Introduction to Continued Fraction Expansions 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 20, 1999

Abstract

Since the continued fraction expansion in real quadratic function fields is a basic tool for performing arithmetics in these fields, we provide an elementary introduction to the polynomial continued fraction expansion. Hereby, we present properties that are in complete analogy to the integer continued fraction expansion. In particular, we prove symmetries with respect to the quasi-period and show how they can be used in baby step algorithms for computing regulators and fundamental units.

1 Introduction

Since any hyperelliptic function field can be represented as a real quadratic function field, it is important to investigate the continued fraction expansion in real quadratic function fields in detail. We summarize some basic properties and provide elementary proofs of some results. In this view, this paper is intended as a "low-brow" approach to the theory of continued fraction expansions of Puiseux series. For the number-theoretic background, we refer to the excellent book of Stichtenoth [Sti93]. For the purpose of this paper, only an elementary knowledge of the subject is needed, and we mainly follow the introductory notes of Artin [Art24].

Let $k = \mathbb{F}_q$ be a finite field of odd characteristic and let $K = k(x)(\sqrt{D})$, where D is a monic, squarefree polynomial of even degree. Such a field is known as a *real quadratic function field* over k (of odd characteristic). Continued fraction expansions in K can be used to compute fundamental units and regulators. For real quadratic function fields of characteristic 2, we refer to [Zuc97]. In this paper, we define continued fraction expansions in the sense of Artin [Art24], and we follow the notations in [WW87, SW88b, SW88a]. Further references are [Per13, AR80]. Indeed, we obtain formulas analogous to those ones derived in number fields. Note that many results concerning continued fractions are valid over any field k.

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 $\mathcal{O}_K$. 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. Because there are exactly two extensions of the infinite place from $k(x)$ to K we can conclude from the Dirichlet unit theorem (see for example [Wei63]) 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

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

the *regulator of K/k with respect to $\mathcal{O}_K$*. The computation of the regulator and the fundamental unit will be our main application of the continued fraction algorithm. We remark here that the regulator is one of the important invariants in real quadratic function fields. A result of F. K. Schmidt [Sch31] shows its connection to further invariants, namely

$$h = R \cdot h' \,,$$

where h' denotes the ideal class number of K with respect to $\mathcal{O}_K$ and h the divisor class number of K. The meaning of these quantities is described in [Art24, Deu73]. The classical method to calculate the fundamental unit of K and the regulator of K is based on the continued fraction expansion of $\alpha = \sqrt{D}$. Therefore let $L := k(x)_{\mathfrak{P}_\infty}$ be the completion of $k(x)$ with respect to $\mathfrak{P}_\infty$. Then L is the field of Puiseux series and the completions of K with respect to $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are isomorphic to L:

$$K_{\mathfrak{P}_1} \cong K_{\mathfrak{P}_2} \cong k(x)_{\mathfrak{P}_\infty} = k((1/x)).$$

Also, K is a subfield of $k((1/x))$, $K \leq k((1/x))$. Now, we only have to fix one of the two places. Let $\mathfrak{P}_1$ be the place which corresponds to the case where $\sqrt{1} = 1$. Then we define continued fraction expansion in K via Puiseux series at $\mathfrak{P}_1$ in the variable $1/x$.

2 Continued Fractions in the Fields of Puiseux Series

In this chapter, k can be an arbitrary field. If k is not finite, then we put $q = 2$. 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

$$\left\{ \begin{array}{rcl} \deg(\alpha) & = & m \\ |\alpha| & = & q^m \\ \operatorname{sgn}(\alpha) & = & c_m \\ \lfloor \alpha \rfloor & = & \sum_{i=0}^{m} c_i x^i . \end{array} \right\} \tag{2.1}$$

If m is negative, then we have that $\lfloor \alpha \rfloor = 0$. For completeness, we set $\deg(0) = -\infty$ and $|0| = 0$. Now, we introduce continued fraction expansions in L in the sense of Artin. Let $\alpha \in L$ and

$$\left\{ \begin{array}{ll} \alpha_0 := \alpha & , \quad a_0 := \lfloor \alpha_0 \rfloor \\ \\ \alpha_{i+1} := \dfrac{1}{\alpha_i - a_i} & , \quad a_{i+1} := \lfloor \alpha_{i+1} \rfloor \end{array} \right\} \tag{2.2}$$

Because $\lfloor \alpha \rfloor$ is the unique polynomial such that $|\alpha - \lfloor \alpha \rfloor| < 1$, we note that

$$|\alpha_i| = |a_i| \geq q > 1 \qquad (i \in \mathbb{N}) \ . \tag{2.3}$$

We get

$$\alpha = \alpha_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}} =: [\, a_0,\, a_1,\, a_2,\, \ldots] \ . \tag{2.4}$$

As usual, we define

$$\left\{ \begin{array}{lll} p_{-2} := 0 & ; & q_{-2} := 1 \\ \\ p_{-1} := 1 & ; & q_{-1} := 0 \\ \\ p_i \ \ := a_i p_{i-1} + p_{i-2} & ; & q_i \ \ := a_i q_{i-1} + q_{i-2} \quad (i \in \mathbb{N}_0) \end{array} \right\} \ . \tag{2.5}$$

We derive by induction that

$$|q_i| > |q_{i-1}| \qquad \text{and} \qquad |q_i| \geq q^i \qquad (i \in \mathbb{N}_0) \ . \tag{2.6}$$

The polynomials p_i and q_i satisfy

$$\frac{p_i}{q_i} = [\, a_0,\, a_1,\, a_2,\, \ldots\, ,\, a_i \,] \ , \tag{2.7}$$

$$\alpha = \frac{p_i \alpha_{i+1} + p_{i-1}}{q_i \alpha_{i+1} + q_{i-1}} \qquad (i \geq -1) \ , \tag{2.8}$$

or, equivalently,

$$\alpha_{i+1} = -\frac{q_{i-1}\alpha - p_{i-1}}{q_i \alpha - p_i} \qquad (i \geq -1) \ . \tag{2.9}$$

Furthermore,

$$q_i p_{i-1} - p_i q_{i-1} = (-1)^i \qquad (i \geq -1) \tag{2.10}$$

and

$$\alpha - \frac{p_i}{q_i} = \frac{(-1)^i}{q_i(q_i \alpha_{i+1} + q_{i-1})} \qquad (i \geq -1)\ . \tag{2.11}$$

