącego wspólną podstawą obu ostrosłupów tworzących piramidę. Takich osi symetrii istnieje (jak widzieliśmy)  $n$ , tak że ruchów drugiego rodzaju istnieje również  $n$ . W ten sposób ilość wszystkich otrzymanych ruchów wynosi  $2n$ . Aby przekonać się, że (z wyjątkiem przypadku  $n = 4$ ) nie istnieją żadne inne ruchy, przeprowadzające n-kątną piramidę podwójną w siebie, zauważmy przede wszystkim, że w przypadku  $n=4$  każda izometria własna rozważanej bryły

powinna bądź pozostawiać w miejscu punkty  $S$  i  $S'$  (symetria własna pierwszego rodzaju), bądź zamieniać je między sobą miejscami (izometria własna drugiego rodzaju). Dalej, podstawa piramidy powinna przy takim ruchu przechodzić w siebie. Zauważmy wreszcie, że suma (tj. kolejne wykonanie) dwóch izometrii własnych pierwszego rodzaju jest izometrią własną pierwszego rodzaju, suma izometrii własnej pierwszego rodzaju i izometrii własnej drugiego rodzaju jest izometrią własną drugiego rodzaju, a suma dwóch izometrii własnych drugiego rodzaju jest izometrią własną pierwszego rodzaju. Przy tym suma dwóch izometrii własnych, z których jedna jest pierwszego rodzaju, a druga drugiego rodzaju, zależy od porządku składników: Jeżeli  $a$  jest izometrią własną pierwszego rodzaju, a  $b$  - izometrią własną drugiego rodzaju, to  $a + b = b - a$ . Rozpatrzmy najpierw izometrie własne pierwszego rodzaju. Przy takiej izometrii własnej podstawa przechodzi na tą samą podstawę pozostając ciągle w tej samej płaszczyźnie; w ten sposób wykonuje ona obrót o jeden z kątów

$$0, 2\pi/n, \dots, (n-1) 2\pi/n$$

i wobec tego cała izometria własna pierwszego rodzaju podwójnej piramidy jest obrotem dookoła jej osi o ten sam kąt. Tak więc izometrii własnych pierwszego rodzaju jest (włączając przekształcenie tożsamościowe) dokładnie  $n$ . Są one po prostu obrotami naszej piramidy wokół jej osi o kąty  $0, 2\pi/n, \dots, (n-1) 2\pi/n$ . Niech dana będzie pewna ustalona izometria własna drugiego rodzaju, tj. takie przekształcenie podwójnej piramidy, przy którym wierzchołki  $S$  i  $S'$  zamieniają się wzajemnie miejscami. Wykonamy teraz, po danej izometrii własnej drugiego rodzaju, pewne określone odwrócenie piramidy, tj. ruch polegający na obrocie naszej bryły o kąt  $\pi$  dookoła pewnej, raz na zawsze ustalonej osi symetrii podstawy. Otrzymamy izometrię własną pierwszego rodzaju, tj. obrót piramidy dookoła jej osi. W ten sposób każda izometria własna drugiego rodzaju przechodzi po wykonaniu pewnego ustalonego odwrócenia w pewną izometrię własną pierwszego rodzaju. Stąd wynika: każdą izometrię własną drugiego rodzaju można otrzymać przeprowadzając (przed lub po pewnej izometrii własnej pierwszego rodzaju) pewne ustalone odwrócenie. Stąd wynika dalej, że ilość izometrii własnych drugiego rodzaju jest równa ilości izometrii własnych pierwszego rodzaju, tj. wynosi  $n$ . Z drugiej strony jest jasne, że wszystkie odwrócenia są izometriami własnymi drugiego rodzaju. Ponieważ tych odwróceń istnieje dokładnie  $n$ , więc wyczerpują one cały zbiór izometrii własnych drugiego rodzaju. Udowodniliśmy zatem co następuje: Grupa izometrii własnych n-kątnej podwójnej piramidy jest grupą nieabelową rzędu  $2n$ , składającą się z  $n$  obrotów dookoła osi piramidy  $SS'$  i z  $n$  odwróceń, tj. obrotów o kąt  $\pi$  i dookoła jednej z  $n$  osi symetrii podstawy piramidy. Wszystkie  $n$  odwróceń otrzymujemy w wyniku dodania jednego z nich do  $n$  obrotów piramidy dookoła osi  $SS'$ . Ponieważ wszystkie obroty naszej podwójnej piramidy otrzymujemy przez kolejne dodawanie do siebie jednego obrotu — mianowicie obrotu o kąt  $2\pi/n$ , więc grupa wszystkich izometrii własnych rozważanej bryły ma układ generatorów, złożony z dwóch elementów: obrotu o kąt  $2\pi/n$  i jednego dowolnego odwrócenia.

Przypadek  $n = 4$  wyłączyliśmy z naszych rozważań dla tego, że przypadkiem szczególnym czworokątnej piramidy podwójnej jest ośmiościan (oktaedr), którego grupa izometrii własnych zawiera nie 8, ale jak zobaczymy niżej 24 elementy. Wynika to stąd, że przy izometriach własnych pewnych czworokątnych piramid podwójnych, a mianowicie ośmiościanów foremnych, wierzchołek  $S$  może przechodzić nie tylko na wierzchołek  $S'$ , ale i na każdy z wierzchołków podstawy. Jeden koniecznych do tego. warunków - jednakowa ilość ścian (i krawędzi) schodzących się w jednym wierzchołku, jest oczywiście spełniony w przypadku dowolnej czworokątnej piramidy podwójnej. W przypadku ośmiościanu foremnego wszystkie kąty - dwuścienne i płaskie - są odpowiednio równe przy dowolnych wierzchołkach, tak samo też jak ściany i krawędzie.

**3.Przypadki zdegenerowane : grupy obrotów odcinka i rombu.** Najmniejszą ilością ścian, jaką może mieć wielokąt, jest 3; w wiadomym sensie jednakże odcinek można rozpatrywać jako przypadek „zdegenerowanego” trójkąta lub, jeśli wygodniej, jako „wielokąt o dwóch wierzchołkach”. Możliwość takiego punktu widzenia potwierdza w szczególności to, że grupa izometrii własnych odcinka w jakiegokolwiek zawierającej go płaszczyźnie jest grupą cykliczną, przy czym rząd jej wynosi 2, Składa się ona oczywiście z przekształcenia tożsamościowego i z obrotu odcinka o kąt  $180^\circ$ .

Podobnie trójkąt równoramienny można rozpatrywać jako przypadek zdegenerowanego ostrosłupa foremnego: Grupa izometrii własnych trójkąta równoramiennego w przestrzeni jest także grupą rzędu 2.

Dalej, zdegenerowaną piramidą podwójną jest oczywiście romb. Grupa izometrii własnych rombu (w przestrzeni) składa się z czterech elementów: przekształcenia tożsamościowego  $a_0$ , obrotów  $a_1$  i  $a_2$  wokół każdej z przekątnych rombu o  $180^\circ$  i z obrotu  $a_3$  dookoła środka rombu o  $180^\circ$  w jego płaszczyźnie (ten obrót jest sumą dwóch poprzednich). Tablica dodawania dla naszej grupy ma postać:

	$a_0$	$a_1$	$a_2$	$a_3$
$a_0$	$a_0$	$a_1$	$a_2$	$a_3$
$a_1$	$a_1$	$a_0$	$a_3$	$a_2$
$a_2$	$a_2$	$a_3$	$a_0$	$a_1$
$a_3$	$a_3$	$a_2$	$a_1$	$a_0$

tj, pokrywa się z tablicą dodawania grupy Kleina rzędu 4, przytoczonej przez nas jako drugi przykład w rozdziale I, § 1, ustęp 3. Można się o tym przekonać bezpośrednio, a jeszcze prościej - rozpatrywać zamiast grupy obrotów rombu izomorficzną jej grupę permutacji z jego czterech wierzchołków  $A, B, C, D$ . Obrotom  $a_0, a_1, a_2, a_3$  odpowiadają oczywiście następujące permutacje wierzchołków ):

$$\left( \begin{matrix} ABCD \\ ABCD \end{matrix} \right), \left( \begin{matrix} ABCD \\ BACD \end{matrix} \right), \left( \begin{matrix} ABCD \\ ABDC \end{matrix} \right), \left( \begin{matrix} ABCD \\ BADC \end{matrix} \right)$$

#### § 4. Grupa izometrii własnych czworościanu foremnego

Dla znalezienia wszystkich izometrii własnych czworościanu  $A_0A_1A_2A_3$  rozpatrzmy początkowo tylko te spośród nich, które pewien ustalony wierzchołek, na przykład wierzchołek  $A_0$ , pozostawiają nieruchomy. Takie izometrie własne pozostawiają trójkąt  $A_1A_2A_3$  w jego pierwotnym położeniu, obracając go dookoła jego środka  $B_0$  o jeden z kątów  $0, 2\pi/3, 4\pi/3$ . Stąd wynika, że izometrii własnych czworościanu  $A_0A_1A_2A_3$ , które pozostawiają wierzchołek  $A_0$  nieruchomy, jest dokładnie 3: przekształcenie tożsamościowe, pozostawiające nieruchome wszystkie elementy czworościanu, i dwa obroty  $a_1$  i  $a_2$  dookoła osi  $A_0B_0$  odpowiednio o kąty  $2\pi/3$  i  $4\pi/3$ . Oznaczmy teraz przez  $x_i$  jakąkolwiek określoną izometrię własną czworościanu przeprowadzającą wierzchołek  $A_0$  w

wierzchołek  $A_i$ ,  $i = 1, 2, 3$ ). Przez  $x_0$  oznaczmy znów przekształcenie tożsamościowe. Udowodnimy, że każdą izometrię własną  $b$  czworościanu można zapisać w postaci

$$(1) \quad b = a_i + x_k,$$

gdzie  $i = 0, 1, 2$  i  $k = 0, 1, 2, 3$  są jednoznacznie określone (tzn. że jeżeli  $b = a_i + x_k$  i  $b' = a_{i'} + x_{k'}$  i zachodzi co najmniej jeden z warunków  $i \neq i'$ ,  $k \neq k'$ , to zachodzi też  $b \neq b'$ ).

Tak więc, niech dana będzie dowolna izometria własna  $b$ ; przeprowadza ona wierzchołek  $A_0$  w pewien określony wierzchołek  $A_k$  gdzie  $k = 0, 1, 2, 3$ . Wówczas jednak izometria własna  $b - x_k$  pozostawia wierzchołek  $A_0$  w miejscu  $i$ , co za tym idzie, jest jedną z izometrii własnych  $a_i$ , tak że  $b - x_k = a_i$  i  $b = a_i + x_k$ , gdzie  $i$  i  $k$  są jednoznacznie określone. Ponieważ i odwrotnie, każdej parze  $(i, k)$  odpowiada na mocy wzoru (1) pewna izometria własna czworościanu, więc istnieje wzajemnie jednoznaczna odpowiedniość między izometriami własnymi czworościanu i wszystkimi parami  $(i, k)$ , gdzie  $i$  przyjmuje wartości  $0, 1, 2$ , a  $k$  - wartości  $0, 1, 2, 3$ . Stąd wynika, że istnieje dokładnie 12 izometrii własnych czworościanu. Każda izometria własna czworościanu wyznacza pewną permutację jego wierzchołków, tj. pewną permutację cyfr  $0, 1, 2, 3$ . Wszystkich jednak permutacji czterech elementów jest 24, z nich tylko 12, jak widzieliśmy, odpowiada przekształceniom czworościanu w przestrzeni. Zbadamy, jakie to permutacje i jakie to symetrie. Rozpatrzmy w tym celu dwa rodzaje osi czworościanu — jedne łączące wierzchołek ze środkiem przeciwległej ściany, a drugie łączące środki dwóch przeciwległych (nie mających wspólnego wierzchołka) krawędzi.

Każdej osi, łączącej wierzchołek ze środkiem przeciwległej ściany odpowiadają dwa nietożsamościowe obroty czworościanu, a mianowicie obroty dookoła tej osi o kąty  $2\pi/3, 4\pi/3$ . Otrzymujemy wobec tego 8 obrotów, które możemy zapisać w postaci permutacji numerów poszczególnych wierzchołków.

$$a_1 = \begin{pmatrix} 0123 \\ 0123 \end{pmatrix}, a_2 = \begin{pmatrix} 0123 \\ 0312 \end{pmatrix}, a_3 = \begin{pmatrix} 0123 \\ 2130 \end{pmatrix},$$

$$(2) a_4 = \begin{pmatrix} 0123 \\ 3102 \end{pmatrix}, a_5 = \begin{pmatrix} 0123 \\ 1320 \end{pmatrix}, a_6 = \begin{pmatrix} 0123 \\ 3021 \end{pmatrix}, a_7 = \begin{pmatrix} 0123 \\ 1203 \end{pmatrix}, a_8 = \begin{pmatrix} 0123 \\ 2013 \end{pmatrix}$$

Dookoła każdej osi łączącej środki dwóch przeciwległych krawędzi mamy jeden nietożsamościowy obrót u kąt  $\pi$ , co daje nam (ponieważ osi tych jest trzy) jeszcze trzy obroty, które możemy zapisać w postaci permutacji

$$(3) a_9 = \begin{pmatrix} 0123 \\ 1032 \end{pmatrix}, a_{10} = \begin{pmatrix} 0123 \\ 2301 \end{pmatrix}, a_{11} = \begin{pmatrix} 0123 \\ 3210 \end{pmatrix}$$

Te jedenaście obrotów wraz z przekształceniem tożsamościowym („obrotom" tożsamościowym)  $a_0$  daje nam 12 izometrii własnych czworościanu. Każda z nich jest obrotem dookoła jednej z siedmiu osi symetrii); dlatego też grupę izometrii własnych czworościanu nazywamy często grupą obrotów czworościanu. Łatwo się przekonać, że wszystkie permutacje (2) i (3) są parzyste, a ponieważ parzystych permutacji z czterech elementów (wierzchołków czworościanu) istnieje 12, więc widzimy, że grupa obrotów czworościanu jest izomorficzna z grupą parzystych permutacji z czterech elementów. Postaramy się teraz zbadać podgrupy grupy obrotów czworościanu. W grupie tej, podobnie jak i w każdej innej, istnieją przede wszystkim dwie tak zwane pod grupy niewłaściwe; jest to po pierwsze cała grupa i po drugie grupa składająca się z jednego tylko elementu zerowego. Nas interesują pozostałe, tak zwane podgrupy właściwe grupy obrotów czworościanu, których istnieje dokładnie osiem. Przede wszystkim zauważmy, że suma obrotów o kąt  $\pi$  dookoła dwóch różnych osi łączących środki przeciwległych krawędzi jest obrotem o kąt  $\pi$  dookoła trzeciej z osi, łączącej środki przeciwległych krawędzi (o tym można się przekonać zarówno za pomocą rozważań geometrycznych, jak i bezpośrednio, przez dodanie do siebie

dowolnych dwóch spośród permutacji (3)). Stąd wynika, że obroty o kąt  $\pi$  dookoła wszystkich trzech osi łączących środki przeciwległych Krawędzi tworzą razem z obrotem tożsamościowym grupę, która jest oczywiście grupą czwartego rzędu; jest ona izomorficzna z grupą Kleina, tj. z grupą wszystkich obrotów rombu. Oznaczmy tę grupę przez  $H$ . Spośród wszystkich podgrup grupy obrotów czworościanu ta grupa ma największy rząd. W niej zawarte są trzy podgrupy drugiego rzędu składające się z obrotów o kąty  $0$  i  $\pi$  dookoła każdej poszczególnej osi łączącej środki przeciwległych krawędzi. Podgrupy te oznaczmy przez  $H_{01}$ ,  $H_{02}$  i  $H_{03}$ . Prócz tych grup istnieją jeszcze cztery podgrupy trzeciego rzędu, a mianowicie grupy  $H_i$ ,  $i = 0, 1, 2, 3$ , składające się z trzech obrotów o kąty  $0, 2\pi/3, 4\pi/3$  dookoła odpowiedniej osi łączącej wierzchołek, oznaczony numerem  $i$ , ze środkiem przeciwległej ściany.

Aby udowodnić, że grupa obrotów czworościanu nie zawiera żadnych innych podgrup, wystarczy pokazać, że dowolne dwa różne od zera elementy wzięte z różnych grup  $H_i$  lub też wzięte jeden z dowolnej grupy  $H_i$  drugi z dowolnej grupy  $H_{0k}$ , tworzą układ generatorów całej grupy obrotów czworościanu. W tym celu wystarczy rozpatrzyć dowolne dwa spośród elementów  $a_1, a_3, a_5, a_7$  na przykład  $a_1$  i  $a_3$ , a także dowolny spośród elementów  $a_1, a_3, a_5, a_7$  i dowolny spośród  $a_9, a_{10}, a_{11}$ . Polecamy czytelnikowi przeprowadzić dowód za pomocą rozważań geometrycznych, a mianowicie wykazać, że każdy obrót czworościanu może być otrzymany za pomocą dodawania elementów dowolnej z wybranych par. Można także otrzymać ten sam rezultat na drodze rachunkowej. Następujące tożsamości pokazują na przykład, że elementy  $a_1$  i  $a_3$  tworzą układ generatorów grupy obrotów czworościanu:

$$\begin{array}{ll} a_0 = a_1 - a_1, & a_7 = a_1 + a_3 - a_1, \\ a_2 = 2a_1, & a_8 = 2a_1 - a_3, \\ a_4 = 2a_3, & a_9 = -a_3 + a_1 + 2a_3 \\ a_5 = -a_3 + a_1 + a_3, & a_{10} = a_1 + a_3 \\ a_6 = -a_3 + 2a_1 + a_3, & a_{11} = a_3 + a_1 \end{array}$$

Nie należy sądzić, że każdy element wyraża się przez generatory jednoznacznie. Na przykład  $a_7 = a_1 + a_3 - a_1$ , i jednocześnie  $a_7 = -a_3 - a_1 + a_3 + a_1 + a_3$ . Grupa obrotów czworościanu nie jest grupą abelową (na przykład  $a_1 + a_3 = a_{10}$ ,  $a_3 + a_1 = a_{11}$ ).

