

ROZDZIAŁ XX

UOGÓLNIENIE CIAŁ LICZBOWYCH

§ 1. Definicja ciała. *Ciałem* nazywamy każdy zbiór K (o dowolnych elementach), w którym określone i wykonalne są dwa działania — nazwijmy je *dodawaniem* i *mnożeniem* oraz oznaczmy przez $+$ i $\cdot$, przy czym dodawanie jest łączne, przemienne i jednoznacznie odwracalne w zbiorze K , mnożenie zaś jest łączne, przemienne i rozdzielne względem dodawania, tudzież spełniające jeszcze warunek W , który podamy dalej.

Względem dodawania zbiór K jest więc grupą abelową. Jedność tej grupy będziemy oznaczali przez 0 . Będzie to więc jedyny element x zbioru K , taki iż $x+x=x$, przy czym będzie $0+a=a+0=a$ dla każdego elementu a zbioru K . W szczególności więc $0+0=0$, skąd wobec rozdzielności mnożenia względem dodawania mamy $a0=a(0+0)=a0+a0$, co dowodzi, że $a0=0$, gdyż na mocy twierdzenia 3, Rozdział XIX, § 3, str. 312, z $x+x=x$ wynika, że x jest jednością działania grupy K .

Mamy więc $a0=0$ dla każdego elementu a zbioru K , a zatem jeżeli zbiór K składa się z więcej niż jednego elementu, to mnożenie w nim nie jest odwracalne (gdyż dla $a \neq 0$ nie ma takiego x iżby $x0=a$) i przeto zbiór K nie jest ze względu na mnożenie grupą.

Otóż zapowiadany warunek W opiewa, że dla każdego elementu a zbioru K oraz każdego elementu b zbioru K różnego od 0 istnieje jeden i tylko jeden taki element x zbioru K , iż $bx=a$. Wobec przemienności mnożenia spełnia on też równanie $ax=a$.

Będziemy go oznaczali przez a/b i nazywali *ilorazem* z dzielenia a przez b .

Dzielenie jest więc jednoznacznie wykonalne w zbiorze K , o ile dzielnik b nie jest zerem.

Twierdzenie 1. *Iloczyn dwu elementów zbioru K różny od zera jest zawsze różny od zera.*

Dowód. Przypuśćmy, że $a \neq 0$ i $b \neq 0$, zaś $ab=0$. Ponieważ $a0=0$, więc wobec $ab=0$ i jednoznaczności dzielenia, o ile dzielnik nie jest zerem, wnosimy, że $b=0$, wbrew założeniu. Musi więc być $ab \neq 0$, c. b. d. o.

Z twierdzenia 1 wynika, że zbiór $K-(0)$, czyli *zbiór wszystkich elementów zbioru K , różnych od zera, tworzy grupę abelową ze względu na mnożenie* (por. Rozdział XIX, § 1, przykład 19, str. 309-310).

Jedność tej grupy będziemy nazywali *jednością ciała* i oznaczali przez e .

Oznaczanie jej przez 1 nie jest wskazane, gdyż wówczas należałoby konsekwentnie oznaczać sumę n jedności przez n , zaś — jak zobaczymy w § 2 na przykładzie 1 — suma n jedności ciała przy naturalnym n , może być zerem. Niektórzy autorzy zamiast e piszą $\bar{1}$, zaś sumę n składników równych e oznaczają przez $\bar{n}$ ¹⁾.

Działanie odwrotne względem dodawania będziemy nazywali *odejmowaniem*, zaś element x , spełniający dla danych a i b ze zbioru K równanie $b+x=x+b=a$, będziemy oznaczali przez $a-b$.

W zbiorze K są więc jednoznacznie wykonalne cztery działania arytmetyczne z wyjątkiem dzielenia przez 0 . W ten sposób rozważane tu ciała są uogólnieniem ciał liczbowych.

§ 2. Przykłady ciał. 1. Niech p będzie liczbą pierwszą, zaś K zbiorem liczb $0, 1, 2, \dots, p-1$. Sumę (iloczyn) elementów a i b zbioru K określimy jako resztę z dzielenia przez p zwykłej sumy (zwykłego iloczynu) liczb a i b . Opierając się na elementarnych twierdzeniach z Teorii liczb dowodzimy z łatwością, że określone w ten sposób dodawanie i mnożenie elementów zbioru K mają wszystkie własności, jakie działania te muszą posiadać w ciele. Zbiór K staje się w ten sposób ciałem. Jednością tego ciała będzie oczywiście liczba 1 ; suma p jedności jest tu równa 0 (czyli $p=0$).

Gdyby jednak p było liczbą złożoną, np. $p=mn$, gdzie m i n są liczbami naturalnymi większymi od 1 , to nie otrzymalibyśmy przy powyższych określeniach ciała, nie istniałby bowiem żaden element zbioru K , taki iż $mx=1$ (gdyż przy wszelkim całkowitym x iloczyn mx daje przy dzieleniu przez $p=mn$ resztę podzielną przez m , zaś $m > 1$).

¹⁾ Ob. np. książkę N. Czebotařew, *Osnowy Teorii Galois*, Część I, Lenin-grad-Moskwa 1934, str. 154 (po rosyjsku).

Istnieją więc ciała, złożone z 2, 3, 5, 7, 11 i t. d. elementów. Ciałami o skończonej liczbie elementów zajmiemy się bliżej w § 4.

2. Niech K będzie zbiorem wszystkich liczb wymiernych, zaś $q \neq 0$ daną liczbą wymierną. Sumą elementów a i b zbioru K niechaj będzie zwykła suma liczb a i b , iloczynem zaś elementów a i b zwykły iloczyn liczb a i b , pomnożony przez q . Łatwo sprawdzić, że zbiór K będzie ciałem izomorficznym (ze względu na dodawanie i na mnożenie) z ciałem $\mathcal{R}$ liczb wymiernych, przy czym odwzorowanie izomorficzne ciała K na ciało $\mathcal{R}$ otrzymamy, przyporządkowując każdemu elementowi a ciała K liczbę qa ciała $\mathcal{R}$. Jednością ciała K jest więc liczba $1/q$.

3. Zbiór wszystkich funkcji wymiernych jednej zmiennej o całkowitych (a tak samo o rzeczywistych, o zespolonych) współczynnikach jest ciałem, jeżeli przez sumę i iloczyn jego elementów rozumieć zwykłą sumę i iloczyn funkcji. Podobnie jest dla funkcji dwu lub większej liczby zmiennych. Można by na tej drodze utworzyć ciało o dowolnej mocy nieskończonej m , jako zbiór wszystkich funkcji wymiernych m zmiennych o współczynnikach całkowitych.

Ciało K wszystkich funkcji wymiernych jednej zmiennej o współczynnikach całkowitych jest izomorficzne ze względu na 4 działania arytmetyczne z ciałem $\mathcal{R}(a)$, gdzie a jest dowolnie daną liczbą przestępną. Dla otrzymania odwzorowania izomorficznego ciała K na ciało $\mathcal{R}(a)$ wystarczy każdej funkcji $f(x)$, należącej do ciała K , przyporządkować liczbę $f(a)$ ciała $\mathcal{R}(a)$.

Można też dowieść, że ciało wszystkich funkcji wymiernych dwu zmiennych o współczynnikach całkowitych jest ze względu na 4 działania arytmetyczne izomorficzne z ciałem $\mathcal{R}(a, \beta)$, gdzie a i β są danymi liczbami przestępnymi, algebraicznie od siebie niezależnymi.

4. Niech p będzie liczbą pierwszą postaci $4k+3$, a K zbiorem p^2 liczb zespolonych postaci $a+bi$, gdzie a i b są liczbami ciągu $0, 1, 2, \dots, p-1$. Dodawanie i mnożenie elementów zbioru K określimy w ten sposób, że po wykonaniu zwykłego dodawania czy mnożenia liczb zespolonych, zastąpimy część rzeczywistą, jako też współczynnik przy i , odpowiednio przez ich reszty przy dzieleniu przez p .

Okażemy, że wówczas K jest ciałem.