For an $\alpha \in L$ we put

$$\theta_1 := 1 \qquad \theta_{i+1} := \prod_{j=1}^{i} \frac{1}{\alpha_j}\ , \tag{2.12}$$

and we derive from (2.9) and (2.12) that

$$\theta_{i+1} = (-1)^i \,(p_{i-1} - \alpha q_{i-1}) \qquad (i \in \mathbb{N}_0)\ . \tag{2.13}$$

In contrast to real quadratic number fields it doesn't suffice to analyze the period of the continued fraction expansion of quadratic irrationalities because the quasi-period plays a more important role. Therefore, we have to distinguish two forms of periodic behavior. Let $\alpha \in L$. We say the continued fraction expansion of α is *quasi-periodic* if there are integers $\nu > \nu_0 \geq 0$ and a constant $c \in k^*$ such that

$$\alpha_\nu = c\, \alpha_{\nu_0} \qquad . \tag{2.14}$$

The smallest positive integer $\nu - \nu_0$ for which (2.14) holds is called the *quasi-period* of the continued fraction expansion of α. The continued fraction expansion of α is called *periodic* if (2.14) holds with $c = 1$. The smallest positive integer $\nu - \nu_0$ for which (2.14) holds with $c = 1$ is called the *period* of the continued fraction expansion of α. From [W2], Proposition 3.5, we know:

Proposition 2.1. *If the continued fraction expansion of $\alpha \in L$ is periodic with period n, then it is quasi-periodic with quasi-period m and m divides n.*

It is easy to see that for an element $\alpha \in L$ the period n and the quasi-period m start at the same index ν_0. That means the nonnegative integer ν_0 is minimal such that

$$\alpha_{\nu_0+m} = c\, \alpha_{\nu_0} \qquad \text{and} \qquad \alpha_{\nu_0+n} = \alpha_{\nu_0} \tag{2.15}$$

with $c \in k^*$. By induction we get the following helpful lemma:

Lemma 2.1. *If the continued fraction expansion of an element $\alpha \in L$ is quasi-periodic with quasi-period m then, with ν_0 and c chosen as in (2.15), we have that*

$$\alpha_{i+\lambda m} = c_i^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}}\ \alpha_i \qquad (i \geq \nu_0\ ,\ \lambda \geq 0) \quad ,$$

where $c_i := c^{(-1)^{i-\nu_0}}$.

To obtain more information about the relation between the period and the quasi-period we have to distinguish between even and odd periods. In special cases, we will obtain explicit results for even periods.

Corollary 2.1. *Let α be an arbitrary element of L.*

1. *If the continued fraction expansion of α is quasi-periodic with odd quasi-period m, then it is periodic with period n, and $n = m$ or $n = 2m$.*
2. *If the continued fraction expansion of α is periodic with odd period, then it is quasi-periodic with quasi-period $m = n$.*

Proof. The first assertion is clear from the above lemma. The second assertion immediately follows from the first assertion and Proposition 2.1. □

3 Real Quadratic Irrationalities and Reduction

Now, let k be a field of odd characteristic. We consider the continued fraction expansion of expressions of the form

$$\alpha = \frac{P + \sqrt{\Delta}}{Q} \qquad (\ 0 \neq Q,\ P,\ \Delta\ \in\ k[x]\ ) \quad , \tag{3.1}$$

where $\alpha \in L - k(x)$, $0 < \deg(\Delta)$ even, Δ not a perfect square in $k[x]$, and $Q \mid (\Delta - P^2)$. We call such an element a *real quadratic irrationality*. In this situation, we put $Q_0 = Q$, $P_0 = P$, $\alpha_0 = \alpha$, $Q_{-1} = (\Delta - P^2)/Q$, and $d = \lfloor \sqrt{\Delta} \rfloor$. For $i \in \mathbb{N}_0$ we use the recursions

$$\left\{ \begin{array}{l} P_{i+1} = a_i Q_i - P_i\ ; \\[2ex] Q_{i+1} = \dfrac{\Delta - P_{i+1}^2}{Q_i}\ ; \end{array} \right\} \tag{3.2}$$

We immediately have

$$\alpha_i = \frac{P_i + \sqrt{\Delta}}{Q_i} \qquad (i \in \mathbb{N}_0) \ , \tag{3.3}$$

where $0 \neq Q_i, P_i \in k[x]$ and $Q_i | (\Delta - P_i^2)$. We compute $a_i = \lfloor \alpha_i \rfloor$ by

$$a_i = (P_i + d) \operatorname{div} Q_i \qquad (i \in \mathbb{N}_0) \ . \tag{3.4}$$

First, wee see from (3.2) that

$$Q_i = Q_{i-1} + a_i(P_i - P_{i+1}) \qquad (i \in \mathbb{N}_0) \ . \tag{3.5}$$

Defining $r_i \in k[x]$ to be the remainder by dividing $P_i + d$ through Q_i, i.e.

$$P_i + d = a_i Q_i + r_i \quad \text{, where } \ 0 \leq \deg(r_i) < \deg(Q_i) \qquad (i \in \mathbb{N}_0) \ , \tag{3.6}$$

we then optimize the formulas as follows:

$$\left\{ \begin{array}{lll} P_{i+1} = d - r_i & (i \in \mathbb{N}_0) & ; \\ Q_{i+1} = Q_{i-1} + a_i(r_i - r_{i-1}) & (i \in \mathbb{N}) & ; \\ a_i = (P_i + d\,) \operatorname{div} Q_i & (i \in \mathbb{N}_0) & ; \\ r_i = (P_i + d\,) \bmod Q_i & (i \in \mathbb{N}_0) & . \end{array} \right\} \tag{3.7}$$

We notice that the computation of r_i causes no further efforts. Also, by applying (3.3) to (2.9) and comparing rational and irrational parts, we get for $i \in \mathbb{N}_0$:

$$\left\{ \begin{array}{l} \Delta q_{i-1} = P_i(p_{i-1}Q_0 - P_0 q_{i-1}) + Q_i(p_{i-2}Q_0 - P_0 q_{i-2}) \ ; \\ Q_0 P_{i-1} = q_{i-1}P_i + q_{i-2}Q_i + P_0 q_{i-1} \ . \end{array} \right\} \tag{3.8}$$

Finally, we deduce that

$$\mathrm{N}(\theta_{i+1}) = \theta_{i+1}\overline{\theta}_{i+1} = (-1)^i \, \frac{Q_i}{Q_0} \qquad (i \in \mathbb{N}_0) \ . \tag{3.9}$$

A real quadratic irrationality is called *reduced*, if $|\overline{\alpha}| < 1 < |\alpha|$, where $\overline{\alpha}$ is the conjugate of α. In view of (3.1), the conjugate of α is $\overline{\alpha} = (P - \sqrt{\Delta})/Q$. So, α is reduced if and only if

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

Remark 3.1. *If the real quadratic irrationality α of the form (3.1) is reduced, then we have:*

1. $|P| = |\sqrt{\Delta}\,| = |d|$.
2. $sgn(P) = sgn(\sqrt{\Delta}) = sgn(d)$. *Even the two highest coefficients must be equal.*
3. $|Q| < |\sqrt{\Delta}| = |P + \sqrt{\Delta}\,|$.

