ROZDZIAŁ XIX

GRUPY

§ 1. Definicja grupy. Przykłady. Zbiór (nie pusty) G o dowolnych elementach nazywamy *grupą*, jeżeli jest w nim określone działanie, które każdym dwom (różnym lub nie) elementom a i b zbioru G przyporządkowuje element zbioru G, który oznaczamy przez ab (niekiedy przez $a+b$), w taki sposób, że spełnione są dwa następujące warunki:

1° *działanie to jest łączne* czyli

$$(ab)c=a(bc) \quad \text{dla wszelkich} \quad a\in G,\ b\in G \ \text{ i } \ c\in G \ [1])$$

(lecz niekoniecznie przemienne, t. j. może być $ab\neq ba$),

2° *oba jego działania odwrotne są w zbiorze G wykonalne*, t. j. dla każdych a i b, należących do zbioru G, istnieje co najmniej jeden element x, należący do zbioru G i taki, że

$$ax=b,$$

oraz co najmniej jeden element y, należący do zbioru G i taki, że

$$ya=b.$$

Grupę, której działanie jest przemienne (t. j. takie, że $ab=ba$ dla wszelkich $a\in G$ i $b\in G$) nazywamy *abelową*.

PRZYKŁADY. 1. Jeżeli G jest zbiorem wszystkich liczb całkowitych, zaś ab oznacza sumę liczb a i b, to G będzie grupą abelową. Zbiór wszystkich liczb całkowitych nie byłby jednak grupą, gdyby ab oznaczało różnicę lub iloczyn liczb a i b. Dla różnicy bowiem działanie nie byłoby łączne, dla iloczynu działania odwrotne nie zawsze byłyby wykonalne.

2. Jeżeli G jest zbiorem wszystkich różnych od zera liczb wymiernych rzeczywistych (albo liczb wymiernych zespolonych), zaś ab oznacza iloczyn liczb a i b, to G będzie grupą (abelową).

[1]) Znak $\in$ oznacza przynależność elementu do zbioru.

3. Zbiór czterech liczb 1, —1, i oraz —i jest grupą (abelową), jeżeli ab oznacza iloczyn liczb a i b. Ogólniej, zbiór wszystkich pierwiastków n-go stopnia z jedności tworzy grupę, jeżeli ab oznacza iloczyn liczb a i b.

4. Zbiór liczb 1, 2, 3 i 4 jest grupą (abelową), jeżeli ab oznacza resztę z dzielenia iloczynu liczb a i b przez 5.

5. Zbiór, złożony z liczb $0,1,2,\ldots,n-1$ jest grupą (abelową), jeżeli ab oznacza resztę z dzielenia sumy liczb a i b przez liczbę naturalną n.

Istnieją więc grupy abelowe o dowolnej skończonej liczbie elementów, jak również grupy abelowe nieskończone.

Istnieją też grupy (abelowe) nieskończone dowolnej mocy. Istotnie, niech m oznacza dowolną liczbę kardynalną, a M jakikolwiek zbiór mocy m. Niech G oznacza zbiór wszystkich funkcyj $f(m)$, określonych na zbiorze M i przybierających tylko dwie wartości, +1 i —1, przy czym wartość —1 tylko dla skończonej (lub równej zeru) liczby elementów zbioru M. Jak wiadomo z Teorii mnogości, zbiór nieskończony mocy m posiada m różnych części skończonych. Wynika stąd, że zbiór G jest mocy m. Jeżeli teraz określimy iloczyn elementów zbioru G jako zwykły iloczyn funkcyj, to, jak łatwo dostrzec, zbiór G stanie się grupą (abelową). Będzie to więc grupa mocy m.

Dowodzi się też, że istnieją grupy nieskończone nie abelowe dowolnej mocy.

Natomiast nie z każdej skończonej liczby elementów można utworzyć grupę nie abelową. Udowodnimy później (Rozdział XIX, § 14, str. 336, wniosek 1), że każda grupa, której liczba elementów jest pierwsza, jest abelową. Również każda grupa z 4 lub 9 elementów jest abelową, ale istnieją grupy nie abelowe, złożone z 6, 8, 10 lub 12 elementów.

Teoria grup gra ważną rolę w matematycznym ujmowaniu zjawisk fizycznych. Sir Eddington np. poświęca jej w swej książce[1]) cały rozdział.

6. Opierając się na elementarnych wiadomościach z Teorii liczb, łatwo dowieść, że dla każdej liczby naturalnej $m>1$ zbiór wszystkich liczb pierwszych względem m, występujących w ciągu $1,2,\ldots,m$, jest grupą (abelową), jeżeli ab oznacza resztę z dzielenia iloczynu liczb a i b przez liczbę m.

7. Zbiór wszystkich pierwiastków wszelkich naturalnych stopni z jedności jest grupą (abelową nieskończoną), jeżeli ab oznacza zwykły iloczyn liczb a i b.

[1]) A. Eddington, *Nauka na nowych drogach* (z angielskiego przełożył prof. S. Szczeniowski), Biblioteka Wiedzy, Tom 30, Rozdział XII, str. 268-291.

8. Sześć funkcyj:

$$z, \quad 1-z, \quad \frac{1}{z}, \quad 1-\frac{1}{z}, \quad \frac{1}{1-z}, \quad \frac{z}{z-1}$$

tworzy grupę, jeżeli przez ab, gdzie $a=f(z)$ i $b=g(z)$, rozumieć funkcję $h(z)=g(f(z))$. Grupa ta nie jest abelową, gdyż np. dla $a=1-z$, $b=\frac{1}{z}$ mamy $ab=\frac{1}{1-z}$ i $ba=\frac{z-1}{z}$, a więc $ab \neq ba$.

9. Zbiór wszystkich funkcyj $\frac{az+b}{cz+d}$, gdzie współczynniki a, b, c i d są liczbami całkowitymi (albo liczbami wymiernymi, albo liczbami rzeczywistymi, albo liczbami zespolonymi) spełniającymi warunek

$$ad-bc=1,$$

tworzy grupę (nie abelową), jeżeli ab określimy jak w przykładzie 8.

10. Zbiór wszystkich przekształceń kuli na siebie, dokonanych za pomocą takich jej ruchów, przy których środek kuli pozostaje na miejscu, tworzy grupę (nie abelową), jeżeli przez iloczyn dwu przekształceń a i b rozumieć przekształcenie, polegające na kolejnym wykonaniu przekształcenia a, a następnie przekształcenia b.

11. Zbiór liczb rzeczywistych (wszystkich, albo tylko wymiernych) x, takich iż $0 \leqslant x < 1$, tworzy grupę (abelową), jeżeli przez ab rozumieć liczbę $a+b-\mathrm{E}(a+b)$, gdzie $\mathrm{E}(t)$ oznacza „Entier" z liczby t (ob. str. 219).

12. Niech G oznacza zbiór wszystkich części dowolnie danego zbioru Z (włączając i część pustą). G jest grupą (abelową), jeżeli przez ab rozumieć zbiór, utworzony z tych wszystkich elementów części a (zbioru Z), które nie należą do części b, oraz z tych wszystkich elementów części b, które nie należą do części a. Dowód opiera się na przemienności i łączności działania $a \bigcirc b=(a-b)+(b-a)$ na zbiorach (por. Rozdz. XVII, § 1, str. 281, przykład 4) oraz na tej jego własności, że wzory $a \bigcirc b=c$ i $a \bigcirc c=b$ są równoważne.

13. Z Teorii przekształceń liniowych (Rozdział IV, § 1) wynika, że przekształcenia liniowe jednorodne danej liczby $n>1$ zmiennych o wyznaczniku równym 1 tworzą grupę (nie abelową), jeżeli przez ab rozumieć przekształcenie, polegające na kolejnym wykonaniu przekształcenia a, a następnie przekształcenia b.

14. Z własności macierzy (ob. Rozdział V, § 2, str. 69) wynika, że macierze kwadratowe utworzone z liczb rzeczywistych (lub tylko wymiernych) o liczbie elementów większej od 1 i o wyznaczniku różnym od 0 tworzą grupę (nie abelową), jeżeli przez ab rozumieć iloczyn macierzy a i b.

15. Cztery macierze:

$$\left\|\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\right\|, \quad \left\|\begin{matrix}-1 & 0\\ 0 & -1\end{matrix}\right\|, \quad \left\|\begin{matrix}1 & 0\\ 0 & -1\end{matrix}\right\|, \quad \left\|\begin{matrix}-1 & 0\\ 0 & 1\end{matrix}\right\|$$

tworzą grupę (abelową), jeżeli ab oznacza iloczyn macierzy a i b.

16. Zbiór wszystkich funkcyj dodatnich (lub tylko dodatnich ciągłych) zmiennej rzeczywistej tworzy grupę, jeżeli przez ab rozumieć zwykły iloczyn funkcyj a i b.

17. Zbiór wszystkich przekształceń wzajemnie jednoznacznych dowolnego zbioru Z (skończonego lub nieskończonego) na siebie tworzy grupę, jeżeli przez iloczyn przekształceń a i b rozumieć przekształcenie, polegające na wykonaniu najpierw przekształcenia a, a następnie b. Grupa ta nie jest abelowa, jeżeli zbiór Z zawiera więcej niż 2 elementy.

W szczególności, zbiór wszystkich $n!$ podstawień (w obrębie wszystkich permutacyj n elementów) tworzy grupę ze względu na mnożenie podstawień.

Grupę tworzą też, jak łatwo widzieć, wszystkie podstawienia, będące iloczynami parzystej liczby transpozycyj (t. j. wszystkie te, które przeprowadzają permutację $1\,2\,\ldots\,n$ na permutację klasy parzystej). Jak wiemy z Rozdziału I (§ 4, tw. 3, str. 5), jest ich $\frac{n!}{2}$.

Cztery podstawienia:

$$1, \quad (1\ 2), \quad (3\ 4), \quad (1\ 2)(3\ 4)$$

też tworzą — jak łatwo widzieć — grupę (abelową).

18. Kwaterniony $1, i, j, k, -1, -i, -j, -k$ (ob. Rozdział VI, § 4, str. 88) tworzą grupę 8-elementową (nie abelową) ze względu na mnożenie kwaternionów.

Zbiór wszystkich kwaternionów różnych od zera też tworzy grupę (nie abelową) ze względu na ich mnożenie.

19. Każde ciało liczbowe (por. Rozdział XIII, § 1, str. 224) oczywiście jest grupą (abelową) ze względu na dodawanie, nie jest jednak grupą ze względu na mnożenie, o ile zawiera więcej niż jeden element (gdyż $a0=0$ dla każdego elementu a ciała).

Natomiast zbiór wszystkich różnych od zera (lub tylko dodatnich) liczb każdego ciała liczbowego jest grupą (abelową) ze względu na mnożenie [1]) (por. przykład 2), lecz nie na dodawanie.

§ 2. Jedność grupy i jej własności. Mamy następujące

Twierdzenie 1. W każdej grupie G istnieje jeden i tylko jeden taki element e, zwany jednością grupy G, iż:

(1) $$ae=ea=a \quad \text{dla wszelkich} \quad a \in G.$$

Dowód. Niech c oznacza dowolny element grupy G. Na mocy własności 2° grupy istnieje taki element $e \in G$, iż:

(2) $$ec=c.$$

Zarazem dla każdego elementu a grupy G istnieje na mocy 2° taki element x grupy G, iż:

$$cx=a,$$

skąd wobec własności 1° grupy oraz wobec (2):

$$ea=e(cx)=(ec)x=cx=a$$

czyli

(3) $$ea=a \quad \text{dla każdego} \quad a \in G.$$

Z drugiej strony, wobec 2° istnieje taki element e' grupy G, iż $ce'=c$, oraz taki element y grupy G, iż $yc=a$, skąd wobec 1°:

$$ae'=(yc)e'=y(ce')=yc=a$$

czyli

(4) $$ae'=a \quad \text{dla każdego} \quad a \in G.$$

Na mocy (3) mamy dla $a=e'$:

(5) $$ee'=e',$$

zaś na mocy (4) dla $a=e$:

(6) $$ee'=e.$$

Wzory (5) i (6) dowodzą, iż $e'=e$, skąd na mocy (4):

(7) $$ae=a \quad \text{dla każdego} \quad a \in G.$$

Wzory (3) i (7) dają wzór (1). Istnienie jedności e w grupie G jest więc udowodnione.

[1]) Jest to prawdziwe i dla ogólniejszych ciał (nie liczbowych), których określenie podamy w Rozdziale XX, § 1, str. 348.

Pozostaje dowieść, że jest ona jedyna. Otóż gdyby było jeszcze $ae_1=e_1a=a$ dla każdego $a \in G$, mielibyśmy dla $a=e$ równość $ee_1=e$, a że wobec (1) dla $a=e_1$ mamy $ee_1=e_1$, więc jest $e_1=e$, c. b. d. d.

Jedność grupy będziemy stale oznaczali przez e.

§ 3. Elementy odwrotne i ich własności. Niech a oznacza dowolny element grupy G. W myśl 2° istnieje taki element a^{-1} grupy G, iż

$$aa^{-1}=e,$$

oraz taki element a' grupy G, iż

$$a'a=e.$$

Wobec (1) i 1° mamy stąd:

$$(a'a)a^{-1}=a'(aa^{-1})=a'e=a' \quad \text{i} \quad (a'a)a^{-1}=ea^{-1}=a^{-1},$$

skąd $a'=a^{-1}$. Jest więc:

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

Gdyby było $ab=e$, znaleźlibyśmy jak wyżej:

$$(a^{-1}a)b=a^{-1}(ab)=a^{-1}e=a^{-1} \quad \text{i} \quad (a^{-1}a)b=eb=b,$$

skąd $b=a^{-1}$. Zachodzi zatem

Twierdzenie 2. Dla każdego elementu a grupy G istnieje jeden i tylko jeden element a^{-1} grupy taki, iż:

(8) $$aa^{-1}=e;$$

element ten spełnia też równość:

(9) $$a^{-1}a=e.$$

Element a^{-1} nazywamy *odwrotnym* albo *odwrotnością* elementu a.

