ROZDZIAŁ XVII

WSTĘP DO TEORII CIAŁ LICZBOWYCH

§ 1. Ciało liczbowe. Najprostsze ciało liczbowe, zawierające liczbę μ. Nazywamy *ciałem liczbowym* każdy zbiór K liczb rzeczywistych lub zespolonych, w którym istnieje przynajmniej jedna liczba różna od 0 i w którym wykonalne są wszystkie cztery działania arytmetyczne (z wyjątkiem oczywiście dzielenia przez 0).

Znaczy to, że jeżeli μ i ν są dwoma jakimikolwiek (różnymi lub nie) elementami zbioru K, to liczby $\mu+\nu$, $\mu-\nu$, $\mu\cdot\nu$, a w razie $\nu\neq 0$ również $\mu:\nu$ należą do K.

Ciałem liczbowym jest więc np. — jak łatwo widzieć — zbiór wszystkich liczb wymiernych, zbiór wszystkich liczb rzeczywistych, zbiór wszystkich liczb zespolonych. Ale zbiór wszystkich liczb całkowitych nie jest ciałem liczbowym, gdyż np. $5:3$ nie jest liczbą całkowitą. Podobnie zbiór wszystkich liczb niewymiernych nie jest ciałem liczbowym, gdyż np. $\sqrt{2}-\sqrt{2}=0$.

Twierdzenie 1. *Każde ciało liczbowe zawiera wszystkie liczby wymierne.*

Dowód. Niech K będzie ciałem liczbowym. W K istnieje więc co najmniej jedna liczba $\mu\neq 0$. W myśl definicji ciała liczbowego liczba naturalna $\mu:\mu=1$ też należy do K. Załóżmy, że do K należy liczba naturalna n (jest to — jak stwierdziliśmy — prawdziwe dla $n=1$). Skoro liczby 1 i n należą do K, to do tego ciała liczbowego należy też $n+1$. Wynika stąd przez indukcję, że do K należy każda liczba naturalna. Wnosimy stąd dalej, że do K należą liczby $\mu-\mu=0$ oraz $0-n=-n$; do K należy więc każda liczba całkowita, a zatem i każda liczba wymierna (gdyż każda liczba wymierna jest ilorazem liczby całkowitej przez liczbę naturalną), c. b. d. o.

Dowiedliśmy więc, że ciało liczbowe R wszystkich liczb wymiernych jest częścią każdego innego ciała liczbowego; jest to zatem *najprostsze ciało liczbowe.*

Każde inne ciało liczbowe zawiera więc przynajmniej jedną liczbę, która albo nie jest wymierna, albo nie jest rzeczywista.

Niech μ będzie liczbą rzeczywistą lub zespoloną, a K — jakimkolwiek ciałem liczbowym, zawierającym liczbę μ. Łatwo widzieć — na mocy definicji ciała liczbowego — że do K musi należeć każda liczba postaci

$$(1)\qquad \frac{a_0+a_1\mu+a_2\mu^2+\ldots+a_m\mu^m}{b_0+b_1\mu+b_2\mu^2+\ldots+b_n\mu^n},$$

gdzie m i n są liczbami całkowitymi nieujemnymi, a współczynniki $a_0, a_1, \ldots, a_m$ i $b_0, b_1, \ldots, b_n$ — liczbami całkowitymi, przy czym

$$b_0+b_1\mu+\ldots+b_n\mu^n\neq 0.$$

Z drugiej strony, łatwo sprawdzić, że cztery działania arytmetyczne, wykonane na liczbach postaci (1) — naturalnie oprócz dzielenia przez zero — doprowadzają znowu do liczb postaci (1). Zbiór wszystkich liczb postaci (1) jest więc ciałem liczbowym. Oznaczamy je przez $K(\mu)$; jest ono w zupełności określone przez liczbę μ.

Udowodniliśmy jednocześnie

Twierdzenie 2. *Ciało $K(\mu)$ jest częścią każdego ciała liczbowego K, zawierającego liczbę μ.*

Jest to więc najprostsze ciało liczbowe, zawierające liczbę μ, *nieprzywiedlne* — jak powiadamy — względem własności zawierania liczby μ.

Mówimy też, że ciało $K(\mu)$ zostało utworzone przez *dołączenie* liczby μ do ciała wymiernego, o ile, naturalnie, samo μ nie jest liczbą wymierną, bo wtedy mielibyśmy $K(\mu)=K(1)=R$ czyli $K(\mu)$ byłoby ciałem wszystkich liczb wymiernych.

§ 2. Ciało liczbowe drugiego stopnia; sprowadzenie go do postaci $K(\sqrt{D})$. Po liczbach wymiernych najprostsze są liczby, spełniające równanie drugiego stopnia o współczynnikach całkowitych. Ciała, powstające przez dołączenie takich liczb do ciała wymiernego, są najprostszymi ciałami liczbowymi po ciele liczb wymiernych [1]). Zajmiemy się nimi teraz bliżej.

[1]) Ciału, powstającemu przez dołączenie do ciała liczb wymiernych pierwiastków trzeciego stopnia z jedności, poświęcił specjalną monografię A. Axer, *Zarys arytmetyki ciała pierwiastków trzecich z jedności* (osobne odbicie z tomów 14, 15 i 16 Wiadomości Matematycznych, Warszawa 1913, stronic IV + 97).

Niech μ będzie liczbą rzeczywistą lub zespoloną — byle nie wymierną — spełniającą równanie

$$Ax^2+Bx+C=0 \tag{2}$$

o współczynnikach A, B, C całkowitych (gdzie, naturalnie, $A\neq 0$).

Niech dalej

$$\Delta=B^2-4AC \tag{3}$$

i niech m^2 będzie największym dzielnikiem kwadratowym liczby Δ; możemy więc napisać

$$\Delta=m^2D, \tag{4}$$

gdzie D jest liczbą całkowitą, niepodzielną przez żaden kwadrat większy od jedności; zarazem $D\neq 1$, gdyż μ nie jest liczbą wymierną.

Okażemy, że

$$K(\mu)=K(\sqrt{D}). \tag{5}$$

Dla dowodu równości (5) wystarczy oczywiście okazać, że ciało $K(\mu)$ jest zawarte w ciele $K(\sqrt{D})$ i na odwrót.

Na mocy (2), (3) i (4) jest

$$\mu=\frac{-B\pm m\sqrt{D}}{2A}, \tag{6}$$

gdzie $-B$, m i $2A$ są liczbami całkowitymi. Widać stąd, że liczba μ należy do ciała $K(\sqrt{D})$.

Lecz $K(\mu)$ jest na mocy twierdzenia 2 częścią każdego ciała liczbowego, zawierającego μ. Wynika stąd, że ciało $K(\mu)$ jest zawarte w ciele $K(\sqrt{D})$.

Na odwrót, wobec $m\neq 0$ z (6) wynika, że

$$\sqrt{D}=\pm\frac{B+2A\mu}{m},$$

skąd wnosimy natychmiast, że $\sqrt{D}$ należy do ciała $K(\mu)$, a stąd na mocy twierdzenia 2, podobnie jak wyżej, że ciało $K(\sqrt{D})$ jest zawarte w ciele $K(\mu)$, c. b. d. o.

Nie uszczuplimy więc ogólności rozważań, jeżeli w teorii ciał liczbowych drugiego stopnia ograniczymy się do badania ciał $K(\sqrt{D})$, gdzie D jest liczbą całkowitą różną od 0 i niepodzielną przez żaden kwadrat, prócz jedności.

Łatwo dowieść, że zbiór wszystkich liczb ciała $K(\sqrt{2})$ jest *gęsty* na prostej, tj. że między każdymi dwiema liczbami rzeczywistymi a i $b>a$ leżą liczby postaci $k+l\sqrt{2}$, gdzie k i l są liczbami całkowitymi wymiernymi. Okażemy, że — ogólniej nawet — *dla każdej liczby niewymiernej ξ zbiór wszystkich liczb postaci $k+l\xi$, gdzie k i l są liczbami całkowitymi rzeczywistymi, jest gęsty na prostej.*

Istotnie, weźmy pod uwagę dla liczb rzeczywistych a i $b>a$ dowolną liczbę naturalną $m>1/(b-a)$. Wobec niewymierności liczby ξ liczby $n\xi-\mathrm{E}(n\xi)$ są dla $n=0,1,2,\ldots,m$ wszystkie różne, a że wszystkie one są nieujemne i mniejsze od 1, więc istnieją wśród nich co najmniej dwie, różniące się nie więcej niż o $1/m$. Różnica tych dwu liczb jest oczywiście postaci $p+q\xi$, gdzie p i q są liczbami całkowitymi wymiernymi i

$$0<p+q\xi\leqslant 1/m<b-a.$$

Lecz — jak łatwo widzieć — jeżeli liczba rzeczywista ϱ spełnia nierówności $0<\varrho<b-a$, to $a<\varrho\mathrm{E}(b/\varrho)\leqslant b$. Niech $\varrho=p+q\xi$, $k=p\mathrm{E}(b/\varrho)$ i $l=q\mathrm{E}(b/\varrho)$. Wówczas $a<k+l\xi<b$, c. b. d. o.

