L'Enseignement Mathématique, t. 36 (1990), p. 321-358

THE DISTANCE BETWEEN IDEALS IN THE ORDERS OF A REAL QUADRATIC FIELD

par Pierre KAPLAN and Kenneth S. WILLIAMS [1])

1. INTRODUCTION

The notion of the distance between two equivalent, reduced, primitive ideals of an order in the ring of integers of a real quadratic field was first introduced by Shanks [7] in 1972 in order to develop a more efficient algorithm for computing the fundamental unit of the field, although this notion was already implicit in the work of earlier authors including Lagrange [2]. Shanks used the language of binary quadratic forms to describe the concept of distance. This concept, still described in terms of binary quadratic forms, was made more precise and exploited by Lenstra [4] (1982) and Schoof [6] (1983) in their work on quadratic fields and factorization. In 1986 Williams and Wunderlich [12] gave a treatment of distance in terms of ideals, and used it to develop a simple algorithm for use in the continued fraction factoring algorithm. Parts of their theory have also been used in numerical studies of Eisenstein's problem [9] [11].

The aim of this papers is two-fold. We first give a complete treatment of the basic theory of the distance between equivalent, reduced, primitive ideals in the hope of making this attractive and useful theory better known and more readily available for further research. Our treatment is based mainly on the presentation of Williams and Wunderlich [12], but, in our view, is simpler in some aspects. Our second objective is to define a homomorphism between the ideal class groups of different orders and to apply this theory to compare distances between corresponding ideals in the two orders. The presentation is self-contained in that factorization of ideals in an order of a quadratic field is not needed, nor do we use the theory of the units of a real quadratic field. Indeed the theory of units is a consequence of our presentation, see Corollary 5. We give known results as Propositions and new results as Theorems.

[1]) Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

Throughout this paper, if A is a unitary commutative ring, and $\alpha_1, \alpha_2, \ldots, \alpha_m$ are elements of A, the Z-module generated by $\alpha_1, \alpha_2, \ldots, \alpha_m$ is denoted by $[\alpha_1, \alpha_2, \ldots, \alpha_m]$ and the A-module (ideal) generated by $\alpha_1, \alpha_2, \ldots, \alpha_m$ by $(\alpha_1, \alpha_2, \ldots, \alpha_m)$. The product of the ideals $(\alpha_1, \ldots, \alpha_m)$ and $(\alpha'_1, \ldots, \alpha'_n)$ is the ideal $(\alpha_1\alpha'_1, \ldots, \alpha_i\alpha'_j, \ldots, \alpha_m\alpha'_r)$. If I is an ideal, we often write the product ideal $(\alpha)I$ as αI.

2. Basic definitions

Let K be a quadratic field of discriminant D_0. As D_0 is a discriminant we have $D_0 \equiv 0 \pmod 4$ or $D_0 \equiv 1 \pmod 4$. In §2 and §3 K may be real ($D_0 > 0$) or imaginary ($D_0 < 0$) but in the remaining sections K will be assumed to be real. An element α of K can be written $\alpha = x + y\sqrt{D_0}$, where x and y are rational numbers. The conjugate of α is the element $\bar{\alpha} = x - y\sqrt{D_0}$ of K. The norm of α is the rational number $N(\alpha) = \alpha\bar{\alpha} = x^2 - D_0y^2$. We define the integer ω_0 of K by

$$\omega_0 = \begin{cases} \dfrac{\sqrt{D_0}}{2}, & \text{if } D_0 \equiv 0 \pmod 4, \\ \dfrac{1}{2}(1 + \sqrt{D_0}), & \text{if } D_0 \equiv 1 \pmod 4. \end{cases} \tag{2.1}$$

The ring of integers of K is $O_{D_0} = [1, \omega_0]$. For a positive integer f, we set

$$D = D_0f^2, \omega = \begin{cases} \dfrac{\sqrt{D}}{2}, & \text{if } D \equiv 0 \pmod 4 \\ \dfrac{1}{2}(1 + \sqrt{D}), & \text{if } D \equiv 1 \pmod 4. \end{cases} \tag{2.2}$$

and

$$O_D = [1, \omega] = [1, f\omega_0]. \tag{2.3}$$

It is easy to check that O_D is the subring of index f in O_{D_0}, called the order of discriminant D. We note that

$$\omega^2 = \begin{cases} \dfrac{D}{4}, & \text{if } D \equiv 0 \pmod 4, \\ \omega + \dfrac{(D-1)}{4}, & \text{if } D \equiv 1 \pmod 4. \end{cases} \tag{2.4}$$

The multiplicative group of K is denoted by K^*.

Next we describe the ideals of the order O_D. Throughout this paper all ideals will be nonzero.

PROPOSITION 1. ([10]: Theorem 5.6, [12]: Theorem 3.2) *(i) The (nonzero) ideals of the order O_D are the Z-modules*

$$I = d\left[a, \frac{b + \sqrt{D}}{2}\right],$$

where

(2.5)
$$c = \frac{D - b^2}{4a}$$

is an integer.

(ii) Two ideals $I = d\left[a, \frac{b + \sqrt{D}}{2}\right]$ *and* $I' = d'\left[a', \frac{b' + \sqrt{D}}{2}\right]$ *are equal if, and only if,* $|d| = |d'|, |a| = |a'|, b \equiv b' \pmod{2a}$.

Proof. (i) Let I be a (nonzero) ideal of O_D. The set $I \cap Z$ is a (nonzero) ideal (a_0) of Z. The set $\{y \in Z : x + y\omega \in I \text{ for some } x \in Z\}$ is also an ideal (d) of Z, and, as $a_0\omega \in I$, we see that $d \mid a_0$, say $a_0 = da$. Let $\alpha_0 \in I$ be such that $\alpha_0 = b_0 + d\omega$. Appealing to (2.4), we see that

$$\omega\alpha_0 = \omega(b_0 + d\omega) = \begin{cases} \dfrac{dD}{4} + b_0\omega, & \text{if } D \equiv 0 \pmod 4, \\ d\left(\dfrac{D-1}{4}\right) + (d + b_0)\omega, & \text{if } D \equiv 1 \pmod 4, \end{cases}$$

so that $d \mid b_0$, say $b_0 = db_1$. Thus we have $\alpha_0 = d(b_1 + \omega)$, which shows that $I \supseteq d[a, b_1 + \omega]$. Now let $\beta = x + dy\omega \in I$. As $\beta - \alpha_0 y = x - b_0 y \in I \cap Z$, there exists $k \in Z$ such that $\beta = ka_0 + \alpha_0 y$, which shows that $I \subseteq [a_0, \alpha_0] = d[a, b_1 + \omega]$. Hence we have $I = d[a, b_1 + \omega]$. As $dN(b_1 + \omega) = d(b_1 + \omega)(b_1 + \bar{\omega}) \in I \cap Z = (da)$, we see that a divides $N(b_1 + \omega)$.

