3. The homomorphism

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **36 (1990)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **20.09.2024**

by Proposition 3, we have $J = \rho I$, where $\psi = \dfrac{p\phi + q}{r\phi + s}$, $\rho = \dfrac{A}{a}\dfrac{1}{r\phi + s}$ $= \varepsilon(r\bar{\phi} + s)$ 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.

(iii) The mapping $C \to \theta(C)$ *is a homomorphism of* $C_{D'}$ *to on* C_D.

Part (ii) of Theorem 1 will be the main tool in relating distances between ideals of different orders of the same real quadratic field.

LEMMA 1. *A primitive ideal* $I = \left[a, \frac{b+\sqrt{D}}{2}\right]$ *contains a number* $\alpha = xa + y\left(\frac{b+\sqrt{D}}{2}\right)$, *where* x *and* y *are coprime integers, such that the integer* $N(\alpha)/a$ *is prime to a given nonzero integer* m.

Proof. We begin by noting that $\frac{1}{a} N\left(xa + y\left(\frac{b+\sqrt{D}}{2}\right)\right) = ax^2 + bxy - cy^2$ in view of (2.5). If $|m| = 1$ we take $x = 1$, $y = 0$, $\alpha = xa + y\left(\frac{b+\sqrt{D}}{2}\right) = a$, so that $GCD(N(\alpha)/a, m) = GCD(a, 1) = 1$, as required. Hence we may suppose that $|m| > 1$. Let $p_i (i = 1, 2, \ldots, n)$ be the distinct prime factors of m. For $i = 1, 2, \ldots, n$ we set

$$(x_i, y_i) = \begin{cases} (1, 0)\ , & \text{if} \quad p_i \nmid a\ , \\ (0, 1)\ , & \text{if} \quad p_i \mid a\ , \quad p_i \nmid c\ , \\ (1, 1)\ , & \text{if} \quad p_i \mid a\ , \quad p_i \mid c\ , \end{cases}$$

so that $p_i \nmid ax_i^2 + bx_i y_i - cy_i^2$. Let x' and y' be integers such that $x' \equiv x_i \pmod{p_i}$ and $y' \equiv y_i \pmod{p_i}$ for $i = 1, 2, \ldots, n$, so that $GCD(ax'^2 + bx'y' - cy'^2, m) = 1$. The required number α is given by $\alpha = xa + y\left(\frac{b+\sqrt{D}}{2}\right)$, where $x = \frac{x'}{GCD(x', y')}$, $y = \frac{y'}{GCD(x', y')}$.

LEMMA 2. *Let* m *be a given nonzero integer. Every class* C *of* C_D *contains a primitive ideal* $\left[a, \frac{b+\sqrt{D}}{2}\right]$ *with* $GCD(a, m) = 1$.

Proof. Let $\left[a', \frac{b'+\sqrt{D}}{2}\right]$ be a primitive ideal of the class C. By Lemma 1 there exist coprime integers x and y such that

$$\text{(3.1)} \qquad GCD(a'x^2 + b'xy - c'y^2, m) = 1\ .$$

Set $a = a'x^2 + b'xy - c'y^2$ and let r and s be integers such that $xs - yr = 1$. Next set

(3.2) $$\rho = x + \left(\frac{b' - \sqrt{D}}{2a'}\right) y, \; b = 2a'xr + b'(xs + yr) - 2c'ys ,$$

so that

$$a = \rho \left(xa' + y \left(\frac{b' + \sqrt{D}}{2} \right) \right)$$

and

$$\frac{b + \sqrt{D}}{2} = \rho \left(ra' + s \left(\frac{b' + \sqrt{D}}{2} \right) \right) .$$

Then we have

$$\left[a, \frac{b + \sqrt{D}}{2} \right] = \rho \left[xa' + y \left(\frac{b' + \sqrt{D}}{2} \right) , ra' + s \left(\frac{b' + \sqrt{D}}{2} \right) \right] = \rho \left[a', \frac{b' + \sqrt{D}}{2} \right]$$

so that $\left[a, \frac{b + \sqrt{D}}{2} \right]$ is an ideal equivalent to the primitive ideal $\left[a', \frac{b' + \sqrt{D}}{2} \right]$. Hence, by Corollary 3, $\left[a, \frac{b + \sqrt{D}}{2} \right]$ is primitive.