§ 3. Forma ogólna liczb ciała $K(\sqrt{D})$. Liczby sprzężone. Norma. Niech D będzie liczbą całkowitą różną od 0 i od 1 oraz niepodzielną przez żaden kwadrat większy od jedności; liczba $\sqrt{D}$ jest więc niewymierna lub urojona.

Twierdzenie 3. *Ciało $K(\sqrt{D})$ jest zbiorem wszystkich liczb postaci*

$$\frac{a+b\sqrt{D}}{c}, \tag{7}$$

gdzie a, b i c są liczbami całkowitymi oraz $c\neq 0$.

Dowód. Zachodzą tożsamości:

$$\frac{a+b\sqrt{D}}{c}\pm\frac{a_1+b_1\sqrt{D}}{c_1}=\frac{ac_1\pm a_1c+(bc_1\pm b_1c)\sqrt{D}}{cc_1},$$

$$\frac{a+b\sqrt{D}}{c}\cdot\frac{a_1+b_1\sqrt{D}}{c_1}=\frac{aa_1+bb_1D+(ab_1+a_1b)\sqrt{D}}{cc_1},$$

$$\frac{a+b\sqrt{D}}{c}:\frac{a_1+b_1\sqrt{D}}{c_1}=\frac{aa_1c_1-bb_1c_1D+(ba_1-ab_1)c_1\sqrt{D}}{c(a_1^2-b_1^2D)},$$

przy czym $a_1^2-b_1^2D\neq 0$, skoro liczba $\sqrt{D}$ nie jest wymierna. Wynika stąd, że zbiór Z wszystkich liczb postaci (7) jest ciałem liczbowym, a ponieważ zawiera on liczbę $\sqrt{D}$ (dla $a=0$ i $b=c=1$), więc ciało $K(\sqrt{D})$ jest zawarte w ciele Z. Ale i na odwrót, gdyż każda liczba postaci (7) należy oczywiście do ciała $K(\sqrt{D})$, c. b. d. o.

O wzorze (7) możemy naturalnie założyć, że liczby a, b i c nie mają wspólnego dzielnika większego od 1, gdyż przez taki dzielnik można by ułamek (7) skrócić. Nadto możemy założyć, że c jest liczbą dodatnią, gdyż w przeciwnym razie wystarczyłoby pomnożyć licznik i mianownik ułamka (7) przez -1.

Przy tych założeniach każda liczba ciała $K(\sqrt{D})$ da się *w jeden tylko sposób* przedstawić w postaci (7).

Istotnie, niech

$$\frac{a+b\sqrt{D}}{c}=\frac{a'+b'\sqrt{D}}{c'},$$

zatem

$$(bc'-cb')\sqrt{D}=a'c-ac',$$

skąd wobec założenia niewymierności liczby $\sqrt{D}$ wnosimy, że $bc'-cb=0$, a więc też $a'c-ac'=0$, czyli

$$bc'=cb' \quad \text{i} \quad ac'=a'c. \tag{8}$$

Niech

$$d=(c,c') \quad c_1=c/d, \quad c_1'=c'/d.$$

Liczby c_1 i c'_1 są oczywiście naturalne, $(c_1,c_1')=1$ oraz na mocy (8)

$$bc_1'=c_1b' \quad \text{i} \quad ac_1'=a'c_1.$$

Wnosimy stąd, że zarówno a jak b są podzielne przez c_1. Gdyby było $c_1\neq 1$, to liczby a, b i c miałyby wspólny dzielnik większy od 1. Jest więc $c_1=1$. Podobnie musi być $c_1'=1$. Zatem $c=d$ i $c'=d$, skąd $c=c'$, a więc w myśl (8) również $b=b'$ i $a=a'$. Jednoznaczność przedstawienia liczb ciała $K\sqrt{D}$ wzorem (7) jest tym samym dowiedziona.

Liczbę $\frac{a-b\sqrt{D}}{c}$ ciała $K(\sqrt{D})$ nazywamy *sprzężoną* z liczbą $x=\frac{a+b\sqrt{D}}{c}$ tego ciała i oznaczamy przez x'.

Oczywiście $(x')'=x$.

Sprawdzamy z łatwością, że dla każdych dwu liczb x,y ciała $K(\sqrt{D})$ jest

$$(x+y)'=x'+y' \quad \text{i} \quad (xy)'=x'y'.$$

Iloczyn liczby x ciała $K(\sqrt{D})$ przez liczbę z nią sprzężoną x' nazywamy *normą* liczby x i oznaczamy przez $N(x)$:

$$N(x)=xx'.$$

Stąd w jednej chwili

$$N(xy)=xy\cdot(xy)'=xx'\cdot yy'=N(x)N(y),$$

czyli *norma iloczynu jest równa iloczynowi norm.*

Jest to oczywiście prawdziwe dla dowolnej skończonej liczby czynników.

Z definicji normy wynika też od razu, że

$$N\left(\frac{a+b\sqrt{D}}{c}\right)=\frac{a^2-Db^2}{c^2};$$

zatem *norma jest zawsze liczbą rzeczywistą wymierną, a zerem jest tylko wtedy, gdy* $a=b=0$, *tj. tylko dla liczby* 0.

§ 4. Liczby całkowite ciała $K(\sqrt{D})$. Nasuwa się teraz myśl, żeby przez liczby całkowite ciała $K(\sqrt{D})$ rozumieć liczby postaci $a+b\sqrt{D}$, gdzie a i b są liczbami całkowitymi wymiernymi.

Jednakże przeciw takiej terminologii przemawiają poważne względy. Gdybyśmy np. przez liczby całkowite ciała $K(\sqrt{-3})$ rozumieli tylko liczby postaci $a+b\sqrt{-3}$ (dla a i b całkowitych wymiernych), to np. liczby

$$2, \quad 1+\sqrt{-3} \quad \text{i} \quad 1-\sqrt{-3} \tag{9}$$

byłyby «pierwsze» w tym znaczeniu, że nie byłyby iloczynami żadnych dwu liczb całkowitych tego ciała, różnych jednocześnie od $+1$ i od -1, a mimo to iloczyn $(1+\sqrt{-3})(1-\sqrt{-3})=4$ byłby podzielny przez liczbę «pierwszą» 2, choć żaden z czynników tego iloczynu nie jest przez nią podzielny.

Że każda z trzech liczb (9) jest istotnie «pierwsza» (w wyżej określonym sensie), łatwo udowodnić, jak następuje.

Przypuśćmy, że którakolwiek z trzech liczb (9) jest równa iloczynowi $(a+b\sqrt{-3})(c+d\sqrt{-3})$, gdzie

(10) $$a+b\sqrt{-3}\neq\pm 1 \quad \text{i} \quad c+d\sqrt{-3}\neq\pm 1.$$

Mnożąc obie strony takiej równości przez iloczyn

$$(a-b\sqrt{-3})(c-d\sqrt{-3}),$$

otrzymujemy — jak łatwo widzieć — dla każdej z tych trzech liczb

$$4=(a^2+3b^2)(c^2+3d^2).$$

Gdyby żaden z czynników po prawej stronie nie był jednością, to byłoby $a^2+3b^2=2$, skąd $b=0$ i $a^2=2$ wbrew założeniu, że a jest liczbą całkowitą wymierną. Jeżeli zaś np. $a^2+3b^2=1$, o $b=0$ i $a=\pm 1$, skąd $a+b\sqrt{-3}=\pm 1$ wbrew założeniu (10).

Widzimy więc, że rozpatrywana definicja liczb całkowitych ciała $K(\sqrt{D})$ nie dałaby nam możności rozwinąć arytmetyki liczb całkowitych tego ciała już dla $D=\sqrt{-3}$.

Okazuje się jednak, że można tę definicję tak zmodyfikować, by tej niedogodności uniknąć.

Mianowicie: *liczbą całkowitą ciała* $K(\sqrt{D})$ nazywać będziemy każdą liczbę x tego ciała, która spełnia równanie postaci

(11) $$x^2-px+q=0,$$

gdzie p i q są liczbami całkowitymi wymiernymi.

Twierdzenie 4. *Liczba całkowita ciała* $K(\sqrt{D})$, *która jest zarazem liczbą wymierną, jest liczbą całkowitą wymierną.*

Dowód. Niech m/l będzie liczbą wymierną w postaci ułamka nieprzywiedlnego, spełniającą równanie (11) o współczynnikach całkowitych. Zatem $l^2-plm+qm^2=0$ czyli $l^2=m(pl-qm)$, co dowodzi wobec $(l,m)=1$, że $m=1$. Tak więc $l/m=l$, c. b. d. o.

Zbadamy obecnie warunki konieczne i wystarczające, żeby liczba x postaci (7) była liczbą całkowitą ciała $K(\sqrt{D})$.

