

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

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

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

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

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

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 rozwiązywalne 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 całkowitą wymierną. 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 całkowitą wymierną, różną od 0 i musi należeć do i, jak również liczba $-\mu\mu'$, a jedna z tych liczb jest naturalna.

Z tego, że — jak dowiedliśmy — w każdym ideale i jest co najmniej jedna liczba naturalna n , wynika w myśl własności II, że do ideału i należą też wszystkie wielokrotności liczby n , a więc że każdy ideał zawiera nieskończenie wiele liczb naturalnych.

Niech i_0 będzie najmniejszą ze wszystkich liczb naturalnych, zawartych w ideale i . Wśród liczb $a+b\omega$, należących do tego ideału, znajdują się napewno i takie, w których b jest liczbą naturalną; liczbą taką jest np. w myśl własności II liczba $i_0\omega$.

Niech i_2 będzie najmniejszą taką liczbą naturalną, że dla pewnego całkowitego wymiernego $a=a_0$ liczba $a_0+i_2\omega$ należy do i . W myśl własności I i II do i należy więc liczba $ki_0+a_0+i_2\omega$ dla wszelkiego naturalnego k . Dla dostatecznie wielkich k liczba ki_0+a_0 jest oczywiście nieujemna; istnieją więc takie liczby całkowite nieujemne a , iż $a+i_2\omega$ należy do i .

Niech i_1 będzie najmniejszą z takich liczb a . Liczba $i_1+i_2\omega$ należy więc do i .

Niech teraz $a+b\omega$ będzie dowolną liczbą ideału i . Okażemy, że b jest podzielne przez i_2 ; wynika stąd w szczególności, że liczba i_0 jest podzielna przez i_2 , (ponieważ liczba $i_0\omega$ należy do i).

Istotnie, gdyby b przy dzieleniu przez i_2 dawało resztę dodatnią r oraz iloraz k , to liczba

$$a - ki_1 + r\omega = a + b\omega - k(i_1 + i_2\omega)$$

należałaby do ideału i wbrew określeniu liczby i_2 .

Możemy więc założyć, że

$$b = l_2 i_2,$$

gdzie l_2 jest liczbą całkowitą wymierną. Liczba rzeczywista

$$(1) \quad a - l_2 i_1 = a + b\omega - l_2(i_1 + i_2\omega)$$

należy do i . Wnosimy stąd analogicznie jak w dowodzie podzielności liczby b przez i_2 , że liczba $a - l_2 i_1$ jest podzielna przez i_0 :

$$a - l_2 i_1 = l_1 i_0,$$

gdzie l_1 jest liczbą całkowitą wymierną. Stąd na mocy (1)

$$(2) \quad a + b\omega = l_1 i_0 + l_2(i_1 + i_2\omega).$$

Dowiedliśmy więc, że każda liczba ideału i daje się przedstawić w postaci (2), gdzie l_1 i l_2 są liczbami całkowitymi wymiernymi.

Ale i na odwrót, każda liczba postaci (2) należy oczywiście do ideału i , gdyż liczby i_0 i $i_1 + i_2\omega$ należą do tego ideału.

Wreszcie, łatwo widzieć, że każda liczba ideału i daje się w jeden tylko sposób przedstawić w postaci (2) o l_1 i l_2 całkowitych wymiernych. Istotnie, na mocy (2) jest

$$a + b\omega = l_1 i_0 + l_2 i_1 + l_2 i_2 \omega,$$

skąd — jak łatwo widzieć — wynika $a = l_1 i_0 + l_2 i_1$ i $b = l_2 i_2$, a przeto współczynniki

$$(3) \quad l_1 = \frac{ai_2 - bi_1}{i_0 i_2} \quad i \quad l_2 = \frac{b}{i_2}$$

są w zupełności wyznaczone. Mamy więc

Twierdzenie 1. *Każdy ideał jest zbiorem wszystkich liczb postaci (2), gdzie i_0 oraz $i_1 + i_2\omega$ są pewnymi liczbami ideału, a l_1 i l_2 — liczbami całkowitymi wymiernymi, określonymi przez wzory (3).*

Tym sposobem ideał jest w zupełności określony przez liczby i_0 oraz $i_1 + i_2\omega$, i na odwrót. Będziemy pisali

$$(4) \quad i = [i_0, i_1 + i_2\omega]$$

i wzór ten nazywali *formą kanoniczną ideału*.

Każda liczba postaci

$$(5) \quad xi_0 + y(i_1 + i_2\omega),$$

gdzie x i y są liczbami całkowitymi ciała $K(\sqrt{D})$, należy oczywiście do ideału i (gdyż i_0 oraz $i_1 + i_2\omega$ należą do i). Z drugiej strony, w myśl twierdzenia 1 każda liczba ideału i jest zawarta we wzorze (5) przy pewnych całkowitych wymiernych x i y . Możemy więc wypowiedzieć

Wniosek. *Ideał i jest zbiorem wszystkich liczb postaci (5), gdzie x i y są liczbami całkowitymi ciała $K(\sqrt{D})$.*

Niech teraz (4) będzie formą kanoniczną ideału i . Jak zauważyliśmy wyżej, i_0 jest podzielne przez i_2 . Okażemy, że i_1 też jest podzielne przez i_2 .

Istotnie, jeżeli $D \not\equiv 1 \pmod{4}$, to $\omega = \sqrt{D}$ i liczba

$$-(i_1 + i_2\omega)\omega' = Di_2 + i_1\sqrt{D} = Di_2 + i_1\omega$$

należy do i , skąd wnosimy, że i_1 jest podzielne przez i_2 .

Jeżeli zaś $D \equiv 1 \pmod{4}$, to $\omega = \frac{1+\sqrt{D}}{2}$ i liczba

$$-(i_1 + i_2 \omega) \omega' = -i_1 + i_2 \frac{D-1}{4} + i_1 \omega$$

należy do i , skąd znowu wnosimy, że i_1 jest podzielne przez i_2 .

Możemy więc założyć, że

$$i_0 = a_0 i_2, \quad i_1 = a_1 i_2,$$

gdzie a_0 i a_1 są liczbami całkowitymi wymiernymi oraz $a_0 > 0$.

Okazemy teraz, że

$$(i_1 + i_2 \omega)(a_1 + \omega') = c i_0,$$

gdzie c jest liczbą całkowitą wymierną.

Istotnie, jeżeli $D \not\equiv 1 \pmod{4}$, to

$$(i_1 + i_2 \omega)(a_1 + \omega') = i_2(a_1 + \sqrt{D})(a_1 - \sqrt{D}) = (a_1^2 - D) i_2$$

jest liczbą całkowitą wymierną, należącą do ideału i , skąd wnosimy, że $(a_1^2 - D) i_2 = c i_0$, gdzie c jest całkowite wymierne, ponieważ — jak wynika z łatwością z określenia liczby i_0 — każda liczba całkowita wymierna, należąca do ideału i , jest podzielna przez i_0 .

