Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 36 (1990)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE DISTANCE BETWEEN IDEALS IN THE ORDERS OF A REAL QUADRATIC FIELD

Autor: Kaplan, Pierre / Williams, Kenneth S.

Kapitel: 2. Basic definitions

DOI: https://doi.org/10.5169/seals-57912

Throughout this paper, if A is a unitary commutative ring, and $\alpha_1, \alpha_2, \ldots, \alpha_m$ are elements of A, the Z-module generated by $\alpha_1, \alpha_2, \ldots, \alpha_m$ is denoted by $[\alpha_1, \alpha_2, \ldots, \alpha_m]$ and the A-module (ideal) generated by $\alpha_1, \alpha_2, \ldots, \alpha_m$ by $(\alpha_1, \alpha_2, \ldots, \alpha_m)$. The product of the ideals $(\alpha_1, \ldots, \alpha_m)$ and $(\alpha'_1, \ldots, \alpha'_n)$ is the ideal $(\alpha_1\alpha'_1, \ldots, \alpha_i\alpha'_j, \ldots, \alpha_m\alpha'_r)$. If I is an ideal, we often write the product ideal $(\alpha)I$ as αI.

2. Basic definitions

Let K be a quadratic field of discriminant D_0. As D_0 is a discriminant we have $D_0 \equiv 0 \pmod 4$ or $D_0 \equiv 1 \pmod 4$. In §2 and §3 K may be real ($D_0 > 0$) or imaginary ($D_0 < 0$) but in the remaining sections K will be assumed to be real. An element α of K can be written $\alpha = x + y\sqrt{D_0}$, where x and y are rational numbers. The conjugate of α is the element $\bar{\alpha} = x - y\sqrt{D_0}$ of K. The norm of α is the rational number $N(\alpha) = \alpha\bar{\alpha} = x^2 - D_0 y^2$. We define the integer ω_0 of K by

$$\omega_0 = \begin{cases} \dfrac{\sqrt{D_0}}{2}, & \text{if } D_0 \equiv 0 \pmod 4, \\ \dfrac{1}{2}(1 + \sqrt{D_0}), & \text{if } D_0 \equiv 1 \pmod 4. \end{cases} \tag{2.1}$$

The ring of integers of K is $O_{D_0} = [1, \omega_0]$. For a positive integer f, we set

$$D = D_0 f^2, \omega = \begin{cases} \dfrac{\sqrt{D}}{2}, & \text{if } D \equiv 0 \pmod 4 \\ \dfrac{1}{2}(1 + \sqrt{D}), & \text{if } D \equiv 1 \pmod 4. \end{cases} \tag{2.2}$$

and

$$O_D = [1, \omega] = [1, f\omega_0]. \tag{2.3}$$

It is easy to check that O_D is the subring of index f in O_{D_0}, called the order of discriminant D. We note that

$$\omega^2 = \begin{cases} \dfrac{D}{4}, & \text{if } D \equiv 0 \pmod 4, \\ \omega + \dfrac{(D-1)}{4}, & \text{if } D \equiv 1 \pmod 4. \end{cases} \tag{2.4}$$

The multiplicative group of K is denoted by K^*.

Next we describe the ideals of the order O_D. Throughout this paper all ideals will be nonzero.

PROPOSITION 1. ([10]: Theorem 5.6, [12]: Theorem 3.2) *(i) The (nonzero) ideals of the order* O_D *are the Z-modules*

$$I = d\left[a, \frac{b+\sqrt{D}}{2}\right],$$

where

$$c = \frac{D-b^2}{4a} \tag{2.5}$$

is an integer.

(ii) Two ideals $I = d\left[a, \frac{b+\sqrt{D}}{2}\right]$ *and* $I' = d'\left[a', \frac{b'+\sqrt{D}}{2}\right]$ *are equal if, and only if,* $|d| = |d'|, |a| = |a'|, b \equiv b' \pmod{2a}$.