Jeżeli spełnia ona równanie (11), to

$$(a+b\sqrt{D})^2-pc(a+b\sqrt{D})+qc^2=0$$

czyli $a^2+b^2D-pac+qc^2+(2ab-pbc)\sqrt{D}=0$, skąd wobec niewymierności liczby $\sqrt{D}$:

(12) $$2ab-pbc=0,$$

(13) $$a^2+b^2D-pac+qc^2=0.$$

Gdyby było $b=0$, to liczba x byłaby wymierna i w myśl twierdzenia 4 na to, by była ona liczbą całkowitą ciała $K(\sqrt{D})$, musiałaby być liczbą całkowitą wymierną, skąd $c=1$ i $x=a$.

Załóżmy więc, że $b\neq 0$. Z równości (12) znajdujemy wówczas $a=pc/2$, wobec czego na mocy (13)

$$\frac{p^2c^2}{4}+b^2D-\frac{p^2c^2}{2}+qc^2=0,$$

skąd

(14) $$b^2D=\frac{p^2c^2}{4}-qc^2,$$

co możemy napisać też w postaci

(15) $$(2b)^2D=(p^2-4q)c^2.$$

Ponieważ liczba D jest z założenia niepodzielna przez żaden kwadrat większy od jedności, więc wzór (15) wskazuje, że $2b=rc$, czyli

(16) $$b=rc/2,$$

gdzie r jest liczbą całkowitą. Wobec $a=pc/2$ i (16) jest

(17) $$\frac{a+b\sqrt{D}}{c}=\frac{p+r\sqrt{D}}{2},$$

a na mocy (16) równość (15) daje $r^2D=p^2-4q$, skąd

(18) $$r^2D\equiv p^2 \pmod 4.$$

Rozróżnimy dwa przypadki:

1° $D\equiv 1 \pmod 4$. Kongruencja (18) przybiera wtedy postać

$$r^2\equiv p^2 \pmod 4,$$

co dowodzi, że liczby p i r są jednocześnie parzyste lub jednocześnie nieparzyste. Liczba

$$l=\frac{p-r}{2}$$

jest więc całkowita i wzór (17) można napisać w postaci

$$\frac{a+b\sqrt{D}}{c}=l+r\frac{1+\sqrt{D}}{2}.$$

2° $D\not\equiv 1 \pmod 4$. Zatem D jest niepodzielne przez $4=2^2$, skąd albo $D\equiv 2 \pmod 4$, albo $D\equiv 3 \pmod 4$.

Dla $D\equiv 2 \pmod 4$ kongruencja (18) przybiera postać

$$2r^2\equiv p^2 \pmod 4,$$

skąd widać, że p jest parzyste. Niech $p=2s$, skąd znowu

$$2r^2\equiv 4s^2 \pmod 4,$$

co dowodzi, że i r jest parzyste. Niech $r=2t$. Mamy tu więc na mocy (17)

$$\frac{a+b\sqrt{D}}{2}=s+t\sqrt{D}. \tag{19}$$

Dla $D\equiv 3 \pmod 4$ kongruencja (18) przybiera postać

$$-r^2\equiv p^2 \pmod 4,$$

skąd wynika, że r jest parzyste, ponieważ w przeciwnym razie byłoby $r^2\equiv -1 \pmod 4$ i $p^2\equiv -1 \pmod 4$, co niemożliwe. Jest przeto r, a wobec (18) również p parzyste i mamy znowu wzór (19).

Tak więc dochodzimy do wniosku, że warunkiem koniecznym na to, by liczba x ciała $K(\sqrt{D})$ była liczbą całkowitą tego ciała, jest, żeby dla pewnych u i v całkowitych wymiernych zachodziła równość

$$x=u+v\omega, \tag{20}$$

w której $\omega=\frac{1+\sqrt{D}}{2}$ lub $\omega=\sqrt{D}$ zależnie od tego, czy mamy $D\equiv 1 \pmod 4$, czy nie.

Ale i na odwrót, łatwo widzieć, że warunek ten jest wystarczający, tj. że każda liczba formy (20) dla u i v całkowitych wymiernych jest liczbą całkowitą ciała $K(\sqrt{D})$.

Istotnie, że x, wyznaczone ze wzoru (20), należy do ciała $K(\sqrt{D})$, jest widoczne; wystarczy więc okazać, że x spełnia pewne równanie postaci (11) o współczynnikach całkowitych wymiernych p i q.

Otóż jeżeli $D\not\equiv 1 \pmod 4$, to $\omega=\sqrt{D}$ i $x=u+v\sqrt{D}$, skąd $(x-u)^2=v^2D$; otrzymujemy więc równanie (11), biorąc $p=2u$ i $q=u^2-v^2D$. Jeżeli zaś $D\equiv 1 \pmod 4$, to mamy $\omega=\frac{1+\sqrt{D}}{2}$ oraz $x=u+v\frac{1+\sqrt{D}}{2}$, skąd $\left(x-u-\frac{v}{2}\right)^2=v^2\frac{D}{4}$ czyli

$$x^2-(2u+v)x+u^2+uv-v^2\frac{D-1}{4}=0$$

i znowu otrzymujemy równanie (11), biorąc

$$p=2u+v, \qquad q=u^2+uv-v^2\frac{D-1}{4},$$

przy czym liczby p i q są całkowite, ponieważ wobec $D\equiv 1 \pmod 4$ liczba $\frac{D-1}{4}$ jest całkowita.

Udowodniliśmy więc następujące

Twierdzenie 5. *Zbiór wszystkich liczb całkowitych ciała liczbowego $K(\sqrt{D})$ jest identyczny ze zbiorem wszystkich liczb formy*

$$u+v\omega,$$

gdzie u i v są liczbami całkowitymi wymiernymi oraz

$$\omega=\begin{cases}\frac{1+\sqrt{D}}{2}, & \text{gdy } D\equiv 1 \pmod 4\\ \sqrt{D}, & \text{gdy } D\not\equiv 1 \pmod 4.\end{cases} \tag{21}$$

Łatwo też widzieć, że każda liczba całkowita ciała $K(\sqrt{D})$ daje się w jeden tylko sposób przedstawić w postaci (20).

Z dowiedzionego twierdzenia 5 wynika z łatwością

Wniosek. *Dwie liczby sprzężone ciała $K(\sqrt{D})$ są jednocześnie całkowite lub niecałkowite.*

Istotnie, jeżeli $x=u+v\omega$ (gdzie u i v są liczbami całkowitymi wymiernymi) jest liczbą całkowitą ciała $K(\sqrt{D})$, to dla $D\not\equiv 1 \pmod 4$ jest

$$x=u+v\sqrt{D}, \qquad x'=u-v\sqrt{D},$$

skąd widać bezpośrednio, że x' też jest liczbą całkowitą ciała $K(\sqrt{D})$, a dla $D\equiv 1 \pmod 4$ jest

$$x=u+v\frac{1+\sqrt{D}}{2}, \qquad x'=u+v\frac{1-\sqrt{D}}{2}=u+v-v\frac{1+\sqrt{D}}{2},$$

skąd też wynika, że x' jest liczbą całkowitą ciała $K(\sqrt{D})$, ponieważ liczby $u+v$ i $-v$ są całkowite wymierne.

W szczególności liczby $\frac{1+\sqrt{-7}}{2}$ i $\frac{1-\sqrt{-7}}{2}$ są liczbami całkowitymi ciała $K(\sqrt{-7})$, a ponieważ, jak łatwo sprawdzić,

$$\left(\frac{1+\sqrt{-7}}{2}\right)^4+\left(\frac{1-\sqrt{-7}}{2}\right)^4=1,$$

więc równanie $x^4+y^4=z^4$ jest rozwiązalne w różnych od zera liczbach całkowitych ciała $K(\sqrt{-7})$.

Podobnie liczby $\frac{\sqrt{93}+3}{2}$ i $\frac{\sqrt{93}-3}{2}$ są liczbami całkowitymi dodatnimi ciała $K(\sqrt{93})$, a ponieważ, jak łatwo sprawdzić,

$$6^3+\left(\frac{\sqrt{93}-3}{2}\right)^3=\left(\frac{\sqrt{93}+3}{2}\right)^3,$$

więc równanie $x^3+y^3=z^3$ jest rozwiązalne w liczbach całkowitych dodatnich ciała $K(\sqrt{93})$.

Łatwo też widzieć, że dla każdego n naturalnego niepodzielnego przez 3 jest

$$(1+\sqrt{-3})^n+(1-\sqrt{-3})^n+2^n=0,$$

więc równanie $x^n+y^n+z^n=0$ jest rozwiązalne dla wykładników naturalnych niepodzielnych przez 3 w różnych od zera liczbach całkowitych ciała $K(\sqrt{-3})$.

Tak więc *wielkie twierdzenie Fermata nie jest prawdziwe w pewnych ciałach liczbowych drugiego stopnia.*

Pizà zajmuje się w cytowanej już przez nas książce (p. str. 247) rozwiązaniami równania $x^n+y^n=z^n$ w liczbach, dających się zbudować z danej jednostki długości za pomocą cyrkla i liniału. Otrzymuje on np. rozwiązania:

$$12^3+(\sqrt{5}-9)^3=(\sqrt{5}+9)^3, \qquad 2^3+(2+i\sqrt{2})^3+(2-i\sqrt{2})^3=0.$$

W ciele $K(\sqrt{-3})$ jest $\omega=\frac{1+\sqrt{-3}}{2}$. Każda więc liczba całkowita tego ciała jest postaci

$$u+v\frac{1+\sqrt{-3}}{2}, \tag{22}$$

gdzie u i v są liczbami całkowitymi wymiernymi, i na odwrót.