Now let $I = d[a, b_1 + \omega]$, where $c = -N(b_1 + \omega)/a$ is an integer. We show that I is an ideal of O_D. It suffices to prove that ωa and $\omega(b_1 + \omega)$ belong to $[a, b_1 + \omega]$. This follows from

$$\omega a = (-b_1)a + a(b_1 + \omega)$$

and

$$\omega(b_1 + \omega) = -(b_1 + \bar{\omega})(b_1 + \omega) + (b_1 + \omega + \bar{\omega})(b_1 + \omega)$$
$$= ca + (b_1 + \omega + \bar{\omega})(b_1 + \omega) .$$

We have thus shown that the ideals of O_D are the Z-modules $d[a, b_1 + \omega]$, where $c = -N(b_1 + \omega)/a$ is an integer. Let b be the integer given by

$$b = \begin{cases} 2b_1 , & \text{if } D \equiv 0 \pmod 3 , \\ 2b_1 + 1 , & \text{if } D \equiv 1 \pmod 4 , \end{cases}$$

so that

$$b_1 + \omega = \frac{b + \sqrt{D}}{2} , \quad \frac{N(b_1 + \omega)}{a} = \frac{b^2 - D}{4a} = -c \in Z .$$

This completes the proof of Proposition 1 (i).

(ii) If $d\left[a, \frac{b + \sqrt{D}}{2}\right] = d'\left[a', \frac{b' + \sqrt{D}}{2}\right]$ we easily see that $d|d', d'|d$, $ad|a'd'$ and $a'd'|ad$, from which Proposition 1 (ii) follows.

Example 1. (i) By Proposition 1 (i) the Z-module $A = \left[3, \frac{1 + \sqrt{45}}{2}\right]$ of O_{45} is not an ideal of O_{45} as $\frac{45 - 1}{12}$ is not an integer. Indeed A is not closed under multiplication by elements of O_{45} as $\frac{1 + \sqrt{45}}{2} \in A$ but

$$\left(\frac{1 - \sqrt{45}}{2}\right)\left(\frac{1 + \sqrt{45}}{2}\right) = -11 \notin A .$$

(ii) By Proposition 1 (i) the Z-module $B = \left[11, \frac{1 + \sqrt{45}}{2}\right]$ of O_{45} is an ideal of O_{45} as $\frac{45 - 1}{44}$ is an integer.

If $I = d\left[a, \frac{b + \sqrt{D}}{2}\right]$ is an ideal of O_D, by Proposition 1 (ii), we see that $GCD(a, b, c)$ does not depend upon the choice of a, b and d. This enables us to define the concept of a primitive ideal of O_D.

Definition 1. (Primitive ideal) The ideal $I = d\left[a, \frac{b+\sqrt{D}}{2}\right]$ of O_D is called *primitive* if, and only if,

$$d = GCD(a, b, c) = 1 ,$$

where c is defined by (2.5).

Our next result gives some basic properties of primitive ideals.

PROPOSITION 2. ([10]: Theorem 5.9) *(i) If* $I = \left[a, \frac{b+\sqrt{D}}{2}\right]$ *is a primitive ideal of* O_D *then*

$$I\bar{I} = (a) ,$$

where $\bar{I} = \left[a, \frac{b-\sqrt{D}}{2}\right]$ *is the conjugate ideal of* I.

(ii) If I *is a primitive ideal of* O_D *and* $\alpha \in K^*$ *is such that* $I = \alpha I$, *then* α *is a unit of* O_D.

(iii) If $I = \left[a, \frac{b+\sqrt{D}}{2}\right]$ *and* $J = \left[A, \frac{B+\sqrt{D}}{2}\right]$ *are primitive ideals of* O_D *such that* $\frac{1}{a}I = \frac{1}{A}J$ *then* $I = J$ *and* $|a| = |A|$.

Proof. (i) We have

$$I\bar{I} = a\left(a, \frac{b+\sqrt{D}}{2}, \frac{b-\sqrt{D}}{2}, c\right) .$$

The ideal $\left(a, \frac{b+\sqrt{D}}{2}, \frac{b+\sqrt{D}}{2}, c\right)$ contains the ideal $(a, b, c) = (1)$, so that $I\bar{I} = (a)$.

(ii) As $\alpha \in K^*$, there exist $\beta \in O_D^*$ and $\gamma \in O_D^*$ such that $\alpha = \beta/\gamma$. Then, we have $\gamma I = \gamma\alpha I = \beta I$, and so, by (i), we obtain $(\gamma)(a) = \gamma I\bar{I} = \beta I\bar{I} = (\beta)(a)$, giving $(\beta) = (\gamma)$, so that $\alpha = \beta/\gamma$ is a unit of O_D.

(iii) We have $AI = aJ$ so that, by (ii), $a/A = \pm 1$ and $I = J$.

Next we define the notion of equivalent ideals.

Definition 2. (Equivalent ideals) Two ideals I and I' of O_D are said to be *equivalent* if there exists $\rho \in K^*$ such that $I' = \rho I$.

Example 2. The ideals

$$I = \left[7, \frac{12 + \sqrt{200}}{2}\right] = [7, 6 + \sqrt{50}] \quad \text{and} \quad J = \left[2, \frac{\sqrt{200}}{2}\right] = [2, \sqrt{50}]$$

of O_{200} are equivalent as

$$\begin{aligned} I &= [7, -8 + \sqrt{50}] \\ &= \left(\frac{-8 + \sqrt{50}}{2}\right)[-8 - \sqrt{50}, 2] \\ &= \left(\frac{-16 + \sqrt{200}}{4}\right)[2, \sqrt{50}] \\ &= \alpha J , \end{aligned}$$

where $$\alpha = \frac{-16 + \sqrt{200}}{4} \in K^* .$$

It is clear that the notion of equivalence given in Definition 2 is an equivalence relation. The equivalence classes are called ideal classes. The ideal class of the ideal I is denoted by $C(I)$. If $I' \in C(I)$ and $J' \in C(J)$ then $I'J' \in C(IJ)$, and we can define multiplication of ideal classes by $C(I)\,C(J) = C(IJ)$.