Bliższego dowodu wymaga tylko jednoznaczna odwracalność mnożenia w zbiorze $K - (0)$. Niech więc $a+bi$ i $c+di \neq 0$ będą liczbami zbioru K .

Mamy dowieść, że istnieje w K jedna i tylko jedna taka liczba $x+yi$, iż

$$(1) \quad (c+di)(x+yi) = a+bi \pmod{p},$$

czyli że istnieje w ciągu $0, 1, \dots, p-1$ jeden i tylko jeden taki układ liczb x, y , iż:

$$(2) \quad cx - dy = a \pmod{p} \quad \text{ i } \quad cy + dx = b \pmod{p}.$$

Załóżmy w tym celu, że układ x, y spełnia kongruencje (2). Mnożąc pierwszą z nich przez c , a drugą przez d i dodając, otrzymamy kongruencję:

$$(3) \quad (c^2 + d^2)x = ac + bd \pmod{p},$$

zaś mnożąc pierwszą przez $-d$, a drugą przez c i dodając, otrzymamy kongruencję:

$$(4) \quad (c^2 + d^2)y = -ad + bc \pmod{p}.$$

Jak wiadomo z Teorii liczb, liczba pierwsza postaci $4k+3$ nie może być dzielnikiem sumy dwu kwadratów liczb przez nią niepodzielnych. Ponieważ $c+di$ jest elementem zbioru K i $c+di \neq 0$, więc mamy $c^2 + d^2 \not\equiv 0 \pmod{p}$. Wobec tego, jak to wynika z teorii kongruencji pierwszego stopnia o module pierwszym, istnieje jedyna para liczb x i y z ciągu $0, 1, \dots, p-1$, spełniająca kongruencje (3) i (4), z których wnosimy z łatwością, że:

$$(c^2 + d^2)(cx - dy) = a(c^2 + d^2) \pmod{p},$$

$$(c^2 + d^2)(cy + dx) = b(c^2 + d^2) \pmod{p}.$$

Wobec $c^2 + d^2 \not\equiv 0 \pmod{p}$ wynikają stąd kongruencje (2), zatem też i kongruencja (1). Ponieważ zaś $x+yi$ jest oczywiście liczbą zbioru K , więc jednoznaczna odwracalność mnożenia w tym zbiorze została w ten sposób udowodniona. Zatem K jest ciałem, c. b. d. o.

Przykład ten dowodzi, że istnieją ciała, których liczba elementów jest kwadratem dowolnej liczby pierwszej postaci $4k+3$. W szczególności, istnieją ciała złożone z 9 oraz z 49 elementów.

Zauważmy, że gdyby p było liczbą 2 lub liczbą pierwszą postaci $4k+1$, to przy tym samym określeniu dodawania i mnożenia w zbiorze K nie otrzymalibyśmy zeń ciała. W tym bowiem przypadku p jest — jak wiadomo z Teorii liczb — sumą kwadratów dwu liczb naturalnych, a zatem istnieją w ciągu $1, 2, \dots, p-1$ takie liczby c i d , iż $p = c^2 + d^2$, skąd $(c+di)(c-di) = 0 \pmod{p}$ i przeto, zgodnie z przy-

jętym w zbiorze K określeniem mnożenia, iloczyn liczb $c+di$ i $c-di$ tego zbioru, obu różnych od zera, jest zerem, co dowodzi, że zbiór K nie jest ciałem.

Nie wynika stąd oczywiście, że nie istnieją ciała złożone z p^2 elementów, gdzie p jest liczbą 2 lub liczbą pierwszą postaci $4k+1$; dowodu istnienia takich ciał należy jednak szukać na innej drodze (ob. przykłady 5 i 6).

5. Niech K oznacza zbiór czterech funkcji zmiennej x (z których pierwsze dwie są stałe):

$$0, \quad 1, \quad x, \quad 1+x.$$

Dodawanie i mnożenie elementów zbioru K określimy w ten sposób, że po dokonaniu zwykłego dodawania lub mnożenia wielomianów podzielimy wynik przez trójmian x^2+x+1 , a w otrzymanej stąd reszcie, która będzie postaci $ax+b$, zastąpimy liczby a i b przez ich reszty z dzielenia przez 2. Zbiór K jest tu więc zbiorem reszt według dwu modułów:

$$x^2+x+1 \quad \text{i} \quad 2,$$

czyli (por. dalej przykład 9) zbiorem reszt

$$(\text{mod } x^2+x+1, 2).$$

Tabliczkami dodawania i mnożenia w zbiorze K będą więc:

Dodawanie					Mnożenie				
	0	1	x	$1+x$		0	1	x	$1+x$
0	0	1	x	$1+x$	0	0	0	0	0
1	1	0	$1+x$	x	1	0	1	x	$1+x$
x	x	$1+x$	0	1	x	0	x	$1+x$	1
$1+x$	$1+x$	x	1	0	$1+x$	0	$1+x$	1	x

Wówczas zbiór K będzie ciałem. Przemienność bowiem i łączność obu działań, jak również jednoznaczna odwracalność dodawania (w zbiorze K), wynika bezpośrednio z ich określeń, zaś jednoznaczna odwracalność mnożenia w zbiorze $K-(0)$ widoczna jest bezpośrednio z tabliczki mnożenia dla zbioru K .

Istnieje więc ciało, złożone z 4 elementów.

6. Niech p będzie liczbą pierwszą nieparzystą, zaś s liczbą z ciągu $0, 1, 2, \dots, p-1$, nie będącą resztą z dzielenia przez p żadnej z liczb $0^2, 1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$. Taka liczba s istnieje, gdyż $p \geq 3$, skąd $1 + \frac{p-1}{2} < p$.

Niech dalej K oznacza zbiór p^2 dwumianów postaci $a+bx$ zmiennej x , gdzie a i b są liczbami ciągu $0, 1, 2, \dots, p-1$. Dodawanie i mnożenie elementów zbioru K określimy w ten sposób, że po dokonaniu zwykłego dodawania i mnożenia wielomianów podzielimy wyniki przez x^2-s , a w otrzymanej reszcie postaci $a+bx$ zastąpimy liczby a i b przez ich reszty z dzielenia przez p .

Okazemy, że zbiór K z określonym w ten sposób dodawaniem i mnożeniem jest ciałem.

Bliższego dowodu wymaga tylko jednoznaczna odwracalność mnożenia w zbiorze $K-(0)$.

Niech więc $a+bx$ i $c+dx$ będą dwoma elementami zbioru K , przy czym liczby c i d niechaj nie będą jednocześnie zerami. Ponieważ resztą z dzielenia iloczynu $(c+dx)(g+hx)$ przez x^2-s jest $cg+dhs+(ch+dg)x$, więc mamy dowieść, że istnieje jeden i tylko jeden taki element $g+hx$ zbioru K , iż:

$$(5) \quad cg+dhs \equiv a \pmod{p} \quad \text{i} \quad ch+dg \equiv b \pmod{p}.$$

Mnożąc pierwszą z tych kongruencyj przez c , a drugą przez ds i odejmując, otrzymamy:

$$(6) \quad (c^2-d^2s)g \equiv ac-dsb \pmod{p},$$

mnożąc zaś pierwszą przez $-d$, a drugą przez c i dodając, otrzymamy:

$$(7) \quad (c^2-d^2s)h \equiv -ad+bc \pmod{p}.$$

Liczby g i h z ciągu $0, 1, \dots, p-1$ będą przez te kongruencje wyznaczone jednoznacznie, jeżeli okażemy, że $c^2-d^2s \not\equiv 0 \pmod{p}$.