Jeżeli zaś $D \equiv 1 \pmod{4}$, to

$$(i_1 + i_2 \omega)(a_1 + \omega') = \\ = i_2 \left(a_1 + \frac{1}{2} + \frac{\sqrt{D}}{2} \right) \left(a_1 + \frac{1}{2} - \frac{\sqrt{D}}{2} \right) = i_2 \left(a_1^2 + a_1 - \frac{D-1}{4} \right)$$

jest liczbą całkowitą wymierną należącą do ideału i , skąd wnosimy, że liczba ta jest równa $c i_0$, gdzie c jest całkowite wymierne.

Dowiedliśmy zarazem, że zawsze

$$(6) \quad N(i_1 + i_2 \omega) = (i_1 + i_2 \omega)(i_1 + i_2 \omega') = (i_1 + i_2 \omega)(a_1 + \omega') i_2 = c i_0 i_2,$$

gdzie c jest liczbą całkowitą wymierną. Ze wzoru tego skorzystamy w § 4.

§ 2. Ideały główne. Ideały jako uogólnienie liczb całkowitych. Niech $g_1, g_2, \dots, g_n$ będą dowolnymi liczbami całkowitymi ciała $K(\sqrt{D})$, z których przynajmniej jedna nie jest zerem. Łatwo widzieć, że zbiór wszystkich liczb postaci

$$(7) \quad x_1 g_1 + x_2 g_2 + \dots + x_n g_n,$$

gdzie $x_1, x_2, \dots, x_n$ są liczbami całkowitymi ciała $K(\sqrt{D})$, tworzy ideał.

Wystarczy w tym celu zauważyć, że w zbiorze tym jest co najmniej jedna liczba różna od 0 (mianowicie jedna z liczb g_i) i

$$(x_1 g_1 + x_2 g_2 + \dots + x_n g_n) + (y_1 g_1 + y_2 g_2 + \dots + y_n g_n) = \\ = (x_1 + y_1) g_1 + (x_2 + y_2) g_2 + \dots + (x_n + y_n) g_n.$$

$$z(x_1 g_1 + x_2 g_2 + \dots + x_n g_n) = (z x_1) g_1 + (z x_2) g_2 + \dots + (z x_n) g_n,$$

oraz że dla $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n$ i z całkowitych liczb

$$x_1 + y_1, \quad x_2 + y_2, \quad \dots, \quad x_n + y_n, \quad z x_1, \quad z x_2, \quad \dots, \quad z x_n$$

są również całkowite.

Ideał, utworzony w powyższy sposób, będziemy oznaczali przez

$$(8) \quad i = [g_1, g_2, \dots, g_n],$$

co jest oczywiście zgodne ze znakowaniem (4) formy kanonicznej ideału.

Łatwo widzieć, że każdy ideał, zawierający liczby $g_1, g_2, \dots, g_n$, zawiera w szczególności każdą liczbę postaci (7), a więc każdą liczbę ideału i .

Ideał i jest więc *najprostszym* ideałem, zawierającym każdą z liczb $g_1, g_2, g_3, \dots, g_n$.

Ideał (8) nie zależy oczywiście od porządku wyrazów $g_1, g_2, \dots, g_n$.

Łatwo też widzieć, że jeżeli liczba g_n należy do ideału $[g_1, g_2, \dots, g_{n-1}]$, to

$$(9) \quad [g_1, g_2, \dots, g_{n-1}, g_n] = [g_1, g_2, \dots, g_{n-1}],$$

skąd w szczególności (ponieważ 0 jest liczbą każdego ideału)

$$(10) \quad [g_1, g_2, \dots, g_k, 0] = [g_1, g_2, \dots, g_k].$$

Każdy ideał, dający się przedstawić w formie $i = [g]$ nazywamy *ideałem głównym*.

Ideał główny $[g]$ jest więc najprostszym ideałem zawierającym liczbę g .

Każda liczba ideału $[g]$ daje się przedstawić w formie iloczynu xg , gdzie x jest liczbą całkowitą ciała $K(\sqrt{D})$, i na odwrót, każdy iloczyn tej postaci należy do ideału $[g]$.

O dwu ideałach i_1 i i_2 mówimy, że są *równe*, pisząc

$$i_1 = i_2,$$

gdy każda liczba ideału i_1 jest zarazem liczbą ideału i_2 i na odwrót.

Niech dla dwu liczb całkowitych g_1 i g_2 ciała $K(\sqrt{D})$ zachodzi równość

$$[g_1] = [g_2].$$

Liczba g_1 jako liczba ideału $[g_1]$ musi należeć do ideału $[g_2]$; dla pewnego więc x_0 całkowitego w ciele $K(\sqrt{D})$ jest $g_1 = x_0 g_2$. Podobnie, dla pewnego y całkowitego w ciele $K(\sqrt{D})$ jest $g_2 = y_0 g_1$, skąd $g_1 = x_0 y_0 g_1$.

Liczba g_1 nie może być zerem, gdyż ideał $[g_1]$ zawiera przynajmniej jedną liczbę różną od zera; ostatnia równość daje więc po podzieleniu obu stron przez g_1

$$x_0 y_0 = 1,$$

co dowodzi, że x_0 i y_0 są dzielnikami jedności. Wynika stąd, że liczby g_1 i g_2 są stowarzyszone.

Na odwrót, niech liczby g_1 i g_2 będą stowarzyszone. Istnieją więc takie dzielniki jedności, x_0 i y_0 , że $g_1 = x_0 g_2$ i $g_2 = y_0 g_1$. Niech μ będzie jakąkolwiek liczbą ideału $[g_1]$. Jest więc $\mu = x g_1$ dla pewnego x całkowitego w ciele $K(\sqrt{D})$, skąd $\mu = (x x_0) g_2$, co dowodzi, że μ należy do ideału $[g_2]$. Podobnie dowiedlibyśmy, że każda liczba ideału $[g_2]$ należy do $[g_1]$. Mamy zatem

Twierdzenie 2. *Na to, by zachodziła równość ideałów $[g_1] = [g_2]$, potrzeba i wystarcza, żeby liczby g_1 i g_2 były stowarzyszone.*

Niech teraz j będzie ideałem głównym. Wszystkie liczby całkowite g ciała liczbowego $K(\sqrt{D})$, dla których $j = [g]$, tworzą na mocy twierdzenia 2 klasę liczb między sobą stowarzyszonych. Każdemu ideałowi głównemu odpowiada więc pewna klasa liczb stowarzyszonych. Lecz — jak łatwo widzieć — i na odwrót: każdej klasie liczb stowarzyszonych odpowiada pewien ideał główny, mianowicie zawierający wszystkie liczby danego ciała liczbowego, podzielne przez liczby tej klasy.

Widać stąd, że istnieje odpowiedniość wzajemnie jednoznaczna między ideałami głównymi a klasami liczb stowarzyszonych. Z tego punktu widzenia ideały można więc uważać za uogólnienie liczb całkowitych, ściślej: klas liczb stowarzyszonych.