**Ćwiczenie.** Polecamy czytelnikowi udowodnić następująco ogólne twierdzenie: Zbiór  $E$  elementów grupy  $G$  tworzy wtedy i tylko wtedy układ generatorów tej grupy, jeżeli nie istnieje żadna podgrupa właściwa grupy  $G$ , zawierająca wszystkie elementy zbioru  $E$ . Posługując się tym twierdzeniem znaleźć wszystkie układy generatorów grupy obrotów czworościanu, składające się nie więcej niż z trzech elementów. Już z tego przykładu widać, jak wiele różnych układów generatorów może mieć grupa skończona.

## § 5. Grupa obrotów sześciianu i ośmiościanu

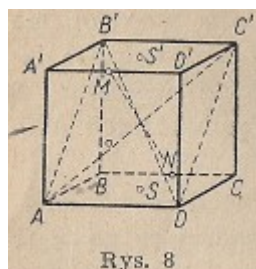
Aby znaleźć wszystkie izometrie własne sześciianu, postąpimy tak samo, jak i w przypadku czworościanu: rozpatrzmy początkowo tylko te izometrie własne sześciianu  $ABCDA'B'C'D'$ , które jeden z wierzchołków — na przykład wierzchołek  $A$  — pozostawiają nieruchomy. Przy każdej izometrii własnej sześciianu wierzchołek przechodzi na wierzchołek, krawędź na krawędź, ściana na ścianę; również i przekątne sześciianu przechodzą na przekątne. Jeżeli dana symetria własna pozostawia wierzchołek  $A$  nieruchomy, to pozostawia ona nieruchomą również i przekątną  $AC'$  (ponieważ istnieje tylko jedna przekątna sześciianu wychodząca z wierzchołka  $A$ ). Zatem rozważana izometria własna jest obrotem sześciianu dookoła przekątnej  $AC'$ . Takich obrotów, oprócz tożsamościowego, istnieje dwa: o kąt  $2\pi/3$  i kąt  $4\pi/3$ . Wobec tego istnieją tylko trzy izometrie własne sześciianu pozostawiające w miejscu wierzchołka  $A$ . Ale wierzchołek  $A$  można przez odpowiednio dobrany obrót przeprowadzić w każdy z ośmiu wierzchołków sześciianu. Stąd, powtarzając te same rozważania co w przypadku czworościanu, łatwo wnioskujemy, że wszystkich izometrii własnych sześciianu istnieje  $3 \cdot 8 = 24$ . Postaramy się znaleźć każdą z tych izometrii

własnych. Zauważmy przede wszystkim, że sześcian ma następujące 13 osi symetrii: 4 przekątne, 3 proste łączące środki dwóch przeciwległych ścian sześcianu i 6 prostych łączących środki dwóch przeciwległych krawędzi sześcianu. Dookoła każdej z przekątnych mamy dwa nietożsamościowe obroty sześcianu, przeprowadzające go w to samo położenie, łącznie zatem mamy 8 obrotów sześcianu dookoła jego przekątnych. Dookoła każdej z osi łączących środki przeciwległych ścian mamy trzy nietożsamościowe obroty, przeprowadzające sześcian w pierwotne położenie; zatem wszystkich obrotów jest 9.

Wreszcie mamy jeden nietożsamościowy obrót (o kąt  $\pi$ ) dookoła każdej z prostych łączących środki przeciwległych krawędzi; razem więc ilość tych obrotów wynosi 6.

Tak więc mamy  $8 + 9 + 6 = 23$  nietożsamościowe obroty, przeprowadzające sześcian w pierwotne położenie. Jeżeli dołączymy do tego jeszcze obrót tożsamościowy, otrzymamy 24 izometrie własne, tj. wszystkie izometrie własne sześcianu, jakie tylko istnieją. W rezultacie:

Obroty sześcianu wokół osi symetrii wyczerpują grupę wszystkich ruchów nie zmieniających położenia tego sześcianu. Dlatego też, podobnie jak i w przypadku czworościanu, grupę izometrii własnych sześcianu nazywamy zazwyczaj grupą obrotów sześcianu. Zanim posuniemy się dalej w badaniu struktury grupy obrotów sześcianu udowodnimy następujący Lemat. Jedynym obrotem sześcianu, który przeprowadza każdą z jego czterech przekątnych w siebie jest obrót tożsamościowy. Istotnie, zauważmy początkowo, że każdy obrót, który nie zmienia położenia dwóch przekątnych sześcianu - przypuśćmy przekątnych  $AC'$  i  $DB'$  — nie zmienia również położenia płaszczyzny przekątnej  $ADC'B'$ .



Rys. 8

Każdy nietożsamościowy obrót, nie zmieniający położenia pewnej płaszczyzny, jest bądź obrotem dookoła pewnej osi leżącej w jej płaszczyźnie - i wówczas jest obrotem o kąt  $\pi$ , bądź też jest obrotem dookoła prostej prostopadłej do tej płaszczyzny. Zauważmy jednak, że obrót płaszczyzny o kąt  $\pi$  wokół osi leżącej w tej płaszczyźnie nie zmienia położenia jedynie tych prostych, które są do tej osi prostopadłe. Ponieważ prostokąt  $ADCB'$  nie jest kwadratem, więc jego przekątne nie są do siebie prostopadłe i nie mogą

pozostać w tym samym położeniu przy żadnym obrocie o kąt  $\pi$  wokół dowolnej osi leżącej w płaszczyźnie tego prostokąta. Tak więc  $AC'$  i  $DB'$  mogą pozostawać w tym samym położeniu jedynie przy obrotach sześcianu dookoła osi prostopadłej do płaszczyzny  $ADC'B'$ . Taką osią jest prosta  $MN$ , łącząca środki ścian  $A'D'$  i  $BC$ . Jedynym nietożsamościowym obrotem sześcianu dookoła osi  $MN$  jest obrót o kąt  $\pi$ , tzn. tylko przy tym obrocie każda z przekątnych  $AC'$  i  $DB'$  nie zmienia swojego położenia. Przy tym obrocie jednak dwie pozostałe przekątne  $BD'$  i  $CA'$  zamieniają się miejscami, tak że nietożsamościowych obrotów, pozostawiających w tym samym położeniu wszystkie cztery przekątne sześcianu w ogóle nie ma. W ten sposób przy każdym nietożsamościowym obrocie sześcianu jego cztery przekątne w pewien sposób zamieniają się ze sobą miejscami, tworząc nietożsamościową permutację. Stąd wynika, że przy dwóch różnych, obrotach  $a$  i  $b$  sześcianu otrzymujemy różne permutacje jego przekątnych; gdybyśmy bowiem przy obrotach  $a$  i  $b$  otrzymywali tę samą permutację przekątnych, to przy obrocie  $a - b$  wszystkie przekątne pozostałyby na miejscu, czyli  $a - b$  byłoby obrotem tożsamościowym i dlatego byłoby  $a = b$ , co, jak założyliśmy, nie zachodzi. Wobec tego wszystkim 24 różnym obrotom sześcianu odpowiadają różne permutacje jego czterech przekątnych, powstałe w wyniku tych obrotów. Wszystkich jednak permutacji z czterech elementów istnieje, jak wiadomo,  $1 \cdot 2 \cdot 3 \cdot 4 = 24$ .

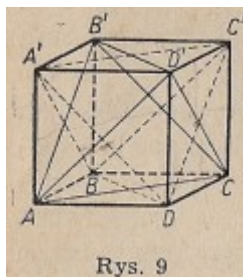
Stąd wynika, że między grupą obrotów sześcianu i grupą wszystkich permutacji czterech elementów da się ustalić odpowiedniość wzajemnie jednoznaczna. Ponieważ przy ustalonej przez nas odpowiedniości sumie obrotów odpowiada oczywiście suma permutacji więc zachodzi następujące twierdzenie:

1. Grupa obrotów sześcianu i grupa wszystkich permutacji czterech elementów są izomorficzne.

Spośród podgrup grupy obrotów sześcianu wymienimy przede wszystkim podgrupy cykliczne drugiego, trzeciego i czwartego rzędu składające się odpowiednio z obrotów dookoła każdej z 13 osi symetrii sześcianu. Podgrup cyklicznych rzędu dwa jest 6 (tyle jest bowiem osi łączących środki

przeciwnych krawędzi), podgrup cyklicznych trzeciego rzędu jest 4 (tyle ile jest przekątnych), podgrup cyklicznych czwartego rzędu jest 3 (tyle, ile jest prostych łączących środki przeciwległych ścian).

Znacznie bardziej interesujące są następujące dalsze podgrupy.



Rys. 9

a) Podgrupa dwunastego rzędu, składająca się z obrotów nie zmieniających położenia (jednocześnie) każdego z dwóch czworokątów  $ACB'D'$  i  $BDA'C'$ , wpisanych w sześcian. Podgrupa ta składa się z  $2 \cdot 4$  nitozsamościowych obrotów dookoła przekątnych, z trzech obrotów o kąt  $\pi$  dookoła osi łączących środki przeciwległych ścian i z obrotu tożsamościowego.

b) Trzy podgrupy ósmego rzędu izomorficzne z grupą i czworokątnej piramidy podwójnej. Każda z tych podgrup składa się z tych obrotów sześcianu, które pozostawiają bez zmiany jedną z prostych łączących środki dwóch przeciwległych ścian, na przykład punkty  $S$  i  $S'$ . Ośmiościan, wpisany w sześcian jest szczególnym przypadkiem czworokątnej piramidy podwójnej; grupa tych jego obrotów, które bądź pozostawiają bez zmiany wierzchołki  $S$  i  $S'$ , bądź też zamieniają je wzajemnie miejscami jest oczywiście grupą izometrii własnych czworokątnej piramidy podwójnej.

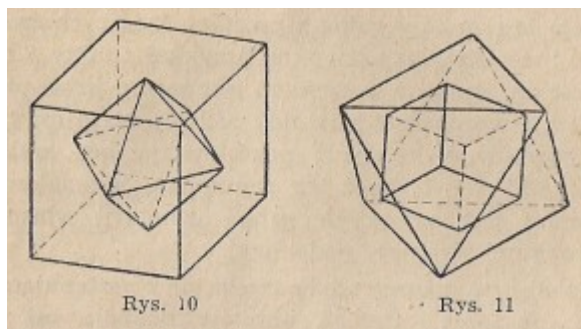
Ta podgrupa ósmego rzędu składa się z następujących ośmiu obrotów: czterech obrotów dookoła osi  $SS'$  (włączając i obrót tożsamościowy), dwóch obrotów o kąt  $\pi$  dookoła osi łączących odpowiednio środki krawędzi  $AA'$  i  $CC'$ ,  $BB'$  i  $DD'$  oraz dwóch obrotów o kąt  $\pi$  dookoła osi łączących odpowiednio środki ścian  $ABB'A'$  i  $CDDC'$ ,  $ADD'A'$  i  $BCC'B'$ .

c) Podgrupa czwartego rzędu składająca się z przekształcenia tożsamościowego i trzech obrotów o kąt  $\pi$  dookoła każdej z osi łączących środki dwóch przeciwległych ścian. Ta grupa składa się z tych obrotów, które wspólne dla wszystkich trzech wymienionych punkcie b) podgrup ósmego rzędu. Ta podgrupa jest abelowa i jest izomorficzna z grupą obrotów rombu (tj grupą Kleina rzędu 4).

Oprócz wymienionych istnieją jeszcze podgrupy czwartego rzędu, także izomorficzne z grupą obrotów rombu.

2. Grupa izometrii własnych (obrotów) ośmiościanu jest izomorficzna z grupą obrotów sześcianu.

Aby się o tym przekonać, wystarczy opisać sześcian na ośmiościanie foremny (rys. 10) lub wpisać sześcian w ośmiościan foremny (rys. 11). Każdy obrót ośmiościanu odpowiada pewnemu obrotowi sześcianu i na odwrót.



Rys. 10

Rys. 11

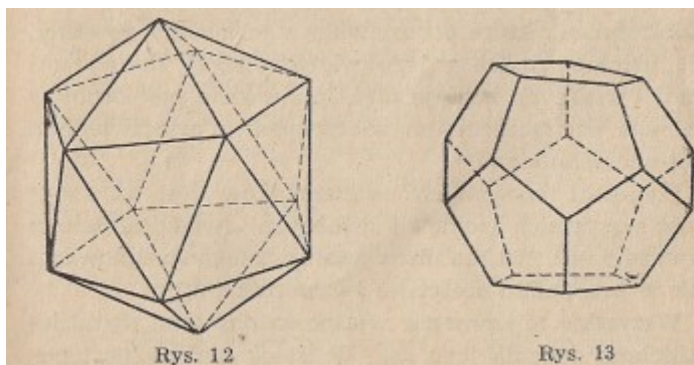
Ta postać rzeczy jest jednym z przejawów dwoistości między sześcianem i ośmiościanem. Określmy, na czym ta dwoistość polega. Przede wszystkim nazwiemy dwa elementy (wierzchołek, krawędź, ścianę) dowolnego wielościanu incydentnymi, jeżeli jeden z tych dwóch elementów należy do drugiego (z kolei jako jego element). W ten sposób ściana i wierzchołek należący do tej ściany, ściana i krawędź tej ściany, a także krawędź i wierzchołek będący końcem tej krawędzi są parami elementów incydentnych. Dwa wielościany nazwiemy dwoistymi, jeżeli elementom jednego z nich można we wzajemnie jednoznaczny sposób przyporządkować elementy drugiego tak, aby param elementów incydentnych jednego wielościanu odpowiadały pary elementów incydentnych drugiego wielościanu i przy tym

- 1° wierzchołkom pierwszego odpowiadały ściany drugiego,
- 2° krawędziom pierwszego odpowiadały krawędzie drugiego,
- 3° ścianom pierwszego odpowiadały wierzchołki drugiego.

Łatwo widzieć, że w tym sensie sześcian i czworościan są wielościanami dwoistymi, a czworościan jest dwoisty względem samego siebie.

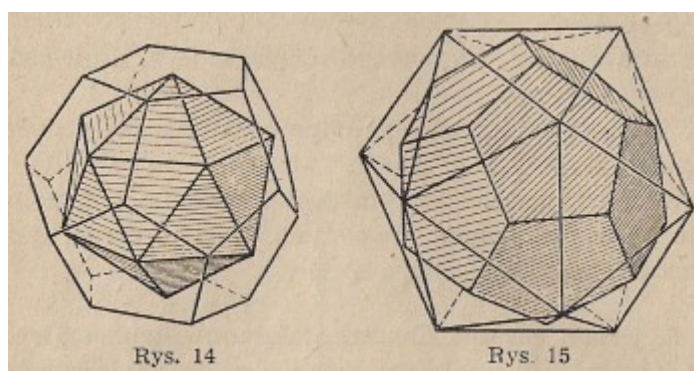
### § 6. Grupa obrotów dwudziestościanu i dwunastościanu). Ogólna uwaga o grupach obrotów wielościanów foremnych

1. Spośród wszystkich pięciu wielościanów foremnych zostały nam do rozpatrzenia dwa: dwudziestościan i dwunastościan (rys. 12 i 13).



Te wielościany są względem siebie dwoiste i grupy ich izometrii własnych są izomorficzne.

Aby się o tym przekonać, wystarczy wpisać dwudziestościan w dwunastościan (rys. 14) lub dwunastościan w dwudziestościan (rys. 15). Wobec tego wystarczy nam



zaznajomić się z grupą izometrii własnych dwudziestościanu. Aby znaleźć ilość jej elementów, postąpimy tak, jak w przypadku czworościanu i sześcianu. Rozpatrzmy mianowicie początkowo tylko te izometrie własne dwudziestościanu, które pozostawiają nieruchomy dowolny, ale ustalony jeden z jego wierzchołków. Takich izometrii własnych istnieje pięć, mianowicie pięć obrotów dookoła osi łączącej ten wierzchołek z przeciwległym mu wierzchołkiem. Ponieważ wszystkich wierzchołków jest 12, więc ilość wszystkich izometrii własnych dwudziestościanu wynosi  $5 \cdot 12 = 60$  (na mocy analogicznego rozumowania jak w przypadku sześcianu i czworościanu).

Wszystkie te izometrie własne są obrotami dwudziestościanu dookoła jego osi. W istocie, mamy następujące osie symetrii dwudziestościanu:

6 osi łączących przeciwległe wierzchołki; dookoła każdej z tych osi mamy 4 nietożsamościowe obroty (o kąty  $2\pi/5$ ,  $4\pi/5$ ,  $6\pi/5$ ,  $8\pi/5$ ) nie zmieniające położenia dwudziestościanu. Łącznie otrzymujemy zatem  $6 \cdot 4 = 24$  obroty.

10 osi łączących środki przeciwległych ścian; dookoła każdej z tych osi mamy 2 nietożsamościowe obroty (o kąt  $2\pi/3$  i  $4\pi/3$ ) nie zmieniające położenia dwudziestościanu. Łącznie zatem 20 obrotów.

15 osi łączących środki przeciwległych krawędzi i dających każda po jednym nietożsamościowym obrocie (u  $180^\circ$ ). Tak więc mamy  $24 + 20 + 15 + 1$  obrót tożsamościowy, łącznie 60 obrotów.

Podobnie jak poprzednio z rozważań tych wynika, że dwudziestościan ma dokładnie 31 osi symetrii. Ponieważ grupa obrotów dwudziestościanu jest dość złożona, nie będziemy prowadzili

dalszego jej badania. Zaznaczymy tylko, że grupa ta jest izomorficzna z grupą parzystych permutacji z pięciu elementów.

