6. Periods of reduced cycles

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **09.08.2024**

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.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

$< \dfrac{2a_{n_0-1}}{a_{n_0}}$. Then, appealing to (5.20), we obtain

$$1 < \phi_1 \dots \phi_{n_0} < \frac{2a_0}{a_{n_0} B_{n_0-3}},$$

so that, by (5.17), we have

$$\frac{a_{n_0}}{a_0} < \delta < \frac{2}{B_{n_0-3}}.$$

It remains to consider the case $n_0 = 1$. If I_0 is reduced then $\delta = 1$. If I_0 is not reduced then $\delta = \dfrac{a_1}{a_0}\phi_1$ and, as above, we have $1 < \phi_1 < \dfrac{2a_0}{a_1}$, giving $\dfrac{a_1}{a_0} < \delta < 2$.

Hence in all cases we have $\dfrac{1}{a_0} \leqslant \delta < 2$. All subsequent Lagrange neighbours of I are reduced by Lemma 5. This completes the proof of Proposition 7.

6. Periods of reduced cycles

We show that any two equivalent reduced, primitive ideals of the same order O_D can be obtained from one another by using the Lagrange reduction process described in §5.

PROPOSITION 8. ([5]: §31, [12]: Theorem 4.5) *Let* $I = a[1, \phi]$ $(a > 0)$ *and* $J = b[1, \psi]$ $(b > 0)$ *be two equivalent, reduced, primitive ideals of* O_D, *so that* $[1, \psi] = \rho[1, \phi]$ *for some* $\rho(>0) \in K^*$. *Interchanging* I *and* J *if necessary we may suppose that* $\rho \geqslant 1$. *Set* $I_0 = I$. *Then there exists a non negative integer* n *such that* $J = I_n$ *and* $\rho = \phi_1 \dots \phi_n$, *so that* $J = I_n = \rho_n I$.

Proof. Recalling that $\phi_n > 1$ $(n \geqslant 1)$, we see from (5.10) and (5.13) that the sequence $\{\phi_1 \dots \phi_n\}_{n=0}^{\infty}$ is monotonically increasing and unbounded. Hence there exists an integer $n \geqslant 0$ such that $\phi_1 \dots \phi_n \leqslant \rho < \phi_1 \dots \phi_{n+1}$. As $I_n = \dfrac{a_n}{a_0}\phi_1 \dots \phi_n I_0$ (by (5.5)), we have $\dfrac{1}{b}J = \dfrac{\rho}{\phi_1 \dots \phi_n}\dfrac{1}{a_n}I_n$. If $\rho = \phi_1 \dots \phi_n$ then

$\frac{1}{b} J = \frac{1}{a_n} I_n$ and so, by Proposition 2 (iii), we have $b = a_n$ and $J = I_n$ as required. This we may suppose that $\rho > \phi_1 \dots \phi_n$. Replacing I_0 by I_n, we obtain

$$(6.1) \qquad \frac{1}{b} J = \rho \frac{1}{a_0} I_0, \quad \text{where} \quad 1 < \rho < \phi_1 .$$

From (6.1), we see that $\frac{a_0}{\rho} J = b I_0$, and so, as $J\bar{J} = (b)$, we have $\frac{a_0}{\rho} = I_0 \bar{J}$, showing that $\frac{1}{\rho} \in \frac{1}{a_0} I_0$. Next we observe that

$$\frac{1}{a_0} I_0 = \frac{1}{\phi_1 a_1} I_1 = \frac{1}{\phi_1} [1, \phi_1] = \left[1, \frac{1}{\phi_1}\right] ,$$

so there are integers x and y such that

$$\frac{1}{\rho} = x + \frac{y}{\phi_1} .$$

Thus, as $1 < \rho < \phi_1$, we have

$$(6.2) \qquad \frac{1}{\phi_1} < x + \frac{y}{\phi_1} < 1 .$$

Appealing to (6.1), we obtain

$$J = \frac{b\rho}{a_0} I_0 = \frac{b\rho}{a_1 \phi_1} I_1 = \frac{b\rho}{\phi_1} [1, \phi_1] ,$$

so that $\frac{b\rho}{\phi_1} \in J$, and $0 < \frac{b\rho}{\phi_1} < b$. As J is reduced, by Proposition 4, we have $\left| \frac{b\bar{\rho}}{\bar{\phi}_1} \right| = \frac{b\,|\bar{\rho}|}{|\bar{\phi}_1|} > b$, so that $\left| \frac{1}{\bar{\rho}} \right| < \left| \frac{1}{\bar{\phi}_1} \right|$, that is

$$(6.3) \qquad \left| x + \frac{y}{\bar{\phi}_1} \right| < \frac{1}{|\bar{\phi}_1|} .$$

From (6.2) we see that $y \neq 0$. Then (6.3) shows that $x \neq 0$, and that, as $\bar{\phi}_1 < 0, xy > 0$. This contradicts (6.2), and completes the proof of Proposition 8.