Jak łatwo stwierdzić, jest:

$$e^{-1}=e,$$

gdyż $ee^{-1}=e$ i $ee^{-1}=e^{-1}$.

Dla elementów odwrotnych zanotujemy jeszcze wzór:

(10) $$(ab)^{-1}=b^{-1}a^{-1},$$

którego dowód wynika z równości:

(11) $$(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)b=b^{-1}eb=b^{-1}b=e;$$

otrzymujemy dalej:

$$(abc)^{-1}=[(ab)c]^{-1}=c^{-1}(ab)^{-1}=c^{-1}b^{-1}a^{-1}$$

i, ogólnie, przez łatwą indukcję:

$$(12)\qquad (a_1a_2\dots a_n)^{-1}=a_n^{-1}a_{n-1}^{-1}\dots a_2^{-1}a_1^{-1}.$$

Wyprowadzimy obecnie pewną własność charakterystyczną elementu e (jedności grupy). Na mocy określenia jedności e grupy G mamy:

$$ee=e;$$

otóż udowodnimy

Twierdzenie 3. *Jedność e jest jedynym elementem x grupy G, spełniającym równanie:*

$$xx=x.$$

Dowód. Jeżeli element x spełnia to równanie, to mnożąc obie strony przez x^{-1}, otrzymamy:

$$(xx)x^{-1}=xx^{-1},$$

a zatem wobec równości $xx^{-1}=e$, zachodzącej na mocy (8), oraz z uwagi na równość $(xx)x^{-1}=x(xx^{-1})=xe=x$, otrzymujemy $x=e$, c. b. d. o.

Równanie $e^2=e$ jest więc dla jedności grupy charakterystyczne.

§ 4. Jednoznaczna wykonalność działań odwrotnych.

Niech teraz dane będą dwa elementy a i b grupy G. W myśl 2^0 istnieje taki element $x\in G$, iż $ax=b$, skąd $(a^{-1}a)x=a^{-1}(ax)=a^{-1}b$, a że $(a^{-1}a)x=ex=x$, więc $x=a^{-1}b$.

Zachodzi zatem

Twierdzenie 4. *Dla każdych dwu elementów a i b grupy G istnieje jeden i tylko jeden taki element x grupy G, iż $ax=b$, mianowicie element $x=a^{-1}b$.*

Podobnie dowodzi się, że zachodzi

Twierdzenie 4′. *Dla każdych dwu elementów a i b grupy G istnieje jeden i tylko jeden taki element y grupy G, iż $ya=b$, mianowicie element $y=ba^{-1}$.*

Twierdzenia 4 i 4′ dowodzą, że *w każdej grupie oba działania odwrotne są wykonalne jednoznacznie.*

Warunek 2^0 można by więc wzmocnić, żądając, aby oba działania odwrotne były wykonalne jednoznacznie.

Działania odwrotne do działania grupy niekoniecznie jednak wyznaczają grupę, jak tego dowodzi przykład 1 z § 1 (str. 306).

Z twierdzeń 4 i 4′ wynika natychmiast następujący

Wniosek 1. *Z $ax=ax'$, jak również z $xa=x'a$, wynika $x=x'$.*

Oto inny łatwy wniosek z tychże twierdzeń:

Wniosek 2. *Jeżeli a jest dowolnym elementem grupy G, zaś x przebiega wszystkie elementy grupy G, każdy raz tylko, to czyni to samo zarówno ax jak xa.*

Iloczyn n czynników, z których każdy jest równy elementowi a, oznaczamy przez a^n.

Potęgi o wykładnikach ujemnych $-n$ określamy wzorem

$$a^{-n}=(a^{-1})^n.$$

Jak łatwo wykazać, będzie też $a^{-n}=(a^n)^{-1}$.

Dla każdego elementu a grupy rozumiemy przez a^0 jedność e grupy.

Dowodzi się z łatwością, że:

$$(13)\qquad a^ka^l=a^{k+l},$$

$$(14)\qquad (a^k)^l=a^{kl}$$

dla każdego elementu a grupy oraz dla wszelkich całkowitych k i l.

Natomiast może być

$$(ab)^2\neq a^2b^2,$$

jak to zobaczymy dalej (ob. § 16, str. 339).

Jeżeli jednak grupa jest abelową, to mamy w niej (dla wszelkich elementów a i b oraz dla każdej liczby całkowitej k):

$$(15)\qquad (ab)^k=a^kb^k.$$

Okażemy teraz, że w definicji pojęcia grupy warunek 2^0 można zastąpić przez zespół dwu warunków 2_1^0 i 2_2^0:

2_1^0 *zachodzi twierdzenie* 1,

2_2^0 *dla każdego elementu a należącego do G istnieje co najmniej jeden taki element a^{-1} należący do G, iż:*

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

Istotnie, jeżeli G jest grupą, to zachodzi twierdzenie 1 czyli 2_1^0 oraz twierdzenie 2, które pociąga za sobą 2_2^0.

Na odwrót, załóżmy, że w zbiorze G określone jest działanie, spełniające warunki 1^0, 2_1^0 i 2_2^0. Niech a i b będą elementami należącymi do G i niech a^{-1} będzie elementem zbioru G, spełniającym warunek 2_2^0. Z uwagi na to, że w myśl 2_1^0 jest $eb=be=e$, będzie więc:

$$a(a^{-1}b)=(aa^{-1})b=eb=b \quad \text{i} \quad (ba^{-1})a=b(a^{-1}a)=be=b,$$

co dowodzi, że spełniony będzie warunek 2^0.

Jak widzimy, dla przekonania się, czy dane działanie, określone w zbiorze G, wyznacza grupę, wystarcza sprawdzić:

czy jest ono łączne,

czy istnieje (jedyna) *jedność tego działania,*

czy każdy element zbioru G posiada (co najmniej jeden) *element odwrotny.*

§ 5. Produkt grup. Z dwu grup G_1 i G_2 powstaje nowa grupa G, której elementami są pary uporządkowane (a_1,a_2), gdzie a_1 jest dowolnym elementem grupy G_1, zaś a_2 dowolnym elementem grupy G_2, przy czym za iloczyn dwóch takich par $(a_1,a_2)(b_1,b_2)$ uważa się parę (a_1b_1,a_2b_2). Jednością tej grupy G jest, jak łatwo sprawdzić, para (e_1,e_2), gdzie e_1 jest jednością grupy G_1, zaś e_2 jednością grupy G_2; odwrotnością elementu (a_1,a_2) jest element (a_1^{-1},a_2^{-1}).

Tę nową grupę G, w ten sposób utworzoną, nazywamy *produktem* (lub *iloczynem kombinatorycznym*) grup G_1 i G_2 i oznaczamy przez $G_1\times G_2$.

Dowodzi się łatwo, że *produkt dwóch grup abelowych jest grupą abelową.*

Możemy też tworzyć produkt nieskończonego ciągu grup $G_1,G_2,G_3,\ldots$, mianowicie grupę:

$$G=G_1\times G_2\times G_3\times\ldots,$$

której elementami są wszystkie ciągi nieskończone $a_1,a_2,a_3,\ldots$, gdzie n-ty wyraz jest dowolnym elementem grupy G_n, a w której iloczynem elementów $(a_1,a_2,a_3,\ldots)$ i $(b_1,b_2,b_3,\ldots)$ jest element $(a_1b_1,a_2b_2,a_3b_3,\ldots)$.

Oczywiście, *produkt ciągu nieskończonego grup abelowych jest grupą abelową.*

Można też tworzyć grupy, będące produktami pozaskończonych ciągów grup.

§ 6. Podgrupy. Przykłady. Niech G_1 oznacza taką część (nie pustą) grupy G, która przy działaniu określonym w G sama jest grupą.

Jeżeli więc a jest elementem G_1, to istnieje w G_1 takie x, iż $ax=a$, skąd (w G) $a^{-1}ax=a^{-1}a$, zatem $ex=e$, co wobec $ex=x$ daje $x=e$. Zatem e jest elementem G_1 (przy czym, jak łatwo widzieć, e jest zarazem jednością grupy G_1). Istnieje więc dla każdego a, należącego do G_1, w grupie G_1 taki element y, iż $ay=e$, skąd $a^{-1}ay=a^{-1}e$, zatem $ey=a^{-1}$, skąd $y=a^{-1}$, co dowodzi, że a^{-1} jest elementem G_1.

Jeżeli więc zbiór G_1 zawarty w G jest grupą, to:

(i) dla każdych dwu jego elementów a i b iloczyn ab jest elementem G_1,

(ii) jeśli a jest elementem G_1, to a^{-1} jest elementem G_1.

Z warunków (i) i (ii) oraz założenia, że $G_1\neq 0$, wynika, że *jedność e grupy G należy do G_1*, gdyż jeżeli a jest elementem G_1, to wobec (i) i (ii) również $e=aa^{-1}$ jest elementem G_1.

Na odwrót, okażemy teraz, że jeżeli G jest grupą, zaś G_1 jej częścią spełniającą warunki (i) i (ii), to G_1 jest grupą.

Wystarczy oczywiście okazać, że G_1 spełnia warunek 2^0.

Załóżmy więc, że a i b są elementami G_1. Wobec (ii), a^{-1} jest elementem G_1; wobec (i), zarówno $x=a^{-1}b$ jak $y=ba^{-1}$ są elementami G_1, skąd:

$$ax=aa^{-1}b=eb=b, \qquad ya=ba^{-1}a=be=b.$$

Warunek 2^0 jest więc spełniony. Mamy zatem:

Twierdzenie 5. *Na to, żeby część (nie pusta) G_1 grupy G była grupą, potrzeba i wystarcza, by spełnione były warunki* (i) *i* (ii).

Załóżmy, w szczególności, że G_1 jest częścią skończoną (nie pustą) grupy G, spełniającą warunek (i).

Dla danego $a\in G_1$ wszystkie wyrazy ciągu nieskończonego $a,a^2,a^3,\ldots$ należą do G_1, a że G_1 jest zbiorem skończonym, więc istnieją takie naturalne k i l, że $a^k=a^{k+l}$. Jest zatem $a^k=a^ka^l$, skąd $(a^k)^{-1}a^k=(a^k)^{-1}a^ka^l$ w G, czyli $e=ea^l=a^l$, skąd $a^l=e$ i przeto e jest elementem G_1. Jeżeli $l=1$, to $a=e$ i $a^{-1}=e^{-1}=e=a$, a więc a^{-1} jest elementem G_1; jeżeli zaś $l>1$, to $aa^{l-1}=a^l=e$ w G, co dowodzi w myśl twierdzenia 2, że $a^{l-1}=a^{-1}$, a zatem że a^{-1} jest elementem grupy G_1. W każdym więc razie jeśli a jest elementem G_1,

to i a^{-1} jest elementem G_1. Warunki (i) i (ii) są więc spełnione i wobec twierdzenia 5 mamy

Twierdzenie 6. *Na to, żeby część skończona (nie pusta) G_1 grupy G była grupą, potrzeba i wystarcza, by działanie określone w G było wykonalne w G_1,* t. j. by spełniony był warunek (i).

W szczególności, *aby pewien zbiór podstawień (dla skończonej liczby elementów) tworzył grupę, potrzeba i wystarcza, by iloczyn dwu podstawień tego zbioru zawsze do niego należał.*

Każdą część danej grupy, która sama jest grupą (ze względu na to samo działanie), nazywamy jej *podgrupą.*

Uwaga. W wysłowieniu twierdzenia 6 nie można skreślić wyrazu „skończona". Np. zbiór wszystkich liczb naturalnych nie tworzy podgrupy grupy G wszystkich liczb całkowitych, w której działaniem jest zwykłe dodawanie liczb, chociaż suma dwu liczb naturalnych jest liczbą naturalną. Do zbioru tego nie należy bowiem liczba 0, która jest jednością grupy G. Ale i zbiór Z wszystkich liczb całkowitych nieujemnych nie tworzy podgrupy grupy G, chociaż suma dwu liczb całkowitych nieujemnych jest liczbą całkowitą nieujemną (bo np. do zbioru tego nie należy liczba -1, która jest w grupie G elementem odwrotnym do elementu $+1$ zbioru Z).

Podobnie zbiór wszystkich funkcyj dodatnich rosnących zmiennej rzeczywistej nie tworzy podgrupy w grupie F wszystkich funkcyj dodatnich zmiennej rzeczywistej, jeżeli przez ab rozumieć zwykły iloczyn funkcyj, chociaż iloczyn dwóch funkcyj dodatnich rosnących jest zawsze funkcją dodatnią rosnącą. Do zbioru tego nie należy bowiem jedność grupy F (którą jest funkcja stale równa 1).

Podgrupa podgrupy danej grupy jest oczywiście jej podgrupą.

PRZYKŁADY. 1. Dla grupy złożonej z liczb 1, -1, i i $-i$, gdzie działaniem jest zwykłe mnożenie liczb, podgrupą jest np. część utworzona z liczb 1 i -1.

2. Jeżeli G jest grupą, zaś e jej jednością, to zbiór złożony z jednego tylko elementu e jest podgrupą grupy G. Jest to najmniejsza podgrupa grupy G, gdyż — jak wiemy — każda podgrupa grupy G musi zawierać jej jedność.

3. Dla grupy G utworzonej ze wszystkich liczb wymiernych dodatnich, gdzie działaniem jest zwykłe mnożenie liczb, podgrupą jest zbiór wszystkich liczb 2^k, gdzie k przebiega wszystkie liczby

całkowite. Oznaczmy tę podgrupę przez G_1. Podgrupą grupy G_1 (a więc tym bardziej grupy G) jest zbiór wszystkich liczb 4^k, gdzie $k=0,\pm 1,\pm 2, \ldots$

4. Jeżeli G jest grupą abelową, zaś k liczbą całkowitą, to k-te potęgi wszystkich elementów grupy G tworzą oczywiście jej podgrupę. Podgrupę grupy abelowej tworzą również wszystkie jej elementy a, dla których przy danym całkowitym k jest $a^k=e$, gdzie e jest jednością grupy.