The proof of this remark is easy and can be found in [Art24, p.194]. Also Artin, showed that if α_i is reduced for $i \in \mathbb{N}_0$, then α_j is reduced for $j \geq i$. Combining this fact with the above remark and (3.2) we get the following

Proposition 3.1. *If, in the continued fraction expansion of a real quadratic irrationality α, it happens that α_{i_0} is reduced for some $i_0 \geq 0$, then it follows for $i \geq i_0$:*

1. $|P_i| = |P_i + \sqrt{\Delta}\,| = |\sqrt{\Delta}\,| = |d|$.
2. $sgn(P_i) = sgn(\sqrt{\Delta}) = sgn(d)$. *Even the two highest coefficients must be equal.*
3. $|a_i Q_i| = |\sqrt{\Delta}|$. *In particular, we have that* $1 < |a_i| \leq |\sqrt{\Delta}\,|$, $1 \leq |Q_i| < |\sqrt{\Delta}\,|$.

It is well-known that the continued fraction algorithm can be interpreted as a reduction process. In the continued fraction expansion of a real quadratic irrationality there is an index $i_0 \geq 0$ such that α_i is reduced for $i \geq i_0$. We give an explicit bound for this index i_0. But, this bound is not minimal and can not be used for algorithmic purposes. In fact, we are able to solve this problem. Hereby, we apply the same beautiful ideas that Kaplan and Williams [KW90] used to prove the corresponding sharp result in real quadratic number fields.

Theorem 3.1. *Let α be a real quadratic irrationality. Then α_i is reduced for*

$$i > i_0 := \max\left\{ 0\,,\ \tfrac{1}{2}\deg(Q_0) - \tfrac{1}{4}\deg(\Delta) + 1 \right\}\ .$$

Proof. Let $i \in \mathbb{N}$ be chosen such that $i > i_0$. First, note that $i \in \mathbb{N}$, and we know from (2.3) that $|\alpha_i| > 1$. Now, $i > i_0$ is equivalent to

$$\frac{|Q_0|}{|\sqrt{\Delta}|} < q^{2i-2}\ .$$

From (2.6) we know that $|q_{i-1}| \geq q^{i-1}$ and therefore

$$|\alpha_0 - \overline{\alpha}_0| = \left| \frac{P_0 + \sqrt{\Delta}}{Q_0} - \frac{P_0 - \sqrt{\Delta}}{Q_0} \right| = \frac{|\sqrt{\Delta}\,|}{|Q_0|} > \frac{1}{|q_{i-1}|^2} \,.$$

On the other side, we get from (2.10) and (2.11) for $i \in \mathbb{N}_0$:

$$(-1)^i(\alpha - \overline{\alpha}) = \frac{1}{q_{i-1}(q_{i-1}\overline{\alpha}_i + q_{i-2})} - \frac{1}{q_{i-1}(q_{i-1}\alpha_i + q_{i-2})} \,. \tag{3.10}$$

Assuming that α_i is not reduced, i.e. $|\overline{\alpha}_i| \geq 1$, we have that

$$|q_{i-1}\alpha_i + q_{i-2}| = |q_{i-1}\alpha_i| \quad \text{and} \quad |q_{i-1}\overline{\alpha}_i + q_{i-2}| = |q_{i-1}\overline{\alpha}_i| \,.$$

Hence,

$$\begin{aligned} |\alpha_0 - \overline{\alpha}_0| &\leq \max\left\{ \frac{1}{|q_{i-1}||q_{i-1}\overline{\alpha}_i + q_{i-2}|}, \frac{1}{|q_{i-1}||q_{i-1}\alpha_i + q_{i-2}|} \right\} \\ &= \frac{1}{|q_{i-1}|^2} \max\left\{ \frac{1}{|\overline{\alpha}_i|}, \frac{1}{|\alpha_i|} \right\} \\ &\leq \frac{1}{|q_{i-1}|^2} \,, \end{aligned}$$

because $|\alpha_i| > 1$, and, by assumption, $|\overline{\alpha}_i| \geq 1$. This leads to a contradiction, and the assertion is proved. $\square$

Theorem 3.2. *Let α be a real quadratic irrationality and let $i \in \mathbb{N}_0$. Then α_{i+1} is reduced if and only if $|Q_i| < |\sqrt{\Delta}\,|$.*

Proof. If α_{i+1} is reduced, we have by definition that $|\overline{\alpha}_{i+1}| < 1 < |\alpha_{i+1}|$. From (3.2) and (3.3) it is easy to see that

$$\overline{\alpha}_{i+1} = \frac{P_{i+1} - \sqrt{\Delta}}{Q_{i+1}} \cdot \frac{P_{i+1} + \sqrt{\Delta}}{P_{i+1} + \sqrt{\Delta}} = -\frac{Q_i}{P_{i+1} + \sqrt{\Delta}} \,. \tag{3.11}$$

Together with Proposition 3.1, we have that

$$\begin{aligned} |Q_i| &= |\overline{\alpha}_{i+1}||P_{i+1} + \sqrt{\Delta}\,| \\ &= |\overline{\alpha}_{i+1}||\sqrt{\Delta}\,| \\ &< |\sqrt{\Delta}\,| \,. \end{aligned}$$

