Infrastructure in Real Quadratic Function Fields

Andreas Stein

Centre for Applied Cryptographic Research

University of Waterloo

Waterloo, Ontario N2L 3G1, Canada

astein@cacr.math.uwaterloo.ca

May 25, 1999

Abstract

The principal topic of this article is to extend Shanks' infrastructure ideas in real quadratic number fields to the case of real quadratic congruence function fields. In this view, this paper is intended as a "low-brow" approach to the theory of ideals and operations in the ideal class group. We summarize some basic properties of ideals and provide elementary proofs of the main results. For the purpose of this paper, only an elementary knowledge of the subject is needed, and we mainly follow the introductory notes of Artin.

1 Introduction

Any hyperelliptic function field can be represented as a real quadratic function field. Since the arithmetic in real quadratic function fields is more "variable" as in imaginary quadratic function fields, it is important to investigate the arithmetic in real quadratic function fields in detail. We explain the idea of the "infrastructure", i.e. the structure within a structure, which goes back to D. Shanks [Sha72]. Most theorems are in complete analogy to the results in real quadratic number fields. Nevertheless, there are some basic differences which seem to make the infrastructure operation more effective and "closer" to a group operation. For the number-theoretic background, we refer to the book of Stichtenoth [Sti93]. This paper is definitely "low-brow", and only an elementary knowledge of the subject is needed. Since many results are due to Artin [Art24], we mainly follow the notations of his introductory notes.

Let $k = \mathbb{F}_q$ be a finite field of odd characteristic and let $K = k(x)(\sqrt{D})$, where D is a squarefree polynomial. Such a field is known as a *quadratic function field* over k (of odd characteristic). Throughout, the following terminology will be fixed. The integral closure of $k[x]$ in K is given by $\mathcal{O}_K = \overline{k[x]}$ and is called the *ring of integers of* K. Let $E = {\mathcal{O}_K}^*$ the *group of units* in $\mathcal{O}_K$. If, in addition, D is monic and of even degree, then K is called a *real quadratic function field* over k (of odd characteristic). Otherwise, we call K imaginary quadratic. For real quadratic function fields of characteristic 2, we refer to [Zuc97]. We neglect the even characteristic case in this paper.

If $K = k(x)(\sqrt{D})$ is real quadratic, where $D \in k[x]$ is monic and squarefree, then the *genus* of K is defined by $g = \deg(D)/2 - 1$. K is a Galois extension of the rational function field $k(x)$ with Galois group $\{1, \sigma\}$, where σ is the K-automorphism which takes $\sqrt{D}$ to $-\sqrt{D}$. The *conjugate* of an element $\alpha = u + v\sqrt{D} \in K$ with $u, v \in k(x)$ is given by $\overline{\alpha} = \sigma(\alpha) = u - v\sqrt{D}$. The *norm* of α is defined by $N(\alpha) = \alpha \cdot \overline{\alpha} = u^2 - v^2 D$, which gives a rational function. The decomposition of the infinite place $\mathfrak{P}_\infty$ of $k(x)$ in K is $\mathfrak{P}_\infty = \mathfrak{P}_1 \cdot \mathfrak{P}_2$, where $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are the infinite places of K/k. We also know that

$$E = k^* \times \langle \epsilon \rangle,$$

where $\epsilon \in K$ is a fundamental unit. If we denote by $v_{\mathfrak{P}_1}$ and $v_{\mathfrak{P}_2}$ the two normalized extensions of the negative degree valuation $v_{\mathfrak{P}_\infty}$ from $k(x)$ to K, we call the positive integer

$$R = |v_{\mathfrak{P}_1}(\epsilon)| = |v_{\mathfrak{P}_1}(\epsilon)| \geq 1$$

the *regulator of* K/k *with respect to* $\mathcal{O}_K$. If h' denotes the ideal class number of K with respect to $\mathcal{O}_K$ and h the divisor class number of K, then we know from [Sch31] that $h = R \cdot h'$. The meaning of h and h' is described in [Art24, Deu73].

Furthermore, K is a subfield of the field of Puiseux series $k((1/x))$, i.e. $K \leq k((1/x))$. Let $\mathfrak{P}_1$ be the place which corresponds to the case where $\sqrt{1} = 1$. Then we consider elements of K as Laurent series at $\mathfrak{P}_1$ in the variable $1/x$. For an element $\alpha \in L = k((1/x))$ such that $0 \neq \alpha = \sum_{i=-\infty}^{m} c_i x^i$ and $c_m \neq 0$, we define

$$\left\{ \begin{array}{rcl} \deg(\alpha) & = & m \\ |\alpha| & = & q^m \\ \operatorname{sgn}(\alpha) & = & c_m \\ \lfloor \alpha \rfloor & = & \sum_{i=0}^{m} c_i x^i . \end{array} \right\} \tag{1.1}$$

If m is negative, then we have that $\lfloor \alpha \rfloor = 0$. For completeness, we set $\deg(0) = -\infty$ and $|0| = 0$.

2 Ideals

In this section, we summarize some important facts about $\mathcal{O}_K$-Ideals in a quadratic function field $K = k(x)(\sqrt{D})$, where $\mathcal{O}_K = k[x][\sqrt{D}]$ and k is an arbitrary field of characteristic different from 2. Here, D is a squarefree polynomial in $k[x]$. We call a non-zero subset $\mathfrak{a}$ of K an *$\mathcal{O}_K$-ideal*, or simply an *ideal*, if $\mathfrak{a}$ possesses the properties:

1. if $\lambda_1, \lambda_2 \in \mathcal{O}_K$ and $\alpha_1, \alpha_2 \in \mathfrak{a}$, then $\lambda_1\alpha_1 + \lambda_2\alpha_2 \in \mathfrak{a}$;
2. there exists a $\lambda, , (\neq 0) \in \mathcal{O}_K$ such that $\lambda\mathfrak{a} \subseteq \mathcal{O}_K$.

If the second condition holds with $\lambda = 1$, we say that $\mathfrak{a}$ is an *integral $\mathcal{O}_K$-ideal.* For elements $\alpha_1, \alpha_2, \ldots, \alpha_r \in K$ the set

$$(\alpha_1, \alpha_2, \ldots, \alpha_r) := \left\{ \sum_{i=1}^{r} \lambda_i \alpha_i \ ; \ r \in \mathbb{N}_0,\ \lambda_i \in \mathcal{O}_K, i = 1, \ldots, r \right\}$$

is clearly an ideal, and it is called the ideal *generated* by $\alpha_1, \alpha_2, \ldots, \alpha_r$. If $\mathfrak{a}$ is generated by a single element $\alpha \in K$, i.e. $\mathfrak{a} = (\alpha) = \alpha\mathcal{O}_K$, we call $\mathfrak{a}$ a *principal $\mathcal{O}_K$-ideal.* For $\omega_1, \omega_2, \ldots, \omega_r \in \mathcal{O}_K$ we let

$$[\omega_1, \omega_2, \ldots, \omega_r] := \left\{ \sum_{i=1}^{r} A_i \omega_i \ ; \ A_i \in k[x], i = 1, \ldots, r \right\} \quad \subseteq \quad \mathcal{O}_K \ .$$

If this set is an integral ideal, and $\omega_1, \omega_2, \dots, \omega_r$ are linearly independent over $k[x]$, then $\{\omega_1, \omega_2, \dots, \omega_r\}$ is called a $k[x]$-*basis* of $\mathfrak{a}$.