5. Jeżeli a jest elementem grupy G, to wszystkie potęgi a^k, gdzie $k=0,\pm 1,\pm 2, \ldots$, tworzą — jak łatwo stwierdzić — podgrupę grupy G (mogącą, w szczególności, być równą grupie G).

6. Element a grupy G, którego iloczyn z każdym innym elementem grupy jest przemienny (t. j. taki, że $ax=xa$ dla każdego x należącego do G) nazywamy *centralnym.*

Udowodnimy, że zbiór wszystkich elementów centralnych grupy tworzy jej podgrupę; nazywa się ona *centrum* grupy G.

Istotnie, jeżeli a i b są centralnymi elementami grupy G, a x jest dowolnym elementem tej grupy, to:

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab),$$

skąd wynika, że ab też jest elementem centralnym. Dalej, jeżeli a jest elementem centralnym grupy G, zaś x jej dowolnym elementem, to $ax = xa$, skąd $a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$, a stąd wobec tożsamości:

$$a^{-1}(ax)a^{-1} = (a^{-1}a)xa^{-1} = exa^{-1} = xa^{-1},$$

$$a^{-1}(xa)a^{-1} = a^{-1}x(aa^{-1}) = a^{-1}xe = a^{-1}x$$

znajdujemy $xa^{-1} = a^{-1}x$, co dowodzi, że a^{-1} też jest elementem centralnym grupy G. Ponieważ ponadto jedność grupy też jest oczywiście jej elementem centralnym, więc zbiór wszystkich elementów centralnych grupy G spełnia warunki (i) i (ii) twierdzenia 5, a więc jest w myśl tego twierdzenia podgrupą grupy G.

Ogólniej, można łatwo dowieść, że *jeżeli Z jest dowolnym podzbiorem grupy G* (niekoniecznie będącym grupą), *to zbiór wszystkich elementów grupy G, przemiennych z każdym elementem zbioru Z, tworzy podgrupę grupy G.*

Podgrupa ta nazywa się *normalizatorem* zbioru Z.

7. Podstawienia:

$$1, \qquad (1\,2), \qquad (3\,4), \qquad (1\,2)\,(3\,4)$$

tworzą podgrupę grupy wszystkich $4!=24$ podstawień, możliwych dla 4 elementów.

8. W grupie, utworzonej ze wszystkich macierzy liczbowych kwadratowych o danej liczbie elementów, podgrupę tworzą macierze ortogonalne.

9. Zbiór Z wszystkich funkcyj ciągłych rosnących zmiennej rzeczywistej, przyjmujących każdą wartość rzeczywistą, będzie oczywiście grupą (nie abelową), jeżeli przez ab, gdzie $a=a(x)$ i $b=b(x)$, będziemy rozumieli funkcję $a(b(x))$. Jednością tej grupy będzie, funkcja $f(x)=x$.

Oto jeszcze przykład elementu grupy Z: funkcja $f(x)=x\cdot|x|$; elementem odwrotnym będzie tu funkcja:

$$f^{-1}(x)=\begin{cases}\sqrt{x} & \text{dla } x\geqslant 0,\\ -\sqrt{-x} & \text{dla } x<0\end{cases}$$

(gdzie pierwiastek należy brać arytmetyczny). Natomiast do grupy Z nie należy funkcja x^2, gdyż nie jest rosnącą w zbiorze wszystkich liczb rzeczywistych.

Grupa Z jest podgrupą grupy T wszystkich funkcyj ciągłych zmiennej rzeczywistej, przyjmujących raz i tylko raz każdą wartość rzeczywistą, przy tak samo określonym działaniu grupowym, zaś obie grupy Z i T są podgrupami grupy G wszystkich przekształceń wzajemnie jednoznacznych zbioru wszystkich liczb rzeczywistych na siebie.

Podgrupą (nie abelową) grupy Z jest zbiór Z_1 wszystkich funkcyj postaci $px+q$, gdzie $p>0$, a q jest dowolną liczbą rzeczywistą.

Podgrupą grupy Z_1 jest zbiór Z_2 wszystkich funkcyj postaci px, gdzie $p>0$.

Zbiór wszystkich funkcyj postaci $px+1$, gdzie $p>0$, nie tworzy jednak grupy przy tak samo określonym działaniu ab, gdyż np. działanie $(x+1)(x+1)$ nie jest w nim wykonalne (bowiem funkcja $x+2$ do zbioru tego nie należy).

Podgrupą (abelową) grupy Z_2 jest zbiór Z_3 wszystkich funkcyj postaci px, gdzie p jest liczbą wymierną dodatnią.

Podgrupą (cykliczną; ob. § 7) grupy Z_3 jest zbiór Z_4 wszystkich funkcyj postaci $2^k x$, gdzie k przebiega wszystkie liczby całkowite.

Podgrupą grupy Z_4 jest zbiór wszystkich funkcyj postaci $2^{2k}x$, gdzie $k=0,\pm1,\pm2,\ldots$ i t. d.

10. Niech $G=G_1\times G_2\times G_3\times\ldots$ będzie produktem ciągu nieskończonego grup $G_1,G_2,\ldots$; podgrupą grupy G będzie zbiór wszystkich ciągów $a_1,a_2,\ldots$, gdzie $a_k\in G_k$ dla $k=1,2,\ldots$ i gdzie tylko skończona lub równa 0 liczba wyrazów a_k nie spełnia warunku $a_k=e_k$, w którym e_k oznacza jedność grupy G_k.

11. Podgrupą grupy wszystkich przekształceń wzajemnie jednoznacznych danego zbioru nieskończonego Z na samego siebie jest zbiór wszystkich tych przekształceń, które zmieniają tylko skończoną lub równą 0 (zmienną) liczbę jego elementów.

§ 7. Podgrupy grup cyklicznych. Zagadnienie wyznaczenia wszystkich podgrup danej grupy nie jest w przypadku ogólnym rozstrzygnięte. Dla pewnych jednak rodzajów grup daje się ono z łatwością rozstrzygnąć, np. dla t. zw. grup cyklicznych.

Cykliczną nazywamy grupę, której wszystkie elementy są potęgami o wykładnikach całkowitych tego samego (niekoniecznie zresztą jednego tylko) elementu grupy.

Np. grupa, określona w przykładzie 3 z § 1 (str. 307), jest cykliczna, gdyż każdy jej element jest potęgą elementu i (ale również elementu $-i$).

Każda grupa cykliczna jest oczywiście abelową.

Niech G będzie grupą cykliczną. Istnieje więc (co najmniej jeden) taki element a grupy G, iż każdy element grupy G jest postaci a^k, gdzie k jest liczbą całkowitą. Przypuśćmy, że Γ jest podgrupą grupy G, zawierającą poza jednością grupy G jeszcze inny jej element b. Jest więc $b=a^k$, gdzie $k\neq 0$, przy czym $b^{-1}=a^{-k}$ również należy do Γ; grupa Γ zawiera więc co najmniej jedną potęgę elementu a o wykładniku naturalnym. Niech m oznacza najmniejszą liczbę naturalną, taką, iż a^m należy do Γ. Do Γ będą więc też należały wszystkie elementy a^{km}, gdzie $k=0,\ \pm1,\ \pm2,\ldots$

Okażemy, że tylko te elementy należą do Γ. Istotnie niech element c należy do Γ. Jest więc $c=a^l$, gdzie l jest liczbą całkowitą. Trzeba dowieść, że c jest postaci a^{km}. Otóż gdyby l nie było podzielne przez m, mielibyśmy $l=qm+r$, gdzie q jest liczbą całkowitą, zaś r liczbą naturalną mniejszą od m. Byłoby więc $c=a^l=a^{qm+r}$. Ponieważ c i a^{-qm} należą do Γ, a Γ jest grupą, więc i $a^{-qm}c=a^r$ należy do Γ, wbrew definicji liczby m. Liczba l jest więc podzielna przez m, czyli $l=km$, gdzie k jest liczbą całkowitą. Zatem istotnie:

$$c=a^l=a^{km}.$$

Jeżeli więc G jest grupą cykliczną, utworzoną przez potęgi całkowite jej elementu a, to jedynymi jej podgrupami poza grupą utworzoną z jej jedności e są grupy (cykliczne) G_m utworzone przez potęgi elementu a o wykładnikach całkowitych podzielnych przez m, przy czym możemy założyć, że m jest najmniejszą liczbą naturalną, taką iż a^m jest elementem G_m.

Aby zbadać, ile spośród tych podgrup jest różnych, rozróżnimy dalej (dla grupy G) dwa przypadki:

1° Istnieje liczba naturalna l, taka iż $a^l=e$, gdzie e jest jednością grupy G. Niech n oznacza najmniejszą z takich liczb l.

Wówczas G składa się z n różnych elementów:

$$e=a^0, \quad a, \quad a^2, \quad \ldots, \quad a^{n-1}.$$

Z jednej bowiem strony, jeżeli a^k jest dowolnym elementem grupy G, możemy przyjąć $k=qn+r$, gdzie q i r są całkowite, przy czym $0<r<n$. Wówczas $a^k=a^{qn+r}=(a^n)^q a^r=e^q a^r=a^r$, a zatem a^k jest jednym z wyrazów ciągu $a^0,a^1,\ldots,a^{n-1}$. Z drugiej zaś strony, wszystkie te wyrazy są różnymi elementami grupy G; gdyby bowiem było $a^k=a^l$ dla $0\leqslant k<l\leqslant n-1$, to mielibyśmy $a^{l-k}=a^{k-k}=a^0=e$ przy $0<l-k<n$, wbrew określeniu liczby n.

Dalej, jeżeli G_m jest podgrupą grupy G, to m jest dzielnikiem liczby n. Istotnie gdyby było $n=qm+r$, gdzie $0<r<m$, to mielibyśmy $a^{qm+r}=a^n=e$, a że e i a^m, a więc i a^{-mq} są elementami grupy G_m, więc $ea^{-mq}=a^r$ należałoby do G_m, wbrew założeniu, że m jest najmniejszą liczbą naturalną, przy której a^m należy do G_m.

Zbadamy jeszcze, ile G_m ma różnych elementów. Skoro $m|n$, to możemy przyjąć $n=mq$, gdzie q jest liczbą naturalną. Każdy element grupy G_m ma, jak dowiedliśmy, postać a^{km}, gdzie k jest liczbą całkowitą. Z drugiej jednak strony, każdy element grupy G_m, jako podgrupy grupy G, jest jednym z jej elementów $a^0,a^1,\ldots,a^{n-1}$. Możemy więc założyć, że $0\leqslant km<n=mq$ czyli że $0\leqslant k<q$. Ale dla $0\leqslant k<k_1<q$ elementy a^{km} i $a^{k_1 m}$ są różne, gdyż $0\leqslant km<k_1 m<qm=n$. Grupa G_m zawiera więc $q=\frac{n}{m}$ różnych elementów.

Wreszcie, jeżeli m_1 i m_2 są różnymi dzielnikami liczby n, to grupy G_{m_1} i G_{m_2} są różne. Jeżeli bowiem $m_1<m_2$, to a^{m_1} należy do G_{m_1}, nie należąc do G_{m_2}.

Widzimy więc, że w przypadku 1° wszystkimi różnymi podgrupami grupy G są grupy G_m, gdzie m przebiega wszystkie dzielniki naturalne liczby n. Liczba tych podgrup jest więc równa liczbie wszystkich dzielników naturalnych liczby n, przy czym wliczamy też i samą grupę $G=G_1$ oraz grupę G_n, złożoną z samej tylko jedności e grupy G.

2° Przy wszelkim naturalnym l jest $a^l\neq e$. Wówczas dla naturalnych m_1 i $m_2\neq m_1$ grupy G_{m_1} i G_{m_2} są różne.

Okażemy w tym celu, że dla całkowitych k_1 i k_2, gdzie $k_1\neq k_2$, mamy $a^{k_1}\neq a^{k_2}$. Gdyby bowiem dla $k_1<k_2$ było $a^{k_1}=a^{k_2}$, to mielibyśmy $a^{k_2-k_1}=a^{k_2}a^{-k_1}=a^{k_1}a^{-k_1}=e$, wbrew założeniu 2°. W razie więc, gdy $m_1<m_2$, element a^{m_1} należy do G_{m_1}, nie należąc do G_{m_2} (gdyż G_{m_2} składa się tylko z elementów a^{km_2}, gdzie k jest liczbą całkowitą, zaś z uwagi na nierówność $m_1<m_2$ i na to, że m_1 jest liczbą naturalną, m_1 nie może być postaci km_2).

W przypadku 2° grupa G ma więc nieskończenie wiele różnych podgrup: są nimi, poza grupą złożoną z samej tylko jedności grupy G, grupy $G_1,G_2,G_3,\ldots$ Oczywiście, są one wszystkie nieskończone.

Ostatecznie więc możemy wypowiedzieć następujące

Twierdzenie 7. *Grupa cykliczna skończona G posiada tyle różnych podgrup (wliczając i samą grupę G), ile dzielników naturalnych ma liczba n jej elementów. Jeżeli d jest dzielnikiem (naturalnym) liczby n, to odpowiada mu podgrupa G_d grupy G, złożona z $q=\frac{n}{d}$ różnych elementów, przy czym, jeżeli G składa się z elementów $a^0,a^1,a^2,\ldots,a^{n-1}$, to G_d składa się z elementów $a^0,a^d,a^{2d},\ldots,a^{(q-1)d}$.*

Grupa cykliczna nieskończona G posiada nieskończenie wiele różnych podgrup. Jeżeli G składa się z potęg całkowitych elementu a, to każdej liczbie naturalnej m odpowiada podgrupa G_m grupy G, złożona z potęg całkowitych elementu a^m (które są wszystkie różne). Poza grupą, złożoną tylko z jedności grupy G, grupy G_m są wszystkimi podgrupami grupy G.