LEMMA 3. *Let C and C' be two classes of C_D. Then there exist primitive ideals $I = \left[a, \frac{B + \sqrt{D}}{2} \right] \in C$ and $I' = \left[a', \frac{B + \sqrt{D}}{2} \right] \in C'$ with $GCD(a, a') = 1$. Moreover the ideal II' is primitive and $II' = \left[aa', \frac{B + \sqrt{D}}{2} \right]$.*

Proof. By Lemma 2 there exist primitive ideals $I = \left[a, \frac{b + \sqrt{D}}{2} \right] \in C$ and $I' = \left[a', \frac{b' + \sqrt{D}}{2} \right] \in C'$ with $GCD(a, a') = 1$. As $b \equiv D \equiv b' \pmod 2$ and $GCD(a, a') = 1$ there are integers k and k' such that $k'a' - ka = \frac{b - b'}{2}$. Set $B = b + 2ka = b' + 2k'a'$ so that

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

Now $D - B^2$ is divisible by both $4a$ and $4a'$, and so, as $GCD(a, a') = 1$, $D - B^2$ is a multiple of $4aa'$, so that $c'' = \dfrac{D - B^2}{4aa'} \in Z$. Hence $\left[aa', \dfrac{B + \sqrt{D}}{2}\right]$ is an ideal of O_D and we have

$$II' = \left(aa', a\left(\frac{B+\sqrt{D}}{2}\right), a'\left(\frac{B+\sqrt{D}}{2}\right), \left(\frac{B+\sqrt{D}}{2}\right)^2\right)$$
$$= \left(aa', \frac{B+\sqrt{D}}{2}\right)$$
$$= \left[aa', \frac{B+\sqrt{D}}{2}\right].$$

Finally, any prime divisor of aa', B, c'' must divide $GCD(a, B, a'c'') = 1$ or $GCD(a', B, ac'') = 1$, as $GCD(a, a') = 1$, which is impossible. Hence the ideal II' is primitive.

We are now ready to prove Theorem 1.

Proof of Theorem 1. (i) By Lemma 2 the class C contains a primitive ideal $I = \left[a, \dfrac{b' + \sqrt{D'}}{2}\right]$ with $GCD(a, f) = 1$. Let k be an integer such that

$$\begin{cases} 2ak \equiv -b' \pmod f, & \text{if} \quad f \equiv 1 \pmod 2, \\ ak \equiv -\dfrac{b'}{2} + D\dfrac{f}{2} \pmod f, & \text{if} \quad f \equiv 0 \pmod 2, \end{cases}$$

and set $b = (b' + 2ak)/f$, so that $I = \left[a, \dfrac{fb + \sqrt{D'}}{2}\right]$. As I is an ideal of $O_{D'}$, $(D' - f^2b^2)/4a$ is an integer, and so, as $GCD(a, f) = 1$, $c = (D - b^2)/4a$ is also an integer, showing that $J = \left[a, \dfrac{b + \sqrt{D}}{2}\right]$ is an ideal of O_D. Further, as I is primitive, we have $GCD(a, bf, cf^2) = 1$, and so $GCD(a, b, c) = 1$, showing that J is primitive.

(ii) If $I' = \rho I$, by Proposition 3, there exist integers p, q, r, s with $ps - qr = \pm 1$ such that

(3.3)
$$\frac{fb' + \sqrt{D'}}{2a'} = \frac{p\left(\dfrac{fb + \sqrt{D'}}{2a}\right) + q}{r\left(\dfrac{fb + \sqrt{D'}}{2a}\right) + s}, \quad \rho = \pm\left(r\left(\frac{fb - \sqrt{D'}}{2a}\right) + s\right).$$

Rearranging the first equation in (3.3), we obtain the following equality among elements of O_D

$$f\left(\frac{b'+\sqrt{D}}{2}\right)\left(rf\left(\frac{b+\sqrt{D}}{2}\right)+sa\right)=a'\left(pf\left(\frac{b+\sqrt{D}}{2}\right)+qa\right),$$

from which we deduce that $f \mid qaa'$. As $GCD(aa', f) = 1$ there exists an integer q' such that $q = q'f$, so (3.3) can be rewritten as

$$\frac{b'+\sqrt{D}}{2a'}=\frac{p\left(\frac{b+\sqrt{D}}{2a}\right)+q'}{rf\left(\frac{b+\sqrt{D}}{2a}\right)+s}, \quad \rho=\pm\left(rf\left(\frac{b-\sqrt{D}}{2a}\right)+s\right).$$

which, by Proposition 3, shows that $J' = \rho J$.

