

5. Lagrange's reduction procedure

Objektyp: **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.

$\phi = \bar{\phi} + \frac{\sqrt{D}}{a} > -1$. Hence, as ϕ cannot satisfy (4.4), we must have $\phi > 1$, so I is reduced.

LEMMA 4. If $I = d \left[a, \frac{b + \sqrt{D}}{2} \right]$ is an ideal of O_D with $0 < a < \frac{\sqrt{D}}{2}$ then I is reduced.

Proof. We can write $I = da[1, \phi]$ with $-1 < \bar{\phi} < 0$. Then we have $\phi = \bar{\phi} + \frac{\sqrt{D}}{a} > 1$ so that I is reduced.

5. LAGRANGE'S REDUCTION PROCEDURE

In this section we describe Lagrange's reduction procedure which was first introduced in [2]. This procedure uses Lagrange neighbours and so is based on the continued fraction algorithm. The procedure, when applied to a given primitive ideal I of O_D , gives all the reduced ideals of O_D which are equivalent to I .

Let $\{a, b\}$ be a representation of the primitive ideal I of O_D . The Lagrange neighbour of $\{a, b\}$ is the representation $\{a', b'\}$ of the primitive ideal I' of O_D given as follows:

$$(5.1) \quad \begin{cases} q = [\phi] = \left[\frac{b + \sqrt{D}}{2a} \right], & \phi = q + \frac{1}{\phi'}, \\ b' = -b + 2aq, & a' = \frac{D - b'^2}{4a} = \frac{D - b^2}{4a} + bq - aq^2, \end{cases}$$

(see (2.10) and (2.11)). We write $\{a, b\} \xrightarrow{L} \{a', b'\}$. The primitive ideal $I' = a'[1, \phi']$ is also called the Lagrange neighbour of I .

We note that

$$\phi' = \frac{1}{\phi - q} > 1, [\phi'] \geq 1,$$

as $q = [\phi]$. We also remark that if a is kept fixed and ϕ is changed modulo 1 then ϕ', b' and a' do not change. Hence the Lagrange neighbour of $\{a, b\}$ depends only upon the sign of a . If $\{a, b\} \xrightarrow{L} \{a', b'\}$ then by Corollary 1 the

ideals $I = a[1, \phi]$ and $I' = a'[1, \phi']$ are equivalent and $I' = \rho I$ with $\rho = \frac{a'}{a} \phi' = \frac{-1}{\bar{\phi}'}$.

PROPOSITION 5. *If $\{a, b\} \xrightarrow{L} \{a', b'\}$, where $a > 0$ and the ideal $I = a[1, \phi]$ is reduced, then the number ϕ' is reduced and the ideal $I' = a'[1, \phi']$ is reduced.*

Proof. As $a > 0$ and the ideal I is reduced, we may assume that ϕ is reduced, so that $-1 < \bar{\phi}' = \frac{1}{\bar{\phi} - q} < 0$, where $q = [\phi]$, showing that ϕ' is reduced. The ideal I' is reduced as ϕ' is reduced.

Remark. If $\{a, b\} \xrightarrow{L} \{a', b'\}$, where $a < 0$ and the ideal $I = a[1, \phi]$ is reduced, it may happen that the Lagrange neighbour $I' = a'[1, \phi']$ of I is not reduced. For example the ideal $I = [3, 7 + \sqrt{82}]$ of O_{328} is reduced and $\{-3, 14\} \xrightarrow{L} \{13, 22\}$, but the Lagrange neighbour $I' = [13, 11 + \sqrt{82}]$ of I is not reduced.

The next proposition gives information about the ideals having a specified Lagrange neighbour.

PROPOSITION 6. (i) *If $\{a_1, b_1\} \xrightarrow{L} \{a', b'\}$ and $\{a_2, b_2\} \xrightarrow{L} \{a', b'\}$ then the primitive ideals $a_1[1, \phi_1], a_2[1, \phi_2]$ are equal.*

(ii) *If $a'[1, \phi']$ is a primitive ideal with $a' > 0$ and ϕ' reduced, then there exists a unique reduced primitive ideal $a[1, \phi]$ such that $\{a, b\} \xrightarrow{L} \{a', b'\}$.*

Proof. (i) Let $q_1 = [\phi_1]$ and $q_2 = [\phi_2]$. Then we have $\phi_1 = q_1 + \frac{1}{\phi'}$ and $\phi_2 = q_2 + \frac{1}{\phi'}$, so that $\frac{b_1 + \sqrt{D}}{2a_1} = (q_1 - q_2) + \frac{b_2 + \sqrt{D}}{2a_2}$, showing that $a_1 = a_2$ and $\phi_1 \equiv \phi_2 \pmod{1}$. Hence we have $a_1[1, \phi] = a_2[1, \phi_2]$.