In [Art24] it is shown that every $k[x]$-base of an integral ideal $\mathfrak{a}$ consists of two elements.

Theorem 2.1. *A nonzero subset $\mathfrak{a}$ of $\mathcal{O}_K$ is an integral ideal if and only if there exist $S, P, Q \in k[x]$ with $Q|(D - P^2)$ such that*

$$\mathfrak{a} = [SQ, SP + S\sqrt{D}] \ . \tag{2.1}$$

We say that an integral $\mathcal{O}_K$-ideal $\mathfrak{a}$ is *primitive*, if in (2.1), S can be chosen to be 1, i.e. if

$$\mathfrak{a} = [Q, P + \sqrt{D}\,]$$

with $Q|(D - P^2)$. A $k[x]$-base of an integral ideal $\mathfrak{a}$ can be chosen to be in *adapted* form, meaning that

$$\mathfrak{a} = [T, R + S\sqrt{D}] \qquad (T, R, S \in k[x]) \ , \tag{2.2}$$

where $\deg(R) < \deg(T)$. The polynomials T, R, S are unique up to constant factors. More precisely, if $\operatorname{sgn}(T) = \operatorname{sgn}(S) = 1$, then the adapted representation is unique.

Let $\mathfrak{a}$ be an integral $\mathcal{O}_K$-ideal given with an arbitrary $k[x]$-base $\{\omega_1, \omega_2\}$. It is easy to see that $\mathfrak{a} = [\omega_1, \omega_2] = (\omega_1, \omega_2)$. We define the *norm* of $\mathfrak{a}$, $N(\mathfrak{a}) \in k[x]$, by

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \overline{\omega}_1 & \overline{\omega}_2 \end{vmatrix}^2 = c^2 \cdot \left(N(\mathfrak{a})^2\right) \cdot D \ ,$$

where $c \in k^*$ and $\operatorname{sgn}(N(\mathfrak{a})) = 1$. The norm of an $\mathcal{O}_K$-ideal does not depend on the given $k[x]$-base. If an integral $\mathcal{O}_K$-ideal $\mathfrak{a}$ is given with a $k[x]$-base as in (2.1), we see that

$$N(\mathfrak{a}) = \frac{Q \cdot S^2}{\operatorname{sgn}\left(Q \cdot S^2\right)} \ \in k[x] \ . \tag{2.3}$$

Note that $\operatorname{sgn}(N(\mathfrak{a})) = 1$.

Next, we generally define the *product* of two $\mathcal{O}_K$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ by

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{n} a_i b_i \ ; \ n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, i = 1, \dots, n \right\} .$$

Again, this set represents an $\mathcal{O}_K$-ideal. For $\beta, \alpha_1, \alpha_2, \ldots, \alpha_r \in K$, we calculate $(\beta) \cdot (\alpha_1, \alpha_2, \ldots, \alpha_r) = (\beta\alpha_1, \beta\alpha_2, \ldots, \beta\alpha_r)$, and $(\alpha_1, \alpha_2) \cdot (\beta_1, \beta_2) = (\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2)$. For any $\mathcal{O}_K$-ideal $\mathfrak{a}$, the $\mathcal{O}_K$-ideal

$$\overline{\mathfrak{a}} := \{\overline{\alpha}\ ;\ \alpha \in \mathfrak{a}\}$$

is called the *conjugate $\mathcal{O}_K$-ideal* of $\mathfrak{a}$. If $\mathfrak{a} = \{\, \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_r \,\}$, then $\overline{\mathfrak{a}} = \{\, \overline{\alpha}_1,\ \overline{\alpha}_2,\ \ldots,\ \overline{\alpha}_r \,\}$. The following lemma describes some properties of the norm and the conjugate of an integral $\mathcal{O}_K$-ideal.

Lemma 2.1. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral $\mathcal{O}_K$-ideals.*

1. $\mathfrak{a}\overline{\mathfrak{a}} = (N(\mathfrak{a}))$.
2. $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.
3. *If $\mathfrak{a}$ is principal, i.e. $\mathfrak{a} = (\alpha)$, where $\alpha \in \mathcal{O}_K$, then there exists a $c \in k^*$ such that $N(\mathfrak{a}) = cN(\alpha)$.*

Finally, we say that two integral $\mathcal{O}_K$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent*, written $\mathfrak{a} \sim \mathfrak{b}$, if there exist some non-zero elements $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$.

3 Ideal Product

For an efficient arithmetic in quadratic function field, we have to define an operation that corresponds to the group operation in any finite Abelian group. The first step is to compute the product of two $\mathcal{O}_K$-ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ given with their unique adapted $k[x]$-bases. By Theorem 2.1 and (2.2), there exists $S_i, Q_i, P_i \in k[x]$ $(i = 1, 2)$ such that $Q_i | (D - P_i^2)$, and

$$\mathfrak{a}_i = (S_i)[Q_i, P_i + \sqrt{D}] = (S_i)\mathfrak{a}'_i \quad (i = 1, 2)\ ,$$

where $\mathfrak{a}'_i = [Q_i, P_i + \sqrt{D}]$ is a primitive $\mathcal{O}_K$-ideal. Then $\mathfrak{a}_1 \cdot \mathfrak{a}_2 = (S_1S_2)\mathfrak{a}'_1 \cdot \mathfrak{a}'_2$ and we have to compute the product of the primitive $\mathcal{O}_K$-ideals $\mathfrak{a}'_1$ and $\mathfrak{a}'_2$. Without loss of generality, we therefore assume that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are primitive, i.e. $S_i = 1$, and that they are given with their unique adapted bases. This means that

$$\mathfrak{a}_i = [Q_i, P_i + \sqrt{D}]\ ,$$

where $Q_i, P_i \in k[x]$, $Q_i|(D - P_i^2)$, and

$$\deg(P_i) < \deg(Q_i) \quad \text{and} \quad \operatorname{sgn}(Q_i) = 1 \ .$$

To compute the product of $\mathfrak{a}_1$ and $\mathfrak{a}_2$, we use the same ideas as Shanks, [Sha71], as employed, for example, in [Len82] or [SW88]. Our aim is to find a primitive $\mathcal{O}_K$-ideal $\mathfrak{c} = [Q, P + \sqrt{D}]$ and a polynomial $S \in k[x]$ such that $\mathfrak{a}_1\mathfrak{a}_2 = (S)\mathfrak{c}$, where $Q|(D - P^2)$, $\deg(P) < \deg(Q)$ and $\operatorname{sgn}(Q) = 1 = \operatorname{sgn}(S)$. We obtain