§ 3. Iloczyn ideałów. Określmy teraz, co należy rozumieć przez *iloczyn* dwu ideałów i_1 i i_2 . Możemy je — jak wiadomo (p. wzór (4)) — przedstawić w postaci

$$i_1 = [g_1, h_1] \quad \text{ i } \quad i_2 = [g_2, h_2].$$

Założmy, że ideał i zawiera każdą liczbę

$$(11) \quad \mu_1 \mu_2,$$

która jest iloczynem jakiejkolwiek liczby ideału i_1 przez jakąkolwiek liczbę ideału i_2 . W szczególności więc ideał i zawiera liczby

$$g_1 g_2, \quad g_1 h_2, \quad h_1 g_2, \quad h_1 h_2,$$

a więc też każdą liczbę postaci

$$(12) \quad x g_1 g_2 + y g_1 h_2 + z h_1 g_2 + t h_1 h_2,$$

gdzie x, y, z, t są dowolnymi współczynnikami całkowitymi z ciała $K(\sqrt{D})$.

Zbiór wszystkich liczb postaci (12) tworzy ideał

$$i_0 = [g_1 g_2, g_1 h_2, h_1 g_2, h_1 h_2].$$

Okazemy, że ideał i_0 zawiera każdą liczbę postaci (11).

Istotnie, niech μ_1 i μ_2 będą dwiema liczbami należącymi odpowiednio do ideałów i_1 i i_2 . W myśl definicji symbolu $[g_1, h_1]$ istnieją więc w ciele $K(\sqrt{D})$ takie liczby całkowite u_1 i v_1 , że

$$\mu_1 = u_1 g_1 + v_1 h_1;$$

podobnie, istnieją w ciele $K(\sqrt{D})$ takie liczby całkowite u_2 i v_2 , iż

$$\mu_2 = u_2 g_2 + v_2 h_2.$$

Stąd

$$\mu_1 \mu_2 = u_1 u_2 g_1 g_2 + u_1 v_2 g_1 h_2 + v_1 u_2 h_1 g_2 + v_1 v_2 h_1 h_2.$$

Wystarczy więc przyjąć oznaczenia:

$$x = u_1 u_2, \quad y = u_1 v_2, \quad z = v_1 u_2, \quad t = v_1 v_2,$$

żeby się przekonać, że $\mu_1 \mu_2$ jest liczbą postaci (12), zatem liczbą ideału i_0 .

Zbierając wyniki tych rozważań, możemy wypowiedzieć

Twierdzenie 3. *Ideał i_0 jest najprostszym ideałem, zawierającym każdy iloczyn postaci (11).*

Utworzony w powyższy sposób ideał i_0 będziemy nazywali *iloczynem* ideałów i_1 i i_2 , pisząc

$$i_0 = i_1 \cdot i_2.$$

Jest więc

$$[g_1, h_1][g_2, h_2] = [g_1 g_2, g_1 h_2, h_1 g_2, h_1 h_2].$$

Z definicji iloczynu ideałów i_1 i i_2 jako najprostszego ideału, zawierającego wszystkie iloczyny postaci (11), widać, że iloczyn $i_1 \cdot i_2$ zależy jedynie od i_1 i i_2 , a nie zależy zaś od tego, w jakich formach $[g_1, h_1]$ i $[g_2, h_2]$ ideały te są przedstawione.

Jasne jest też, że iloczyn dwu ideałów podlega prawu *przemienności*, tj. nie zależy od porządku czynników.

Rozumując jak wyżej, dowodzi się z łatwością, że

$$[g_1, g_2, \dots, g_n][g, h] = [g_1 g, g_1 h, g_2 g, g_2 h, \dots, g_n g, g_n h].$$

Niech teraz dane będą trzy ideały i_1, i_2 i i_3 . Przedstawmy je w postaci

$$i_1 = [g_1, h_1], \quad i_2 = [g_2, h_2], \quad i_3 = [g_3, h_3].$$

Mamy

$$\begin{aligned} (i_1 \cdot i_2) \cdot i_3 &= [g_1 g_2, g_1 h_2, h_1 g_2, h_1 h_2] \cdot [g_3, h_3] = \\ &= [g_1 g_2 g_3, g_1 g_2 h_3, g_1 h_2 g_3, g_1 h_2 h_3, h_1 g_2 g_3, h_1 g_2 h_3, h_1 h_2 g_3, h_1 h_2 h_3], \end{aligned}$$

$$\begin{aligned} i_1 \cdot (i_2 \cdot i_3) &= [g_1, h_1][g_2 g_3, g_2 h_3, h_2 g_3, h_2 h_3] = \\ &= [g_1 g_2 g_3, g_1 g_2 h_3, g_1 h_2 g_3, g_1 h_2 h_3, h_1 g_2 g_3, h_1 g_2 h_3, h_1 h_2 g_3, h_1 h_2 h_3], \end{aligned}$$

skąd widać, że

$$(i_1 \cdot i_2) \cdot i_3 = i_1 \cdot (i_2 \cdot i_3),$$

czyli że iloczyn ideałów podlega też prawu *łączności*.

Z prawa łączności iloczynu trzech czynników wynika natychmiast przez indukcję prawo łączności dla każdej skończonej liczby czynników. Wobec prawa przemienności iloczynu dla dwu czynników mamy więc jeszcze (w zestawieniu z prawem łączności) prawo przemienności dla dowolnej skończonej liczby czynników.

§ 4. Dowód, że norma ideału jest ideałem głównym. Niech Z będzie zbiorem wszystkich liczb sprzężonych z liczbami ideału i . Okażemy, że zbiór Z jest ideałem.

Każda liczba zbioru Z jest oczywiście całkowita w ciele $K(\sqrt{D})$, jako sprzężona z pewną liczbą całkowitą tego ciała.

Niech x i y będą jakimikolwiek liczbami, należącymi do zbioru Z . Zatem liczby z nimi sprzężone x' i y' należą do ideału i . Liczba $x' + y' = (x + y)'$ też więc należy do i , a w takim razie liczba z nią sprzężona $(x + y)'' = (x + y)$ należy do zbioru Z . Tym sposobem suma dwu liczb zbioru Z jest zawsze liczbą zbioru Z .

Niech teraz t będzie liczbą całkowitą ciała $K(\sqrt{D})$. Zatem liczba $t'x' = (tx)'$ należy do i , ponieważ liczba x' należy do i . Wnosimy stąd, że liczba $(tx)'' = tx$ należy do Z . Zbiór Z posiada więc własności I i II, co dowodzi, że jest on ideałem.

Będziemy go nazywali *ideałem sprzężonym* z ideałem i i oznaczali przez i' .

Twierdzenie 4. Jeżeli $i = [g, h]$, to $i' = [g', h']$.

Dowód. Niech μ będzie jakąkolwiek liczbą ideału i' . Liczba μ' należy więc do ideału i . Zatem dla pewnych liczb całkowitych x i y ciała $K(\sqrt{D})$ jest $\mu' = xg + yh$, skąd $\mu = x'g' + y'h'$, czyli $\mu = \xi g' + \eta h'$, gdzie ξ i η są liczbami całkowitymi ciała $K(\sqrt{D})$. Dowodzi to, że μ należy do ideału

$$(13) \quad i_0 = [g', h'].$$

Niech teraz ν będzie jakąkolwiek liczbą ideału i_0 . Zatem dla pewnych liczb całkowitych x i y ciała $K(\sqrt{D})$ jest $\nu = xg' + yh'$, skąd $\nu' = x'g + y'h$, co dowodzi, że liczba ν' należy do i , a przeto, że liczba $\nu = (\nu)'$ należy do i' .