Proof. (i) Let I be a (nonzero) ideal of O_D. The set $I \cap Z$ is a (nonzero) ideal (a_0) of Z. The set $\{y \in Z: x + y\omega \in I$ for some $x \in Z\}$ is also an ideal (d) of Z, and, as $a_0\omega \in I$, we see that $d | a_0$, say $a_0 = da$. Let $\alpha_0 \in I$ be such that $\alpha_0 = b_0 + d\omega$. Appealing to (2.4), we see that

$$\omega\alpha_0 = \omega(b_0 + d\omega) = \begin{cases} \dfrac{dD}{4} + b_0\omega\,, & \text{if } D \equiv 0 \pmod 4\,, \\ d\left(\dfrac{D-1}{4}\right) + (d+b_0)\omega\,, & \text{if } D \equiv 1 \pmod 4\,, \end{cases}$$

so that $d | b_0$, say $b_0 = db_1$. Thus we have $\alpha_0 = d(b_1 + \omega)$, which shows that $I \supseteq d[a, b_1 + \omega]$. Now let $\beta = x + dy\omega \in I$. As $\beta - \alpha_0 y = x - b_0 y \in I \cap Z$, there exists $k \in Z$ such that $\beta = ka_0 + \alpha_0 y$, which shows that $I \subseteq [a_0, \alpha_0] = d[a, b_1 + \omega]$. Hence we have $I = d[a, b_1 + \omega]$. As $dN(b_1 + \omega) = d(b_1 + \omega)(b_1 + \bar{\omega}) \in I \cap Z = (da)$, we see that a divides $N(b_1 + \omega)$.

Now let $I = d[a, b_1 + \omega]$, where $c = -N(b_1 + \omega)|a$ is an integer. We show that I is an ideal of O_D. It suffices to prove that ωa and $\omega(b_1 + \omega)$ belong to $[a, b_1 + \omega]$. This follows from

$$\omega a = (-b_1)a + a(b_1 + \omega)$$

and

$$\omega(b_1 + \omega) = -(b_1 + \bar{\omega})(b_1 + \omega) + (b_1 + \omega + \bar{\omega})(b_1 + \omega)$$
$$= ca + (b_1 + \omega + \bar{\omega})(b_1 + \omega) .$$

We have thus shown that the ideals of O_D are the Z-modules $d[a, b_1 + \omega]$, where $c = -N(b_1 + \omega) | a$ is an integer. Let b be the integer given by

$$b = \begin{cases} 2b_1 , & \text{if } \; D \equiv 0 \pmod 3 , \\ 2b_1 + 1 , & \text{if } \; D \equiv 1 \pmod 4 , \end{cases}$$

so that

$$b_1 + \omega = \frac{b + \sqrt{D}}{2} , \quad \frac{N(b_1 + \omega)}{a} = \frac{b^2 - D}{4a} = -c \in Z .$$

This completes the proof of Proposition 1 (i).

(ii) If $d\left[a, \dfrac{b + \sqrt{D}}{2}\right] = d'\left[a', \dfrac{b' + \sqrt{D}}{2}\right]$ we easily see that $d | d', d' | d$, $ad | a'd'$ and $a'd' | ad$, from which Proposition 1 (ii) follows.

Example 1. (i) By Proposition 1 (i) the Z-module $A = \left[3, \dfrac{1 + \sqrt{45}}{2}\right]$ of O_{45} is not an ideal of O_{45} as $\dfrac{45 - 1}{12}$ is not an integer. Indeed A is not closed under multiplication by elements of O_{45} as $\dfrac{1 + \sqrt{45}}{2} \in A$ but

$$\left(\frac{1 - \sqrt{45}}{2}\right)\left(\frac{1 + \sqrt{45}}{2}\right) = -11 \notin A .$$

(ii) By Proposition 1 (i) the Z-module $B = \left[11, \dfrac{1 + \sqrt{45}}{2}\right]$ of O_{45} is an ideal of O_{45} as $\dfrac{45 - 1}{44}$ is an integer.

If $I = d\left[a, \dfrac{b + \sqrt{D}}{2}\right]$ is an ideal of O_D, by Proposition 1 (ii), we see that $GCD(a, b, c)$ does not depend upon the choice of a, b and d. This enables us to define the concept of a primitive ideal of O_D.

Definition 1. (Primitive ideal) The ideal $I = d\left[a, \frac{b+\sqrt{D}}{2}\right]$ of O_D is called *primitive* if, and only if,

$$d = GCD(a, b, c) = 1 ,$$

where c is defined by (2.5).

Our next result gives some basic properties of primitive ideals.

PROPOSITION 2. ([10]: Theorem 5.9) *(i) If* $I = \left[a, \frac{b+\sqrt{D}}{2}\right]$ *is a primitive ideal of* O_D *then*

$$I\bar{I} = (a) ,$$

where $\bar{I} = \left[a, \frac{b-\sqrt{D}}{2}\right]$ *is the conjugate ideal of* I.

(ii) If I *is a primitive ideal of* O_D *and* $\alpha \in K^*$ *is such that* $I = \alpha I$, *then* α *is a unit of* O_D.