$$S = \gcd(Q_1, Q_2, P_1 + P_2) \ , \tag{3.1}$$

$$Q = \frac{Q_1 Q_2}{S^2} \ , \tag{3.2}$$

$$P \equiv \left(P_1 + \frac{Q_1}{S}\left[U(P2 - P_1) + W\left(\frac{D - P_1^2}{Q_1}\right)\right]\right) \pmod{Q} \ , \tag{3.3}$$

where $U, V, W \in k[x]$ are polynomials such that $S = UQ_1 + VQ_2 + W(P_1 + P_2)$. Therefore, we proceed as follows: using the extended Euclidean algorithm, we compute polynomials S_1, X_1 such that $S_1 = \gcd(Q_1, Q_2) \equiv X_1 Q_1 \pmod{Q_2}$. By using the extended Euclidean algorithm again, we compute polynomials S, X_2, Y_2 such that $S = \gcd(G_1, P_1 + P_2) = X_2 S_1 + Y_2(P_1 + P_2)$. Thus, $U = X_2 X_1$ and $W = Y_2$. Finally, we can apply the formulas for P and Q. In many cases, we have $S_1 = 1$, and we continue with $S = 1$, $X_2 = 1$, $Y_2 = 0$.

4 Reduced Ideals in the Real Case

Here and throughout the remainder of this paper, we consider K to be a real quadratic function field over the finite field $k = \mathbb{F}_q$ of odd characteristic, i.e. $K = k(x)(\sqrt{D})$, where D is a monic, squarefree polynomial in $k[x]$ of even degree. First, we state a helpful Lemma which describes equivalent ideals in the real case.

Lemma 4.1. *If $\mathfrak{a}$ and $\mathfrak{b}$ are two equivalent integral $\mathcal{O}_K$-ideals, then there exists a $\gamma \in \mathfrak{a}$ such that*

$$(\gamma)\mathfrak{b} = (N(\mathfrak{b}))\,\mathfrak{a} \ ,$$

where $0 < |\gamma| \leq |N(\mathfrak{a})|$.

Proof. Since $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent and integral, there exist nonzero $\alpha, \beta \in \mathcal{O}_K$ such that

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{b} .$$

From Lemma 2.1 it follows that

$$c_1 \alpha\overline{\alpha} N(\mathfrak{a}) = c_2 \beta\overline{\beta} N(\mathfrak{b})$$

for some $c_1, c_2 \in k^*$. We put

$$\gamma' = c_1 \cdot \frac{\overline{\alpha}}{\overline{\beta}} \cdot N(\mathfrak{a}) = c_2 \cdot \frac{\beta}{\alpha} \cdot N(\mathfrak{b}) .$$

Then $0 \neq \gamma' \in \mathfrak{a}$, since $N(\mathfrak{b}) \in \mathfrak{b}$. Furthermore, we have that

$$(\alpha)(\gamma')\mathfrak{b} = (\beta)(N(\mathfrak{b}))\mathfrak{b} = (\alpha)\,(N(\mathfrak{b}))\,\mathfrak{a} .$$

Deleting (α) on both sides leads to $(\gamma')\mathfrak{b} = (N(\mathfrak{b}))\mathfrak{a}$. We know that the unit group E is nontrivial in the real quadratic case. Therefore, let $\epsilon \in E$ with $|\epsilon| > 1$. If we choose a nonnegative integer n_0 such that

$$\frac{|\gamma'|}{|\epsilon|^{n_0}} \leq |N(\mathfrak{a})| ,$$

then the assertion follows with $\gamma := \epsilon^{-n_0} \cdot \gamma'$. □

An integral $\mathcal{O}_K$-ideal $\mathfrak{a}$ is called a *reduced $\mathcal{O}_K$-ideal* if $\mathfrak{a}$ is primitive and if there exists a $k[x]$-base of the form $\{Q, P + \sqrt{D}\}$ with polynomials $Q, P \in k[x]$, $Q|(D - P^2)$ and

$$|P - \sqrt{D}| < |Q| = |N(\mathfrak{a})| < |P + \sqrt{D}| ,$$

or, equivalently, if $(P + \sqrt{D})/Q$ is a reduced real quadratic irrationality. The equality $|Q| = |N(\mathfrak{a})|$ is an immediate consequence of (2.3). In this case, we call the $k[x]$-base $\{Q, P + \sqrt{D}\}$ a *reduced $k[x]$-base* of $\mathfrak{a}$. If $\operatorname{sgn}(Q) = 1$, then the reduced $k[x]$-base is unique. We can characterize reduced ideals as follows.

Theorem 4.1. *A primitive $\mathcal{O}_K$-ideal $\mathfrak{a}$ is reduced if and only if*

$$|N(\mathfrak{a})| < |\sqrt{D}| ,$$

i.e. $\deg N(\mathfrak{a}) \leq g$*, where g denotes the genus of K.*

Proof. If $\mathfrak{a}$ is a reduced $\mathcal{O}_K$-ideal, then $\mathfrak{a} = [Q, P + \sqrt{D}]$, where $Q, P \in k[x]$ are such that $Q|(D - P^2)$ and

$$|P - \sqrt{D}| < |Q| = |N(\mathfrak{a})| < |P + \sqrt{D}| \ .$$

This can only happen if $|P| = |\sqrt{D}|$ and even the two highest coefficients of P and $\sqrt{D}$ are equal (Note that the characteristic of k is different from 2). Thus,

$$|N(\mathfrak{a})| = |Q| < |P + \sqrt{D}| = |\sqrt{D}| \ .$$

Conversely, if $\mathfrak{a}$ is a primitive $\mathcal{O}_K$-ideal with $|N(\mathfrak{a})| < |\sqrt{D}|$, then $\mathfrak{a} = [Q, P + \sqrt{D}]$ with $Q, P \in k[x]$. We put

$$P' := P - \left\lfloor \frac{P - \sqrt{D}}{Q} \right\rfloor \cdot Q \ .$$

Clearly, $\mathfrak{a} = [Q, P' + \sqrt{D}]$ and $|P' - \sqrt{D}| < |Q|$, since

$$\left| \frac{P' - \sqrt{D}}{Q} \right| = \left| \frac{P - \sqrt{D}}{Q} - \left\lfloor \frac{P - \sqrt{D}}{Q} \right\rfloor \right| < 1 \ .$$