Conversely, let $i \in \mathbb{N}_0$ with $|Q_i| < |\sqrt{\Delta}\,|$. By (2.3) we have to show that $|\overline{\alpha}_{i+1}| < 1$ or, equivalently, that $|P_{i+1} - \sqrt{\Delta}\,| < |Q_{i-1}|$. From (3.7) we know that $P_{i+1} = d - r_i$, and by (3.6) we then obtain that

$$0 \le |r_i| < |Q_i| < |\sqrt{\Delta}\,| = |d| \ .$$

Because the characteristic of k is different from 2, we deduce that

$$|P_{i+1} + \sqrt{\Delta}\,| = |\sqrt{\Delta}\,| = |P_{i+1}| \ .$$

Substituting this into (3.2), we get

$$\begin{aligned} |Q_{i+1}| &= \frac{|\Delta - P_{i+1}^2|}{|Q_i|} = \frac{|\sqrt{\Delta} + P_{i+1}|}{|Q_i|} \cdot |\sqrt{\Delta} - P_{i+1}| \\ &= \frac{|\sqrt{\Delta}|}{|Q_i|} \cdot |\sqrt{\Delta} - P_{i+1}| \\ &> |\sqrt{\Delta} - P_{i+1}| \ , \end{aligned}$$

by assumption. □

Lemma 3.1. *Let α be a real quadratic irrationality. If there exists a minimal $i_0 \in \mathbb{N}$ such that $|Q_{i_0}| < |\sqrt{\Delta}|$, i.e. $|Q_j| \ge |\sqrt{\Delta}|$ for $j \in \{0, \ldots, i_0 - 1\}$, then α_{i_0} is not reduced.*

Proof. (3.11) together with the assumption leads to

$$|\,\overline{\alpha}_{i_0}\,| = \frac{|\,Q_{i_0-1}\,|}{|\,P_{i_0} + \sqrt{\Delta}\,|} \ge \frac{|\,\sqrt{\Delta}\,|}{|\,P_{i_0} + \sqrt{\Delta}\,|} \ .$$

Suppose that α_{i_0} is reduced. We then deduce from Proposition 3.1 that

$$|\,\overline{\alpha}_{i_0}\,| \ge \frac{|\,\sqrt{\Delta}\,|}{|\,\sqrt{\Delta}\,|} = 1 \ ,$$

which gives a contradiction. □

We are now able to provide a simpler proof of Theorem 3.1 by using the above lemma, (2.12), and (3.9). Let $l \in \mathbb{N}$ be minimal such that α_{l+1} is reduced. It follows from Theorem 3.2 that $\deg(Q_l) \le \deg(\Delta)/2 - 1$, and we then have that α_i is reduced for $i \ge l + 1$. However, we derive from the above lemma that α_l is not reduced. Thus, by

Theorem 3.2, we have that $\deg(Q_{l-1}) \geq \deg(\Delta)/2$ and $\deg(\overline{\alpha}_l) \geq 0$. Since we also have that α_i is not reduced for $i = 1, \ldots, l-1$, we must have that $\deg(\alpha_i) \geq 1$ and that $\deg(\alpha_i) = \deg(\overline{\alpha}_i) = \deg(P_i) - \deg(Q_i) \geq 1$ $(1 \leq i \leq l-1)$. By (2.12), and (3.9), we then easily see that

$$\begin{aligned} \deg(Q_0) &= \deg(Q_{l-1}) + \sum_{i=1}^{l-1} \deg(\alpha_i) + \sum_{i=1}^{l-1} \deg(\overline{\alpha}_i) \\ &\geq \tfrac{1}{2}\deg(\Delta) + 2(l-1)\ , \end{aligned}$$

or, equivalently,

$$l \leq \tfrac{1}{2}\deg(Q_0) - \tfrac{1}{4}\deg(\Delta) + 1\ .$$

The bounds in Proposition 3.1 and Theorem 3.2 for the polynomials P_i and Q_i lead to the periodicity of the continued fraction expansion of a real quadratic irrationality in the case of a finite field k. Now, we summarize our results in the following theorem. We remark that the proof of "3. $\Rightarrow$ 1." can be shown similar to [Ros93, Lagrange's Theorem].

Theorem 3.3. *Let α be an element of $L - k(x)$, where k is a finite field of odd characteristic. Then the following statements are equivalent:*

1. *The continued fraction expansion of α is periodic.*
2. *The continued fraction expansion of α is quasi-periodic.*
3. *α is a real quadratic irrationality.*

Next, we state that the reduction of a real quadratic irrationality by means of the continued fraction algorithm is equivalent to the computation of the pre-period. This is a well-known result and can be shown as in the case of a real number quadratic number field (see for example [Per13]).

Theorem 3.4. *If the continued fraction expansion of the real quadratic irrationality $\alpha \in L$ is periodic, then it is pure periodic, i.e. the period begins at $\nu_0 = 0$, if and only if α is reduced.*

Finally, we develop properties for the polynomials P_i and Q_i in view of their periodic behavior. We apply Lemma 2.1 to (3.3) and obtain

Proposition 3.2. *If the continued fraction expansion of a real quadratic irrationality α is quasi-periodic with quasi-period m and $\nu_0 \geq 0$, then we have for $i \geq \nu_0$ and $\lambda \geq 1$ that*

$$\begin{aligned} P_i &= P_{i+\lambda m} \quad , \\ Q_i &= c_i^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}} Q_{i+\lambda m} \ , \end{aligned}$$

where $c_i := c^{(-1)^{i-\nu_0}}$ and $c \in k^*$ is defined as in (2.15),

4 Symmetries

The case $\alpha = \sqrt{D}$ plays a particular role because the fundamental unit of a real quadratic function field $k(x)(\sqrt{D})$ can be calculated by applying the continued fraction algorithm to the element $\alpha = \sqrt{D}$. Also, there are symmetries with respect to the period and to the quasi-period. Throughout, let k be a field of characteristic different from 2, and let $\alpha \in L - k(x)$ with

$$\alpha = \sqrt{\Delta} \quad , \ 0 < \deg(\Delta) \quad \text{even} \ , \tag{4.1}$$

where Δ is not a perfect square. Of course, α is a real quadratic irrationality in the sense of (3.1), where $P = 0$, $Q = 1$ and $1|(\Delta - 0^2)$. Also, note that the case $\alpha = \sqrt{D}$ is included in these considerations, since D is squarefree.

Furthermore, we assume that the continued fraction expansion of α is periodic. For example, this is true if k is a finite field. We easily see that α is not reduced. However, we know from Theorem 3.2 that α_i is reduced for $i \in \mathbb{N}$. Theorem 3.4 implies that the period starts at $\nu_0 = 1$. If $c \in k^*$ is such that

$$\alpha_{1+m} = c\,\alpha_1 \qquad \text{and} \qquad \alpha_{1+n} = \alpha_1 \ , \tag{4.2}$$

then $\alpha_{i+n} = \alpha_i$ for $i \in \mathbb{N}$. Results concerning periodicity can be deduced in the same way as for real numbers. We list them without proof.