Grupa cykliczna nieskończona posiada więc przeliczalną mnogość różnych podgrup. Można z nich tworzyć ciągi nieskończone malejące podgrup, t. j. w których każdy wyraz jest zawarty w poprzednim, np. ciąg $G=G_1,G_2,G_4,G_8,\ldots,G_{2^n},\ldots$ Grupa cykliczna nie zawiera jednak żadnego ciągu nieskończonego rosnącego podgrup. Gdyby bowiem $Z_1,Z_2,\ldots$ było takim ciągiem podgrup grupy G, zawierających więcej niż 1 element, to w myśl twierdzenia 6 grupa Z_k składałaby się ze wszystkich potęg całkowitych pewnego elementu a^{m_k} grupy G, gdzie m_k jest liczbą naturalną. Skoro Z_k jest podgrupą grupy Z_{k+1}, element a^{m_k} mu-

siałby być całkowitą potęgą elementu a^{m_k+1}, zatem m_k musiałoby być podzielne przez m_{k+1}, przy tym różne od m_{k+1}, skoro grupy Z_k i Z_{k+1} są różne. Byłoby więc $m_k > m_{k+1}$ dla $k=1,2,\ldots$, a zatem istniałby ciąg nieskończony malejący liczb naturalnych, co nie jest możliwe.

Istnieją jednak grupy nie cykliczne, posiadające ciągi nieskończone rosnące różnych podgrup. Np. jeżeli przez Γ_n oznaczymy grupę wszystkich pierwiastków n-go stopnia z jedności, to $\Gamma_2, \Gamma_4, \Gamma_8, \ldots, \Gamma_{2^n}, \ldots$ jest ciągiem nieskończonym rosnącym podgrup grupy Γ wszystkich pierwiastków wszelkich naturalnych stopni z jedności.

Zauważymy też, że istnieją grupy przeliczalne, mające nieprzeliczalnie wiele różnych podgrup. Taką jest np. grupa wszystkich tych podstawień dla ciągu liczb naturalnych, które zmieniają tylko co najwyżej skończoną liczbę wyrazów tego ciągu. Można okazać, że grupa ta ma continuum różnych podgrup.

§ 8. Część wspólna podgrup. Rząd elementu grupy. Przykłady.

Udowodnimy następujące

Twierdzenie 8. *Część wspólna dowolnej mnogości podgrup grupy G jest podgrupą grupy G.*

Dowód. Niech M oznacza dowolną mnogość podgrup danej grupy G, zaś G_1 część wspólną wszystkich podgrup należących do M, t. j. zbiór wszystkich tych i tylko tych elementów, które należą do każdej należącej do M podgrupy grupy G. Aby stwierdzić, że G_1 jest grupą, wystarczy w myśl twierdzenia 5 okazać, że zbiór G_1 spełnia warunki (i) i (ii) z § 6, str. 315.

Ad (i). Niech a i b będą elementami zbioru G_1. Na mocy określenia G_1 zarówno a jak i b są elementami każdej grupy H należącej do M, zatem też (skoro H jest grupą) ab jest elementem H, co dowodzi, że ab jest elementem zbioru G_1.

Ad (ii). Jeżeli a jest elementem zbioru G_1, to dla każdej grupy H, należącej do mnogości M, a jest elementem H, a ponieważ H jest grupą, więc a^{-1} też jest elementem H, skąd wynika, że a^{-1} jest elementem zbioru G_1.

Warunki (i) i (ii) są więc spełnione i przeto zbiór G_1 jest grupą, c. b. d. d.

Niech Z będzie nie pustym zbiorem elementów grupy G. Istnieją podgrupy grupy G, zawierające zbiór Z (np. samo G). Część wspólna wszystkich podgrup grupy G, zawierających Z jest w myśl twierdzenia 8 podgrupą grupy G i oczywiście zawiera Z.

Jest to więc *najmniejsza podgrupa grupy G zawierająca Z* (t. j. podgrupa zawarta w każdej podgrupie grupy G zawierającej Z).

Mamy więc

Twierdzenie 9. *Dla każdego nie pustego zbioru Z elementów grupy G istnieje najmniejsza podgrupa grupy G, zawierająca Z.*

Podgrupa taka musi na mocy określenia pojęcia grupy zawierać wszystkie iloczyny skończone, których czynnikami są elementy zbioru Z lub ich odwrotności. Ale z twierdzenia 5 wynika, że zbiór wszystkich takich iloczynów tworzy grupę. Możemy więc wypowiedzieć

Wniosek. *Najmniejsza podgrupa grupy G, zawierająca podzbiór Z tej grupy, składa się ze wszystkich iloczynów skończonych, których czynnikami są elementy zbioru Z lub ich odwrotności.*

W szczególności, jeżeli zbiór Z składa się z jednego elementu a, to najmniejsza podgrupa grupy G zawierająca element a tej grupy składa się ze wszystkich potęg $a^{\pm n}$, gdzie $n=0,1,2,\ldots$

Grupa ta jest oczywiście cykliczną, zatem abelową. Rozróżnimy dalej dla każdego elementu a grupy G dwa przypadki:

1. Wszystkie potęgi $a^0, a^1, a^2, \ldots$ są różne. Element a grupy G nazywamy wówczas jej *elementem rzędu nieskończonego*.

2. Istnieją takie liczby całkowite $k \geqslant 0$ i $l > 0$, dla których $a^k = a^{k+l}$. Mamy stąd $a^k a^l = a^k$, skąd $(a^k)^{-1} a^k a^l = (a^k)^{-1} a^k$, zatem $a^l = e$. Jeżeli n jest najmniejszą liczbą naturalną, taką że $a^n = e$, to a nazywamy *elementem rzędu n* (grupy G).

Wówczas elementy $a^0, a^1, \ldots, a^{n-1}$ są wszystkie różne i tworzą najmniejszą grupę zawierającą a.

Jeżeli grupa jest skończoną, to może zachodzić oczywiście tylko przypadek 2.

W każdej grupie jedynym elementem rzędu 1 jest jedność grupy.

Każdy element grupy jest oczywiście tego samego rzędu, co jego odwrotność.

PRZYKŁADY. 1. W grupie (nieskończonej), utworzonej ze wszystkich pierwiastków z jedności wszelkich stopni naturalnych, gdzie ab oznacza iloczyn liczb a i b, każdy element jest rzędu skończonego, przy czym istnieją elementy dowolnego rzędu skończonego.

2. W grupie, utworzonej ze wszystkich liczb wymiernych (i podobnie: algebraicznych, rzeczywistych, zespolonych), gdzie ab oznacza sumę liczb a i b, każdy element prócz liczby 0 (która jest jednością grupy) jest rzędu nieskończonego.

3. W grupie, utworzonej ze wszystkich liczb algebraicznych różnych od zera, gdzie ab oznacza iloczyn liczb a i b, istnieje nieskończenie wiele elementów rzędu skończonego (są to pierwiastki dowolnego naturalnego stopnia $n>1$ z jedności i tylko one) oraz nieskończenie wiele elementów rzędu nieskończonego.

4. W grupie, utworzonej ze wszystkich wielomianów o współczynnikach wymiernych (i podobnie: rzeczywistych, zespolonych), gdzie ab oznacza sumę wielomianów a i b, każdy element prócz wielomianu tożsamościowo równego zeru (który jest jednością grupy) jest rzędu nieskończonego.

5. Istnieją grupy nieskończone, w których każdy element, nie będący jednością grupy, jest rzędu 2. Grupą taką jest np. produkt $\Gamma=G\times G\times G\times\ldots$ jednakowych G, utworzonych z liczb 1 i -1, w których iloczynem elementów jest zwykły iloczyn liczb. Grupa Γ jest nieprzeliczalną (mocy continuum).

Chcąc mieć grupę przeliczalną, której każdy element, poza jednością grupy, jest rzędu 2, wystarczyłoby wziąć podgrupę Γ_1 grupy Γ, utworzoną ze wszystkich tych elementów $a=(a_1,a_2,\ldots)$ grupy Γ, które zawierają co najwyżej skończoną liczbę wyrazów równych -1.

Można też utworzyć grupę mocy wyższej niż continuum, której każdy element, poza jednością, jest rzędu 2. Taką jest np. grupa Γ, utworzona ze wszystkich funkcyj zmiennej rzeczywistej, przyjmujących tylko dwie wartości 1 i -1, gdzie iloczynem elementów grupy jest zwykły iloczyn funkcyj. Grupa Γ jest mocy hypercontinuum (t. j. mocy $2^{2^{\aleph_0}}$).

Innym przykładem grupy nieskończonej, której każdy element, poza jednością grupy, jest rzędu 2, jest grupa złożona ze zbioru pustego i ze skończonych zbiorów liczb naturalnych, gdzie ab oznacza zbiór $(a-b)+(b-a)$, t. j. zbiór utworzony z elementów zbioru a nie należących do b oraz z elementów zbioru b nie należących do a. Jednością tej grupy jest zbiór pusty (por. przykład 12 z § 1, str. 308).

Dowiedzione jest, że istnieją grupy nieskończone, których każdy element, nie będący jednością grupy, jest rzędu 3 (a także dowolnie danego rzędu p, gdzie p jest liczbą pierwszą).

Natomiast nie istnieje żadna grupa, której każdy element różny od jej jedności byłby rzędu 4, gdyż jeżeli a jest elementem rzędu 4, to a^2 jest oczywiście elementem rzędu 2.

6. Iloczyn dwóch elementów rzędu 2 może być elementem rzędu nieskończonego. Np. w grupie G wszystkich przekształceń wzajemnie jednoznacznych zbioru wszystkich liczb całkowitych na siebie przekształcenia $f(x)=-x$ oraz $g(x)=1-x$ są rzędu 2, zaś przekształcenie $h(x)=g(f(x))=1+x$ jest rzędu nieskończonego.

Na odwrót, iloczyn dwu elementów rzędu nieskończonego może być elementem rzędu skończonego (np. iloczyn elementu rzędu nieskończonego i jego odwrotności jest elementem rzędu 1).

Natomiast w grupie abelowej iloczyn dwu elementów rzędu skończonego jest zawsze elementem rzędu skończonego, gdyż jeżeli $a^m=e$ i $b^n=e$, to $(ab)^{mn}=a^{mn}b^{mn}=e$. Zatem:

Zbiór wszystkich elementów rzędu skończonego grupy abelowej tworzy jej podgrupę.

Twierdzenie 10. *Dla każdej pary a,b elementów grupy (choćby nie abelowej) elementy ab i ba są tego samego rzędu.*

Dowód. Jeżeli $(ab)^n=e$, to $b(ab)^na=bea=ba$. Lecz $b(ab)^na=(ba)^nba$. Zatem $(ba)^nba=ba$, skąd $(ba)^n=e$.

Tak więc ba nie może być wyższego rzędu niż ab. Oczywiście tak samo na odwrót, skąd równość rzędów, c. b. d. d.

Z twierdzenia 10 wynika natychmiast

Wniosek. *Dla wszelkich elementów a,b,c grupy jej elementy $abc=a(bc)$, $bca=(bc)a=b(ca)$ i $cab=(ca)b$ są tego samego rzędu.*

Natomiast rząd elementów acb, bac i cba (który też jest dla wszystkich trzech ten sam) może się różnić od rzędu elementów abc, bca i cab, jak to stwierdzimy na przykładzie w § 16, str. 339.

§ 9. Podgrupy przekształcone. Podgrupy sprzężone. Dzielniki normalne. Jeżeli a jest elementem grupy G, zaś H jej częścią, to zbiór wszystkich elementów ah, gdzie h jest elementem H, będziemy oznaczali przez aH, zaś zbiór wszystkich elementów ha, gdzie h jest elementem H, przez Ha.

Jeżeli element a grupy G nie należy do H, to ani aH, ani Ha nie jest grupą. Gdyby bowiem aH było grupą, a więc podgrupą grupy G, to aH musiałoby — jak wiemy z § 6, str. 315 — zawierać jedność e grupy G, a więc istniałby taki element h grupy H, iż $ah=e$, skąd byłoby $a=h^{-1}$. Ponieważ jednak h jest elementem H, więc z założenia, że H jest grupą, wynika że h^{-1} też jest elementem H; zatem a byłoby elementem H wbrew założeniu. Podobnie dowodzi się, że Ha nie jest grupą.

Udowodnimy natomiast

Twierdzenie 11. *Dla każdego elementu a grupy G, jeżeli H jest jej podgrupą, to zbiór $a^{-1}Ha$ jest grupą.*

Dowód. Jeżeli h_1 i h_2 są elementami podgrupy H grupy G, to $(a^{-1}h_1a)(a^{-1}h_2a)=(a^{-1}h_1)(aa^{-1})(h_2a)=(a^{-1}h_1)(h_2a)=a^{-1}(h_1h_2)a$, skąd wynika, że iloczyn dwu elementów zbioru $a^{-1}Ha$ zawsze należy do tego zbioru. Następnie, z uwagi na to, że $a^{-1}ea=a^{-1}a=e$ i że e należy do H, wynika, że e należy do $a^{-1}Ha$. Wreszcie, jeżeli h należy do H, to i h^{-1} należy do H (gdyż H jest grupą), a więc też $(a^{-1}ha)^{-1}=a^{-1}h^{-1}a$ należy do H, zatem odwrotność każdego elementu zbioru $a^{-1}Ha$ należy do tego zbioru. W myśl twierdzenia 5 zbiór $a^{-1}Ha$ jest więc grupą, c. b. d. o.

Grupę $a^{-1}Ha$ nazywamy *przekształconą przy pomocy elementu a.*

Grupy, otrzymane w ten sposób z grupy H (gdy a jest elementem G), nazywamy grupami *sprzężonymi* z podgrupą H grupy G.

Jeżeli wszystkie grupy sprzężone z podgrupą H grupy G są równe H, to H nazywamy *podgrupą wyróżnioną* lub *niezmienną*, albo *dzielnikiem normalnym* grupy G.

Dzielnik normalny grupy G jest to więc każda taka jej podgrupa H, że dla dowolnego elementu a grupy G mamy:

$$a^{-1}Ha=H$$

lub, co na to samo wychodzi:

$$Ha=aH.$$

W szczególności, podgrupa utworzona z samej tylko jedności grupy G jest jej dzielnikiem normalnym.

§ 10. Liczba elementów podgrupy grupy skończonej.