Furthermore, we see that

$$|P' + \sqrt{D}| = |(P' - \sqrt{D}) + 2\sqrt{D}| = |\sqrt{D}| > |Q| \ ,$$

by assumption. Therefore, $\{Q, P' + \sqrt{D}\}$ is a reduced $k[x]$-base of $\mathfrak{a}$, and thus $\mathfrak{a}$ is reduced. □

Lemma 4.2. *If $\mathfrak{a}$ is a reduced $\mathcal{O}_K$-ideal, then there does not exist any nonzero $\alpha \in \mathfrak{a}$ such that*

$$|\alpha| < |N(\mathfrak{a})| \quad \textit{and} \quad |\overline{\alpha}| \leq |N(\mathfrak{a})| \ .$$

Proof. We have $\mathfrak{a} = [Q, P + \sqrt{D}]$ where $Q, P \in k[x]$ and

$$|P - \sqrt{D}| < |Q| = |N(\mathfrak{a})| < |P + \sqrt{D}| \ .$$

For any nonzero $\alpha \in \mathfrak{a}$ there exist $U, V \in k[x]$ such that

$$\alpha = UQ + V(P + \sqrt{D}) \qquad \text{and} \qquad \overline{\alpha} = UQ + V(P - \sqrt{D}) \ .$$

If $V = 0$ then $U \neq 0$, i.e. $|U| \geq 1$, and $|\alpha| = |\overline{\alpha}|$. Hence

$$|\alpha| = |UQ| \geq |Q| = |N(\mathfrak{a})|$$

and the assertion follows. Now, let $V \neq 0$, i.e. $|V| \geq 1$. We distinguish between two cases. If $|U| \leq |V|$, then $|UQ| < |V||P + \sqrt{D}|$, by assumption. Thus

$$|\alpha| = |V||P + \sqrt{D}| \geq |P + \sqrt{D}| > |N(\mathfrak{a})| \ .$$

If $|U| > |V|$, then we analogously show that $|\overline{\alpha}| > |N(\mathfrak{a})|$. □

5 Continued Fractions and Ideals

In this section, we show that the continued fraction expansion of real quadratic irrationalities and the continued fraction expansion of primitive ideals is closely related. Let $\mathfrak{a}$ be any primitive $\mathcal{O}_K$-ideal, and let $Q, P \in k[x]$ with $Q|(D-P^2)$ be such that $\mathfrak{a} = [Q, P+\sqrt{D}]$. If we set $\alpha := (P + \sqrt{D})/Q$, then α is a real quadratic irrationality, and we can carry through the continued fraction expansion of α. For details on the continued fraction expansion, we refer to [Ste99]. We put $\alpha_0 = \alpha$, $a_0 = \lfloor \alpha_0 \rfloor$, and, for $i \in \mathbb{N}$, we put $a_{i+1} = 1/(\alpha_i - a_i)$, $a_{i+1} = \lfloor \alpha_{i+1} \rfloor$. Note that $\deg(\alpha_i) \geq 1$ for $(i \in \mathbb{N})$. If we let $Q_0 = Q$, $P_0 = P$, and

$$P_{i+1} = a_i Q_i - P_i \ , \ Q_{i+1} = \frac{D - P_{i+1}^2}{Q_i} \quad (i \in \mathbb{N}_0) \ , \tag{5.1}$$

then $Q_i, P_i \in k[x]$, $Q_i|(D - P_i^2)$, and $\alpha_i = (P_i + \sqrt{D})/Q_i$. The real quadratic irrationality $\alpha = (P + \sqrt{D})/Q$ is called *reduced*, if $|\overline{\alpha}| < 1 < |\alpha|$, where $\overline{\alpha}$ is the conjugate of α, or equivalently, if

$$|P - \sqrt{D}\,| < |\,Q\,| < |P + \sqrt{D}\,| \ .$$

Now, we define $\mathfrak{a}_1 = \mathfrak{a}$. If we let

$$\mathfrak{a}_i = [Q_{i-1}, P_{i-1} + \sqrt{D}] \quad (i \in \mathbb{N}) \ , \tag{5.2}$$

then each $\mathfrak{a}_i$ is a primitive (integral) $\mathcal{O}_K$-ideal.

Most of the following results correspond to those for real quadratic number fields which can be found, for example, in [WW87]. However, we shall prove them using the terminology of integral ideals.

First, we derive that each $\mathfrak{a}_i$ is equivalent to $\mathfrak{a} = \mathfrak{a}_1$. By (5.1), we notice that

$$\mathfrak{a}_i = [Q_{i-1}, -P_i + \sqrt{D}] \quad (i \in \mathbb{N}) \ , \tag{5.3}$$

$$(\sqrt{D} - P_i)\mathfrak{a}_{i+1} = (Q_i)\mathfrak{a}_i \quad (i \in \mathbb{N}) \ . \tag{5.4}$$

As usual, we put $\theta_1 = 1$, and

$$\theta_{i+1} = \prod_{j=1}^{i} \frac{1}{\alpha_j} \quad (i \in \mathbb{N}_0) \ . \tag{5.5}$$

We see that

$$\mathrm{N}(\theta_{i+1}) = \theta_{i+1}\overline{\theta}_{i+1} = (-1)^i \frac{Q_i}{Q_0} \quad (i \in \mathbb{N}_0) \ . \tag{5.6}$$

Theorem 5.1. *If $\mathfrak{a} = [Q, P + \sqrt{D}]$ is any primitive $\mathcal{O}_K$-ideal and $\mathfrak{a}_i$ is defined as in (5.2), then $\mathfrak{a}_i$ is a primitive $\mathcal{O}_K$-ideal for $i \in \mathbb{N}$, and we have that*

$$(Q_0\theta_i)\mathfrak{a}_i = (Q_{i-1})\mathfrak{a}_1 \quad (i \in \mathbb{N}) \ ,$$

where $Q_0\theta_i, Q_0\overline{\theta}_i \in \mathcal{O}_K$.