Otóż gdyby było $c^2-d^2s \equiv 0 \pmod{p}$ i $d \equiv 0 \pmod{p}$, mielibyśmy też $c^2 \equiv 0 \pmod{p}$, skąd (ponieważ p jest liczbą pierwszą) $c \equiv 0 \pmod{p}$, a więc (ponieważ c i d są liczbami ciągu $0, 1, \dots, p-1$) byłoby $c=d=0$, wbrew założeniu. Jeżeli więc $c^2-d^2s \equiv 0 \pmod{p}$, to musi być $d \not\equiv 0 \pmod{p}$ i — jak wiemy z Teorii liczb — istnieje w ciągu $1, 2, \dots, p-1$ taka liczba z , iż $dz \equiv 1 \pmod{p}$, skąd $(zc)^2 \equiv (zd)^2s \equiv s \pmod{p}$. Niech r oznacza resztę z dzielenia liczby

ze przez p . Jest więc $r^2 \equiv s \pmod{p}$ i $(p-r)^2 \equiv r^2 \equiv s \pmod{p}$, przy czym jedna z liczb r i $p-r$ należy do ciągu $0, 1, 2, \dots, \frac{p-1}{2}$, wbrew określeniu liczby s . Dowiedliśmy więc, że $c^2 - d^2 s \equiv 0 \pmod{p}$, a przeto istnieją w ciągu $0, 1, \dots, p-1$ liczby g i h , dla których zachodzą kongruencje (6) i (7). Kongruencje te dają:

$$\begin{aligned}(c^2 - d^2 s)(cg + dhs) &\equiv (c^2 - d^2 s)a \pmod{p}, \\ (c^2 - d^2 s)(ch + dg) &\equiv (c^2 - d^2 s)b \pmod{p},\end{aligned}$$

co wobec $c^2 - d^2 s \equiv 0 \pmod{p}$ daje kongruencje (5). Zatem K jest ciałem, c. b. d. o.

Wynika stąd, że istnieją ciała, których liczba elementów jest kwadratem dowolnej liczby pierwszej nieparzystej.

7. Niech K oznacza zbiór wszystkich funkcji (zmiennej x) postaci $px + q$, gdzie p i q są dowolnymi liczbami rzeczywistymi. Zbiór K będzie ciałem, jeżeli przez sumę jego elementów rozumieć zwykłą sumę funkcji, zaś przez iloczyn jego elementów a i b rozumieć resztę z dzielenia iloczynu dwumianów a i b przez dwumian $x^2 + 1$. Iloczynem elementów $p_1x + q_1$ i $p_2x + q_2$ będzie więc element

$$(p_1q_2 + p_2q_1)x - p_1p_2 + q_1q_2.$$

Łatwo widzieć, że K jest ciałem, które (względem dodawania i mnożenia) jest izomorficzne z ciałem wszystkich liczb zespolonych, przy czym otrzymamy ten izomorfizm, przyporządkowując liczbie zespolonej $pi + q$ funkcję $px + q$.

8. Niech $f(x) = x^2 + c_1x + c_2$ będzie trójmianem 2-go stopnia o współczynnikach wymiernych, nie mającym pierwiastków wymiernych (innymi słowy takim, że $c_1^2 - 4c_2$ nie jest kwadratem liczby wymiernej). Niech K oznacza zbiór wszystkich dwumianów $px + q$, gdzie p i q są liczbami wymiernymi. Przez sumę elementów zbioru K będziemy rozumieli zwykłą sumę dwumianów, zaś przez iloczyn elementów tego zbioru — resztę z dzielenia ich zwykłego iloczynu przez trójmian $f(x)$.

Aby okazać, że przy takim określeniu sumy i iloczynu elementów K będzie ciałem, wystarczy dowieść, że dla każdego elementu $a_1x + a_2$ zbioru K i każdego elementu $b_1x + b_2$ tegoż zbioru, różnego od elementu 0 (t. j. nie równego tożsamościowo zeru), istnieje jeden i tylko jeden taki element $p_1x + p_2$ zbioru K , iż wielomian

$$(8) \quad (b_1x + b_2)(p_1x + p_2) - (a_1x + a_2)$$

jest podzielny przez trójmian $f(x)$.

Otóż, jak łatwo obliczyć, wielomian (8) daje przy dzieleniu przez trójmian $f(x)$ resztę:

$$(b_2p_1 + b_1p_2 - a_1 - b_1c_1p_1)x + b_2p_2 - a_2 - b_1p_1c_2.$$

Na to więc, aby ta reszta była zerem, potrzeba i wystarcza, żeby było:

$$(9) \quad (b_2 - b_1c_1)p_1 + b_1p_2 = a_1 \quad \text{ i } \quad -b_1c_2p_1 + b_2p_2 = a_2.$$

Mnożąc pierwsze z tych równań przez b_2 , a drugie przez $-b_1$ i dodając, otrzymamy:

$$(10) \quad (b_2^2 - b_1b_2c_1 + b_1^2c_2)p_1 = a_1b_2 - a_2b_1,$$

zaś mnożąc pierwsze przez b_1c_2 , a drugie przez $b_2 - b_1c_1$ i dodając, otrzymamy:

$$(11) \quad (b_2^2 - b_1b_2c_1 + b_1^2c_2)p_2 = a_1b_1c_2 + a_2b_2 - a_2b_1c_1.$$

Jeżeli $b_1 \neq 0$, to b_2/b_1 jest liczbą wymierną taką, że:

$$\left(\frac{b_2}{b_1}\right)^2 - c_1\frac{b_2}{b_1} + c_2 \neq 0,$$

gdyż wielomian $f(x)$ nie ma pierwiastków wymiernych. Mamy więc wówczas:

$$(12) \quad b_2^2 - b_1b_2c_1 + b_1^2c_2 \neq 0$$

i równania (10) i (11) dają po jednej tylko wartości wymiernej na p_1 i p_2 .

Jeżeli zaś $b_1 = 0$, to $b_2 \neq 0$ (gdyż z założenia $b_1x + b_2$ nie jest tożsamościowo zerem) i znowu mamy nierówność (12), zatem równania (10) i (11) znowu dają po jednej tylko wartości wymiernej na p_1 i p_2 .

Z drugiej strony, wobec (12) sprawdzamy z łatwością, że liczby p_1 i p_2 , wyznaczone z równań (10) i (11), spełniają równania (9). Zbiór K jest więc ciałem, c. b. d. o.

Zauważmy, że jednomian $g = g(x) = x$ jest elementem ciała K , spełniającym (w tym ciele) równanie:

$$(13) \quad g^2 + c_1g + c_2 = 0,$$

albowiem g^2 daje przy dzieleniu przez $f(x)$ resztę $-c_1x - c_2$, a przeto mamy w ciele K :

$$g^2 + c_1g + c_2 = -c_1x - c_2 + c_1x + c_2 \equiv 0.$$

Ciało K zawiera w sobie ciało wszystkich liczb wymiernych $\mathcal{R}$ (które otrzymujemy z $px+q$ dla $p=0$). W ciele $\mathcal{R}$ równanie (13) nie posiadało rozwiązań (względem g), zaś po rozszerzeniu go do ciała K już je posiada.

Niech teraz a będzie jednym z pierwiastków trójkianu $f(x)$. Jest to więc liczba algebraiczna 2-go stopnia. Niech K_1 oznacza ciało liczbowe $\mathcal{R}(a)$.

Okazemy, że ciała K i K_1 są izomorficzne względem dodawania i mnożenia. Co do dodawania jest to oczywiste, gdyż — jak wiemy z twierdzenia 8 Rozdziału XIII (§ 3, str. 229) — każda liczba ciała $K_1=\mathcal{R}(a)$ może być w jeden i tylko w jeden sposób przedstawiona w postaci $pa+q$, gdzie liczby p i q są wymierne. Co zaś do mnożenia, to mamy tu wobec $f(a)=0$ wzór:

$$(b_1a+b_2)(p_1a+p_2)=b_1p_1a^2+(b_2p_1+b_1p_2)a+b_2p_2=\\=(b_2p_1+b_1p_2-b_1p_1c_1)a+b_2p_2-b_1p_1c_2,$$

a że resztą z dzielenia wielomianu $(b_1x+b_2)(p_1x+p_2)$ przez $f(x)$ jest:

$$(b_2p_1+b_1p_2-b_1p_1c_1)x+b_2p_2-b_1p_1c_2,$$

więc przyporządkowując każdemu elementowi p_1x+p_2 ciała K odpowiednio liczbę p_1a+p_2 ciała K_1 , otrzymamy odwzorowanie, ustalające izomorfizm tych ciał względem dodawania i mnożenia.