Każda liczba ideału i' należy więc do i_0 i na odwrót. Zatem $i' = i_0$, skąd na mocy (13) $i' = [g', h']$, c. b. d. o.

Tak samo dowiedlibyśmy ogólniej, że jeżeli $i = [g_1, g_2, \dots, g_n]$, to $i' = [g'_1, g'_2, \dots, g'_n]$.

Jako łatwy wniosek wynika stąd, że

$$(i_1 \cdot i_2)' = i_1' \cdot i_2',$$

co daje się również natychmiast uogólnić na dowolną skończoną liczbę czynników.

Iloczyn $i \cdot i'$ nazywamy *normą ideału* i i oznaczamy przez $N(i)$.

Twierdzenie 5. Jeżeli $i = [i_0, i_1 + i_2 \omega]$ jest formą kanoniczną ideału i , to

$$N(i) = [i_0 i_2].$$

Dowód. Niech μ będzie jakąkolwiek liczbą, należącą do ideału $N(i) = i \cdot i'$. Ponieważ

$$i = [i_0, i_1 + i_2 \omega], \quad i' = [i_0, i_1 + i_2 \omega'],$$

więc dla pewnych liczb całkowitych x, y, z, t ciała $K(\sqrt{D})$ jest

$$\mu = x i_0^2 + y i_0 (i_1 + i_2 \omega) + z i_0 (i_1 + i_2 \omega') + t (i_1 + i_2 \omega) (i_1 + i_2 \omega').$$

Lecz — jak dowiedliśmy w § 1 (str. 446) — jest $i_0 = a_0 i_2$ oraz $i_1 = a_1 i_2$, skąd

$$i_0^2 = a_0 i_0 i_2, \quad i_0 (i_1 + i_2 \omega) = (a_1 + \omega) i_0 i_2, \quad i_0 (i_1 + i_2 \omega') = (a_1 + \omega') i_0 i_2;$$

zatem na mocy (6) jest $(i_1 + i_2 \omega) (i_1 + i_2 \omega') = c i_0 i_2$; liczby a_0, a_1 i c są tu całkowite wymierne. Tak więc

$$\mu = (x a_0 + y (a_1 + \omega) + z (a_1 + \omega') + t c) i_0 i_2$$

czyli $\mu = u i_0 i_2$, gdzie u jest pewną liczbą całkowitą ciała $K(\sqrt{D})$. Każda liczba ideału $N(i)$ należy więc do ideału głównego $[i_0 i_2]$.

Aby udowodnić, że i na odwrót, wystarczy oczywiście okazać, że liczba $i_0 i_2$ należy do ideału $N(i)$. Rozróżnimy dwa przypadki:

1° $D \not\equiv 1 \pmod{4}$. Wówczas $\omega = \sqrt{D}$ i

$$N(i_1 + i_2 \omega) = i_1^2 - i_2^2 D = (a_1^2 - D) i_2^2,$$

$$c i_0 i_2 = c a_0 i_2^2,$$

a ponieważ $c i_0 i_2 = (i_1 + i_2 \omega) (i_1 + i_2 \omega') = i_1^2 - i_2^2 D$, więc

$$c = \frac{a_1^2 - D}{a_0}.$$

Gdyby liczby a_0 i D miały wspólny dzielnik pierwszy $q > 2$, to liczba $a_1^2 = D + c a_0$ też byłaby podzielna przez q , a więc i przez q^2 , gdyż jest kwadratem. Gdyby jeszcze liczba c była podzielna przez q , to liczba $D = a_1^2 - a_0 c$ byłaby podzielna przez q^2 , wbrew założeniu, że D nie ma dzielnika kwadratowego większego od 1. Zatem liczby a_0, D i c , a więc też liczby $a_0, 2D$ i c , nie mają wspólnego czynnika pierwszego $q > 2$.

Gdyby liczby a_0 i c były parzyste, to wobec $D = a_1^2 - a_0 c$ byłoby w razie a_1 parzystego $D \equiv 0 \pmod{4}$, w razie zaś a_1 nieparzystego $D \equiv 1 \pmod{4}$, gdy tymczasem w rozpatrywanym przypadku może być tylko $D \equiv 2 \pmod{4}$ lub $D \equiv 3 \pmod{4}$.

Liczby $a_0, 2D$ i c nie mają więc żadnego wspólnego dzielnika prócz jedności. Możemy zatem (ob. Rozdział II, § 6, str. 38) wyznaczyć takie liczby całkowite wymierne x, y i z , żeby było

$$x a_0 + y \cdot 2D + z c = 1.$$

Wobec $\omega = \sqrt{D}$ i $\omega' = -\sqrt{D}$ wynika stąd, że

$$\begin{aligned} i_0 i_2 &= (x a_0 + y \cdot 2D + z c) i_0 i_2 = \\ &= x i_0^2 + y \omega [i_0 (i_1 + i_2 \omega) - i_0 (i_1 + i_2 \omega')] + z (i_1 + i_2 \omega) (i_1 + i_2 \omega'), \end{aligned}$$

skąd widać bezpośrednio w myśl określenia ideałów i i i' , że liczba $i_0 i_2$ należy do ideału $i \cdot i' = N(i)$.

$$2^\circ D \equiv 1 \pmod{4}. \text{ Wówczas } \omega = \frac{1 + \sqrt{D}}{2} \text{ i}$$

$$N(i_1 + i_2 \omega) = i_1^2 + i_1 i_2 - \frac{D-1}{4} i_2^2 = \left(a_1^2 + a_1 - \frac{D-1}{4} \right) i_2^2,$$

$$c i_0 i_2 = c a_0 i_2^2,$$

skąd na mocy (6)

$$c = \frac{a_1^2 + a_1 - \frac{D-1}{4}}{a_0} = \frac{(2a_1 + 1)^2 - D}{4a_0}.$$

Gdyby liczby a_0, D i c miały wspólny dzielnik pierwszy $q > 1$, to wobec $(2a_1 + 1)^2 = 4a_0 c + D$ liczba $(2a_1 + 1)^2$ byłaby podzielna przez q , a więc i przez q^2 , jako kwadrat. Liczba $D = (2a_1 + 1)^2 - 4a_0 c$ byłaby zatem podzielna przez q^2 , wbrew założeniu, że nie ma ona żadnego dzielnika kwadratowego większego od 1.

Możemy więc wyznaczyć takie liczby całkowite wymierne x, y i z , żeby było

$$x a_0 + y D + z c = 1.$$

Wobec $\omega = \frac{1 + \sqrt{D}}{2}$ i $\omega' = \frac{1 - \sqrt{D}}{2}$ wynika stąd, że

$$\begin{aligned} i_0 i_2 &= (x a_0 + y D + z c) i_0 i_2 = \\ &= x i_0^2 + y (2\omega - 1) (i_0 (i_1 + i_2 \omega) - i_0 (i_1 + i_2 \omega')) + z (i_1 + i_2 \omega) (i_1 + i_2 \omega'), \end{aligned}$$

skąd znowu widać w myśl określenia ideałów i i i' , że liczba $i_0 i_2$ należy do ideału $i \cdot i' = N(i)$.

Tym samym dowód twierdzenia 5 jest zakończony.