Definition 3. (Primitive class) An ideal class of O_D containing a primitive ideal is called a *primitive* class.

It follows from Proposition 2(i) that the primitive classes are invertible, and so form a group C_D with respect to multiplication.

Definition 4. (Ideal class group) The group C_D of primitive classes of the order O_D is called the *ideal class group* of O_D.

The unit class of the ideal class group is called the principal class and consists of all the principal primitive ideals of O_D. In fact C_D is a finite group.

Next we give a necessary and sufficient condition for two ideals I and I' of O_D to be equivalent, and, when I and I' are equivalent, a means of calculating ρ in the relationship $I' = \rho I$. It suffices to consider ideals of the form $\left[a, \frac{b + \sqrt{D}}{2}\right]$ that is with $d = 1$.

PROPOSITION 3. ([10]: Theorem 5.27) *Let*

$$I = \left[a, \frac{b+\sqrt{D}}{2}\right] \quad \text{and} \quad J = \left[A, \frac{B+\sqrt{D}}{2}\right]$$

be two ideals of O_D. *Set*

$$\phi = \frac{b+\sqrt{D}}{2a}, \quad \psi = \frac{B+\sqrt{D}}{2A}.$$

(i) The ideals I *and* J *are equivalent if, and only if, there exists a* 2×2 *integral matrix* $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ *of determinant* $\varepsilon = ps - qr = \pm 1$ *such that* $\psi = \dfrac{p\phi + q}{r\phi + s}$.

(ii) If I *and* J *are equivalent the numbers* $\rho \in K^*$ *such that* $J = \rho I$ *are given by*

$$\rho = \frac{A}{a} \frac{1}{r\phi + s} = \varepsilon(r\bar{\phi} + s) \tag{2.6}$$

and satisfy

$$N(\rho) = \varepsilon \frac{A}{a}. \tag{2.7}$$

Proof. We have $J = \rho I$, that is $A[1, \psi] = \rho a[1, \phi]$, if, and only if, there exists an integral matrix $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ of determinant $\varepsilon = \pm 1$ such that

$$\begin{cases} A = r\rho a\varphi + s\rho a, \\ A\psi = p\rho a\phi + q\rho a. \end{cases} \tag{2.8}$$

The equations (2.8) are equivalent to

$$\psi = \frac{p\phi + q}{r\phi + s}, \quad \rho = \frac{A}{a} \frac{1}{r\phi + s}.$$

This establishes (i) and the first equality of (2.6).

Taking conjugates in (2.8), we have

$$\begin{cases} A = r\bar{\rho}a\bar{\phi} + s\bar{\rho}a, \\ A\bar{\psi} = p\bar{\rho}a\bar{\phi} + q\bar{\rho}a, \end{cases} \tag{2.9}$$

so that (2.8) and (2.9) are equivalent to the matrix equality

$$\begin{bmatrix} A\psi & A \\ A\bar{\psi} & A \end{bmatrix} = \begin{bmatrix} a\phi\rho & a\rho \\ a\bar{\phi}\bar{\rho} & a\bar{\rho} \end{bmatrix} \begin{bmatrix} p & r \\ q & s \end{bmatrix}.$$

Taking determinants we obtain

$$A^2(\psi - \bar{\psi}) = \varepsilon\rho\bar{\rho}a^2(\phi - \bar{\phi}),$$

which gives, as $\psi - \bar{\psi} = \dfrac{\sqrt{D}}{A}$ and $\phi - \bar{\phi} = \dfrac{\sqrt{D}}{a}$, $\rho\bar{\rho} = \varepsilon\dfrac{A}{a}$, proving (2.7). Then the first equality in (2.6) shows that $\bar{\rho} = \varepsilon(r\phi + s)$, establishing the second equality in (2.6).

COROLLARY 1. *Let* $I = \left[a, \dfrac{b + \sqrt{D}}{2}\right]$ *be a primitive ideal of* O_D, *and set* $\phi = \dfrac{b + \sqrt{D}}{2a}$. *For* $q \in Z$ *define* $\phi', b' a'$ *and* I' *by*

(2.10)

$$\phi = q + \frac{1}{\phi'}, \quad b' = -b + 2aq, \quad a' = \frac{D - b'^2}{4a}, \quad I' = \left[a', \frac{b' + \sqrt{D}}{2}\right].$$

Then

(2.11)

$$a' = \frac{D - b^2}{4a} + bq - aq^2 \in Z, \quad \phi' = \frac{b' + \sqrt{D}}{2a'},$$

and I' *is a primitive ideal of* O_D *such that*

(2.12)

$$I' = \frac{a'}{a}\phi' I = \frac{-1}{\phi'} I.$$

Proof. The formulas in (2.11) for a' and ϕ' are easily proved by a straightforward calculation, and Proposition 3 with $p = 0$, $q = 1$, $r = 1$, $s = -q$ gives

$$I' = \frac{a'}{a}\frac{1}{\phi - q} I = -(\bar{\phi} - q) I,$$

which is equivalent to (2.12) as $\phi' = \dfrac{1}{\phi - q}$.

By Proposition 1 a primitive ideal I of O_D can be written in the form $I = a[1, \phi]$ $(\phi = (b + \sqrt{D})/2a)$, where a is an integer uniquely determined up to sign by I and $a\phi$ is determined modulo a by I.

Definition 5. (Representation of a primitive ideal). Let I be a primitive ideal of O_D. A pair $\{a, b\}$ such that $I = a[1, \phi]$, where $\phi = (b + \sqrt{D})/2a$, is called a *representation* of I.

Definition 6. (q-neighbour). When the representation $\{a, b\}$ of the ideal I and the representation $\{a', b'\}$ of the ideal I' are related as in (2.10), we say that $\{a', b'\}$ is *q-neighbour* to $\{a, b\}$.