Twierdzenie 12. *Jeżeli H jest podgrupą grupy G i jeżeli dla pewnych elementów a i b grupy G zbiory aH i bH mają element wspólny, to $aH=bH$.*

Dowód. Jeżeli $ah_1=bh_2$, gdzie h_1 i h_2 są elementami H, to h_1^{-1} należy do H (gdyż H jest grupą) oraz dla h należącego do H również $h_2h_1^{-1}h$ należy do H i wzór $ah=ah_1h_1^{-1}h=bh_2h_1^{-1}h$ dowodzi, że ah należy do bH. Wynika stąd, że aH jest zawarte w bH. Podobnie dowodzimy, że bH jest zawarte w aH. Jest więc $aH=bH$, c. b. d. o.

Dla a należącego do G oczywiście a jest elementem aH, gdyż $a=ae$, zaś e należy do H, skoro H jest grupą. W ten sposób dla każdej podgrupy H grupy G mamy rozkład (skończony lub nie) grupy G na składniki rozłączne:

$$G=a_1H+a_2H+\ldots, \tag{16}$$

gdzie $a_1, a_2, \ldots$ są elementami grupy G. Co najwyżej jeden z nich może być podgrupą grupy G (gdyż jeden tylko z nich, wobec ich rozłączności, zawiera jedność grupy G).

Składniki (16) są tej samej mocy co H. Aby ustalić odpowiedniość wzajemnie jednoznaczną między elementami zbiorów aH i H, wystarczy dla h należącego do H elementowi ah przyporządkować element h. W szczególności, jeżeli podgrupa H jest skończona, złożona z m elementów, to każdy ze składników (16) zawiera m elementów. Jeżeli grupa G też jest skończona i zawiera n elementów, to G rozpada się na skończoną liczbę części rozłącznych, zawierających po m elementów, skąd wynika, że m jest dzielnikiem liczby n.

Mamy więc

Twierdzenie 13. *Liczba elementów podgrupy grupy skończonej jest dzielnikiem liczby elementów tej grupy.*

Wniosek 1. *Grupa skończona G, której liczba elementów jest liczbą pierwszą, nie posiada żadnych innych podgrup prócz równej G lub złożonej z jednego tylko elementu* (z jedności grupy G).

Jeżeli bowiem grupa G ma p elementów, gdzie p jest liczbą pierwszą, to w myśl twierdzenia 13 dowolna jej podgrupa może mieć albo p elementów — a wtedy pokrywa się z grupą G — albo 1 element, którym musi być jedność grupy, gdyż jak wiemy z § 6, str. 315, każda podgrupa grupy G zawiera jej jedność.

Dowodzi się, że i twierdzenie odwrotne jest prawdziwe:

Jeżeli grupa G nie posiada żadnych innych podgrup, prócz równej G lub złożonej z jednego tylko elementu, to jest skończoną, a liczba jej elementów jest pierwszą.

Z twierdzenia 13 otrzymujemy też (na mocy określenia rzędu elementu grupy) następujący

Wniosek 2. *Rząd elementu grupy skończonej jest zawsze dzielnikiem liczby jej elementów.*

Wynika stąd, że jeżeli grupa składa się z n elementów, to każdy jej element x spełnia równanie:

$$x^n=e,$$

gdzie e jest jednością grupy.

Możemy to uważać za uogólnienie małego twierdzenia Fermata z Teorji liczb, które jest szczególnym przypadkiem wniosku 2, gdy $n+1$ jest liczbą pierwszą, a grupa składa się z liczb $1,2,\ldots,n$, przy czym ab oznacza resztę z dzielenia iloczynu liczb a i b przez $n+1$ (por. § 1, przykład 6 str. 307).

Na tej drodze można również otrzymać twierdzenie Eulera z Teorji liczb, gdy dla dowolnego naturalnego m grupa składa się ze wszystkich $n=\varphi(m)$ liczb naturalnych nie większych od m i pierwszych względem m, przy czym ab oznacza resztę z dzielenia iloczynu liczb a i b przez m.

Z wniosku 2 wynika też, że jeżeli grupa G ma p elementów, gdzie p jest liczbą pierwszą, to rząd każdego jej elementu a, różnego od jedności grupy, jest równy p. Ciąg $a^0, a^1, \ldots, a^{p-1}$ składa się wówczas z samych różnych elementów grupy G, zatem zawiera wszystkie jej elementy. Grupa G jest więc cykliczną. Mamy zatem

Wniosek 3. *Grupa, której liczba elementów jest pierwszą, jest cykliczną, a każdy jej element jest potęgą każdego innego jej elementu, różnego od jedności grupy.*

Istnieją oczywiście też grupy cykliczne, których liczba elementów jest złożoną (por. § 1, przykład 3, str. 307), a także grupy cykliczne nieskończone (por. § 1, przykład 1, str. 306).

Można dowieść, że dla każdego naturalnego n grupa określona w przykładzie 5 z § 1 (str. 307) jest cykliczna.

Dla danej grupy G i danego jej dzielnika normalnego H oznaczmy przez G_1 zbiór wszystkich różnych zbiorów aH (gdzie a przebiega elementy grupy G). W zbiorze G_1 określmy mnożenie za pomocą wzoru $aH \cdot bH = abH$. Jak łatwo widzieć, przy tak określonym mnożeniu G_1 staje się grupą (której jednością jest zbiór eH, gdzie e jest jednością grupy G).

Grupę tę oznaczamy przez G/H i nazywamy *grupą ilorazową.*

Uwaga. Gdyby H było podgrupą grupy G, lecz nie było jej dzielnikiem normalnym, to iloczyn określony za pomocą wzoru $aH \cdot bH = abH$ mógłby uledz zmianie, gdybyśmy zamiast a i b wzięli inne elementy, należące odpowiednio do aH i bH.

§ 11. Kompleksy i ich iloczyny. Każdy zbiór elementów danej grupy G nazywamy *kompleksem.*

Przez *iloczyn* HK dwu kompleksów grupy G rozumiemy zbiór wszystkich elementów hk, gdzie h jest elementem H, a k jest elementem K.

Iloczyn kompleksów ma własność łączności:

$$(HK)L = H(KL).$$

Twierdzenie 14. *Na to, by iloczyn HK podgrup H i K grupy G był jej podgrupą, potrzeba i wystarcza, żeby było:*

$$HK = KH. \tag{17}$$

Dowód. Załóżmy, że iloczyn HK jest grupą. Jeżeli a jest elementem HK, to na mocy określenia iloczynu kompleksów jest $a=hk$, gdzie h należy do H i k do K. Skoro HK jest grupą, to również a^{-1} należy do HK, zatem $a^{-1}=h_1k_1$, gdzie h_1 należy do H, a k_1 do K. Stąd $a=(a^{-1})^{-1}=(h_1k_1)^{-1}=k_1^{-1}h_1^{-1}$ na mocy wzoru (10) z § 3, str. 311. Skoro zbiory K i H są podgrupami, to z uwagi na to, że h należy do H, a k do K, wnosimy też, że h_1^{-1} należy do H i k_1^{-1} do K. Wzór $a=k_1^{-1}h_1^{-1}$ dowodzi więc, że a jest elementem KH, a zatem że HK jest zawarte w KH.

Z drugiej strony, jeżeli a jest elementem KH, to $a=kh$, gdzie k jest elementem K, a h elementem H, skąd $a^{-1}=h^{-1}k^{-1}$. Skoro H i K są grupami, to h^{-1} należy do H i k^{-1} do K, zatem a^{-1} należy do HK. Ponieważ HK jest z założenia grupą, więc wynika stąd, że a też należy do HK. Zatem KH jest zawarte w HK, a że wyżej znaleźliśmy, iż HK jest zawarte w KH, więc mamy $HK=KH$. Warunek (17) jest więc konieczny.

Na odwrót, załóżmy teraz, że zachodzi równość (17). Jeżeli H i K są podgrupami grupy G, a e oznacza jej jedność, to e należy do H i do K, skąd wobec $e=ee$, e należy do HK. Dalej, jeżeli a należy do HK, to $a=hk$, gdzie h jest elementem H, a k elementem K. Wnosimy stąd (ponieważ H i K są grupami), że h^{-1} należy do H, a k^{-1} do K, zatem $a^{-1}=k^{-1}h^{-1}$ należy do KH, i wobec (17) a^{-1} należy do HK. Wreszcie, jeżeli a i b są elementami HK, to ab należy do $(HK)(HK)$ i w myśl (17), wobec łączności iloczynu kompleksów, ab należy do $H(KH)K=H(HK)K=(HH)(KK)=HK$, gdyż z uwagi, że H i K są grupami, mamy — jak łatwo widzieć — $HH=H$ oraz $KK=K$. Na mocy twierdzenia 5 (§ 6, str. 315), HK jest więc podgrupą grupy G. Warunek (17) jest więc zarazem dostateczny, c. b. d. o.

Jeżeli grupa G jest abelową, to warunek (17) jest oczywiście zawsze spełniony. Z twierdzenia 14 wynika więc następujący

Wniosek. *Iloczyn dwu podgrup grupy abelowej jest zawsze jej podgrupą.*

§ 12. Izomorfizm i automorfizm grup. Przykłady. Jeżeli między elementami dwu grup G i G' istnieje taka odpowiedniość wzajemnie jednoznaczna, przy której wyniki działań określonych w grupach G i G', a dokonanych na odpowiadających sobie elementach tych grup są zawsze odpowiadającymi sobie elementami, to mówimy, że grupy G i G' są *izomorficzne*, a ich rozważaną odpowiedniość nazywamy *izomorfizmem*.

Jeżeli więc a' oznacza ogólnie element grupy G', odpowiadający elementowi a grupy G i rozważana odpowiedniość między elementami grup G i G' jest wzajemnie jednoznaczna, to aby ustalała ona izomorfizm między grupami G i G', potrzeba i wystarcza, żeby dla wszystkich a i b należących do G było:

$$(ab)' = a'b'. \tag{18}$$

W tym bowiem przypadku, oznaczając ogólnie przez $(a')' = a$ element grupy G, odpowiadający elementowi a' grupy G', będziemy mieli na mocy (18) również:

$$(a'b')' = [(ab)']' = ab \quad \text{dla } a' \text{ i } b' \text{ należących do } G'.$$

W szczególnym przypadku, gdy $G = G'$, izomorfizm między grupami G i G' nazywamy *automorfizmem* (grupy G).

Wszystkie grupy nieskończone cykliczne są oczywiście izomorficzne. Wynika stąd natychmiast, że grupa nieskończona może być izomorficzna ze swą częścią właściwą.

Np. grupa wszystkich liczb całkowitych, gdzie ab oznacza sumę liczb a i b, jest izomorficzna ze swą podgrupą, utworzoną z liczb całkowitych parzystych.

Niech dana będzie grupa G i jej element a. Przyporządkujmy każdemu elementowi x grupy G jej element

$$x' = axa^{-1}. \tag{19}$$

Okażemy, że *to przyporządkowanie wyznacza automorfizm grupy* G.

Istotnie, równość (19) daje:

$$a^{-1}x'a = a^{-1}(axa^{-1})a = (a^{-1}a)x(a^{-1}a) = exe = x.$$

Odpowiedniość między x a x' jest więc wzajemnie jednoznaczna; przy tym dla x i y należących do G mamy w myśl (19):

$$x'y' = (axa^{-1})(aya^{-1}) = (ax)(a^{-1}a)(ya^{-1}) = (ax)e(ya^{-1}) = (ax)(ya^{-1}) = a(xy)a^{-1} = (xy)'.$$

Dla każdej grupy G możemy rozważać zbiór wszystkich jej przekształceń wzajemnie jednoznacznych na samą siebie, ustalających automorfizm grupy G.

Zbiór ten stanowi grupę przekształceń.

W grupie abelowej otrzymamy automorfizm, przyporządkowując każdemu elementowi grupy jego element odwrotny. Łatwo też stwierdzamy, że na odwrót: jeżeli takie przyporządkowanie daje automorfizm grupy, to jest ona abelową. Wówczas bowiem mamy dla a i b należących do G:

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

a że wobec (10):

$$(a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba,$$

więc $ab = ba$, czyli grupa jest przemienna.

Dowodzi się, że grupa cykliczna nieskończona posiada jeden tylko automorfizm nie będący tożsamością, mianowicie ten, przy którym każdy element grupy przechodzi na swój element odwrotny.

Istnieją atoli grupy przeliczalne, mające nieprzeliczalną mnogość automorfizmów.

Taką jest np. grupa, utworzona ze wszystkich funkcyj liczbowych (t. j. funkcyj zmiennej naturalnej), przyjmujących tylko dwie wartości: $+1$ i -1, z których wartość -1 tylko co najwyżej skończoną liczbę razy, przy czym iloczynem elementów grupy jest zwykły iloczyn funkcyj. Otrzymamy bowiem automorfizm dla tej grupy, przyporządkowując każdej należącej do niej funkcji $f(n)$ funkcję $f(\varphi(n))$, gdzie $\varphi(n)$ jest dowolną (ale stałą dla wszystkich elementów grupy) permutacją ciągu nieskończonego liczb naturalnych.

PRZYKŁADY. 1. Niech grupa G składa się z czterech liczb $1, -1, i$ oraz $-i$, a jej działaniem niech będzie zwykłe mnożenie liczb. Otrzymamy automorfizm tej grupy, jeżeli elementom $1, -1, i, -i$ przyporządkujemy odpowiednio elementy $1, -1, -i, i$.

2. Grupa G, utworzona ze wszystkich pierwiastków n-go stopnia z jedności, gdzie działaniem jest zwykłe mnożenie liczb, jest izomorficzna z grupą G', utworzoną z liczb $0,1,2,\ldots,n-1$, gdzie ab jest resztą z dzielenia sumy liczb a i b przez n. Aby otrzymać izomorfizm grup G i G', wystarczy elementom $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ grupy G, gdzie ε oznacza pierwiastek pierwotny n-go stopnia z jedności, przyporządkować odpowiednio elementy $0,1,2,\ldots,n-1$ grupy G'.