Let I_0 be a reduced, primitive ideal of a class C of O_D. By the Lagrange reduction process described in §5, we obtain (by Proposition 5) an infinite sequence $\{I_n\}_{n=0}^{\infty}$ of reduced, primitive ideals with each ideal I_n equivalent to I_0. By Proposition 8, this sequence contains all the reduced, primitive ideals of the class C. As C contains only a finite number of reduced, primitive ideals (§4), there exist integers r and l with $0 \leqslant r < r + l$ such that $I_r = I_{r+l}$. Applying Proposition 6 (ii), we obtain successively $I_{r-1} = I_{r+l-1}, I_{r-2} = I_{r+l-2}, \ldots$, and, after r steps, we have $I_0 = I_l$, which shows that the sequence $\{I_n\}_{n=0}^{\infty}$ is purely periodic.

Definition 12. (Period) Let I_0 be a reduced, primitive ideal of a class C of O_D. Let l be the least positive integer with $I_0 = I_l$. The set $\{I_0, \ldots, I_{l-1}\}$ is called the *period* of the class C. The length of the period is the integer l.

The period of the class C of O_D consists of all the reduced, primitive ideals in C. It is easy to see that if $I_s = I_t$ then l divides $s - t$. As $I_l = I_0$, we see, from (5.5), that $I_0 = \eta I_0$, where

$$\eta = \rho_l = \prod_{i=1}^{l} \phi_i , \tag{6.4}$$

and so, by Proposition 2 (ii), η is a unit (> 1) of O_D.

PROPOSITION 9. (i) *If $I = I_0$ and J are equivalent, reduced, primitive ideals of O_D with $J = \alpha I_0$, where $\alpha (\geqslant 1) \in K^*$, then there exist unique integers q and s such that*

$$\alpha = \eta^q \rho_s \quad (\rho_s \textit{ is defined in (5.5), } \eta \textit{ in (6.4)})$$

where

$$q \geqslant 0 , \quad 0 \leqslant s \leqslant l - 1 .$$

(ii) If $J = I$ then we have $s = 0$ and $\alpha = \eta^q$.

Proof. (i) By Proposition 8 there exists a nonnegative integer n such that

$$J = I_n = \rho_n I_0 , \quad \alpha = \rho_n .$$

Let $q (\geqslant 0)$ and s be the integers defined uniquely by

$$n = ql + s , \quad 0 \leqslant s \leqslant l - 1 .$$

Then, by periodicity, we have

$$\alpha = \rho_s (\rho_l)^q = \eta^q \rho_s ,$$

where

$$\eta = \rho_l = \phi_1 \dots \phi_l .$$

This shows the existence of the integers $q(\geqslant 0)$ and $s(0 \leqslant s \leqslant l-1)$.

We next show that q and s are unique. Suppose we have $\alpha = \eta^{q_1}\rho_{s_1} = \eta^{q_2}\rho_{s_2}$ with $s_1 \leqslant s_2$. If $s_2 > s_1$ then $q_1 > q_2$ and, appealing to (5.5) and recalling that $-1 < \bar{\phi}_i < 0 (i \geqslant 1)$, we obtain

$$\eta \leqslant \eta^{q_1 - q_2} = \frac{\rho_{s_2}}{\rho_{s_1}} = \prod_{i=s_1+1}^{s_2} \left(\frac{-1}{\bar{\phi}_i}\right) < \prod_{i=1}^{l} \left(\frac{-1}{\bar{\phi}_i}\right) = \eta ,$$

which is a contradiction. Hence we must have $s_1 = s_2$. Then $\eta^{q_1} = \eta^{q_2}$ and, as $\eta > 1$, we must have $q_1 = q_2$. This completes the proof of (i).