Theorem 4.1. *If the continued fraction expansion of $\alpha = \sqrt{\Delta}$ is periodic with period n, then we have the following symmetries:*

$$
\begin{aligned}
a_n &= 2a_0 && , \\
a_i &= a_{n-i} && (\, i = 1, \ldots, n-1 \,) , \\
\alpha_{i+1} &= -\frac{1}{\overline{\alpha}_{n-i}} && (\, i = 0, \ldots, n-1 \,) , \\
P_{i+1} &= P_{n-i} && (\, i = 1, \ldots, n-1 \,) , \\
Q_i &= Q_{n-i} && (\, i = 1, \ldots, n \,) .
\end{aligned}
$$

In particular, we have $Q_{\lambda n} = Q_n = Q_0 = 1$ for $\lambda \geq 1$.

The additional fact of the theorem provides us with a criterion to recognize the period. Now, we give an analogous criterion to recognize the quasi-period.

Theorem 4.2. *If the continued fraction expansion of $\alpha = \sqrt{\Delta}$ is periodic with period n and quasi-period m, then $Q_s \in k^*$ if and only if $s = \lambda m$ for some $\lambda \geq 0$.*

Proof. Let $s = \lambda m$. If $\lambda = 0$ or $n = m$, then there is nothing to show. Now, let $n = lm$ where $l \geq 2$. Defining $c_m = c^{(-1)^{m-1}}$, we see from Proposition 3.2 that

$$Q_m = c_m^{1+(-1)^m+\ldots+(-1)^{(\lambda-2)m}} \, Q_{\lambda m} \quad (\lambda \geq 2) \, . \tag{4.3}$$

Therefore, we only have to prove that $Q_m \in k^*$. But, the assertion follows from the same result with $\lambda = l$ and $Q_{lm} = Q_n = 1$. Conversely, let $Q_s \in k^*$. If $s = 0$, then the assertion is true. Therefore, let $s \geq 1$. We have to show that $m = s$. From the first assertion we have that $m \geq s$, because $Q_m \in k^*$. It suffices to show that $\alpha_{s+1} = c\alpha_1$, since then $m \leq s$. First, we know that $P_0 = 0$, $Q_0 = 1$, $a_0 = d = \lfloor \sqrt{\Delta} \rfloor$, $P_1 = d$, and $Q_1 = \Delta - d^2$. Furthermore, $\alpha_s = (P_s + \sqrt{\Delta})/Q_s = (P_s + \sqrt{\Delta})/c$ is reduced. This means that $|\overline{\alpha}_s| = |P_s - \sqrt{\Delta}\,| < 1$. Consequently $P_s = \lfloor \sqrt{\Delta} \rfloor = d$ and $a_s = 2d/c$. Also, $P_{s+1} = d = P_1$ and $Q_{s+1} = Q_1/c$. We get $\alpha_{s+1} = c\alpha_1$ and the assertion is proved. □

Corollary 4.1. *In the situation of Theorem 4.2 we have that*

$$N(\,\overline{\theta}_{\lambda m+1}\,) = p_{\lambda m-1}^2 - \Delta\, q_{\lambda m-1}^2 \,\in\, k^* \qquad (\,\lambda \geq 1\,) \, .$$

Proof. See (3.9), (2.13), and Theorem 4.2. □

Lemma 4.1. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m. Then, for every $\lambda \geq 1$ there exists a constant $c(\lambda) \in k^*$ such that*

$$\overline{\theta}_{\lambda m+1} \;=\; c(\lambda)\,(\,\overline{\theta}_{m+1}\,)^{\lambda}\;.$$

Proof. From Lemma 2.1 we get for $i \in \mathbb{N}$ that

$$\alpha_{i+\lambda m} = c_i^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}}\;\alpha_i\;,$$

where $c_i := c^{(-1)^{i-1}}$. By (2.12) we derive that

$$\prod_{j=\lambda m+1}^{\lambda m+m}\frac{1}{\overline{\alpha}_j} = \prod_{j=1}^{m}\frac{1}{\overline{\alpha}_{\lambda m+j}} = \hat{c}\cdot\overline{\theta}_{m+1}\;,$$

where

$$\hat{c} \;=\; \prod_{j=1}^{m} c_j^{-1-(-1)^m-\ldots-(-1)^{(\lambda-1)m}}\;.$$

Then, the assertion easily follows by induction. □

Now, we use symmetries with respect to the period to derive relations between the period and the quasi-period.

Theorem 4.3. *Let the continued fraction expansion of the element $\alpha = \sqrt{\Delta}$ be periodic with period n.*

1. *If there exists an index ν, $1 \leq \nu \leq n-1$, such that $P_\nu = P_{\nu+1}$, then $n = 2\nu$. Conversely, if $n = 2\nu$ for some $\nu \in \mathbb{N}$, then $P_\nu = P_{\nu+1}$.*

2. *If there exists an index μ, $0 \leq \mu \leq n-1$, such that $Q_\mu = Q_{\mu+1}$, then $n = 2\mu+1$. Conversely, if $n = 2\mu+1$ for some $\mu \in \mathbb{N}_0$, then $Q_\mu = Q_{\mu+1}$.*

Proof. Easy. See [Per13, p.24]. □

Corollary 4.2. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m. Then there are three cases that can occur:*

1. *$n = m$ odd;*

2. *$n = m$ even;*

3. *$n = 2m$ even, m odd.*

Proof. If the period n is odd, then we know from Corollary 2.1 that $n = m$, and thus both m and n are odd. Now, let n be even and $n \neq m$. First, we know from Proposition 2.1 that $n = l \cdot m$ with $l \geq 2$. We get

$$\begin{aligned} P_{m+1} &= P_{(l-1)m+1} && \text{from Proposition 3.2,} \\ &= P_{n-(l-1)m} && \text{from Theorem 4.1,} \\ &= P_m \ , \end{aligned}$$

because $n = l \cdot m$. From Theorem 4.3 we deduce that $n = 2m$. Assuming that $m = 2s$ even, we conclude as above that

$$P_{s+1} = P_{m+s+1} = P_{n-(m+s)} = P_s \ ,$$

since $n-(m+s) = 2m-(m+s) = m-s = 2s-s = s$. Again, we deduce that $n = 2s = m$, which contradicts the fact that $n \neq m$. Therefore, m is odd. □

Note that all three cases do occur and that there is exactly one nontrivial case, i.e. one case where the period is different from the quasi-period. Next, we develop symmetries with respect to the quasi-period.