Definition 7. (Lagrange neighbour). When $D > 0$ and $\{a', b'\}$ is q-neighbour to $\{a, b\}$ with $q = [\phi]$, we say that $\{a', b'\}$ is the *Lagrange neighbour* of $\{a, b\}$ and write $\{a, b\} \xrightarrow{L} \{a', b'\}$.

Definition 8. (Gauss neighbour). When $D > 0$ and $\{a', b'\}$ is q-neighbour to $\{a, b\}$ with $q = \dfrac{a}{|a|}\left[\dfrac{a}{|a|}\phi\right]$, we say that $\{a', b'\}$ is the *Gauss neighbour* of $\{a, b\}$ and write $\{a, b\} \xrightarrow{G} \{a', b'\}$.

Lagrange's reduction process using Lagrange neighbours is described in § 5 and Gauss's reduction process using Gauss neighbours in § 8.

COROLLARY 2. *The ideals* $I = \left[a, \dfrac{b + \sqrt{D}}{2}\right]$ *and* $J = \left[c, \dfrac{-b + \sqrt{D}}{2}\right]$, *where* c *is given by (2.5), are equivalent and satisfy*

$$J = \frac{(-b + \sqrt{D})}{2a} I .$$

Proof. We have $\psi = \dfrac{1}{\bar{\phi}}$, where $\phi = \dfrac{b + \sqrt{D}}{2a}$ and $\psi = \dfrac{-b + \sqrt{D}}{2c}$, so that, by Proposition 3(ii), we have $J = \rho I$ with $\rho = (-1)\bar{\phi} = \dfrac{-b + \sqrt{D}}{2a}$.

COROLLARY 3. *If* $I = \left[a, \dfrac{b + \sqrt{D}}{2}\right]$ *and* $J = \left[A, \dfrac{B + \sqrt{D}}{2}\right]$ *are two equivalent ideals of* O_D *with* I *primitive then* J *is also primitive.*

Proof. Set $\phi = \dfrac{b + \sqrt{D}}{2a}$ and $\psi = \dfrac{B + \sqrt{D}}{2A}$. As I and J are equivalent,

by Proposition 3, we have $J = \rho I$, where $\psi = \dfrac{p\phi + q}{r\phi + s}$, $\rho = \dfrac{A}{a}\dfrac{1}{r\phi + s}$ $= \varepsilon(r\bar{\phi} + s)$ and $\varepsilon = ps - qr = \pm 1$. Clearly we have

$$\begin{aligned} A &= \varepsilon a(r\phi + s)\,(r\bar{\phi} + s) = \varepsilon(as^2 + bsr - cr^2)\,, \\ B &= A(\psi + \bar{\psi}) = \varepsilon a(\psi + \bar{\psi})\,(r\phi + s)\,(r\bar{\phi} + s) \\ &= \varepsilon a\big((p\phi + q)\,(r\bar{\phi} + s) + (p\bar{\phi} + q)\,(r\phi + s)\big) \\ &= \varepsilon(2asq + b(sp + rq) - 2cpr), \\ -C &= A\psi\bar{\psi} = \varepsilon a\psi\bar{\psi}(r\phi + s)\,(r\bar{\phi} + s) = \varepsilon a(p\phi + q)\,(p\bar{\phi} + q) \\ &= \varepsilon(aq^2 + bqp - cp^2)\,. \end{aligned}$$

Thus A, B, C are integral linear combinations of a, b, c. Similarly, a, b, c are integral linear combinations of A, B, C. Hence $GCD(A, B, C) = GCD(a, b, c) = 1$ so that J is primitive.

3. The homomorphism θ

Let O_D and $O_{D'}$ be two orders of O_{D_0} with $O_{D'} \subset O_D$. Then we have $D' = Df^2$ for some positive integer f. This notation will be used throughout the rest of the paper. Our aim is to define a surjective homomorphism θ from the ideal class group $C_{D'}$ onto the ideal class group C_D. After proving three lemmas, we will prove the following theorem.

THEOREM 1. *(i) Every class C of $C_{D'}$ contains a primitive ideal I of the form $I = \left[a, \dfrac{fb + \sqrt{D'}}{2}\right]$, where $GCD(a, f) = 1$, such that the ideal $J = \left[a, \dfrac{b + \sqrt{D}}{2}\right]$ is a primitive ideal of O_D.*

(ii) If $I = \left[a, \dfrac{fb + \sqrt{D'}}{2}\right]$ $(GCD(a, f) = 1)$ and $I' = \left[a', \dfrac{fb' + \sqrt{D'}}{2}\right]$ $(GCD(a', f) = 1)$ are two primitive ideals in the same class C of $C_{D'}$ with $I' = \rho I (\rho \in K^*)$, then the ideals

$$J = \left[a, \frac{b + \sqrt{D}}{2}\right] \quad \text{and} \quad J' = \left[a', \frac{b' + \sqrt{D}}{2}\right]$$

of O_D satisfy $J' = \rho J$ and are in the same class $\theta(C)$ of C_D.

(iii) The mapping $C \to \theta(C)$ *is a homomorphism of* $C_{D'}$ *to on* C_D.

Part (ii) of Theorem 1 will be the main tool in relating distances between ideals of different orders of the same real quadratic field.

LEMMA 1. *A primitive ideal* $I = \left[a, \frac{b+\sqrt{D}}{2}\right]$ *contains a number* $\alpha = xa + y\left(\frac{b+\sqrt{D}}{2}\right)$, *where* x *and* y *are coprime integers, such that the integer* $N(\alpha)/a$ *is prime to a given nonzero integer* m.

Proof. We begin by noting that $\frac{1}{a} N\left(xa + y\left(\frac{b+\sqrt{D}}{2}\right)\right) = ax^2 + bxy - cy^2$ in view of (2.5). If $|m| = 1$ we take $x = 1$, $y = 0$, $\alpha = xa + y\left(\frac{b+\sqrt{D}}{2}\right) = a$, so that $GCD(N(\alpha)/a, m) = GCD(a, 1) = 1$, as required. Hence we may suppose that $|m| > 1$. Let $p_i (i = 1, 2, \ldots, n)$ be the distinct prime factors of m. For $i = 1, 2, \ldots, n$ we set

$$(x_i, y_i) = \begin{cases} (1,0), & \text{if } p_i \nmid a, \\ (0,1), & \text{if } p_i \mid a, \ p_i \nmid c, \\ (1,1), & \text{if } p_i \mid a, \ p_i \mid c, \end{cases}$$

so that $p_i \nmid ax_i^2 + bx_iy_i - cy_i^2$. Let x' and y' be integers such that $x' \equiv x_i \pmod{p_i}$ and $y' \equiv y_i \pmod{p_i}$ for $i = 1, 2, \ldots, n$, so that $GCD(ax'^2 + bx'y' - cy'^2, m) = 1$. The required number α is given by $\alpha = xa + y\left(\frac{b+\sqrt{D}}{2}\right)$, where $x = \frac{x'}{GCD(x', y')}$, $y = \frac{y'}{GCD(x', y')}$.