W szczególnym przypadku, gdy $c_1=0$ i $c_2=1$, ciało K jest izomorficzne (względem dodawania i mnożenia) z ciałem wszystkich liczb zespolonych postaci p_1i+p_2 , gdzie p_1 i p_2 są liczbami wymiernymi.

Ogólniej, niech $f(x)$ będzie wielomianem nieprzywiedlnym n -go stopnia o współczynnikach wymiernych. Oznaczmy przez K zbiór wszystkich wielomianów stopnia mniejszego od n o współczynnikach wymiernych. Określimy w zbiorze K dodawanie jako zwykłe dodawanie wielomianów, iloczyn zaś elementów tego zbioru jako resztę z dzielenia zwykłego iloczynu wielomianów przez $f(x)$. Można z łatwością okazać, że ze względu na tak określone dodawanie i mnożenie zbiór K jest izomorficzny z ciałem $\mathcal{R}(a)$, gdzie a jest (którymkolwiek) pierwiastkiem wielomianu $f(x)$.

Ponieważ definicja ciała K nie wymaga wprowadzenia liczb niewymiernych (ani zespolonych), więc różne własności ciała $\mathcal{R}(a)$,

jako izomorficznego z ciałem K , mogą być badane bez pomocy liczb niewymiernych (i zespolonych).

Podane przykłady można by jeszcze uogólnić, zakładając, że $f(x)$ jest wielomianem o współczynnikach należących do danego ciała K_0 (niekoniecznie liczbowego) i nieprzywiedlnym w tym ciele. Określone podobnie jak wyżej ciało K będzie wówczas zawierało element $g=g(x)=x$, spełniający równanie $f(x)=0$ (tożsamościowo ze względu na x , t. j. $f(g(x))=0$), oczywiście przy uwzględnieniu określenia sumy i iloczynu elementów ciała K , a więc i wielomianów w tym ciele.

Ponieważ ciało K_0 jest częścią ciała K , więc możemy też powiedzieć, że ciało K_0 zostało rozszerzone (do ciała K) w ten sposób, że wielomian $f(x)$, nieprzywiedlny w ciele K_0 , stał się przywiedlnym w ciele K .

9. Mówimy, że wielomian $f(x)$ o współczynnikach całkowitych jest *nieprzywiedlny modulo p* (gdzie p jest liczbą naturalną), jeżeli nie istnieją żadne trzy takie wielomiany $\varphi(x)$, $\psi(x)$ i $\vartheta(x)$ o współczynnikach całkowitych, że $\varphi(x)$ i $\psi(x)$ są stopni niższych od stopnia $f(x)$ oraz że równość:

$$f(x)=\varphi(x)\psi(x)+p\vartheta(x)$$

zachodzi tożsamościowo względem x , czyli takie, dla których mamy tożsamościowo:

$$f(x)=\varphi(x)\psi(x) \pmod{p}.$$

Niech $f(x)$ oznacza wielomian stopnia n o współczynnikach całkowitych, nieprzywiedlny modulo p , gdzie p jest daną liczbą pierwszą. Niech dalej K oznacza zbiór p^n wielomianów stopnia co najwyżej $n-1$ o współczynnikach, będących liczbami z ciągu $0,1,2,\dots,p-1$. Dodawanie i mnożenie elementów zbioru K określimy w ten sposób, że po dokonaniu zwykłego dodawania i mnożenia wielomianów podzielimy wyniki przez wielomian $f(x)$, a w otrzymanej stąd reszcie (która będzie wielomianem stopnia co najwyżej $n-1$) zastąpimy każdy współczynnik przez jego resztę z dzielenia przez p .

O zbiorze K mówimy wówczas, że jest *zbiorem reszt według dwu modułów: $f(x)$ i p* , co piszemy krócej (por. str. 352):

$$(\text{modd } f(x), p).$$

Można okazać, że określony w ten sposób zbiór K tworzy ciało (złożone z p^n elementów)¹⁾ oraz że każde ciało skończone jest izomorficzne z jednym co najmniej z otrzymanych w ten sposób ciał.

Przykładem szczególnym takiego ciała K jest ciało zbadane w przykładzie 5 (str. 352). Zajmiemy się tu bliżej innym przypadkiem szczególnym, mianowicie, gdy $f(x) = x^3 - 2$ i $p = 7$.

Okażemy przede wszystkim, że wielomian $f(x)$ jest nieprzywiedlny modulo 7.

Istotnie, gdyby było:

$$x^3 - 2 \equiv (ax + b)(cx^2 + dx + e) \pmod{7},$$

musielibyśmy mieć:

$$\begin{aligned} ac &\equiv 1 \pmod{7}, & ad + bc &\equiv 0 \pmod{7} \\ ae + bd &\equiv 0 \pmod{7}, & be &\equiv -2 \pmod{7}. \end{aligned}$$

Trzecia z tych kongruencji daje $ae \equiv -bd \pmod{7}$, skąd $a^2e \equiv -bad \pmod{7}$, a że na skutek drugiej kongruencji jest $ad \equiv -bc \pmod{7}$, więc mamy $a^2e \equiv b^2e \pmod{7}$, skąd dostajemy:

$$a^2e^2be \equiv (bc)^3 \pmod{7},$$

co wobec pierwszej i czwartej kongruencji daje:

$$(bc)^3 \equiv -2 \pmod{7}.$$

Łatwo jednak sprawdzić, że ostatnia kongruencja przy całkowitych b i c zachodzić nie może. Bo jeżeli $x \equiv 0, \pm 1, \pm 2, \pm 3 \pmod{7}$, to $x^3 \equiv 0, \pm 1, \pm 1, \pm 1 \pmod{7}$, zatem $x^3 \not\equiv -2 \pmod{7}$ dla każdej liczby całkowitej x . Wielomian $f(x)$ jest więc nieprzywiedlny modulo 7.

Aby okazać, że zbiór wszystkich reszt $(\text{mod } x^3 - 2, 7)$ czyli zbiór wszystkich 7^3 wielomianów $ax^2 + bx + c$, gdzie a, b, c są liczbami

¹⁾ Jedyną trudność stanowi tu dowód, że mnożenie w zbiorze $K - (0)$ jest jednoznacznie odwracalne. Dowód ten opiera się na następującym twierdzeniu udowodnionym przez J. A. Serret'a w jego dziele *Cours d'Algèbre Supérieure*, Tom II, Wyd. 5-e, Paryż 1885, str. 125:

Jeżeli $\varphi(x)$ i $\psi(x)$ są takimi wielomianami o współczynnikach całkowitych, iż:

$$\varphi(x)\psi(x) \equiv 0 \pmod{f(x), p} \quad \text{ i } \quad \varphi(x) \not\equiv 0 \pmod{f(x), p},$$

to $\psi(x) \equiv 0 \pmod{f(x), p}$.

Wynika stąd z łatwością, że jeżeli $\varphi(x)$ jest daną resztą według dwu modułów $f(x)$ i p , różną od zera, to gdy $\psi(x)$ przebiega wszystkie różne reszty według modułów $f(x)$ i p , reszty $(\text{mod } f(x), p)$ iloczynu $\varphi(x)\psi(x)$ czynią to samo, co już pociąga za sobą jednoznaczność odwracalności mnożenia w ciele $K - (0)$.

z ciągu $0, 1, 2, 3, 4, 5, 6$, tworzy ciało, wystarczy okazać, że mnożenie jest jednoznacznie odwracalne w zbiorze $K - (0)$.