Liczby 2 *i* $1+\sqrt{-3}$ *ciała* $K(\sqrt{-3})$ *są stowarzyszone*, ponieważ liczby

$$(1+\sqrt{-3}):2=\frac{1+\sqrt{-3}}{2} \quad \text{i} \quad 2:(1+\sqrt{-3})=1-\frac{1+\sqrt{-3}}{2}$$

są w tym ciele całkowite.

Liczba 2 *jest w ciele* $K(\sqrt{-3})$ *liczbą pierwszą.* Istotnie, z $z|2$ wynika $N(z)|N(2)=4$, a że z, jako liczba całkowita tego ciała, jest postaci (22), więc mielibyśmy $(2u+v)^2+3v^2|16$, co dla u i v całkowitych może zachodzić tylko wtedy, gdy albo $v=0$ oraz $z=u=\pm 1$ lub $z=u=\pm 2$, albo $v=\pm 1$ oraz $u=0$ lub $u=\mp 1$, co daje w obu przypadkach $z=\pm\frac{1}{2}(1+\sqrt{-3})$, albo wreszcie $v=\pm 2$ oraz $u=0$ lub $u=\mp 2$, co daje $z=\pm(1+\sqrt{-3})$ lub $z=\mp(1-\sqrt{3})$.

W każdym z tych przypadków liczba z jest stowarzyszona bądź z 1 bądź z 2.

Liczba 2, jako mająca w ciele $K(\sqrt{-3})$ jedynie dzielniki stowarzyszone z nią samą albo z jednością, jest więc liczbą pierwszą w tym ciele.

Twierdzenie 6. *Dla każdych dwu liczb całkowitych* z *i* $t\neq 0$ *ciała* $K(\sqrt{-3})$ *istnieją takie liczby całkowite* c *i* r *tego ciała, że*

$$z=ct+r \quad \text{i} \quad N(r)<\tfrac{1}{2}N(t). \tag{23}$$

Dowód. Niech

$$z/t=x+y\sqrt{-3},$$

gdzie x i y są liczbami wymiernymi. Oznaczmy przez η liczbę całkowitą wymierną najbliższą do $2y$, a przez ξ liczbę całkowitą wymierną najbliższą do $x-\eta/2$ i niech

$$x=\xi+\frac{\eta}{2}+x_1, \qquad y=\frac{\eta}{2}+y_1;$$

zatem $|2y-\eta|\leqslant\frac{1}{2}$ i $|x-\frac{\eta}{2}-\xi|\leqslant\frac{1}{2}$, skąd $|y_1|\leqslant\frac{1}{4}$ i $|x_1|\leqslant\frac{1}{2}$.

Niech teraz

$$c=\xi+\eta\frac{1+\sqrt{-3}}{2}, \qquad r=z-ct.$$

Liczby c i r są więc liczbami całkowitymi ciała $K(\sqrt{-3})$ i zachodzi pierwszy ze wzorów (23). Zarazem

$$r=t\left[x-\xi-\frac{\eta}{2}+\left(y-\frac{\eta}{2}\right)\sqrt{-3}\right]=t(x_1+y_1\sqrt{-3}),$$

a ponieważ

$$N(x_1+y_1\sqrt{-3})=x_1^2+3y_1^2\leqslant\frac{1}{4}+\frac{3}{16}=\frac{7}{16}<\frac{1}{2},$$

więc zachodzi również drugi ze wzorów (23), c. b. d. o.

Widzimy równocześnie, że dla ciała $K(\sqrt{-3})$ zachodzi algorytm analogiczny do algorytmu Euklidesa. Podobnie jak dla liczb ciała $K(\sqrt{-1})$ wynika stąd (por. Rozdział XVI, § 4), że liczby nierozkładalne ciała $K(\sqrt{-3})$ grają w tym ciele rolę liczb pierwszych.

Wyprowadzimy stąd teraz twierdzenie, z którego skorzystamy w dowodzie wielkiego twierdzenia Fermata dla wykładnika 3 (p. § 9, str. 439).

Twierdzenie 7. *Jeżeli liczby naturalne p i q są względnie pierwsze, p jest niepodzielne przez 3, a liczba p^2+3q^2 jest sześcianem liczby naturalnej, to istnieją takie liczby całkowite wymierne t i u, że*

$$p=t(t^2-9u^2), \qquad q=3u(t^2-u^2).$$

Dowód. Niech $p^2+3q^2=n^3$, gdzie n jest liczbą naturalną. Okażemy, że liczby całkowite ciała $K(\sqrt{-3})$

$$p+q\sqrt{-3} \quad \text{i} \quad p-q\sqrt{-3}$$

są w tym ciele względnie pierwsze.

Przypuśćmy, że $t|p+q\sqrt{-3}$ i $t|p-q\sqrt{-3}$ w ciele $K(\sqrt{-3})$. Wnosimy stąd od razu że jest w nim również $t|2p$ i $t|2q\sqrt{-3}$, tym bardziej więc $t|6$. Ponieważ jednak liczby p i $3q$ są względnie pierwsze w ciele liczb wymiernych, a przeto (wobec twierdzenia 2 Rozdziału II, str. 29) również w każdym innym ciele, więc t musi być dzielnikiem liczby 2. Ponieważ jednak 2 jest w ciele $K(\sqrt{-3})$ liczbą pierwszą (p. str. 427), więc jeżeli $t\neq\pm1$, to bądź $t=2$, bądź t jest liczbą stowarzyszoną z 2, a zatem musiałoby być $2|p+q\sqrt{-3}$ i $2|p-q\sqrt{-3}$, skąd $4|p^2+3q^2=n^3$ i przeto n byłoby postaci $n=2m$, gdzie m jest liczbą całkowitą wymierną. Mielibyśmy więc $p^2+3q^2=8m^3$, a przeto

$$8|(p+q\sqrt{-3})(p-q\sqrt{-3}) \quad \text{i} \quad 2|\frac{p+q\sqrt{-3}}{2}\cdot\frac{p-q\sqrt{-3}}{2},$$

skąd wynika, że co najmniej jedna z liczb $\frac{p+q\sqrt{-3}}{2}$ i $\frac{p-q\sqrt{-3}}{2}$ musiałaby być podzielna przez 2. Ale — jak łatwo widzieć — z $2|\frac{p+q\sqrt{-3}}{2}$ wynika $2|\frac{p-q\sqrt{-3}}{2}$ i na odwrót. Liczby $p+q\sqrt{-3}$ i $p-q\sqrt{-3}$ byłyby więc obie podzielne przez 4, co niemożliwe, gdyż — jak dowiedliśmy — każdy wspólny dzielnik t tych liczb jest dzielnikiem liczby 2.

Udowodniliśmy więc, że liczby $p+q\sqrt{-3}$ i $p-q\sqrt{-3}$ są w ciele $K(\sqrt{-3})$ względnie pierwsze. Stąd i z równości

$$(p+q\sqrt{-3})(p-q\sqrt{-3})=n^3$$

wnosimy zupełnie tak samo jak dla liczb naturalnych, że istnieje w ciele $K(\sqrt{-3})$ liczba z, dla której

$$p+q\sqrt{-3}=z^3. \tag{24}$$

Jest więc $z=x+y\frac{1+\sqrt{-3}}{2}$, gdzie x i y są liczbami całkowitymi wymiernymi. Porównując we wzorze (24) po obu stronach części rzeczywiste i części urojone, otrzymujemy:

$$p=\left(x+\frac{y}{2}\right)^3-9\left(x+\frac{y}{2}\right)\frac{y^2}{4}, \qquad q=3\left(x+\frac{y}{2}\right)^2\frac{y}{2}-\frac{3y^3}{8},$$

skąd

$$2p=(2x+y)(x^2+xy-2y^2), \qquad 2q=3xy(x+y). \tag{25}$$

Jeżeli y jest parzyste, to dla $y=2u$ i $t=x+u$ jest na mocy wzorów (25)

$$p=t(t^2-9u^2), \qquad q=3u(t^2-u^2). \tag{26}$$

Jeżeli zaś y i x są nieparzyste, a więc $x+y$ i $x-y$ parzyste, to dla $x+y=-2u$ i $x-y=-2t$ wzory (25) znowu dają (26).

Jeżeli wreszcie y jest nieparzyste, a x parzyste, to $x=2u$ i dla $t=-(u+y)$ znowu dostajemy z (25) wzory (26).

Tym samym twierdzenie 7 zostało dowiedzione.