§ 5. Dzielenie ideałów. Ideały względnie pierwsze. Mówimy, że ideał i jest *podzielny* przez ideał i_1 i piszemy $i_1|i$, gdy istnieje taki ideał i_2 , że

$$i = i_1 \cdot i_2.$$

Okażemy, że jeżeli $i_1|i$, to każda liczba ideału i jest zarazem liczbą ideału i_1 .

Istotnie, niech $i = i_1 \cdot i_2$ oraz $i_1 = [g_1, h_1]$ i $i_2 = [g_2, h_2]$. W myśl definicji iloczynu dwu ideałów każda liczba μ ideału i da się napisać w formie

$$\begin{aligned} \mu &= xg_1g_2 + yg_1h_2 + zh_1g_2 + th_1h_2 = \\ &= (xg_2 + yh_2)g_1 + (zg_2 + th_2)h_1 = \xi g_1 + \eta h_1, \end{aligned}$$

co dowodzi, że μ należy do ideału i_1 .

Okażemy też, że i na odwrót, jeżeli każda liczba ideału i jest zarazem liczbą ideału i_1 , to $i_1|i$. Wprzód jednak udowodnimy

Twierdzenie 6. *Jeżeli ideał i jest podzielny przez ideał i_1 , to istnieje jeden i tylko jeden taki ideał i_2 , że*

$$i = i_1 \cdot i_2.$$

Dowód. Niech

$$i_1 \cdot i_2 = i_1 \cdot i_3.$$

Mnożąc obie strony przez i_1' i pisząc w myśl twierdzenia 5 $N(i_1) = [a]$, gdzie a jest liczbą całkowitą wymierną, otrzymujemy

$$[a] \cdot i_2 = [a] \cdot i_3.$$

Niech

$$i_2 = [g_2, h_2], \quad i_3 = [g_3, h_3].$$

Ideał $[a] \cdot i_2$ jest zbiorem wszystkich liczb $xag_2 + yah_2$, ideał zaś $[a] \cdot i_3$ jest zbiorem wszystkich liczb $zag_3 + tah_3$, gdzie x, y, z i t są całkowite w ciele $K(\sqrt{D})$. Niech $\mu = xg_2 + yh_2$ będzie jakąkolwiek liczbą ideału i_2 . Ponieważ liczba $xag_2 + yah_2$ należy do ideału $[a] \cdot i_2 = [a] \cdot i_3$, więc istnieją takie liczby z i t całkowite w ciele $K(\sqrt{D})$, że

$$xag_2 + yah_2 = zag_3 + tah_3,$$

skąd

$$xg_2 + yh_2 = zg_3 + th_3,$$

co dowodzi, że μ należy do ideału i_3 .

Podobnie dowodzimy, że każda liczba ideału i_3 należy do ideału i_2 . Stąd $i_2 = i_3$, c. b. d. o.

W myśl twierdzenia 6, iloraz ideałów, o ile istnieje, jest określony jednoznacznie.

Założmy teraz, że każda liczba ideału i jest liczbą ideału i_1 . Niech μ będzie jakąkolwiek liczbą ideału $i \cdot i_1'$. Możemy więc napisać

$$\mu = xgg_1' + yh_1g_1' + zg_1h_1' + thh_1'.$$

Lecz g , jako liczba ideału i , jest liczbą ideału i_1 i podobnie h ; zatem

$$g = \xi g_1 + \eta h_1 \quad i \quad h = \zeta g_1 + \tau h_1,$$

skąd

$$\mu = (x\xi + y\zeta)g_1g_1' + (x\eta + y\tau)h_1g_1' + (z\xi + t\zeta)g_1h_1' + (z\eta + t\tau)g_1h_1',$$

co dowodzi, że μ należy do ideału $i_1 \cdot i_1' = N(i_1)$. Jeżeli $N(i_1) = [a]$, to mamy stąd dla każdej liczby μ ideału $i \cdot i_1'$

$$\mu = ua,$$

gdzie u jest pewną liczbą całkowitą ciała $K(\sqrt{D})$.

Weźmy pod uwagę zbiór W wszystkich takich liczb całkowitych m ciała $K(\sqrt{D})$, że ma jest liczbą ideału $i \cdot i_1'$. Zbiór W jest — jak łatwo widzieć — ideałem, gdyż jeżeli liczby m i m_1 należą do W , to ma i m_1a należą do $i \cdot i_1'$; zatem też liczba $ma + m_1a = (m + m_1)a$ należy do $i \cdot i_1'$, czyli liczba $m + m_1$ należy do zbioru W . Jeżeli zaś m należy do zbioru W , to ma i przeto xma należy do $i \cdot i_1'$, skąd wnosimy, że xm należy do W . Zbiór liczb ideału $i \cdot i_1'$ jest więc identyczny ze zbiorem wszystkich liczb postaci ua , gdzie u jest liczbą pewnego ideału i_0 .

Niech $i_0 = [g_0, h_0]$. Dla każdej liczby u ideału i_0 jest więc

$$u = \gamma g_0 + \delta h_0,$$

gdzie γ i δ są liczbami całkowitymi ciała $K(\sqrt{D})$. Zatem dla każdej liczby μ ideału $i \cdot i_1'$ jest $\mu = \gamma ag_0 + \delta ah_0$, skąd wniosek, że μ należy do ideału $[a] \cdot i_0$.

Na odwrót, dla każdej liczby v ideału $[a] \cdot i_0$ jest

$$v = \gamma^* ag_0 + \delta^* ah_0$$

czyli $v = (\gamma^* g_0 + \delta^* h_0)a$, gdzie γ^* i δ^* są liczbami całkowitymi ciała $K(\sqrt{D})$. Zatem liczba $\gamma^* g_0 + \delta^* h_0$ należy do ideału i_0 , a wobec tego v należy do $i \cdot i_1'$.

Tak więc $i \cdot i_1' = i_0 \cdot [a] = i_0 \cdot N(i_1) = i_0 \cdot i_1 \cdot i_1'$ czyli $i \cdot i_1' = (i_0 \cdot i_1) \cdot i_1'$, skąd wynika na mocy twierdzenia 6, że $i = i_0 \cdot i_1$, a zatem $i_1 | i$.

Udowodniliśmy tym sposobem następujące

Twierdzenie 7. *Na to, by ideał i był podzielny przez ideał i_1 , potrzeba i wystarcza, żeby każda liczba ideału i należała do ideału i_1 .*

Z twierdzenia 7 otrzymujemy natychmiast następujące wnioski:

Wniosek 1. *Na to, by ideał i był wspólnym dzielnikiem ideałów i_1 i i_2 , potrzeba i wystarcza, żeby ideał i zawierał wszystkie liczby każdego z ideałów i_1 i i_2 .*

Wniosek 2. *Na to, by ideał i był wspólną wielokrotną ideałów i_1 i i_2 , potrzeba i wystarcza, żeby każda liczba ideału i należała zarówno do i_1 jak do i_2 .*

Niech dalej:

$$i = [g, h], \quad i_1 = [g_1, h_1], \quad i_2 = [g_2, h_2].$$

Na to, by ideał i zawierał wszystkie liczby ideału i_1 — jak łatwo widzieć — potrzeba i wystarcza, żeby ideał i zawierał liczby g_1 i h_1 . Na to więc, by ideał i był wspólnym dzielnikiem ideałów i_1 i i_2 , potrzeba, żeby ideał i zawierał liczby g_1, h_1, g_2 i h_2 . Jak wiemy z § 2 (str. 447), najprostszym ideałem, zawierającym te cztery liczby, jest ideał

$$(15) \quad i_0 = [g_1, h_1, g_2, h_2],$$

a przy tym każdy inny ideał, zawierający te liczby, zawiera każdą liczbę ideału i_0 , czyli jest dzielnikiem ideału i_0 .