Niech więc $ax^2 + bx + c$ i $dx^2 + ex + f$ będą dwoma elementami zbioru K , przy czym liczby d, e i f niech nie będą jednocześnie równe 0. Ponieważ resztą z dzielenia iloczynu $(dx^2 + ex + f)(qx^2 + rx + s)$ przez $x^3 - 2$ jest:

$$(fq + er + ds)x^2 + (fr + es + 2dq)x + fs + 2(eq + dr),$$

więc mamy dowieść, że istnieje jeden i tylko jeden taki element $qx^2 + rx + s$ zbioru K , iż:

$$\begin{aligned} fq + er + ds &\equiv a \pmod{7}, \\ fr + es + 2dq &\equiv b \pmod{7}, \\ fs + 2(eq + dr) &\equiv c \pmod{7}. \end{aligned}$$

Na to, żeby ten układ 3 kongruencji miał jedno i tylko jedno rozwiązanie w liczbach q, r, s z ciągu $0, 1, 2, \dots, 6$, potrzeba i wystarczy, by dla wyznacznika tego układu

$$D = \begin{vmatrix} f & e & d \\ 2d & f & e \\ 2e & 2d & f \end{vmatrix} = f^3 + 4d^3 + 2e^3 - 6def$$

było $D \not\equiv 0 \pmod{7}$. Otóż z uwagi na to, że liczby f, d i e nie są jednocześnie równe 0 oraz że dla całkowitych x , nie podzielnych przez 7, mamy $x^3 \equiv \pm 1 \pmod{7}$, stwierdzamy za pomocą łatwych prób, że istotnie $D \not\equiv 0 \pmod{7}$. Zbiór K jest więc ciałem, złożonym z $7^3 = 343$ elementów.

§ 3. Dołączanie elementu do ciała. Jeżeli ciało L zawiera ciało K oraz element a , nie należący do K , i jeżeli każde ciało, zawarte w L i zawierające K oraz a , pokrywa się z L , to mówimy, że ciało L zostało otrzymane z ciała K przez dołączenie do niego elementu a , i oznaczamy je przez $K(a)$.

Jak łatwo widzieć, $K(a)$ jest zbiorem wszystkich elementów postaci $f(a)$, gdzie f jest funkcją wymierną o współczynnikach, należących do K . Jeżeli x należy do $K(a)$, to K jest zawarte w $K(x)$, a $K(x)$ w $K(a)$, przy czym może być $K \neq K(x) \neq K(a)$.

Np. gdy $\mathcal{R}$ jest ciałem wszystkich liczb wymiernych, to i należy do $\mathcal{R}\left(\frac{i+1}{\sqrt{2}}\right)$ oraz $\mathcal{R} \neq \mathcal{R}(i) \neq \mathcal{R}\left(\frac{i+1}{\sqrt{2}}\right)$.

Element a (nie należący do K) nazywamy *przestępnym względem ciała K* , jeżeli nie jest pierwiastkiem żadnego wielomianu o współ-

czynnikach należących do K , z których nie wszystkie są równe 0; w przeciwnym razie element a nazywamy *algebraicznym względem ciała K* .

Łatwo dowieść, że wszystkie ciała, otrzymane z ciała K przez dołączenie do niego elementu przestępnego względem K , są izomorficzne ze względu na 4 działania arytmetyczne.

Inaczej jest w przypadku dołączenia do K elementu algebraicznego względem K . Np. ciała $\mathcal{R}(\sqrt{2})$ i $\mathcal{R}(i)$ nie są izomorficzne.

Można dowieść, że jeżeli a jest elementem przestępnym względem ciała K , to każdy element zbioru $K(a) - K$ jest przestępny względem tegoż ciała.

Ciało L zawierające K nazywa się *algebraicznym względem ciała K* , jeżeli każdy element ciała L jest algebraiczny względem K .

Ciało K nazywamy *algebraicznie zamkniętym*, jeżeli się pokrywa z każdym zawierającym K ciałem algebraicznym względem K .

Np. zbiór wszystkich liczb algebraicznych jest ciałem algebraicznie zamkniętym.

Można dowieść, że dla każdego ciała istnieje zawierające je ciało algebraicznie zamknięte¹⁾. Znanе dowody tego twierdzenia posługują się pewnikiem wyboru (twierdzeniem E. Zermelo o dobrym uporządkowaniu) i nie dają metody efektywnego wyznaczenia ciała algebraicznie zamkniętego, zawierającego dane ciało²⁾.

§ 4. Podciała. Ciała proste. Część danego ciała, będącą ciałem, nazywamy jego *podciałem*.

Każde ciało K jest własnym podciałem, jako też zawiera podciało, złożone z jednego tylko elementu: zera ciała K . O ile zaś podciało ciała K zawiera więcej niż jeden element, to — jak łatwo widzieć — zawiera ono zero i jedność ciała K (które zarazem są odpowiednio zerem i jednością podciała).

Aby dowieść, że część danego ciała jest jego podciałem, wystarczy okazać, że są w niej wykonalne cztery działania arytmetyczne z wyjątkiem dzielenia przez 0.

Ciało, złożone więcej niż z jednego elementu i mające tylko dwa podciała: samo siebie oraz podciało złożone tylko z zera, nazywamy *prostym*.

¹⁾ Ob. E. Steinitz, *Algebraische Theorie der Körper*, Berlin-Lipsk 1930, str. 113.

²⁾ Por. tamże str. 129.

Twierdzenie 2. Każde ciało, złożone z więcej niż jednego elementu, posiada jedno i tylko jedno podciało proste.

Dowód. Niech K będzie danym ciałem, złożonym z więcej niż jednego elementu. Oznaczmy przez P iloczyn (część wspólną) wszystkich podciał ciała K , zawierających jego zero i jego jedność (podciała takie istnieją, np. samo K). Z definicji ciała wynika natychmiast, że P jest ciałem prostym. Jeżeli bowiem P_1 jest podciałem ciała P , zawierającym więcej niż jeden element, to P_1 jest zarazem podciałem ciała K , zawierającym jego zero i jego jedność, a przeto w myśl definicji ciała P , ciało P_1 jest jednym z czynników iloczynu P , skąd wynika, że P jest zawarte w P_1 , co (wobec tego, że P_1 jest zawarte w P) daje $P_1 = P$.

Gdyby teraz ciało K posiadało jeszcze podciało proste P' , to część wspólna PP' byłaby podciałem ciał P i P' , zawierającym więcej niż jeden element; ponieważ zaś ciała P i P' są proste, więc wynikałoby stąd, że $PP' = P$ i $PP' = P'$, czyli że $P = P'$. Uodowodniliśmy zatem twierdzenie 2.

Postaramy się teraz wyznaczyć wszystkie ciała proste. Niech P oznacza dane ciało proste, e jego jedność. Rozróżnimy dalej dwa przypadki:

1° Wszystkie wyrazy ciągu nieskończonego

$$(14) \quad e, \quad e+e, \quad e+e+e, \quad \dots$$

są różnymi elementami ciała P . Oznaczmy, dla skrócenia, sumę n składników równych e przez ne , a element $0 - ne$ przez $(-n)e$. Jak łatwo widzieć, jeżeli każdej liczbie wymiernej p/q przyporządkujemy element pe/qe ciała P , to otrzymamy odwzorowanie izomorficzne (ze względu na 4 działania arytmetyczne) ciała $\mathcal{R}$ wszystkich liczb wymiernych na pewną część P_1 ciała P . Ciało P_1 będzie więc podciałem ciała prostego P , złożonym z więcej niż jednego elementu, skąd wynika, że $P_1 = P$. W przypadku 1° ciało proste P jest więc izomorficzne z ciałem $\mathcal{R}$.

2° Nie wszystkie wyrazy ciągu (14) są różne. Niech $me = ne$ dla $m > n$. Przyjmując $m = n + k$, będziemy mieli $ne + ke = ne$, co daje $ke = 0$ na mocy określenia zera. Niech p oznacza najmniejszą liczbę naturalną, taką iż $pe = 0$. Nie może być $p = 1$, gdyż $e \neq 0$, jak to wynika z definicji jedności ciała (§ 1, str. 349). Gdyby p było liczbą złożoną $p = rs$, gdzie r i s są liczbami naturalnymi mniejszymi od p , to wobec $ee = e$ (gdyż e jest jednością ciała P) mie-

libyśmy $re \cdot se = rs \cdot e = pe = 0$, gdy tymczasem z określenia liczby p wynika, że $re \neq 0$ i $se \neq 0$, co daje $re \cdot se \neq 0$, skąd sprzeczność. Liczba p musi więc być pierwszą.