LEMMA 2. *Let* m *be a given nonzero integer. Every class* C *of* C_D *contains a primitive ideal* $\left[a, \frac{b+\sqrt{D}}{2}\right]$ *with* $GCD(a, m) = 1$.

Proof. Let $\left[a', \frac{b'+\sqrt{D}}{2}\right]$ be a primitive ideal of the class C. By Lemma 1 there exist coprime integers x and y such that

$$\text{GCD}(a'x^2 + b'xy - c'y^2, m) = 1 . \tag{3.1}$$

Set $a = a'x^2 + b'xy - c'y^2$ and let r and s be integers such that $xs - yr = 1$. Next set

$$(3.2) \qquad \rho = x + \left(\frac{b' - \sqrt{D}}{2a'}\right) y,\ b = 2a'xr + b'(xs + yr) - 2c'ys\ ,$$

so that

$$a = \rho\left(xa' + y\left(\frac{b' + \sqrt{D}}{2}\right)\right)$$

and

$$\frac{b + \sqrt{D}}{2} = \rho\left(ra' + s\left(\frac{b' + \sqrt{D}}{2}\right)\right)\ .$$

Then we have

$$\left[a, \frac{b + \sqrt{D}}{2}\right] = \rho\left[xa' + y\left(\frac{b' + \sqrt{D}}{2}\right),\ ra' + s\left(\frac{b' + \sqrt{D}}{2}\right)\right]$$

$$= \rho\left[a', \frac{b' + \sqrt{D}}{2}\right]$$

so that $\left[a, \frac{b + \sqrt{D}}{2}\right]$ is an ideal equivalent to the primitive ideal $\left[a', \frac{b' + \sqrt{D}}{2}\right]$. Hence, by Corollary 3, $\left[a, \frac{b + \sqrt{D}}{2}\right]$ is primitive.

LEMMA 3. *Let C and C' be two classes of C_D. Then there exist primitive ideals $I = \left[a, \frac{B + \sqrt{D}}{2}\right] \in C$ and $I' = \left[a', \frac{B + \sqrt{D}}{2}\right] \in C'$ with $GCD(a, a') = 1$. Moreover the ideal II' is primitive and $II' = \left[aa', \frac{B + \sqrt{D}}{2}\right]$.*

Proof. By Lemma 2 there exist primitive ideals $I = \left[a, \frac{b + \sqrt{D}}{2}\right] \in C$ and $I' = \left[a', \frac{b' + \sqrt{D}}{2}\right] \in C'$ with $GCD(a, a') = 1$. As $b \equiv D \equiv b' \pmod 2$ and $GCD(a, a') = 1$ there are integers k and k' such that $k'a' - ka = \frac{b - b'}{2}$. Set $B = b + 2ka = b' + 2k'a'$ so that

$$I = \left[a, \frac{B + \sqrt{D}}{2}\right] \quad \text{and} \quad I' = \left[a', \frac{B + \sqrt{D}}{2}\right]\ .$$

Now $D - B^2$ is divisible by both $4a$ and $4a'$, and so, as $GCD(a, a') = 1$, $D - B^2$ is a multiple of $4aa'$, so that $c'' = \dfrac{D - B^2}{4aa'} \in Z$. Hence $\left[aa', \dfrac{B + \lfloor \sqrt{D} \rfloor}{2}\right]$ is an ideal of O_D and we have

$$\begin{aligned} II' &= \left(aa', a\left(\frac{B + \lfloor \sqrt{D} \rfloor}{2}\right), a'\left(\frac{B + \lfloor \sqrt{D} \rfloor}{2}\right), \left(\frac{B + \lfloor \sqrt{D} \rfloor}{2}\right)^2\right) \\ &= \left(aa', \frac{B + \lfloor \sqrt{D} \rfloor}{2}\right) \\ &= \left[aa', \frac{B + \lfloor \sqrt{D} \rfloor}{2}\right]. \end{aligned}$$

Finally, any prime divisor of aa', B, c'' must divide $GCD(a, B, a'c'') = 1$ or $GCD(a', B, ac'') = 1$, as $GCD(a, a') = 1$, which is impossible. Hence the ideal II' is primitive.

We are now ready to prove Theorem 1.

Proof of Theorem 1. (i) By Lemma 2 the class C contains a primitive ideal $I = \left[a, \dfrac{b' + \lfloor \sqrt{D'} \rfloor}{2}\right]$ with $GCD(a, f) = 1$. Let k be an integer such that

$$\begin{cases} 2ak \equiv -b' \pmod{f}, & \text{if} \quad f \equiv 1 \pmod 2, \\ ak \equiv -\dfrac{b'}{2} + D\dfrac{f}{2} \pmod{f}, & \text{if} \quad f \equiv 0 \pmod 2, \end{cases}$$

and set $b = (b' + 2ak)/f$, so that $I = \left[a, \dfrac{fb + \lfloor \sqrt{D'} \rfloor}{2}\right]$. As I is an ideal of $O_{D'}$, $(D' - f^2b^2)/4a$ is an integer, and so, as $GCD(a, f) = 1$, $c = (D - b^2)/4a$ is also an integer, showing that $J = \left[a, \dfrac{b + \lfloor \sqrt{D} \rfloor}{2}\right]$ is an ideal of O_D. Further, as I is primitive, we have $GCD(a, bf, cf^2) = 1$, and so $GCD(a, b, c) = 1$, showing that J is primitive.