2. Grupy izometrii własnych wielokątów i wielomianów, które dotychczas określaliśmy, były zawsze pewnymi grupami obrotów. Rozpatrzmy jak gdyby dwa egzemplarze przestrzeni włożone jeden w drugi. Jedną przestrzeń wyobrazimy sobie w postaci rozciągającego u nieskończenie we wszystkie strony ciała sztywnego i nazwiemy ją „przestrzenią sztywną”. Drugą przestrzeń wyobrazimy sobie jako „przestrzeń pustą”. „Sztywną” przestrzeń umieszczamy w „pustej”, gdzie może się ona przemieszczać. Nasz wielościan wyobrazamy sobie jako część przestrzeni „sztywnej” na stałe z nią związanej i mogącą się poruszać tylko razem z nią. Z tego punktu widzenia można rozpatrywać obroty całej przestrzeni „sztywnej” w przestrzeni „pustej” (wokół pewnych osi), które dany wielościan pozostawiają w tym samym położeniu. Ponieważ każdy ruch, nie zmieniający rozpatrywanych przez nas wielościanów, był obrotem dookoła pewnej osi, a każdy obrót wielościanu dookoła tej osi można uważać za wywołany przez obrót całej przestrzeni dookoła tej osi, więc grupa obrotów danego wielościanu jest izomorficzna z grupą obrotów przestrzeni, które nie zmieniają danego wielościanu. Mówiąc o grupach obrotów wielościanów foremnych mamy zazwyczaj na myśli właśnie tę ostatnią grupę. Często po prostu nazywa się ją także „grupą wielościanu foremnego”. Grupy ostrosłupów foremnych (tj. grupy cykliczne skończone), grupy piramid podwójnych i dopiero co rozpatrywane grupy wielościanów foremnych są jedynymi podgrupami skończonymi grupy wszystkich ruchów przestrzeni.

## Rozdział VI

### PODGRUPY NIEZMIENNICZE

#### § 1. Elementy sprzężone i podgrupy sprzężone

**1. Transformacja danego elementu grupy za pomocą innego elementu.** Rozpatrzmy dwa dowolne elementy  $a$  i  $b$  grupy  $G$ . Element

$$-b + a + b$$

nazywamy transformacją elementu  $a$  za pomocą elementu  $b$ .

Zastanówmy się, przy jakich założeniach zachodzi równość

$$(1) \quad -b + a + b = a.$$

Jeżeli równość ta jest spełniona, to dodając lewostronnie  $b$  do obu jej stron otrzymamy

$$(1') \quad a + b = b + a.$$

Jeżeli spełnione jest (1), to spełnione jest też (1'), tj. elementy  $a$  i  $b$  są przemienne. Na odwrót, jeżeli zachodzi (1'), to

$$-b + a + b = -b + b + a = a,$$

tj. zachodzi też równość (1). Tak więc:

Na to, aby dla danych  $a$  i  $b$  zachodziła równość (1), tj. aby transformacja elementu  $a$  za pomocą elementu  $b$  równała się elementowi  $a$ , potrzeba i wystarcza, ażeby elementy  $a$  i  $b$  były przemienne (spełniały warunek (1')).

W szczególności w grupach abelowych równość (1) zachodzi dla każdego elementu  $a$  i  $b$ .

Jako ilustrację pojęcia transformacji rozpatrzmy grupę  $G$  wszystkich permutacji  $n$  elementów. Niech

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ b_1 & b_2 & b_3 & \dots & b_n \end{pmatrix}$$

Wówczas oczywiście

$$-b = \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix},$$

$$-b+a = \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}$$

$$(2) -b+a+b = \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_n \\ b_{a_1} & b_{a_2} & b_{a_3} & \dots & b_{a_n} \end{pmatrix}$$

Wzór (2) możemy też sformułować w postaci następującej zasady:  
Niech

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ b_1 & b_2 & b_3 & \dots & b_n \end{pmatrix}$$

Aby otrzymać transformację permutacji a za pomocą permutacji b, należy w obu wierszach permutacji a dokonać permutacji b.

Zilustrujemy jeszcze tę zasadę na przykładzie. Niech np.  $n = 3$  i

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Otrzymujemy

$$-b+a+b = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq a$$

Znacznie łatwiej zrozumieć wyjaśnioną zasadę posługując się terminem odwzorowania, czyli funkcji. Permutacja a oznacza funkcję  $y = f(x)$ ,  $x = 1, 2, \dots, n$ ,  $y = 1, 2, \dots, n$ , przy czym dwóm różnym wartościom x zawsze odpowiadają dwie różne wartości y. Permutacja b jest funkcją  $y = \varphi(x)$  o tych samych własnościach co f(x). Permutacja  $-b+a+b$  jest funkcją  $y = F(x)$  określoną wzorem

$$(6) \quad F(x) = \varphi\{f[\varphi^{-1}(x)]\}$$

Wzór ten otrzymujemy, jeżeli elementowi  $\varphi(x)$  przyporządkujemy element  $\varphi[f(x)]$ ; jest to bezpośrednio widoczne, jeżeli we wzorze (3) zamiast x podstawimy  $\varphi(x)$  i zauważymy, że

$$\varphi^{-1}[\varphi(x)] = x$$

Ponieważ gdy x przebiega wartości  $1, 2, 3, \dots, n$ , to  $\varphi(x)$  również przebiega te wartości, tylko w innym porządku, więc wzór

$$(4) \quad F[\varphi(x)] = \varphi[f(x)]$$

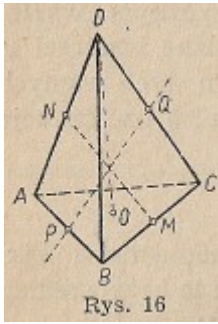
określa nam dokładnie funkcję F(x), tj. permutację  $-b+a+b$ .

Wzór (4) jest tylko inną postacią wzoru (2). Wreszcie, jeżeli oznaczymy f(x) przez y, to otrzymany rezultat można sformułować następująco:

Permutacja F polega na tym, że element  $\varphi(x)$  zastępujemy przez element  $\varphi(y)$ .

Ponieważ każda grupa skończona jest izomorficzna z pewną grupą permutacji, więc wzór (2) wyjaśnia w pewnym sensie użycie terminu „transformacja” w każdym, razie dla grup skończonych.

**2.Przykład grapy czworościanu.** Jako dalszy przykład rozpatrzmy grupę obrotów czworościanu ABCD) (rys. 16).



Niech  $a$  oznacza obrót czworościanu dookoła osi  $MN$  (łączącej środki krawędzi  $BC$  i  $AD$ ) o kąt  $\pi$  niech  $b$  oznacza obrót czworościanu dookoła osi  $DO$  przeprowadzający  $A$  w  $C$ ,  $B$  w  $A$  i  $C$  w  $B$ . Wówczas  $-b + a + b$  jest obrotem o kąt  $\pi$  dookoła osi  $PQ$  łączącej środki krawędzi  $AB$  i  $CD$ , O tym można się przekonać zarówno bezpośrednio, jak i zauważywszy, że obrót  $a$  pociąga za sobą permutację wierzchołków :

$$\begin{pmatrix} ABCD \\ DCBA \end{pmatrix}$$

podczas gdy obrót  $b$  pociąga za sobą permutację wierzchołków

$$\begin{pmatrix} ABCD \\ CABD \end{pmatrix}$$

Jeżeli w wyrażeniu  $\begin{pmatrix} ABCD \\ DCBA \end{pmatrix}$  dokonamy w każdym wierszu permutacji  $\begin{pmatrix} ABCD \\ CABD \end{pmatrix}$

to otrzymamy permutację  $\begin{pmatrix} CABD \\ DBAC \end{pmatrix}$ , czyli  $\begin{pmatrix} ABCD \\ BADC \end{pmatrix}$

odpowiadającą obrotowi dookoła osi  $PQ$  o kąt  $180^\circ$ .

W ten sam sposób przekonamy się, że

$$-a+b+a$$

jest obrotem przeprowadzającym  $B$  w  $C$ ,  $C$  w  $D$ ,  $D$  w  $B$  dookoła osi łączącej wierzchołek

ze środkiem ściany  $BCD$  (temu obrotowi odpowiada permutacja  $\begin{pmatrix} ABCD \\ ACDB \end{pmatrix}$ )

**3.Elementy sprzężone.** Niech  $G$  będzie dowolną grupą.

**TWIERDZENIE I'.** Jeżeli element  $b$  jest transformacją elementu  $a$  za pomocą elementu  $c$ , to element  $a$  jest transformacją elementu  $b$  za pomocą elementu  $-c$ .

Istotnie, z warunku

$$b = -c+a+c$$

wynika (dodając do obu części lewostronnie  $c$ , a prawostronnie  $-c$ )

$$c + b + (-c) = a,$$

to znaczy

$$a = -(-c)+b + (-c),$$

czego należało dowieść.

**Określenie.** Dwa elementy grupy nazywają się elementami sprzężonymi, jeżeli jeden z nich jest transformacją drugiego.

**TWIERDZENIE I''.** Jeżeli  $a$  jest sprzężone z  $b$  i  $b$  jest sprzężone z  $c$ , to  $a$  jest sprzężone z  $c$ .

Istotnie, ponieważ  $a$  jest sprzężone z  $b$ , więc istnieje taki element  $d$ , że

$$(5) \quad b = -d + a + d.$$

Ponieważ  $b$  jest sprzężone z  $c$ , więc istnieje taki element  $e$ , że

$$(5') \quad b = -e + c + e,$$

tak, że

$$-d+a+d = -e+c+e.$$

Dodając do obu części ostatniej równości lewostronnie  $d$  i prawostronnie  $-d$  otrzymamy

$$a=(d - e) + c + (e - d) = -(e - d)+c + (e - d),$$

tzn.  $a$  jest transformacją elementu  $c$  za pomocą elementu  $e - d$ , co należało okazać.

**Twierdzenie I'''.** Każdy element jest sprzężony sam z sobą.

Istotnie,

$$a = -0 + a + 0..$$

Sens twierdzeń I', I'' i I''' polega na tym, że mówią one, iż relacja sprzężenia dwóch elementów grupy jest zwrotna, symetryczna i przechodnia. Stąd na podstawie twierdzenia III wynika

Twierdzenie 1. Każda grupa  $G$  rozpada się na klasy elementów wzajemnie sprzężonych.

Przy tym klasa dowolnego elementu  $a$  grupy  $G$  składa się ze wszystkich elementów grupy  $G$  sprzężonych z  $a$ , tzn. ze wszystkich transformacji elementu  $a$  za pomocą elementu grupy  $G$ .

Zauważmy, że klasa elementu zerowego każdej grupy  $G$  składa się z jednego tylko elementu zerowego (ponieważ przy dowolnym  $a$  mamy  $-a + 0 + a = 0$ ).

**Ćwiczenie.** Udowodnić, że grupa obrotów czworościanu rozpada się na następujące klasy elementów sprzężonych:

1. klasę składającą się z samego elementu zerowego;

2. klasę składającą się z obrotów o kąt  $2\pi/3$  wokół każdej z czterech osi łączących wierzchołek czworościanu ze środkiem przeciwległej ściany;

3. klasę składającą się z czterech obrotów o kąt  $4\pi/3$  dookoła tych samych osi (zawsze zgodnie (lub przeciwnie) do ruchu wskazówek zegara, jeżeli patrzeć z nieruchomego wierzchołka),

4. klasę składającą się z obrotów o kąt  $\pi$  wokół każdej z trzech osi łączących środki dwóch przeciwległych krawędzi czworościanu.

Polecamy również czytelnikowi znalezienie klas elementów sprzężonych w innych grupach obrotów.

**4. Transformacja podgrupy.** Klasa elementów sprzężonych, do której należy dany element  $a$  grupy  $G$ , składa się z transformacji elementu  $a$  za pomocą wszystkich możliwych elementów  $b$  grupy  $G$ . Weźmiemy teraz pod uwagę dowolną podgrupę  $H$  grupy  $G$  i będziemy rozpatrywali transformacje wszystkich możliwych elementów  $x$  tej podgrupy za pomocą jednego dowolnego, ale ustalonego elementu  $b$  grupy  $G$ .

Otrzymałyśmy zbiór elementów, tj. zbiór wszystkich elementów postaci

$$-b+x+b,$$

gdzie  $b$  jest wybranym przez nas ustalonym elementem grupy  $G$ , a  $x$  przebiega zbiór wszystkich elementów podgrupy  $H$ , nazywamy transformacją podgrupy  $H$  za pomocą elementu  $b$  i oznaczamy przez

$$-b+H+b.$$

Udowodnimy, że  $-b + H + b$  jest grupą.

1. Niech elementy  $c_1$  i  $c_2$  należą do  $-b + H + b$ . Udowodnimy, że  $c_1 + c_2$  należy do  $-b + H + b$ . Mamy

$$(6) \quad c_1 = -b+x_1+b, \quad c_2 = -b+x_2+b$$

gdzie  $x_1$  i  $x_2$  są elementami grupy  $H$ . Z równości (6) wynika bezpośrednio

$$(7) \quad c_1 + c_2 = -b+x_1+x_2+b;$$

tak więc  $c_1 + c_2$ , jest transformacją elementu  $x_1 + x_2$  za pomocą  $b$ , a wobec tego  $c_1 + c_2$  należy do  $-b + H + b$ .

2. Udowodnimy, że element zerowy  $0$  grupy  $G$  należy do  $-b + H + b$ . Istotnie,  $0$  należy do  $H$ , a ponieważ

$$-b + 0 + b = 0,$$

więc należy  $-b+H+b$

3. Wreszcie, jeżeli  $a$  należy do  $-b + H + b$ , to  $-a$  należy do  $-b + H + b$ . W istocie, jeżeli  $a$  należy do  $-b + H + b$ , to  $a = -b+x+b$ , gdzie  $x$  jest pewnym elementem  $H$ . Ale wówczas  $-a = -(-b+x+b) = -b + (-x) + b$ , tj.  $-a$  jest transformacją elementu  $-x$  grupy  $H$  za pomocą elementu  $b$ , wobec czego  $-a$  jest elementem zbioru  $-b + H + b$ .

Tak więc  $-b + H + b$  jest grupą.

Każdemu elementowi  $x$  grupy  $H$  odpowiada ściśle określony element grupy  $-b + H + b$ , mianowicie element  $-b+x+b$  grupy  $-b + H + b$ . Przy tym dwu różnym elementom  $x_1$ , i  $x_2$  odpowiadają różne elementy  $-b+x_1+b$  i  $-b+x_2+b$ , ponieważ jeżeli  $x_1$  i  $x_2$  są różne, to na mocy jednoznaczności odejmowania różne są też elementy  $x_1+b$  i  $x_2+b$  są różne, to elementy  $-b + (x_1+b)$  i  $-b + (x_2+b)$

także są różne. Tak więc przyporządkowując elementowi  $x$  grupy  $H$  element  $-b+x+b$  grupy  $-b+H+b$  otrzymamy wzajemnie jednoznaczność między  $H$  i  $-b+H+b$ . Na mocy wzorów (6) i (7) sumie dwóch elementów  $x_1$  i  $x_2$  odpowiada przy tym suma elementów  $-(b+x_1+b)$  i  $(-b+x_2+b)$ , tj. odpowiedniość ta jest izomorfizmem między grupami  $H$  i  $-b+H+b$ .

Udowodniliśmy więc następujące

**Twierdzenie 2.** Transformacja podgrupy  $H$  grupy  $G$  za pomocą elementu  $b$  grupy  $G$  jest podgrupą grupy  $G$ , izomorficzną z grupą  $H$ .

Uwaga. Z określeń powyższych wynikają natychmiast następujące wnioski:

1. Jeżeli  $G$  jest grupą abelową, a  $H$  - jej podgrupą, to transformacja podgrupy  $H$  za pomocą dowolnego elementu  $b$  grupy  $G$  jest po prostu grupą  $H$  (w tym przypadku bowiem transformacja dowolnego elementu  $x$  za pomocą elementu  $b$  jest tym samym elementem  $x$ ;

$-b+x+b = x$ ).

2. Jeżeli  $G$  jest dowolną grupą,  $H$  - jej podgrupą, a  $b$  elementem grupy  $H$ , to

$$-b+H+b = H,$$

ponieważ dla dowolnego elementu  $x$  grupy  $H$ , jeżeli  $b$  należy do  $H$ , to element  $-b+x+b$  także należy do  $H$ . Jeżeli podgrupa  $H_2$  jest transformacją podgrupy  $H$ , za pomocą elementu  $b$ , to  $H_2$  jest transformacją podgrupy  $H_2$  za pomocą elementu  $-b$ .

Dowód wynika bezpośrednio z twierdzenia 1' ustępu 3.

**Określenie.** Dwie podgrupy  $G$ , z których jedna jest transformacją drugiej nazywamy podgrupami sprzężonymi.

Ponieważ  $-0+H+0 = H$ , więc każda grupa jest sprzężona sama z sobą.

Z twierdzenia 2 ustępu 4 wynika, że dwie podgrupy sprzężone z trzecią są też sprzężone między sobą; zbiór wszystkich podgrup grupy  $G$  rozpada się więc na klasy podgrup sprzężonych między sobą. Wiemy już (twierdzenie 2 tego ustępu), że wszystkie sprzężone podgrupy są izomorficzne.

**5. Przykłady.** Widzieliśmy, że w grupie obrotów czworościanu istnieją następujące podgrupy:

1. Dwie podgrupy niewłaściwe: pierwsza składająca się tylko z elementu zerowego, a druga składająca się ze wszystkich dwunastu obrotów czworościanu. Każda z tych podgrup jest oczywiście sprzężona tylko sama ze sobą.

2. Trzy podgrupy drugiego rzędu:  $H_{01}, H_{02}$  i  $H_{03}$ , z których każda składa się z obrotów o kąty  $0$  i  $\pi$  dookoła pewnej osi łączącej środki przeciwległych krawędzi. Wszystkie te grupy tworzą jedną klasę podgrup sprzężonych:

3. Grupa  $H$  czwartego rzędu (Kleina) będąca sumą (w sensie teorii mnogości)  $H_{01}, H_{02}$  i  $H_{03}$  (tj. składająca się z obrotu tożsamościowego i z obrotów o kąt  $\pi$  wokół każdej z trzech osi łączących środki przeciwległych krawędzi). Z określenia grupy  $H$  jako sumy grup  $H_{01}, H_{02}$  i  $H_{03}$  i z tego, że grupy  $H_{01}, H_{02}$  i  $H_{03}$  tworzą jedną klasę podgrup sprzężonych wynika, że grupa  $H$  jest sprzężona sama ze sobą.

