

7. COMPARISON OF DISTANCES BETWEEN CORRESPONDING IDEALS IN DIFFERENT ORDERS

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **12.07.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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

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

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 $\sigma \equiv \rho^{-1} \pmod{\times \eta}$, 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 $\theta: C_{D'} \rightarrow C_D$.*

(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,*

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

(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,*

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

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 $\phi = \frac{b + \sqrt{D'}}{2a}$ and $\phi' = \frac{b' + \sqrt{D'}}{2a'}$ reduced. Let $\delta \in K^*$ be such that $I' = \delta I, \delta > 0$.

(i) If $\text{GCD}(a, f) = 1$ we set $I_1 = I$. If $\text{GCD}(a, f) > 1$, 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 $a_1 = |ax^2 + bxy - \left(\frac{D' - b^2}{4a}\right)y^2|$, $GCD(a_1, f) = 1$, $GCD(x, y) = 1$, $0 \leq x < f$, $0 \leq y < f$.

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

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

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

and

$$(7.3) \quad 1 \leq a_1 < 2\sqrt{D'} f^2.$$

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

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

By the way in which we have defined $I_1 = \left[a_1, \frac{b_1 + \sqrt{D'}}{2} \right]$, 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 $I_1 = \left[a_1, f \left(\frac{b_2 + \sqrt{D}}{2} \right) \right]$.

Similarly there exists an ideal $I'_1 = \left[a'_1, f \left(\frac{b'_2 + \sqrt{D}}{2} \right) \right]$ such that $I'_1 = \rho'I'$

with ρ' satisfying (7.4). Now, by Theorem 1, $J_1 = \left[a_1, \frac{b_2 + \sqrt{D}}{2} \right]$ and

$J'_1 = \left[a'_1, \frac{b'_2 + \sqrt{D}}{2} \right]$ 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))

$$\frac{1}{2f^2\sqrt{D'}} < \frac{1}{a_1} \leq \alpha < 2, \frac{1}{2f^2\sqrt{D'}} < \frac{1}{a'_1} \leq \alpha' < 2.$$

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

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

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 $\text{GCD}(a_1, b_1, a) = 1$ 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 $1 \leq b_1 < \sqrt{D'}$, and

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

giving

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

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

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

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

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