(iii) Let $C \in C_{D'}$ and $C' \in C_{D'}$. By Lemma 2 and (i), we can choose an ideal $I = \left[a, f\left(\frac{b+\sqrt{D}}{2}\right)\right]$ in C with $GCD(a, f) = 1$ and then an ideal $I' = \left[a', f\left(\frac{b'+\sqrt{D}}{2}\right)\right]$ in C' with $GCD(a', af) = 1$. By (i) $\left[a, \frac{b+\sqrt{D}}{2}\right]$ and $\left[a', \frac{b'+\sqrt{D}}{2}\right]$ are ideals of O_D and so we have $b \equiv b' \pmod 2$. We choose integers K' and K such that $K'a' - Ka = \frac{b-b'}{2}$, and set $B = b + 2Ka = b' + 2K'a'$, so that $I = \left[a, f\left(\frac{B+\sqrt{D}}{2}\right)\right]$ and $I' = \left[a, f\left(\frac{B+\sqrt{D}}{2}\right)\right]$. By Lemma 3 we see that $II' = \left[aa', f\left(\frac{B+\sqrt{D}}{2}\right)\right]$ is a primitive ideal of the class CC'. But the primitive ideals $J = \left[a, \frac{B+\sqrt{D}}{2}\right]$, $J' = \left[a', \frac{B+\sqrt{D}}{2}\right]$, $J'' = \left[aa', \frac{B+\sqrt{D}}{2}\right]$ belong respectively to the classes $\theta(C)$, $\theta(C')$, $\theta(CC')$, and, as $JJ' = J''$ by Lemma 3, we have $\theta(C)\,\theta(C') = \theta(CC')$, showing that θ is a homomorphism: $C_{D'} \to C_D$.

Finally we show that θ is surjective. Let C be a class of C_D and let $J = \left[a, \frac{b+\sqrt{D}}{2}\right]$ be a primitive ideal of C with $GCD(a, f) = 1$ (Lemma 2).

Then we have $GCD(a, b, c) = 1$, where $\dfrac{D - b^2}{4a} = c$, and so $GCD(a, bf, cf^2) = 1$, showing that $I = \left[a, f\left(\dfrac{b + \sqrt{D}}{2}\right)\right]$ is a primitive ideal of $O_{D'}$. Hence C is the image of the class of I under θ.

COROLLARY 4. *If the class C of $O_{D'}$ contains the primitive ideal $I = \left[a, \dfrac{b + \sqrt{D'}}{2}\right]$, where $f^2 \mid a$, then $f \mid b$ and the class $\theta(C)$ contains the primitive ideal* $J = \left[\dfrac{a}{f^2}, \dfrac{\frac{b}{f} + \sqrt{D}}{2}\right]$ *of* O_D.

Proof. As $D' = Df^2 = b^2 + 4ac$, and $f^2 \mid a$, we see that $f \mid b$, and so $GCD(f, c) = 1$. By Corollary 2 we have $I = \left(\dfrac{\sqrt{D'} - b}{2a}\right)\left[c, \dfrac{-b + \sqrt{D'}}{2}\right]$ and so, by Theorem 1, we see that $\left[c, \dfrac{-\frac{b}{f} + \sqrt{D}}{2}\right] \in \theta(C)$. Finally, by Corollary 2, $J = \left[\dfrac{a}{f^2}, \dfrac{b/f + \sqrt{D}}{2}\right] = \dfrac{\left(\sqrt{D} + \frac{b}{f}\right)}{2c}\left[c, \dfrac{\frac{-b}{f} + \sqrt{D}}{2}\right]$, showing that $J \in \theta(C)$.

4. REDUCED IDEALS

From now on in this paper we suppose that $D_0 > 0$ so that we are only considering ideals in orders of a real quadratic field. An ideal I of O_D can be written in the form $I = ad[1, \phi]$, where $\phi = \dfrac{b + \sqrt{D}}{2a}$. By Proposition 1 (ii), if $I = a'd'[1, \phi']$ is another representation of I, then $a' = \pm a$ and $\phi' \equiv \dfrac{a}{a'} \phi \pmod 1$. A real number of the form $\dfrac{b + \sqrt{D}}{2a}$, where $c = \dfrac{D - b^2}{4a}$ is an integer and $GCD(a, b, c) = 1$ is called a quadratic irrationality of discriminant D.