4. Cztery podgrupy trzeciego rzędu:  $H_0, H_1, H_2, H_3$ ; każda z nich składa się z obrotów o kąty  $0, 2\pi/3, 4\pi/3$  dookoła pewnej osi łączącej wierzchołek ze środkiem przeciwległej ściany. Wszystkie te grupy także tworzą jedną klasę podgrup sprzężonych.

Tak więc wszystkie dziesięć podgrup grupy obrotów czworościanu foremego rozpadły się na następujące klasy podgrup sprzężonych:

1° Trzy klasy składające się każda z jednego elementu: dwie klasy zawierające po jednej tylko niewłaściwej podgrupie i klasa składająca się z jednej grupy  $H$  rzędu czwartego.

2° Klasa składająca się z trzech podgrup rzędu drugiego.

3° Klasa składająca się z czterech podgrup rzędu trzeciego.

## § 2. Podgrupy niezmiennicze (dzielniki normalne)

**1. Określenie.** Jeżeli podgrupa  $H$  danej grupy  $G$  nie ma żadnej od siebie sprzężonej z nią podgrupy (tj. jeżeli klasa wszystkich podgrup, sprzężonych w grupie  $G$  z podgrupą  $H$  składa się z jednej tylko grupy  $H$ ) to podgrupę  $H$  nazywamy podgrupą niezmienniczą (lub dzielnikiem normalnym) grupy  $G$ .

Oczywiście, określenie podgrupy niezmienniczej można też sformułować następująco:

Podgrupę  $H$  grupy  $G$  nazywamy podgrupą niezmienniczą, jeżeli transformacja dowolnego elementu grupy  $H$  za pomocą dowolnego elementu grupy  $G$  jest elementem grupy  $H$ .

Pojęcie podgrupy niezmienniczej jest jednym z ważniejszych pojęć całej algebry; jeżeli nawet nie jest możliwe w tym krótkim wykładzie wyjaśnić czytelnikowi całej doniosłości tego pojęcia, wychodzącej na jaw w algebrze; szczególnie w tzw. teorii Galois, to w każdym razie można mieć nadzieję, że z rozważań tego i następnego rozdziału czytelnik zrozumie, jak wielkie jest znaczenie podgrup niezmienniczych w logicznej budowie samej teorii grup.

**2.Przykłady.** Trywialnymi przykładami podgrup niezmienniczych są obie podgrupy niewłaściwe dowolnej grupy. Prócz tego dowolna podgrupa grupy abelowej jest oczywiście niezmienniczą. Podamy teraz kilka przykładów mniej trywialnych:

1. Grupa ślizgania prostej po sobie jest podgrupą niezmienniczą grupy wszystkich izometrii własnych prostej (rozdz. V, § 2).

2. Cykliczna grupa  $A$  rzędu  $n$  składająca się ze wszystkich izometrii własnych pierwszego rodzaju  $n$ -kątnej piramidy podwójnej jest podgrupą niezmienniczą grupy wszystkich izometrii własnych tej bryły.

3. Naprzemienna grupa  $A_n$  permutacji z  $n$  elementów (grupa permutacji parzystych z  $n$  elementów) i jest podgrupą niezmienniczą grupy  $S_n$  wszystkich permutacji z  $n$  elementów. Istotnie, jeżeli  $b$  jest dowolnym elementem grupy  $A_n$ , czyli dowolną permutacją parzystą, a zaś jest dowolnym elementem grupy  $S_n$  (tj. dowolną permutacją, parzystą lub nie), to permutacją  $-a+b+a$  ma jako znak iloczyn trzech liczb równych  $+1$  lub  $-1$ :

$$\text{sgn}(-a) \text{sgn} b \text{sgn} a .$$

Ponieważ  $\text{sgn}(-a) = \text{sgn} a$ , więc  $\text{sgn}(a) \text{sgn} a$  w każdym przypadku (tj. dla dowolnego  $a$ ) równa się  $+1$ , a co za tym idzie

$$\text{sgn}(-a + b + a) = \text{sgn} b = +1,$$

a to oznacza, że  $-a + b + a$  jest permutacją parzystą czyli elementem grupy  $A_n$ .

Tak więc transformacja dowolnego elementu  $b$  grupy  $A_n$  jest elementem grupy  $A_n$  (ogólnie biorąc różnym od  $b$ ), tzn.  $A_n$  jest podgrupą niezmienniczą grupy  $S_n$ . Zajmiemy się jeszcze przykładami podgrup niezmienniczych.

Widzieliśmy już, że w grupie obrotów czworościanu istnieje jedna właściwa podgrupa niezmienniczą czwartego rzędu. Ponieważ grupa obrotów czworościanu jest izomorficzna z grupą naprzemienną  $A_4$  (grupą permutacji parzystych czterech elementów), więc możemy też powiedzieć, co następuje: Naprzemienna grupa permutacji z czterech elementów zawiera podgrupę niezmienniczą czwartego rzędu. Ta okoliczność zasługuje na uwagę; okazuje się, że dla  $n > 4$  naprzemienna grupa  $A_n$  permutacji  $n$  elementów nie zawiera żadnej podgrupy niezmienniczej (prócz obu podgrup niewłaściwych). Ten fakt, ma wielkie znaczenie w algebrze: jest ściśle związany z tym, że ogólne równanie stopnia  $n > 4$  nie ma rozwiązań wyrażalnych przez pierwiastki. Grupa obrotów sześciianu jest, jak już wiemy, izomorficzna z grupą  $S_4$ . Wobec tego z góry możemy powiedzieć, że musi ona zawierać podgrupę niezmienniczą izomorficzną z grupą  $A_4$ . Tę podgrupę już znamy (rozdz. V, § 5); składa się ona z obrotów sześciianu pozostawiających w miejscu każdy z dwóch czworościanów wpisanych w sześciian. Wspominaliśmy także o trzech podgrupach ósmego rzędu, zawartych w grupie obrotów sześciianu. Te trzy grupy tworzą klasę podgrup sprzężonych, a co za tym idzie, żadna z nich nie jest podgrupą niezmienniczą. Natomiast podgrupą niezmienniczą jest iloczyn (w sensie teorii mnogości) tych trzech grup, który jak wiemy jest grupą składającą się z elementu zerowego i trzech obrotów sześciianu o kąt  $\pi$  dookoła każdej z trzech prostych łączących środki dwóch przeciwległych ścian.

Żadnych innych właściwych podgrup niezmienniczych, prócz wyżej wymienionych grup dwunastego i czwartego rzędu w grupie obrotów sześciianu, nie ma. Wymienimy jeszcze następujące klasy sprzężonych ze sobą podgrup:

1. Klasa składająca się z trzech grup cyklicznych rzędu 4 (każda z tych grup składa się z obrotów dookoła jednej z osi łączącej środki dwóch przeciwległych ścian sześciianu).

2. Klasa składająca się z czterech grup cyklicznych rzędu 3 (każda z tych grup składa się z obrotów

sześcianu dookoła przekątnej).

3. Klasa składająca się z sześciu grup cyklicznych rzędu 2 (każda z tych grup składa się z obrotów dookoła jednej osi łączącej środki dwóch przeciwległych krawędzi).

Rozpatrzmy wreszcie dokładniej znaną nam już grupę ruchów całej płaszczyzny (rozdz. V, § 2).

Przede wszystkim podamy następującą uwagę. Każdy ruch płaszczyzny przyporządkowuje każdemu punktowi  $x$  płaszczyzny pewien dokładnie określony punkt płaszczyzny  $f(x)$ , mianowicie ten punkt  $f(x)$ , na który przy danym ruchu przechodzi punkt  $x$ .

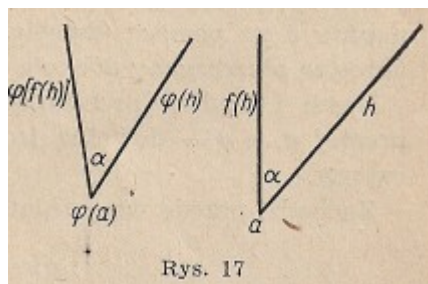
Tak więc każdy ruch możemy rozpatrywać jako pewne przekształcenie płaszczyzny samej na siebie. To przekształcenie jest izometrią, tj. zachowuje odległość między punktami: Jeżeli dwa punkty  $x$  i  $y$  przekształcimy odpowiednio na  $f(x)$  i  $f(y)$ , to odległość między punktami  $f(x)$  i  $f(y)$  jest równa odległości między punktami  $x$  i  $y$ . Stąd w szczególności wynika, że żadne dwa różne punkty nie mogą przy takim przekształceniu przejść na jeden punkt, jeśli bowiem punkty  $x$  i  $y$  są różne, to odległość między nimi jest różna od zera; wówczas jednak odległość między punktami  $f(x)$  i  $f(y)$  także powinna być różna od zera, czyli punkty  $f(x)$  i  $f(y)$  nie mogą się pokrywać. Tak więc każdy ruch płaszczyzny jest przekształceniem wzajemnie jednoznaczny płaszczyzny na siebie.

Rozpatrując izometrie własne jako przekształcenia wzajemnie jednoznaczne płaszczyzny na samą siebie będziemy oznaczali je symbolami odwzorowań  $f(x)$ , gdzie  $x$  jest dowolnym punktem płaszczyzny. Niech dane będą dwa ruchy  $f(x)$  i  $\varphi(x)$ . Postaramy się przedstawić sobie jasno, co oznacza transformacja ruchu  $f(x)$  za pomocą ruchu  $\varphi(x)$ : Według określenia będzie to ruch

$$(1) \quad F(x) = \varphi\{f[\varphi^{-1}(x)]\}.$$

Ponieważ  $\varphi(x)$  jest wzajemnie jednoznaczny odwzorowaniem płaszczyzny, więc ruch  $F(x)$  będzie dokładnie określony, jeżeli będzie wskazane, na jaki punkt przy tym ruchu przejdzie punkt  $\varphi(x)$  dla dowolnego  $x$ . Innymi słowy — przekształcenie  $F(x)$  będzie określone dla dowolnego  $x$ , jeżeli będziemy wiedzieli, także dla dowolnego  $x$ , na co przeprowadza ono punkt  $\varphi(x)$ . Ale zastępując we wzorze (1)  $x$  przez  $\varphi(x)$  i uwzględniając, że  $\varphi^{-1}[\varphi(x)] = x$ , otrzymamy

$$(2) \quad F[\varphi(x)] = \varphi[f(x)]$$



Ten wzór określa dokładnie ruch  $F(x)$ . Jeśli przyjmiemy  $f(x) = y$  to wzór (2) oznacza, co następuje: Dla dowolnego  $x$  ruch  $F$  przeprowadza punkt  $\varphi(x)$  na punkt  $\varphi(y)$ . Udowodnimy teraz następujące twierdzenie:

Jeżeli  $f$  jest obrotem wokół punktu  $a$  o kąt  $\alpha$ , to  $F$  jest obrotem dookoła punktu  $\varphi(a)$  także o kąt  $\alpha$ .

Ponieważ  $f$  jest obrotem dookoła  $a$ , więc

$$f(a) = a,$$

stąd na mocy wzoru (2)

$$F[\varphi(a)] = \varphi(a)$$

czyli  $F$  jest obrotem wokół  $\varphi(a)$ . Ruch  $f$  obraca dowolną półprostą  $h$  wychodzącą z punktu  $a$  o kąt  $\alpha$  i przeprowadza ją tym samym w półprostą  $f(h)$ ; ruch  $\varphi$ , będący izometrią, przeprowadza figurę składającą się z dwóch półprostych  $h$  i  $f(h)$  wychodzących z punktu  $a$  i tworzących ze sobą kąt  $\alpha$  w figurę przystającą, składającą się z dwóch półprostych  $\varphi(h)$  i  $\varphi[f(h)] = F[\varphi(h)]$  wychodzących z  $\varphi(a)$ ; tak więc półprostą  $F[\varphi(h)]$  otrzymujemy z półprostej  $\varphi(h)$  także przez obrót o kąt  $\alpha$ , tj. ruch  $F$

obraca półprostą  $\varphi(h)$  o kąt  $\alpha$  i, co za tym idzie,  $F$  jest obrotem o kąt  $\alpha$ .

Stąd wynika, że:

Transformacja grupy obrotów płaszczyzny wokół punktu  $a$  za pomocą dowolnego ruchu  $\varphi$  jest grupą obrotów płaszczyzny dookoła punktu  $\varphi(a)$ .

Niech  $f$  będzie przesunięciem płaszczyzny wzdłuż prostej  $g$ , a  $\varphi$  - dowolną izometrią własną tej płaszczyzny. Zachodzi przede wszystkim tożsamość

$$f(g) = g,$$

która mówi, że przy ruchu  $\varphi$  prosta  $g$  nie ulega zmianie. Ruch  $\varphi$  przeprowadza prostą  $g$  w prostą  $\varphi(g)$ . Ze wzoru (2) zastosowanego do dowolnego punktu  $x$  prostej  $g$  wynika

$$F[\varphi(g)] = \varphi(g),$$

tj. ruch  $F$  przeprowadza prostą  $\varphi(g)$  na tę samą prostą i, co za tym idzie, jest poślizgiem wzdłuż tej prostej. Ponieważ  $\varphi$  jest izometrią, więc odległość między  $x$  a  $y = f(x)$  jest równa odległości między  $\varphi(x)$  a  $\varphi[f(x)]$ , tj. między  $\varphi(x)$  i  $F[\varphi(x)]$ .

Oznacza to, że poślizg  $F$  przesuwają punkty płaszczyzny o tę samą odległość co poślizg  $f$ . Z tego wynika, że

Grupa przesunięć równoległych płaszczyzny wzdłuż linii prostej  $g$  transformuje się za pomocą dowolnie danej izometrii własnej  $\varphi$  na grupę przesunięć równoległych płaszczyzny wzdłuż prostej  $\varphi(g)$ .

Ponieważ za pomocą dowolnej izometrii własnej  $\varphi$  każde równoległe przesunięcie płaszczyzny transformuje się na przesunięcie równoległe, więc otrzymaliśmy następujący ważny rezultat:

Grupa wszystkich przesunięć równoległych (wzdłuż wszystkich możliwych prostych) jest podgrupą niezmienniczą grupy wszystkich izometrii własnych płaszczyzny.

## Rozdział VII

### ODWZOROWANIA HOMOMORFICZNE

#### § 1. Określenie odwzorowania homomorficznego i jego jądra

**Określenie i elementarne własności.** Niech każdemu elementowi  $a$  grupy  $A$  przyporządkowany będzie element

$$b = f(a)$$

grupy  $B$ . Zbiór wszystkich otrzymanych tym sposobem elementów  $b = f(a)$  grupy  $B$  oznaczymy przez  $f(A)$ . Mn wiemy, że mamy do czynienia z odwzorowaniem grupy  $A$  w grupę  $B$ , a mianowicie na zbiór  $f(A) \subset B$ .

Wprowadzimy teraz następujące podstawowe określenie: Odwzorowanie  $f$  grupy  $A$  w grupę  $B$  nazywa się homomorfizmem, jeżeli dla dowolnych elementów  $a_1$  i  $a_2$  grupy  $A$  zachodzi warunek

$$(1) \quad f(a_1 + a_2) = f(a_1) + f(a_2)$$

przy czym znak  $+$  w lewej części równości (1) należy oczywiście rozumieć jako symbol dodawania w grupie  $A$ , a w prawej części równości (1) jako symbol dodawania w grupie  $B$ .

**Twierdzenie.** Jeżeli  $f$  jest odwzorowaniem homomorficznym grupy  $A$  w grupę  $B$ , to zbiór  $f(A) \subset B$  tworzy podgrupę grupy  $B$ .

**Dowód.** Wystarczy udowodnić, że

1. jeżeli  $b_1$  i  $b_2$ , są elementami zbioru  $f(A)$ , to  $b_1 + b_2$  także jest elementem zbioru  $f(A)$ ;
2. element zerowy grupy  $B$  jest elementem zbioru  $f(A)$
3. jeżeli  $b$  jest elementem zbioru  $f(A)$ , to  $-b$  także jest elementem zbioru  $f(A)$ .

Udowodnimy kolejno punkty 1, 2, 3.

1. Niech  $b_1$  i  $b_2$  będą dwoma elementami zbioru  $f(A)$ . Oznacza to, że istnieją takie elementy  $a_1$  i  $a_2$  grupy  $A$ , że  $f(a_1) = b_1$  i  $f(a_2) = b_2$ .

Ale na mocy tego, że  $f$  jest odwzorowaniem homomorficznym mamy

$$f(a_1 + a_2) = b_1 + b_2.$$

Wobec tego  $b_1 + b_2$  jako obraz elementu  $a_1 + a_2$  przy odwzorowaniu grupy  $A$  jest elementem zbioru  $f(A)$ . W ten sposób udowodniliśmy 1.

2. Niech  $0$  oznacza element zerowy, a  $a$  - dowolny element grupy  $A$ . Mamy (w grupie  $A$ )

$$a+0=a,$$

skąd (w grupie  $B$ )

$$f(a+0) = f(a)$$

i na mocy tego, że  $f$  jest homomorfizmem

$$f(a) + f(0) = f(a),$$

tzn.  $f(0)$  jest elementem zerowym grupy  $B$ . W ten sposób udowodniliśmy 2.

3. Niech  $b$  będzie dowolnym elementem zbioru  $f(A) \subset B$ . Istnieje taki element  $a$  grupy  $A$ , że

$$f(a) = b.$$

Oznaczmy przez  $b'$  element  $f(-a)$  zbioru  $f(A)$ . Udowodnimy, że

$$b' = -b.$$

Istotnie,

$$a+(-a) = 0.$$

Wobec tego

$$f(a)+f(-a)=0$$

( $0$  z prawej strony oznacza element zerowy grupy  $B$ ), to znaczy że

$$b+b' = 0,$$

czyli

$$b' = -b,$$

co należało okazać.