Theorem 4.4. *If the continued fraction expansion of $\alpha = \sqrt{\Delta}$ is periodic with period n and quasi-period m, then we have the following symmetries with respect to the quasi-period:*

$$P_{i+1} = P_{m-i} \qquad (\ i = 0, \ \dots\ , \ m-1\ )\ ,$$

$$Q_i = c^{(-1)^{i-1}} \cdot Q_{m-i} \qquad (\ i = 0, \ \dots\ , \ m\ )\ ,$$

$$-\frac{1}{\overline{\alpha}_{m-i}} = c^{(-1)^i} \cdot \alpha_{i+1} \qquad (\ i = 0, \ \dots\ , \ m-1\ )\ ,$$

where $c \in k^*$ is given as in (4.2).

Proof. If $n = m$, then there is nothing to prove, because the symmetries can be deduced from Theorem 4.1 with $c = 1$. Therefore, let $n = 2m$, m odd. From Proposition 3.2 we have that

$$P_{i+1} = P_{i+m+1} \qquad \text{and} \qquad Q_i = c^{(-1)^{i-1}} \cdot Q_{i+m} \ .$$

Furthermore, we know from Theorem 4.1 that

$$P_{i+m+1} = P_{n-(i+m)} \qquad \text{and} \qquad Q_{i+m} = Q_{n-(i+m)} \ ,$$

and the symmetries hold true, since $n = 2m$. The index transformation $i \to i+1$ for Q_i and (3.3) leads to

$$c^{(-1)^i} \cdot \alpha_{i+1} = c^{(-1)^i} \cdot \left(\frac{P_{i+1} + \sqrt{\Delta}}{Q_{i+1}} \right) = \frac{P_{m-i} + \sqrt{\Delta}}{Q_{m-i-1}} = -\frac{1}{\overline{\alpha}_{m-i}} \ .$$

□

Theorem 4.5. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m.*

1. *If there exists an index ν, $1 \le \nu \le m-1$, such that $P_\nu = P_{\nu+1}$, then $m = 2\nu = n$. Conversely, if $m = 2\nu$ for some $\nu \in \mathbb{N}$, then $P_\nu = P_{\nu+1}$ and $n = m$.*

2. *If there exists an index μ, $0 \le \mu \le m-1$, such that $Q_{\mu+1} = c' \cdot Q_\mu$, where $c' \in k^*$, then $m = 2\nu + 1$. If in addition $c' = 1$, then $n = m$. If $c' \neq 1$, then $n = 2m$. Conversely, if $m = 2\mu + 1$ for some $\mu \in \mathbb{N}_0$, then there exists a $c' \in k^*$ such that $Q_{\mu+1} = c' \cdot Q_\mu$.*

Proof. If $P_\nu = P_{\nu+1}$, then we know from Theorem 4.3 that $n = 2\nu$. Since $\nu \le m-1$, Corollary 4.2 tells us that $m = 2\nu = n$. Conversely, if $m = 2\nu$, then we conclude from Corollary 4.2 that $n = m$, and the assertion follows from Theorem 4.3. To prove the second statement we use (3.3) and Theorem 4.4 to derive that

$$\alpha_{m-\mu} = \frac{P_{m-\mu} + \sqrt{\Delta}}{Q_{m-\mu}} = c^{(-1)^{\mu-1}} \cdot \left(\frac{P_{\mu+1} + \sqrt{\Delta}}{Q_\mu} \right) = c' \cdot c^{(-1)^{\mu-1}} \cdot \alpha_{\mu+1} \ .$$

Because m is minimal with this property we deduce that $m - \mu = \mu + 1$, or, equivalently, that $m = 2\mu + 1$ odd. The final part is trivial. □

We wish to finish the continued fraction algorithm at about $m/2$ steps in the continued fraction expansion. In this context, we have to consider different constants. We use the constant $c \in k^*$ of (4.2) only for theoretical purposes. The further constant $c' \in k^*$ can be determined after half of the quasi-period has been computed:

$$c' = \frac{\operatorname{sgn}(Q_{\mu+1})}{\operatorname{sgn}(Q_\mu)} .$$

We need the further constant

$$c(\mu) = \prod_{j=0}^{\mu} c^{(-1)^j} \qquad \in k^* . \tag{4.4}$$

The following remark shows how $c(\mu)$ can be computed and how it is related to c, c'.

Remark 4.1. *In above notation we get:*

1. $c' = c^{(-1)^\mu}$,

2. $c(\mu) = \begin{cases} c' & , \quad \mu \text{ even} \\ 1 & , \quad \mu \text{ odd} \end{cases} .$

Proof. Easy. □

Finally, we are able to formulate the duplication formulas. They are based on symmetries with respect to the quasi-period.

Theorem 4.6. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m.*

1. *If there exists an index ν, $1 \le \nu \le m-1$, such that $P_\nu = P_{\nu+1}$, then we have that*

$$\overline{\theta}_{m+1} = (-1)^\nu \cdot \frac{\overline{\theta}_{\nu+1}}{\theta_{\nu+1}} = \frac{\overline{\theta}_{\nu+1}^{\,2}}{Q_\nu} = \frac{Q_\nu}{\theta_{\nu+1}^2} .$$

2. *If there exists an index μ, $0 \le \mu \le m-1$, such that $Q_{\mu+1} = c' \cdot Q_\mu$, where $c' \in k^*$, then we have that*

$$\overline{\theta}_{m+1} = c(\mu) \cdot \frac{\overline{\theta}_{\mu+1}\overline{\theta}_{\mu+2}}{Q_{\mu+1}} = -c(\mu) \cdot \overline{\theta}_{\mu+1}^{\,2} \frac{\overline{\alpha}_{\mu+1}}{Q_\mu} = -c(\mu) \cdot \frac{\alpha_{\mu+1} Q_\mu}{\theta_{\mu+1}^2} ,$$

where $c(\mu)$ is defined as above.