(iii) If $I = \left[a, \frac{b+\sqrt{D}}{2}\right]$ *and* $J = \left[A, \frac{B+\sqrt{D}}{2}\right]$ *are primitive ideals of* O_D *such that* $\frac{1}{a} I = \frac{1}{A} J$ *then* $I = J$ *and* $|a| = |A|$.

Proof. (i) We have

$$I\bar{I} = a\left(a, \frac{b+\sqrt{D}}{2}, \frac{b-\sqrt{D}}{2}, c\right) .$$

The ideal $\left(a, \frac{b+\sqrt{D}}{2}, \frac{b+\sqrt{D}}{2}, c\right)$ contains the ideal $(a, b, c) = (1)$, so that $I\bar{I} = (a)$.

(ii) As $\alpha \in K^*$, there exist $\beta \in O_D^*$ and $\gamma \in O_D^*$ such that $\alpha = \beta/\gamma$. Then, we have $\gamma I = \gamma\alpha I = \beta I$, and so, by (i), we obtain $(\gamma)(a) = \gamma I\bar{I} = \beta I\bar{I} = (\beta)(a)$, giving $(\beta) = (\gamma)$, so that $\alpha = \beta/\gamma$ is a unit of O_D.

(iii) We have $AI = aJ$ so that, by (ii), $a/A = \pm 1$ and $I = J$.

Next we define the notion of equivalent ideals.

Definition 2. (Equivalent ideals) Two ideals I and I' of O_D are said to be *equivalent* if there exists $\rho \in K^*$ such that $I' = \rho I$.

Example 2. The ideals

$$I = \left[7, \frac{12+\sqrt{200}}{2}\right] = [7, 6+\sqrt{50}] \quad \text{and} \quad J = \left[2, \frac{\sqrt{200}}{2}\right] = [2, \sqrt{50}]$$

of O_{200} are equivalent as

$$\begin{aligned} I &= [7, -8+\sqrt{50}] \\ &= \left(\frac{-8+\sqrt{50}}{2}\right) [-8-\sqrt{50}, 2] \\ &= \left(\frac{-16+\sqrt{200}}{4}\right) [2, \sqrt{50}] \\ &= \alpha J\,, \end{aligned}$$

where
$$\alpha = \frac{-16+\sqrt{200}}{4} \in K^*\,.$$

It is clear that the notion of equivalence given in Definition 2 is an equivalence relation. The equivalence classes are called ideal classes. The ideal class of the ideal I is denoted by $C(I)$. If $I' \in C(I)$ and $J' \in C(J)$ then $I'J' \in C(IJ)$, and we can define multiplication of ideal classes by $C(I)\,C(J) = C(IJ)$.

Definition 3. (Primitive class) An ideal class of O_D containing a primitive ideal is called a *primitive* class.

It follows from Proposition 2 (i) that the primitive classes are invertible, and so form a group C_D with respect to multiplication.

Definition 4. (Ideal class group) The group C_D of primitive classes of the order O_D is called the *ideal class group* of O_D.

The unit class of the ideal class group is called the principal class and consists of all the principal primitive ideals of O_D. In fact C_D is a finite group.

Next we give a necessary and sufficient condition for two ideals I and I' of O_D to be equivalent, and, when I and I' are equivalent, a means of calculating ρ in the relationship $I' = \rho I$. It suffices to consider ideals of the form $\left[a, \frac{b+\sqrt{D}}{2}\right]$ that is with $d = 1$.

PROPOSITION 3. ([10]: Theorem 5.27) *Let*

$$I = \left[a, \frac{b+\sqrt{D}}{2}\right] \quad \textit{and} \quad J = \left[A, \frac{B+\sqrt{D}}{2}\right]$$

be two ideals of O_D. *Set*

$$\phi = \frac{b+\sqrt{D}}{2a}, \quad \psi = \frac{B+\sqrt{D}}{2A}.$$

(i) The ideals I *and* J *are equivalent if, and only if, there exists a* 2×2 *integral matrix* $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ *of determinant* $\varepsilon = ps - qr = \pm 1$ *such that* $\psi = \dfrac{p\phi + q}{r\phi + s}$.

