

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 36 (1990)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE DISTANCE BETWEEN IDEALS IN THE ORDERS OF A REAL QUADRATIC FIELD
Autor: Kaplan, Pierre / Williams, Kenneth S.
Kapitel: 8. GAUSS'S REDUCTION PROCESS
DOI: <https://doi.org/10.5169/seals-57912>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 19.08.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

(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 $p^2 D = b_1^2 + 4aa_1$, 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

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

The representation $\{a', b'\}$ and the ideal I' are the Gauss neighbour of the representation $\{a, b\}$ and of the ideal I respectively, so that

$$\{a, b\} \xrightarrow{G} \{a', b'\}.$$

Proof. As $c' = \frac{(D - b'^2)}{4a'} = a$ (by (2.10)), the q -neighbour representation $\{a', b'\}$ of $\{a, b\}$ is half-reduced if

$$0 < \frac{-b' + \sqrt{D}}{2|a|} < 1,$$

that is, by (2.10), if $0 < \frac{b + \sqrt{D}}{2|a|} - \frac{a}{|a|} q < 1$, giving $q = \frac{a}{|a|} \left[\frac{b + \sqrt{D}}{2|a|} \right]$,

which shows that q and $\{a', b'\}$ are determined by $\{a, b\}$. Let $\{\pm a, b + 2K|a|\} = \{a_1, b_1\}$ be another representation of I giving rise to a half-reduced representation, say $\{a'_1, b'_1\}$. As $b'_1 \equiv -b_1 \equiv -b \equiv b' \pmod{2|a|}$ and $|a_1| = |a|$, we see from the inequalities

$$0 < \frac{\sqrt{D} - b'}{2|a|} < 1 \quad \text{and} \quad 0 < \frac{\sqrt{D} - b'_1}{2|a_1|} < 1$$

that $b'_1 = b'$. Hence, as $|a| = |a_1|$ and $b' = b'_1$, from $D = b'^2 + 4aa' = b'^2_1 + 4a_1a'_1$, we see that $|a'| = |a'_1|$. This shows that $I'_1 = I$, which completes the proof of Lemma 7.

PROPOSITION 11. Let $\{a, b\}$ be a half-reduced representation of a half-reduced ideal I . Let $\{a, b\} \xrightarrow{G} \{a', b'\}$ and set $I' = \left[a', \frac{b' + \sqrt{D}}{2} \right]$. We have

(i) if $b < -\sqrt{D}$ then $b' > b + 2\sqrt{D}$,

(ii) if $b > -\sqrt{D}$ then I' is reduced.

(iii) if I is reduced, then I' is reduced, and moreover if $\{a, b\}$ is the representation of I such that $a > 0$ and $\phi = \frac{b + \sqrt{D}}{2a}$ is reduced, then the Lagrange neighbour and the Gauss neighbour are the same.

Proof. For any representation $\{a, b\}$ of any primitive ideal, we have

$$(8.3) \quad \left| \frac{\sqrt{D} - b}{2c} \right| \left| \frac{\sqrt{D} + b}{2a} \right| = 1.$$

Now take $\{a, b\}$ to be a half-reduced representation of the half-reduced ideal I so that $0 < \frac{-b + \sqrt{D}}{2|c|} < 1$, where $c = (D - b^2)/4a$.

- (i) Suppose that $b < -\sqrt{D}$. Then we have $b^2 - D = 4|a||c|$ so that (8.3) becomes $\left(\frac{\sqrt{D}-b}{2|c|}\right)\left(\frac{-b-\sqrt{D}}{2|a|}\right) = 1$. As $0 < \frac{-b + \sqrt{D}}{2|c|} < 1$, we see that $\frac{-b - \sqrt{D}}{2|a|} > 1$. But, as $\{a', b'\}$ is also half-reduced, we have $\frac{-b' + \sqrt{D}}{2|a|} < 1$, so that $-b' + \sqrt{D} < 2|a| < -b - \sqrt{D}$, proving that $b' > b + 2\sqrt{D}$.
- (ii) Suppose that $b > -\sqrt{D}$. Then, we have $|b| < \sqrt{D}$, and (8.3) can be written

$$\left(\frac{\sqrt{D}-b}{2|c|}\right)\left(\frac{\sqrt{D}+b}{2|a|}\right) = 1.$$

showing that $\frac{\sqrt{D}+b}{2|a|} > 1$. On the other hand, as $\{a', b'\}$ is half-reduced, we have $0 < \frac{\sqrt{D}-b'}{2|a|} < 1$, that is $0 < \frac{\sqrt{D}+b}{2|a|} - \frac{a}{|a|}q < 1$, so that

$$\frac{a}{|a|}q = \left\lceil \frac{\sqrt{D}+b}{2|a|} \right\rceil \geq 1.$$

Hence we obtain

$$\sqrt{D} + b' = \sqrt{D} - b + 2aq = (\sqrt{D} - b) + 2|a|\left(\frac{aq}{|a|}\right) > 2|a|,$$

which, together with the inequalities $0 < \frac{\sqrt{D}-b'}{2|a|} < 1$, shows that ϕ' is

reduced if $a > 0$ and $-\phi'$ is reduced if $a < 0$, proving that I' is reduced.