(ii) If $I' = \rho I$, by Proposition 3, there exist integers p, q, r, s with $ps - qr = \pm 1$ such that

(3.3)
$$\frac{fb' + \lfloor \sqrt{D'} \rfloor}{2a'} = \frac{p\left(\dfrac{fb + \lfloor \sqrt{D'} \rfloor}{2a}\right) + q}{r\left(\dfrac{fb + \lfloor \sqrt{D'} \rfloor}{2a}\right) + s}, \qquad \rho = \pm\left(r\left(\frac{fb - \lfloor \sqrt{D'} \rfloor}{2a}\right) + s\right).$$

Rearranging the first equation in (3.3), we obtain the following equality among elements of O_D

$$f\left(\frac{b'+\sqrt{D}}{2}\right)\left(rf\left(\frac{b+\sqrt{D}}{2}\right)+sa\right)=a'\left(pf\left(\frac{b+\sqrt{D}}{2}\right)+qa\right),$$

from which we deduce that $f \mid qaa'$. As $GCD(aa', f) = 1$ there exists an integer q' such that $q = q'f$, so (3.3) can be rewritten as

$$\frac{b'+\sqrt{D}}{2a'}=\frac{p\left(\frac{b+\sqrt{D}}{2a}\right)+q'}{rf\left(\frac{b+\sqrt{D}}{2a}\right)+s}, \qquad \rho=\pm\left(rf\left(\frac{b-\sqrt{D}}{2a}\right)+s\right).$$

which, by Proposition 3, shows that $J' = \rho J$.

(iii) Let $C \in C_{D'}$ and $C' \in C_{D'}$. By Lemma 2 and (i), we can choose an ideal $I = \left[a, f\left(\frac{b+\sqrt{D}}{2}\right)\right]$ in C with $GCD(a, f) = 1$ and then an ideal $I' = \left[a', f\left(\frac{b'+\sqrt{D}}{2}\right)\right]$ in C' with $GCD(a', af) = 1$. By (i) $\left[a, \frac{b+\sqrt{D}}{2}\right]$ and $\left[a', \frac{b'+\sqrt{D}}{2}\right]$ are ideals of O_D and so we have $b \equiv b' \pmod 2$. We choose integers K' and K such that $K'a' - Ka = \frac{b-b'}{2}$, and set $B = b + 2Ka = b' + 2K'a'$, so that $I = \left[a, f\left(\frac{B+\sqrt{D}}{2}\right)\right]$ and $I' = \left[a, f\left(\frac{B+\sqrt{D}}{2}\right)\right]$. By Lemma 3 we see that $II' = \left[aa', f\left(\frac{B+\sqrt{D}}{2}\right)\right]$ is a primitive ideal of the class CC'. But the primitive ideals $J = \left[a, \frac{B+\sqrt{D}}{2}\right]$, $J' = \left[a', \frac{B+\sqrt{D}}{2}\right]$, $J'' = \left[aa', \frac{B+\sqrt{D}}{2}\right]$ belong respectively to the classes $\theta(C)$, $\theta(C')$, $\theta(CC')$, and, as $JJ' = J''$ by Lemma 3, we have $\theta(C)\,\theta(C') = \theta(CC')$, showing that θ is a homomorphism: $C_{D'} \to C_D$.

Finally we show that θ is surjective. Let C be a class of C_D and let $J = \left[a, \frac{b+\sqrt{D}}{2}\right]$ be a primitive ideal of C with $GCD(a, f) = 1$ (Lemma 2).

Then we have $GCD(a, b, c) = 1$, where $\dfrac{D - b^2}{4a} = c$, and so $GCD(a, bf, cf^2) = 1$, showing that $I = \left[a, f\left(\dfrac{b + \sqrt{D}}{2}\right)\right]$ is a primitive ideal of $O_{D'}$. Hence C is the image of the class of I under θ.

COROLLARY 4. *If the class C of $O_{D'}$ contains the primitive ideal $I = \left[a, \dfrac{b + \sqrt{D'}}{2}\right]$, where $f^2 \mid a$, then $f \mid b$ and the class $\theta(C)$ contains the primitive ideal $J = \left[\dfrac{a}{f^2}, \dfrac{\dfrac{b}{f} + \sqrt{D}}{2}\right]$ of O_D.*

Proof. As $D' = Df^2 = b^2 + 4ac$, and $f^2 \mid a$, we see that $f \mid b$, and so $GCD(f, c) = 1$. By Corollary 2 we have $I = \left(\dfrac{\sqrt{D'} - b}{2a}\right)\left[c, \dfrac{-b + \sqrt{D'}}{2}\right]$ and so, by Theorem 1, we see that $\left[c, \dfrac{-\dfrac{b}{f} + \sqrt{D}}{2}\right] \in \theta(C)$. Finally, by Corollary 2, $J = \left[\dfrac{a}{f^2}, \dfrac{b/f + \sqrt{D}}{2}\right] = \dfrac{\left(\sqrt{D} + \dfrac{b}{f}\right)}{2c}\left[c, \dfrac{\dfrac{-b}{f} + \sqrt{D}}{2}\right]$, showing that $J \in \theta(C)$.

4. REDUCED IDEALS

From now on in this paper we suppose that $D_0 > 0$ so that we are only considering ideals in orders of a real quadratic field. An ideal I of O_D can be written in the form $I = ad[1, \phi]$, where $\phi = \dfrac{b + \sqrt{D}}{2a}$. By Proposition 1 (ii), if $I = a'd'[1, \phi']$ is another representation of I, then $a' = \pm a$ and $\phi' \equiv \dfrac{a}{a'}\phi \pmod 1$. A real number of the form $\dfrac{b + \sqrt{D}}{2a}$, where $c = \dfrac{D - b^2}{4a}$ is an integer and $GCD(a, b, c) = 1$ is called a quadratic irrationality of discriminant D.

Definition 9. (Reduced number). The quadratic irrationality $\phi = \dfrac{b + \sqrt{D}}{2a}$ of discriminant D is said to be *reduced* if

$$\phi > 1 , \quad -1 < \bar{\phi} < 0 . \tag{4.1}$$

It is easy to check that (4.1) is equivalent to each of the inequalities in (4.2)

$$\text{(i)} \quad 0 < \sqrt{D} - b < 2a < \sqrt{D} + b , \tag{4.2}$$

$$\text{(ii)} \quad 0 < \sqrt{D} - b < 2c < \sqrt{D} + b .$$

Moreover (4.2) implies

$$0 < a < \sqrt{D} , \quad 0 < b < \sqrt{D} , \quad 0 < c < \sqrt{D} . \tag{4.3}$$

Definition 10. (Reduced ideal). The ideal $I = ad[1, \phi]$ of O_D, where $\phi = \dfrac{b + \sqrt{D}}{2a}$, is said to be *reduced* if, and only if, ϕ can be chosen to be reduced.