Rozumiejąc ogólnie przez *algorytm Euklidesa w ciele $K(\sqrt{D})$*, gdzie D nie jest podzielne przez żaden kwadrat różny od 1, istnienie do każdych z i $t\neq0$ całkowitych tego ciała takiego c całkowitego tegoż ciała, że

$$|N(z-ct)|<|N(t)|,$$

L. E. Dickson dowiódł, że spośród D ujemnych algorytm ten zachodzi tylko dla $D=-1, -2, -3, -7$ i -11. Wyznaczanie D dodatnich, dla których zachodzi tak rozumiany algorytm Euklidesa, jest bardzo trudne [1]). P. Erdös i Ko dowiedli, że

[1]) Co do historii tego zagadnienia ob. A. Brauer, American Journal of Mathematics, tom 62 (1940), str. 697-716, oraz L. Rédei, Mathematische Annalen, tom 118 (1942), str. 588-608.

dla dostatecznie wielkich liczb pierwszych p (według Hua dla $p \geqslant e^{250}$) algorytm Euklidesa nie zachodzi w ciele $K(\sqrt{p})$ [1]).

§ 5. Twierdzenie o sumie, różnicy i iloczynie liczb całkowitych. Wyprowadzimy teraz dalsze wnioski z twierdzenia 5.

Twierdzenie 8. *Suma, różnica i iloczyn dwu (różnych lub równych) liczb całkowitych ciała $K(\sqrt{D})$ jest znowu liczbą całkowitą tego ciała.*

Dowód. Niech x i y będą liczbami całkowitymi ciała $K(\sqrt{D})$. Na mocy twierdzenia 5 możemy je więc przedstawić w postaci

$$x = u + v\omega, \qquad y = s + t\omega,$$

gdzie u, v, s i t są liczbami całkowitymi wymiernymi, ω zaś spełnia wzór (21). Równość

$$x \pm y = u \pm s + (v \pm t)\omega$$

dowodzi natychmiast, że liczby $x+y$ i $x-y$ są całkowite. Wystarczy więc okazać, że xy jest całkowite.

Jeżeli $D \not\equiv 1 \pmod 4$, to

$$xy = (u + v\sqrt{D})(s + t\sqrt{D}) = us + vtD + (ut + vs)\sqrt{D},$$

skąd widać, że liczba xy jest w ciele $K(\sqrt{D})$ całkowita.

Jeżeli zaś $D \equiv 1 \pmod 4$, to

$$xy = (u + v\omega)(s + t\omega) = us + (ut + vs)\omega + vt\omega^2,$$

a że w tym przypadku

$$\omega^2 = \left(\frac{1+\sqrt{D}}{2}\right)^2 = \frac{D-1}{4} + \frac{1+\sqrt{D}}{2} = \frac{D-1}{4} + \omega,$$

więc

$$x \cdot y = us + \frac{D-1}{4} vt + (ut + vs + vt)\omega,$$

skąd znowu widać wobec całkowitości liczby $\frac{D-1}{4}$, że xy jest liczbą całkowitą ciała $K(\sqrt{D})$, c. b. d. o.

Z twierdzenia 8 wynika natychmiast, że norma liczby całkowitej ciała $K(\sqrt{D})$ jest liczbą całkowitą, a że norma jest zawsze liczbą wymierną (p. str. 421), więc w danym razie jest to liczba

[1]) Ob. S. Min, Journal of London Mathematical Society, tom 22 (1947), str. 88.

całkowita wymierna. Widać to zresztą i bezpośrednio ze wzorów dla normy. Mianowicie

$$N(u + v\omega) = \begin{cases} u^2 - Dv^2, & \text{jeżeli } D \not\equiv 1 \pmod 4, \\ u^2 + uv - \frac{D-1}{4} v^2, & \text{jeżeli } D \equiv 1 \pmod 4. \end{cases}$$

§ 6. Podzielność liczb całkowitych. Dzielniki jedności. Powiadamy, że liczba α, całkowita w ciele $K(\sqrt{D})$, jest *podzielna* przez liczbę całkowitą β tegoż ciała, jeżeli istnieje w nim taka liczba całkowita γ, że

$$\alpha = \beta\gamma.$$

Mówimy też wtedy, że β jest *dzielnikiem* liczby α.

Na bliższą uwagę zasługują dzielniki liczby 1. Dzielniki te są oczywiście wspólnymi dzielnikami wszystkich liczb całkowitych ciała $K(\sqrt{D})$ i na odwrót.

Niech liczba ε, całkowita w ciele $K(\sqrt{D})$, będzie dzielnikiem liczby 1. Istnieje więc w ciele $K(\sqrt{D})$ taka liczba całkowita η, że $\varepsilon\eta = 1$. Normując obie strony, otrzymujemy równość

$$N(\varepsilon)N(\eta) = 1,$$

a ponieważ norma liczby całkowitej ciała $K(\sqrt{D})$ jest liczbą całkowitą wymierną, więc

$$N(\varepsilon) = \pm 1.$$

Odwrotnie, niech liczba ε, całkowita w ciele $K(\sqrt{D})$, ma normę ± 1. Oznaczając przez ε' liczbę sprzężoną z ε, możemy więc napisać

$$\pm \varepsilon\varepsilon' = 1,$$

co dowodzi, że ε jest dzielnikiem liczby 1. Mamy zatem

Twierdzenie 9. *Na to, by liczba ε, całkowita w ciele $K(\sqrt{D})$, była dzielnikiem jedności, potrzeba i wystarcza, żeby bezwzględna wartość jej normy była równa jedności.*

§ 7. Wyznaczanie wszystkich dzielników jedności. Wyznaczymy obecnie wszystkie dzielniki jedności w ciele $K(\sqrt{D})$. Rozróżnimy w tym celu następujące przypadki:

1° $D < 0$ i $D \not\equiv 1 \pmod 4$. Ponieważ w tym przypadku

$$N(u + v\omega) = u^2 - Dv^2,$$

więc na to, by liczba całkowita $\varepsilon = u + v\omega$ była dzielnikiem jedności, potrzeba i wystarcza, żeby było

$$|u^2 - Dv^2| = 1,$$

a że dla $D<0$ liczba $u^2 - Dv^2$ jest zawsze nieujemna, więc ostatnie równanie możemy napisać w postaci

$$u^2 - Dv^2 = 1. \tag{27}$$

Dla $D=-1$ mamy — jak łatwo widzieć — cztery układy rozwiązań:

$$1,\ 0, \qquad -1,\ 0, \qquad 0,\ 1 \qquad 0,\ -1,$$

zatem istnieją też cztery dzielniki jedności w ciele $K(\sqrt{-1})$, mianowicie

$$1, \qquad -1, \qquad \sqrt{-1}, \qquad -\sqrt{-1}.$$

Dla $D<-1$ musi być $v=0$ w równaniu (27), gdyż w przeciwnym razie byłoby $-Dv^2>1$ i lewa strona równania (27) byłaby większa od 1. Istnieją więc wtedy — jak łatwo widzieć — tylko dwa dzielniki jedności w ciele $K(\sqrt{D})$ mianowicie 1 i -1.

2° $D<0$ i $D\equiv 1 \pmod 4$. Ponieważ w tym przypadku

$$N(u+v\omega) = \left(u+\frac{v}{2}\right)^2 - D\frac{v^2}{4},$$

więc dla $\varepsilon = u + v\omega$ warunek $|N(\varepsilon)|=1$ ma postać

$$|(2u+v)^2 - Dv^2| = 4$$

czyli wobec $D<0$

$$(2u+v)^2 - Dv^2 = 4. \tag{28}$$

Dla $D<-4$ musi być w tym równaniu $v=0$, gdyż inaczej byłoby $-Dv^2>4$. Istnieją więc w ciele $K(\sqrt{D})$ tylko dwa dzielniki jedności, mianowicie 1 i -1.

Z drugiej strony — jak łatwo widzieć — tylko liczba $D=-3$ spełnia w rozważanym przypadku warunek $0>D\geqslant -4$. Równanie (28) przybiera więc postać

$$(2u+v)^2 + 3v^2 = 4. \tag{29}$$

Jeżeli $v=0$, to $(2u)^2=4$ czyli $u=\pm 1$; jeżeli zaś $v=1$, to $(2u+1)^2+3=4$, skąd $2u+1=\pm 1$ czyli $u=0$ lub $u=-1$; wreszcie jeżeli $v=-1$, to $(2u-1)^2+3=4$, skąd $2u-1=\pm 1$

czyli $u=1$ lub $u=0$. Innych zaś wartości prócz 0, 1 i -1 liczba v mieć nie może, ponieważ wtedy byłoby $v^2\geqslant 4$, skąd $3v^2>4$, co niemożliwe wobec (29).