(ii) As ϕ' is reduced we have $\phi' > 1$ and $-1 < \bar{\phi}' < 0$. Hence there is a unique integer $q (\geq 1)$ such that $-1 - \frac{1}{\bar{\phi}'} < q < \frac{-1}{\bar{\phi}'}$. Set $\phi = q + \frac{1}{\phi'} > 1$. It is easy to check that $\phi = \frac{b + \sqrt{D}}{2a}$, where $a, b \in \mathbb{Z}$. Then $\bar{\phi} = q + \frac{1}{\bar{\phi}'}$ satisfies $-1 < \bar{\phi} < 0$. Thus ϕ is reduced and the ideal $a[1, \phi]$ is both primitive and

reduced. Clearly $\{a, b\} \xrightarrow{L} \{a', b'\}$ and the uniqueness of the ideal $a[1, \phi]$ follows from (i).

Now that we have the notion of Lagrange neighbour and its basic properties, we can define the Lagrange reduction process, which transforms a given primitive ideal into a reduced ideal.

Definition 11. (Lagrange reduction process) We start a representation $\{a_0, b_0\}$ with $a_0 > 0$ of a primitive ideal I of O_D , and define the sequence of representations $\{a_n, b_n\}$ of the primitive ideals I_n by

$$(5.2) \quad \{a_n, b_n\} \xrightarrow{L} \{a_{n+1}, b_{n+1}\} \quad (n=0, 1, 2, \dots) .$$

In the Lagrange reduction process the integers q_n and the quantities ϕ_n are given by

$$(5.3) \quad q_n = [\phi_n] , \quad \phi_n = \frac{b_n + \sqrt{D}}{2a_n} ,$$

so that

$$(5.4) \quad I_n = a_n[1, \phi_n] = \left[a_n, \frac{b_n + \sqrt{D}}{2} \right] .$$

By Corollary 1, we have

$$(5.5) \quad I_n = \rho_n I_0, \rho_n = \prod_{i=1}^n \left(\frac{-1}{\bar{\phi}_i} \right) = \frac{a_n}{a_0} \prod_{i=1}^n \phi_i .$$

We remark that $q_n \geq 1$ for $n \geq 1$.

The next lemma tells us that if $\bar{\phi}_n$ is negative for some $n \geq 1$ then I_n and its successive Lagrange neighbours are all reduced.

LEMMA 5. *If $n \geq 1$ and $\bar{\phi}_n < 0$*

then

(i) $a_m > 0$, for $m \geq n - 1$,

and

(ii) $I_m = a_m[1, \phi_m]$ is reduced for $m \geq n$.

Proof. (i) As $q_n \geq 1$ and $\bar{\phi}_n < 0$, we see that $\bar{\phi}_{n+1} = \frac{1}{\bar{\phi}_n - q_n} < 0$, and so $\bar{\phi}_m < 0$ for $m \geq n$. For $m \geq n$ we have $\phi_m = \frac{b_m + \sqrt{D}}{2a_m} > 1$ and

$\bar{\phi}_m = \frac{b_m - \sqrt{D}}{2a_m} < 0$, so that $a_m > 0$ and $|b_m| < \sqrt{D}$. By (5.1) we have $D - b_m^2 = 4a_m a_{m-1} > 0$, so that $a_{m-1} > 0$. This completes the proof that $a_m > 0$ for $m \geq n - 1$.

(ii) We have $I_m = a_m [1, \phi_m] = a_m [1, \psi_m]$, where $\psi_m = \phi_m + [|\bar{\phi}_m|]$. For $m \geq n \geq 1$, as $\psi_m \geq \phi_m > 1$ and $-1 < \bar{\psi}_m = \bar{\phi}_m + [|\bar{\phi}_m|] < 0$, we see that ψ_m is a reduced number, and so the ideal $I_m (m \geq n)$ is reduced.