Zatem ideał i_0 jest takim wspólnym dzielnikiem ideałów i_1 i i_2 , który jest podzielny przez każdy inny wspólny dzielnik tych ideałów.

Usprawiedliwiona więc jest dla ideału (15) nazwa *największego wspólnego dzielnika* ideałów i_1 i i_2 .

Największy wspólny dzielnik ideałów i_1 i i_2 oznaczamy przez (i_1, i_2) .

Niech w szczególności $i_1 = [g_1]$ i $i_2 = [g_2]$ będą ideałami głównymi. Ich największy wspólny dzielnik $([g_1], [g_2])$ jest więc ideałem $i_0 = [g_1, g_2]$. Wynika stąd

Wniosek 3. *Każdy ideał jest największym wspólnym dzielnikiem dwu ideałów głównych:*

$$[g_1, g_2] = ([g_1], [g_2]).$$

Zachodzi ponadto następujące

Twierdzenie 8. *Największy wspólny dzielnik dwu ideałów i_1 i i_2 jest identyczny ze zbiorem wszystkich sum $\mu_1 + \mu_2$, gdzie μ_1 i μ_2 są dowolnymi liczbami, z których μ_1 należy do i_1 , a μ_2 — do i_2 .*

Dowód. Niech $i_1 = [g_1, h_1]$, $i_2 = [g_2, h_2]$ i $i_0 = (i_1, i_2)$. Z określenia ideału i_0 jako największego wspólnego dzielnika ideałów i_1 i i_2 jest na mocy (15) $i_0 = [g_1, h_1, g_2, h_2]$. Każda liczba ideału i_0 da się więc przedstawić w postaci

$$xg_1 + yh_1 + zg_2 + th_2 = (xg_1 + yh_1) + (zg_2 + th_2),$$

gdzie x, y, z i t są liczbami całkowitymi ciała $K(\sqrt{D})$. Widać stąd, że każda liczba ideału i_0 jest sumą liczb $\mu_1 + \mu_2$, gdzie μ_1 należy do ideału i_1 , μ_2 zaś — do ideału i_2 .

Ale i na odwrót, jeżeli μ_1 i μ_2 są liczbami, należącymi odpowiednio do ideałów i_1 i i_2 , to liczby te należą też do ideału i_0 ; stąd w myśl własności I ideału (p. str. 445) wnosimy, że $\mu_1 + \mu_2$ należy do i_0 .

Tym samym twierdzenie 8 zostało dowiedzione.

Dwa ideały, których największym wspólnym dzielnikiem jest ideał [1], nazywamy *względnie pierwszymi*.

Twierdzenie 9. *Jeżeli liczby całkowite wymierne a i b są względnie pierwsze w ciele liczb wymiernych, to ideały $[a]$ i $[b]$ są względnie pierwsze.*

Dowód. Niech $i = ([a], [b])$. Ideał i zawiera oczywiście każdą liczbę postaci $ax + by$, gdzie x i y są liczbami całkowitymi ciała $K(\sqrt{D})$. Lecz skoro liczby a i b są względnie pierwsze w ciele liczb wymiernych, to istnieją takie liczby całkowite wymierne x_0 i y_0 , że

$$ax_0 + by_0 = 1.$$

Wynika stąd, że liczba 1 należy do ideału i , który zawiera więc każdą liczbę całkowitą ciała $K(\sqrt{D})$, czyli $i = [1]$, c. b. d. o.

Weźmy jeszcze pod uwagę zbiór Z wszystkich liczb, które należą jednocześnie do dwu ideałów i_1 i i_2 . Łatwo widzieć, że zbiór Z jest ideałem. Ideał ten — oznaczmy go przez i_0 — jest oczywiście wspólną wielokrotnością ideałów i_1 i i_2 , i to taką, że każda liczba jakiegokolwiek innego ideału, będącego wspólną wielokrotnością ideałów i_1 i i_2 , należy do i_0 (gdyż należy jednocześnie do i_1 i i_2). Innymi słowy, i_0 jest dzielnikiem każdej wspólnej wielokrotności ideałów i_1 i i_2 .

Usprawiedliwiona więc jest dla ideału i_0 nazwa *najmniejszej wspólnej wielokrotności* ideałów i_1 i i_2 .

§ 6. Ideały pierwsze. Ideał p , różny od ideału $[1]$ i podzielny tylko przez ideały $[1]$ i p , nazywamy *ideałem pierwszym*.

Łatwo widzieć, że jeżeli p jest ideałem pierwszym, to p' również jest ideałem pierwszym.

Istotnie, gdyby p' miał dzielnik i , różny od $[1]$ i od p' , to byłoby $p' = i \cdot i'$, skąd $p = i' \cdot i'$, co dowodzi, że i' jest dzielnikiem ideału p . Lecz gdyby było $i' = [1]$, mielibyśmy $i = (i') = [1]$ wbrew założeniu, gdyby zaś było $i' = [p]$, mielibyśmy $i = (i')' = p'$, znów wbrew założeniu. Dzielnik i' ideału p byłby więc różny od $[1]$ i od p , wbrew założeniu, że p jest ideałem pierwszym.

Dowiedliśmy więc, że *ideał, sprzężony z ideałem pierwszym, sam jest ideałem pierwszym*.

Twierdzenie 10. *Jeżeli iloczyn $i_1 \cdot i_2$ dwoi ideałów jest podzielny przez ideał pierwszy p , to przynajmniej jeden z czynników jest podzielny przez p .*

Dowód. Załóżmy, że ideał i_1 nie jest podzielny przez p . Ideał p , jako ideał pierwszy, ma tylko dwa dzielniki: $[1]$ i p , a że i_1 nie jest podzielny przez p , więc największym wspólnym dzielnikiem ideałów i_1 i p jest ideał $i_0 = (i_1, p) = [1]$ czyli zbiór wszystkich liczb całkowitych ciała $K(\sqrt{D})$. Lecz na mocy twierdzenia 8 każda liczba, należąca do największego wspólnego dzielnika, w szczególności więc liczba 1 daje się w rozważanym przypadku przedstawić w postaci

$$1 = \mu_1 + \mu_2$$

gdzie μ_1 jest pewną liczbą ideału i_1 , μ_2 zaś — pewną liczbą ideału p .