(ii) From the proof of (i) we see that $I_n = J = I_0$, so that $l \mid n$, and thus $q = n/l$ and $s = 0$.

COROLLARY 5. $\eta = \prod_{i=1}^{l} \phi_i$ *is a unit* (>1) *of* O_D *such that every unit* ε *of* O_D *is given by* $\varepsilon = \pm \eta^r$, *where* r *is an integer.* η *is called the fundamental unit of* O_D.

Proof. Let ε be a unit of O_D and let

$$\delta = \begin{cases} \varepsilon , & \text{if} \quad \varepsilon \geqslant 1 , \\ 1/\varepsilon , & \text{if} \quad 0 < \varepsilon < 1 , \\ -1/\varepsilon , & \text{if} \quad -1 < \varepsilon < 0 , \\ -\varepsilon , & \text{if} \quad \varepsilon \leqslant -1 , \end{cases}$$

so that δ is a unit of O_D satisfying $\delta \geqslant 1$. Applying Proposition 9 (ii) to I_0 and $J = \delta I_0$, we see that $\delta = \eta^q$, and so $\varepsilon = \pm \eta^r$.

Corollary 5 was first proved by Lagrange in the case of the principal class [3: p. 452] (see also [8]). We see that the theory of periods of reduced, primitive ideals in O_D not only gives the structure of the group of units of O_D but also provides the structure of each period (the "infrastructure" of Shanks [7]).

COROLLARY 6. *With* I_0 *a reduced, primitive ideal of* O_D, *we have*

(i) $\eta = B_{l-1}\phi_0 + B_{l-2}$,

(ii) $\eta = A_{l-1} - B_{l-1}\bar{\phi}_0$,

(iii) $l \log \left(\frac{1+\sqrt{5}}{2}\right) \leqslant \log \eta < l \log \sqrt{D}$

Proof. Taking $n = Nl (N = 1, 2, \ldots)$ in (5.13) we obtain, as $\phi_{Nl} = \phi_0$,

$$\eta^N = B_{Nl-1}\phi_0 + B_{Nl-2} . \tag{6.5}$$

The assertion (i) is the case $N = 1$.

From (5.7), (5.9) and (5.13), we obtain for $n \geqslant 1$

$$\phi_1 \ldots \phi_n = \frac{(-1)^{n-1}}{B_{n-1}\phi_0 - A_{n-1}} .$$

Taking $n = Nl (N = 1, 2, \ldots)$ and recalling that $\eta\bar{\eta} = (-1)^l$, we obtain $\eta^N = -\dfrac{(\eta\bar{\eta})^N}{B_{Nl-1}\phi_0 - A_{Nl-1}}$, so that taking conjugates we deduce

$$\eta^N = A_{Nl-1} - B_{Nl-1}\bar{\phi}_0 . \tag{6.6}$$

The assertion (ii) is the case $N = 1$.

From (6.5) and (5.10) we have

$$\eta^N > B_{Nl-1} + B_{Nl-2} \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{Nl-2} + \left(\frac{1+\sqrt{5}}{2}\right)^{Nl-3} = \left(\frac{1+\sqrt{5}}{2}\right)^{Nl-1},$$

so that

$$\eta > \left(\frac{1+\sqrt{5}}{2}\right)^{l-(1/N)} \qquad (N = 1, 2, 3, \ldots) .$$

Letting $N \to \infty$, we obtain

$$\eta \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{l},$$

proving the first equality in (iii).

Finally, as $\phi_i < \sqrt{D} (i \geqslant 0)$, we have

$$\eta = \phi_1 \ldots \phi_l < (\sqrt{D})^l ,$$

proving the second assertion in (iii).

Example 3. $(D = 1892)$ The period of the class containing the ideal $[1, 21 + \sqrt{473}]$ is

$$\{[1, 21 + \sqrt{473}],\ [32, 21 + \sqrt{473}],\ [11, 11 + \sqrt{473}],\ [32, 11 + \sqrt{473}]\}.$$

Thus, by Corollary 5, the fundamental unit of O_{1892} is

$$(21 + \sqrt{473}) \left(\frac{21+\sqrt{473}}{32}\right) \left(\frac{11+\sqrt{473}}{11}\right) \left(\frac{11+\sqrt{473}}{32}\right)$$

$$= \frac{1}{11.32^2}(21+\sqrt{473})^2(11+\sqrt{473})^2$$
$$= \frac{1}{11.32^2}(704+32\sqrt{473})^2$$
$$= \frac{1}{11}(22+\sqrt{473})^2$$
$$= 87+4\sqrt{473}$$
$$= 87+2\sqrt{1892}.$$

