7. COMPARISON OF DISTANCES BETWEEN CORRESPONDING IDEALS IN DIFFERENT ORDERS

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **26.09.2024**

PROPOSITION 10. *If I and J are equivalent, reduced, primitive ideals of O_D then*

$$d(J,I) \equiv d(I,J)^{-1} \quad (\text{mod}^{\times} \eta) .$$

Proof. As I and J are in the same period we have $J = \rho I (\rho \in K^*)$ and $I = \sigma J (\sigma \in K^*)$. As $I = \rho^{-1} J$ we have $\sigma \equiv \rho^{-1} (\text{mod}^{\times} \eta)$, which proves Proposition 10.

7. COMPARISON OF DISTANCES BETWEEN CORRESPONDING IDEALS IN DIFFERENT ORDERS

Let C be a primitive class of the order O_{Df^2} and let $\theta(C)$ be the image of C by the mapping θ defined in § 3. As an application of the concept of distance described in § 6, we explain how to define a mapping of the period of C into the period of $\theta(C)$, which approximately preserves distance.

THEOREM 2. *For $D' = Df^2$ let $C \in C_{D'}$ and $\theta(C)$ its image by the surjective homomorphism $\theta : C_{D'} \to C_D$.*

(i) There exists a mapping τ from the period of C into the period of $\theta(C)$ such that for I and I' in the period of C we have, for a choice of d modulo units,

$$\frac{d(I,I')}{8f^7 D^{3/2}} < d(\tau(I), \tau(I')) < 8f^7 D^{3/2} d(I,I') . \tag{7.1}$$

(ii) When $f = p$ (prime) there exists a mapping σ from the period of C into the period of $\theta(C)$ such that for I and I' in the period of C we have, for a choice d modulo units,

$$\frac{d(I,I')}{2Dp^2} < d(\sigma(I), \sigma(I')) < 2Dp^2 d(I,I') . \tag{7.2}$$

Proof. Let $I = a[1,\phi]\,(a > 0)$ and $I' = a'[1,\phi']\,(a' > 0)$ be two equivalent, reduced, primitive ideals of a class C of $O_{D'} (D' = Df^2)$ with $\phi = \dfrac{b + \sqrt{D'}}{2a}$ and $\phi' = \dfrac{b' + \sqrt{D'}}{2a'}$ reduced. Let $\delta \in K^*$ be such that $I' = \delta I, \delta > 0$.

(i) If $GCD(a,f) = 1$ we set $I_1 = I$. If $GCD(a,f) > 1$, from the proof of Lemma 2, we see that there exists an ideal $I_1 = a_1[1,\phi_1] = \rho I$ in C with

$\rho = |x + \bar{\phi} y|$, where x and y are integers such that $a_1 = \left| ax^2 + bxy - \left(\frac{D' - b^2}{4a}\right) y^2 \right|$, $GCD(a_1, f) = 1$, $GCD(x, y) = 1, 0 \leqslant x < f,\ 0 \leqslant y < f$.

As $\phi = \dfrac{b + \sqrt{D'}}{2a}$ is reduced, we have

$$1 \leqslant a < \sqrt{D'},\ 1 \leqslant b < \sqrt{D'},\ 1 \leqslant c < \sqrt{D'} \quad \left(c = \frac{D' - b^2}{4a}\right),$$

so that $\phi < \sqrt{D'}, |\bar{\rho}| = x + \phi y < f(1 + \sqrt{D'}) < 2f\sqrt{D'}$,
and

$$(7.3) \qquad 1 \leqslant a_1 < 2\sqrt{D'}\, f^2 .$$

Also $\phi > 1,\ -1 < \bar{\phi} < 0$, so, as $\rho|\bar{\rho}| = a_1/a$, we have

$$(7.4) \qquad \frac{1}{2fD'} < \rho < f .$$

By the way in which we have defined $I_1 = \left[a_1, \dfrac{b_1 + \sqrt{D'}}{2}\right]$, we have $GCD(a_1, f) = 1$. Appealing to the proof of Theorem 1 (i), we see that there exists an integer b_2 such that $I_1 = \left[a_1, f\left(\dfrac{b_2 + \sqrt{D}}{2}\right)\right]$.

Similarly there exists an ideal $I_1' = \left[a_1', f\left(\dfrac{b_2' + \sqrt{D}}{2}\right)\right]$ such that $I_1' = \rho' I'$ with ρ' satisfying (7.4). Now, by Theorem 1, $J_1 = \left[a_1, \dfrac{b_2 + \sqrt{D}}{2}\right]$ and $J_1' = \left[a_1', \dfrac{b_2' + \sqrt{D}}{2}\right]$ are ideals of $\theta(C)$ such that $J_1' = \rho' \delta \rho^{-1} J_1$. Applying the Lagrange reduction process to J_1 and J_1', we obtain reduced ideals J and J', and, by Proposition 7, we have $J = \alpha J_1$, and $J' = \alpha' J_1'$, with (by (7.3))

$$\frac{1}{2f^2\sqrt{D'}} < \frac{1}{a_1} \leqslant \alpha < 2, \frac{1}{2f^2\sqrt{D'}} < \frac{1}{a_1'} \leqslant \alpha' < 2 .$$

Thus we have $J' = \delta' J$, where $\delta' = \alpha' \rho' \delta \rho^{-1} \alpha^1$ satisfies

$$\frac{\delta}{8f^4 D'^{3/2}} < \delta' < 8f^4 D'^{3/2} \delta .$$

Setting $J = \tau(I)$ gives the required mapping and proves (7.1).

(ii) When $f = p$ (prime) and p does not divide a, we set $I_1 = I$. If p divides a, we take for I the ideal $a_1[1, \phi_1]$ following I in its period. In this case, as $p \mid a$, from $p^2D = b_1^2 + 4aa_1$, we see that $p \mid b_1$ and so, as $GCD(a_1, b_1, a) = 1$ we see that p does not divide a_1. Then, by (2.12), we have $I_1 = \rho I$ with $\rho = \frac{a_1}{a}\phi_1$. Now, by Proposition 5, $\phi_1 = \frac{b_1 + \sqrt{D'}}{2a_1}$ is reduced, so that $1 \leqslant b_1 < \sqrt{D'}$, and

(7.5) $$1 \leqslant a_1 < \sqrt{D'}\ ,$$

giving

(7.6) $$1 \leqslant \rho < \sqrt{D'}\ .$$

The rest of the proof follows exactly as in the proof of (i) using (7.5) (resp. (7.6)) in place of (7.3) (resp. (7.4)).

8. Gauss's reduction process

Definition 14. (Half-reduced) A representation $\{a, b\}$ of an ideal I is said to be *half-reduced* if

(8.1) $$0 < \frac{-b + \sqrt{D}}{2|c|} < 1\ ,$$

where $c = (D - b^2) \mid 4a$.

An ideal I is called *half-reduced* if there exists a half-reduced representation of I.

Clearly, if $\{a, b\}$ is half-reduced, then $b < \sqrt{D}$ and $\{-a, b\}$ is half-reduced.

LEMMA 7. *Let I be a primitive ideal of O_D. To each representation $\{a, b\}$ of I corresponds a unique integer q such that the q-neighbour representation $\{a', b'\}$ is half-reduced. The integer b' and the ideal $I' = \left[a', \frac{b' + \sqrt{D}}{2}\right]$ are determined by I. The value of q is*

(8.2) $$q = \frac{a}{|a|}\left[\frac{b + \sqrt{D}}{2|a|}\right].$$