Niech μ_2 będzie jakąkolwiek liczbą ideału i_2 . Na mocy twierdzenia 3 iloczyn $i_1 \cdot i_2$ zawiera wszystkie liczby postaci $\mu_1 \mu_2$. Na mocy założenia podzielności iloczynu $i_1 \cdot i_2$ przez p każda liczba tego iloczynu należy w myśl twierdzenia 7 do ideału p . Zatem $\mu_1 \mu_2$ należy do p , a że oczywiście μ_2 też należy do p (gdyż μ należy do p), więc liczba

$$\mu_1 \mu_2 + \mu \mu_2 = (\mu_1 + \mu) \mu_2 = \mu_2$$

również należy do p . Każda więc liczba ideału i_2 należy do ideału p , a zatem w myśl twierdzenia 7 jest $p \mid i_2$, c. b. d. o.

§ 7. Rozkład ideału na czynniki pierwsze. Oznaczać będziemy symbolem $\mathfrak{N}(i)$ najmniejszą liczbę naturalną, zawartą w ideale $N(i)$. Wobec $N(i) = [i_0 i_2]$ (ob. twierdzenie 5) łatwo widzieć, że $\mathfrak{N}(i) = i_0 i_2$. Łatwo też udowodnić

Twierdzenie 11. $\mathfrak{N}(i_1 \cdot i_2) = \mathfrak{N}(i_1) \cdot \mathfrak{N}(i_2)$.

Dowód. Niech

$$\mathfrak{N}(i_1) = n_1, \quad \mathfrak{N}(i_2) = n_2, \quad \mathfrak{N}(i_1 \cdot i_2) = n.$$

Oczywiście

$$N(i_1) = [n_1], \quad N(i_2) = [n_2], \quad N(i_1 \cdot i_2) = [n],$$

a ponieważ jak łatwo widzieć,

$$N(i_1 \cdot i_2) = N(i_1) \cdot N(i_2),$$

więc

$$[n] = [n_1] \cdot [n_2],$$

skąd w jednej chwili

$$[n] = [n_1 n_2].$$

Dowodzi to, że liczby n i $n_1 n_2$ są stowarzyszone, a że są to liczby naturalne, więc muszą być równe. Jest więc $n = n_1 n_2$ czyli $\mathfrak{N}(i_1 \cdot i_2) = \mathfrak{N}(i_1) \mathfrak{N}(i_2)$, c. b. d. o.

Niech teraz $\mathfrak{N}(i) = 1$. Wobec $\mathfrak{N}(i) = i_0 i_2$ (twierdzenie 5) jest więc $i_0 i_2 = 1$, skąd $i_0 = 1$, gdyż i_0 i i_2 są liczbami naturalnymi. Ponieważ zaś i_0 jest liczbą ideału i , więc ideał ten zawiera liczbę 1, skąd $i = [1]$. Mamy zatem

Twierdzenie 12. *Jeżeli $\mathfrak{N}(i) = 1$, to $i = [1]$.*

Z definicji symbolu $\mathfrak{N}(i)$ wynika też natychmiast, że jeżeli a jest liczbą całkowitą wymierną, to $\mathfrak{N}([a]) = a^2$. Wystarczy w tym celu zauważyć, że wtedy $N([a]) = [a] \cdot [a]' = [a]^2 = [a^2]$.

Weźmy z kolei pod uwagę ideał i , mający dzielnik i_1 różny od i i od $[1]$. Możemy więc napisać $i = i_1 \cdot i_2$, skąd w myśl twierdzenia 11

$$(16) \quad \mathfrak{N}(i) = \mathfrak{N}(i_1) \cdot \mathfrak{N}(i_2).$$

Gdyby było $\mathfrak{N}(i_2) = 1$, mielibyśmy $i_2 = [1]$, zatem $i = i_1 \cdot [1]$, skąd w jednej chwili $i = i_1$, wbrew założeniu.

Jest więc $\mathfrak{N}(i_2) > 1$, a zatem $\mathfrak{N}(i_1) < \mathfrak{N}(i)$ wobec (16). Z drugiej strony, na mocy twierdzenia 12 jest $\mathfrak{N}(i_1) > 1$, gdyż $i_1 \neq [1]$, więc

$$1 < \mathfrak{N}(i_1) < \mathfrak{N}(i).$$

Niech Z będzie zbiorem wszystkich liczb naturalnych $\mathfrak{N}(i)$, odpowiadających wszystkim dzielnikom i danego ideału $i_0 \neq [1]$. W zbiorze Z istnieją liczby większe od 1, gdyż, wobec $i_0 \neq [1]$ taką jest np. liczba $\mathfrak{N}(i_0)$, należąca do Z . Oznaczmy przez n najmniejszą z tych liczb zbioru Z , które są większe od 1.

W myśl określenia liczby n istnieje więc taki dzielnik i_1 ideału i_0 , dla którego $\mathfrak{N}(i_1) = n$.

Okażemy, że ideał i_1 jest ideałem pierwszym. Istotnie — jak dowiedliśmy przed chwilą — gdyby ideał i_1 posiadał dzielnik i_2 , różny od $[1]$ i od i_1 , byłoby $1 < \mathfrak{N}(i_2) < \mathfrak{N}(i_1)$, a zarazem i_2 byłby, jako dzielnik ideału i_1 , również dzielnikiem ideału i_0 . Liczba $\mathfrak{N}(i_2)$, mniejsza od liczby $\mathfrak{N}(i_1) = n$, a jednocześnie większa od 1, byłaby więc liczbą zbioru Z wbrew określeniu liczby n .

Udowodniliśmy więc

Twierdzenie 13. *Każdy ideał różny od $[1]$ ma przynajmniej jeden dzielnik, który jest ideałem pierwszym.*

Jeżeli więc $i \neq [1]$, to ideał i albo sam jest pierwszy, albo posiada dzielnik pierwszy $p_1 \neq i$ i wtedy

$$i = p_1 \cdot i_1,$$

przy czym $1 < \mathfrak{N}(p_1) < \mathfrak{N}(i)$, a więc też

$$1 < \mathfrak{N}(i_1) < \mathfrak{N}(i).$$

Jeżeli ideał i_1 nie jest pierwszy, to znowu

$$i_1 = p_2 \cdot i_2,$$

gdzie też

$$1 < \mathfrak{N}(i_2) < \mathfrak{N}(i_1).$$

Ponieważ ciąg liczb naturalnych malejących

$$\mathfrak{N}(i) > \mathfrak{N}(i_1) > \mathfrak{N}(i_2) > \dots$$

nie może być nieskończony, więc musimy dojść w końcu do ideału pierwszego $i_k = p_k$. Zatem

$$i = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

i tym samym udowodniliśmy

Twierdzenie 14. *Każdy ideał $i \neq [1]$ jest iloczynem skończenie wielu ideałów pierwszych.*

Na mocy twierdzenia 10 wynika stąd — podobnie jak w teorii liczb całkowitych wymiernych — następujący łatwy

Wniosek. *Każdy ideał $i \neq [1]$ rozkłada się, i to w jeden tylko sposób, na czynniki pierwsze.*

Jest to tak zwane *zasadnicze twierdzenie teorii ideałów*.

§ 8. Ideały pierwsze 1-go i 2-go stopnia. Rozkład na czynniki pierwsze ideałów głównych, utworzonych przez liczby pierwsze.