Okazemy teraz, że zbiór Z_p wszystkich elementów ke dla $k=0, 1, 2, \dots, p-1$ tworzy ciało. Ponieważ elementy te należą do ciała P , więc wystarczy okazać, że w zbiorze Z_p wykonalne są 4 działania arytmetyczne z wyjątkiem dzielenia przez 0.

Otóż jeżeli k_1 i k_2 są dwiema liczbami z ciągu $0, 1, \dots, p-1$, to możemy napisać $k_1 + k_2 = mp + k$, gdzie k jest liczbą z tegoż ciągu, skąd $k_1e + k_2e = mpe + ke = ke$, gdyż $mpe = m \cdot pe = 0$. Podobnie, pisząc $k_1 - k_2 = m'p + k'$ (gdzie może być $m' \leq 0$), otrzymamy $k_1e - k_2e = k'e$. Wreszcie, pisząc $k_1k_2 = mp + k$, otrzymamy $k_1ek_2e = ke$.

Pozostaje do okazania, że w razie, gdy $k_2 \neq 0$, istnieje w ciągu $0, 1, \dots, p-1$ taka liczba k , iż $k_2e \cdot ke = k_1e$. Otóż, skoro liczba p jest pierwszą, zaś liczba k_2 naturalną, to — jak wiemy z Teorii liczb — istnieje w ciągu $1, \dots, p-1, p$ taka liczba k , że $k_2k \equiv k_1 \pmod{p}$, czyli że $k_2k = mp + k_1$, gdzie m jest liczbą całkowitą. Mamy zatem $k_2e \cdot ke = k_2k \cdot e = (mp + k_1)e = mpe + k_1e = k_1e$.

Zbiór Z_p jest więc ciałem. Łatwo spostrzec, że jest ono ze względu na 4 działania arytmetyczne izomorficzne z ciałem P_p wszystkich reszt modulo p , zbadanym w § 2 (przykład 1, str. 349). Ciało to, jako podciało ciała prostego P złożone z więcej niż jednego elementu, musi z nim być identyczne.

Otrzymane wyniki doprowadzają więc do następującego twierdzenia:

Twierdzenie 3. Każde ciało proste nieskończone jest izomorficzne z ciałem $\mathcal{R}$ liczb wymiernych, zaś ciałami prostymi skończonymi są ciała izomorficzne z ciałami wszystkich reszt modulo p , gdzie p jest (dowolnie daną) liczbą pierwszą, i tylko takie ciała.

Nie dla każdego jednak dwu ciał K_1 i K_2 istnieje ciało K , zawierające podciało izomorficzne z K_1 i podciało izomorficzne z K_2 .

Np. jeżeli K_1 jest ciałem złożonym z 2 elementów, a K_2 ciałem złożonym z 3 elementów, to takiego ciała K nie ma. Gdyby bowiem ono istniało, to jego jedność e byłaby zarazem jednością ciał K_1 i K_2 . Lecz w ciele K_1 mamy $e + e = 0$, a w ciele K_2 mamy $e + e \neq 0$ ¹⁾.

¹⁾ Istotnie, ciało K_1 składa się z 2 elementów, a więc tylko z elementów 0 i e , skąd $e + e = 0$ lub $e + e = e$, przy czym druga równość dawałaby $e = 0$, co jest niemożliwe. W ciele zaś K_2 , które względem dodawania jest grupą (gdzie jednością grupy jest 0), mamy $e + e + e = 0$; gdyby więc było $e + e = 0$, mielibyśmy $e = 0$, co niemożliwe.

Natomiast każde ciało K jest podciałem innego większego ciała, np. ciała W wszystkich funkcji wymiernych jednej zmiennej, których współczynniki należą do ciała K . W szczególności, ciała K i W mogą być izomorficzne, np. jeżeli K jest ciałem wszystkich funkcji wymiernych o współczynnikach całkowitych przeliczalnej mnogości zmiennych. Można by jednak okazać, że każde ciało K jest podciałem innego ciała, nie izomorficznego z ciałem K . Takim jest np. ciało wszystkich funkcji wymiernych m zmiennych, o współczynnikach należących do K , gdzie m jest liczbą kardynalną większą od mocy ciała K .

§ 5. Ciała skończone. Niech K oznacza dane ciało skończone. W myśl twierdzenia 2 posiada ono jedno tylko podciało proste P , oczywiście skończone, a więc w myśl twierdzenia 3 złożone z p elementów, gdzie p jest liczbą pierwszą, i izomorficzne z ciałem P_p wszystkich reszt modulo p .

Liczbę p nazywamy *charakterystyką* ciała skończonego K .

Twierdzenie 4. Liczba elementów ciała skończonego jest zawsze potęgą jego charakterystyki.

Dowód. Niech m oznacza liczbę elementów ciała skończonego K , którego podciało proste P zawiera p elementów. Jeżeli $K = P$, to mamy oczywiście $m = p$ i twierdzenie jest słuszne. Załóżmy więc, że $K \neq P$.

Istnieje zatem element a ciała K , nie należący do P . Utwórzmy p^2 elementów (ciała K) postaci $x_1 + ax_2$, gdzie x_1 i x_2 należą do P . Wszystkie one są różne. Istotnie, gdyby było $x_1 + ax_2 = y_1 + ay_2$, gdzie x_1, x_2, y_1 i y_2 są elementami P , to w razie, gdy $x_2 = y_2$, mielibyśmy $ax_2 = ay_2$, a zatem też $x_1 = y_1$. Jeżeli zaś $x_2 \neq y_2$, to ponieważ element $z = \frac{e}{x_2 - y_2}$ należy do P , mielibyśmy $a = (y_1 - x_1)z$, więc a należałoby do P , wbrew założeniu.

Gdyby elementy $x_1 + ax_2$ wyczerpywały ciało K , mielibyśmy oczywiście $m = p^2$. W przeciwnym razie oznaczmy przez b element ciała K różny od nich wszystkich i utwórzmy p^3 elementów (ciała K) postaci $x_1 + ax_2 + bx_3$, gdzie x_1, x_2 i x_3 należą do P . Łatwo znowu okazać, że są one wszystkie różne. Gdyby bowiem było $x_1 + ax_2 + bx_3 = y_1 + ay_2 + by_3$, to w razie, gdy $x_3 = y_3$, znaleźlibyśmy $x_1 + ax_2 = y_1 + ay_2$, co daje $x_1 = y_1$ i $x_2 = y_2$, w razie zaś, gdy $x_3 \neq y_3$, przyjmując $z = \frac{e}{x_3 - y_3}$, wnosilibyśmy, że z należy do P i że

$b = (y_1 - x_1)z + (y_2 - x_2)za = \xi_1 + \xi_2 a$, gdzie ξ_1 i ξ_2 należą do P , wbrew określeniu elementu b .

Gdyby elementy $a_1 + ax_2 + bx_3$ wyczerpywały ciało K , znaleźlibyśmy $m = p^3$. W przeciwnym razie oznaczamy przez c element ciała K różny od nich wszystkich i rozumiemy jak poprzednio.

Ponieważ ciało K jest skończone, więc ostatecznie znajdziemy skończoną liczbę n jego elementów:

$$a_1 = e, \quad a_2 = a, \quad a_3 = b, \quad \dots, \quad a_n = l$$

takich, iż każdy element ciała K daje się, i to w jeden tylko sposób, przedstawić w postaci:

$$x_1 a_1 + x_2 a_2 + \dots + x_n a_n,$$

gdzie x_i należy do P dla $i = 1, 2, \dots, n$. Jest więc $m = p^n$, c. b. d. o.

O elementach $a_1, a_2, \dots, a_n$ mówimy, że tworzą bazę liniową dla ciała K .

Z twierdzenia 4 wynika

Wniosek. Liczba elementów ciała skończonego (o ile przewyższa 1) jest zawsze potęgą liczby pierwszej.