Proof. In the first case, we know from Theorem 4.5 that $n = m = 2\nu$. By using Theorem 4.4, we get

$$\prod_{j=\nu+1}^{m} \frac{1}{\overline{\alpha}_j} = \prod_{j=0}^{\nu-1} \frac{1}{\overline{\alpha}_{m-j}} = \prod_{j=0}^{\nu-1}(-\alpha_{j+1}) = \frac{(-1)^\nu}{\theta_{j+1}} .$$

Thus,

$$\overline{\theta}_{m+1} = \prod_{j=1}^{m} \frac{1}{\overline{\alpha}_j} = \prod_{j=1}^{\nu} \frac{1}{\overline{\alpha}_j} \cdot \prod_{j=\nu+1}^{m} \frac{1}{\overline{\alpha}_j} = \overline{\theta}_{\nu+1} \cdot \frac{(-1)^\nu}{\theta_{\nu+1}} .$$

This proves the first equality. The other equalities follow from (3.9). In the second case, we see that $n = 2\mu + 1$. Let $c \in k^*$ as in (4.2) and $c(\mu)$ as in (4.4). Again, by using Theorem 4.4 and (2.12) we get

$$\prod_{j=\mu+1}^{m} \frac{1}{\overline{\alpha}_j} = \prod_{j=0}^{\mu} \frac{1}{\overline{\alpha}_{m-j}} = \frac{(-1)^{\mu+1} \cdot c(\mu)}{\theta_{\mu+2}} .$$

Thus,

$$\overline{\theta}_{m+1} = \prod_{j=1}^{m} \frac{1}{\overline{\alpha}_j} = \prod_{j=1}^{\mu} \frac{1}{\overline{\alpha}_j} \cdot \prod_{j=\mu+1}^{m} \frac{1}{\overline{\alpha}_j} = \overline{\theta}_{\mu+1} \cdot \frac{(-1)^{\mu+1} \cdot c(\mu)}{\theta_{\mu+2}} .$$

The statements can now be derived from (3.9) and the fact that

$$\frac{1}{\overline{\alpha}_{\mu+1}} = -\alpha_{\mu+1} \cdot \frac{Q_{\mu+1}}{Q_\mu} \qquad . \tag{4.5}$$

□

Since we are also interested in the degree of $\overline{\theta}_{m+1}$, or more generally in the degree of θ_{i+1}, we introduce the positive numbers

$$A_{i+1} = \sum_{j=1}^{i} \deg(a_j) \quad (i \in \mathbb{N}) . \tag{4.6}$$

By (2.12) and (3.9), we see that

$$A_{i+1} = -\deg(\theta_{i+1}) = \deg(\overline{\theta}_{i+1}) + \deg(Q_i) . \tag{4.7}$$

Corollary 4.3. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m.*

1. *If there exists an index ν, $1 \leq \nu \leq m-1$, such that $P_\nu = P_{\nu+1}$, then we have that*

$$\deg(\overline{\theta}_{m+1}) = 2\deg(\overline{\theta}_{\nu+1}) - \deg(Q_\nu) = 2A_{\nu+1} + \deg(Q_\nu) \ .$$

2. *If there exists an index μ, $0 \leq \mu \leq m-1$, such that $Q_{\mu+1} = c' \cdot Q_\mu$, where $c' \in k^*$, then we have that*

$$\deg(\overline{\theta}_{m+1}) = 2\deg(\overline{\theta}_{\mu+1}) - \deg(Q_\mu) + \deg(a_{\mu+1}) = 2A_{\mu+1} + \deg(\sqrt{\Delta}) \ .$$

Proof. We can immediately derive the statements from Theorem 4.6. Note that for the second equality in the second statement we apply Proposition 3.1 to derive that

$$\deg(\sqrt{\Delta}) = \deg(a_{\mu+1}) + \deg(Q_{\mu+1}) = \deg(a_{\mu+1}) + \deg(Q_\mu) \ ,$$

since we must have that $Q_{\mu+1} = c' \cdot Q_\mu$ in this case. □

Corollary 4.4. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m.*

1. *If there exists an index ν, $1 \leq \nu \leq m-1$, such that $P_\nu = P_{\nu+1}$, then we have that*

$$\begin{aligned} p_{m-1} &= p_{\nu-1}q_{\nu-2} + p_\nu q_{\nu-1} \qquad , \\ q_{m-1} &= q_{\nu-1}(q_\nu + q_{\nu-2}) \ . \end{aligned}$$

2. *If there exists an index μ, $0 \leq \mu \leq m-1$, such that $Q_{\mu+1} = c' \cdot Q_\mu$, where $c' \in k^*$, then we have that*

$$\begin{aligned} p_{m-1} &= \frac{c(\mu)}{c'} \cdot (p_\mu q_\mu + c' p_{\mu-1} q_{\mu-1}) \qquad , \\ q_{m-1} &= \frac{c(\mu)}{c'} \cdot (q_\mu^2 + c' q_{\mu-1}^2) \ , \end{aligned}$$

where $c(\mu)$ is defined in (4.4).

Proof. In the first case, we have $m = n = 2\nu$, and we can apply Theorem 4.6 with

$$Q_\nu \cdot \overline{\theta}_{m+1} = \overline{\theta}_{\nu+1}^2 \ .$$

By equating rational and irrational parts, we deduce from (2.13) that

$$\left\{ \begin{aligned} Q_\nu p_{m-1} &= p_{\nu-1}^2 + q_{\nu-1}^2 \Delta \\ Q_\nu q_{m-1} &= 2p_{\nu-1} q_{\nu-1} \end{aligned} \right\}$$

Hence, by (3.9) and (3.8), we have that

$$Q_\nu p_{m-1} = (-1)^\nu Q_\nu + q_{\nu-1}(p_{\nu-1} 2P_\nu + 2p_{\nu-2} Q_\nu) \ .$$

From (3.2) and the fact that $P_\nu = P_{\nu+1}$ we derive that $a_\nu Q_\nu = 2P_\nu$. Therefore, we can delete Q_ν on both sides. Then the assertion for p_{m-1} follows from (2.10) and (2.5). Again, by (3.8) and the above equation, we see that

$$Q_\nu q_{m-1} = q_{\nu-1}(q_{\nu-1} 2P_\nu + 2q_{\nu-2} Q_\nu) \ .$$

Because $a_\nu Q_\nu = 2P_\nu$, we delete Q_ν on both sides. Then the assertion follows from (2.5). In the second case, we have that $m = 2\mu + 1$, and we can apply Theorem 4.6 with

$$Q_{\mu+1} \cdot \overline{\theta}_{m+1} = c(\mu) \cdot \overline{\theta}_{\mu+1} \cdot \overline{\theta}_{\mu+2} \ .$$

By using the same reasoning as above, we get

$$\left\{ \begin{aligned} Q_{\mu+1} \cdot p_{m-1} &= c(\mu)(p_{\mu-1} p_\mu + q_{\mu-1} q_\mu \Delta) \\ Q_{\mu+1} \cdot q_{m-1} &= c(\mu)(p_{\mu-1} q_\mu + q_{\mu-1} p_\mu) \end{aligned} \right\} \ .$$

Hence, by (3.8) and (3.2), we have that

$$Q_{\mu+1} \cdot p_{m-1} = c(\mu)(p_{\mu-1} q_\mu a_\mu Q_\mu + p_{\mu-1} q_{\mu-1} Q_{\mu+1} + p_{\mu-2} Q_\mu q_\mu) \ .$$