3. Niech G_1 oznacza zbiór wszystkich liczb postaci $k+l\sqrt{2}$, gdzie liczby k i l są całkowite; niech dalej G_2 oznacza zbiór wszystkich liczb wymiernych, a G_3 zbiór wszystkich liczb algebraicznych. Każdy z tych zbiorów będzie oczywiście grupą, jeżeli przez ab rozumieć będziemy sumę liczb a i b.

Okażemy, że grupa G_1 nie jest izomorficzna z żadną podgrupą grupy G_2.

Istotnie, jeżeli a i b są jakimikolwiek elementami grupy G_2, różnymi od jej jedności (którą jest liczba 0), to istnieją liczby całkowite, różne od zera, t i u, takie iż $a^t=b^u$ (w grupie G_2). Jeżeli bowiem $a=\frac{m}{n}$ i $b=\frac{p}{q}$, gdzie liczby m i p są całkowite różne od zera, zaś liczby n i q są naturalne, to w grupie G_2 będzie $a^{np}=b^{mq}$. Gdyby grupa G_1 była izomorficzna z pewną podgrupą grupy G_2, to i każde dwa elementy grupy G_1 posiadałyby taką własność. Tak jednak nie jest, gdyż dla $a=1$ i $b=\sqrt{2}$ równość $a^t=b^u$ oznaczałaby w grupie G_1, że $t=u\sqrt{2}$, co jest niemożliwe przy t i u całkowitych różnych od zera.

Ponieważ G_1 jest podgrupą grupy G_3, więc wynika też stąd, że grupa G_3 nie jest izomorficzna z żadną podgrupą grupy G_2. Tym bardziej więc grupy G_2 i G_3 nie są izomorficzne.

Okażemy teraz, że i na odwrót: grupa G_2 nie jest izomorficzna z żadną podgrupą grupy G_1.

Istotnie, dla każdego elementu a grupy G_2, w szczególności dla elementu a równego liczbie 1, oraz dla każdej liczby naturalnej n istnieje w grupie G_2 element x_n taki, iż (w tej grupie) $x_n^n=a$. Gdyby grupa G_2 była izomorficzna z pewną podgrupą grupy G_1, to w tym izomorfizmie elementom a i x_n grupy G_2 odpowiadałyby takie elementy a' i x_n' (gdzie $n=1,2,\ldots$) grupy G_1, iż byłoby $(x_n')^n=a'$ dla $n=1,2,\ldots$ (w grupie G_1). Jeżeli $a'=k+l\sqrt{2}$ i $x_n'=k_n+l_n\sqrt{2}$ dla $n=1,2,\ldots$, to w grupie G_1 mielibyśmy $nk_n+nl_n\sqrt{2}=k+l\sqrt{2}$, skąd $nk_n=k$ i $nl_n=l$ dla $n=1,2,\ldots$, co daje $k=0$ i $l=0$, zatem $a'=0$. Element a' byłby więc jednością grupy G_1; wówczas jednak na mocy twierdzenia ogólnego, które podamy w § 13 (ob. twierdzenie 15, str. 334), element a musiałby być jednością grupy G_2, t. j. byłoby $a=0$, gdy tymczasem $a=1\neq 0$.

Żadna więc z grup G_1 i G_2 nie jest izomorficzna z żadną częścią drugiej.

4. Niech G_1 będzie grupą, utworzoną ze wszystkich pierwiastków z jedności wszelkich naturalnych stopni, gdzie ab oznacza iloczyn liczb a i b; niech G_2 będzie grupą, utworzoną ze wszystkich liczb wymiernych nieujemnych mniejszych od 1, gdzie ab oznacza liczbę $a+b-\mathrm{E}(a+b)$ [1]).

Grupy G_1 i G_2 są izomorficzne. Istotnie, każda liczba grupy G_1 daje się w jeden i tylko jeden sposób przedstawić w postaci $\cos 2w\pi+i\sin 2w\pi$, gdzie w jest liczbą wymierną nieujemną mniejszą od 1, przy czym:

$$(\cos 2w_1\pi+i\sin 2w_1\pi)(\cos 2w_2\pi+i\sin 2w_2\pi)=$$
$$=\cos 2[(w_1+w_2)-\mathrm{E}(w_1+w_2)]\pi+i\sin 2[(w_1+w_2)-\mathrm{E}(w_1+w_2)]\pi.$$

Aby ustalić izomorfizm grup G_1 i G_2, wystarczy każdemu elementowi $r=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$ grupy G_1 (gdzie $k=0,1,\ldots,n-1$) przyporządkować liczbę k/n.

5. Grupa, utworzona z sześciu macierzy:

$$\left\|\begin{matrix}1&0\\0&1\end{matrix}\right\|,\quad \left\|\begin{matrix}-1&1\\-1&0\end{matrix}\right\|,\quad \left\|\begin{matrix}0&-1\\1&-1\end{matrix}\right\|,\quad \left\|\begin{matrix}0&1\\1&0\end{matrix}\right\|,\quad \left\|\begin{matrix}-1&0\\-1&1\end{matrix}\right\|,\quad \left\|\begin{matrix}1&-1\\0&-1\end{matrix}\right\|,$$

gdzie działaniem jest mnożenie macierzy, jest izomorficzna z grupą (nie abelową) podstawień:

$$1,\quad (1\ 2\ 3),\quad (1\ 3\ 2),\quad (1\ 2),\quad (1\ 3),\quad (2\ 3).$$

Natomiast pierwsze trzy z tych macierzy tworzą grupę izomorficzną z grupą abelową podstawień:

$$1,\quad (1\ 2\ 3),\quad (1\ 3\ 2).$$

Gdybyśmy do tych trzech macierzy dołączyli jeszcze macierze:

$$\left\|\begin{matrix}-1&0\\0&-1\end{matrix}\right\|,\quad \left\|\begin{matrix}1&-1\\1&0\end{matrix}\right\|,\quad \left\|\begin{matrix}0&1\\-1&1\end{matrix}\right\|,$$

otrzymalibyśmy grupę izomorficzną z grupą pierwiastków 6-go stopnia z jedności [2]).

---

[1]) E znaczy tu „entier“ (ob. str. 219, odnośnik).

[2]) Ob. G. A. Miller, H. F. Blichfeldt, L. E. Dickson, *Theory and Applications of Finite Groups*, New York 1916, str. 13.

§ 13. Własności izomorfizmu. Grupy a podstawienia.

Udowodnimy zapowiedziane w przykładzie 3, str. 332:

Twierdzenie 15. *Przy izomorfizmie grup G i G' jedność grupy G przechodzi na jedność grupy G', zaś element odwrotny każdego elementu a grupy G na element odwrotny odpowiedniego elementu a' grupy G'.*

Dowód. Jeżeli e oznacza jedność grupy G, zaś a dany jej element, to — jak wiemy — zachodzi równość (1) z § 2, str. 310, skąd wobec $(ae)'=a'e'$ i $(ea)'=e'a'$ (gdyż grupy G i G' są z założenia izomorficzne):

$$a'e'=e'a'=a';$$

wobec dowolności elementu a' grupy G' dowodzi to, że e' jest jednością grupy G'.

Jeżeli teraz a^{-1} oznacza element odwrotny elementu a grupy G, to:

$$aa^{-1}=e,$$

skąd:

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

co wobec twierdzenia 2 (§ 3, str. 311) dowodzi, że $(a^{-1})'$ jest (w grupie G') elementem odwrotnym elementu a', czyli że $(a^{-1})'=(a')^{-1}$.

Z pierwszej części twierdzenia 15 wynika

Wniosek. *Przy izomorfizmie grup odpowiednie elementy mają ten sam rząd.*

Twierdzenie 16. *Każda grupa złożona z n elementów jest izomorficzna z pewną podgrupą grupy $n!$ podstawień ciągu liczb $1,2,\ldots,n$.*

Dowód. Niech G oznacza grupę złożoną z n elementów $a_1,a_2,\ldots,a_n$. Dla każdego a z grupy G iloczyny a_1a, a_2a, ..., a_na, tworzą — jak to wynika z własności 2° pojęcia grupy — ciąg różniący się co najwyżej porządkiem wyrazów od ciągu $a_1,a_2,\ldots,a_n$. Niech to będzie ciąg $a_{k_1},a_{k_2},\ldots,a_{k_n}$. Ciąg wskaźników $k_1,k_2,\ldots,k_n$ jest więc permutacją ciągu $1,2,\ldots,n$. Przyporządkujmy elementowi a grupy G podstawienie:

$$\begin{pmatrix}1 & 2 & \ldots & n\\ k_1 & k_2 & \ldots & k_n\end{pmatrix}.$$

Otóż *zbiór wszystkich podstawień, przyporządkowanych w ten sposób elementom grupy G, tworzy grupę izomorficzną z grupą G.*

Istotnie, niech a i b będą dowolnymi elementami grupy G. Mamy więc:

(19) $$a_ia=a_{k_i} \quad \text{i} \quad a_ib=a_{l_i} \quad \text{dla } i=1,2,\ldots,n,$$

gdzie ciągi $k_1,k_2,\ldots,k_n$ i $l_1,l_2,\ldots,l_n$ są dwiema permutacjami ciągu $1,2,\ldots,n$. W myśl przyjętego przyporządkowania elementowi a grupy G odpowiada podstawienie $a'=\begin{pmatrix}1 & 2 & \ldots & n\\ k_1 & k_2 & \ldots & k_n\end{pmatrix}$, zaś elementowi b podstawienie $b'=\begin{pmatrix}1 & 2 & \ldots & n\\ l_1 & l_2 & \ldots & l_n\end{pmatrix}$.

Wobec (19) mamy $a_iab=a_{k_i}b=a_{l_{k_i}}$ dla $i=1,2,\ldots,n$. Elementowi ab grupy G odpowiada więc podstawienie:

$$(ab)'=\begin{pmatrix}1 & 2 & \ldots & n\\ l_{k_1} & l_{k_2} & \ldots & l_{k_n}\end{pmatrix}.$$

Lecz, jak wiemy (ob. Rozdział XVIII, § 2, str. 301):

$$\begin{pmatrix}1 & 2 & \ldots & n\\ k_1 & k_2 & \ldots & k_n\end{pmatrix}\begin{pmatrix}1 & 2 & \ldots & n\\ l_1 & l_2 & \ldots & l_n\end{pmatrix}=\begin{pmatrix}1 & 2 & \ldots & n\\ l_{k_1} & l_{k_2} & \ldots & l_{k_n}\end{pmatrix}.$$

Mamy więc $(ab)'=a'b'$, co wobec dowolności elementów a i b grupy G dowodzi, że przyjęte przyporządkowanie ustala izomorfizm grupy G z pewną częścią zbioru wszystkich $n!$ podstawień dla ciągu $1,2,\ldots,n$. Udowodniliśmy więc twierdzenie 16.

Z twierdzenia 16 wynika, że *Teoria grup skończonych sprowadza się do Teorii grup podstawień.* Można by więc też powiedzieć, że Teoria grup skończonych jest równoważna Teorii grup podstawień (dla skończonego ciągu elementów).

Uogólniając twierdzenie 16, można dowieść, że każda grupa (skończona lub nieskończona) G jest izomorficzna z pewną podgrupą grupy wszystkich przekształceń wzajemnie jednoznacznych zbioru G na siebie. Wynika stąd, że grupa wszystkich przekształceń wzajemnie jednoznacznych zbioru dowolnej mocy $\mathfrak{m}$ na siebie ma tę własność, że dla każdej grupy mocy $n\leqslant\mathfrak{m}$ zawiera podgrupę z nią izomorficzną.

Nie wiadomo natomiast, czy istnieje grupa przeliczalna, zawierająca dla każdej grupy przeliczalnej podgrupę z nią izomorficzną. Pp. Mazur i Ulam twierdzą[1]), że udowodnili istnienie grupy przeliczalnej abelowej, zawierającej dla każdej grupy przeliczalnej abelowej podgrupę z nią izomorficzną.

Można by stąd dalej wywnioskować, że dla każdego zbioru Z grup istnieje grupa, zawierająca dla każdej grupy zbioru Z podgrupę z nią izomorficzną.

[1]) Ob. S. Mazur i S. Ulam, Rocznik Polskiego Towarzystwa Matematycznego, Tom 9 (1930), str. 204.

§ 14. Grupy, których liczba elementów jest liczbą pierwszą. Ich automorfizmy. Dwie grupy izomorficzne mogą być uważane za różniące się tylko znakowaniem. Wobec tego ważnym jest pytanie, jakie grupy można tworzyć z danych elementów (przy różnych określeniach działania grupy), tak by żadne dwie nie były izomorficzne.

Niech p będzie liczbą pierwszą, a G grupą złożoną z p elementów. Niech e oznacza jedność grupy G i $a \neq e$ jakikolwiek jej element. W myśl wniosku 3 z twierdzenia 13 (§ 10, str. 328) grupa G składa się z potęg elementu a, od zerowej do $(p-1)$-ej włącznie.

Wynika stąd, że dwie grupy, złożone każda z p elementów, gdzie p jest liczbą pierwszą, są izomorficzne. Bo niech G_1 oznacza grupę złożoną z p elementów i a_1 jej element różny od jej jedności. Grupa G_1 jest więc utworzona z elementów $a_1^0, a_1^1, \ldots, a_1^{p-1}$. Aby ustalić odwzorowanie izomorficzne grup G i G_1, oczywiście wystarczy przyporządkować elementom $a^0, a^1, \ldots, a^{p-1}$ grupy G odpowiednio elementy $a_1^0, a_1^1, \ldots, a_1^{p-1}$ grupy G_1. Mamy zatem

Twierdzenie 17. *Dwie grupy, których liczba elementów jest tą samą liczbą pierwszą, są izomorficzne.*

Ogólniej, dowodzi się w sposób analogiczny, że *dwie grupy cykliczne o tej samej liczbie elementów są zawsze izomorficzne.*

W szczególności, jeżeli grupa G składa się z p elementów, gdzie p jest liczbą pierwszą, to grupa G jest izomorficzna z grupą, utworzoną ze wszystkich pierwiastków p-go stopnia z jedności, gdzie mnożenie grupy jest zwykłym mnożeniem liczb zespolonych. Jest ona również izomorficzna z grupą utworzoną z liczb $0,1,2,\ldots,p-1$, gdzie ab oznacza resztę z dzielenia sumy liczb a i b przez p (por. § 12, przykład 2, str. 331).