Tak więc dla $D=-3$ dochodzimy do wniosku, że w ciele $K(\sqrt{-3})$ istnieje sześć dzielników jedności, mianowicie:

$$1, \qquad \omega = \frac{1+\sqrt{-3}}{2}, \qquad 1-\omega = \frac{1-\sqrt{-3}}{2},$$

$$-1, \qquad -\omega = -\frac{1+\sqrt{-3}}{2}, \qquad -1+\omega = -\frac{1+\sqrt{-3}}{2}.$$

Ponieważ $-\omega^{-1} = \frac{-1+\sqrt{-3}}{2} = -1+\omega$, więc dzielniki te możemy jeszcze przedstawić w postaci

$$\pm 1, \qquad \pm\omega, \qquad \pm\omega^{-1}.$$

3° $D>0$ i $D\not\equiv 1 \pmod 4$. Wyznaczymy tu wszystkie dzielniki jedności $\varepsilon = u + v\sqrt{D}$ z równania

$$u^2 - Dv^2 = \pm 1. \tag{30}$$

Na mocy twierdzenia 4 z Rozdziału XI (§ 2, str. 259) równanie to ma w liczbach całkowitych u, v nieskończenie wiele rozwiązań, które otrzymujemy ze wzoru

$$u + v\sqrt{D} = \pm(u_1 + v_1\sqrt{D})^n,$$

gdzie $n=0, \pm 1, \pm 2, \ldots$, a u_1, v_1 jest najmniejszym rozwiązaniem dodatnim równania (30).

Pisząc $\varepsilon_1 = u_1 + v_1\sqrt{D}$, możemy więc powiedzieć, że wszystkie dzielniki jedności zawarte są we wzorze

$$\varepsilon = \pm\varepsilon_1^n,$$

gdzie $n=0, \pm 1, \pm 2, \ldots$, a ε_1 jest tzw. *podstawowym dzielnikiem* jedności.

4° $D>0$ i $D\equiv 1 \pmod 4$. Równanie $N(u+v\omega)=\pm 1$ przybiera tu postać

$$(2u+v)^2 - Dv^2 = \pm 4. \tag{31}$$

Niech

$$x = 2u+v, \qquad y = v. \tag{32}$$

Jeżeli liczby całkowite u, v spełniają równanie (31), to liczby x, y wyznaczone ze wzorów (32) też są całkowite i spełniają równanie

$$x^2 - D y^2 = \pm 4; \tag{33}$$

na odwrót, jeżeli liczby całkowite x, y spełniają równanie (33), to liczby u, v wyznaczone ze wzorów (32), czyli liczby

$$u = \frac{x-y}{2}, \qquad v = y$$

są całkowite (gdyż wobec $D \equiv 1 \pmod 4$), liczby x, y, spełniające równanie (33), muszą być albo obie parzyste, albo obie nieparzyste) i spełniają równanie (31).

Można dowieść, że równanie (33) ma w rozważanym przypadku nieskończenie wiele rozwiązań w liczbach całkowitych, które otrzymujemy ze wzoru

$$\frac{x + y\sqrt{D}}{2} = \pm\left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^n,$$

gdzie $n = 0, \pm 1, \pm 2, \ldots$, a x_1, y_1 jest najmniejszym rozwiązaniem dodatnim tego równania [1]). Zatem wszystkie dzielniki jedności są zawarte we wzorze

$$\varepsilon = u + v\omega = \frac{x-y}{2} + y\frac{1+\sqrt{D}}{2} = \frac{x + y\sqrt{D}}{2} = \pm\left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^n,$$

czyli — pisząc $\varepsilon_1 = \frac{x_1 + y_1\sqrt{D}}{2}$ — we wzorze

$$\varepsilon = \pm \varepsilon_1^n,$$

gdzie $n = 0, \pm 1, \pm 2, \ldots$

Wyniki, otrzymane we wszystkich czterech rozpatrzonych przypadkach, możemy ująć w następujące

Twierdzenie 10. *W każdym ciele $K(\sqrt{D})$ istnieje podstawowy dzielnik jedności ε_1 o tej własności, że wszystkie dzielniki jedności w tym ciele i tylko one są zawarte we wzorze*

$$\pm \varepsilon_1^n,$$

gdzie n jest liczbą całkowitą wymierną.

[1]) Ob. drugie wydanie tej książki (z 1925 r.), str. 223.

W szczególności dla $D = -1$ istnieją 4 różne dzielniki jedności, dla $D = -3$ jest ich 6, dla wszystkich zaś innych D ujemnych — tylko 2, a dla $D > 0$ — nieskończenie wiele.

Oto podstawowe dzielniki jedności w kilku ciałach $K(\sqrt{D})$:

w $K(\sqrt{2})$ $\varepsilon_1 = 1 + \sqrt{2}$, w $K(\sqrt{3})$ $\varepsilon_1 = 2 + \sqrt{3}$,

w $K(\sqrt{5})$ $\varepsilon_1 = \frac{1+\sqrt{5}}{2}$,

w $K(\sqrt{6})$ $\varepsilon_1 = 5 + 2\sqrt{6}$, w $K(\sqrt{7})$ $\varepsilon_1 = 8 + 3\sqrt{7}$.

Sommer[1]) podaje tabliczkę podstawowych dzielników jedności w ciałach $K(\sqrt{D})$ dla $0 < D \leqslant 101$.

§ 8. Liczby nierozkładalne. Przykład niejednoznaczności rozkładu na czynniki nierozkładalne. Dwie liczby całkowite μ i ν danego ciała liczbowego, podzielne jedna przez drugą, tj. takie, że $\mu|\nu$ i $\nu|\mu$, nazywamy *stowarzyszonymi* (p. str. 382). W kwestiach podzielności każdą liczbę całkowitą można zastąpić przez stowarzyszoną z nią (korzystaliśmy już z tego w dowodzie twierdzenia 7, str. 428), gdyż jeżeli liczba μ jest stowarzyszona z liczbą ν, liczba zaś μ_1 — z liczbą ν_1, to podzielność $\mu|\mu_1$ pociąga za sobą podzielność $\nu|\nu_1$ i na odwrót.

Istotnie, załóżmy, że $\mu|\mu_1$. Skoro μ jest stowarzyszone z ν, a μ_1 z ν_1, to $\nu|\mu$ i $\mu_1|\nu_1$; z $\nu|\mu$, $\mu|\mu_1$ i $\mu_1|\nu_1$ wnosimy w jednej chwili, że $\nu|\nu_1$.

Twierdzenie 11. *Iloraz dwu liczb stowarzyszonych jest zawsze dzielnikiem jedności.*

Dowód. Niech μ i ν będą liczbami stowarzyszonymi. Wobec $\mu|\nu$ i $\nu|\mu$ możemy napisać $\nu = \varepsilon\mu$ i $\mu = \eta\nu$, gdzie ε i η są liczbami całkowitymi rozważanego ciała liczbowego. Ostatnie dwie równości dają $\nu = \varepsilon\eta\nu$, a ponieważ liczba ν, jako dzielnik liczby μ, nie może być zerem, więc

$$\varepsilon\eta = 1,$$

czyli liczby ε i η są dzielnikami jedności, c. b. d. o.

Ponieważ 1 jest oczywiście dzielnikiem każdej liczby całkowitej ciała liczbowego, więc w szczególności każdy dzielnik jedności jest liczbą stowarzyszoną z liczbą 1.

[1]) Ob. J. Sommer, *Vorlesungen über Zahlentheorie*, Lipsk-Berlin 1907, str. 355-358.

Każda liczba całkowita μ ciała liczbowego $K\sqrt{D}$ jest oczywiście podzielna przez liczby stowarzyszone z liczbą μ i przez liczby stowarzyszone z liczbą 1; jeżeli liczba μ nie ma innych dzielników, to nazywamy ją *nierozkładalną*, ponieważ nie można jej wtedy rozłożyć na iloczyn dwu czynników (całkowitych w tym ciele), z których żaden nie byłby dzielnikiem liczby 1.

Definicja liczb nierozkładalnych przypomina więc definicję liczb pierwszych w ciele wymiernym.

Analogia z definicją liczb pierwszych nasuwa przypuszczenie że liczby nierozkładalne grają w teorii ciał liczbowych rolę podobną do roli liczb pierwszych w ciele liczb całkowitych wymiernych. Otóż liczby pierwsze zawdzięczają swą rolę w ciele liczb całkowitych wymiernych następującemu twierdzeniu: *jeżeli iloczyn dwu liczb całkowitych wymiernych jest podzielny przez liczbę pierwszą p, to co najmniej jeden z czynników jest podzielny przez p.* Z twierdzenia tego wynika jako wniosek jednoznaczność rozkładu na czynniki pierwsze.

Okazuje się jednak, że analogiczne twierdzenie dla liczb nierozkładalnych zachodzi nie w każdym ciele. Udowodnimy mianowicie, że w ciele $K(\sqrt{-5})$ iloczyn dwu liczb nierozkładalnych μ i ν może być podzielny przez liczbę nierozkładalną γ, pomimo że ani μ, ani ν nie jest podzielne przez γ.

Istotnie każda liczba całkowita ciała $K(\sqrt{-5})$ daje się w myśl twierdzenia 5 przedstawić w postaci

$$a+b\sqrt{-5},$$

gdzie a i b są liczbami całkowitymi wymiernymi.

Jedynymi dzielnikami jedności w ciele $K(\sqrt{-5})$ są — jak udowodniliśmy w § 7 — liczby $+1$ i -1 (p. str. 432). Dowiedziemy, że liczby 2, 3 i $1+\sqrt{-5}$ są w ciele $K(\sqrt{-5})$ nierozkładalne. Oczywiście żadna z tych liczb nie jest w ciele $K(\sqrt{-5})$ dzielnikiem jedności (gdyż jest różna od $+1$ i od -1).