Tak więc każde odwzorowanie homomorficzne grupy  $A$  w grupę  $B$  jest odwzorowaniem homomorficznym grupy  $A$  na pewną podgrupę grupy  $B$ .

Uwaga 1. W tych rozważaniach zawarty jest dowód następujących ważnych twierdzeń, prawdziwych dla dowolnego odwzorowania homomorficznego grupy  $A$  w grupę  $B$ :

$$(2) \quad f(0) = 0$$

(gdzie z lewej strony  $0$  oznacza element zerowy grupy  $A$ , a z prawej — element zerowy grupy  $B$ );

$$(3) \quad f(-a) = -f(a)$$

Uwaga 2. Na podstawie uwagi w rozdziale III § 2, możemy powiedzieć:

Wzajemnie jednoznaczne i homomorficzne odwzorowanie grupy  $A$  w grupę  $B$  jest odwzorowaniem izomorficznym.

Określenie. Niech  $f$  będzie odwzorowaniem homomorficznym grupy  $A$  w grupę  $B$ . Zbiór tych elementów  $x$  grupy  $A$ , które odwzorowanie  $f$  przekształca na element zerowy grupy  $B$  nazywamy jądrem homomorfizmu i oznaczamy przez  $f^{-1}(0)$ .

Twierdzenie. Jądro homomorfizmu  $f$  grupy  $A$  i w grupę  $B$  jest podgrupą niezmienniczą grupy  $A$ .

Dowód. Z określenia homomorfizmu wynika bezpośrednio, że jeżeli

$$f(a_1) = 0, f(a_2) = 0, \text{ to } f(a_1 + a_2) = 0,$$

tj. jeżeli  $a_1$  i  $a_2$  są elementami  $f^{-1}(0)$ , to  $a_1 + a_2$  jest także elementem  $f^{-1}(0)$

Dalej, przy dowodzie poprzedniego twierdzenia widzieliśmy, że  $f(0)$  jest elementem zerowym grupy  $B$ , czyli  $0$  jest elementem  $f^{-1}(0)$

Wreszcie, jeżeli  $f(a) = 0$ , to  $f(-a) = -f(a) = 0$ , tj. jeżeli  $a$  jest elementem  $f^{-1}(0)$ , to  $-a$  jest także elementem  $f^{-1}(0)$ . Stąd już wynika, że  $f^{-1}(0)$  jest podgrupą grupy  $A$ . Aby pokazać, że  $f^{-1}(0)$  jest podgrupą niezmienniczą grupy  $A$ , należy sprawdzić, że transformacja  $-a + x + a$  dowolnego elementu  $x$  grupy  $f^{-1}(0)$  za pomocą dowolnego elementu  $a$  grupy  $A$  jest elementem grupy  $f^{-1}(0)$ . Innymi słowy, należy przekonać się o tym, że

$$f(-a+x+a) = 0,$$

jeżeli tylko  $f(x) = 0$ . Jest to jednak prawie oczywiste, ponieważ dla  $f(x) = 0$  mamy

$$\begin{aligned} f(-a + x + a) &= f(-a) + f(x) + f(a) = \\ &= f(-a) + 0 + f(a) = -f(a) + f(a) = 0. \end{aligned}$$

Tak więc twierdzenie zostało całkowicie udowodnione.

Zobaczymy dalej, że i odwrotnie, każda podgrupa niezmiennicza grupy  $A$  jest jądrem pewnego odwzorowania homomorficznego tej grupy.

## § 2. Przykłady odwzorowań homomorficznych

I. Rozpatrzmy grupę  $G$  wszystkich liczb całkowitych

$$\dots, -n, -(n-1), \dots, -2, -1, 0, 1, 2, \dots, (n-1), n, \dots$$

i grupę  $G_2$  rzędu drugiego. Niech elementami tej grup będą  $b_0$  i  $b_1$ , a tablica dodawania następująca

$$b_0 + b_0 = b_0, b_0 + b_1 = b_1 + b_0 = b_1, b_1 + b_1 = b_0.$$

Oczywiście  $b_0$  jest elementem zerowym grupy  $G_2$ . Określimy następujące odwzorowanie  $f$  grupy  $G$  na grupę  $G_2$ : Każdej liczbie parzystej przyporządkujemy element  $b_0$  grupy  $G_2$ , a każdej liczbie nieparzystej przyporządkujemy element  $b_1$  grupy  $G_2$ .

To przekształcenie jest homomorfizmem. W istocie, niech  $a$  i  $a'$  będą dwiema liczbami całkowitymi.

Jeżeli  $a$  i  $a'$  są obie parzyste, to  $a + a'$  jest także liczbą parzystą

i mamy

$$f(a+a') = f(a) = f(a') = b_0 = f(a) + f(a')$$

Jeżeli jedna z liczb  $a$  i  $a'$  (np.  $a$ ) jest parzysta, a druga nieparzysta, to  $a + a'$  jest nieparzyste, tak że

$$f(a) = b_0, f(a') = b_1, f(a+a') = b_1 = b_0 + b_1 = f(a) + f(a')$$

Jeżeli wreszcie  $a$  i  $a'$  są nieparzyste, to  $a + a'$  jest parzyste i mamy

$$f(a) = f(a') = b_1, f(a + a') = b_0 = b_1 + b_1 = f(a) + f(a')$$

Jądrem naszego homomorfizmu jest oczywiście grupa wszystkich liczb parzystych. Uogólnimy ten przykład. Niech dana będzie dowolna liczba naturalna  $m > 2$ . Rozpatrzmy grupę cykliczną  $G_m$  rzędu  $m$  o elementach  $b_0, b_1, b_2, \dots, b_{m-1}$  i tablicy dodawania:

	$b_0$	$b_1$	$b_2$	$\dots$	$b_{m-2}$	$b_{m-1}$
$b_0$	$b_0$	$b_1$	$b_2$	$\dots$	$b_{m-2}$	$b_{m-1}$
$b_1$	$b_1$	$b_2$	$b_3$	$\dots$	$b_{m-1}$	$b_0$
$b_2$	$b_2$	$b_3$	$b_4$	$\dots$	$b_1$	$b_1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$
$b_{m-2}$	$b_{m-2}$	$b_{m-1}$	$b_0$	$\dots$	$b_{m-4}$	$b_{m-3}$
$b_{m-1}$	$b_{m-1}$	$b_0$	$b_1$	$\dots$	$b_{m-3}$	$b_{m-2}$

(element zerowy oznaczyliśmy przez  $b_0$ ). Określimy homomorfizm  $f$  grupy  $G$  wszystkich liczb całkowitych w grupę  $G_m$ . W tym celu przypomnimy przede wszystkim następujące twierdzenie z arytmetyki:

Każda liczba całkowita daje jako resztę przy dzieleniu przez liczbę naturalną  $m$  jedną z liczb  $0, 1, \dots, m-1$ . Przy tym reszta ta określona jest jako jedyna liczba nieujemna  $r$  spełniająca warunki

$$(1) \quad a = mq + r, \quad 0 \leq r \leq m-1,$$

przy całkowitym  $q$  (które nazywamy ilorazem z dzielenia  $a$  przez  $m$ ).

Twierdzenie to jest oczywiście znane wszystkim dla  $a$  dodatniego. Dla  $a = 0$  mamy oczywiście

$$0 = m \cdot 0 + 0,$$

tj. przy dzieleniu zera przez dowolną liczbę naturalną iloraz i reszta są równe zeru.

Przypadek gdy  $a$  jest ujemne wymaga być może pewnych objaśnień. Jeżeli  $a$  jest ujemne, to  $-a$  jest dodatnie. Podzielimy liczbę naturalną  $-a$  przez liczbę naturalną  $m$ , oznaczmy iloraz przez  $q'$ , a resztę przez  $r'$ . Możemy założyć, że  $r' > 0$  (ponieważ jeżeli byłoby  $r' = 0$ , to  $-a$  i, co za tym idzie,  $a$  byłoby podzielne przez  $m$  bez reszty). Tak więc

$$-a = mq' + r'$$

lub

$$a = -mq' - r' = -m - mq' + m - r = m(-1 - q') + (m - r')$$

Z tegoż, że  $0 < r' \leq m - 1$ , wynika oczywiście, że

$$0 \leq m - r' \leq m - 1.$$

Podstawiając zatem  $q = -1 - q'$ ,  $r = m - r'$  mamy dla całkowitych  $a$ ,  $q$ ,  $r$  związki

$$(2) \quad a = mq + r, \quad 0 \leq r \leq m - 1.$$

Łatwo przekonać się, że przy danych liczbach całkowitych  $m$ ,  $q$  i  $r$ , gdzie  $0 \leq r \leq m - 1$ , przedstawienie liczby całkowitej  $a$  wzorem (2) jest jednoznaczne, tj. że liczby całkowite  $q$  i  $r$  są przez warunki (2) całkowicie określone.

Istotnie, niech

$$(2') \quad a = mq_1 + r_1, \quad 0 \leq r_1 \leq m - 1.$$

Odejmijmy stronami równość (2') od równości (2) Otrzymamy

$$0 = m(q - q_1) + (r - r_1)$$

lub

$$r - r_1 = m(q_1 - q).$$

Stąd wynika, że liczba całkowita  $r - r_1$  jest podzielna bez reszty przez  $m$ . Jednakże  $r - r_1$  jest różnicą dwóch liczb nieujemnych i nie większych od  $m - 1$ , a co za tym idzie wartość bezwzględna tej różnicy także nie przekracza  $m - 1$ . Wobec tego liczba  $r - r_1$  może być podzielna bez reszty przez  $m$  tylko w tym przypadku, gdy równa się ona zero. Tak więc

$$(3) \quad \begin{aligned} r - r_1 &= 0, \quad r = r_1, \\ a &= mq_1 + r. \end{aligned}$$

Z równości (3) i (2) otrzymujemy

$$q_1 = a - r_1 / m, \quad q = a - r / m$$

czyli

$$q_1 = q$$

co należało okazać.

Liczbę całkowitą  $r$  na mocy nierówności

$$0 \leq r \leq m - 1$$

odpowiada element  $b_r$  grupy  $G_m$ . Tak więc przy ustalonym  $m \geq 2$  każdej liczbie całkowitej  $a$  odpowiada dokładnie określony element grupy cyklicznej  $G_m$  rzędu  $m$ , a mianowicie element  $b_r$ , gdzie  $r$  jest resztą z dzielenia  $a$  przez  $m$ . Ten element  $b_r$  nazywa się resztą liczby  $a$  modulo  $m$ . Ta odpowiedniość jest pewnym odwzorowaniem  $f$  grupy  $G$  na grupę  $G_m$ . Udowodnimy, że

odwzorowanie  $f$  jest homomorfizmem.

Niech  $a$  i  $a'$  będą dwiema liczbami

$$(4) \quad \begin{aligned} a &= mq+r & 0 \leq r \leq m-1 \\ a' &= mq'+r' & 0 \leq r' \leq m-1 \end{aligned}$$

Wówczas

$$a + a' = m(q + q') + r + r'.$$

Liczba  $r + r'$  spełnia wprawdzie nierówność  $0 \leq r + r'$  może jednak nie spełniać nierówności  $r + r' \leq m-1$ . Zawsze jednak

$$r+r' = mq'' + \rho$$

gdzie  $q''$  jest ilorazem z dzielenia  $r + r'$  przez  $m$  (jest on równy, jak łatwo się przekonać, 0 lub 1), a  $\rho$  jest resztą z tego dzielenia, tak że

$$a + a' = m(q + q' + a'') + \rho, \quad 0 \leq \rho \leq m-1$$

Tak więc elementowi  $a + a'$  odpowiada przy naszym odwzorowaniu element  $b_\rho$  grupy  $G_m$

Rozpatrując tablicę dodawania grupy cyklicznej rzędu  $m$  widzimy, że

$$b_r + b_{r'} = b_\rho$$

(gdzie  $\rho$  jest, jak poprzednio, resztą z dzielenia  $r + r'$  przez  $m$ ). Tak więc

$$f(a + a') = b_\rho = b_r + b_{r'} = f(a) + f(a'),$$

co dowodzi, że odwzorowanie  $f$  jest homomorfizmem.

To odwzorowanie homomorficzne  $f$  grupy liczb całkowitych na grupę cykliczną rzędu  $m$  jest podstawowym faktem w elementarnej teorii liczb; homomorfizm ten oznaczamy będziemy przez  $f_m$ .

Jądrem homomorfizmu  $f_m$  jest grupa liczb całkowitych podzielnych bez reszty przez  $m$ .

II. Niech  $A$  będzie grupą wszystkich izometrii własnych płaszczyzny. Obierzmy na tej płaszczyźnie określony punkt  $O$  i określony promień  $h$  wychodzący z punktu  $O$ . Każda izometria własna  $f$  płaszczyzny przeprowadza promień  $h$  w promień  $f(h)$  wychodzący z punktu  $f(O)$ . Promień  $f(h)$  tworzy z promieniem  $h$  pewien kąt, który oznaczymy przez  $\omega$ . Kąt ten równa się zeru wtedy i tylko wtedy, gdy promienie  $f(h)$  i  $h$  są równoległe z jednakowym zwrotem, czyli gdy symetria  $f$  jest przesunięciem.

Przyporządkujemy teraz izometrii własnej  $f$  obrót płaszczyzny o kąt  $\omega_f$ . W ten sposób ustalimy odwzorowanie grupy wszystkich izometrii własnych płaszczyzny na grupę wszystkich obrotów płaszczyzny dookoła punktu  $O$  i na izomorficzną z nią grupę  $\chi$  (patrz rozdz. V, § 2).

Odwzorowanie to, jak się czytelnik może łatwo przekonać, jest homomorfizmem. Jądrem tego homomorfizmu jest grupa wszystkich przesunięć równoległych płaszczyzny.

III. W rozdziale V, § 2 (drugi przykład), pokazaliśmy, że każdej liczbie rzeczywistej odpowiada pewien element grupy  $\chi$ . Ta odpowiedniość ustala homomorfizm grupy wszystkich liczb rzeczywistych na grupę  $\chi$ , przy czym jądrem tego homomorfizmu jest grupa cykliczna nieskończona składająca się ze wszystkich liczb rzeczywistych będących wielokrotnościami  $2\pi$ .

## Rozdział VIII

### ROZBICIE GRUPY NA WARSTWY WZGLĘDEM DANEJ PODGRUPY . GRUPA ILORAZOWA

#### § 1. Warstwy lewostronne i prawostronne

**1. Warstwy lewostronne.** Niech dana będzie grupa  $G$  i jej podgrupa  $U$ . Nasze zadanie będzie polegało obecnie na tym, aby udowodnić co następuje: Podanie podgrupy  $U$  określa (i przy tym na ogół dwoma różnymi sposobami) rozbitcie grupy  $G$  na pewien układ wzajemnie rozłącznych podzbiorów, z których jednym jest sama podgrupa  $U$ , a pozostałe za pomocą prostego prawa mogą być we wzajemnie jednoznaczny sposób odwzorowane na  $U$ .

Aby otrzymać ten rozkład grupy  $G$ , postąpimy następująco: Nazwiemy dwa elementy grupy  $G$  równoważnymi względem podgrupy  $U$ , jeżeli lewostronna różnica elementów  $b$  i  $a$ , tzn. element  $-a+b$ , jest elementem podgrupy  $U$ . Ta równoważność (zwana też równoważnością lewostronną) ma własność symetrii, jeżeli bowiem

$$-a+b=u,$$

gdzie  $u$  jest elementem grupy  $U$

Równoważność ta ma także własność przechodniości, jeżeli bowiem

$$-a+b = u_1$$

$$-b+c = u_2,$$

gdzie  $u_1$ , i  $u_2$  są elementami podgrupy  $U$ , to

$$-a+c=(-a+b) + (-b+c) = u_1+u_2$$

jest także elementem podgrupy  $U$ .

Wreszcie, rozpatrywana równoważność ma własność zwrotności ponieważ

$$-a+a=0$$

jest elementem podgrupy  $U$ .

Wobec tego grupa  $G$  na podstawie twierdzenia III Uzupełnienia (§ 5) rozpada się na klasy elementów równoważnych między sobą względem podgrupy  $U$ . Klasy te nazywają się warstwami lewostronnymi grupy  $G$  względem podgrupy  $U$ . Zauważmy, że warstwa lewostronna  $'K_a$  elementu  $a$  grupy  $G$  składa się ze wszystkich takich elementów  $x$ , że  $-a+x = u$  jest elementem grupy  $U$ , tj. innymi słowy ze wszystkich elementów postaci  $x = a + u$ , gdzie  $u$  jest elementem podgrupy  $U$ .

Zauważmy jeszcze, że jeżeli  $a$  jest elementem  $U$  (w szczególności jeżeli  $a = 0$ ), to  $'K_a = U$ , ponieważ w tym przypadku  $a + u$  przy dowolnym  $u$  z grupy  $U$  jest elementem grupy  $U$  i każdy element grupy  $U$  może być przedstawiony w postaci  $a + u$ , gdzie  $u_1 = -a+u$  jest elementem grupy  $U$ . Ponieważ każdy element zbioru  $'K_a$  może być przedstawiony w postaci  $a + u$  i przy różnych elementach  $u_1$  i  $u_2$ , grupy  $U$  elementy  $a + u_1$  i  $a + u_2$  zbioru  $'K_a$  są różne, więc otrzymamy wzajemnie jednoznaczność między  $U$  i dowolnym  $'K_a$ , jeżeli każdemu elementowi  $u$  grup  $U$  przyporządkujemy element  $a + u$  warstwy  $'K_a$ . Zauważmy wreszcie, że wśród wszystkich warstw  $'K_a$  istnieje tylko jedna warstwa będąca podgrupą grupy  $G$  a mianowicie  $U$ . Istotnie, jeżeli  $'K_a$  jest podgrupą, to element zerowy grupy  $G$  powinien należeć do  $'K_a$ ; jest on zatem elementem wspólnym dla warstwy  $'K_a$  i warstwy  $U$ , wobec czego  $'K_a$  pokrywa się z  $U$ .