Wniosek 1. *Każda grupa skończona, której liczba elementów jest pierwszą, jest grupą cykliczną, a zatem abelową.*

Jako inny łatwy wniosek z twierdzenia 17 wyprowadzimy

Wniosek 2. *Grupa, której liczba elementów p jest liczbą pierwszą, posiada $p-2$ automorfizmów, nie będących tożsamością* [1]).

[1]) Ogólniej, można okazać, że grupa cykliczna o n elementach posiada $\varphi(n)-1$ automorfizmów, nie będących tożsamością (gdzie $\varphi(n)$ oznacza funkcję liczbową Gauss'a; ob. Rozdział VI, § 8, str. 95).

Możemy bowiem, dla otrzymania automorfizmu grupy G przyporządkować jej elementowi $a \neq e$ dowolny inny jej element $b \neq e$, przez co elementom $a^0, a^1, \ldots, a^{p-1}$ będą przyporządkowane odpowiednio elementy $b^0, b^1, \ldots, b^{p-1}$.

W szczególności, *grupa złożona z dwu elementów nie posiada żadnego automorfizmu, nie będącego tożsamością.*

Badanie grup skończonych, których liczba elementów jest pierwszą, możemy uważać w ten sposób za wyczerpane. Znacznie trudniejszym jest badanie grup skończonych, których liczba elementów jest złożoną. Najprostszym przypadkiem są tu grupy 4-elementowe.

§ 15. Grupy o 4 elementach. Z 4 elementów: e (jedność grupy), a, b i c można utworzyć dwie grupy (abelowe) G_1 i G_2, w których mnożenia są określone odpowiednio za pomocą następujących tabliczek:

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Pierwszą z nich otrzymuje się, przyjmując:

$$e=1, \quad a=i, \quad b=i^2=-1 \quad \text{i} \quad c=i^3=-i,$$

przy czym iloczyn elementów grupy jest zwykłym iloczynem liczb.

Drugą otrzymuje się, przyjmując:

$$e=1, \quad a=3, \quad b=5 \quad \text{i} \quad c=7,$$

przy czym iloczyn elementów grupy jest resztą z dzielenia zwykłego iloczynu tych elementów przez liczbę 8. Grupa ta jest też izomorficzna — jak łatwo sprawdzić — z grupą utworzoną z 4 funkcyj:

$$x, \quad -x, \quad \frac{1}{x} \quad \text{i} \quad -\frac{1}{x},$$

gdzie fg oznacza funkcję $f(g(x))$.

Że grupy G_1 i G_2 nie są izomorficzne, wynika już stąd, że pierwsza zawiera elementy (a i c), których kwadraty nie są jednością grupy, druga zaś takich elementów nie zawiera.

Niech teraz G oznacza jakąkolwiek grupę, złożoną z 4 elementów: e (jedność grupy), a, b i c. W myśl wniosku 2 z twierdzenia 13 (str. 327) rząd elementów grupy G musi być dzielnikiem liczby 4, a więc jest jedną z trzech liczb 1, 2, 4.

Jeżeli istnieje w grupie G element rzędu 4, np. a, to grupa ta jest cykliczna, a zatem izomorficzna z grupą G_1 (ponieważ wszystkie grupy cykliczne złożone z 4 elementów są izomorficzne).

Jeżeli zaś w grupie G nie ma elementu rzędu 4, to każdy z elementów a, b, c jest rzędu 2. Mamy więc $ae=a$ i $aa=e$, a przeto (wobec twierdzenia 3) ab jest różne od a i od e. Lecz nie może być $ab=b$, gdyż $eb=b$, zaś $a\neq e$. Musi więc być $ab=c$. Podobnie wnosimy, że iloczyn każdych dwu elementów grupy G, różnych między sobą i różnych od jedności grupy, jest różny od każdego z tych elementów i od jedności grupy, a zatem iloczyn ten jest pozostałym (czwartym) elementem grupy G. Dla grupy G zachodzi więc ta sama tabliczka mnożenia, co dla grupy G_2: grupy te są więc izomorficzne.

Dowiedliśmy tym sposobem, że *każda grupa złożona z 4 elementów jest izomorficzna bądź z grupą G_1, bądź z grupą G_2.*

W obrębie grup złożonych z 4 elementów można więc utworzyć dwie i tylko dwie grupy, które nie są izomorficzne.

Co do automorfizmów w grupach złożonych z 4 elementów, to dla grupy G_1 otrzymamy przekształcenie automorficzne, zastępując wzajemnie przez siebie elementy a i c, przy czym jest to jedyne przekształcenie automorficzne grupy G_1, nie będące tożsamościowym. Dla grupy zaś G_2 otrzymamy automorfizmy, dokonując dowolnej permutacji elementów a, b, c. Mamy więc dla tej grupy 5 różnych automorfizmów, nie będących tożsamością.

Grupa G_1 ma jedną tylko podgrupę różną od niej i nie jednostkową, mianowicie podgrupę złożoną z elementów e i b, zaś grupa G_2 ma 3 takie podgrupy (mianowicie podgrupy złożone z elementów e i a, e i b oraz e i c).

§ 16. Grupy o 6 i więcej elementach. Ponieważ każda grupa złożona z 4 elementów jest abelowa, więc na mocy wniosku 3 z twierdzenia 13 (str. 328), w myśl którego każda grupa, której liczba elementów jest pierwszą, jest grupą cykliczną, a więc abelową, stwierdzamy, że *każda grupa mająca mniej niż 6 elementów jest abelową.*

Inaczej jest jednak dla grup złożonych z 6 elementów. Tutaj już grupa wszystkich $3!=6$ podstawień dla ciągu 1, 2, 3 nie jest abelową.

Przyjmując:

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

$$c=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad d=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad f=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$

otrzymamy następującą tabliczkę mnożenia:

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Mamy tu $ac=f$ i $ca=d$, zatem $ac\neq ca$. Grupa nie jest więc abelową.

Mamy tu też $(ca)^2=d^2=e$ i $c^2a^2=eb=b$, zatem $(ca)^2\neq c^2a^2$.

Zbiór wszystkich rozwiązań równania $x^2=e$ składa się tu (jak wskazuje tabliczka) z elementów e, c, d i f, zatem nie tworzy grupy, gdyż $cd=a$ (por. § 6, przykład 4, str. 317). Natomiast zbiór kwadratów wszystkich elementów grupy tworzy jej podgrupę (złożoną z elementów e, a i b). Lecz zbiór sześcianów wszystkich elementów grupy nie tworzy już podgrupy, gdyż $e^3=a^3=b^3=e$, $c^3=c$, $d^3=d$ i $f^3=f$, ale $cd=a$.

Mamy tu dalej:

$$bcf=df=a,\qquad fcb=ab=e,\qquad bfc=cc=e,\qquad cbf=ff=e,$$

a że $a^2=b\neq e$, więc element bcf jest innego rzędu niż każdy z elementów fcb, bfc i cbf [1]) (por. § 8, str. 325).

Istnieje też oczywiście grupa abelowa złożona z 6 elementów, np. grupa (cykliczna) wszystkich pierwiastków 6-go stopnia z jedności.

Można okazać, że *każda grupa złożona z 6 elementów jest izomorficzna z jedną z tych dwu grup.*

[1]) Ob. L. Baumgartner, *Gruppentheorie*, Sammlung Göschen 1921, str. 39, zadanie 11.

Można dalej okazać, że wśród grup utworzonych z 8 elementów istnieje 5 nie izomorficznych między sobą i takich, że każda grupa utworzona z 8 elementów jest izomorficzna z jedną z nich; spośród tych pięciu grup 3 są abelowe.

Z 9 elementów można utworzyć tylko 2 grupy nie izomorficzne między sobą; obie są abelowe.

Z 10 elementów można utworzyć również tylko dwie grupy: jedną abelową, drugą nie abelową.

Z 12 elementów można utworzyć aż 5 grup, z nich 2 abelowe.

Następująca tablica [1]) podaje ilość g_n grup nie izomorficznych między sobą, jakie można utworzyć z n elementów dla $n<32$:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
g_n	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14
n	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
g_n	1	5	1	5	2	2	1	15	2	2	5	4	1	4	1

Z przeliczalnej mnogości elementów można utworzyć nieprzeliczalnie wiele (mianowicie continuum) grup abelowych i tyleż nie abelowych, z których żadne dwie nie są izomorficzne.

§ 17. Homomorfizm. Endomorfizm. Niech teraz każdemu elementowi a grupy G przyporządkowany będzie pewien element $f(a)$ grupy G_1 w sposób jednoznaczny (ale niekoniecznie wzajemnie jednoznaczny, t. j. różnym elementom grupy G może odpowiadać jeden ten sam element grupy G_1), a przy tym taki, że wzór

$$ab=c \tag{20}$$

dla elementów grupy G pociąga za sobą zawsze wzór

$$f(a)f(b)=f(c) \tag{21}$$

dla elementów grupy G_1.

Okażemy, że zbiór $f(G)$ wszystkich elementów $f(x)$ grupy G_1, przyporządkowanych w ten sposób elementom x grupy G, tworzy grupę (podgrupę grupy G_1, mogącą być równą G_1).

Istotnie, jeżeli a_1 i b_1 są elementami zbioru $f(G)$, to w myśl określenia tego zbioru istnieją takie elementy a i b grupy G, że:

$$a_1=f(a) \quad \text{i} \quad b_1=f(b). \tag{22}$$

[1]) Ob. W. Burnside, *The Theory of Groups of Finite Order*, Wydanie 2-e, Cambridge 1911, str. 160 i 145-146.

Niech $c=ab$. Jest to więc element grupy G i będziemy mieli wzór (20), który—jak założyliśmy—pociąga za sobą wzór (21) czyli wobec (22) wzór:

$$a_1b_1=f(c),$$

gdzie $f(c)$ jest elementem zbioru $f(G)$, gdyż c jest elementem zbioru G. Dowiedliśmy więc, że jeżeli a_1 i b_1 należą do $f(G)$, to i a_1b_1 należy do $f(G)$.

Niech dalej e oznacza jedność grupy G i niech $e_1=f(e)$. Wobec $ee=e$ mamy dla $a=b=c=e$ wzór (20), zatem też i wzór (21) czyli wzór $e_1e_1=e_1$, który—jak wiemy z twierdzenia 3 (str. 312)—dowodzi, że e_1 jest jednością grupy G_1. Element $f(e)=e_1$ jest więc jednością grupy G_1.

Niech teraz a_1 oznacza jakikolwiek element zbioru $f(G)$. Istnieje więc taki element a grupy G, iż $a_1=f(a)$. Niech $a_1'=f(a^{-1})$. Jest to również element zbioru $f(G)$, przy czym na mocy określenia odpowiedniości f mamy:

$$a_1a_1'=f(a)f(a^{-1})=f(aa^{-1})=f(e)=e_1;$$

na mocy twierdzenia 2 (str. 311) dowodzi to, że $a_1'=a^{-1}$. Zbiór $f(G)$ zawiera zatem dla każdego ze swych elementów element odwrotny. Tak więc dowiedliśmy, że zbiór $f(G)$ spełnia warunki (i) i (ii) twierdzenia 5 (str. 315), a przeto na mocy tego twierdzenia jest on grupą, c. b. d. o.

Grupę $f(G)$ nazywamy *homomorficzną* z grupą G, a przyporządkowanie f *homomorfizmem* [1]).

Szczególnym przypadkiem homomorfizmu jest izomorfizm, mianowicie gdy $f(a)$ jest odwzorowaniem wzajemnie jednoznacznym.

Odwzorowanie homomorficzne grupy na jej część nazywamy *endomorfizmem*.

Podgrupa dowolnej grupy G_1, utworzona z jednego tylko elementu, mianowicie z jedności e_1 grupy G_1, jest homomorficzna z dowolną grupą G.

Aby otrzymać ten homomorfizm, wystarczy przyjąć $f(a)=e_1$ dla każdego elementu a grupy G.

[1]) Niektórzy autorzy nazywają homomorfizm izomorfizmem *meriedrycznym* czyli *częściowym* (lub *wielostopniowym*), zaś izomorfizm w naszym znaczeniu izomorfizmem *holoedrycznym* czyli *całkowitym* (lub *jednostopniowym*).

Dla grupy abelowej łatwo otrzymać endomorfizm, mianowicie przez odwzorowanie $f(a)=a^2$, lub ogólniej $f(a)=a^k$, gdzie k jest daną liczbą całkowitą.

Dla grup nie abelowych może tak nie być, nawet jeżeli zbiór $f(G)$ jest grupą. Np. dla grupy z 6 elementów, badanej w § 16, mamy $(ca)^2=c^2a^2$. Grupa ilorazowa G/H (ob. § 10, str. 328) jest homomorficzna z grupą G: homomorfizm ten ustala, jak łatwo widzieć, funkcja $f(x)=xH$.

Twierdzenie 18. *Dla każdej grupy Γ, homomorficznej z daną grupą G, istnieje taki dzielnik normalny H grupy G, iż grupa Γ jest izomorficzna z grupą G/H.*

Dowód. Niech f oznacza przekształcenie homomorficzne grupy G na grupę Γ i niech e oznacza jedność grupy G. Oznaczmy przez H zbiór wszystkich tych elementów h grupy G, dla których $f(h)=f(e)$. Jak łatwo sprawdzić, H będzie dzielnikiem normalnym grupy G.

Przyporządkujmy teraz każdemu elementowi α grupy Γ element grupy G/H, będący zbiorem wszystkich elementów grupy G postaci ah, gdzie h należy do H i gdzie a jest takim elementem grupy G, iż $f(a)=\alpha$. Można dowieść z łatwością, że przyporządkowanie to ustala izomorfizm między grupami Γ i G/H.