- (iii) We suppose that I is reduced and choose the representation $\{a, b\}$ of I with $a > 0$ and $\phi = \frac{b + \sqrt{D}}{2a}$ reduced. As ϕ is half-reduced and $b > -\sqrt{D}$ from (ii)

we see that I' is reduced. Moreover, the integer q used to obtain both the Lagrange neighbour and the Gauss neighbour of $\{a, b\}$ is $[\phi]$. This shows that the two neighbours of $\{a, b\}$ are the same and concludes the proof of Proposition 11.

Definition 15. (Gauss's reduction process ([1]: §§ 183-185)) We start with

a primitive ideal I_0 of O_D and a representation $\{a, b\}$ of I_0 , and define the sequence of representations $\{a_n, b_n\}$ of the primitive ideals I_n by

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

We now show that Gauss's reduction process leads to a reduced ideal equivalent to I_0 . In addition we give an upper bound for the number of steps required to obtain a reduced ideal I_n as well as bounds for a quantity ρ in the relation $I_n = \rho I_0$.

PROPOSITION 12. (i) The ideal I_n is reduced for

$$n > \max \left(\left\lfloor \frac{|a_0|}{\sqrt{D}} \right\rfloor + 1, 2 \right).$$

(ii) Let I' be the first reduced ideal obtained by applying Gauss's reduction to I_0 . Then $I = \rho I_0$ with $\frac{1}{|a_0|} \leq \rho < \sqrt{D}$.

Proof. We suppose that $n > \max \left(\left\lfloor \frac{|a_0|}{\sqrt{D}} \right\rfloor + 1, 2 \right)$ so that $n \geq 3$.

If $b_1 > -\sqrt{D}$, by Proposition 11 (ii), I_2 is reduced and so, by Proposition 11 (iii), I_n is reduced.

Suppose on the other hand that $b_1 < -\sqrt{D}$ and that I_n is not reduced. Then, by Proposition 11 (ii), we see that $b_i < -\sqrt{D}$ for $i = 1, 2, \dots, n-1$. Then, by Proposition 11 (i), we have

$$b_{n-1} > b_1 + 2(n-2)\sqrt{D}.$$

Hence we obtain

$$\begin{aligned} b_{n-1} &> -b_0 + 2a_0 \left(\frac{a_0}{|a_0|} \left[\frac{a_0}{|a_0|} \frac{(b_0 + \sqrt{D})}{2a_0} \right] \right) + 2 \left(\left\lfloor \frac{|a_0|}{\sqrt{D}} \right\rfloor - 1 \right) \sqrt{D} \\ &> -b_0 + 2|a_0| \left(\frac{b_0 + \sqrt{D}}{2|a_0|} - 1 \right) + 2 \left(\left\lfloor \frac{|a_0|}{\sqrt{D}} \right\rfloor - 1 \right) \sqrt{D} \\ &= -\sqrt{D}, \end{aligned}$$

which is a contradiction. This completes the proof that I_n is reduced for $n > \max \left(\left\lfloor \frac{|a_0|}{\sqrt{D}} \right\rfloor + 1, 2 \right)$.

(ii) Let I_n be the first reduced ideal obtained from I_0 by Gauss's reduction

process. If $n = 0$ then $\rho = 1$, so that $\frac{1}{|a_0|} \leq \rho < \sqrt{D}$. If $n \geq 1$ we have $I_n = \rho I_0$ with (by (2.12))

$$\rho = \left| \frac{a_1}{a_0} \phi_1 \dots \frac{a_n}{a_{n-1}} \phi_n \right| = \left| \frac{a_n}{a_0} \right| \left| \frac{b_1 + \sqrt{D}}{2a_1} \right| \dots \left| \frac{b_n + \sqrt{D}}{2a_n} \right|.$$