**2.Przypadek grupy skończonej  $G$ .** Na mocy wzajemnie jednoznacznej odpowiedniości, która istnieje między każdą z warstw  $'K_a$  i podgrupą  $U$ , wszystkie  $'K_a$  - w przypadku gdy grupa  $G$  jest skończona - składają się z jednej i tej samej ilości elementów  $m$ , gdzie  $m$  jest rzędem grupy  $U$ . Jeżeli ilość wszystkich różnych warstw wynosi  $j$ , a  $n$  jest rzędem grupy  $G$  to mamy oczywiście  $n = mj$ . Stąd w szczególności wynika wspomniany już przez nas wcześniej fakt (rozdz. II, § 1), a mianowicie:

Twierdzenie Lagrange'a. Rząd każdej podgrupy grupy skończonej  $G$  jest dzielnikiem rzędu grupy  $G$ . Liczbę  $j$ , tj. ilość warstw lewostronnych grupy  $G$  względem podgrupy  $U$  nazywamy indeksem podgrupa  $U$  w grupie  $G$ .

**3.Warstwy prawostronne.** Nazwiemy dwa elementy  $a$  i  $b$  równoważnymi (równoważność prawostronna) względem podgrupy  $U$ , jeżeli prawostronna różnica  $b - a = b + (-a)$  jest elementem podgrupy  $U$ . Łatwo przekonać się, że własności symetrii, przechodniości i zwrotności dla tej relacji są spełnione. Istotnie, z warunku

$$b - a = u,$$

gdzie  $u$  jest elementem grupy  $U$ , wynika warunek

$$a - b = -(b - a) = -u,$$

a z warunków

$$b - a = u_1, c - b = u_2$$

dla  $u_1$  i  $u_2$  należących do  $U$  wynika warunek

$$c - a = (c - b) + (b - a) = u_2 + u_1.$$

Wreszcie element

$$a - a = 0$$

należy do  $U$ .

Prawostronna równoważność określa rozbitcie grupy  $G$  na warstwy prawostronne, przy czym warstwa prawostronna  $K'_a$  danego elementu  $a$  składa się ze wszystkich takich elementów  $x$ , dla których  $x - a = u$  jest elementem grupy  $U$ , tj. ze wszystkich elementów postaci

$$x - u + a,$$

gdzie  $u$  należy do  $U$ .

Dla  $a$  należącego do  $U$  warstwa  $K'_a$  pokrywa się z  $U$ . Przyporządkowując elementowi  $u$  podgrupy  $U$  elementu  $u+a$  warstwy  $K'_a$  otrzymamy wzajemnie jednoznaczność między  $U$  i dowolną warstwą  $K'_a$ . W przypadku gdy podgrupa  $U$  jest skończona, wszystkie warstwy względem tej podgrupy są skończone i składają się z tej samej ilości elementów co i  $U$ . Jeżeli grupa  $G$  jest skończona i ma rząd  $n$ , a podgrupa  $U$  ma rząd  $m$ , to mamy podobnie jak poprzednio

$$n = mj,$$

gdzie  $j$  oznacza ilość wszystkich różnych warstw prawostronnych względem podgrupy  $U$  i równe jest też ilości wszystkich różnych warstw lewostronnych względem tej podgrupy.

Tak więc indeks podgrupy  $U$  względem grupy  $G$  może być określony zarówno jako ilość lewostronnych jak i ilość prawostronnych warstw grupy  $G$  względem podgrupy  $U$ ; równy jest on ilorazowi rzędu grupy  $G$  i rzędu podgrupy  $U$ .

**4. Pokrywanie się warstw lewostronnych i prawostronnych w przypadku podgrup niezmienniczych.** Zadamy sobie pytanie: W jakim przypadku dla dowolnego  $a$  grupy  $G$  zachodzi

$$K_a = K'_a$$

Na to oczywiście potrzeba i wystarcza, aby każdy element postaci  $a+u$  był równy pewnemu elementowi  $u'+a$  i odwrotnie, każdy element postaci  $u+a$  był równy pewnemu elementowi  $a+u'$  (przy tym zawsze w dalszym ciągu  $u$  i  $u'$  oznaczają będą elementy pod grupy  $U$ ). Oba te warunki są równoważne. Istotnie pierwszy warunek oznacza, że dla każdego  $a$  z grupy  $G$  i  $u$  z grupy  $U$  można dobrać takie  $u'$  z  $U$ , żeby

$$a + u = u' + a,$$

tj. żeby

$$a+u + (-a) = u'$$

lub

$$-(-a) + U + (-a) = U.$$

Ponieważ dowolny element grupy  $G$  może być przy odpowiednim doborze elementu  $a$  przedstawiony w postaci  $-a$ , więc pierwszy warunek oznacza po prostu że transformacja podgrupy  $U$  za pomocą dowolnego elementu grupy  $G$  pokrywa się z  $U$ , czyli  $U$  jest podgrupą niezmienniczą grupy  $G$ . Drugi warunek mówi, że dla każdego  $a$  z  $G$  i  $u$  z  $U$  można wybrać  $u'$  z  $U$  tak, by

$$u + a = a + u',$$

tj

$$-a + u + a = u',$$

czyli

$$-a+U+a = U.$$

W ten sposób drugi warunek także oznacza, że  $U$  powinno być podgrupą niezmienniczą grupy  $G$ . Udowodniliśmy zatem

Twierdzenie. Niech  $U$  będzie podgrupą grupy  $G$ . Na to aby dla każdego elementu  $a$  grupy  $G$  warstwa lewostronna tego elementu względem podgrupy  $U$  pokrywała się z warstwą prawostronną tego elementu względem podgrupy  $U$ , potrzeba i wystarcza, aby  $U$  było podgrupą niezmienniczą grupy  $G$ .

Ponieważ w przypadku gdy  $U$  jest podgrupą niezmienniczą mamy dla dowolnego elementu  $a$  grupy  $G$

$$K_a = K'_a,$$

więc można zamiast  $K_a$  i  $K'_a$  pisać  $K_a = K'_a = K_a$  i zbiór lin nazwać po prostu warstwą elementu  $a$  względem podgrupy niezmienniczej  $U$ . W szczególności pokrywanie się warstw lewostronnych i prawostronnych ma miejsce wtedy, gdy  $U$  jest podgrupą grupy abelowej  $G$ , ponieważ wszystkie podgrupy grupy abelowej są niezmiennicze (rozdz. VI, § 2, ustęp 2).

**5. Przykłady.** 1. Niech  $G$  oznacza grupę wszystkich liczb całkowitych, a  $U \subset G$  niech oznacza grupę wszystkich liczb podzielnych bez reszty przez  $m$ . Jeżeli  $a$  jest dowolną liczbą całkowitą, to  $K_a$  składa się ze wszystkich liczb postaci  $a + mq$ , gdzie  $q$  jest liczbą całkowitą; będą to wszystkie te liczby, które przy dzieleniu przez  $m$  dają tę samą resztę co  $a$ . W ten sposób różnych warstw będzie tyle, ile istnieje różnych reszt przy dzieleniu przez  $m$ ; tych ostatnich będzie  $m$ , ponieważ jako reszty przy dzieleniu przez  $m$  otrzymujemy liczby  $0, 1, 2, \dots, m-1$  i tylko te liczby. Tak więc mamy następujące warstwy:

0° Warstwa wszystkich liczb dających przy dzieleniu przez  $m$  resztę 0. Ta warstwa pokrywa się z grupą  $U$  i składa się z liczb

$$\dots, -qm, -(q-1)m, \dots, -2m, -m, 0, m, 2m, \dots, qm, \dots$$

1° Warstwa wszystkich liczb dających przy dzieleniu przez  $m$  resztę 1. Będą to liczby

$$\dots, -qm+1, -(q-1)m+1, \dots, -3m+1, -2m+1, -m+1, 1, m+1, 2m+1, 3m+1, \dots, qm+1, \dots$$

2° Warstwa wszystkich liczb dających przy dzieleniu przez  $m$  resztę 2. Będą to liczby

$$\dots, -qm+2, -(q-1)m+2, \dots, -3m+2, -2m+2, -m+2, 2, m+2, \dots, qm+2, \dots$$

( $m-1$ )° Warstwa wszystkich liczb dających przy dzieleniu przez  $m$  resztę  $m-1$ . Warstwa ta składa się z liczb

$$\dots, -qm+(m-1), -(q-1)m+(m-1), \dots, -3m+(m-1), -2m+(m-1), -m+(m-1), m-1, m+(m-1), 2m+(m-1), \dots, qm+(m-1), \dots$$

lub, co na jedno wychodzi, z liczb

$$\dots, -2m-1, -m-1, -1, m-1, 2m-1, 3m-1, \dots$$

2. Niech  $G$  oznacza grupę  $S_3$  wszystkich permutacji trzech elementów, a  $U$  - podgrupę rzędu 2 (co za tym idzie, indeksu 3) składającą się z permutacji

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{i} \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Rozkład grupy na warstwy lewostronne i prawostronne przedstawiony jest w następującej tabeli:

Warstwy lewostronne	Warstwy prawostronne
$U = \{P_0, P_2\}$	$U = \{P_0, P_2\}$
$\{P_1, P_3\}$	$\{P_1, P_4\}$
$\{P_4, P_5\}$	$\{P_3, P_5\}$

3. Grupa naprzemienna  $A_n$  permutacji z  $n$  elementów jest podgrupą niezmienniczą indeksu 2 grupy  $S_n$ . Dwie warstwy odpowiadające tej podgrupie, to klasa permutacji parzystych i klasa permutacji

nieparzystych.

4. Grupa  $U$  wszystkich poślizgów prostej po sobie jest podgrupą niezmienniczą o indeksie 2 w grupie  $G$  wszystkich izometrii własnych prostej. Dwie warstwy odpowiadające tej podgrupie są: sama ta podgrupa i klasa wszystkich izometrii własnych drugiego rodzaju.

5. Niech  $G$  oznacza grupę wszystkich liczb zespolonych (ze zwykłym dodawaniem jako operacją grupową). Niech  $U$  oznacza podgrupę wszystkich liczb rzeczywistych. Warstwami, na które rozpada się grupa abelowa  $G$  względem swej podgrupy  $U$ , są zbiory  $K_\beta$  z których każdy składa się ze wszystkich liczb zespolonych postaci

$$x + i\beta,$$

gdzie  $x$  i  $\beta$  są liczbami rzeczywistymi,  $\beta$  jest dane, a  $x$  przebiega wszystkie wartości rzeczywiste. Jeżeli, jak to się zazwyczaj czyni, będziemy interpretowali liczby zespolone jako punkty płaszczyzny, to każda z warstw będzie prostą równoległą do osi rzeczywistej (tj. osi odciętych).

### § 1. Grupa ilorazowa względem danej podgrupy niezmienniczej

**1. Określenie.** Niech  $U$  będzie podgrupą niezmienniczą pewnej danej grupy  $G$ . Rozpatrzmy zbiór tych warstw, na które rozpada się grupa  $G$  względem  $U$ . Oznaczmy ten zbiór przez  $V$  i pokażemy, że można w nim określić operację dodawania tak, aby  $V$  stało się grupą, na którą da się odwzorować homomorficznie grupę  $G$ . Niech  $v_1$  i  $v_2$  będą dwoma dowolnymi elementami zbioru  $V$ ; znaczy to, że  $v_1$  i  $v_2$  są dwiema warstwami grupy  $G$  względem podgrupy niezmienniczej  $U$ . Wybieramy z każdej z tych warstw po jednym elemencie, a mianowicie wybieramy element  $x_1$  z warstwy  $v_1$  i element  $x_2$  z warstwy  $v_2$ . Oznaczmy przez  $v_3$  warstwę, do której należy element  $x_1 + x_2$  grupy  $G$ . Udowodnimy, że warstwa  $v_3$  nie zależy od tego, jakie elementy  $x_1$  i  $x_2$  wybraliśmy z warstwy  $v_1$  i  $v_2$ . Innymi słowy udowodnimy, że jeżeli  $x_1'$  jest dowolnym elementem warstwy  $v_1$ , na ogół biorąc różnym od  $x_1$  a  $x_2$  jest dowolnym elementem warstwy  $v_2$ , także na ogół biorąc różnym od  $x_2$ , to element  $x_1' + x_2$  należy do tej samej warstwy  $v_3$  co i element  $x_1 + x_2$ .

Istotnie, dwa elementy  $a$  i  $b$  wtedy i tylko wtedy należą do jednej warstwy względem podgrupy niezmienniczej  $U$ , gdy ich różnica  $b-a$  należy do  $U$ . Rozpatrzmy różnicę

$$(x_1 + x_2) - (x_1' + x_2) = x_1 + x_2 - x_1' - x_2 = x_1 - x_1'.$$

Ponieważ  $x_2$  i  $x_2'$  należą do tej samej warstwy  $v_2$ , więc

$$x_2 - x_2' = u_2$$

gdzie  $u_2$  jest pewnym elementem  $U$  i mamy

$$(1) \quad (x_1 + x_2) - (x_1' + x_2) = x_1 - x_1' + u_2$$

Ale  $U$  jest podgrupą niezmienniczą, więc

$$x_1 - x_1' + u_2 = u' + x_1 - x_1',$$

Gdzie  $u'$  jest pewnym elementem grupy  $U$ . Uwzględniając to we wzorze (1) otrzymujemy

$$(x_1 + x_2) - (x_1' + x_2) = u' + x_1 - x_2.$$

Ale  $x_1$  i  $x_1'$  należą do tej samej warstwy  $v_1$ , dlatego  $x_1 - x_1' = u_1$ , gdzie  $u_1$  jest pewnym elementem grupy  $U$ . Wobec tego

$$(x_1 + x_2) - (x_1' + x_2) = u' + u_1,$$

tj.  $(x_1 + x_2) - (x_1' + x_2)$  jest pewnym elementem  $u = u' + u_1$  grupy  $U$ , co należało okazać.

Ponieważ warstwa  $v_3$  określona jest w ten sposób przez podanie warstw  $v_1$  i  $v_2$ , więc przyjmujemy

$$(2) \quad v_3 = v_1 + v_2$$

Jest to określenie sumy  $v_1$  i  $v_2$  dwóch warstw  $v_1$  i  $v_2$

Tak więc

Sumą dwóch warstw  $v_1$  i  $v_2$  nazywamy warstwę  $i$ , otrzymaną na podstawie następującej reguły: W każdej z warstw  $v_1$  i  $v_2$  wybieramy po jednym dowolnym elemencie, dodajemy te dwa elementy i bierzemy warstwę, do której ta suma należy. Warstwa ta jest właśnie warstwą  $v_3 = v_1 + v_2$ .

Z tego określenia  $i$  z tego, że dodawanie elementów w grupie  $G$  spełnia postulat łączności, wynika bezpośrednio, że  $i$  dodawanie warstw spełnia postulat łączności. Udowodnimy, że rolę elementu zerowego w określonym przez nas dodawaniu warstw spełnia warstwa  $U$ , tj. że dla dowolnej warstwy  $v$  zachodzi równość

$$(3) \quad v + U = U + v = v.$$

W tym celu wybierzmy dowolny element  $x$  z warstwy  $v$  i element  $0$  z warstwy  $U$ . Na mocy określenia dodawania warstwa  $v + U$  jest tą warstwą, do której należy element  $x + 0 = x$ , czyli jest warstwą  $v$ . Dokładnie tak samo  $U + v$  jest warstwą  $x$  zawierającą element  $0 + x = x$ , czyli warstwą  $v$ . W ten sposób udowodniliśmy wzór (3).

Udowodnimy wreszcie, że dla każdej warstwy  $K$  istnieje pewna warstwa jej przeciwna, którą oznaczamy przez  $-K$  i która spełnia warunek

$$K + (-K) = -K + K = U.$$

W tym celu wybierzmy z warstwy  $K$  dowolny element  $a$  i jako warstwę  $-K$  przyjmijmy tę warstwę, do której należy element  $-a$ . Na mocy określenia dodawania warstw każda z warstw  $K + (-K)$  i  $(-K) + K$  jest warstwą zawierającą element  $a + (-a) = (-a) + a = 0$ , czyli warstwą  $U$ .

Tak więc określone przez nas dodawanie spełnia wszystkie aksjomaty grupy. Wobec tego przy naszej operacji dodawania zbiór warstw grupy  $G$  względem jej podgrupy niezmienniczej  $U$  jest pewną grupą  $V$ . Warstwa  $U$  gra przy tym rolę elementu zerowego grupy  $V$ . Grupę  $V$  nazywamy grupą ilorazową grupy  $G$  względem jej podgrupy niezmienniczej  $U$ .

Twierdzenie o odwzorowaniach homomorficznych. Niech, podobnie jak poprzednio, dana będzie grupa  $G$  i jej podgrupa niezmiennicza  $U$ . Przyporządkujmy każdemu elementowi  $x$  grupy  $G$  określony element grupy ilorazowej  $V$ , mianowicie tę warstwę, która zawiera element  $x$ . W ten sposób określimy pewne odwzorowanie  $\varphi$  grupy  $G$  na grupę  $V$  i z określenia dodawania w grupie  $V$  bezpośrednio wynika, że to odwzorowanie jest homomorfizmem.

Jakie elementy grupy  $G$  zostają odwzorowane na element zerowy grupy  $V$ ? Ponieważ elementem zerowym grupy  $V$  jest podgrupa  $U$ , więc oczywiście odpowiedź na nasze pytanie brzmi:

Wszystkie elementy podgrupy niezmienniczej  $U$  i tylko one zostają przy odwzorowaniu  $\varphi$  przekształcone na element zerowy grupy  $V$ .