Next we define two sequences of integers $\{A_n\}$ and $\{B_n\}$ for $n \geq -2$ by

$$(5.6) \quad \begin{cases} A_{-2} = 0, & A_{-1} = 1, & A_n = q_n A_{n-1} + A_{n-2}, \\ B_{-2} = 1, & B_{-1} = 0, & B_n = q_n B_{n-1} + B_{n-2}. \end{cases}$$

These sequences have the following basic properties:

$$(5.7) \quad \phi_n = - \left(\frac{B_{n-2} \phi_0 - A_{n-2}}{B_{n-1} \phi_0 - A_{n-1}} \right), \quad n \geq 0,$$

$$(5.8) \quad \phi_0 = \frac{A_{n-1} \phi_n + A_{n-2}}{B_{n-1} \phi_n + B_{n-2}}, \quad n \geq 0,$$

$$(5.9) \quad A_n B_{n-1} - A_{n-1} B_n = (-1)^{n-1}, \quad n \geq -1,$$

$$(5.10) \quad \begin{cases} B_n \geq \left(\frac{1 + \sqrt{5}}{2} \right)^{n-1}, & n \geq 0, \\ \text{if } q_0 \geq 1 \text{ then } A_n \geq \left(\frac{1 + \sqrt{5}}{2} \right)^n, & n \geq 0, \end{cases}$$

$$(5.11) \quad \frac{A_n}{B_n} - \phi_0 = \frac{(-1)^{n-1}}{B_n^2 \phi_{n+1} + B_n B_{n-1}}, \quad n \geq 0,$$

$$(5.12) \quad (-1)^n (\phi_0 - \bar{\phi}_0) = \frac{1}{(B_{n-1}^2 \bar{\phi}_n + B_{n-1} B_{n-2})}$$

$$- \frac{1}{(B_{n-1}^2 \phi_n + B_{n-1} B_{n-2})}, \quad n \geq 0,$$

$$(5.13) \quad \phi_1 \dots \phi_n = B_{n-1} \phi_n + B_{n-2}, \quad n \geq 1.$$

We now briefly mention how these properties can be proved. The equalities (5.8) and (5.13) follow by induction using $\phi_n = q_n + \frac{1}{\phi_{n+1}}$. The assertion

(5.7) is just a reformulation of (5.8). The assertions (5.9) and (5.10) follow by induction using (5.6); (5.11) follows from (5.8) and (5.9); and (5.12) follows from (5.11).

The next result shows that $\bar{\phi}_n$ does eventually become negative.

LEMMA 6. (Compare [12]: Corollary 4.2.1) *Let*

$$(5.14) \quad M_0 = \max \left(\frac{1}{2} \frac{\text{Log}(a_0/\sqrt{D})}{\text{Log}((1+\sqrt{5})/2)} + \frac{5}{2}, 2 \right).$$

For $n \geq M_0$ we have $\bar{\phi}_n < 0$.

Proof. For $n \geq M_0$, we have $n \geq 2$, and, appealing to (5.10) and (5.14), we obtain

$$(5.15) \quad B_{n-1}B_{n-2} \geq \left(\frac{1 + \sqrt{5}}{2} \right)^{2n-5} \geq \frac{a_0}{\sqrt{D}} = \frac{1}{|\phi_0 - \bar{\phi}_0|}.$$

If $\bar{\phi}_n > 0$, then, by (5.12), we have

$$|\phi_0 - \bar{\phi}_0| < \max \left(\frac{1}{B_{n-1}^2 \bar{\phi}_n + B_{n-1}B_{n-2}}, \frac{1}{B_{n-1}^2 \phi_n + B_{n-1}B_{n-2}} \right) < \frac{1}{B_{n-1}B_{n-2}},$$

which contradicts (5.15). Hence we must have $\bar{\phi}_n < 0$, for $n \geq M_0$.

The next proposition gives an upper bound for the number of steps needed in the Lagrange reduction process to obtain a reduced ideal I from a given primitive ideal I_0 of O_D and at the same time gives upper and lower bounds for δ in the relation $I = \delta I_0$.