(ii) If I *and* J *are equivalent the numbers* $\rho \in K^*$ *such that* $J = \rho I$ *are given by*

$$\rho = \frac{A}{a}\,\frac{1}{r\phi + s} = \varepsilon(r\bar{\phi} + s) \tag{2.6}$$

and satisfy

$$N(\rho) = \varepsilon\,\frac{A}{a}. \tag{2.7}$$

Proof. We have $J = \rho I$, that is $A[1, \psi] = \rho a[1, \phi]$, if, and only if, there exists an integral matrix $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ of determinant $\varepsilon = \pm 1$ such that

$$\begin{cases} A = r\rho a\varphi + s\rho a, \\ A\psi = p\rho a\phi + q\rho a. \end{cases} \tag{2.8}$$

The equations (2.8) are equivalent to

$$\psi = \frac{p\phi + q}{r\phi + s}, \quad \rho = \frac{A}{a}\,\frac{1}{r\phi + s}.$$

This establishes (i) and the first equality of (2.6).

Taking conjugates in (2.8), we have

$$\begin{cases} A = r\bar{\rho} a\bar{\phi} + s\bar{\rho} a, \\ A\bar{\psi} = p\bar{\rho} a\bar{\phi} + q\bar{\rho} a, \end{cases} \tag{2.9}$$

so that (2.8) and (2.9) are equivalent to the matrix equality

$$\begin{bmatrix} A\psi & A \\ A\bar{\psi} & A \end{bmatrix} = \begin{bmatrix} a\phi\rho & a\rho \\ a\bar{\phi}\bar{\rho} & a\bar{\rho} \end{bmatrix} \begin{bmatrix} p & r \\ q & s \end{bmatrix}.$$

Taking determinants we obtain

$$A^2(\psi - \bar{\psi}) = \varepsilon\rho\bar{\rho}a^2(\phi - \bar{\phi}),$$

which gives, as $\psi - \bar{\psi} = \dfrac{\sqrt{D}}{A}$ and $\phi - \bar{\phi} = \dfrac{\sqrt{D}}{a}$, $\rho\bar{\rho} = \varepsilon\dfrac{A}{a}$, proving (2.7). Then the first equality in (2.6) shows that $\bar{\rho} = \varepsilon(r\phi + s)$, establishing the second equality in (2.6).

COROLLARY 1. *Let* $I = \left[a, \dfrac{b+\sqrt{D}}{2}\right]$ *be a primitive ideal of* O_D, *and set* $\phi = \dfrac{b+\sqrt{D}}{2a}$. *For* $q \in Z$ *define* $\phi', b' a'$ *and* I' *by*

(2.10)
$$\phi = q + \frac{1}{\phi'}, \quad b' = -b + 2aq, \quad a' = \frac{D - b'^2}{4a}, \quad I' = \left[a', \frac{b' + \sqrt{D}}{2}\right].$$

Then

$$(2.11) \qquad a' = \frac{D - b^2}{4a} + bq - aq^2 \in Z, \quad \phi' = \frac{b' + \sqrt{D}}{2a'},$$

and I' *is a primitive ideal of* O_D *such that*

$$(2.12) \qquad I' = \frac{a'}{a}\phi' I = \frac{-1}{\bar{\phi}'} I.$$

Proof. The formulas in (2.11) for a' and ϕ' are easily proved by a straightforward calculation, and Proposition 3 with $p = 0$, $q = 1$, $r = 1$, $s = -q$ gives

$$I' = \frac{a'}{a}\frac{1}{\phi - q} I = -(\bar{\phi} - q)I,$$

which is equivalent to (2.12) as $\phi' = \dfrac{1}{\phi - q}$.

By Proposition 1 a primitive ideal I of O_D can be written in the form $I = a[1, \phi]$ $(\phi = (b+\sqrt{D})/2a)$, where a is an integer uniquely determined up to sign by I and $a\phi$ is determined modulo a by I.

Definition 5. (Representation of a primitive ideal). Let I be a primitive ideal of O_D. A pair $\{a, b\}$ such that $I = a[1, \phi]$, where $\phi = (b+\sqrt{D})/2a$, is called a *representation* of I.

Definition 6. (q-neighbour). When the representation $\{a, b\}$ of the ideal I and the representation $\{a', b'\}$ of the ideal I' are related as in (2.10), we say that $\{a', b'\}$ is *q-neighbour* to $\{a, b\}$.

Definition 7. (Lagrange neighbour). When $D > 0$ and $\{a', b'\}$ is q-neighbour to $\{a, b\}$ with $q = [\phi]$, we say that $\{a', b'\}$ is the *Lagrange neighbour* of $\{a, b\}$ and write $\{a, b\} \xrightarrow{L} \{a', b'\}$.