Twierdzenie 15. *Jeżeli p jest ideałem pierwszym, to $\mathfrak{N}(p)$ jest albo liczbą pierwszą wymierną, albo kwadratem takiej liczby.*

Dowód. Liczbę naturalną większą od 1, nie będącą ani liczbą pierwszą, ani kwadratem liczby pierwszej, można — jak łatwo widzieć — rozłożyć na dwa czynniki naturalne, różne między sobą i różne od 1. Gdyby więc liczba $\mathfrak{N}(p)$, która jest liczbą naturalną większą od 1, nie była ani liczbą pierwszą, ani kwadratem liczby pierwszej, to mielibyśmy rozkład

$$\mathfrak{N}(p) = a \cdot b,$$

gdzie a i b są liczbami naturalnymi, $a > 1$, $b > 1$ i

$$(17) \quad a \neq b.$$

Wynika stąd, wobec $N(p) = p \cdot p' \mid N(p) = [\mathfrak{N}(p)]$, że

$$p \cdot p' = [a \cdot b] = [a] \cdot [b].$$

Ponieważ w tej równości czynniki lewej strony są ideałami pierwszymi, czynniki zaś prawej strony są różne od $[1]$, więc w myśl wniosku o jednoznaczności rozkładu ideałów na czynniki pierwsze wnosimy stąd natychmiast, że oba iloczyny różnią się co najwyżej porządkiem czynników. Jest więc np.

$$p = [a], \quad p' = [b],$$

skąd

$$[b] = [a]' = [a] = [a].$$

co dowodzi, że liczby a i b są stowarzyszone, zatem równe jako liczby naturalne. Sprzeciwia się to jednak nierówności (17). Twierdzenie 15 jest tym samym dowiedzione.

Jeżeli $\mathfrak{N}(p)$ jest liczbą pierwszą, to ideał pierwszy p nazywamy ideałem *pierwszego stopnia*, jeżeli zaś liczba $\mathfrak{N}(p)$ jest kwadratem liczby pierwszej, to ideał pierwszy p nazywamy ideałem *drugiego stopnia*.

Wniosek. *Każdy ideał pierwszy jest dzielnikiem pełnego ideału $[p]$, gdzie p jest liczbą pierwszą wymierną.*

Istotnie, $pp' = [\mathfrak{N}(p)]$, zatem w myśl twierdzenia 15 musi być $p \cdot p' = [p]$ lub $p \cdot p' = [p] \cdot [p]$, gdzie p jest liczbą pierwszą wymierną.

W każdym więc razie ideał $[p]$ jest podzielny przez p na mocy twierdzenia 10.

Zbadamy obecnie, jak rozkładają się na ideały pierwsze ideały $[p]$, gdzie p jest liczbą pierwszą wymierną.

Okazemy najpierw, że $[p]$ nie może być iloczynem trzech ideałów, z których każdy jest różny od $[1]$.

Istotnie, przypuśćmy, że $[p] = i_1 \cdot i_2 \cdot i_3$, gdzie żaden z ideałów i_1, i_2, i_3 nie jest ideałem $[1]$. Zatem $\mathfrak{N}(i_1) > 1$, $\mathfrak{N}(i_2) > 1$ i $\mathfrak{N}(i_3) > 1$, skąd wobec $\mathfrak{N}([p]) = p^2$ wynika rozkład

$$p^2 = \mathfrak{N}(i_1) \cdot \mathfrak{N}(i_2) \cdot \mathfrak{N}(i_3),$$

co niemożliwe.

Tak więc ideał główny $[p]$, gdzie p jest liczbą pierwszą wymierną, jest albo ideałem pierwszym, albo iloczynem dwu ideałów pierwszych.

Okazemy obecnie, że jeżeli ideał główny $[p]$, gdzie p jest liczbą pierwszą wymierną, jest iloczynem dwu ideałów pierwszych, to ideały te są sprzężone.

Istotnie, jeżeli $[p] = p_1 p_2$, gdzie p_1 i p_2 są ideałami pierwszymi, to $\mathfrak{N}([p]) = \mathfrak{N}(p_1) \cdot \mathfrak{N}(p_2)$, czyli wobec $\mathfrak{N}([p]) = p^2$

$$p^2 = \mathfrak{N}(p_1) \cdot \mathfrak{N}(p_2).$$

Ponieważ zaś każda z liczb $\mathfrak{N}(p_1)$ i $\mathfrak{N}(p_2)$ jest większa od 1, więc $\mathfrak{N}(p_1) = p$ i $\mathfrak{N}(p_2) = p$, skąd

$$[\mathfrak{N}(p_1)] = [p].$$

Ponieważ wreszcie $N(p_1) = [\mathfrak{N}(p_1)]$ i zarazem $N(p_1) = p_1 \cdot p_1'$, więc ostatecznie

$$[p] = p_1 \cdot p_1'.$$

Możemy zatem wypowiedzieć następujące

Twierdzenie 16. *Jeżeli p jest liczbą pierwszą wymierną, to ideał $[p]$ jest albo ideałem pierwszym, albo kwadratem ideału pierwszego, albo wreszcie iloczynem dwu różnych ideałów pierwszych sprzężonych.*

Z wniosku z twierdzenia 15 wynika, że dla wyznaczenia wszystkich ideałów pierwszych danego ciała liczbowego $K(\sqrt{D})$ wystarczy wyznaczyć czynniki pierwsze ideałów $[p]$, gdzie p jest liczbą pierwszą wymierną.

ROZDZIAŁ XIX

WIELKIE TWIERDZENIE FERMATA DLA WYKŁADNIKÓW 5 i 7

§ 1. Ciała liczbowe, w których każdy ideał jest główny.

Udowodnimy najpierw ogólnie następujący

Lemat I. *Jeżeli w ciele liczbowym $K(\sqrt{D})$ warunki*

$$(1) \quad |u| \leq 1/2, \quad |v| \leq 1/2$$

pociągają za sobą zawsze warunek

$$(2) \quad |N(u + v\omega)| < 1,$$

to każdy ideał ciała $K(\sqrt{D})$ jest ideałem głównym.

Dowód. Niech i będzie ideałem w ciele $K(\sqrt{D})$. Dla każdej liczby $\lambda \neq 0$ ideału i utworzmy liczbę $|N(\lambda)|$. Jest to liczba naturalna. Niech n będzie najmniejszą z tych wszystkich liczb. Istnieje więc taka liczba λ_0 należąca do i , że $|N(\lambda_0)| = n$.

Okazemy, że

$$i = [\lambda_0].$$

Istotnie, niech

$$\lambda_0 = u_0 + v_0 \omega,$$

gdzie u_0 i v_0 są liczbami całkowitymi wymiernymi i niech $\lambda = u + v\omega$ będzie jakkolwiek liczbą ideału i . Ponieważ $n = |N(\lambda_0)| > 0$, więc $\lambda_0 \neq 0$. Iloraz λ/λ_0 , jako liczba ciała $K(\sqrt{D})$, może być przedstawiony w formie

$$(3) \quad \lambda/\lambda_0 = x + y\omega,$$

gdzie x i y są liczbami rzeczywistymi wymiernymi. Możemy dalej wyznaczyć takie liczby całkowite wymierne a i b , że

$$(4) \quad |x - a| \leq 1/2 \quad \text{ i } \quad |y - b| \leq 1/2.$$

Niech

$$x - a = \xi \quad \text{ i } \quad y - b = \eta.$$