PROPOSITION 7. (Compare [12]: Theorem 4.3) *Let $I_0 = a_0[1, \phi_0]$ be a primitive ideal of O_D with $a_0 > 0$. Then the Lagrange reduction process applied to I_0 yields a reduced, primitive ideal I equivalent to I_0 with*

$$(5.16) \quad I = \delta I_0, \quad \frac{1}{a_0} \leq \delta < 2,$$

in at most M_0 steps. All the subsequent Lagrange neighbours of I are also reduced.

Proof. Let n_0 be the least positive integer such that $\bar{\phi}_{n_0} < 0$. By Proposition 7 we have $n_0 \leq M_0$. By Lemma 5 the ideal I_{n_0} is reduced, and $a_{n_0-1} > 0, a_{n_0} > 0$.

We set

$$(5.17) \quad \delta = \begin{cases} \frac{a_{n_0-1}}{a_0} \phi_1 \dots \phi_{n_0-1}, & \text{if } I_{n_0-1} \text{ is reduced,} \\ \frac{a_{n_0}}{a_0} \phi_1 \dots \phi_{n_0}, & \text{if } I_{n_0-1} \text{ is not reduced,} \end{cases}$$

so that by (5.3) $I = \delta I_0$ is reduced, and it remains to show that $\frac{1}{a_0} \leq \delta < 2$.

For $n_0 \geq 2$, by (5.13), we have

$$(5.18) \quad \phi_1 \dots \phi_{n_0-1} = B_{n_0-2} \phi_{n_0-1} + B_{n_0-3},$$

so that

$$(5.19) \quad \bar{\phi}_1 \dots \bar{\phi}_{n_0-1} = B_{n_0-2} \bar{\phi}_{n_0-1} + B_{n_0-3} > B_{n_0-3},$$

by the definition of n_0 . As $\phi_n \bar{\phi}_n = \frac{-a_{n-1}}{a_n}$, for $n \geq 1$, we have

$$(5.20) \quad (\phi_1 \dots \phi_{n_0-1}) (\bar{\phi}_1 \dots \bar{\phi}_{n_0-1}) = (-1)^{n_0-1} \frac{a_0}{a_{n_0-1}},$$

which shows (as $a_0 > 0, a_{n_0-1} > 0, \phi_i > 1 (i \geq 1), \phi_i > 0 (1 \leq i \leq n_0 - 1)$) that n_0 is odd. Hence $n_0 \geq 3$ and we have $B_{n_0-3} \geq 1$. Then, from (5.19) and (5.20), we obtain

$$(5.21) \quad 1 < \phi_1 \dots \phi_{n_0-1} < \frac{a_0}{a_{n_0-1}} \frac{1}{B_{n_0-3}}.$$

If I_{n_0-1} is reduced then, by (5.17) and (5.21), we obtain

$$\frac{a_{n_0-1}}{a_0} < \delta < \frac{1}{B_{n_0-3}}.$$

If I_{n_0-1} is not reduced then, as $a_{n_0-1} > 0$, by Lemma 4 we have $a_{n_0-1} > \frac{\sqrt{D}}{2}$.

Further, as $a_{n_0} > 0$ and $D = b_{n_0}^2 + 4a_{n_0-1}a_{n_0}$, we see that $1 < \phi_{n_0} < \frac{\sqrt{D}}{a_{n_0}}$

$< \frac{2a_{n_0-1}}{a_{n_0}}$. 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 $\delta = \frac{a_1}{a_0} \phi_1$ and, as above, we have $1 < \phi_1 < \frac{2a_0}{a_1}$, giving

$$\frac{a_1}{a_0} < \delta < 2.$$

Hence in all cases we have $\frac{1}{a_0} \leq \delta < 2$. 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 $\rho \geq 1$. 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 $\phi_n > 1$ ($n \geq 1$), 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 $n \geq 0$ such that $\phi_1 \dots \phi_n \leq \rho < \phi_1 \dots \phi_{n+1}$. As

$I_n = \frac{a_n}{a_0} \phi_1 \dots \phi_n I_0$ (by (5.5)), we have $\frac{1}{b} J = \frac{\rho}{\phi_1 \dots \phi_n} \frac{1}{a_n} I_n$. If $\rho = \phi_1 \dots \phi_n$ then