The period of the class containing the ideal $[7, 16+\sqrt{473}]$ is

$$\{[7,16+\sqrt{473}], [16,19+\sqrt{473}], [19,13+\sqrt{473}], [23,6+\sqrt{473}], [8,17+\sqrt{473}], [31,15+\sqrt{473}]\}$$

so, by Corollary 5, the fundamental unit of O_{1892} is also given by

$$\left(\frac{16+\sqrt{473}}{7}\right)\left(\frac{19+\sqrt{473}}{16}\right)\left(\frac{13+\sqrt{473}}{19}\right)\left(\frac{6+\sqrt{473}}{23}\right)\left(\frac{17+\sqrt{473}}{8}\right)\left(\frac{15+\sqrt{473}}{31}\right)$$
$$= \left(\frac{111+5\sqrt{473}}{16}\right)\left(\frac{29+\sqrt{473}}{23}\right)\left(\frac{91+4\sqrt{473}}{31}\right)$$
$$= \frac{(349+16\sqrt{473})}{23}\,\frac{(91+4\sqrt{473})}{31}$$
$$= 87+4\sqrt{473} = 87+2\sqrt{1892}.$$

We are now in a position to define the distance between two reduced, primitive ideals in the same period.

Definition 13. (Distance between ideals) If I and J are equivalent, reduced, primitive ideals of O_D then we define the (mutiplicative) *distance* $d(I, J)$ from I to J by

$$d(I, J) \equiv \rho_s (\mathrm{mod}^{\times}\, \eta)$$

where ρ_s is given as in Proposition 9 (i).

It is clear that $d(I, I) = 1$.

Example 4. $(D = 1892)$ The two reduced, primitive ideals

$$I = [19, 6+\sqrt{473}] \quad \text{and} \quad J = [31, 16+\sqrt{473}]$$

of O_{1892} are equivalent. Applying the Lagrange reduction process to $[19, 6+\sqrt{473}]$, we obtain

$$[19, 6+\sqrt{473}] \xrightarrow{L} [16, 13+\sqrt{473}] \xrightarrow{L} [7, 19+\sqrt{473}] \xrightarrow{L} [31, 16+\sqrt{473}] ,$$

so that

$$\begin{aligned} d(I, J) = \rho_3 &= \frac{31}{19}\left(\frac{13+\sqrt{473}}{16}\right)\left(\frac{19+\sqrt{473}}{7}\right)\left(\frac{16+\sqrt{473}}{31}\right) \\ &= \frac{(13+\sqrt{473})\ (111+5\sqrt{473})}{19 \times 16} \\ &= \frac{238+11\sqrt{473}}{19} . \end{aligned}$$

On the other hand, applying the Lagrange reduction process to $[31, 16+\sqrt{473}]$, we obtain

$$[31, 16+\sqrt{473}] \xrightarrow{L} [8, 15+\sqrt{473}] \xrightarrow{L} [23, 17+\sqrt{473}] \xrightarrow{L} [19, 6+\sqrt{473}] ,$$

so that

$$\begin{aligned} d(J, I) &= \frac{19}{31}\left(\frac{15+\sqrt{473}}{8}\right)\left(\frac{17+\sqrt{473}}{23}\right)\left(\frac{6+\sqrt{473}}{19}\right) \\ &= \frac{(91+4\sqrt{473})\ (6+\sqrt{473})}{31 \times 23} \\ &= \frac{2438+115\sqrt{473}}{31 \times 23} \\ &= \frac{106+5\sqrt{473}}{31} . \end{aligned}$$

We note that

$$\begin{aligned} &\left(\frac{238+11\sqrt{473}}{19}\right)\left(\frac{106+5\sqrt{473}}{31}\right) \\ &= \frac{51243+2356\sqrt{473}}{589} \\ &= 87+4\sqrt{473} = \eta \\ &\equiv 1 \,(\mathrm{mod}^{\times}\, \eta) . \end{aligned}$$

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

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

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 $\sigma \equiv \rho^{-1} (\bmod^{\times} \eta)$, 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