Definition 8. (Gauss neighbour). When $D > 0$ and $\{a', b'\}$ is q-neighbour to $\{a, b\}$ with $q = \dfrac{a}{|a|}\left[\dfrac{a}{|a|}\phi\right]$, we say that $\{a', b'\}$ is the *Gauss neighbour* of $\{a, b\}$ and write $\{a, b\} \xrightarrow{G} \{a', b'\}$.

Lagrange's reduction process using Lagrange neighbours is described in § 5 and Gauss's reduction process using Gauss neighbours in § 8.

COROLLARY 2. *The ideals* $I = \left[a, \dfrac{b+\sqrt{D}}{2}\right]$ *and* $J = \left[c, \dfrac{-b+\sqrt{D}}{2}\right]$, *where* c *is given by (2.5), are equivalent and satisfy*

$$J = \frac{(-b+\sqrt{D})}{2a} I .$$

Proof. We have $\psi = \dfrac{1}{\phi}$, where $\phi = \dfrac{b + \sqrt{D}}{2a}$ and $\psi = \dfrac{-b + \sqrt{D}}{2c}$, so that, by Proposition 3(ii), we have $J = \rho I$ with $\rho = (-1)\bar{\phi} = \dfrac{-b + \sqrt{D}}{2a}$.

COROLLARY 3. *If* $I = \left[a, \dfrac{b + \sqrt{D}}{2}\right]$ *and* $J = \left[A, \dfrac{B + \sqrt{D}}{2}\right]$ *are two equivalent ideals of* O_D *with* I *primitive then* J *is also primitive.*

Proof. Set $\phi = \dfrac{b + \sqrt{D}}{2a}$ and $\psi = \dfrac{B + \sqrt{D}}{2A}$. As I and J are equivalent, by Proposition 3, we have $J = \rho I$, where $\psi = \dfrac{p\phi + q}{r\phi + s}$, $\rho = \dfrac{A}{a}\dfrac{1}{r\bar{\phi} + s} = \varepsilon(r\phi + s)$ and $\varepsilon = ps - qr = \pm 1$. Clearly we have

$$\begin{aligned}
A &= \varepsilon a(r\phi + s)\,(r\bar{\phi} + s) = \varepsilon(as^2 + bsr - cr^2)\,,\\
B &= A(\psi + \bar{\psi}) = \varepsilon a(\psi + \bar{\psi})\,(r\phi + s)\,(r\bar{\phi} + s)\\
&= \varepsilon a((p\phi + q)\,(r\bar{\phi} + s) + (p\bar{\phi} + q)\,(r\phi + s))\\
&= \varepsilon(2asq + b(sp + rq) - 2cpr),\\
-C &= A\psi\bar{\psi} = \varepsilon a\psi\bar{\psi}(r\phi + s)\,(r\bar{\phi} + s) = \varepsilon a(p\phi + q)\,(p\bar{\phi} + q)\\
&= \varepsilon(aq^2 + bqp - cp^2)\,.
\end{aligned}$$

Thus A, B, C are integral linear combinations of a, b, c. Similarly, a, b, c are integral linear combinations of A, B, C. Hence $GCD(A, B, C) = GCD(a, b, c) = 1$ so that J is primitive.

3. THE HOMOMORPHISM θ

Let O_D and $O_{D'}$ be two orders of O_{D_0} with $O_{D'} \subset O_D$. Then we have $D' = Df^2$ for some positive integer f. This notation will be used throughout the rest of the paper. Our aim is to define a surjective homomorphism θ from the ideal class group $C_{D'}$ onto the ideal class group C_D. After proving three lemmas, we will prove the following theorem.

THEOREM 1. *(i) Every class* C *of* $C_{D'}$ *contains a primitive ideal* I *of the form* $I = \left[a, \dfrac{fb + \sqrt{D'}}{2}\right]$, *where* $GCD(a, f) = 1$, *such that the ideal* $J = \left[a, \dfrac{b + \sqrt{D}}{2}\right]$ *is a primitive ideal of* O_D.

(ii) If $I = \left[a, \dfrac{fb + \sqrt{D'}}{2}\right]$ $(GCD(a, f) = 1)$ *and* $I' = \left[a', \dfrac{fb' + \sqrt{D'}}{2}\right]$ $(GCD(a', f) = 1)$ *are two primitive ideals in the same class* C *of* $C_{D'}$ *with* $I' = \rho I (\rho \in K^*)$, *then the ideals*

$$J = \left[a, \frac{b + \sqrt{D}}{2}\right] \quad \text{and} \quad J' = \left[a', \frac{b' + \sqrt{D}}{2}\right]$$

of O_D *satisfy* $J' = \rho J$ *and are in the same class* $\theta(C)$ *of* C_D.