Z rozważań z tego i poprzedniego ustępu wynika, każda podgrupa niezmiennicza  $U$  grupy  $G$  jest jądrem pewnego odwzorowania homomorficznego grupy  $G$ , mianowicie odwzorowania homomorficznego grupy  $G$  na jej podgrupę ilorazową względem podgrupy  $U$ . Niech dane będzie teraz dowolne odwzorowanie homomorficzne  $f$  jakiegokolwiek grupy  $A$  na jakąkolwiek grupę  $B$ . Niech  $U$  oznacza jądro tego homomorfizmu, Wiemy, że  $U$  jest podgrupą niezmienniczą grupy  $A$ , Oznaczmy przez  $V$  grupę ilorazową grupy  $A$  względem podgrupy  $U$ . Niech  $b$  będzie dowolnym elementem grupy  $B$ , Istnieje co najmniej jeden element  $a$  grupy  $A$ , który na mocy przekształcenia  $f$  zostaje odwzorowany na element  $b$ :

$$b = f(a).$$

Określmy przeciwobraz elementu  $b$  przy przekształceniu  $f$ , tj. zbiór wszystkich elementów  $x$  grupy  $A$ , które za pomocą odwzorowania  $f$  przechodzą na  $b$ . Ten przeciwobraz oznaczmy jak zwykle przez  $f^{-1}(b)$ . Zbiór  $f^{-1}(b)$  jest zatem zbiorem tych wszystkich  $x$  z grupy  $A$ , dla których zachodzi równość

$$f(x) = b.$$

Niech, jak już powiedzieliśmy,  $a$  będzie jakimkolwiek elementem ze zbioru  $f^{-1}(b)$ ; jeżeli  $x$  jest innym elementem zbioru  $f^{-1}(b)$  to

$$f(a) = b, f(x) = b, f(-a) = b, f[x+(-a)] = b + (-b) = 0$$

(zero z prawej strony oznacza element zerowy grupy  $B$ ), oznacza to, że  $x + (-a)$  jest pewnym

elementem  $u$  grupy  $U$ , tj.  $x = a+u$  jest elementem tej warstwy względem podgrupy niezmienniczej  $U$ , do której należy element  $a$ . Odwrotnie, jeżeli  $a$  i  $x$  należą do tej samej warstwy, to

$$\begin{aligned}x &= a+u, \\ f(a+u) &= f(x) = f(a) + f(u) = f(a) + 0 = f(a)\end{aligned}$$

tj.  $a$  i  $x$  są odwzorowane na jeden i ten sam element grupy  $B$ , czyli innymi słowy zawarte są w przeciwobrazie  $f^{-1}(b)$ .

Tak więc przeciwobrazy  $f^{-1}(b)$  elementów grupy  $B$  są warstwami grupy  $A$  względem podgrupy niezmienniczej  $U$ . W ten sposób ustalona jest wzajemnie jednoznaczna odpowiedniość  $\psi$  między grupą  $B$  i grupą  $V$ .

Każdemu elementowi grupy  $V$ , czyli pewnej warstwie grupy  $A$  względem podgrupy niezmienniczej  $U$ , tj. przeciwobrazowi pewnego elementu  $b$  grupy  $B$ , odpowiada właśnie ten element  $b$  grupy  $B$ ; przy tym każdy element  $b$  grupy  $B$  jest przyporządkowany dokładnie jednej warstwie, tj. dokładnie jednemu elementowi grupy  $V$ , mianowicie tej warstwie, która jest przeciwobrazem elementu  $b$ . Odwzorowanie  $\psi$  jest homomorfizmem. Niech  $v_1$  i  $v_2$ , będą dwoma elementami grupy  $V$  i

$$(1) \quad v_1 + v_2 = v_3.$$

Niech  $a_1$  będzie dowolnym elementem warstwy  $v_1$  a  $a_2$  dowolnym elementem warstwy  $v_2$  i  $a_3 = a_1 + a_2$ . Wiemy, że wówczas  $a_3$  należy do  $v_3$ . Przyjmijmy

$$f(a_1)=b_1, f(a_2) = b_2, f(a_3) = b_3,$$

Ponieważ  $f$  jest homomorfizmem, więc

$$(2) \quad b_1 + b_2 = b_3$$

Ponieważ jednak  $v_1, v_2, v_3$  są przeciwobrazami elementów  $b_1, b_2, b_3$ , więc

$$\psi(v_1) = b_1, \psi(v_2) = b_2, \psi(v_3) = b_3$$

tak, że równość (2) możemy przepisać w postaci

$$\psi(v_1) + \psi(v_2) = \psi(v_3)$$

co dowodzi, że  $\psi$  jest homomorfizmem. Jako wzajemnie jednoznaczne odwzorowanie homomorficzne grupy  $V$  na grupę  $B$  przekształcenie  $\psi$  jest też izomorfizmem.

Podsumowaniem wszystkiego co powiedzieliśmy jest następujące twierdzenie o homomorfizmie:

**Twierdzenie.** Każde odwzorowanie homomorficzne w pewnej grupy  $A$  na inną grupę  $B$  ma jako jądro pewną podgrupę niezmienniczą grupy  $A$ . Odwrotnie, każda podgrupa niezmiennicza  $U$  grupy  $A$  jest jądrem pewnego homomorfizmu  $\phi$  grupy  $A$  na grupę ilorazową  $V$  grupy  $A$  względem podgrupy  $U$ . Odwzorowanie  $\phi$  otrzymujemy, gdy każdemu elementowi grupy  $A$  przyporządkujemy jego warstwę względem podgrupy niezmienniczej  $U$ . Jeżeli  $f$  jest dowolnym homomorfizmem grupy  $A$  na grupę  $B$ , to przeciwobrazami elementów grupy  $B$  przy tym odwzorowaniu są warstwy grupy  $A$  względem jądra  $U$  odwzorowania  $f$  i grupa  $B$  jest izomorficzna z grupą ilorazową  $V$  grupy  $A$  względem grupy  $U$ .

Tak więc podgrupy niezmiennicze danej grupy  $A$  pokrywają się z jądrami wszystkich możliwych homomorfizmów tej grupy, a wszystkie grupy będące homomorficznymi obrazami grupy  $A$  pokrywają się z grupami, które są izomorficzne z grupami ilorazowymi grupy  $A$  względem jej wszystkich możliwych podgrup niezmienniczych.

**Wniosek.** Na to, aby odwzorowanie homomorficzne grupy  $A$  na grupę  $B$  było izomorfizmem, potrzeba i wystarcza, aby jądro tego homomorfizmu składało się z jednego tylko elementu zerowego grupy  $A$ .

# UZUPEŁNIENIE

## ELEMENTARNE POJĘCIA TEORII MNOGOŚCI

Podstawowe pojęcia teorii mnogości, o których będziemy mówili w tym uzupełnieniu i które są obecnie bezustannie stosowane w matematyce, są to przede wszystkim pojęcia zbioru, odwzorowania, rozbicia na klasy, a także elementarne operacje na zbiorach, jak dodawanie i mnożenie kilku (a czasem i nieskończenie wielu) zbiorów.

### § 1. Pojęcie zbioru

Pojęcia zbioru i odwzorowania należą do tych pojęć matematycznych, których nie da się sprowadzić do pojęć prostszych i dlatego w ogóle ich nie definiujemy. Można wobec tego mówić jedynie o wyjaśnieniu sensu tych pojęć. W życiu codziennym, podobnie jak i w każdych naukowych rozważaniach, stale posługujemy się pojęciem zbioru; można mówić o zbiorze przedmiotów znajdujących się w danym momencie w danym pokoju, o zbiorze ludzi siedzących w audytorium lub w sali koncertowej, o zbiorze książek, z których składa się dana biblioteka, o zbiorze gwiazd Drogi Mlecznej. Można dalej mówić o zbiorze cząsteczek, zawartych w danej objętości danej masy, o zbiorze komórek żywego organizmu. Jeśli mówimy: stado gęsi, worek kartofli, koszyk jabłek, to z matematycznego punktu widzenia mamy do czynienia ze zbiorem: gęsi, z których składa się dane stado, kartofli lub jabłek, znajdujących się w worku czy koszyku. Przytoczone przykłady są przykładami zbiorów skończonych; wszystkie te zbiory, o których mówiliśmy, składają się z pewnej skończonej ilości przedmiotów, być może bardzo wielkiej (jak np. przypadku cząsteczek wody znajdujących się w danej objętości wody), ale w każdym przypadku ilość elementów każdego z tych zbiorów była skończona. Istnieją jednak także zbiory nieskończone. Takimi są . na przykład: zbiór wszystkich liczb naturalnych (tzn liczb całkowitych dodatnich), zbiór wszystkich prostych przechodzących przez dany punkt (na płaszczyźnie lub w przestrzeni), zbiór wszystkich okręgów przechodzących przez dane dwa punkty płaszczyzny i stycznych do danej prostej itd. Teoria mnogości poświęcona jest głównie badaniu właśnie zbiorów nieskończonych. Teoria mnogości zastosowana do zbiorów skończonych nazywa się czasami kombinatoryką. Jednak elementarne własności zbiorów - te, o których tu będziemy mówili - w większości przypadków odnoszą się w równej mierze zarówno do zbiorów skończonych, jak i do zbiorów nieskończonych. Zwrócimy jeszcze uwagę na pewną okoliczność. W matematyce zupełnie dopuszczalne jest rozpatrywanie zbiorów składających się tylko z jednego elementu, a także zbiorów, które w ogóle nie zawierają żadnych elementów (zbiory puste).

Załóżmy, że mówimy ogólnie o zbiorze okręgów przechodzących przez kilka danych punktów. Jeżeli tych punktów jest dwa, to zbiór okręgów przechodzących przez te punkty jest nieskończony; jeżeli jest ich trzy, to (w przypadku gdy nie leżą one na jednej prostej) I, sinieje tylko jeden przechodzący przez nie okrąg. Innymi słowy zbiór okręgów, przechodzący przez trzy punkty nie leżące na jednej prostej składa się z jednego tylko elementu. Zbiór okręgów przechodzących przez trzy punkty leżące na jednej prostej nie zawiera ani jednego elementu, czyli jest, jak mówimy, zbiorem pustym, ponieważ takich okręgów w ogóle nie ma. Wyjaśnimy tę kwestię na przykładzie z życia codziennego. Przypuśćmy, że mówimy o zbiorze uczniów biorących udział w danej lekcji, których wiek zawarty jest między 17 a 19 rokiem (włącznie). Zbiór ten jest w pełni określony w tym sensie, że o każdym z obecnych na tej lekcji uczniów możemy za pomocą prostego pytania rozstrzygnąć, czy należy on do naszego zbioru, czy nie. Niemniej jednak zawczasu wcale nie wiemy, ilu właściwie uczniów należy do naszego zbioru. Może ich być 10, może być 5, może być tylko 1, a może się zdarzyć, że w naszej klasie nie będzie ani jednego ucznia w wieku 17-19 lat, a wszyscy mogą być np. młodsi niż, 17 lat. W ostatnim przypadku nasz zbiór będzie zbiorem pustym, w poprzednich - będzie się on składał z 10, 5 i z 1 elementu.

Zbiory składające się z jednego elementu będziemy spotykali w tej książce bardzo często. Zbiorów

pustych w tej książce nie będziemy rozpatrywali, ogólnie jednak w matematyce są one często istotnym czynnikiem w rozważaniach.

## § 2. Podzbiory

Rozpatrzmy zbiór A wszystkich ludzi znajdujących się w danym audytorium. Wówczas zbiór obecnych w tym audytorium mężczyzn, podobnie jak zbiór obecnych w tym audytorium kobiet, są przykładami podzbiorów zbioru A. Przykładami innych podzbiorów zbioru A są: zbiór ludzi w wieku poniżej 30 lat; zbiór ludzi, których wzrost zawarty jest między 160 a 170 cm; zbiór ludzi o wzroście większym niż 165 cm; zbiór ludzi mających dany wzrost lub dane stanowisko społeczne itd. Jest zupełnie zrozumiałe, że niektóre z tych zbiorów mogą zawierać tylko jeden element, a niektóre mogą w ogóle nie zawierać ani jednego elementu. Może się jednak okazać, że pewien z wymienionych przez nas podzbiorów pokrywa się z całym zbiorem A, na przykład, jeżeli wszystkie obecne w audytorium osoby są mężczyznami lub wszystkie mają mniej niż 30 lat. Może się poza tym zdarzyć, że niektóre z tych podzbiorów pokrywają się między sobą (na przykład jeżeli wszyscy obecni na sali mężczyźni i tylko oni mają mniej niż 30 lat) lub że kilka podzbiorów jednocześnie pokrywa się z całym zbiorem A. Ogólne określenie podzbiorów jest następujące:

Zbiór B nazywamy podzbiorem zbioru A, jeżeli każdy element zbioru B jest zarazem elementem zbioru A. Podzbiór zbioru A nazywa się niewłaściwy, jeżeli pokrywa się z całym zbiorem A (innymi słowy, zbiór A jest swoim podzbiorem i nazywa się podzbiorem niewłaściwym). Jeżeli B jest podzbiorem A, to mówimy też, że B jest zawarte w A, lub że A zawiera B, co oznaczamy symbolem  $B \subset A$  lub  $A \supset B$ . Znak  $\subset$  nazywamy symbolem zawierania lub inkluzji. Zbiór pusty jest podzbiorem każdego zbioru.

Podamy jeszcze przykłady:

Zbiór wszystkich liczb parzystych jest podzbiorem zbioru wszystkich liczb całkowitych, a zbiór wszystkich liczb całkowitych jest podzbiorem zbioru wszystkich liczb wymiernych.

## § 3. Działania na zbiorach

**1. Suma zbiorów.** Powrócimy do przykładu rozpatrzonego na początku poprzedniego paragrafu.

Spośród wszystkich ludzi obecnych w danym audytorium rozpatrzmy zbiór M tych ludzi, którzy mają chociażby jedną z następujących cech:

1. mają mniej niż 20 lat,
2. mają więcej niż 165 cm wzrostu.

Innymi słowy, do zbioru M wejdą wszyscy ludzie naszego audytorium, którzy mają mniej niż 20 lat (niezależnie od ich wzrostu) i wszyscy ci, których wzrost wynosi więcej niż 165 cm (niezależnie od ich wieku). Zbiór M nazywamy sumą dwóch zbiorów: zbioru  $M_1$  wszystkich obecnych w audytorium mających mniej niż 20 lat i zbioru  $M_2$ , takich, których wzrost wynosi więcej niż 165 cm.

Ogólne określenie sumy dwóch zbiorów A i B jest następujące:

Sumą zbiorów A i B nazywamy zbiór składający się ze wszystkich elementów zbioru A i ze wszystkich elementów zbioru B.

Uwaga. Z dopiero co przytoczonego przykładu widać, że można dodawać zbiory także i w tym przypadku, jeżeli istnieją elementy należące do obu zbiorów jednocześnie; często może się zdarzyć, że zbiory  $M_1$  i  $M_2$ , mają elementy wspólne, tj. że w naszym audytorium są ludzie, którzy np. mają mniej niż 20 lat, a których wzrost wynosi więcej niż 165 cm. Zaznaczymy jeszcze w szczególności, że jeżeli zbiór B jest podzbiorem zbioru A, to suma zbiorów B i A pokrywa się ze zbiorem A. Na przykład, jeżeli zbiór A składa się ze wszystkich obecnych w audytorium, którzy mają mniej niż 30 lat, a zbiór B z tych obecnych, którzy mają mniej niż 20 lat, to suma zbiorów A i B jest oczywiście zbiorem A.

Analogicznie określamy sumę trzech, czterech i większej ilości zbiorów. Można też określić sumę nieskończonej ilości zbiorów. Ogólne określenie jest następujące:

Niech dana będzie pewna skończona lub nieskończona rodzina zbiorów. Sumą zbiorów danej rodziny nazywamy zbiór wszystkich elementów, które należą co najmniej do jednego ze zbiorów tej rodziny. Niech np.  $A_k$  będzie zbiorem wszystkich  $k$ -kątów foremnych na płaszczyźnie ( $k = 3, 4, 5, \dots$ ). W ten sposób  $A_3$  jest zbiorem wszystkich trójkątów równobocznych,  $A_4$  -zbiorem wszystkich kwadratów itd. Zbiór wszystkich foremnych wielokątów jest sumą zbiorów  $A_3, A_4, A_5, \dots, A_k, \dots$

Oznaczmy przez  $B_k, k = 3, 4, 5, \dots$ , zbiór wszystkich wielokątów foremnych, których liczba boków nie przewyższa  $k$ . Wówczas  $B_k$  jest sumą zbiorów  $B_3, B_4, B_5, \dots, B_{k-1}, B_k$  i zbiór wszystkich wielokątów foremnych jest sumą wszystkich zbiorów  $B_k, k = 3, 4, 5, \dots$

Oczywiście,  $A_3 = B_3$  i zachodzi

$$B_3 \subset B_4 \subset B_5 \subset \dots B_k \subset B_{k+1} \subset \dots$$

**2.Iloczyn zbiorów.** Niech  $M_1$  będzie zbiorem wszystkich obecnych w audytorium, których wiek wynosi mniej niż 20 lat, a  $M_2$  - zbiorem tych spośród obecnych, których wzrost wynosi więcej niż 165 cm. Iloczynem dwóch zbiorów  $M_1$  i  $M_2$  będziemy nazywali zbiór elementów, które należą i do zbioru  $M_1$  i do zbioru  $M_2$ , tj. w naszym przykładzie zbiór wszystkich obecnych, których wiek wynosi mniej niż 20 lat i których wzrost jednocześnie wynosi więcej niż 165 cm. Oczywiście, zbiór ten może być zbiorem pustym. W ogóle iloczynem danej (skończonej lub nieskończonej) rodziny zbiorów nazywamy zbiór, składający się z tych elementów, które należą jednocześnie do wszystkich zbiorów danej rodziny.

Zauważmy, że jeżeli  $B \subset A$ , to iloczyn zbiorów  $A$  i  $B$  pokrywa się ze zbiorem  $B$ .

Ćwiczenie. Umówimy się, że przez trójkąt będziemy rozumieli zbiór wszystkich punktów leżących wewnątrz tego trójkąta. Udowodnić, że suma wszystkich trójkątów równobocznych wpisanych w okrąg o środku  $O$  i promieniu 1 jest zbiorem wszystkich punktów leżących wewnątrz tego okręgu, a iloczyn tych trójkątów jest zbiorem punktów leżących wewnątrz okręgu o środku  $O$  i promieniu  $1/3$ .