Przypuśćmy, że istnieje rozkład

$$2=(a+b\sqrt{-5})(c+d\sqrt{-5}).$$

Biorąc kwadraty modułów po obu stronach, otrzymujemy

$$4=(a^2+5b^2)(c^2+5d^2).$$

Gdyby żaden z czynników po prawej stronie nie był równy 1, to byłoby $a^2+5b^2=2$ i $c^2+5d^2=2$, co niemożliwe, gdyż w razie $b=0$ byłoby $a^2=2$, a w razie $b\neq 0$ byłoby $2=a^2+5b^2\geqslant 5$. Musi więc być $a^2+5b^2=1$ lub $c^2+5d^2=1$, a zatem $a+b\sqrt{-5}$ lub $c+d\sqrt{-5}$ jest dzielnikiem jedności. Wnosimy stąd, że liczba 2 jest w ciele $K(\sqrt{-5})$ nierozkładalna.

Przypuśćmy z kolei, że istnieje rozkład

$$3=(a+b\sqrt{-5})(c+d\sqrt{-5}),$$

skąd jak wyżej

$$9=(a^2+5b^2)(c^2+5d^2).$$

Gdyby żaden z czynników po prawej stronie nie był równy 1, to byłoby $a^2+5b^2=3$ i $c^2+5d^2=3$, co niemożliwe, gdyż w razie $b=0$ byłoby $a^2=3$, w razie zaś $b\neq 0$ byłoby $a^2+5b^2\geqslant 5$. Wnosimy stąd jak wyżej, że liczba 3 jest w ciele $K(\sqrt{-5})$ nierozkładalna.

Przypuśćmy wreszcie, że istnieje rozkład

$$1+\sqrt{-5}=(a+b\sqrt{-5})(c+d\sqrt{-5}),$$

skąd jak wyżej

$$6=(a^2+5b^2)(c^2+5d^2).$$

Gdyby żaden z czynników po prawej stronie nie był równy 1, to byłoby $a^2+5b^2=2$ lub $a^2+5b^2=3$, co — jak już widzieliśmy — jest niemożliwe. Wynika stąd jak wyżej, że liczba $1+\sqrt{-5}$ jest w ciele $K(\sqrt{-5})$ nierozkładalna.

Mimo to

$$2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5}),$$

co dowodzi, że iloczyn liczb nierozkładalnych 2 i 3 jest podzielny przez liczbę nierozkładalną $1+\sqrt{-5}$.

Udowodnimy teraz, że ani liczba 2, ani liczba 3 nie jest w ciele $K(\sqrt{-5})$ podzielna przez liczbę $1+\sqrt{-5}$.

Przypuśćmy, że $2=(1+\sqrt{-5})(x+y\sqrt{-5})$; zatem

$$2=x-5y+(x+y)\sqrt{-5},$$

skąd $x-5y=2$ i $x+y=0$, a więc $x={}^1/_3$ wbrew całkowitości liczby $x+y\sqrt{-5}$ w ciele $K(\sqrt{-5})$.

Przypuśćmy teraz, że $3=(1+\sqrt{-5})(x+y\sqrt{-5})$; podobnie jak przed chwilą, otrzymalibyśmy $x={}^1/_2$, znowu wbrew całkowitości liczby $x+y\sqrt{-5}$ w ciele $K(\sqrt{-5})$.

Tak więc *iloczyn dwu liczb 2 i 3, nierozkładalnych w ciele $K(\sqrt{-5})$ jest podzielny przez liczbę $1+\sqrt{-5}$, również nierozkładalną w tym ciele, pomimo że żaden z czynników nie jest przez nią podzielny.*

Oczywiście w tym wyniku nie ma żadnego paradoksu: dowodzi on tylko, że liczby nierozkładalne nie grają w rozpatrywanym ciele liczbowym tej roli, co liczby pierwsze w ciele liczb całkowitych wymiernych, jakby się tego można było spodziewać pod wrażeniem pewnej analogii.

Analogia z ciałem liczb wymiernych daje się jednak uratować przez nowe rozszerzenie pojęcia liczby. Dołączymy mianowicie do zbioru liczb całkowitych ciała $K(\sqrt{D})$ pewne elementy i określimy dla nich mnożenie w ten sposób, żeby nowy zbiór zachował jak najdalej idące analogie ze zbiorem liczb całkowitych wymiernych. Zajmiemy się tym w Rozdziale XVIII.

Teraz zaś jako zastosowanie teorii ciała liczbowego $K(\sqrt{-3})$, wyłożonej w § 4, udowodnimy wielkie twierdzenie Fermata dla wykładnika 3.

§ 9. Dowód wielkiego twierdzenia Fermata dla $n=3$. Przypuśćmy, że istnieją takie trzy liczby całkowite x, y, z, różne od zera, że

$$x^3+y^3=z^3. \tag{34}$$

Możemy założyć, że liczby te są względnie pierwsze, gdyż inaczej wystarczyłoby je podzielić przez ich największy wspólny dzielnik. Gdyby dwie z tych liczb były parzyste, to i trzecia musiałaby być parzysta, co jednak niemożliwe, skoro są one względnie pierwsze. Zatem co najmniej dwie spośród liczb x, y, z są nieparzyste. Możemy założyć, że są to liczby x i y, gdyż w przeciwnym razie wystarczyłoby napisać równanie (34) w postaci $x^3+(-z)^3=(-y)^3$ lub $y^3+(-z)=(-x)^3$.

Jest więc

$$x+y=2p \quad \text{i} \quad x-y=2q,$$

gdzie p i q są liczbami całkowitymi. Możemy nawet założyć, że liczby p i q są naturalne, gdyż inaczej wystarczyłoby zmienić

ich znaki lub zastąpić x przez y i na odwrót (a napewno jest $x\neq y$, gdyż w przeciwnym razie byłoby $2x^3=z^3$, wbrew niewymierności liczby $\sqrt[3]{2}$, a także $x\neq -y$, gdyż $z\neq 0$).

Liczby p i q są względnie pierwsze, ponieważ

$$x=p+q, \quad y=p-q \quad \text{i} \quad (x,y)=1. \tag{35}$$

Ostatnie wzory dowodzą też, że liczby p i q nie mogą być obie parzyste, ani obie nieparzyste.

Wstawiając wartości (35) do równania (34), otrzymujemy

$$2p(p^2+3q^2)=z^3. \tag{36}$$

Zarazem na mocy (36) jest $2|z^3$, zatem $2|z$, skąd $2^3|z^3$. Ponieważ zaś jedna z liczb p i q jest parzysta, a druga nie, więc liczba p^2+3q^2 jest nieparzysta. Wobec tego wzór (36) daje $8|2p$, skąd $4|p$.

Przypuśćmy teraz, że p nie jest podzielne przez 3. Okażemy, że w tym przypadku

$$(2p, p^2+3q^2)=1. \tag{37}$$

Istotnie, niech h będzie taką liczbą pierwszą, że $h|2p$ i $h|p^2+3q^2$. Wobec nieparzystości liczby p^2+3q^2 musi być $h>2$. Wobec $h|2p$ i $h>2$ byłoby więc $h|p$, skąd $h|p^2$, a więc wobec $h|p^2+3q^2$ byłoby $h|3q^2$, co wobec $h|p$ i $(p,q)=1$ daje $h|3$ czyli $h=3$ wbrew przypuszczeniu, że p jest niepodzielne przez 3.

Udowodniliśmy więc, że niepodzielność liczby p przez 3 pociąga za sobą wzór (37). Z (36) i (37) wnosimy, że p^2+3q^2 jest sześcianem liczby naturalnej. W myśl twierdzenia 7 istnieją więc takie liczby całkowite wymierne t i u, że

$$p=t(t^2-9u^2), \quad q=3u(t^2-u^2), \tag{38}$$

skąd wnosimy wobec $(p,q)=1$, że

$$(t,u)=1. \tag{39}$$

Wzory (38) dowodzą też, że u i t^2-u^2 są nieparzyste (jako dzielniki liczby q), zatem że t jest parzyste. Zarazem t jest w myśl (38) niepodzielne przez 3, gdyż takie jest p.

Na mocy (36) i (37) liczba $2p$ jest sześcianem liczby naturalnej:

$$2p=n^3,$$

skąd na mocy (38)

$$2t(t+3u)(t-3u)=n^3. \tag{40}$$

Okażemy, że każde dwie z liczb

(41) $$2t, \quad t+3u, \quad t-3u$$

są względnie pierwsze.