Proof. It is easy to see that $Q_0\theta_i, Q_0\overline{\theta}_i \in \mathcal{O}_K$. The main assertion can be proved by induction. For $i = 1$, we trivially have that $(Q_0\theta_1)\mathfrak{a}_1 = (Q_{i-1})\mathfrak{a}_1$. Since $D - P_i^2 = Q_iQ_{i-1}$, we find that

$$\alpha_i = \frac{P_i + \sqrt{D}}{Q_i} = \frac{Q_{i-1}}{\sqrt{D} - P_i} \ .$$

It follows by (5.5) that

$$Q_{i-1}\theta_{i+1} = (\sqrt{D} - P_i)\theta_i \ . \tag{5.7}$$

Using this fact and (5.4) we obtain

$$(Q_{i-1})(Q_0\theta_{i+1})\mathfrak{a}_{i+1} = (Q_0\theta_i)(Q_i)\mathfrak{a}_i \ .$$

By induction, the last term equals $(Q_{i-1})(Q_i)\mathfrak{a}_1$. Thus, we can delete (Q_{i-1}) on both sides and our result follows. □

In view of (2.3), the statement of the theorem is equivalent to

$$(N(\mathfrak{a})\theta_i)\mathfrak{a}_i = (N(\mathfrak{a}_i))\mathfrak{a} \ , \tag{5.8}$$

Corollary 5.1. *In the situation of Theorem 5.1, we have for $i \in \mathbb{N}$ that*

$$\mathfrak{a}_1 = [Q_0\theta_i, Q_0\theta_{i+1}] \ .$$

Proof. From (5.7) and (5.3), we derive that

$$(Q_{i-1})[Q_0\theta_i, Q_0\theta_{i+1}] = (Q_0\theta_i)\mathfrak{a}_i$$

and the statement is an immediate consequence of Theorem 5.1. □

Next, we deal with the question, whether there is an index $i \in \mathbb{N}_0$ such that $\mathfrak{a}_{i+1}$ is reduced. We are interested in finding a criterion which is sufficient for this property.

Remark 5.1. *If, in the continued fraction expansion of $\alpha = \alpha_0 := (P_0 + \sqrt{D})/Q_0$, there is an index $i \in \mathbb{N}_0$ such that $\alpha_i = (P_i + \sqrt{D})/Q_i$ is reduced, then the ideal $\mathfrak{a}_{i+1}$ is reduced, because the reduced $k[x]$-base for $\mathfrak{a}_{i+1}$ is given by $\{Q_i, P_i + \sqrt{D}\}$.*

Theorem 5.2. *If $\mathfrak{a} = \mathfrak{a}_1 = [Q_0, P_0 + \sqrt{D}]$ is any primitive $\mathcal{O}_K$-ideal, then $\mathfrak{a}_i$ is reduced for*

$$i > I_0 := \max\{1, \deg(Q_0)/2 - (g+1)/2 + 2\} \ .$$

Proof. See [Ste99, Theorem 3.1], the above remark, and note that the genus of K is defined by $g = \deg(D)/2 - 1$. □

Conversely, if $\mathfrak{a}_i$ is reduced, the basis representation in (5.2) need not be the reduced one. This means that α_{i-1} is not necessarily reduced. For example, the ideal $\mathfrak{r} = [1, \sqrt{D}\,]$ is obviously reduced, since $\deg(N(\mathfrak{r})) = 0 \leq g$. But, the real quadratic irrationality $\alpha = \sqrt{D}$ is not reduced, since $|-\sqrt{D}| = |\sqrt{D}|$.

Lemma 5.1. *If $\mathfrak{a}_i$ is reduced for an index $i \in \mathbb{N}$, then α_i is reduced.*

Proof. This follows from Theorem 4.1 and [Ste99, Theorem 3.2]. □

Using similar ideas as those employed in the proof of Theorem 4.3 of [WW87], we can prove the following lemma.

Lemma 5.2. *If, in the continued fraction expansion of* $\alpha = \alpha_0 := (P_0 + \sqrt{D})/Q_0$*, there exists a minimal* $l \in \mathbb{N}$ *such that* $|Q_{l-1}| < |\sqrt{D}|$*, then* $\mathfrak{a}_l$ *is reduced, and*

$$|\overline{\theta}_l| \le 1 \ , \quad |\theta_l| \ge \frac{|Q_{l-1}|}{|Q_0|} \ .$$

Proof. By the assumption and (2.3), we have that

$$|Q_l| = |N(\mathfrak{a}_l)| < |\sqrt{D}| \ .$$

Thus, we can apply Theorem 4.1 to derive that $\mathfrak{a}_l$ is reduced. If $l = 1$, then $Q_{l-1} = Q_0$ and $|\overline{\theta}_1| = 1 = |\theta_1|$. Let $l \ge 2$. First, we notice that

$$|\overline{\alpha}_j| \ge 1 \quad (j \in \{1, \dots, l-2\} \ .$$

Since, if we assume that $|\overline{\alpha}_j| < 1$ for some index $j \in \{1, \dots, l-2\}$, then α_j is reduced. By the above remark, $\mathfrak{a}_{j+1}$ is reduced, and by Theorem 4.1 we conclude that $|Q_j| = |N(\mathfrak{a}_{j+1})| < |\sqrt{D}|$, which is a contradiction to the minimality of l with this property.

Furthermore, we know from [Ste99, Lemma 3.1] that α_l is not reduced. Since $l \ge 1$, this happens only if $|\overline{\alpha}_l| \ge 1$. Thus, we see from (5.5) that

$$|\overline{\theta}_{l+1}| = \frac{1}{|\overline{\alpha}_l|} \prod_{j=1}^{l-1} \frac{1}{|\overline{\alpha}_j|} \le 1 \ .$$

The final part of the theorem follows from (5.6). □

The latter Lemma gives an algorithmic criterion for recognizing an index l for which the ideal $\mathfrak{a}_l$ is reduced. Now, let $\mathfrak{b}$ be another reduced ideal which is equivalent to $\mathfrak{a} = \mathfrak{a}_1$. We would like to know if $\mathfrak{b}$ can appear among the ideals found by applying the continued fraction algorithm to $\mathfrak{a}$ in the above manner. The following theorem gives an answer to this question.

Theorem 5.3. *Let* $\mathfrak{a} = \mathfrak{a}_1$ *and* $\mathfrak{b}$ *be two equivalent reduced integral* $\mathcal{O}_K$*-ideals, and let* $\gamma \in \mathfrak{a}$ *be such that*

$$(\gamma)\mathfrak{b} = (N(\mathfrak{b}))\mathfrak{a} \ ,$$

where $0 < |\gamma| \le |N(\mathfrak{a})|$*. Then there exists some* $\nu \in \mathbb{N}$ *and* $c \in \mathbb{F}_q^{\,*}$ *such that* $\mathfrak{b} = \mathfrak{a}_\nu$ *and* $\gamma = cN(\mathfrak{a})\theta_\nu$*.*

Proof. The existence of such a $\gamma \in \mathfrak{a}$ can be guaranteed by Lemma 4.1. We prove the Theorem in several steps.