As the representations $\{a_k, b_k\}$ are half-reduced for $k \geq 1$, we see, by (8.3), that $\left| \frac{b_k + \sqrt{D}}{2a_k} \right| > 1$ ($k \geq 1$) so that $\rho > \left| \frac{a_n}{a_0} \right| \geq \frac{1}{|a_0|}$. On the other hand we have

$$\rho = \left| \frac{b_1 + \sqrt{D}}{2a_0} \right| \dots \left| \frac{b_n + \sqrt{D}}{2a_{n-1}} \right|.$$

As $\{a_k, b_k\}$ is a half-reduced representation for $k = 1, 2, \dots, n$, we have $0 < \sqrt{D} - b_k < 2|a_{k-1}|$. Furthermore, for $k = 1, 2, \dots, n-1$, we have $\sqrt{D} + b_k < 2|a_{k-1}|$, as otherwise $0 < \sqrt{D} - b_k < 2|a_{k-1}| < \sqrt{D} + b_k$, which is equivalent to $0 < \sqrt{D} - b_k < 2|a_k| < \sqrt{D} + b_k$ so that by (4.2) the primitive ideal I_k would be reduced. Therefore, for $k = 1, 2, \dots, n-1$, we have

$$|\sqrt{D} + b_k| \leq \sqrt{D} + |b_k| = \begin{cases} \sqrt{D} + b_k < 2|a_{k-1}|, & \text{if } b_k \geq 0, \\ \sqrt{D} - b_k < 2|a_{k-1}|, & \text{if } b_k < 0, \end{cases}$$

so that, as $\{a_n, b_n\}$ is reduced,

$$\rho < \frac{b_n + \sqrt{D}}{2|a_{n-1}|} < \sqrt{D}$$

which completes the proof of Proposition 12.

We remark that Proposition 7 and 12 suggest that Lagrange's reduction process may lead to a reduced ideal much faster than Gauss's reduction process, as the number M_0 of Lemma 6 is much smaller than $\max \left(\frac{|a_0|}{\sqrt{D}} + 1, 2 \right)$.

Example 5. We apply both Lagrange reduction and Gauss reduction to the representation $\{3655, 7068\}$ of the primitive ideal $[3655, 3534 + \sqrt{21}]$ of O_{84} . We obtain

$$\{3655, 7068\} \xrightarrow{L} \{-3417, -7068\} \xrightarrow{L} \{4, 234\} \xrightarrow{L} \{3, 6\} \quad (3 \text{ steps})$$

and

$$\begin{aligned} \{3655, 7068\} \xrightarrow{G} \{-3417, -7068\} \xrightarrow{G} \{3187, -6600\} \xrightarrow{G} \{-2965, -6148\} \xrightarrow{G} \dots \\ \xrightarrow{G} \{-1, -12\} \xrightarrow{G} \{-5, 8\} \quad (30 \text{ steps}) . \end{aligned}$$

We remark that M_0 is approximately 8.72 and $\frac{|a_0|}{\sqrt{D}} + 1$ is approximately 399.8.

REFERENCES

- [1] GAUSS, C.F. *Disquisitiones Arithmeticae*, in *Untersuchungen über höhere Arithmetik*, reprinted Chelsea Publishing Co., New York (1965).
- [2] LAGRANGE, J.-L. Solution d'un problème d'arithmétique (1766), *Œuvres de Lagrange*, Vol. 1, pp. 671-731. (Gauthier-Villars (1867)).
- [3] ——— Sur la solution des problèmes indéterminés du second degré (1769), *Œuvres de Lagrange*, Vol. 2, pp. 377-535. (Gauthier-Villars (1868)).
- [4] LENSTRA, H.W., Jr. On the calculation of regulators and class numbers of quadratic fields. *London Math. Soc. Lecture Note Ser.* 56 (1982), 123-150.
- [5] SCHOLZ, A. and B. SCHOENEBOG. *Einführung in die Zahlentheorie*. Walter de Gruyter. Berlin and New York (1973).
- [6] SCHOOF, R.G. Quadratic fields and factorization. *Computational Methods in Number Theory* (H. W. Lenstra Jr. and R. Tijdeman, eds). Math. Centrum Tracts. Number 155, Part II, Amsterdam, 1983, 235-286.
- [7] SHANKS, D. The infrastructure of a real quadratic field and its applications. *Proc. 1972. Number Theory Conference*, Boulder, Colorado, 1972, 217-224.
- [8] SMITH, H.J.S. Note on the theory of the Pellian equation, and of binary quadratic forms of a positive determinant. *Proc. Lond. Math. Soc.* 7 (1876), 199-208.
- [9] STEPHENS, A.J. and H.C. WILLIAMS. Some computational aspects on a problem of Eisenstein. Preprint.