From (4.3) we see that the number of reduced, primitive ideals of O_D is finite.

PROPOSITION 4. ([12]: Definition and Theorem 3.5). *The ideal*

$$I = d\left[a, \frac{b + \sqrt{D}}{2}\right]$$

of O_D, *where* $a > 0$ *and* $d > 0$, *is reduced if, and only if,* I *does not contain a nonzero element* α *satisfying* $|\alpha| < da, |\bar{\alpha}| < da$.

Proof. It suffices to prove that I is reduced if, and only if, the Z-module $[1, \phi]$ does not contain a nonzero element $\lambda = x + y\phi$ such that

$$|\lambda| < 1 , \quad |\bar{\lambda}| < 1 . \tag{4.4}$$

If I is reduced we can suppose that $\phi > 1$, $-1 < \bar{\phi} < 0$. Let x and y be integers such that $0 < \lambda = x + y\phi < 1$.

Clearly we have $y \neq 0$. If $y \geqslant 1$, then we have $y\phi > 1$, so $x \leqslant -1$, showing that $\bar{\lambda} = x + y\bar{\phi} < -1$. If $y \leqslant -1$, then we have $y\phi < -1$, so $x \geqslant 2$, showing that $\bar{\lambda} = x + y\bar{\phi} > 2$. This proves that $[1, \phi]$ does not contain an element $\lambda \neq 0$ such that $|\lambda| < 1, |\bar{\lambda}| < 1$.

Now suppose the Z-module $[1, \phi]$ does not contain an element $\lambda \neq 0$ satisfying (4.4). We can choose ϕ so that $-1 < \bar{\phi} < 0$, in which case

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

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

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

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

(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

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

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 $\rho = \dfrac{a'}{a}\,\phi' = \dfrac{-1}{\bar{\phi}'}$.

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 $-1 < \bar{\phi}' = \dfrac{1}{\bar{\phi} - q} < 0$, 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 $\phi_1 = q_1 + \dfrac{1}{\phi'}$ and $\phi_2 = q_2 + \dfrac{1}{\phi'}$, so that $\dfrac{b_1 + \sqrt{D}}{2a_1} = (q_1 - q_2) + \dfrac{b_2 + \sqrt{D}}{2a_2}$, 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 $q (\geqslant 1)$ such that $-1 - \dfrac{1}{\bar{\phi}'} < q < \dfrac{-1}{\bar{\phi}'}$. Set $\phi = q + \dfrac{1}{\phi'} > 1$. It is easy to check that $\phi = \dfrac{b + \sqrt{D}}{2a}$, where $a, b \in Z$. Then $\bar{\phi} = q + \dfrac{1}{\bar{\phi}'}$ 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

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

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

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

so that

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

By Corollary 1, we have

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

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

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

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

then

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

and

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

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

$\bar{\phi}_m = \dfrac{b_m - \sqrt{D}}{2a_m} < 0$, 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 $m \geqslant n-1$.

(ii) We have $I_m = a_m[1, \phi_m] = a_m[1, \psi_m]$, where $\psi_m = \phi_m + [|\bar{\phi}_m|]$. For $m \geqslant n \geqslant 1$, as $\psi_m \geqslant \phi_m > 1$ 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 $I_m (m \geqslant n)$ is reduced.

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

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

These sequences have the following basic properties:

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

$$\phi_0 = \frac{A_{n-1}\phi_n + A_{n-2}}{B_{n-1}\phi_n + B_{n-2}}, \quad n \geqslant 0, \tag{5.8}$$

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

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

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

$$(-1)^n(\phi_0 - \bar{\phi}_0) = \frac{1}{(B_{n-1}^2 \bar{\phi}_n + B_{n-1}B_{n-2})} - \frac{1}{(B_{n-1}^2 \phi_n + B_{n-1}B_{n-2})}, \quad n \geqslant 0, \tag{5.12}$$

$$\phi_1 \ldots \phi_n = B_{n-1}\phi_n + B_{n-2}, \quad n \geqslant 1. \tag{5.13}$$

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

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

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

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

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

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 $n \geqslant M_0$.

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*

$$I = \delta I_0,\ \frac{1}{a_0} \leqslant \delta < 2, \tag{5.16}$$

in atmost 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 $n_0 \leqslant M_0$. By Lemma 5 the ideal I_{n_0} is reduced, and $a_{n_0-1} > 0$, $a_{n_0} > 0$.

We set

$$\delta = \begin{cases} \dfrac{a_{n_0-1}}{a_0}\,\phi_1 \ldots \phi_{n_0-1}, & \text{if } I_{n_0-1} \text{ is reduced}, \\ \dfrac{a_{n_0}}{a_0}\,\phi_1 \ldots \phi_{n_0}, & \text{if } I_{n_0-1} \text{ is not reduced}, \end{cases} \tag{5.17}$$

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

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

$$\phi_1 \ldots \phi_{n_0-1} = B_{n_0-2}\phi_{n_0-1} + B_{n_0-3}, \tag{5.18}$$

so that

$$\bar{\phi}_1 \ldots \bar{\phi}_{n_0-1} = B_{n_0-2}\phi_{n_0-1} + B_{n_0-3} > B_{n_0-3}, \tag{5.19}$$

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

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

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

$$1 < \phi_1 \ldots \phi_{n_0-1} < \frac{a_0}{a_{n_0-1}}\,\frac{1}{B_{n_0-3}}. \tag{5.21}$$

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

$< \dfrac{2a_{n_0-1}}{a_{n_0}}$. 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

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

From (6.1), we see that $\frac{a_0}{\rho} J = bI_0$, 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

$$\frac{1}{\phi_1} < x + \frac{y}{\phi_1} < 1 . \tag{6.2}$$

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

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

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*

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

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

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

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

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

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*

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

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 $\sigma \equiv \rho^{-1} \pmod{\eta}$, which proves Proposition 10.