Można okazać, że może to być dowolna potęga dowolnej liczby pierwszej (por. przykład 9 z § 2, str. 358-359).

Wyprowadzimy tu jeszcze jedną własność elementów ciała skończonego. Niech $a_1, a_2, \dots, a_{m-1}$ będą wszystkimi różnymi od zera elementami ciała skończonego K i niech a oznacza którykolwiek z nich. Iloczyn:

$$aa_1, \quad aa_2, \quad \dots, \quad aa_{m-1}$$

są oczywiście wszystkie różne (gdyż $aa_i = aa_j$ wobec $a \neq 0$ daje $a_i = a_j$) i różne od zera (jako iloczyny elementów różnych od zera). Różnią się one więc co najwyżej porządkiem od elementów $a_1, a_2, \dots, a_{m-1}$. Wynika stąd, że:

$$aa_1 \cdot aa_2 \cdot \dots \cdot aa_{m-1} = a_1 a_2 \dots a_{m-1}$$

czyli:

$$a^{m-1} a_1 a_2 \dots a_{m-1} = a_1 a_2 \dots a_{m-1},$$

co wobec $a_1 a_2 \dots a_{m-1} \neq 0$ (gdyż $a_i \neq 0$ dla $i = 1, 2, \dots, m-1$) daje:

$$(15) \quad a^{m-1} = e.$$

Mamy więc

Twierdzenie 5. Potęga $(m-1)$ -a każdego różnego od zera elementu ciała skończonego o m elementach jest jednością tego ciała.

Inny dowód tego twierdzenia wynika stąd, że zbiór wszystkich różnych od zera elementów ciała tworzy grupę ze względu na mnożenie (ob. str. 349) i że w grupie skończonej rząd każdego elementu jest dzielnikiem liczby elementów grupy (ob. Rozdział XIX, § 10, str. 327, wniosek 2), a więc w danym razie liczby $m-1$.

W szczególnym przypadku, dla ciała P_p , gdzie p jest liczbą pierwszą, otrzymujemy stąd znane z Teorii liczb t. zw. małe twierdzenie Fermata (p. str. 237).

Mnożąc równość (15) przez a , otrzymujemy z niej równość:

$$a^m - a = 0,$$

zachodzącą również i dla $a = 0$, a zatem dla każdego bez wyjątku elementu ciała K . Mamy więc

Wniosek. Każdy element ciała skończonego o m elementach jest pierwiastkiem równania

$$x^m - x = 0.$$

§ 6. Ciała złożone z 4 elementów. Dowiedliśmy, że istnieje ciało złożone z 4 elementów (ob. § 2, str. 352, przykład 5). Postaramy się obecnie wyznaczyć wszystkie takie ciała.

Załóżmy, że K jest ciałem o 4 elementach: $0, e$ (jedność ciała), a i b . Elementy e, a i b tworzą ze względu na mnożenie grupę, której jednością jest e . Tabliczka mnożenia dla takiej grupy może być tylko następująca:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Wobec tego tabliczką mnożenia w ciele K musi być:

$$(16) \quad \begin{array}{c|ccc|c} & 0 & e & a & b \\ \hline 0 & 0 & 0 & 0 & 0 \\ e & e & a & b & e \\ a & a & b & e & a \\ b & b & e & a & b \end{array}$$

Co zaś do dodawania, to — jak wiemy (p. str. 348) — ciało K jest ze względu na nie grupą, przy czym jednością tej grupy jest 0.

Aby obliczyć tabliczkę dodawania w ciele K , obliczmy na-
przód $e+e$.

Nie może być $e+e=e$, gdyż wynikałoby stąd, że $e=0$, co jest niemożliwe. Gdyby było $e+e=a$, mielibyśmy $a(e+e)=aa$, skąd wobec $aa=b$ i $a(e+e)=ae+ae=a+a$, znaleźlibyśmy $a+a=b$, a zatem $e+e+e+e=b$. Lecz z uwagi na to, że grupa K składa się z 4 elementów i że jednością tej grupy jest 0, wynika, że $e+e+e+e=0$. Byłoby więc $b=0$, co jest niemożliwe. Podobnie, gdyby było $e+e=b$, mielibyśmy $b(e+e)=bb$, skąd wobec $bb=a$ znaleźlibyśmy $b+b=b(e+e)=bb=a$, co daje $e+e+e+e=a$, skąd $a=0$, co też nie jest możliwe. Suma $e+e$ nie jest więc żadnym z elementów e , a i b , a zatem może być tylko pozostałym elementem grupy czyli zerem, t. j.

$$e+e=0.$$

Mamy stąd dalej dla każdego elementu x grupy K :

$$x+x=xe+xe=x(e+e)=x0=0,$$

zatem $a+a=0$ i $b+b=0$.

Wreszcie, obliczmy $e+a$. Gdyby było $e+a=0$, mielibyśmy wobec $e+e=0$ równość $a=e$, co niemożliwe. Gdyby było $e+a=e$, mielibyśmy $a=0$, co również nie jest możliwe. Gdyby wreszcie było $e+a=a$, mielibyśmy $e=0$, co też jest niemożliwe. Musi więc być $e+a=b$. Stąd wobec $e+e=0$ znajdujemy:

$$e+b=e+(e+a)=(e+e)+a=a$$

czyli $e+b=a$, zaś wobec $b+b=0$ znajdujemy:

$$a+b=(e+b)+b=e+(b+b)=e$$

czyli $a+b=e$. Z uwagi wreszcie na przemienność dodawania otrzymujemy:

$$a+e=e+a=b, \quad b+e=e+b=a, \quad b+a=a+b=e.$$

Tabliczka dodawania w rozważanym ciele jest więc następująca:

(17)

	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

Jeżeli przeto K jest ciałem o 4 elementach, to tabliczki mnożenia i dodawania w tym ciele są w zupełności określone. Wynika stąd natychmiast, że:

Każde dwa ciała o 4 elementach są izomorficzne (ze względu na 4 działania arytmetyczne).

Zastanowimy się jeszcze nad tym, jakby można sprawdzić bezpośrednio, że znalezione przez nas tabliczki mnożenia i dodawania wyznaczają ciało.

Łatwo spostrzec, że na to, aby dane tabliczki mnożenia i dodawania wyznaczały ciało, potrzeba i wystarcza, żeby:

1° tabliczka dodawania wyznaczała grupę abelową,

2° w tabliczce mnożenia wiersz i kolumna o nagłówku 0 były wypełnione samymi zerami, po usunięciu zaś tego wiersza i kolumny aby tabliczka wyznaczała grupę abelową,

3° mnożenie było rozdzielne względem dodawania.

Sprawdzenie, że tabliczki (16) i (17) spełniają te warunki, nie przedstawia trudności. Warunek 2° wynika od razu z budowy tabliczki mnożenia, a warunek 1° z uwagi, że tabliczka dodawania jest izomorficzna z drugą tabliczką z Rozdziału XIX, § 15, str. 337. Warunek zaś 3° sprawdzić można bezpośrednio z tabliczek, badając, czy zawsze jest $(x+y)z=xz+yz$, przy czym wystarczy sprawdzić ten wzór tylko w 12 przypadkach, ponieważ dla $z=0$ i $z=e$, jak również dla $x=0$ i dla $y=0$, wzór ten jest oczywisty; skorzystać nadto należy z przemienności dodawania.

Można dowieść ogólnie, że:

Dwa ciała skończone o tej samej liczbie elementów są zawsze izomorficzne (ze względu na 4 działania arytmetyczne).

Inaczej natomiast jest dla ciał nieskończonych, choćby przeliczalnych. Np. ciała $\mathcal{R}$ i $\mathcal{R}(\sqrt{2})$ nie są izomorficzne ze względu na dodawanie. W ciele $\mathcal{R}$ bowiem dla każdego dwu elementów a i b różnych od 0 istnieją takie liczby całkowite k i l , iż $ka=lb$, zaś ciało $\mathcal{R}(\sqrt{2})$ własności tej nie posiada (np. dla $a=1$ i $b=\sqrt{2}$).