Step 1: There exists an index $\nu \in \mathbb{N}$ such that

$$|N(\mathfrak{a})\theta_{\nu+1}| < |\gamma| \leq |N(\mathfrak{a})\theta_\nu| \ .$$

proof(Step 1): Since $\mathfrak{a} = \mathfrak{a}_1$ is reduced, we know from Theorem 5.1 that α_i is reduced for $i \in \mathbb{N}$. Therefore $|\overline{\alpha_i}| < 1 < |\alpha_i|$. By (5.5) we get

$$|\theta_{i+1}| < |\theta_i| \ , \ |\theta_1| = 1 \quad \text{and} \quad |\overline{\theta}_{i+1}| > |\overline{\theta}_i| \ . \tag{5.9}$$

Also, we see that $|\theta_{i+1}| \leq \dfrac{1}{q^i}$, since $\deg(\alpha_i) \geq 1$ for $i \geq 1$. This means that $\{|\theta_i|\}_{i\in\mathbb{N}}$ is strictly decreasing and converges to 0. Since $0 < |\gamma| \leq |N(\mathfrak{a})|$, there must exist some $\nu \in \mathbb{N}$ such that

$$|\theta_{\nu+1}| < \frac{|\gamma|}{|N(\mathfrak{a})|} \leq |\theta_\nu| \ .$$

Step 2: We have that

$$|N(\mathfrak{a})\overline{\theta}_{\nu+1}| > |\overline{\gamma}| \ .$$

proof(Step 2): By Corollary 5.1, we have that $N(\mathfrak{a})\theta_{\nu+1} \in \mathfrak{a}$. Hence,

$$N(\mathfrak{a})\theta_{\nu+1}N(\mathfrak{b}) \in (N(\mathfrak{b}))\mathfrak{a} = (\gamma)\mathfrak{b}$$

and $N(\mathfrak{a})\theta_{\nu+1}N(\mathfrak{b}) = \gamma\beta$ for some $0 \neq \beta \in \mathfrak{b}$. From the first step, we see that $|\beta| < |N(\mathfrak{b})|$. Since $\mathfrak{b}$ is reduced, we can apply Lemma 4.2 to deduce that

$$|N(\mathfrak{b})| < |\overline{\beta}| = \frac{|N(\mathfrak{a})\overline{\theta}_{\nu+1}|}{|\overline{\gamma}|}|N(\mathfrak{b})| \ ,$$

and the assertion follows by deleting $|N(\mathfrak{b})|$ on both sides.

Step 3: There exists a $c \in {\mathbb{F}_q}^*$ such that $\gamma = c \cdot N(\mathfrak{a})\theta_\nu$.

proof(Step 3): Since $\gamma \in \mathfrak{a}$, Corollary 5.1 yields some polynomials $U, V \in k[x]$ such that

$$\gamma = UN(\mathfrak{a})\theta_\nu + VN(\mathfrak{a})\theta_{\nu+1} \quad \text{and} \quad \overline{\gamma} = UN(\mathfrak{a})\overline{\theta}_\nu + VN(\mathfrak{a})\overline{\theta}_{\nu+1} \ .$$

Suppose that $|U| \leq |V|$. Then,

$$|\overline{\gamma}| = |VN(\mathfrak{a})\overline{\theta}_{\nu+1}| \ .$$

It follows from the second step that we must have $|V| < 1$. Thus, $U = V = 0$ and $\gamma = 0$, which is a contradiction. Now, let $|U| > |V|$. Hence,

$$|\gamma| = |UN(\mathfrak{a})\theta_\nu| \ .$$

By using Step 1, we conclude that $|U| \leq 1$. Then $V = 0$ and $U = c$ for some $c \in \mathbb{F}_q{}^*$.

Step 4: We have that

$$N(\mathfrak{b}) = N(\mathfrak{a}_\nu) \ .$$

proof(Step 4): First, we apply Lemma 2.1 to (5.8) to obtain $N(\mathfrak{a})N(\theta_\nu) = c_1 N(\mathfrak{a}_\nu)$ for some $c_1 \in k^*$. Step 3 yields $N(\gamma) = c_2 N(\mathfrak{a})^2 N(\theta_\nu) = c_3 N(\mathfrak{a})N(\mathfrak{a}_\nu)$ for some $c_2, c_3 \in k^*$. On the other hand, $N(\gamma) = c_4 N(\mathfrak{b})N(\mathfrak{a})$ for some $c_4 \in k^*$, since $(\gamma)\mathfrak{b} = (N(\mathfrak{b}))\mathfrak{a}$. We find that $N(\mathfrak{b}) = N(\mathfrak{a}_\nu)$, since $\operatorname{sgn}(N(\mathfrak{b})) = \operatorname{sgn}(N(\mathfrak{a}_\nu)) = 1$.

Step 5: $\mathfrak{b} = \mathfrak{a}_\nu$.

proof(Step 5): By Step 4, we have that

$$(\gamma)\mathfrak{b} = (N(\mathfrak{b}))\mathfrak{a} = (N(\mathfrak{a}_\nu))\mathfrak{a} \ .$$

From (5.8) and Step 3, we know that the last term equals $(\gamma)\mathfrak{a}_\nu$. Thus, we must have that $\mathfrak{b} = \mathfrak{a}_\nu$. □

So far, we have proved that the continued fraction algorithm applied to a reduced ideal produces all equivalent, reduced ideals. This fact is essential for the establishment of our giant steps. In each $\mathcal{O}_K$-ideal class, we therefore have precisely on cycle of reduced ideals. Since k is finite, this cycle is finite. The continued fraction expansion applied to any primitive $\mathcal{O}_K$-ideal in a class yields a reduced $\mathcal{O}_K$-ideal in the same class after a finite number of steps and then produces all reduced ideals in the class. Thus, each ideal class can be represented by exactly one cycle of reduced ideals. Basically, one has a structure (the cycle of reduced ideals) within a structure (the ideal class group). This concept is called the *infrastructure* in real quadratic function fields and is due to Shanks [Sha72]. These considerations correspond to the observations made in real quadratic number fields (see also [Coh93]).

6 Distance and Giant Steps

We now introduce the concept of distance between equivalent, reduced ideals; this will allow us to provide an ordering of the reduced ideals belonging to the same ideal class. We will follow the notation of [SW88] which differs somewhat from that of [WW87]. Let $\mathfrak{a} = \mathfrak{a}_1$ and $\mathfrak{b}$ be two equivalent, reduced, integral $\mathcal{O}_K$-ideals. By Theorem 5.3, there exists some $\nu \in \mathbb{N}$ such that $\mathfrak{b} = \mathfrak{a}_\nu$, and by Theorem 5.1, we have $(N(\mathfrak{a})\theta_\nu)\mathfrak{a}_\nu = (N(\mathfrak{a}_\nu))\mathfrak{a}$. Then we define the *distance from* $\mathfrak{a}$ *to* $\mathfrak{b}$ as

$$\delta(\mathfrak{b}, \mathfrak{a}) = \delta(\mathfrak{a}_\nu, \mathfrak{a}) := \deg(\overline{\theta}_\nu) \ . \tag{6.1}$$