§ 18. Grupy podstawień, nie zmieniających wielomianu n zmiennych. Jeżeli $f(x_1,x_2,\ldots,x_n)$ jest wielomianem (lub ogólniej, funkcją) n zmiennych $x_1,x_2,\ldots,x_n$, to wszystkie podstawienia zamiast ciągu $x_1,x_2,\ldots,x_n$ takiej permutacji zmiennych, po której dokonaniu f nie ulega zmianie dla żadnego układu wartości zmiennych (czyli pozostaje tym samym wielomianem), tworzą grupę.

Jeżeli bowiem tożsamościowo:

$$f(x_1,x_2,\ldots,x_n)=f(x_{\alpha_1},x_{\alpha_2},\ldots,x_{\alpha_n}), \tag{23}$$

$$f(x_1,x_2,\ldots,x_n)=f(x_{\beta_1},x_{\beta_2},\ldots,x_{\beta_n}), \tag{24}$$

to z (23) wynika tożsamość:

$$f(x_{\beta_1},x_{\beta_2},\ldots,x_{\beta_n})=f(x_{\beta_{\alpha_1}},x_{\beta_{\alpha_2}},\ldots,x_{\beta_{\alpha_n}}),$$

skąd wobec (24) znajdujemy tożsamość:

$$f(x_1,x_2,\ldots,x_n)=f(x_{\beta_{\alpha_1}},x_{\beta_{\alpha_2}},\ldots,x_{\beta_{\alpha_n}}).$$

Zatem iloczyn dwu podstawień nie zmieniających f również nie zmienia f, skąd wnosimy na mocy twierdzenia 6 (str. 316), że podstawienia nie zmieniające f tworzą grupę.

Jeżeli funkcja f jest symetryczna względem zmiennych $x_1,x_2,\ldots,x_n$, to — jak wiemy z określenia (ob. Rozdział IX, § 1, str. 157) — nie ulegnie ona zmianie przy żadnym z $n!$ podstawień (w obrębie permutacyj ciągu $x_1,x_2,\ldots,x_n$).

Z tego względu grupa wszystkich $n!$ podstawień nazywa się *grupą symetryczną*.

Dla

$$f(x_1,x_2,\ldots,x_n)=\prod_{k=2}^{n}\prod_{l=1}^{k-1}(x_k-x_l)$$

grupą wszystkich podstawień nie zmieniających f jest, oczywiście, grupa wszystkich $n!/2$ podstawień, będących iloczynami parzystej liczby transpozycyj.

Nazywamy ją grupą *naprzemienną*, gdyż funkcja f zmienia znak przy każdej transpozycji zmiennych.

Dla

$$f(x_1,x_2,x_3,x_4)=x_1x_2+x_3x_4$$

możemy oczywiście, nie zmieniając f, zamiast permutacji 1 2 3 4 wskaźników przy zmiennych, brać permutacje:

1243, 2134, 2143, 3412, 4312, 3421, 4321

i tylko te permutacje. Grupa podstawień nie zmieniających f składa się tu więc z 8 podstawień (wliczając oczywiście i podstawienie tożsamościowe).

Udowodnimy teraz

Twierdzenie 19. *Dla każdej podgrupy G grupy wszystkich $n!$ podstawień (dokonywanych na ciągu $x_1,x_2,\ldots,x_n$) istnieje wielomian n zmiennych $f(x_1,x_2,\ldots,x_n)$, który (dla żadnego układu wartości tych zmiennych) nie zmienia swej wartości przy podstawieniach należących do G i tylko przy takich podstawieniach.*

Dowód. Jeżeli W jest jednomianem:

$$W=W(x_1,x_2,\ldots,x_n)=x_1x_2^2x_3^3\ldots x_n^n, \tag{25}$$

a S podstawieniem:

$$S=\begin{pmatrix}1 & 2 & \ldots & n\\ \alpha_1 & \alpha_2 & \ldots & \alpha_n\end{pmatrix}, \tag{26}$$

to przez W_S będziemy oznaczali jednomian:

$$W_S = W(x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_n}) = x_{\alpha_1} x_{\alpha_2}^2 x_{\alpha_3}^3 \ldots x_{\alpha_n}^n. \tag{27}$$

Niech $S_1=1$, S_2, S_3, ..., S_m będą wszystkimi podstawieniami tworzącymi grupę G i niech:

$$f(x_1, x_2, \ldots, x_n) = W_{S_1} + W_{S_2} + \ldots + W_{S_m}. \tag{28}$$

Dla S danego wzorem (26) oznaczmy przez f_S funkcję:

$$f_S = f(x_{\alpha_1}, x_{\alpha_1}, \ldots, x_{\alpha_n}). \tag{29}$$

Jeżeli podstawienie S należy do grupy G, to ciąg podstawień

$$S_1 S,\ S_2 S,\ \ldots,\ S_m S$$

będzie się różnił co najwyżej porządkiem wyrazów od ciągu $S_1, S_2, \ldots, S_m$, skąd wnosimy, że:

$$W_{S_1 S} + W_{S_2 S} + \ldots + W_{S_m S} = W_{S_1} + W_{S_2} + \ldots + W_{S_m}, \tag{30}$$

a zatem wobec (28), (26), (27) i (29):

$$f_S = f \tag{31}$$

dla każdego podstawienia S należącego do grupy G oraz dla każdego układu wartości $x_1, x_2, \ldots, x_n$.

Okażemy teraz, że jeżeli S jest podstawieniem nie należącym do grupy G, to równość (31) nie może zachodzić tożsamościowo względem $x_1, x_2, \ldots, x_n$.

Istotnie przypuśćmy, że dla podstawienia (26) mamy równość (31) tożsamościowo względem $x_1, x_2, \ldots, x_n$. Wobec (29), (28) i (27) będziemy więc mieli równość (30) tożsamościowo wgzlędem $x_1, x_2, \ldots, x_n$. Lecz, jak wiemy z twierdzenia 4, skoro S jest podstawieniem nie należącym do grupy G, to wszystkie podstawienia:

$$S_1,\ S_2,\ \ldots,\ S_m,\ S_1 S,\ S_2 S,\ \ldots,\ S_m S \tag{32}$$

są różne, a więc przekształcają permutację $1\,2 \ldots n$ na same różne permutacje. Wobec (27) wynika stąd, że wszystkie $2m$ jednomianów występujących po lewej i po prawej stronie równości (31) są różne. Równość (31) nie może więc zachodzić tożsamościowo, gdyż np. pierwszym składnikiem jej lewej strony jest $x_{\alpha_1} x_{\alpha_2}^2 \ldots x_{\alpha_n}^n$, a składnika takiego po prawej stronie nie ma.

Przypuszczenie, że mamy tożsamościowo (względem zmiennych $x_1, x_2, \ldots, x_n$) równość (31) dla pewnego podstawienia S nie należącego do grupy G, prowadzi więc do sprzeczności. Zatem twierdzenie 19 zostało udowodnione.

W szczególności, jeżeli grupa G składa się z samego tylko podstawienia tożsamościowego, to wzór (28) daje wobec (25):

$$f(x_1, x_2, \ldots, x_n) = W_{S_1} = W = x_1 x_2^2 \ldots x_n^n.$$

Jednomian $x_1 x_2^2 x_3^3 \ldots x_n^n$ zmienia więc swoją wartość (przynajmniej dla pewnego układu wartości zmiennych $x_1, x_2, \ldots, x_n$) przy każdej z $n!$ permutacyj zmiennych.

Tę samą własność posiada też wyrażenie liniowe:

$$x_1 + 2x_2 + 3x_3 + \ldots + nx_n.$$

Między wielomianami a grupami podstawień istnieje więc tego rodzaju związek, że każdemu wielomianowi n zmiennych odpowiada oznaczona w zupełności grupa podstawień (przy których i tylko przy których wielomian ten nie zmienia swej wartości dla żadnego układu wartości zmiennych), zaś każdej grupie podstawień dla liczb ciągu $1, 2, \ldots, n$ odpowiada pewien (nie pusty) zbiór wielomianów n zmiennych (które przy podstawieniach tej grupy i tylko przy tych podstawieniach nie zmieniają swej wartości dla żadnego układu wartości zmiennych).

Niech teraz $f(x_1, x_2, \ldots, x_n)$ będzie wielomianem n zmiennych, a G odpowiadającą mu grupą, złożoną z podstawień $S_1=1$, S_2, ..., S_m. Mamy więc tożsamościowo względem $x_1, x_2, \ldots, x_n$:

$$f_{S_1} = f_{S_2} = \ldots = f_{S_m}. \tag{33}$$

Niech dalej S będzie podstawieniem nie należącym do grupy G. Wobec (33) będzie tożsamościowo względem $x_1, x_2, \ldots, x_n$:

$$f_{S_1 S} = f_{S_2 S} = \ldots = f_{S_m S}. \tag{34}$$

Lecz w myśl określenia grupy G nie będzie tożsamościowo (względem $x_1, x_2, \ldots, x_n$) $f_S = f$, czyli nie będzie $f_{S_i} = f_{S_i S}$. Wielomiany (34) są więc różne od wielomianów (33). Jeżeli $2m < n!$ i jeżeli T jest podstawieniem różnym od każdego z podstawień (32), to podobnie znajdziemy tożsamość::

$$f_{S_1 T} = f_{S_2 T} = \ldots = f_{S_m T}, \tag{35}$$

przy czym wielomiany (35) będą różne od wielomianów (33), jakoteż od wielomianów (34). Gdyby bowiem było $f_{S_1T}=f_{S_1S}$ czyli $f_T=f_S$, to mielibyśmy stąd $f=f_{S\cdot S^{-1}}=f_{TS^{-1}}$, zatem TS^{-1} należałoby do G, czyli przy pewnym k z ciągu $1,2,\ldots,m$ byłoby $TS^{-1}=S_k$, skąd $T=S_kS$, wbrew założeniu co do T.

Rozumując w ten sposób dalej aż do wyczerpania wszystkich $n!$ podstawień, dojdziemy do wniosku, że wielomian $f(x_1,x_2,\ldots,x_n)$ będzie przy wszystkich $n!$ permutacjach zmiennych $x_1,x_2,\ldots,x_n$ dawał $n!/m$ różnych wielomianów.

Więc np. jednomian $x_1x_2^2x_3^3\ldots x_n^n$, jakoteż wielomian:

$$x_1+2x_2+3x_3+\ldots+nx_n$$

(którego grupa składa się, jak wiemy, z jednego tylko elementu, skąd $m=1$), daje przy wszystkich $n!$ permutacjach zmiennych same różne wielomiany.

§ 19. Grupa Galois danego równania. Możemy też badać, dla jakich podstawień (w ciągu $x_1,x_2,\ldots,x_n$) wartość danego wielomianu $f(x_1,x_2,\ldots,x_n)$ lub ogólniej, danej funkcji, nie ulegnie zmianie *dla danych liczb* $x_1,x_2,\ldots,x_n$. Zbiór wszystkich takich podstawień może jednak nie tworzyć grupy.

Niech np. ε oznacza pierwiastek pierwotny 5-go stopnia z jedności i niech:

$$f(x_1,x_2,x_3,x_4,x_5)=x_1^4-x_2^3x_3.$$

Dla $x_j=\varepsilon^j$ (gdzie $j=1,2,3,4,5$) wartość funkcji f jest równa $\varepsilon^4-\varepsilon^9=0$ i nie ulega zmianie przy podstawieniu:

$$S=\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}$$

(gdyż $f(x_2,x_3,x_4,x_5,x_1)=x_2^4-x_3^3x_4=\varepsilon^8-\varepsilon^9\varepsilon^4=0$), ani też przy podstawieniu:

$$T=\begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix}$$

(gdyż $f(x_3,x_4,x_5,x_2,x_1)=x_3^4-x_4^3x_5=\varepsilon^{12}-\varepsilon^{17}=0$), zaś ulega zmianie przy podstawieniu:

$$ST=\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix},$$

gdyż $f(x_4,x_5,x_2,x_1,x_3)=x_4^4-x_5^3x_2=\varepsilon^{16}-\varepsilon^2=\varepsilon(1-\varepsilon)\neq 0$.

Natomiast dla każdego układu danych liczb $x_1,x_2,\ldots,x_n$ grupą będzie zbiór wszystkich podstawień $S=\begin{pmatrix}1&2&\ldots&n\\\alpha_1&\alpha_2&\ldots&\alpha_n\end{pmatrix}$, mających tę własność, że jeżeli dla jakiejkolwiek funkcji (lub wielomianu) f zmiennych $x_1,x_2,\ldots,x_n$ zachodzi przy danych wartościach tych zmiennych równość:

$$f(x_1,x_2,\ldots,x_n)=0, \tag{36}$$

to zachodzi też przy nich równość:

$$f(x_{\alpha_1},x_{\alpha_2},\ldots,x_{\alpha_n})=0. \tag{37}$$

Jeżeli bowiem $T=\begin{pmatrix}1&2&\ldots&n\\\beta_1&\beta_2&\ldots&\beta_n\end{pmatrix}$ jest podstawieniem takim, że skoro dla jakiejś funkcji g mamy przy danych wartościach $x_1,x_2,\ldots,x_n$:

$$g(x_1,x_2,\ldots,x_n)=0, \tag{38}$$

to mamy też:

$$g(x_{\beta_1},x_{\beta_2},\ldots,x_{\beta_n})=0, \tag{39}$$

to dla

$$g(t_1,t_2,\ldots,t_n)=f(t_{\alpha_1},t_{\alpha_2},\ldots,t_{\alpha_n}) \tag{40}$$

będziemy mieli wobec (37) równość (38), pociągającą za sobą równość (39), czyli wobec (40) równość

$$f(x_{\beta_{\alpha_1}},x_{\beta_{\alpha_2}},\ldots,x_{\beta_{\alpha_n}})=0. \tag{41}$$

Równość (36) pociąga więc za sobą równość (41), co dowodzi, że podstawienie ST należy do omawianego zbioru podstawień, który zatem jest grupą.

W szczególności, jeżeli liczby $x_1,x_2,\ldots,x_n$ są wszystkimi pierwiastkami równania $f(x)=0$, to tak określoną grupę podstawień nazywamy *grupą Galois* tego równania.