7. COMPARISON OF DISTANCES BETWEEN CORRESPONDING IDEALS IN DIFFERENT ORDERS

Let C be a primitive class of the order $O_{D/2}$ 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 $\phi = \frac{b + \sqrt{D'}}{2a}$ 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

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

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

$$\frac{1}{2fD'} < \rho < f . \tag{7.4}$$

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))

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

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 $p^2 D = b_1^2 + 4aa_1$, 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 $\rho = \dfrac{a_1}{a}\phi_1$. Now, by Proposition 5, $\phi_1 = \dfrac{b_1 + \lfloor \sqrt{D} \rfloor}{2a_1}$ is reduced, so that $1 \leqslant b_1 < \lfloor \sqrt{D} \rfloor$, and

$$1 \leqslant a_1 < \lfloor \sqrt{D} \rfloor , \tag{7.5}$$

giving

$$1 \leqslant \rho < \lfloor \sqrt{D} \rfloor . \tag{7.6}$$

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

$$0 < \frac{-b + \lfloor \sqrt{D} \rfloor}{2 \mid c \mid} < 1 , \tag{8.1}$$

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 $b < \lfloor \sqrt{D} \rfloor$ 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 $I' = \left[a', \dfrac{b' + \lfloor \sqrt{D} \rfloor}{2}\right]$ are determined by I. The value of q is*

$$q = \frac{a}{\mid a \mid}\left[\frac{b + \lfloor \sqrt{D} \rfloor}{2 \mid a \mid}\right] . \tag{8.2}$$

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*

$$\{a, b\} \overset{G}{\to} \{a', b'\} .$$

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

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

that is, by (2.10), if $0 < \dfrac{b + \lfloor \sqrt{D} \rfloor}{2 \mid a \mid} - \dfrac{a}{\mid a \mid} q < 1$, giving $q = \dfrac{a}{\mid a \mid} \left[\dfrac{b + \lfloor \sqrt{D} \rfloor}{2 \mid a \mid} \right]$, which shows that q and $\{a', b'\}$ are determined by $\{a, b\}$. Let $\{\pm a, b + 2K \mid a \mid\} = \{a_1, b_1\}$ be another representation of I giving rise to a half-reduced representation, say $\{a_1', b_1'\}$. As $b_1' \equiv -b_1 \equiv -b \equiv b' \pmod{2 \mid a \mid}$ and $\mid a_1 \mid = \mid a \mid$, we see from the inequalities

$$0 < \frac{\lfloor \sqrt{D} \rfloor - b'}{2 \mid a \mid} < 1 \quad \text{and} \quad 0 < \frac{\lfloor \sqrt{D} \rfloor - b_1'}{2 \mid a_1 \mid} < 1$$

that $b_1' = b'$. Hence, as $\mid a \mid = \mid a_1 \mid$ and $b' = b_1'$, from $D = b'^2 + 4aa' = b_1'^2 + 4a_1 a_1'$, we see that $\mid a' \mid = \mid a_1' \mid$. 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* $\{a, b\} \overset{G}{\to} \{a', b'\}$ *and set* $I' = \left[a', \dfrac{b' + \lfloor \sqrt{D} \rfloor}{2} \right]$. *We have*

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

(ii) if $b > -\lfloor \sqrt{D} \rfloor$ *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* $\phi = \dfrac{b + \lfloor \sqrt{D} \rfloor}{2a}$ *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

$$\left| \frac{\lfloor \sqrt{D} \rfloor - b}{2c} \right| \left| \frac{\lfloor \sqrt{D} \rfloor + b}{2a} \right| = 1 . \tag{8.3}$$

Now take $\{a, b\}$ to be a half-reduced representation of the half-reduced ideal I so that $0 < \dfrac{-b+\sqrt{D}}{2|c|} < 1$, 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 $\left(\dfrac{\sqrt{D}-b}{2|c|}\right)\left(\dfrac{-b-\sqrt{D}}{2|a|}\right) = 1$. As $0 < \dfrac{-b+\sqrt{D}}{2|c|} < 1$, we see that $\dfrac{-b-\sqrt{D}}{2|a|} > 1$. But, as $\{a', b'\}$ is also half-reduced, we have $\dfrac{-b'+\sqrt{D}}{2|a|} < 1$, 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 $\dfrac{\sqrt{D}+b}{2|a|} > 1$. Or the other hand, as $\{a', b'\}$ is half-reduced, we have $0 < \dfrac{\sqrt{D}-b'}{2|a|} < 1$, that is $0 < \dfrac{\sqrt{D}+b}{2|a|} - \dfrac{a}{|a|}q < 1$, so that

$$\frac{a}{|a|}q = \left[\frac{\sqrt{D}+b}{2|a|}\right] \geqslant 1 .$$

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

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

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*

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

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

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

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 $i = 1, 2, \ldots, n-1$. Then, by Proposition 11 (i), we have

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

Hence we obtain

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

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

(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 $\frac{1}{|a_0|} \leqslant \rho < |\sqrt{D}$. If $n \geqslant 1$ we have $I_n = \rho I_0$ with (by (2.12))

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

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

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

As $\{a_k, b_k\}$ is a half-reduced representation for $k = 1, 2, \ldots, n$, we have $0 < |\sqrt{D} - b_k < 2|a_{k-1}|$. Furthermore, for $k = 1, 2, \ldots, n-1$, 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 $k = 1, 2, \ldots, n-1$, we have

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

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

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

and

$$\{3655, 7068\} \overset{G}{\to} \{-3417, -7068\} \overset{G}{\to} \{3187, -6600\} \overset{G}{\to} \{-2965, -6148\} \overset{G}{\to} \ldots$$
$$\overset{G}{\to} \{-1, -12\} \overset{G}{\to} \{-5, 8\} \quad (30 \text{ steps}) .$$

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

REFERENCES

[1] GAUSS, C.F. Disquisitiones Aritmeticae, 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. SCHOENEBERG. *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.

[10] TAKAGI, T. *Elementary Number Theory*. Kyoritsu, Tokyo, 1971 (in Japanese).
[11] WILLIAMS, H. C. Eisenstein's problem and continued fractions. Preprint.
[12] WILLIAMS, H. C. and M. C. WUNDERLICH. On the parallel generation of the residues for the continued fraction factoring algorithm. *Math. Comp. 48* (1987), 405-423.

(Reçu le 20 mars 1990)

P. Kaplan

Département de Mathématiques
Université de Nancy 1
B.P. 239
54506 Vandœuvre les Nancy Cedex (France)

K. S. Williams

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada KIS 5B6