Remark 6.1. *Distance is only defined between equivalent, reduced ideals. From (5.5) and because $\mathfrak{a}_i$ is reduced for $i \geq 1$, we deduce that the distance function δ_i is strictly increasing in i, i.e. $\delta(\mathfrak{a}_{i+1}, \mathfrak{a}) > \delta(\mathfrak{a}_i, \mathfrak{a})$. Since the values of the distance function are integers, we have $\delta_{t+i} \geq \delta_t + i$. Thus, if $\delta(\mathfrak{a}_i, \mathfrak{a}) = \delta(\mathfrak{a}_j, \mathfrak{a})$, we conclude that $\mathfrak{a}_i = \mathfrak{a}_j$. Especially, if there are $\nu, j, l \in \mathbb{N}$ such that $\delta(\mathfrak{a}_j, \mathfrak{a}) \leq \delta(\mathfrak{a}_\nu, \mathfrak{a}) \leq \delta(\mathfrak{a}_l, \mathfrak{a})$, then $\mathfrak{a}_\nu \in \{\mathfrak{a}_i; j \leq i \leq l\}$, and $\delta(\mathfrak{a}_i, \mathfrak{a}) = 0$ if and only if $\mathfrak{a}_i = \mathfrak{a}_1$. Conversely, if $\mathfrak{a}_i = \mathfrak{a}_j$ then $\delta(\mathfrak{a}_i, \mathfrak{a}) = \delta(\mathfrak{a}_j, \mathfrak{a}) + lR$, where R is the regulator of K. In this case, we deduce from Theorem 5.1 that $\overline{\theta}_i$ and $\overline{\theta}_j$ differ only by a $\mathcal{O}_K$-unit.*

Furthermore, by (5.6), (5.5), and [Ste99, Proposition 3.1], we know that

$$\delta(\mathfrak{a}_i, \mathfrak{a}) = \tfrac{1}{2}\deg(D) - \deg(Q_0) + \sum_{j=1}^{i-2} \deg(a_j) \quad (i \in \mathbb{N}, i \geq 2) \ . \tag{6.2}$$

In the sequel, we let $\mathfrak{r} = \mathfrak{r}_1 = (1) = \mathcal{O}_K = [1, \sqrt{D}]$. With reference to (5.2), we have $P_0 = P = 0$, $Q_0 = Q = 1$ and $\alpha_0 = \alpha = \sqrt{D}$. Clearly, $\mathfrak{r}$ is reduced, because $|N(\mathfrak{r})| = 1 < |\sqrt{D}|$. By Theorem 5.1 and (5.6), the ideals in (5.2) are reduced principal ideals, i.e. $\mathfrak{r}_{i+1} = (\overline{\theta}_{i+1})$, for $i \in \mathbb{N}_0$, where $\overline{\theta}_{i+1} \in \mathcal{O}_K$. We always put $\delta_i := \delta(\mathfrak{r}_i, \mathfrak{r})$. Then δ_i is defined for all $i \in \mathbb{N}$. Let $\mathfrak{b}$ be an arbitrary reduced $\mathcal{O}_K$-ideal. We develop the continued fraction expansion of $\mathfrak{b}$ as in (5.2) and denote by P_i', Q_i', θ_i' and $\delta_i' := \delta(\mathfrak{b}_i, \mathfrak{b})$ the quantities appearing in the continued fraction expansion applied to $\mathfrak{b}$. For any $s, t \in \mathbb{N}$, we find a polynomial $S \in k[x]$ and a primitive $\mathcal{O}_K$-ideal $\mathfrak{c}$ such that $\mathfrak{r}_s\mathfrak{b}_t = (S)\mathfrak{c}$. We apply the continued fraction algorithm to $\mathfrak{c} = \mathfrak{c}_1$. By Theorem 5.2, it is guaranteed that, after a finite number of steps, we obtain a reduced ideal equivalent to $\mathfrak{c}$. We denote by

P_i'', Q_i'' and θ_i'' the quantities appearing in the continued fraction expansion applied to $\mathfrak{c}$. In view of Lemma 5.2, let $l \in \mathbb{N}$ minimal such that $|Q_{l-1}''| < |\sqrt{D}|$; hence, $\mathfrak{c}_l$ is reduced. Summarizing, we get the following chain of equivalent ideals

$$\mathfrak{c}_l \sim \mathfrak{c} \sim (S)\mathfrak{c} = \mathfrak{r}_s\mathfrak{b}_t = (\overline{\theta}_s)\mathfrak{b}_t \sim \mathfrak{b}_t \sim \mathfrak{b} \ .$$

Thus, $\mathfrak{c}_l$ and $\mathfrak{b}$ are equivalent. Since they both are reduced, by Theorem 5.3 there must exist some $\nu \in \mathbb{N}$ such that $\mathfrak{c}_l = \mathfrak{b}_\nu$.

Theorem 6.1. *In above situation there exists some $C \in k^*$ such that*

$$\theta_\nu' = C\theta_s\,\theta_t'\,\frac{\theta_l''}{S} \ .$$

Furthermore, we have that

$$\delta_\nu' = \delta_t' + \delta_s - f \ ,$$

where $f := \deg(S) - \deg(\overline{\theta_l''}) \in \mathbb{N}$ is such that $0 \le f \le 2g$.

Proof. From (5.8), we see that

$$(\theta_s)\mathfrak{r}_s = (N(\mathfrak{r}_s)) \ ,$$
$$(N(\mathfrak{b})\theta_t')\mathfrak{b}_t = (N(\mathfrak{b}_t))\mathfrak{b} \ ,$$

and

$$(N(\mathfrak{c})\theta_l'')\mathfrak{c}_l = (N(\mathfrak{c}_l))\mathfrak{c} \ .$$

Since $\mathfrak{r}_s\mathfrak{b}_t = (S)\mathfrak{c}$, we can apply Lemma 2.1 to conclude that

$$N(\mathfrak{r}_s)N(\mathfrak{b}_t) = C_1 \cdot S^2 N(\mathfrak{c})$$

for some constant $C_1 \in k^*$. This yields

$$(N(\mathfrak{b})N(\mathfrak{c})S\theta_s\theta_t'\theta_l'')\mathfrak{c}_l = (S^2N(\mathfrak{c})N(\mathfrak{c}_l))\mathfrak{b} \ .$$

Hence,

$$0 \neq \gamma := \frac{N(\mathfrak{b})N(\mathfrak{c})S\theta_s\theta_t'\theta_l''}{S^2N(\mathfrak{c})N(\mathfrak{c}_l)} \cdot N(\mathfrak{c}_l) = \theta_s\theta_t'\theta_l'' \cdot \frac{N(\mathfrak{b})}{S}d \ \in \ \mathfrak{b} \ .$$