Sformułować i rozwiązać analogiczne zadanie dla kwadratów wpisanych w okrąg i innych wielokątów foremnych, a także dla wielokątów foremnych opisanych na okręgu.

#### § 4. Odwzorowania, czyli funkcje

Załóżmy, że pewna ilość ludzi wybrała się, przypośćmy, do teatru. Przy wejściu ludzie ci rozebrali się i otrzymali z szatni numerki na płaszcze. Co w tym znanym każdemu zjawisku jest interesującego z punktu widzenia matematycznego? Interesuje nas tu fakt, który możemy sformułować w sposób następujący:

Każdemu widzowi odpowiada (lub: jest przyporządkowany) pewien przedmiot, mianowicie ten numer, który otrzymał on w szatni. Jeżeli każdemu elementowi  $a$  pewnego zbioru  $A$  przyporządkowany jest w dowolny sposób pewien określony element  $b$  zbioru  $B$ , to mówimy, że mamy do czynienia z odwzorowaniem zbioru  $A$  w zbiór  $B$ , lub inaczej, że mamy do czynienia z funkcją, której argumenty przebiegają zbiór  $A$ , a wartości należą do zbioru  $B$ . Aby zaznaczyć, że danemu elementowi  $a$  zbioru  $A$  przyporządkowany jest element  $b$  zbioru  $B$ , piszemy  $b = f(a)$  i mówimy, że  $b$  jest obrazem elementu  $a$  przy odwzorowaniu  $f$  (lub że  $b$  jest wartością funkcji  $f$  dla argumentu  $a$ ). Mogą tu zachodzić różne przypadki, które zaraz rozpatrzemy. Może się zdarzyć, że na dany spektakl rozsprzedane są wszystkie bilety. Wówczas w szatni zazwyczaj nie zostaje ani jedno wolne miejsce; nie tylko każdy widz otrzymał numerki, ale i wszystkie numerki będą rozdane między widzów. Ten przypadek w ogólnym matematycznym sformułowaniu możemy scharakteryzować następująco: każdemu elementowi  $a$  zbioru  $A$  przyporządkowany jest element  $b$  zbioru  $B$ , przy czym każdy element zbioru  $B$  jest przyporządkowany co najmniej jednemu elementowi zbioru  $A$  (podkreślone słowa wyrażają w odniesieniu do naszego przykładu właśnie to, że wszystkie numerki zostały rozdane).

W tym przypadku mówimy, że mamy do czynienia z odwzorowaniem zbioru  $A$  na zbiór  $B$ .

Dlaczego mówimy: każdy element zbioru B jest przyporządkowany co najmniej jednemu elementowi zbioru A?

Dlatego, że może się zdarzyć, że kilku różnym elementom zbioru A zostanie przyporządkowany jeden i ten sam element zbioru B. W naszym szczególnym przypadku oznacza to, że kilku ludzi powiesiło swoje płaszcze na jednym i tym samym wieszaku i otrzymało jeden i ten sam numer.

Najważniejszym przypadkiem odwzorowania jest przypadek odwzorowania jednego zbioru na drugi. Ogólny przypadek odwzorowania jednego zbioru w drugi łatwo do tego przypadku sprowadzić. Istotnie, niech dane będzie pewne odwzorowanie  $f$  zbioru A w zbiór B; zbiór tych elementów zbioru B, które są przyporządkowane chociażby jednemu elementowi zbioru A nazywamy obrazem zbioru A przy odwzorowaniu  $f$  i oznaczamy przez  $f(A)$ . Oczywiście, że odwzorowanie  $f$  jest odwzorowaniem zbioru A na zbiór  $f(A)$ .

Ta uwaga pozwala nam w dalszym ciągu ograniczyć się do rozpatrywania tylko odwzorowania jednych zbiorów na drugie.

W naszym przykładzie z teatrem A jest zbiorem wszystkich widzów, którzy przybyli na dany spektakl, a  $f(A)$  jest zbiorem wszystkich zajętych numerków w szatni. Określenie. Niech dane będzie odwzorowanie  $f$  zbioru A na zbiór B. Niech  $b$  będzie dowolnym elementem zbioru B. Przeciwobrazem elementu  $b$  przy odwzorowaniu  $f$  nazywamy zbiór wszystkich tych elementów zbioru A, którym przy odwzorowaniu  $f$  przyporządkowany jest element  $b$ . Zbiór ten oznaczamy przez  $f^{-1}(b)$ .

W rozważanym przykładzie  $b$  może być dowolnym z numerków w szatni; przeciwobrazem elementu  $b$  jest zbiór tych wszystkich widzów, którzy powiesili swoje okrycia właśnie na wieszaku o numerze  $b$ .

Rozpatrzmy teraz przypadek, kiedy na każdy wieszak przypada tylko jedno palto, tj. kiedy przeciwobraz  $f^{-1}(b)$  każdego elementu  $b$  zbioru B składa się z jednego tylko elementu zbioru A. W tym przypadku odwzorowanie zbioru A na zbiór B nazywa się wzajemnie jednoznaczne.

Podamy jeszcze jeden przykład ilustrujący pojęcie odwzorowania wzajemnie jednoznacznego.

Wyobraźmy sobie oddział kawalerii. Każdy jeździec siedzi na jednym koniu i na każdym koniu siedzi jeden jeździec. W ten sposób ustalone zostało wzajemnie jednoznaczne odwzorowanie zbioru wszystkich jeźdźców na zbiór wszystkich koni (danego oddziału), a także wzajemne jednoznaczne odwzorowanie zbioru wszystkich koni na zbiór wszystkich jeźdźców (mowa jest cały czas o jeźdźcach i koniach danego oddziału). Ten przykład pokazuje, że odwzorowanie wzajemnie jednoznaczne zbioru A na zbiór B wyznacza także odwzorowanie wzajemnie jednoznaczne zbioru B na zbiór A; przecie jeżeli każdy ze zbiorów  $f^{-1}(b)$ , gdzie  $b$  jest dowolnym elementem B, składa się z jednego tylko elementu  $a$ , to odwzorowanie  $f^{-1}$  zbioru B na zbiór A otrzymujemy przyporządkowując każdemu elementowi  $b$  zbioru B element  $a = f^{-1}(b)$  zbioru A. Odwzorowanie  $f^{-1}$  nazywa się odwzorowaniem odwrotnym do odwzorowania  $f$ . Tak więc przy odwzorowaniu wzajemnie jednoznacznym zbioru A na zbiór B każdy element  $a$  zbioru A łączymy w parę z pewnym elementem  $f(a)$ , przy czym okazuje się, że każdy element  $b$  zbioru B jest połączony w parę z dokładnie jednym elementem  $a$  zbioru A. Przyporządkowując każdemu elementowi  $b$  zbioru B tworzący razem z nim parę element  $a$  zbioru A otrzymujemy wzajemnie jednoznaczne odwzorowanie  $f^{-1}$  zbioru B na zbiór A, odwrotne do odwzorowania  $f$ .

W ten sposób przy odwzorowaniu wzajemnie jednoznacznym zbioru A na zbiór B oba te zbiory mają niejako jednakowe prawa (ponieważ każdy jest we wzajemnie jednoznaczny sposób odwzorowany na drugi). Aby to równouprawnienie podkreślić, mówimy często o odpowiedności wzajemnie jednoznacznej między dwoma zbiorami, rozumiejąc przez to oba wzajemnie jednoznaczne i wzajemnie odwrotne odwzorowanie każdego ze zbiorów na drugi.

## § 5. Rozbicie zbioru na podzbiory

**1. Zbiory zbiorów.** Możemy rozpatrywać zbiory składające się z przeróżnych elementów. W szczególności możemy rozpatrywać zbiory zbiorów, tj. zbiory, których elementami są zbiory. Spotkaliśmy się z tym już, gdy wprowadziliśmy określenie sumy i iloczynu zbiorów; przecie

mówiliśmy tam o sumie i iloczynie pewnej (skończonej lub nieskończonej) rodziny zbiorów, tj. właśnie o zbiorze zbiorów. Do przytoczonych tam przykładów dodamy jeszcze kilka przykładów wziętych z życia codziennego. Zbiorem zbiorów jest na przykład zbiór wszystkich moskiewskich klubów sportowych (jeżeli każdy klub sportowy uważać za zbiór należących do niego sportowców); zbiór wszystkich towarzystw naukowych danego miasta lub danego kraju, zbiór wszystkich związków zawodowych, zbiór wszystkich jednostek wojskowych (dywizji, pułków, batalionów, kompanii, plutonów etc.) danej armii — są także przykładami rodzin zbiorów. Przykłady te pokazują, że zbiory, będące elementami danej rodziny zbiorów, mogą mieć w jednych przypadkach wspólne elementy, w innych mogą być między sobą rozłączne, nie mieć wspólnych elementów. Tak na przykład zbiór wszystkich związków zawodowych ZSRR jest rodziną zbiorów parami rozłącznych, ponieważ obywatel Rosji nie może być jednocześnie członkiem dwóch związków zawodowych. Z drugiej strony zbiór wszystkich jednostek dowolnej armii jest przykładem rodziny zbiorów, których pewne elementy są podzbiorem innych elementów, ponieważ każda kompania jest podzbiorem pewnego pułku, a każdy pułk jest podzbiorem pewnej dywizji itd. Zbiór wszystkich klubów sportowych danego miasta składa się, ogólnie biorąc, ze zbiorów mających wspólne elementy, ponieważ jeden i ten sam człowiek może należeć do kilku klubów (na przykład do klubu pływackiego i do klubu siatkarskiego lub łyżwiarskiego).

**2. Rozbicie na klasy.** Bardzo ważną klasę rodzin zbiorów otrzymamy, jeżeli będziemy rozpatrywali wszystkie możliwe podziały danego zbioru na zbiory parami rozłączne. Innymi słowy, niech dany będzie zbiór  $M$  przedstawiony w postaci sumy parami rozłącznych podzbiorów (w ilości skończonej lub nieskończonej). Te podzbiory (zbiory będące składnikami naszej sumy) są elementami pewnego rozbicia zbioru  $M$ .

**Przykład 1.** Niech  $M$  będzie zbiorem uczniów dowolnej szkoły; szkoła jest podzielona na klasy, które oczywiście tworzą parami rozłączne podzbiory dające w sumie zbiór  $M$ .

**Przykład 2.**  $M$  jest zbiorem wszystkich uczniów moskiewskich szkół średnich. Zbiór  $M$  można podzielić na parami rozłączne podzbiory na przykład na dwa następujące sposoby: 1. zaliczamy do jednego podzbioru wszystkich uczniów jednej i tej samej szkoły (tj. rozbijamy nasz zbiór według szkół); 2. zaliczamy do jednego podzbioru wszystkich uczniów jednej i tej samej klasy (choćby i z różnych szkół).

**Przykład 3.** Niech  $M$  będzie zbiorem wszystkich punktów płaszczyzny; obierzmy na tej płaszczyźnie dowolną prostą  $g$  i podzielmy tę płaszczyznę na proste równoległe do prostej  $g$ . Zbiory punktów każdej z tych prostych są właśnie tymi podzbiorem, na które podzieliśmy zbiór  $M$ .

Uwaga 1. Czytelnicy, którzy wiedzą co to jest układ współrzędnych, mogą sobie wyobrazić  $g$  jako jedną z osi współrzędnych (np. oś rzędnych) tego układu.

Uwaga 2. Jeżeli dany zbiór  $M$  jest podzielony na sumę parami rozłącznych podzbiorów, to mówimy dla krótkości o rozbiciu zbioru  $M$  na klasy.

Twierdzenie 1. Niech dane będzie odwzorowanie  $f$  zbioru  $A$  na zbiór  $B$ . Przeciwobrazy  $f^{-1}(b)$  wszystkich możliwych elementów  $b$  zbioru  $B$  tworzą rozbicie zbioru  $A$  na klasy. Zbiór tych klas znajduje się w odpowiedności wzajemnie jednoznacznej ze zbiorem  $B$ .

Twierdzenie to jest właściwie oczywiste; każdemu elementowi  $a$  zbioru  $A$  odpowiada na mocy odwzorowania  $f$  dokładnie jeden element  $b=f(a)$  zbioru  $B$ , tak że  $a$  należy do jednego tylko przeciwobrazu  $f^{-1}(b)$ . Stąd właśnie wynika, że przeciwobrazy elementów  $b$  po pierwsze — dają w sumie cały zbiór  $A$ , a po drugie — są parami rozłączne. Zbiór tych klas znajduje się w odpowiedności wzajemnie jednoznacznej ze zbiorem  $B$ : każdemu elementowi  $b$  zbioru  $B$  odpowiada klasa  $f^{-1}(b)$  i każdej klasie  $f^{-1}(b)$  odpowiada element  $b$  zbioru  $B$ .

Twierdzenie 2. Niech dane będzie rozbicie zbioru  $A$  na klasy. Rozbicie to generuje odwzorowanie zbioru  $A$  na pewien zbiór  $B$ , mianowicie na zbiór wszystkich klas danego rozbicia. Odwzorowanie to otrzymujemy przyporządkowując każdemu elementowi zbioru  $A$  tę klasę, do której on należy.

Dowód twierdzenia zawiera się już w jego sformułowaniu.

Przykład. Już przez to, że moskiewscy uczniowie rozdzieleni są według szkół, zostało ustalone odwzorowanie zbioru  $A$  wszystkich uczniów na zbiór  $B$  wszystkich szkół; każdemu uczniowi przyporządkowana jest ta szkoła, do której uczęszcza.

Pomimo oczywistości naszych dwóch twierdzeń fakty, które z nich wynikają, nie od razu otrzymały w matematyce jasne sformułowanie; otrzymawszy jednak to sformułowanie nabrały od razu dużej wagi w logicznej budowie różnych dyscyplin matematycznych, a przede wszystkim algebry.

3. Relacja równoważności. Niech dane będzie rozbitcie zbioru  $M$  na klasy. Wprowadzimy następujące określenie:

Dwa elementy zbioru  $M$  nazwiemy równoważnymi względem danego rozbitcia zbioru  $M$  na klasy, jeżeli należą one do jednej i tej samej klasy. W ten sposób, jeżeli rozbijemy uczniów moskiewskich według szkół, to dwóch uczniów będziemy nazywali równoważnymi, jeżeli będą oni uczęszczali do jednej i tej samej szkoły (choćby do różnych klas). Jeżeli natomiast rozbijemy uczniów według klas, to dwóch uczniów nazwiemy równoważnymi, jeżeli będą oni uczęszczali do jednej i tej samej klasy (choćby i w różnych szkołach). Wyżej określona relacja równoważności spełnia oczywiście następujące warunki:

Własność symetrii. Jeżeli  $a$  jest równoważne  $b$ , to także  $b$  jest równoważne  $a$ .

Własność przechodniości. Jeżeli  $a$  jest równoważne  $b$  oraz  $b$  jest równoważne  $c$ , to  $a$  jest równoważne  $c$  (dwa elementy ( $a$  i  $c$ ) równoważne trzeciemu ( $b$ ) są równoważne między sobą).

Wreszcie, każdy element uważamy za równoważny samemu sobie; ta własność relacji równoważności nazywa się *zwrotnością*.

Tak więc każde rozbitcie danego zbioru na klasy określa pewną relację równoważności między elementami tego zbioru, spełniającą własności symetrii, przechodniości i zwrotności.

Załóżmy teraz, że udało się nam w jakikolwiek sposób ustalić pewne kryterium pozwalające nam mówić o pewnych parach elementów zbioru  $M$  jako o parach elementów równoważnych. Przy tym od równoważności tej wymagamy tylko, aby miała ona własności symetrii, przechodniości i zwrotności. Udowodnimy, że ta relacja równoważności określa pewne rozbitcie zbioru  $M$  na klasy.

W istocie, nazwijmy klasą  $K_a$  danego elementu  $a$  zbioru  $M$  zbiór wszystkich elementów równoważnych elementowi  $a$ . Na mocy tego, że nasza relacja równoważności z założenia jest zwrotna, każdy element  $a$  należy do swojej klasy. Udowodnimy, że jeżeli dwie klasy mają chociażby jeden element wspólny, to są one identyczne (tj. każdy element jednej klasy jest zarazem elementem drugiej). W istocie, niech klasy  $K_a$  i  $K_b$  mają wspólny element  $c$ . Oznaczając równoważność dwóch dowolnych elementów  $x$  i  $y$  symbolem  $x \sim y$  mamy według określenia klas

$$a \sim c, b \sim c.$$

Zatem na mocy symetrii mamy  $c \sim b$  i na mocy przechodniości

$$(1) \quad a \sim b$$

Niech  $y$  będzie dowolnym elementem klasy  $K_b$ . Mamy

$$b \sim y$$

czyli na mocy przechodniości (1)

$$a \sim y,$$

tzn.  $y$  jest elementem klasy  $K_a$ .

Niech teraz  $x$  będzie dowolnym elementem klasy  $K_a$ . Mamy

$$a \sim x$$

i na mocy symetrii

$$x \sim a,$$

a na mocy (1) i przechodniości

$$x \sim b.$$

Na mocy symetrii

$$b \sim x,$$

tzn.  $x$  należy do klasy  $K_b$ .

W ten sposób dwie klasy  $K_a$  i  $K_b$  mające wspólny element  $c$  rzeczywiście pokrywają się ze sobą.

Udowodniliśmy, że różne klasy  $K_a$  tworzą układ wzajemnie rozłącznych podzbiorów zbioru  $M$ .

Klasy te w sumie dają cały zbiór  $M$ , ponieważ każdy element zbioru  $M$  należy do swojej klasy.

Powtórzmy jeszcze raz rezultaty tego ustępu łącząc je w następujące

Twierdzenie 3. Każde rozbitcie na klasy dowolnego zbioru  $M$  określa pewną relację równoważności między elementami tego zbioru mającą własności symetrii, przechodności i zwrotności. Odwrotnie, każda relacja równoważności między elementami zbioru  $M$  spełniająca, własności symetrii, przechodności i zwrotności, określa pewne rozbitcie zbioru  $M$  na klasy elementów równoważnych,