Dwa ciała nieskończone mogą też być izomorficzne ze względu na dodawanie (a więc i odejmowanie), a nie być izomorficzne ze względu na mnożenie. Np. ciała $\mathcal{R}(\sqrt{2})$ i $\mathcal{R}(i)$, których izomorfizm

ze względu na dodawanie ustalamy, przyporządkowując każdej liczbie $p + q\sqrt{2}$ ciała $\mathcal{R}(\sqrt{2})$ liczbę $p + qi$ ciała $\mathcal{R}(i)$, nie są izomorficzne ze względu na mnożenie, gdyż w ciele $\mathcal{R}(i)$ równanie $x^4 = 1$ ma cztery różne pierwiastki $(1, -1, i, -i)$, zaś w ciele $\mathcal{R}(\sqrt{2})$ tylko dwa.

ĆWICZENIA Z RÓŻNYCH ROZDZIAŁÓW.

1. Dowieść, że:

$$(1+i)^2 + (1-i)^2 = 0, \quad (1+i)^{-1} + (1-i)^{-1} = 1.$$

2. Obliczyć:

$$u = (1+i\sqrt{7})^4 + (1-i\sqrt{7})^4, \quad v = (1+i\sqrt{3})^5 + (1-i\sqrt{3})^5.$$

Odp.: $u=16$, $v=32$.

3. Obliczyć $u_k = (1+i)^k + (1-i)^k$ dla całkowitych k .

$$\text{Odp.: } u_k = \begin{cases} (-1)^l 2^{2l+1} & \text{dla } k=4l \text{ i } k=4l+1, \\ 0 & \text{dla } k=4l+2, \\ (-1)^{l+1} 2^{2l+2} & \text{dla } k=4l+3. \end{cases}$$

4. Obliczyć $v_k = (1+i\sqrt{3})^k + (1-i\sqrt{3})^k$ dla całkowitych k .

$$\text{Odp.: } v_k = \begin{cases} (-1)^l 2^{3l+1} & \text{dla } k=3l \text{ i } k=3l+1, \\ (-1)^{l+1} 2^{3l+2} & \text{dla } k=3l+2. \end{cases}$$

5. Znaleźć wszystkie pierwiastki rzeczywiste równania:

$$\left(\frac{1+ix}{2}\right)^4 + \left(\frac{1-ix}{2}\right)^4 = 1.$$

Odp.: $\sqrt{7}i$ i $-\sqrt{7}i$.

6. Zbadać, jakiego stopnia liczbą algebraiczną jest

$$x = \sqrt{6 + \sqrt{20}}.$$

Odp.: 2-go stopnia, gdyż

$$(x^2 - 6)^2 - 20 = 0,$$

ale

$$(x^2 - 6)^2 - 20 = (x^2 + 2x - 4)(x^2 - 2x - 4),$$

skąd z łatwością wnosimy, że $x = \sqrt{5} + 1$.

7. O ciągu nieskończonym macierzy mówimy, że zmierza do granicy g (będącej macierzą), jeżeli odpowiednie elementy macierzy, będących wyrazami ciągu, zmierzają do odpowiednich elementów macierzy g .

Okazać, że dla

$$a = \begin{pmatrix} 1/2 & 2 \\ 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 1/2 & 0 \\ 2 & 0 \end{pmatrix}$$

będzie:

$$a^n = \begin{pmatrix} 2^{-n} & 2^{-n+2} \\ 0 & 0 \end{pmatrix} \rightarrow 0, \quad b^n = \begin{pmatrix} 2^{-n} & 0 \\ 2^{-n+2} & 0 \end{pmatrix} \rightarrow 0,$$

lecz:

$$(ab)^n = \begin{pmatrix} (4^{1/4})^n & 0 \\ 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} +\infty & 0 \\ 0 & 0 \end{pmatrix}.$$

8. Znaleźć wszystkie rozwiązania w różnych od zera liczbach rzeczywistych x, y układu dwu równań:

$$x^8 y^{10} = a(x-y)^3, \quad x^5 y^7 = b(x-y)^2,$$

Odp.: $x = ab^{-2} \sqrt[5]{a^2 - b^3}$, $y = a^{-1} b \sqrt[5]{a^2 - b^3}$, gdzie wartość pierwiastka należy wziąć rzeczywistą.

9. Dowieść, że każde z dwu działań 9 i 15, podanych na str. 285, da się wyrazić jedno przez drugie.

Dowód. Łatwo sprawdzić, że oznaczając przez $\odot$ działanie 9, a przez $\ominus$ działanie 15, będziemy mieli dla jakichkolwiek elementów x i y zbioru $\{a, b\}$:

$$x \odot y = [(x \odot x) \odot (y \odot y)] \odot [(x \odot x) \odot (y \odot y)],$$

$$x \ominus y = [(x \odot x) \odot (y \odot y)] \odot [(x \odot x) \odot (y \odot y)].$$

10. Dowieść, że każde z 16 działań, podanych na str. 285, da się wyrazić za pomocą jednego tylko działania 9, a także za pomocą jednego tylko działania 15 (fakt ten ma zastosowanie w Logice).

1) Por. O. Tausky i J. Todd, Journal of London Mathematical Society, Tom 17 (1942), str. 146 i następn.

Uwaga. Można dowieść — co jest jednak rzeczą trudną — że każde z 19683 działań, określonych i wykonalnych w zbiorze o 3 elementach a, b i c (por. str. 286), daje się wyrazić za pomocą działania określonego tabliczką ¹⁾:

	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

¹⁾ Por. D. Webb, American Journal of Mathematics, Tom 58 (1936), str. 193-194.

Andrzej Mostowski

ZARYS TEORII GALOIS

CZĘŚĆ I

GRUPA GALOIS

§ 1. Grupy podstawień. Pojęcie symetrii. Niech A oznacza dowolny zbiór.

Podstawieniem zbioru A nazywamy każdą funkcję φ , odwzorowującą zbiór A na samego siebie w sposób wzajemnie jednoznaczny.

Iloczynem dwu podstawień φ i ψ nazywamy podstawienie $\vartheta = \varphi\psi$, dane wzorem $\vartheta(x) = \varphi(\psi(x))$ ¹⁾.

Jeśli zbiór G podstawień zbioru A jest grupą ze względu na tak określone pojęcie iloczynu (por. Rozdział XIX, § 1, str. 309, przykład 17), to mówimy, że G jest *grupą podstawień*.

Jednością 1 takiej grupy jest podstawienie *tożsamościowe*: $1(x) = x$ dla każdego elementu x zbioru A . Elementem odwrotnym do φ jest podstawienie φ^{-1} , odwrotne do φ .

Ilość elementów zbioru A nazywamy *stopniem* grupy G .

Pojęcie grupy podstawień zjawia się wszędzie tam, gdzie jest mowa o niezmienniczości pewnych relacji.

Załóżmy, że w zbiorze A określone są pewne relacje między elementami: $R(x, y, z, \dots)$, $S(x, y, z, \dots)$, ...

Mówimy, że relacje te są *niezmiennicze*, albo *symetryczne*, ze względu na podstawienie φ , jeśli z zachodzenia ich między elementami $x, y, z, \dots$ wynika zawsze zachodzenie ich między elementami $\varphi(x), \varphi(y), \varphi(z), \dots$:

$$R(x, y, z, \dots) \rightarrow R(\varphi(x), \varphi(y), \varphi(z), \dots), \quad S(x, y, z, \dots) \rightarrow S(\varphi(x), \varphi(y), \varphi(z), \dots).$$

¹⁾ Podstawienie to oznacza się też często przez $\psi\varphi$ (por. Rozdział XVIII, § 2, str. 301), aby zaznaczyć porządek, w jakim wykonywane są podstawienia. Symbolika taka nie jest jednak konsekwentna, jeśli podstawienia chcemy traktować jako funkcje. Najwłaściwszym wydaje się pisać: $\vartheta = \varphi\psi$, lecz czytać ten wzór: „ ϑ jest równe ψ razy φ “.