γ also has the property that $(\gamma)\mathfrak{c}_l = (N(\mathfrak{c}_l))\mathfrak{b}$. We also derive from (5.9) that

$$0 < |\gamma| \leq |N(\mathfrak{b})| \ .$$

Theorem 5.3 then says that there must exist some $\nu \in \mathbb{N}$ and a constant $C_2 \in k^*$ such that

$$\gamma = C_2 N(\mathfrak{b})\theta'_\nu \ .$$

By comparing this with the definition of γ, we find that

$$\theta'_\nu = C \cdot \theta_s \theta'_t \frac{\theta''_l}{S}$$

for some $C \in k^*$. Conjugation yields

$$\delta'_\nu = \delta'_t + \delta_s - f \ .$$

Finally, by (5.9), (5.8), and (5.6) we obtain

$$\frac{|\overline{\theta''_l}|}{|S|} \geq \frac{|\overline{\theta''_l}\theta''_l|}{|S|} \geq \frac{|N(\mathfrak{c}_l)|}{|S||N(\mathfrak{c})|} \geq \frac{1}{|N(\mathfrak{r}_s)||N(\mathfrak{b}_t)|} \ ,$$

since $|N(\mathfrak{r}_s)N(\mathfrak{b}_t)| = |S^2 N(\mathfrak{c})|$ and $0 \neq S \in k[x]$. Equivalently, we have that

$$f \leq \deg(N(\mathfrak{r}_s)) + \deg(N(\mathfrak{b}_t)) \leq 2g \ ,$$

since $\mathfrak{r}_s$ and $\mathfrak{b}_t$ are reduced, and from Theorem 4.1 we deduce

$$\deg(N(\mathfrak{r}_s)), \deg(N(\mathfrak{b}_t)) \leq \frac{1}{2}\deg(D) - 1 = g \ .$$

Thus, we proved the upper bound on f. The lower bound trivially follows from Lemma 5.2. □

Note that the quantities s, t can be arbitrarily large here, but l is bounded by a fixed small quantity which depends on D. Furthermore, the integer f, the "error", is bounded and is always nonnegative. In general, f is small compared to δ_s or δ'_t. The result is of special interest for large s, t. As in the number field case, we expect the distance function to be roughly linear. Therefore, we really have large steps. In the situation of the Theorem we define a new operation called *giant step* by

$$\mathfrak{r}_s * \mathfrak{b}_t := (\mathfrak{b}_\nu, f) = (\mathfrak{c}_l, f) \ . \tag{6.3}$$

Consequently, a giant step is a composition of two operations, namely computation of the product of two primitive $\mathcal{O}_K$-ideals and reduction of the primitive part of the product using the continued fraction algorithm.

So far, we haven't used any information about periodicity and symmetry. Let m be the quasi-period of the continued fraction expansion of $\alpha = \sqrt{D}$. From [Ste99, Theorem 4.2], we deduce that $\mathfrak{r}_{m+1} = \mathfrak{r}_1 = \mathfrak{r} = \mathcal{O}_K$, since $Q_m \in k^*$. Furthermore, $\epsilon = \overline{\theta}_{m+1}$ is a fundamental unit of K; thus, we see that $R = \delta_{m+1}$, where R is the regulator of K. By induction (see [Ste99, Proposition 3.2]), we get

$$\mathfrak{r}_{\lambda m+i+1} = \mathfrak{r}_{i+1} \quad (i \in \mathbb{N}) \ . \tag{6.4}$$

Also, by [Ste99, Lemma 2.1, Lemma 4.1], and 5.5, we get

$$\delta_{\lambda m+i+1} = \lambda \cdot R + \delta_{i+1} \quad (i, \in \mathbb{N}) \ . \tag{6.5}$$

By Remark 6.1 and (6.2) with $t := 2$ and $i = t + (i-2)$ we have that

$$\delta_i \geq \frac{1}{2}\deg(D) + i - 2 = g + i - 1 \quad (i \in \mathbb{N}, i \geq 2) \ . \tag{6.6}$$

Finally, we consider the effects of symmetries in the case $\alpha = \sqrt{D}$. We continue applying the continued fraction algorithm to $\mathfrak{r}_1 = \mathfrak{r} = \mathcal{O}_K$. For $\mathfrak{r}_i$ defined in (5.2), we get

$$\overline{\mathfrak{r}}_i = [Q_{i-1}, -P_{i-1} + \sqrt{D}] = [Q_{i-1}, P_i + \sqrt{D}] \quad (i \in \mathbb{N}) \ , \tag{6.7}$$

where $\overline{\mathfrak{r}}_i$ denotes the conjugate ideal of $\mathfrak{r}_i$.

Proposition 6.1. *Let $\tilde{\delta}_i := \delta(\overline{\mathfrak{r}}_i, \mathfrak{r})$. Then, we have for $i = 1, 2, \ldots, m+1$:*

1. $\overline{\mathfrak{r}}_i = \mathfrak{r}_{m-i+2}$;
2. $\tilde{\delta}_i = \delta_{m-i+2}$;
3. $R = \tilde{\delta}_i + \delta_i - \deg(Q_{i-1})$.

Proof. This follows easily from [Ste99, Theorem 4.4] and (5.6). □

We see that the conjugate ideals are exactly those which occur before the quasi-period is reached and they can be easily computed from the original ideals.

References

[Art24] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen I, II. *Math. Zeitschr.*, 19:153–206, 1924.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin, 1993.

[Deu73] M. Deuring. *Lectures on the Theory of Algebraic Functions of One Variable.* Number 314 in Lect. Notes in Math. Springer-Verlag, Berlin, 1973.

[Len82] H. W. Lenstra. On the calculation of regulators and class numbers of quadratic fields. *London. Math. Soc. Lec. Note Ser.*, 56:123–150, 1982.

[Sch31] F. K. Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik p. *Mathematische Zeitschrift*, 33:1–32, 1931.

[Sha71] D. Shanks. Class number, a theory of factorization and genera. In *Proc. Symp. Pure Math. 20*, pages 415–440. AMS, Providence, R.I., 1971.

[Sha72] D. Shanks. The infrastructure of a real quadratic field and its applications. In *Proc. 1972 Number Th. Conf., Boulder, Col.*, pages 217–224, 1972.

[Ste99] A. Stein. Introduction to continued fraction expansions in real quadratic function field. Technical Report CORR 99-15, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, 1999. 23 pages.

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer, Berlin, 1993.

[SW88] A. Stephens and H. C. Williams. Some computational results on a problem concerning powerful number. *Mathematics of Computation*, 50:619–632, 1988.

[WW87] H. C. Williams and M. C. Wunderlich. On the parallel generation of the residues for the continued fraction algorithm. *Mathematics of Computation*, 48:405–423, 1987.

[Zuc97] R. Zuccherato. The continued fraction algorithm and regulator for quadratic function fields of characteristic 2. *Journal of Algebra*, 190:563–587, 1997.