Istotnie, liczby $t+3u$ i $t-3u$ są nieparzyste i niepodzielne przez 3, gdyż t jest parzyste i niepodzielne przez 3, a u jest nieparzyste. Gdyby więc miały one wspólny dzielnik pierwszy h, to byłoby $h>3$. Lecz w takim razie suma i różnica tych liczb czyli $2t$ i $6u$ byłyby podzielne przez h, skąd wypadłoby wobec $h>3$, że liczby t i u są podzielne przez h, wbrew (39). Jest więc

(42) $$(t+3u, t-3u)=1.$$

Gdyby z kolei liczby $2t$ i $t+3u$ miały wspólny dzielnik $h>1$, to byłby on też dzielnikiem ich różnicy $t-3u$, wbrew (42). Gdyby wreszcie liczby $2t$ i $t-3u$ miały wspólny dzielnik $h>1$, to byłby on też dzielnikiem ich różnicy $t+3u$, znowu wbrew (42).

Z tego, że — jak dowiedliśmy — każde dwie spośród liczb (41) są względnie pierwsze, wnosimy na mocy (40), że przy pewnych ξ, η i ζ całkowitych wymiernych jest

(43) $$2t=\zeta^3, \quad t-3u=\xi^3, \quad t+3u=\eta^3,$$

skąd

(44) $$\xi^3+\eta^3=\zeta^3,$$

gdzie wobec niepodzielności liczby t przez 3 liczby ξ, η i ζ — jak wskazują wzory (43) — też są niepodzielne przez 3. Jest zatem $\xi=3k\pm1$, skąd $\xi^3=27k^3\pm27k^2+9k\pm1\equiv\pm1 \pmod 9$ i podobnie $\eta^3\equiv\pm1 \pmod 9$ oraz $\zeta^3\equiv\pm1 \pmod 9$, skąd na mocy (44)

$$\pm1\pm1\equiv\pm1 \pmod 9,$$

co — jak łatwo sprawdzić — jest niemożliwe przy żadnej z 8 kombinacyj znaków $+$ i $-$. Przypuszczenie, że p nie jest podzielne przez 3, doprowadza więc do sprzeczności.

Mamy przeto $3|p$ i możemy napisać:

(45) $$p=3p_1, \quad q=q_1,$$

gdzie p_1 i q_1 są liczbami naturalnymi; stąd na mocy (36)

(46) $$18p_1(3p_1^2+q_1^2)=z^3.$$

Wobec $(p,q)=1$ jest tym bardziej $(p_1,q_1)=1$, skąd wynika na mocy (45), że liczba q_1 jest niepodzielna przez 3. Wobec parzystości

liczby p i nieparzystości liczby q liczba p_1 jest parzysta, a liczba q_1 nieparzysta. Liczba $3p_1^2+q_1^2$ nie jest więc podzielna ani przez 2, ani przez 3.

Okażemy, że

(47) $$(18p_1, 3p_1^2+2q_1^2)=1.$$

Istotnie, gdyby liczby $18p_1$ i $3p_1^2+q_1^2$ miały wspólny dzielnik pierwszy h, to wobec niepodzielności drugiej z tych liczb ani przez 2, ani przez 3, musiałoby być $h>3$; z $h|18p_1$ mielibyśmy więc $h|p_1$, a zatem z $h|3p_1^2+q_1^2$ mielibyśmy $h|q_1^2$, więc również $h|q_1$, wbrew $(p_1,q_1)=1$. Musi więc zachodzić wzór (47).

W myśl (46) i (47) jest

(48) $$18p_1=a_1^3, \quad 3p_1^2+q_1^2=b_1^3,$$

gdzie a_1 i b_1 są liczbami naturalnymi.

W myśl (47) i (48) istnieją na mocy twierdzenia 7 takie liczby całkowite wymierne t_1 i u_1, że

(49) $$q_1=t_1(t_1^2-9u_1^2), \quad p_1=3u_1(t_1^2-u_1^2),$$

skąd wnosimy wobec $(p_1,q_1)=1$, że $(t_1,u_1)=1$, i zarazem wobec nieparzystości liczby q_1, że liczba t_1 jest nieparzysta, a liczba u_1 parzysta. Na mocy (48) liczba a_1 jest podzielna przez 3; możemy więc napisać $a_1=3a_2$, gdzie a_2 jest liczbą naturalną, skąd $2p_1=3a_2^3$ na mocy (48), a zatem na mocy (49)

(50) $$2u_1(t_1+u_1)(t_1-u_1)=a_2^3.$$

Okażemy, że każde dwie z liczb

(51) $$2u_1, \quad t_1+u_1, \quad t_1-u_1$$

są względnie pierwsze.

Istotnie, liczby t_1+u_1 i t_1-u_1 są nieparzyste, gdyż t_1 jest nieparzyste, a u_1 parzyste. Każdy więc wspólny dzielnik liczb t_1 i u_1 jest nieparzysty. Jeżeli dalej $h|t_1+u$ i $h|t_1-u_1$, to $h|2t_1$ i $h|2u_1$, a zatem (wobec nieparzystości dzielnika h) $h|t_1$ i $h|u_1$, co niemożliwe dla $h>1$. Mamy więc $(t_1+u_1, t_1-u_1)=1$.

Podobnie, gdyby $h>1$ było wspólnym dzielnikiem liczb $2u_1$ i t_1+u_1, mielibyśmy $h|2u_1-(t_1+u_1)=u_1-t_1$ wbrew temu, że $(t_1+u_1, t_1-u_1)=1$. Mamy więc $(2u_1, t_1+u_1)=1$. Wreszcie stwierdzamy tak samo, że $(2u_1, t_1-u_1)=1$. Z tego, że każde dwie

spośród liczb (51) są względnie pierwsze, wnosimy na mocy równości (50), że

$$(52) \qquad 2u_1=\zeta^3, \qquad t_1+u_1=\xi^3, \qquad u_1-t_1=\eta^3,$$

gdzie ξ, η, ζ są liczbami całkowitymi wymiernymi, z których każde dwie są względnie pierwsze. Na mocy (52) jest zarazem

$$(53) \qquad \xi^3+\eta^3=\zeta^3$$

i liczba ζ jest parzysta, a więc liczby ξ i η — nieparzyste. Wreszcie, na mocy (49) i (52) jest $|\zeta^3|<p_1$, a że $p_1<p$ i w myśl (36) jest $p|z^3$, więc $|\zeta|<|z|$,

Żadna z liczb ξ, η, ζ nie jest zerem, gdyż wobec (50) i (52) byłoby wówczas $a_2=0$, co niemożliwe, ponieważ a_2 jest liczbą naturalną.

Wzór (53) daje zatem rozwiązanie równania (34) w liczbach względnie pierwszych różnych od 0, w którym niewiadoma parzysta jest co do wartości bezwzględnej mniejsza od niewiadomej z. Postępując z równaniem (53) jak wyżej z równaniem (34) itd., otrzymalibyśmy ciąg nieskończony liczb całkowitych różnych od zera i malejących co do wartości bezwzględnej, co niemożliwe. Tak więc równanie (34) nie jest rozwiązalne w liczbach całkowitych różnych od zera, c. b. d. o.

ROZDZIAŁ XVIII

WSTĘP DO TEORII IDEAŁÓW

§ 1. Ideały w ciele $K\sqrt{D}$. Forma kanoniczna ideałów. *Ideałem* ciała liczbowego $K(\sqrt{D})$ nazywamy każdy zbiór i liczb całkowitych tego ciała, zawierający przynajmniej jeden element różny od zera i mający następujące dwie własności:

I. Suma każdych dwu liczb zbioru i znowu należy do i.

II. Iloczyn każdej liczby zbioru i przez jakąkolwiek liczbę całkowitą ciała $K(\sqrt{D})$ należy do zbioru i.

Okażemy najpierw, że każdy ideał i zawiera co najmniej jedną liczbę naturalną. Istotnie niech $\mu=a+b\omega$ będzie liczbą różną od zera i należącą do ideału i. Rozróżnimy dwa przypadki:

1° $D\not\equiv 1 \pmod 4$. Wówczas $\mu=a+b\sqrt{D}$. Liczba $\mu=a-b\sqrt{D}$ jest w myśl twierdzenia 5 Rozdziału XVII (§ 4, str. 425) liczbą całkowitą ciała $K(\sqrt{D})$. W myśl własności II ideału wnosimy stąd, że liczba $\mu\mu'=a^2-b^2D$ też należy do i. Jest $\mu\mu'\neq 0$, ponieważ liczba $\sqrt{D}$ nie jest wymierna. Liczba $\mu\mu'=N(\mu)$ jest na mocy określenia całkowita wymierna. Zatem jeżeli $\mu\mu'<0$, to $-\mu\mu'$ jest liczbą naturalną, należącą do ideału i jako iloczyn liczby $\mu\mu'$ tego ideału przez liczbę całkowitą -1.

2° $D\equiv 1 \pmod 4$. Wówczas $\mu=a+b\frac{1+\sqrt{D}}{2}$. Liczba

$$\mu'=a+b-b\frac{1+\sqrt{D}}{2}$$

jest liczbą całkowitą ciała $K(\sqrt{D})$, różną od zera, gdyż inaczej byłoby $b=0$ i $a=0$, skąd $\mu=0$. Liczba $\mu'=a^2+ab-\frac{D-1}{4}b^2$ jest całkowita wymierna, różna od 0 i musi należeć do i, jak również liczba $-\mu\mu'$, a jedna z tych liczb jest naturalna.