Since $Q_{\mu+1} = c' \cdot Q_\mu$, we can delete Q_μ on both sides. Together with (2.5) we see that

$$c' p_{m-1} = c(\mu)(q_\mu p_\mu + c' q_{\mu-1} p_{\mu-1}) \ .$$

By using (3.8) twice, we get

$$Q_{\mu+1} \cdot q_{m-1} = c(\mu)(q_\mu^2 Q_\mu + q_{\mu-1}^2 Q_{\mu+1}) \ .$$

Replacing $Q_{\mu+1}$ by $c' \cdot Q_\mu$ and deleting Q_μ on both sides leads to

$$c' q_{m-1} = c(\mu)(q_\mu^2 + c' q_{\mu-1}^2) \ .$$

□

5 Fundamental Unit and Regulator

Let $K = \mathbb{F}_q(x)(\sqrt{D})$ be a real quadratic function field over the finite field $\mathbb{F}_q$ of odd characteristic, where $D \in \mathbb{F}_q[x]$ is a monic, squarefree polynomial of even degree. From Theorem 3.3 we know that the continued fraction expansion of $\alpha = \sqrt{D}$ is periodic and quasi-periodic. The computation of the fundamental unit and the regulator of K is based on a standard result of Artin. We sketch its proof in our terminology. Also, we use the symmetries of the previous section. First, we need a simple remark.

Remark 5.1. *Let $\eta = U + V \cdot \sqrt{D} \in \mathcal{O}_K$, where $U, V \in \mathbb{F}_q[x]$. Then η is a unit in $\mathcal{O}_K$ if and only if $N(\eta)$ is a trivial unit, i.e. $N(\eta) \in k^*$.*

Proof. see [Art24, p. 195]. □

Theorem 5.1. *Let $D \in \mathbb{F}_q[x]$ be a monic, squarefree polynomial of even degree. Then the continued fraction expansion of $\alpha = \sqrt{D}$ is periodic and quasi-periodic. If m denotes the quasi-period, then*

$$\epsilon = p_{m-1} + q_{m-1} \cdot \sqrt{D}$$

is a fundamental unit of $K = \mathbb{F}_q(x)(\sqrt{D})$ and

$$E = k^* \times \langle\, \overline{\theta}_{m+1} \,\rangle = k^* \times \langle\, p_{m-1} + q_{m-1} \cdot \sqrt{D} \,\rangle \ .$$

Proof. The second equality follows from (2.13). We have to show that $E = k^* \times \langle\, \overline{\theta}_{m+1} \,\rangle$. " $\subseteq$ " is an easy consequence of Corollary 4.1 and the above remark. To show " $\supseteq$ " we choose an arbitrary unit $\eta = U + V \cdot \sqrt{D} \in E$, where $U, V \in \mathbb{F}_q[x]$. If $|\eta| = 1$, then the assertion is trivial. Let $|\eta| > 1$. In a first step, we prove that there exists a $c_0 \in k^*$ and an index $j \geq 0$ such that

$$U = c_0 \cdot p_{j-1} \qquad , \qquad V = c_0 \cdot q_{j-1} \ .$$

From the above remark we know that $N(\eta) \in k^*$. On the other side,

$$N(\eta) = U^2 - V^2 \cdot D = c_0^2 \left(p_{j-1}^2 - q_{j-1}^2 \cdot D \right) = c_0^2 \cdot (-1)^j \cdot Q_j \ ,$$

by (3.9). That means $Q_j \in k^*$. Theorem 4.2 and Lemma 4.1 then imply that

$$\eta = \hat{c} \cdot \overline{\theta}_{m+1}^{\,t} \ ,$$

with $\hat{c} \in k^*$ and $t \in \mathbb{N}$. If $|\eta| < 1$, then $|\overline{\eta}| = |\frac{1}{\eta}| > 1$, and we use $1/\eta$ instead of η. □

Corollary 5.1. *In the situation of Theorem 5.1, we have that*

$$R = \deg(\overline{\theta}_{m+1}) = A_{m+1} \ ,$$

where R is the regulator of K/k with respect to $\mathcal{O}_K$, and A_i is defined in (4.6).

Proof. The first equality follows from Theorem 5.1, since the regulator is defined to be the degree of the fundamental unit. The second equality is a consequence of (4.7) and Theorem 4.2. We have $Q_m \in k^*$, and therefore $\deg(Q_m) = 0$, $\deg(a_m) = \deg(\Delta)/2$. □

From the above theorem and corollary we derive algorithms to compute the fundamental unit and the regulator of K. quasi-period. For the fundamental unit, we calculate recursively the quantities a_i, r_i, p_i, q_i, P_i, Q_i, where we use (2.5) and the optimized formulas in (3.7). We terminate the algorithm as soon as one of the conditions of Corollary 4.4 is satisfied. To calculate the regulator, we don't need the quantities p_i, q_i. Instead, we calculate the additional quantities A_i. Note that the A_i's are nonnegative integers. It is a great advantage to avoid the computation of the polynomials p_i and q_i, because they both increase in its degree. This can be deduced from (2.6). Whereas, we see from Proposition 3.1 that a_i, r_i, P_i, Q_i are bounded in its degree because α_i is reduced ($i \in \mathbb{N}$). To stop the regulator algorithm we use the conditions of Corollary 4.3. This iterative process is known as the *baby step algorithm.*

References

[AR80] W. W. Adams and M. J. Razar. Multiples of points on elliptic curves and continued fractions. *Proc. London Math Soc.*, 41:481–498, 1980.

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

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

[KW90] P. Kaplan and K. S. Williams. The distance between ideals in the orders of a real quadratic field. *Enseign. Math.*, 36(3-4):321–358, 1990.

[Per13] O. Perron. *Die Lehre von den Kettenbrüchen.* Teubner, Leipzig, 1913.

[Ros93] K. H. Rosen. *Elementary Number Theory and its Applications.* Addison Wesley, Reading, Massachusetts, third edition edition, 1993.

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

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

[SW88a] A. Stephens and H. C. Williams. Computation of real quadratic fields with class number one. *Mathematics of Computation*, 51:809–824, 1988.

[SW88b] A. Stephens and H. C. Williams. Some computational results on a problem concerning powerful number. *Mathematics of Computation*, 50:619–632, 1988.

[Wei63] E. Weiss. *Algebraic Number Theory.* McGraw-Hill Book Company, New York, 1963.

[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.